Ю.Н. Федоров

СПРАВОЧНИК ИНЖЕНЕРА ПО АСУТП:

ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА

«Инфра-Инженерия»

АН08

Ю.Н. Федоров

СПРАВОЧНИК ИНЖЕНЕРА ПО АСУТП: Проектирование и разработка

Учебно-практическое пособие

Инфра-Инженерия
Москва
2008

УДК (665.6/.7:681.5).002.2
ББК 35.514: 32.965
Ф33

Федоров Ю.Н.
Справочник инженера по АСУТП: Проектирование и разработка. *Учебно-практическое пособие. - М.: Инфра-Инженерия, 2008. -928 стр., 12 ил.*

Справочник задает систему базовых определений и требований, выполнение которых реализуется в правилах создания АСУТП. Даются рекомендации по выбору архитектуры автоматизированных систем управления и защиты технологических процессов. Последовательно определяется состав и распределение работ по созданию АСУТП, устанавливается состав и содержание проектной документации.

Достоинством книги является её практическая направленность. Процедуры выполнения работ по проектированию и разработке АСУТП, рекомендации по учету особенностей проектирования систем защиты технологических процессов окажут методическую помощь всем, кто связан с этими проблемами - от разработчиков систем, до руководителей предприятий. Вместе с тем, книга может использоваться в качестве учебного пособия для преподавателей и студентов высших и средних специальных учебных заведений соответствующих специальностей.

Представленная в работе методология создания АСУТП является шагом к разработке современных отечественных стандартов промышленной автоматизации, согласованных с международным опытом.

Рецензенты:
Э.Л. Ицкович - доктор технических наук, профессор, заведующий лабораторией Института проблем управления РАН.
Л.Р. Соркин - доктор технических наук, профессор, заведующий кафедрой Московского физико-технического института.

ISBN 978-5-9729-0019-0

Произведения всех действительно даровитых голов отличаются от остальных характером решительности и определённости, и вытекающими из них отчётливостью и ясностью. Ибо такие головы всегда определённо и ясно сознают, что они хотят выразить, - всё равно, будет ли это проза, стихи или звуки. Этой решительности и ясности недостаёт прочим, и они тотчас же распознаются по этому недостатку. Характеристический признак первостепенных умов есть непосредственность всех их суждений и приговоров. Всё, что они производят, есть результат их самособственного мышления, который повсюду обнаруживается как таковой уже в самом изложении.

Артур Шопенгауэр,
Максимы: О самостоятельном мышлении

ПРЕДИСЛОВИЕ

В настоящей работе предлагается система правил создания АСУТП на основе авторского опыта проектирования, разработки, внедрения, эксплуатации и сопровождения АСУТП с максимально возможным учетом существующей отечественной нормативной базы. Даются точные определения ключевых понятий, без знания и понимания которых невозможно приступить к результативному созданию системы:

- Определение стадий и этапов создания АСУТП
- Определение состава организаций-участников проекта создания АСУТП;
- Определение состава документации технического и рабочего (технорабочего) проектов;
- Определение требований и ограничений, имеющих решающее значение при создании надежных и безопасных систем управления и защиты.

Центральная часть книги посвящена жизненно важным аспектам построения АСУТП - формализации основных стадий создания АСУТП, разработке и оформлению проектной документации, - то есть комплексному и корректному проведению проектных и инженерных работ. Определяется состав и распределение работ по созданию АСУТП, приводятся образцы конкретной проектной и эксплуатационной документации технического и рабочего (технорабочего) проектов АСУТП. В две самостоятельные главы выделена часть проектной документации, посвященная стадиям, определяющим начало и завершение проекта создания АСУТП.

Отработанный на опыте практической реализации на многих технологических объектах образец "Технического задания на создание АСУТП" стал непосредственной основой при создании ряда АСУТП разного масштаба. Приводится "Программа и методика испытаний" с полным комплектом документов, необходимых при оформлении и утверждении результатов опытных и промышленных испытаний системы.

Исключительное по важности значение имеет изучение международных подходов к промышленной безопасности. Вместе с тем, исследование современных западных стандартов безопасности ANSI/ISA 84.01-96, DIN V 19520, V VDE 0801, IEC 61508, IEC 61511 приводит к определению границ применимости предлагаемых методик. Наиболее серьезным пробелом стандартов МЭК, - и в этом с автором солидарны ведущие западные эксперты, - является полное отсутствие оценок вероятности ложного срабатывания систем управления и защиты. Общие решения для систем произвольной архитектуры - и для вероятности опасного отказа, и для ложного срабатывания, - представлены в настоящей работе.

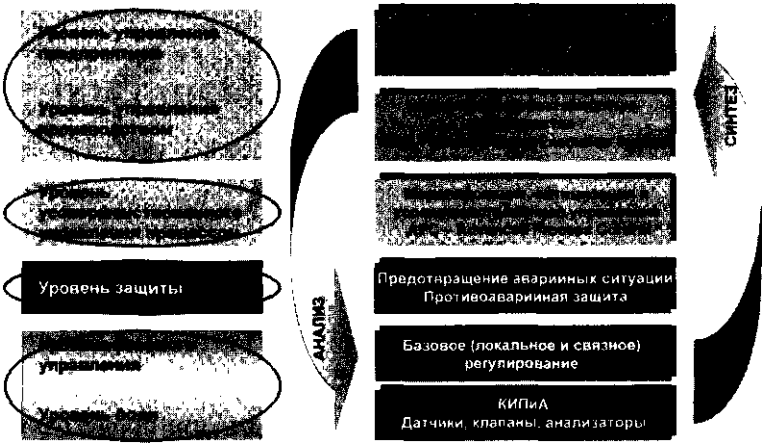
Здесь же делается анализ соответствия отечественных категорий взрывоопасное™, и зарубежных классов *(Requirement Class - RC, AnforderungsKlasse - AK)* по немецким стандартам DIN, и уровней безопасного допуска *(Safety Integrity Level - SIL)* по американским стандартам ISA, и по стандартам Международной электротехнической комиссии (IEC). Даются конкретные рекомендации по выбору архитектуры систем управления и защиты технологических объектов.

Самостоятельное значение имеет решение проблемы идентификации параметров АСУТП - проблемы, созданной на многие годы никудышным ГОСТом 21.404-85 "Обозначения условные приборов и средств автоматизации в схемах". На основе анализа существующих стандартов и методик предлагается система идентификации, которая отличается согласованностью и целесообразностью решений. Приводятся подготовленные к практическому использованию библиотеки символьных и графических элементов монтажно-технологических и функциональных схем автоматизации.

Можно много рассуждать о том, насколько представительны проектные оценки надежности автоматизированных систем. Однако будучи проведенными по единым методикам,

эти расчеты вполне позволяют сопоставить характеристики надежности различных конфигураций оборудования. Поэтому требование проектной оценки надежности системы должно стать обязательным компонентом Технического задания на создание АСУТП.

ИЕРАРХИЯ УРОВНЕЙ УПРАВЛЕНИЯ



По независимым оценкам фирм Honeywell и Yokogawa, экономический эффект от внедрения пакетов усовершенствованного управления составляет от 40% до 60% в общей доле прибыли от внедрения комплексных автоматизированных систем управления производством, со сроком окупаемости 6-12 месяцев. Невостребованность современных методов управления в лучшем случае низводит процесс создания АСУТП до тривиальной модернизации, не привнося никаких существенных улучшений.

Однако без современных средств КИПиА, без надежной системы базового управления и защиты невозможно перейти к реализации функций управления более высокого порядка.

Поэтому необходимо иметь дело с такими компаниями, которые могут выполнить весь спектр работ, **подтвержденный** на аналогичных производствах, и ориентироваться на долговременное сотрудничество. Успешно работающие предприятия - это успешно организованные предприятия, - от определения начальных условий, до сопровождения системы.

И если мы делаем правильный выбор, то результат практически предопределен. Можно даже сказать, что происходит инверсия действий по управлению проектом:

- Если начальные условия верны, то управление проектом сводится к тому, чтобы предотвращать действия, способные нарушить нормальный ход проекта.
- И наоборот: неверный изначальный выбор приводит к тому, что весь проект будет связан с поиском решений, способных хоть как-то спасти проект, и с постоянной угрозой провала. И никаких перспектив перепрыгнуть через барьер примитивной самозащиты.

Появление международных стандартов безопасности, определяющих особые требования к проектированию и конкретной реализации систем управления и защиты, связано с всё большим усложнением и технологических процессов, и средств автоматизации, и соответствующим увеличением риска и масштабов аварий на производстве.

Всё, что способно снизить уровень этих требований, должно рассматриваться как проявление легкомыслия и с профессиональной, и с социальной точки зрения, и с позиции коммерческих интересов.

Глава 1

ПОСТАНОВКА ЗАДАЧ АВТОМАТИЗАЦИИ

1.1. Область определения

В данной работе рассматриваются ключевые аспекты автоматизации технологических процессов, которые существенно пересекаются с проблемами развития отечественной нормативной базы (рис. 1.1). Работа является непосредственной основой для разработки:

- Стандартов предприятия по промышленной безопасности;
- Стандарта предприятия по созданию АСУТП;
- Технического задания на создание АСУТП;
- Комплекса технической и рабочей документации АСУТП;
- Программ и методик приемо-сдаточных испытаний.

1.2. Статистика причин инцидентов и аварий

По данным Инспекции по охране труда и здоровья HSE (Health Safety Executive), Великобритания, около 50% всех неприятностей, связанных с системами управления технологическими процессами, предопределяются ошибками спецификации (рис. 1.2). В отечественной практике постановку задач автоматизации и конкретные требования к системе управления и защиты технологического процесса определяет **Техническое задание на создание АСУТП.** Неформальное отношение к разработке ТЗ имеет исключительно важное значение для будущей системы: ни с того ни с сего кирпич на голову никому не упадет.

Область действия настоящего руководства в общей иерархии стандартов

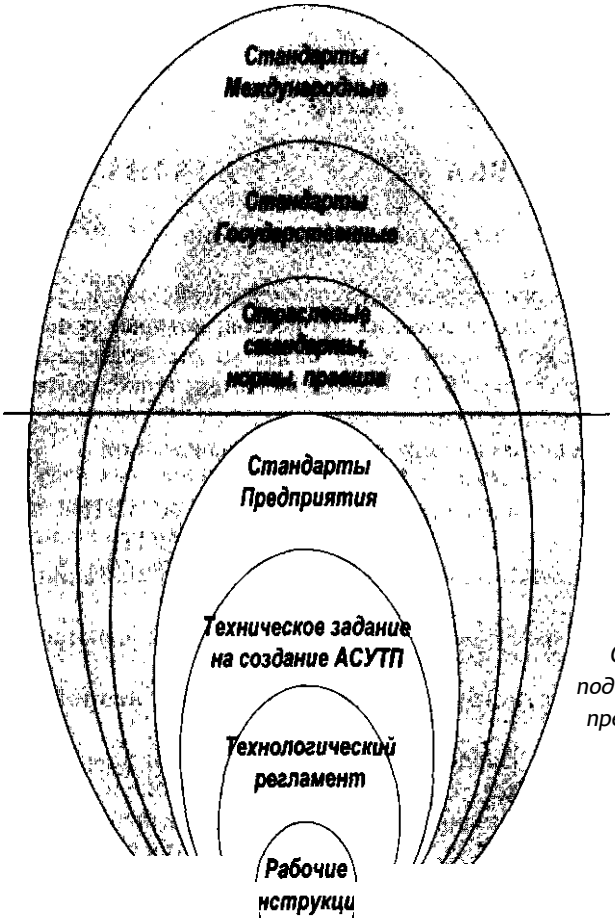


Рис. 1.1

Рис. 1.2

Однако Техническое задание охватывает только часть жизненного цикла системы - от первоначальной концепции до приемо-сдаточных испытаний. Принципы существования систем автоматизации в течение всего жизненного цикла в соответствии с диаграммой рис. 1.1 должны регламентироваться:

- Специфическими стандартами предприятия
- Отраслевыми стандартами
- Государственными стандартами
- Международными стандартами.

1.3. Общие положения

Современный подход к автоматизации заключается в формировании автоматизированных систем управления и защиты как главного элемента единой системы защиты процесса. Классическая система управления технологическими процессами (АСУТП) в самом общем виде объединяет в себе два взаимосвязанных компонента:

- Система ПротивоАварийной Защиты - ПАЗ
- Распределенная Система Управления - РСУ.

При непосредственном выборе и проектировании программно-технического комплекса часто рассматривается только центральная часть системы - основное оборудование АСУТП. При этом совершенно упускается из виду общая надежность контуров управления и защиты - функций безопасности, - начиная от датчиков, и заканчивая исполнительными устройствами.

Современные международные стандарты безопасной автоматизации предписывают рассматривать системы управления и защиты комплексно, целиком, причем одновременно и в самом широком и всестороннем смысле - как всеобъемлющие системы безопасности, и как конкретную систему для конкретного технологического объекта.

Ключевым аспектом современного подхода является концепция **жизненного цикла,** определяющая все этапы существования системы от зарождения идеи до списания. Современные стандарты дают возможность перейти от интуитивных представлений о достаточности той или иной архитектуры к количественным оценкам вероятности отказа, и дают соответствующие соотношения, позволяющие определить интегральную безопасность системы. В последние годы появились добротные отечественные нормативные документы по анализу рисков и оценке последствий отказов:

- РД 03-418-01 *"Методические указания по проведению анализа риска опасных производственных объектов";*
- ГОСТ 27.310-95 *"Анализ видов, последствий и критичности отказов"*

Согласно РД 03-418-01, из категорий и критериев тяжести отказов следует, что взрывоопасные объекты нефтегазодобывающей, химической, нефтехимической и нефтеперерабатывающей промышленности относятся к объектам, для которых **количественный анализ риска обязателен.**

Таким образом, у производственников появляется формальная основа для предъявления требований к поставщикам оборудования и разработчикам систем, соответствие которым будет обеспечивать приемлемый уровень риска в реальных обстоятельствах. Главные вопросы, на которые необходимо получить ответ, прежде чем приступить к реализации конкретного проекта, состоят в следующем:

1. Как обрести уверенность, что система обеспечит безопасность, то есть действительно выполнит заложенные функции защиты, когда в этом возникнет необходимость?
2. Как должна быть построена система, чтобы исключить возможность ложных, немотивированных остановов технологического процесса по вине оборудования системы?

3. Как должно быть организовано техническое обслуживание АСУТП (автономное тестирование, диагностика, самодиагностика), чтобы технологический персонал не растерял доверия к ее дееспособности?

Тенденция развития современных стандартов безопасности заключается в разработке формальных правил, методик, алгоритмов для оценки и сертификации уровня безопасности не просто для применяемого оборудования, но самой системы безопасности как комплексной системы защиты **конкретного** технологического процесса.

1.4. Специфика автоматизированных систем

Многие неприятности, связанные с системами зашиты, связаны с НЕ учетом специфики этих систем. Системы управления вообще, а системы противоаварийной защиты в особенности обладают рядом специфических свойств, присущих только этим системам:

1. Система защиты может формально находиться в работе, но в момент наступления опасного события на процессе не способна отреагировать на него. Подобный тип отказа принято называть **опасным отказом.**
2. Система защиты может совершить ложный немотивированный аварийный останов процесса, в то время как в действительности ничего опасного на процессе не произошло. Подобный тип отказа некоторые люди называют **"безопасным" отказом.**

Любой останов и запуск производства - это серьезные и ответственные операции, не говоря об экономических потерях. Процедура останова, предназначенная для защиты процесса, сама по себе представляет значительную опасность, ибо требует согласованного изменения состояния многих элементов технологического оборудования, и зависит от безупречного выполнения вполне определенных последовательностей операций - как автоматических, так и согласованных действий технологического персонала. Каждому, кто соприкасался с современными крупнотоннажными взрывоопасными технологическими процессами не надо объяснять, что любой останов - чрезвычайное происшествие на производстве, связанное с серьезным риском и для людей, и для оборудования.

Тем более, ложный останов, исходящий из системы, предназначенной для предотвращения аварийных ситуаций, - нонсенс, в причинах которого необходимо разобраться.

Особо подчеркивается, что в общей структуре отказов основную долю отказов несут полевые устройства. По данным TUV, см. *"Functional safety of programmable systems, devices & components: Requirements from global & national standards"* Matthias R. Heinze, Vice President Engineering TUV of North America, 0ct-2001, существует следующее распределение частоты отказов по главным компонентам систем защиты:

Тип устройства	**Отказы, %**
Датчик	35
Центральная часть системы (PLC)	15
Исполнительный элемент	50

Поэтому при создании систем безопасности основной упор должен делаться на модернизацию полевого оборудования, сертифицированного на применение в системах защиты, и с режимом оперативной диагностики в реальном времени. Реализация этой функции предоставляется специализированными системами обслуживания полевого оборудования - *Plant Asset Management Systems.* Появление этих систем стало возможным с созданием полевого оборудования, способного в режиме *on-line* взаимодействовать с системой обслуживания по гибридным аналогово-цифровым протоколам типа HART, или полностью цифровым протоколам типа Fieldbus.

Потенциальная возможность несрабатывания и ложного останова затрагивает самый сложный аспект безопасности, связанный с участием человека, или, говоря сугубо утилитарным современным языком, с мощнейшим воздействием так называемого "человеческого фактора". Люди - существенно нелинейные системы и вообще склонны к катастрофическому поведению. Именно человек является основным источником ошибок. И система безопасности должна строиться с учетом склонности людей к безрассудному поведению и неоправданному риску.

Вместе с тем, анализ применяемых схем защиты показывает, что повышенная вероятность опасных отказов и ложных срабатываний может быть заложена в систему изначально на этапе проектирования.

1.5. Стереотипы резервирования

Небольшой пример. Рассмотрим простейшую систему безопасности:

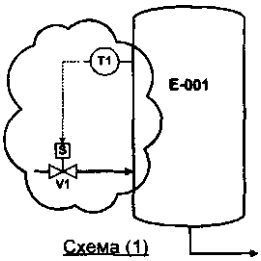


Рис. 1.3

Где T1 - некий датчик, V1 - отсечной клапан (это может быть, например, контур защиты от превышения уровня, или давления в некотором аппарате посредством отсечки поступающего в аппарат продукта).

Сделаем оценку вероятности ложных (нижний индекс S) срабатываний $P_s(1)$, и вероятности опасных (нижний индекс **D)** отказов $P_D(1)$ для данного контура. Вероятность ложных срабатываний и опасных отказов датчика :

$$P_S^T = P_S^{T1}$$

$$P_D^T = P_D^{T1}$$

Вероятность ложных срабатываний и опасных отказов клапана:

$$P_S^V = P_S^{V1}$$

$$P_D^V = P_D^{V1}$$

Тогда искомые вероятности ложных срабатываний и опасных отказов данного контура определяются простым сложением вероятностей данного события для составных элементов контура:

$P_S(V = PI+P_S{}^V$

$P_D(V\text{-}Po\text{^}Po$

Теперь допустим, что нас беспокоит проблема ложных срабатываний данного контура защиты.

Можно просто поставить дополнительный датчик, но мы с целью дальнейшего развития предусмотрим сразу АСУТП, состоящую из системы управления и системы защиты, которую мы будем строить с учетом так называемого "доведения до норм".

При этом предполагается, что система будет иметь свои собственные средства контроля и управления, независимые от системы ПАЗ с тем, чтобы контроль над состоянием процесса не терялся ни при каких обстоятельствах.

Допустим, что нам сказочно повезло, и мы выбрали центральную часть системы защиты - *программируемый логический контроллер*, - такой, что имеет **абсолютную надежность.** То есть ПЛК имеет нулевую вероятность всех мыслимых отказов, и имеет все мыслимые разрешения от всех мыслимых инспекций, включая разрешение на **безграничную одноканальную** работу по максимально возможному уровню допуска. Но мы для безоговорочной уверенности в защите поставим дублированный вариант ПЛК. Вероятность отказа этого чудо - компьютера

$P_s^{l}=PD=0,$

то есть он таков, что не оказывает никакого влияния на надежность системы. Это означает, что его как бы и нету. Так и будем считать.

Теперь с расчетом "доведения до норм" заложим в нашу систему два датчика, подключенных по схеме 1oo2, что означает, что для срабатывания системы защиты достаточно сигнала от одного из них (см. схему (2) на рис. 1.4). Обозначим:

$$pr\_pT1\_pT2$$
$$'O \sim D \sim\sim D$$

Работа по схеме 1oo2 имеет следующие особенности:

1. Для того чтобы система осуществила ложное срабатывание ("безопасный" отказ), достаточно, чтобы
   - Любой из сенсоров подал ложный сигнал (и клапан его отработал),
   - Либо клапан ложно сработал.
2. Для того чтобы система в нужный момент НЕ сработала (опасный отказ), необходимо, чтобы
   - Либо оба сенсора не сработали,
   - Либо отказал отсечной клапан.

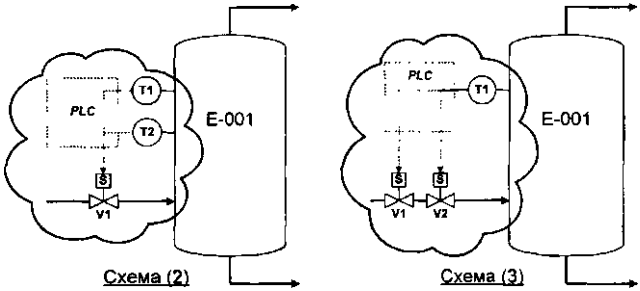


Рис. 1.4

Записываем логические выражения для вероятности каждого из этих событий. Для вероятности ложных срабатываний:

$$P_S(^2) = P^{T}_{S}{}^{1OO2}{}_{\sim}{}^{V1O\circ l} = 2\bullet PI + P_S{}^{L} + PL = 2 \quad PI + РГ$$

Для вероятности опасных отказов:

$$P_D(2j = Pl^{l}{}_{TM^2}{}_{-}{}''{}_{TM^1} = (PI\ f + {}_{R}l + pv = (pr\ f + pv$$

Пусть вероятности отказов датчика и отсекателя в течение 1 года равны $1.0>10^{3}$ (один из тысячи). Тогда

$$P_s(^2) = PI^{002\wedge 1001} = 2\ \ Pi + Pi = 2.0 \bullet 10\sim^{3} + 1.0\text{-}\ Ю\text{-}^{3} = 3.0 \bullet 10^{3}$$

$$P_d(2) = = fPj / + p^{*} = 1.0.10^{6} + 1.0\text{ -}10\sim^{3} =$$

$$= 1.000001\ \ 10\sim^{3} = 1.0\ \ 10\sim^{3}$$

Результат, мягко говоря, обескураживает. Рассчитывая улучшить общие показатели контура и поставив 2 датчика вместо одного, мы получили совершенно неожиданный результат:

Частота ложных срабатываний по вине датчика по сравнению с одноканальным вариантом возросла в два раза. Более того, если бы мы вообще не предпринимали никаких действий, результаты оказались бы, может, и не лучше, но и не хуже!

Ведь исходная схема (1) давала вполне сопоставимые значения:

$$P_3(1) = PI^{\circ\circ l\wedge 1001} = Pl + P1 = 1.0\ \ 10\sim^{3} + 1.0\ \ Ю\text{-}^{3}\ \text{-}2.0'\,10^{3}$$

$$P_D(V = Pl^{1001}\text{-}^{V1O\circ l} = P^{*} + P\% = 1.0\text{-}10\text{-}^{*} + 1.0 \bullet 10\sim^{3} = 2.0 \bullet Ю\text{-}^{3}$$

Посмотрим, что произойдет, если мы поставим второй отсекатель - схема (3) на рис. 1.4.

Получаем:

$P_s(3) \sim Pr^{\circ\circ 1} \sim^{V1002} = P^T_S + 2 - P^* = 1.0\ 10\sim^3 + 2.0\ 10\sim^3 =$

$= 3.0\ 10\sim^3$

$P_D(3) = Pl^{1001} -^{V1002} = P_D^r + (P\wedge)^2 = 1.0\ 10^* + 1.0 > 10^* =$

$= 1.000001\ 10\sim^3 = 1.0\text{-}10\sim^*$

То же, что и *для* схемы (2) .

Полученные результаты однозначно показывают, что при формировании спецификации требований к системе безопасности необходимо учитывать не просто характеристики надежности отдельных компонентов системы, но архитектуру и параметры всего контура безопасности для каждого контура безопасности - "от трубы до трубы". Именно это требуют современные международные стандарты безопасности.

Но пойдем дальше. Попробуем совместить достоинства схем (2) и (3), и поставим 2 датчика и 2 клапана. Количество вариантов архитектуры возрастает, но проверим хотя бы следующие два (рис. 1.5).

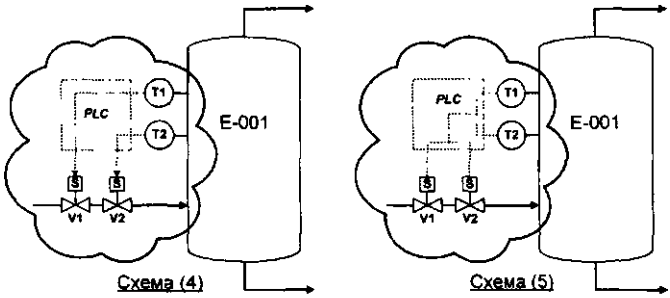


Рис. 1.5

Схема (4V

$P_8(4) = P^{*(T1OO1} -^{V1OO1)} = (PI + Pl) + (Pl + P^*) =$

$= 2.0\text{-}10\sim^3 + 2.0\text{-}10\sim^3 = 4.0\text{-}10^{\circ 3}$

$P_d(4) = p\ w\ w\ » = (Pi + Pi) \bullet (Pi + Pl) =$

$= 2.0\ \text{-}10^{\circ 3}\ \text{-}2.0'10\sim^3 = 4.0\ \text{-}10\sim^6$

Схема *(5):*

$P_s(5) = Pi^{1002} -^{\prime\prime 002} = 2\text{-}Pi + 2\ \text{-}Pi = 2.0\text{-}10\sim^3 + 2.0\text{-}10^{\circ 3} =$

$= 4.0\text{-}10\sim^3$

$$P_d(5) = P^t_d{}^{1oo2}\text{-}^{v1o\circ2} = (P^J_D f + (Pi)^2 = 1.0\text{-}fO''^6 + 1.010\sim^6 =$$
$$= 2.0\text{-}10\text{-}*$$

Обе схемы имеют отличные характеристики по опасным отказам (по несрабатыванию), но

Вероятность ложных срабатываний по сравнению с исходной одноканальной Схемой (1) **выросла в два раза!**

Картина будет неполной, если не посмотреть еще один вариант архитектуры, который, как будет показано в дальнейшем, играет ключевую роль в архитектурах систем безопасности типа loo2D. Это - классическая архитектура 2oo2. Система работает, когда оба канала работают (рис. 1.6).

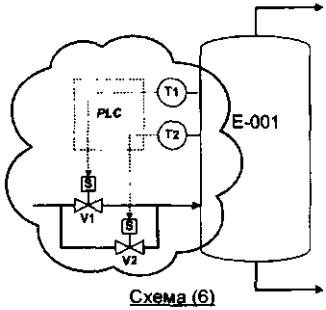


Схема (6)

Рис. 1.6

Схема (6):

$$P_s(6) = Pl^{2oo2,V2o\circ2} = (Pi + Pi)^2 = 4.0\text{-}Ю\text{-}^6$$
$$P_D(6) = Pl^{2oo2}\text{-}^{V2o\circ2} = 2 \quad (Pi + Pl4.0 \quad 10\sim^3$$

Наконец, нам удалось найти схему с минимальной вероятностью ложных срабатываний, но, к сожалению, с самой высокой вероятностью опасных отказов (несрабатывания в нужный момент) - **она в два раза выше одноканальной системы.** Выигрыш одного параметра означает проигрыш другого.

Вот такое "доведение до норм". Где же выход? Ведь полученные характеристики являются органическим свойством рассмотренных архитектур. И, как мы видим, установка самого современного ПЛК и дополнительного полевого оборудования вовсе не является гарантией увеличения надежности и безопасности системы защиты.

Как добиться баланса архитектур полевого оборудования и логических устройств, чтобы система безопасности была соразмерной и обеспечивала приемлемый уровень интегральной безопасности?

Попытка ответить на поставленные вопросы и делается в настоящей работе.

Простых решений не существует. И надо очень внимательно подходить к прямолинейным априорным решениям. Иначе эти решения могут привести совсем не к тем результатам, которые ожидались.

1.6. Стандарты промышленной безопасности МЭК

(IEC - International Electrotechnical Commission, Geneva, Switzerland)

Системы управления и защиты технологических процессов становятся все более сложными, и возникает серьезная проблема обоснованности применения электронных систем во всех отраслях промышленности, неизбежно связанных с опасностью. С появлением микроэлектронных средств автоматизации корректность их применения практически не поддается непосредственной проверке.

Исследования, проведенные Международной Электротехнической Комиссией в конце 80-х - начале 90-х годов, были направлены на разработку стандарта, который мог бы стать руководящим документом **для проектировщиков и разработчиков систем безопасности промышленных объектов,** позволяющим удостовериться, что электронные системы действительно обеспечивают приемлемую безопасность в предопределенных обстоятельствах.

Первый вариант стандарта под названием IEC 61508 "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems" (Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью) появился в 1995 году. Уже предварительный вариант стандарта получил международное признание. Формальное утверждение нового стандарта промышленной безопасности IEC 61508 "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems" состоялось в апрелё 2000 года.

Часть 1 стандарта IEC 61508, пункт 1Л, непосредственно определяет главную цель стандарта:

"Главной целью данного стандарта является содействие развитию прикладного сектора международных стандартов через технические комитеты, отвечающие за прикладной сектор. Это позволит принять во внимание все факторы, связанные с приложением, и тем самым ответить на специфические требования прикладного сектора. Параллельная цель этого стандарта - дать возможность развития Электрических / Электронных / Программируемых Электронных (E/E/PE) связанных с безопасностью систем в тех областях, в которых прикладной сектор международных стандартов отсутствует".

1.7. Жизненный цикл безопасности

Краеугольное понятие стандарта - понятие *Жизненного цикла безопасности.* В отличие от традиционного подхода к оценке системы на основе только выходных характеристик производителя или, в лучшем случае, во время приемосдаточных испытаний, IEC 61508 рассматривает все аспекты безопасности в течение всего цикла существования системы - от первоначальной концепции до списания.

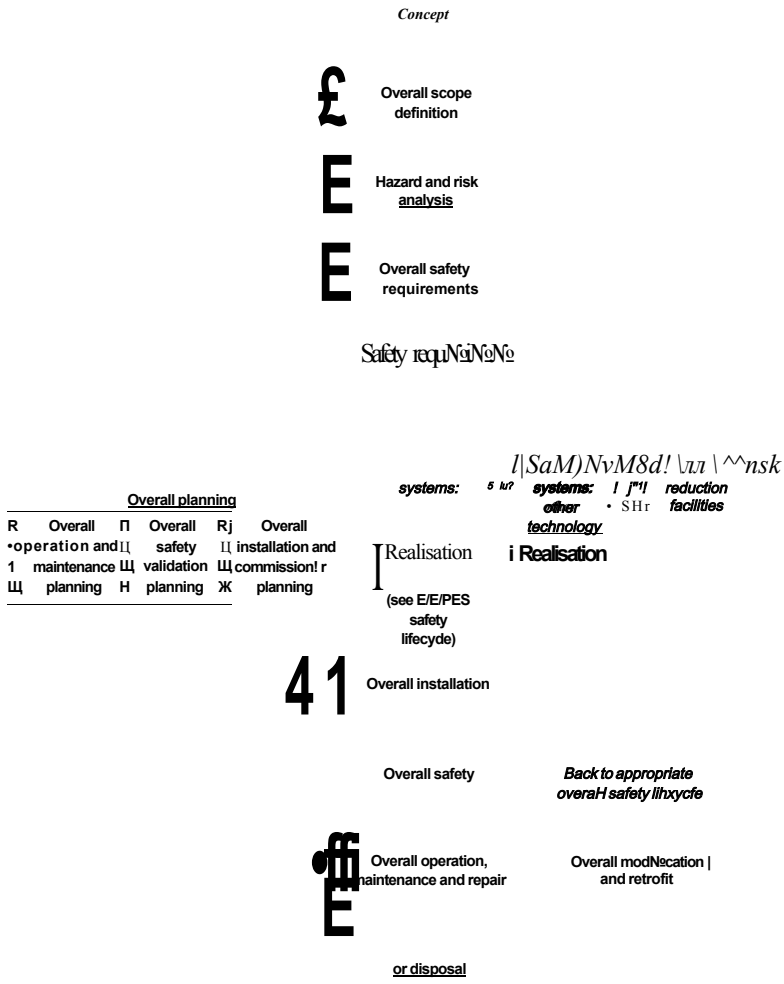
Влияние этого понятия на стандарт столь велико, что собственно сам стандарт построен в соответствии с этой моделью, и повторяет ее структуру (рис. 1.7).

1.8. Интегральная и функциональная безопасность

Стандарт отстаивает новый подход к общей (интегральной) и функциональной безопасности. Вместо того чтобы проектировать систему "*настолько хорошо, насколько это возможно*", а затем считать ее достаточно безопасной, стандарт предлагает подход, основанный на анализе рисков.

Все действия по обеспечению безопасности должны основываться на понимании и оценке риска, который неизбежно присутствует в любой системе. Стандарт подразделяет меры по снижению риска на два компонента:

- Общие, интегральные требования безопасности *{Safety integrity requirements).*
- Функциональные требования *{Functional requirements).*



NOTE 1 Activities relating to *\mtication, management ыймкХюоы safety and functi^* not shewn for reasons of clarity but are releuent to all overall. E/E/PES and softoore safety lifecyde phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope

NOTE3 Parts 2 and 3 deal vnth box 9 (realisation) but they also feal, vtfere relevant, wrth the programmable electronic (hardware and software) aspects of boxes 13,14 and 15

Рис. 1.7

Соответственно, Спецификация требований безопасности должна определять:

- Спецификацию требований интегральной безопасности, содержащую общие требования безопасности, которые должна обеспечивать система, и
- Спецификацию требований функциональной безопасности, содержащую требования к самим функциям (контурам) безопасности, которые должна выполнять система.

Небольшой комментарий

"Изысканные" формулировки и определения стандарта - именно таковы, и с этим приходится считаться.

Интегральный компонент определяется **Интегральным уровнем** безопасности - *Safety Integrity Level (SIL),* который задает требуемую меру снижения риска. Проще говоря, чем более ответственным является объект, тем более надежной должна быть система. То есть чем большее снижение риска требуется, тем более объект становится зависимым от самой системы защиты, обеспечивающей это снижение, и соответственно, тем большее значение SIL необходимо для общей безопасности.

1.9. Проектная документация

Важнейшим компонентом системы является полнота документации, которая давала бы исчерпывающее представление о системе в соответствии с реальным состоянием системы.

Стандарт IEC 61508-1 в Приложении А с подзаголовком "информативное" дает только общую концепцию комплекта, без детализации конкретного состава и содержания документов (рис. 1.8).

В последующих главах настоящей работы приводится состав и содержание полного комплекта документации Технического и Рабочего (Технорабочего) проекта по созданию АСУТП, подготовленного на основе авторского опыта проектирования, разработки, внедрения, эксплуатации и обслуживания АСУТП.

При этом ставилась задача максимально возможного использования существующей и вполне добротной отечественной нормативно-справочной базы:

- ГОСТ 34.601-90 ЕСС АСУ "Автоматизированные системы. Стадии создания".
- ГОСТ 24.104-85 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы управления. Общие требования.
- ГОСТ 34.003-90 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Термины и определения.
- ГОСТ 34.201-89 "Виды, комплектность и обозначение документов при создании автоматизированных систем".
- РД 50-34.698-90 "Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов".
- ГОСТ 34.602-89 "Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы".
- ГОСТ 34.603-92 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды испытаний автоматизированных систем.

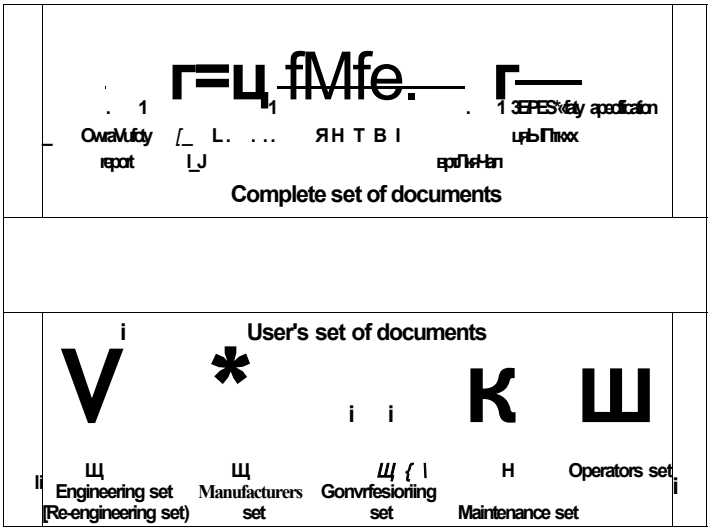


Рис. 1.8

1.10. Огрехи стандарта IEC 61508

Завышение оценок вероятности и частоты опасных отказов - PFD и PFH. Стандарт IEC 61508 подразделяет отказы системы безопасности на опасные и безопасные - обнаруженные и необнаруженные, - и в части 4 дает их определения. Стандарт в шестой части приводит соотношения для средней вероятности опасного отказа на запрос PFD_{AVG} в течение преопределенного межповерочного интервала (в отечественной практике - 1 год), и средней интенсивности (частоты) опасных отказов PFH_{AVG}, однако дает их без каких бы то ни было объяснений, откуда они взялись.

Примечание

Необходимо понимать, что все рассмотренные в стандарте модели систем безопасности в полной мере относятся:

- *И к конфигурации измерительных устройств,*
- *И к собственно логическим устройствам,*
- *И к исполнительным устройствам,*
- *И к системе в целом.*

Анализ этих соотношений показывает, что они дают завышенные оценки вероятности отказа для высоких уровней самодиагностики. Это довольно странно, если учесть, что для соответствия, например, уровню SIL3 надежность системы по определению должна быть выше 99.9%, и система должна обладать исключительно высоким уровнем самодиагностики.

В настоящей работе в главе 5 *"JEC 6]508 - Вероятность отказа. Альтернативные решения"* приводятся соотношения PFD_{AVG} **и** PFH_{AVG} для граничных значений степени диагностического охвата, то есть для *DC-0* и *DC=1*, подтверждающие неточность оценок IEC 61508 для высоких уровней самодиагностики.

Отсутствие оценок вероятности ложного срабатывания. Наиболее серьезным пробелом стандарта является не доведенное до конца исследование структуры отказов систем безопасности. Стандарт не дает никаких рекомендаций по оценке вероятности так называемых "безопасных" отказов, которые фактически означают немотивированный, неоправданный останов процесса, и как раз-то и могут представлять значительную опасность.

По непонятным причинам в стандарте вообще отсутствует важнейшее понятие **ложного срабатывания,** которому мы только что уделили столько времени, когда рассматривали пример. Зато в стандарте есть очень расплывчатое определение **безопасного отказа.**

Согласно стандарту,

Безопасный отказ *{Safe failure) - это "Отказ, который потенциально не способен привести систему безопасности к опасному состоянию или к неспособности осуществлять функции безопасности***". Можно смело утверждать, что отказов, потенциально не способных привести систему безопасности к опасному состоянию, в природе не существует.**

Напротив, авторская позиция прямо противоположна:

При построении систем безопасности необходимо исходить из того, что ЛЮБОЙ ОТКАЗ СИСТЕМЫ ПОТЕНЦИАЛЬНО СПОСОБЕН ПРИВЕСТИ К ОПАСНОМУ СОСТОЯНИЮ.

Можно представить, что произойдет с технологическим блоком, если в ответ на дребезг контакта система защиты произведет отсечку выхода блока, но не сработает отсекатель на входе в блок. Далее стандарт дает тавтологическое определение **Безопасного состояния** *{Safety state):*

"Состояние контролируемого оборудования, при котором безопасность достигается" (буквальный перевод).

За всеми этими вроде бы спокойными и обтекаемыми формулировками кроется крайне неприятный смысл, который не сразу обнаруживается: для реального производства практически во всех случаях "безопасный" отказ в лучшем случае означает ложный останов производства.

Можно сказать, что в стандарте МЭК понятие "безопасный отказ" - самое неудачное понятие для тех, кто *использует* оборудование и системы безопасности. И в то же время это понятие очень удобно для производителей и поставщиков оборудования. Фактически оно означает безопасность самой системы безопасности от технологического процесса:

Система защиты просто снимает с себя какую бы то ни было ответственность за <|/акт и результат ложного срабатывания. В отличие от стандарта МЭК, американский стандарт ANSI/ISA 84.01-96 дает вполне корректные определения. Согласно этому стандарту, ложное срабатывание определяется как ***Spurious trip, nuisance trip. false shut down:***

Ложное, беспричинное срабатывание блокировки, ши немотивированный останов процесса по причинам, не связанным с действительными событиями на процессе.

Ложное срабатывание может произойти:

- По причине отказа оборудования,
- Из-за ошибки программного обеспечения,
- Из-за ошибки обслуживания,
- Неправильной калибровки,
- Неправильной предаварийной уставки,
- Отказа полевого оборудования,
- Отказа модулей ввода-вывода,
- Отказа центрального процессора,
- Электрического сбоя,
- Электромагнитной наводки, и т. д.
- Короче - из-за чего угодно.

Доступность и наглядность стандарта. Фантастически изощренная терминология, как будто авторы специально стремились забыть все привычное и общепринятое, и непременно изобрести нечто необыкновенное. Всего один, но чрезвычайно важный пример.

Авторы не просто избегают понятия "Надежность". **Трудно поверить, но понятие надежности** вообще отсутствует **в части 4 *"Определения и сокращения"* стандарта IEC 61508.** Но всмотримся внимательно:

Целостность, полнота безопасности - термин **IEC** 61508:

Safety integrity

Вероятность того, что система безопасности удовлетворительно (?!) выполняет требуемые функции безопасности по всем предопределенным условиям в течение установленного интервала времени.

Сравниваем, **Надежность** - термин ISA 84.01-96:

Reliability

Вероятность того, что система может выполнять определенные функции при всех предопределенных условиях в течение установленного интервала времени.

Направленность стандарта. Как сказано, стандарт ориентирован, прежде всего, на производителей, проектировщиков, разработчиков систем безопасности, но не на потребителя.

Поэтому в стандарте отсутствуют простые и наглядные процедуры для оценки границ применимости конкретных систем. В настоящей работе приводятся процедуры, диаграммы, таблицы и графики, которые могут служить ориентиром для живых пользователей.

1.11. Применимость одноканальных систем

Начнем с того, что введем следующее утверждение, которое одновременно является и определением:

Алгоритм действия системы 1oo1 не зависит от категории взрывоопасности объекта. При любом отказе система 1oo1 снимает питание с выходных реле, и происходит аппаратный, программно неконтролируемый останов процесса по физически предопределенной последовательности операций.

Это обстоятельство послужило поводом к тому, что некоторые хитроумные производители и поставщики систем объявили свои одноканальные системы соответствующими любому классу требований безопасности - вплоть до шестого по стандартам DIN, поскольку одноканальная система в случае своего отказа переведет процесс в "безопасное" состояние - состояние останова. Более того, утверждается, что **время работы одноканальной системы на объектах любого класса не ограничено.** Это заявление отвергает саму идею резервирования, как средство противодействия отказам оборудования, поэтому требует адекватной оценки.

Принципиальная разница между одноканальной и многоканальными системами состоит в том, что в случае отказа последние имеют жизненный ресурс для восстановления, сохраняя при этом контроль над процессом.

1oo1D - действительно система с неограниченной по времени работой: эту границу невозможно предугадать. Система работает до тех пор, пока не откажет. В отличие от систем 1oo2D, 2oo3, для которых состояние и поведение после частичного отказа вполне предсказуемо и поправимо, в случае с одноканальной системой невозможно предсказать, что произойдет с нею в следующий момен+.

Утверждать, что для одноканальной системы "разрешено" неограниченное время работы - вводить в заблуждение. Не то что время как таковое, но и конкретное одноканальное время

просто невозможно запретить. Равно как и для систем более высокого порядка. Однако принципиальная разница состоит в том, что для систем loo2D, 2oo3 мы имеем возможность восстановления исходной конфигурации в течение некоторого предопределенного промежутка реального времени, - пусть не 72 часа, а хотя бы полчаса, - а это уже совершенно другое дело. Единственное, что достоверно известно о системе loo1D - это ее прошлое. И системой с неограниченной по времени работой она является только во взаимоотношении с только что отработанным моментом времени.

Правильнее было бы определить **одноканальные системы как такие системы, работа которых ничем не была ограничена в прошедшем до останова времени.**

Поэтому и называться системой с неограниченным временем работы она может далеко не всегда, а только до тех пор, пока не прекратит эту самую работу. Нельзя абстрактно, отвлеченно, на словах или на бумаге утверждать, что такой-то тип, такая-то модель одноканальной системы является системой некоторого класса. Для этого типа систем не имеет никакого значения, к какому классу они отнесены. Да они и не могут быть отнесены к какому-либо классу:

Одноканальная система будет являться системой конкретного, любого необходимого, неважно какого класса, только во время своего конкретного применения в данном классе, и только в данное время. Причем это ее свойство никак не зависит от решений комитетов по безопасности. Будь то TUV или какой-то другой. И даже от того, существуют ли сами эти комитеты. Эта система проработает ровно столько, сколько сможет, независимо ни от каких разрешений. И никакая самодиагностика здесь не поможет. Причем алгоритм ее поведения будет один:

ОДНОКАНАЛЬНАЯ СИСТЕМА МОЖЕТ РАБОТАТЬ ПО ЛЮБОМУ КЛАССУ И ПРОРАБОТАЕТ РОВНО СТОЛЬКО, СКОЛЬКО СМОЖЕТ ПРОРАБОТАТЬ, ОБЕСПЕЧИВ ПОСЛЕ СВОЕЙ ПОГИБЕЛИ **внеплановый останов процесса,** который будет проходить в жестком аппаратном режиме, и уже **никак не будет контролироваться** системой защиты.

Система произведет НЕКОНТРОЛИРУЕМЫЙ ОСТАНОВ ПРОЦЕССА, ВОЗМОЖНО ДАЖЕ БЕЗАВАРИЙНЫЙ, ЕСЛИ НЕ ЗАКЛИНИТ ЗАДВИЖКА И СРАБОТАЕТ ОТСЕКАТЕЛЬ.

Спрашивается: ради чего было менять пусть и не слишком надежную, но полностью распределенную релейную систему защиты на суперсовременный черный ящик, если максимум, что может инициировать реле, - это запустить один-единственный контур защиты, а черный ящик в самый неожиданный момент одним махом остановит все производство?

Именно поэтому для дублированных систем loo2D в течение определенного ЗАПАСА ВРЕМЕНИ нам предоставляется возможность восстановления частичной потери исходной конфигурации, и продолжения нормальной работы. Последние рекомендации TUV вполне определенно регламентируют действия систем безопасности типа loo2D в случае частичного отказа:

В том случае, если данные в ДВУХ центральных модулях отличаются, и причина отказа определена программой самодиагностики, то происходит отключение ОБОИХ модулей, или работа на одном канале в течение 1 часа. Если причина расхождения не определена, то происходит отключение ОБОИХ центральных модулей.

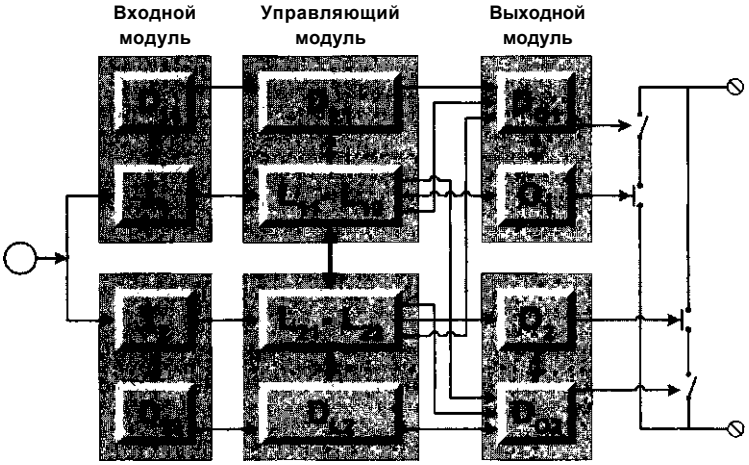
Аналогичные рекомендации даются и в случае частичного отказа систем типа 2оо3. При отказе одного из трех плеч (legs) на входном или выходном модуле, или при отказе центрального процессора **настоятельно** рекомендуется произвести замену отказавшего компонента в течение принятого в отрасли среднего времени на замену.

Авторская позиция состоит в том, что на **взрывоопасных** объектах **ни для каких систем, ни при каких обстоятельствах нельзя давать разрешение на постоянную одноканальную работу.** Разрешение одноканальной работы на неопределенное время и для членов семейства более высокого порядка означает разрешение на деградацию до этого состояния.

Таким образом, любая система, способная достичь режима одноканальной работы, могла бы рассчитывать на "бесконечное" пребывание в этом качестве. Сказанное могло бы означать, что и изначально на взрывоопасные объекты можно ставить одноканальную систему. Но сказанное означает совершенно противоположное, а именно: для взрывоопасных объектов система защиты должна предоставлять интервал реального времени, в течение которого конфигурация системы должна быть восстановлена до исходного состояния.

1.12. Существуют ли четырехканальные системы 2oo4 и 2oo4D?

Существуют модификации систем loo2D с дублированными процессорами в каждом управляющем модуле:



1 q q 2 D

Рис. 1.9

Центральная часть системы построена по принципу 2*2, то есть каждый из двух управляющих модулей содержит по 2 микропроцессора. **В** случае расхождения в работе какой-либо пары микропроцессоров на одном канале данный канал выключается из работы, и система продолжает работу по одноканальной схеме **loolD.** Исходная конфигурация системы может быть восстановлена в течение предопределенного интервала в реальном времени. Если заранее известно, что замена дефектного модуля не может быть произведена, то в течение предопределенного интервала времени система может произвести программно-управляемый останов процесса. По окончанию предопределенного интервала времени система должна просто снять питание с выходов. Таким образом, по алгоритму действий в случае отказа данная модификация архитектуры полностью эквивалентна архитектуре loo2D.

Поэтому на поставленный вопрос мы даем вполне однозначный ответ: СИСТЕМ 2oo4D В ПРИРОДЕ НЕ СУЩЕСТВУЕТ. Данный ответ подтверждают и ведущие специалисты ISA, и специалисты экспертной группы Exida, не менее, а для многих и более авторитетной, чем TUV.

В этой связи довольно странно наблюдать претензии поклонников оборудования некоторых фирм на новое слово в построении систем с архитектурой рис. 1.9, для которой ими придумано новое определение: 2oo4, или даже 2oo4D.

Это определение совершенно справедливо не признается стандартом Международной Электротехнической Комиссии IEC 61508: в стандарте даже вскользь не упомянуто о таком, казалось бы, революционном событии, как появление новой архитектуры. Однако сторонники, по крайней мере, двух систем с родственной архитектурой, - FSC-system (QMR) фирмы Honeywell и H41/51-HRS (HI Quad) фирмы HIMA, - до последнего момента претендовали на это звание. Далее будет представлен подробный разбор двух статей доктора Бэкмана - большого энтузиаста аббревиатуры 2oo4D на примере контроллеров HIMA.

Замечание

Самое удивительное здесь заключается в том, что семейство контроллеров фирмы HIMA, вне всякого сомнения, является одним из безусловных лидеров среди множества существующих на сегодняшний день систем защиты - и по архитектуре, и по качеству программного обеспечения. И совершенно не нуждается в каком-то искусственном утверждении своего превосходства.

*Как мы увидим, лобовая попытка преподнести в качестве преимущества аргументы типа 2*2 приводит прямо к противоположному, можно сказать, нелепому результату:*
В чистом виде вероятность отказа архитектуры "2oo4" (2*2) в ЧЕТЫРЕ РАЗА ВЫШЕ, ЧЕМ АРХИТЕКТУРЫ 1oo2.
Такова плата за высший уровень диагностики:

Лучше ТОЧНО знать, что один из четырех процессоров 2oo4 отказал, чем просто констатировать расхождение в результатах двух процессоров 1oo2, U гадать в чем причина.

Но самое главное - это не забывать, что смысл имеет только ВЕСЬ контур безопасности. И если вероятность отказа пары реальных модулей HIMA CPU 8650E с дублирован-

ными процессорами равна 4.0 •10~^{6} (вполне реальное значение), а вероятности отказа реле уровня и соленоида отсечного клапана равны по 1.0-10~^{4} (это еще хорошо), то понятно, что потенциально узким местом системы является полевое оборудование, а не процессорные модули:

2oo4: 2-1.0-10~^{4} +4.0-10~^{6} = 2.04 -10~^{4},

1oo2: 2-1.0-10~^{4} + 40 -10~^{6} /4 = 2.01 - 10~^{A}.

А если таких реле и клапанов не по одному, а по нескольку сотен, то уже как-то по-иному представляется проблема отказа центральных процессоров. Другое дело, что процессорных модулей в данном случае всего два, и их роль в обеспечении безопасности неизмеримо выше, чем конкретного датчика или клапана.

Внимательно посмотрим на архитектуру PLC H41/51-HRS (рис. 1.10). На самом деле центральная часть этой системы работает по принципу 2*2. Каждая пара процессоров находится на одном модуле, и на выходы системы воздействует модуль, а не индивидуальный процессор.

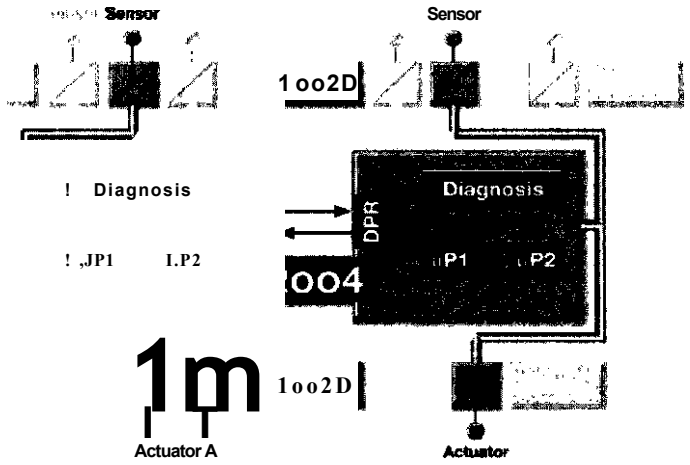


Рис. 1.10

Необходимо помнить, что по определению

Под каналом понимается элемент, или группа элементов, способных самостоятельно выполнять предопределенную функцию.

Кстати говоря, четверка в коде архитектуры подразумевает существование не только схемы 2oo4, но и схем 1oo4, и 3oo4, но об этом благоразумно не упоминается, поскольку системы 2*2 по схемам деградации 1oo4 и 3oo4 работать не могут.

Более того, и шины ввода-вывода, и входные и выходные модули сами авторы определяют как 1oo2. Поэтому даже если бы централь-ная часть этой системы действительно реализовала архитектуру 2oo4 (для чего требуется разместить процессоры на четырех модулях), общеизвестно, что итоговая конфигурация определяется наиболее слабым звеном, в том числе и в архитектурном отношении, и даже в этом случае система определялась бы как система 1oo2. Система работает следующим образом:

Поскольку **оба процессора находятся на одной плате,** то при выходе из строя одного из процессоров канал считается неработоспособным, а состояние выходов продолжает полностью контролировать оставшийся в работе канал, **то есть система переходит на работу по схеме 1oo1D.**

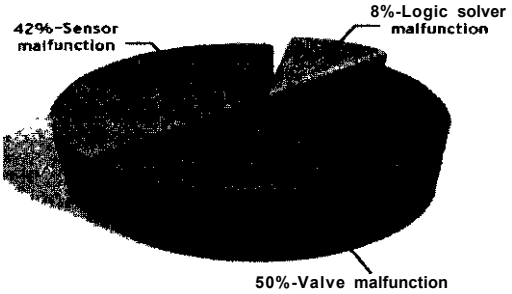
Попутное замечание

Объявленная фирмой Эмерсон система противоаварийной защиты DeltaV SIS (SLS 1508) также претендует на работу без ограничения по времени (см. Презентацию "*Подход Emerson к вопросам ПАЗ",* 2004, стр. 69, автор Koen Leekens).

Как мы теперь знаем, потенциально безопасность таким образом обеспечить можно, а вот программно-логическую последовательность останова, если не дублировать контроллеры, может оказаться затруднительным. Каждый контроллер DeltaV SIS может обрабатывать только 16 каналов ввода-вывода. При выходе не дублированного контроллера из строя последовательность операций разрывается.

Аргументаци^ в виде эффектных картинок с процентами отказов логических устройств в данном случае не очень срабатывает (рис. 1.11). По ходу настоящей работы будут представлены и другие, не столь радужные для производителей PLC, но чрезвычайно авторитетные данные.

К тому же если для системы защиты из восьмисот сигналов поставить 800/16= 50 контроллеров, да еще и резервировать их, то соотношение может сильно поменяться: вероятность отказа одного из пятидесяти контроллеров в пятьдесят раз больше, чем просто одного.



Because of the majority of malfunctions in safety applications occur in the devices, increased logic solver reliability does not by itself Improve the reliability of the entire safety loop.

Источники изображения:

- *Приложение к журналу CONTROL за май 2004, "An advertising supplement to CONTROL For the process industries: A NEW WORLD OF SAFETY";*
- *А также брошюра Safety Instrumented Systems, "The Smart Approach", Emerson Process Management, USA, 2004.*

Рис. LI 1

Но все же самое главное состоит даже не в увеличении вероятности отказа, а в уменьшении функциональности. Программно-логические устройства систем безопасности для того и создавались, чтобы полностью контролировать состояние объекта и обеспечивать выполнение функций безопасности в едином информационно-управляющем поле.

Если вероятность отказа современных программно-логических устройств по отношению к полю на самом деле гак мала, то совершенно нет никакой необходимости создавать себе дополнительные трудности в реализации функций чащиты, разнося алгоритм по цепочке из многих десятков контроллеров.

В данном случае ситуация полностью аналогична тому, что существует во взаимоотношении локального регулирования и связного, или усовершенствованного управления. Сонрсмснные электронные регуляторы тоже имеют по нескольку иходон и выходов, и позволяют осуществлять взаимодействие

между собой для реализации функций связного регулирования. Однако же основной путь автоматизации пошел по пути интеграции на основе универсальных подсистем управления в составе АСУТП. Если алгоритмы защиты настолько элементарны, что состоят только из одномерных контуров, то они вполне могут быть реализованы на чем угодно - и на релейных схемах, и на локальных контроллерах. И вполне возможно, что никакого резервирования в данном случае не требуется. Поэтому для тех процессов, для которых не требуется жестко согласованное выполнение операций защиты, или программно-логическое управление, этот вариант архитектуры может оказаться вполне приемлемым.

Если же все шестнадцатиканальные контроллеры должны резервироваться, то по функциональности данная архитектура вполне сопоставима с общепринятыми централизованными архитектурами, но с некоторым увеличением вероятности отказа за счет увеличения количества составных элементов.

Разумеется, можно было бы этими комментариями и ограничиться. Но интерпретации архитектур "2oo4" и 2oo3 обросли таким количеством недоразумений, предрассудков и мифов, что необходимо детально разобраться в том, как ведет себя та или иная архитектура в реальных обстоятельствах. Это обсуждение будет плодотворным для понимания времени и места пребывания каждой архитектуры в общей иерархии систем безопасности. В нескольких следующих разделах рассматриваются самые изысканные образцы аргументации в пользу превосходства архитектур "2oo4" и 2oo3 над всеми прочими. Печально, что некоторые из этих аргументов подкрепляются сумрачным германским авторитетом TUV, который для многих является символом непогрешимости.
На сайте tuv-fs.com до сих пор можно увидеть сентенции типа *"System-structure:* ***Central Unit:*** *2oo4D, TUV Rheinland, May* ***2002".***

1.13. Научно-техническая мифология

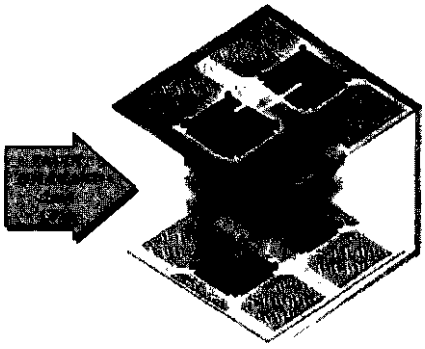
Стандарт IEC 61508 абсолютно справедливо определяет мерой жизнеспособности различных архитектур систем безопасности не количество работающих процессоров, а количество работающих каналов.

Тем не менее, ряд заинтересованных исследователей и после формального утверждения стандарта в 2000 году продолжают интерпретировать положения стандарта весьма своеобразно. В качестве примера разберем две статьи доктора Бэкмана - большого энтузиаста квадро архитектуры фирмы HIMA. Первая из статей:

The New Quad Architecture: Explanation and Evaluation,
Lawrence V. Beckman, Mr., Dr. 2001,
SafePlex Systems Inc, HIMA Exclusive distributor,

начинается с эффектной картинки отказоустойчивой Quad Архитектуры 2oo4:

Quad Architecture



Hgure 1

Рис. 1.12

Аргументация Бэкмана в пользу мифических систем типа "2oo4" настолько необыкновенна, что требует адекватного ответа буквально по каждому пункту.

Пункт №1 - Безграничное время.

"The new Quad (QMR) Architecture is a major breakthrough in safety performance. This architecture provides four (4) processors - two per channel, and remedies problems associated with dual processor architectures, as regards the dangerous undetected failure of one of the two (dual) processors. Please refer to Figurel for additional information. Both pairs of active processors operate synchronously with the same user program. A hardware comparator and a separate fail-safe watchdog monitors the operation of each pair of processors to diagnose and resolve anomalies. As such, this architecture can operate at the SIL3 (RC6) level on ex-

ther one or both channels, for an unrestricted period of time. It achieves a significant increase in both safety and availability which exceeds that provided by TMR architectures by a factor of three. In addition, it has significantly less susceptibility to common cause failure because of the absolute separation, isolation and operation of the redundant channels. Please see Figure 2 for more details on the HI Quad Architecture".

Попробуем перевести как можно ближе к оригиналу:

"Новая Quad (QMR) архитектура является главным прорывом в исполнении безопасности. Эта архитектура обеспечивает четыре (4) процессора - ДВА НА КАНАЛи снимает проблемы, связанные с двухпроцессорной архитектурой по отношению к опасным необнаруженным отказам одного из двух (ДУБЛИРОВАННЫХ) процессоров. Пожалуйста, обратитесь к ***Figure 1*** *за дополнительной информацией (рис. 1.12- даже интересно, что ж такого на этой переводной картинке можно увидеть - Ю. Ф.). Обе пары процессоров синхронно выполняют одну и ту же пользовательскую программу. Аппаратный компаратор и отдельный отказоустойчивый сторожевой таймер отслеживают работу каждой пары процессоров с целью выявления и обработки отклонений. Таким образом, эта архитектура может работать при уровне SIL3 (RC6) на одном или на двух каналах* ***В ТЕЧЕНИЕ НЕОГРАНИЧЕННОГО ПЕРИОДА ВРЕМЕНИ.*** *Она (данная архитектура) достигает значительного увеличения, как безопасности, так и готовности, которые* ***превосходят эти показатели для троированных архитектур TMR В ТРИ РАЗА.*** *Кроме того, она (данная архитектура) имеет значительно меньшую подверженность отказам общего порядка из-за абсолютного разделения, изоляции и работы резервированных каналов. Пожалуйста, посмотрите на* ***Figure 2*** *(рис. 1.13) для большего количества деталей архитектуры HI Quad".*

Относительно "неограниченного периода времени" было и еще будет сказано достаточно и вполне определенно по ходу настоящей работы. Доктор не замечает, что до беззаботного одноканального пребывания по американскому образцу еще надо дожить: если на выходе одного из управляющих модулей - ноль, а на выходе другого - единица, то кому в этой жизни вообще можно верить?

HIQuad Arhitecture

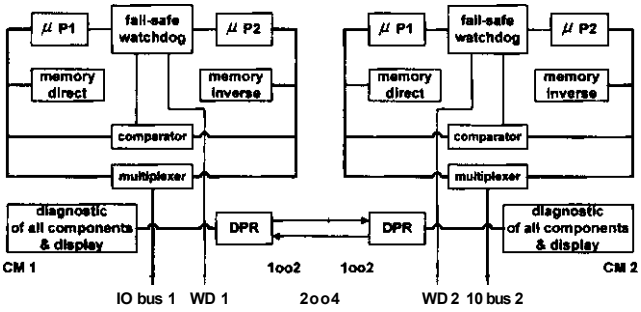


Figure 2

Рис. 1.13

Как мы увидим, именно этим обстоятельством определяется жесткая позиция TUV при ЛЮБОМ расхождении в результатах работы модулей управления. Выполнение рекомендаций TUV конкретно для систем HI Quad дает возможность встретить опасность на самых ранних подступах. Вот что говорит по этому поводу документ фирмы HIMA "*Survey Current status",* VM 9842, Manuals 02.2000, стр. 28:

"В том случае, если данные в ДВУХ центральных модулях отличаются, и причина отказа определена программой самодиагностики, то происходит:
А) отключение ОБОИХ модулей, или работа на одном канале в течение 1 часа.
Если причина расхождения не определена, то происходит:
В) отключение ОБОИХ центральных модулей".

Высший уровень самодиагностики архитектуры loo2D (в том числе и ее модификации типа 2*2) для того и создан, что если уж возникает необходимость восстановления исходной конфигурации, то она ДЕЙСТВИТЕЛЬНО возникает.

И это не недостаток, а одно из основных преимуществ архитектуры. Тем не менее, эксклюзивный дистрибьютор продолжает старую песню о главном - о неограниченной одноканальной работе. Все это можно было бы считать курьезом саморекламы, если бы не означало фактический призыв к созданию предпосылок аварийной ситуации: при одноканальной работе резко возрастает вероятность и опасного отказа, и ложного срабатывания.

Пункт №2 - Тройное превосходство. По поводу "показателей, В ТРИ РАЗА превосходящих троированные архитектуры TMR" у нас еще неоднократно будет возможность убедиться, что соотношение 1:3 соблюдается только для обычных архитектур loo2D и 2oo3.

Архитектуры "2oo4" по вероятности отказов уступают и архитектурам loo2D, и архитектурам с тройным модульным резервированием. Это связано с тем, что дублированные системы loo2D и системы тройного модульного резервирования *(TMR - Triple Modular Redundancy)* на самом деле таковыми и являются, то есть системами с двойным и тройным МОДУЛЬНЫМ резервированием (по крайней мере - центральная часть). А вот системы с архитектурой 2*2 *(QMR - Quad Modular Redundant)* на самом деле УЧЕТВЕРЕННОГО МОДУЛЬНОГО РЕЗЕРВИРОВАНИЯ НЕ ИМЕЮТ, а имеют обычное дублирование модулей по схеме 1oo2.

Принадлежность к семейству систем loo2D само по себе, и без искусственного учетверения превращает системы QMR "2oo4" в системы с очень хорошими характеристиками. Тем не менее, при вычислении конкретных вероятностей отказа выясняется, что архитектура 2*2 ("2oo4") при прочих равных условиях все же несколько уступает даже архитектуре 2oo3.

В последующем автор идет еще дальше (см. **Пункт** №6). Утверждается, что архитектура QMR "2oo4^{и} превосходит и архитектуру loo2D, и архитектуру TMR не в три раза, а на порядки, поскольку базовая частота отказов входит в уравнения вероятности отказа архитектуры "2oo4^{и} уже не во второй, а в третьей степени! Но читаем далее:

"Operation under Fault Condition

For safety applications, single channel systems (1-0) are not fault tolerant and must fail safe. Dual architectures can either operate fail safe (2-0) or degrade to single channel operation (2-1-0) under specific fault conditions, and with severe time limitations as defined in their safety certification report

Соответствующий перевод:

"Действия в условиях отказа>

По отношению к приложениям, связанным с безопасностью, одноканальные системы (1-0) не являются отказоустойчивыми, поэтому должны совершить безопасный останов. Дублированные архитектуры могут работать как в

безопасном режиме (2-0), так и в одноканальном режиме (2-1-0) при определенных условиях отказа, и с серьезными временными ограничениями, как определено в их отчете о сертификации безопасности".

Просто замечательно, что даже не упомянуты системы с архитектурой 1oo2D, к семейству которых принадлежит и сама архитектура QMR "2oo4"!

Пункт №3 - Аббревиатура QMR. Еще раз: аббревиатура QMR - *Quad Modular Redundant* - совершенно не соответствует действительности. Архитектура QMR "2oo4" вовсе не имеет учетверенной модульной избыточности, а имеет обычную, двойную. И это хорошо видно по Figure 2 (рис. 1.13). Читаем далее:

"Both the TMR (3-2-0) and Quad (4-2-0) architectures degrade to a 2-0 mode of operation after the first fault. However, the Quad (QMR) architecture retains its comprehensive internal diagnostics, ***has no time restrictions while operating in this mode,*** *and provides full SIL3 (RC6) protection as well. Please refer to* ***Figure*** *3 for a table of operating scenarios after the First Fault".*

"И TMR (3-2-0), и Quad (4-2-0) архитектуры деградируют к режиму работы 2-0 после первого сбоя. Однако, Quad (QMR) архитектура, сохраняя свою изощренную внутреннюю диагностику, ***не имеет временных ограничений при работе в этом режиме,*** *и продолжает обеспечивать полноценную защиту по SIL3 (RC6). Пожалуйста, обратитесь к* ***Figure*** *3 (рис. 1.14) за таблицей сценариев работы после первого отказа".*

Safe Operation after First Fault

Simplex:	1 - 0	Fail-Safe (RC4 only)
Dual:	1oo2D	1oo1D (Severe Time Restriction)
TMR:	2oo3	1oo2 (Time Restriction)
QMR:	2oo4	1oo2D **(No Time Restriction!)**

Figure 3

Рис. 1.14

Вполне возможно, что отсутствие временных ограничений существовало до принятия стандарта IEC 61508, и скорее было рассчитано на людей, не слишком искушенных в автоматизации.

Авторская позиция, полностью совпадающая с нынешними рекомендациями TUV, однозначна: как неоднократно подчеркивается на протяжении всей настоящей работы, неограниченное время одноканальной работы - прямой путь к аварии.

Пункт №4 - Сценарий первого отказа. Автор статей приводит схемы деградации различных архитектур систем безопасности после первого отказа. Сразу необходимо сказать, что последняя строка Figure 3 (рис. 1.18) НЕ СООТВЕТСТВУЕТ ДЕЙСТВИТЕЛЬНОСТИ:

Как и все системы loo2D, QMR "2oo4" никак не может деградировать к своему исходному состоянию loo2D. Как и все системы loo2D, QMR "2oo4" может деградировать только к состоянию looID. И в данном случае с*Люол D в кодировке looID символизирует особый способ самодиагностики путем сравнения результатов работы двух процессоров на одном управляющем модуле. Утверждение энтузиастов архитектуры "2oo4", что система деградирует к состоянию 1oo2 никак нельзя признать корректным, поскольку оно совершенно неплодотворно, и не привносит в архитектуру никаких дополнительных преимуществ. **Алгоритмы действий систем looID и 1oo2 (1+1) в случае отказа тождественны:** питание с выходных цепей снимается, и происходит программно неконтролируемый физический останов процесса.

Пункт №5 - Одноканальный дубль. Затем в статье приводятся уже совершенно неопровержимые аргументы в пользу архитектуры Quad (QMR) "2oo4":

"The Quad (QMR) architecture provides a pair of dual processors operating in the safety (2-0) mode for each channel The resulting significant increase in diagnosability of the operation of these processors has in fact completely remedied safety concerns related to dangerous undetected failure of the processors, and consequently the removal of all time restrictions on single channel operation of the system

И сказано здесь буквально следующее:

"Quad (QMR) архитектура обеспечивает пару дублированных процессоров, работающих в безопасном (2-0) режиме для каждого канала. Результирующее значительное увеличение diagnosability, пардон, диагностируемости работы этих процессоров фактически полностью снимает "озабоченности" безопасностью, имеющие отношение к не выявленным

опасным отказам процессоров, и, следовательно, снимает все временные ограничения на одноканальную работу системы ".

Оптимизм, высказанный здесь с таким энтузиазмом, не имеет под собой абсолютно никаких оснований. В том и состоит проблема опасных отказов, что часть из них до окончания межтестового интервала остаются необнаруженными. Доказать абсолютное отсутствие опасных необнаруженных отказов *"по любому"* просто невозможно. И доказывать *таким* образом отказ от временных ограничений просто несерьезно. Преимущества способа диагностики посредством сравнения двух идентичных элементов в архитектуре 1oo2 по сравнению с физической диагностической цепью архитектуры 1oo1D могут быть вполне эфемерными, или просто мифическими.

Именно с этим обстоятельством связано применение самых изощренных способов *альтернативной* диагностики по всему тракту преобразования входного сигнала в выходной, какие мы наблюдаем в схемах систем класса 1oo2D, и к которым, собственно, и принадлежит сама система QMR. Вообще необходимо предостеречь потенциальных пользователей от того, чтобы абсолютизировать все решения TUV, на которые мы все с таким удовольствием ссылаемся.

Как известно, чтобы доказать нечто, необходимо это нечто доказать. А чтобы опровергнуть, достаточно привести всего лишь один пример, противоречащий утверждению. Но мы приведем сразу два очень показательных примера. К примеру, можно задать любопытный вопрос:

Почему одноканальная система 1oo1D Quadlog (см. рис. 1.15), которая в отличие от одноканального варианта системы QMR "2oo4" имеет **ДВА САМОСТОЯТЕЛЬНЫХ МОДУЛЯ** управления, и точно так же осуществляет межпроцессорное взаимодействие, при этом даже не пытается использовать данное преимущество? И почему не объявляет себя системой 1 oo2D с неограниченной во времени работой - хотя бы с целью рекламы? ЭТА СИСТЕМА С ДВУМЯ РАЗДЕЛЬНЫМИ МОДУЛЯМИ УПРАВЛЕНИЯ отнесена не к архитектуре 1oo2D, а к архитектуре 1oo1D. И аттестована эта система изначально по RC4 и SIL2 без нелепых разрешений на "безграничную" работу по любому классу. А ведь вполне можно было бы декларировать аббревиатуру 1oo2D по аналогии с логикой Figure 3 (рис. 1.14):

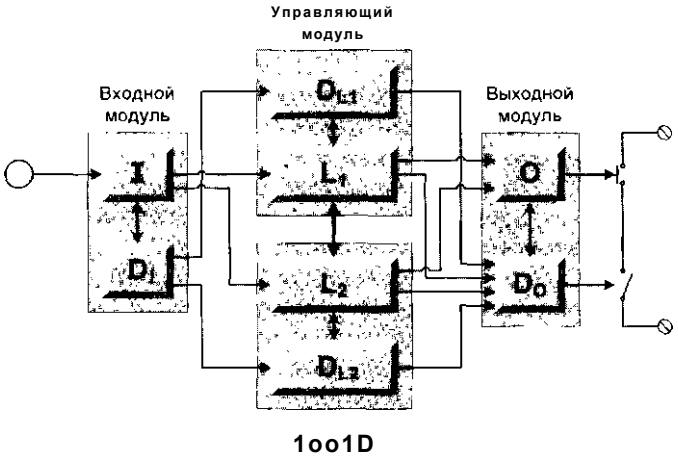


Рис. 1.15

Вполне очевидно, что создателям системы Quadlog просто в голову не приходит отстаивать безграмотное утверждение, и на этой основе устанавливать неограниченную работу своей системы. Просто потому, что система на рис. 1.15 — это одноканальная система 1oo1D с возможностью восстановления в оперативном режиме исходной конфигурации *только* модулей управления. А неограниченная одноканальная работа - это прямой путь к аварии.

Следующий пример еще более впечатляющ. Системы семейства Centum фирмы Yokogawa Electric в течение не одного десятка лет используют резервированную двухпроцессорную архитектуру "Pair & Spare" (2*2) для своих станций управления FCS. Однако никогда и нигде Yokogawa не относила свои системы к категории 2oo4D.

Пункт №6 - Порядок превосходства.

Следующая цитата:

"Referring to ISA TR 84.02, Part 2, 1998, one can quickly determine that the Quad (2oo4) architecture is comparable to the ultra safe loo3 architecture, as both have cubic terms in their equations for PFD. By comparison, TMR (2oo3) is comparable to the loo2D architecture in that both have squared (second order) terms in their equations.

This comparison concludes that the QMR (2oo4) architecture provides an order of magnitude better safety performance than either TMR (2oo3) or loo2D architecture, and is a major technological enhancement in safety system perjormance. Please refer to Figure 4 for a comparison of these architectures".

Comparison of the Best PFD_{AVG}

loo2	$PFD_{avg} = \lambda_{DU}^2 \frac{TI^2}{3}$
loo3	$PFD_{avg} = \lambda_{DU}^3 \frac{TI^2}{4}$
2oo3	$PFD_{avg} = \lambda_{DU}^2 \cdot TI^2$
2oo4	$PFD_{avg} = \lambda_{DU}^3 \cdot TI^3$

Source: dTR 84.02, Part 2-1998
Figure 4

Рис. 1.16

Перевод:

"Обратившись к Техническому отчету ISA TR 84.02, Part 2, 1998, можно быстро определить, что Quad (2oo4) архитектура сравнима с ультра безопасной архитектурой 1oo3, поскольку обе имеют третий порядок в своих уравнениях для PFD. Для сравнения, архитектура TMR (2oo3) сопоставима с архитектурой loo2D, так как обе имеют квадратичную зависимость (второй порядок) в своих уравнениях.

Это сравнение приводит к выводу, что архитектура QMR (2oo4) обеспечивает на порядок лучшие показатели безопасности, чем архитектуры TMR (2oo3) или loo2D, и является главным технологическим достижением в исполнении систем безопасности. Пожалуйста, обратитесь к Figure 4 (рис. 1.16) для сравнения этих архитектур".

Единственное достоверное утверждение в приведенном отрывке - это второй порядок частоты отказов для архитектур loo2D и 2oo3. Забыто и перекрыто даже ошибочное заявление Пункта №2 "Тройное превосходство" о троекратном превосходстве архитектуры QMR над архитектурой 2oo3 - здесь оно достигает "порядка" (автор оговорился: имеется в виду третья степень произведения $(Л\ t)^3$. Порядок вероятности отказа при условии $A\ \ t \ll 1$ будет еще меньше).

Остальные два утверждения в приведеьДюм отрывке о превосходстве архитектуры Quad (QMR) "2oo4" по вероятности отказов над архитектурами loo2D и 2oo3 не соответствуют действительности.

Все три архитектуры - loo2D, 2oo3, "2oo4" - имеют второй порядок вероятности отказа от базовой частоты отказа. Причем архитектура и"2oo4" имеет более высокую вероятность отказа, и чем архитектура loo2D, и чем архитектура 2oo3.
При этом вероятности отказа соотносятся как

1oo2 : 2oo3 : "2oo4" = 1 : 3 : 4 .

Пункт №7 - Таблица сравнения вероятностей отказа (рис. 1.16). В последней строке данной таблицы автор публикации, апеллируя к Техническому отчету ISA TR84.02, приводит совершенно правильное соотношение вероятности отказа, но **совершенно другой архитектуры,** а именно отказа **ТРЕХ КАНАЛОВ ЧЕТЫРЕХКАНАЛЬНОЙ АРХИТЕКТУРЫ.**
Вспомним смысл аббревиатуры 2oo4:

Если для нормальной работы четырехканальной системы необходимо 2 канала, то система способна безболезненно выдержать отказ 4 - 2 = ДВУХ каналов. Отказ системы произойдет после отказа (4 - 2) + 1 = ТРЕХ каналов.

И действительно, вероятность опасного необнаруженного отказа трех каналов четырехканальной системы ничтожно мала. Но все дело в том, что представленное на рис. 1.16 соотношение справедливо **именно и только** для ЧЕТЫРЕХКАНАЛЬНОЙ архитектуры, и не имеет никакого отношения к ДВУХКАНАЛЬНОЙ архитектуре HI Quad (QMR) "2oo4^{M}.

Еще раз: **мерой жизнеспособности различных архитектур систем безопасности является не количество работающих процессоров, а количество работающих каналов.**

Каждая пара процессоров архитектуры 2*2 (HI Quad "2oo4") находится на одной плате, и только пара синхронно работающих процессоров формирует работоспособный канал. Это означает, что отказ любого ОДНОГО ИЗ ЧЕТЫРЕХ ПРОЦЕССОРОВ будет означать отказ ОДНОГО ИЗ ДВУХ КАНАЛОВ.
Поэтому совершенно неправильно считать вероятность отказа архитектуры 2*2 (HI Quad (QMR) "2oo4") как вероятность отказа ТРЕХ КАНАЛОВ ЧЕТЫРЕХКАНАЛЬНОЙ СИСТЕМЫ.

А ведь именно эта вероятность приведена на Figure 4 (рис. 1.16). К анатомии этого фокуса мы еще вернемся.

А пока обратим внимание, что при этом доктор Бэкман признает, что обе архитектуры, - и TMR, и QMR, - после первого отказа деградируют к состоянию 2 - 0 .

Это как раз и означает, что вероятность отказа любого одного из четырех процессоров архитектуры "2oo4" является вероятностью отказа того модуля, и, соответственно, канала, на котором этот процессор находится. Именно вероятность отказа любого одного из четырех процессоров будет определять вероятность отказа одного из двух каналов архитектуры "2oo4". При этом возникает еще одна особенность архитектуры "2oo4", которую Бэкман просто не замечает:

Два отказавших процессора архитектуры 2*2 могут находиться на одном управляющем модуле, - и тогда система сохраняет работоспособность одного канала и возможность восстановления в режиме *on-line*, - а могут и на разных, и тогда система не работоспособна. Это наблюдение непосредственно указывает на то, что расчет вероятности отказа архитектуры QMR "2oo4" необходимо начинать с определения вероятности отказа одного из четырех процессоров. И отказ всего одного процессора на одном из двух двухпроцессорных модулей вышибает из работы сразу оба процессора, и тем самым означает отказ всего модуля, что должно отражаться в алгоритме первого шага деградации архитектуры QMR "2oo4":

4 - (3 = 2) - 0, а не просто 4 - 2 - 0 .

Пункт №8 - Схемы деградации. В своей следующей статье *Determining the required safety integrity level for your Process, Lawrence V. Beckman, Dr. SafePlex Systems, Inc, 2001,* доктор Бэкман приводит логические блок-схемы различных систем безопасности, и режимы их деградации (рис. 1.17).

Схемы доктора Бэкмана неполны и некорректны одновременно:

- Отсутствует схема самой важной из архитектур - 1oo2D.
- Отсутствует схема "4oo6" для архитектуры 2oo3 с парой элементов в каждом канале - аналог схемы "2oo4".
- Схема архитектуры и режим деградации QMR "2oo4" некорректны.

SeisoKs)	PES	Finn! Elemкnt(s)	Configuration	Operating Mode	Channels Needed to Operate	Channels Needed to Trip
X	X	X	1001 y__ _____	1-0	1	1
X	X	X	1002 n _и	2-0	2	1
X	X	X	1003 -4n—Sf ~i f	3-0	3	1
X	X	X	2002 -OHO-	2-1-0	1	2
X	X		2003 -HHZE^Zn^U-	3-2-0	2	2
X	X	X	2004 -E^^fU-	4-2-0	2	2

Рис. 1.17

Архитектура loo2D существенно отличается от прямолинейной архитектуры 1oo2 не просто **наличием** диагностических цепей, **но специальной организацией** взаимного контроля над состоянием соседнего канала, и на основе этой информации - контроля и управления выходом системы в целом.

Конфигурация архитектуры loo2D немыслима как без учета межпроцессорного взаимодействия, так и без учета конфигурации и взаимодействия выходных диагностических цепей, и на самом деле должна выглядеть в терминах Бэкмана так, как представлено на рис. 1.18, где контакты D_0i и D02 символизируют выходные диагностические цепи, способные распознавать состояние соседнего канала. Исходная схема Бэкмана для системы QMR "2oo4" (рис. 1.19) совершенно правильно отражает главное свойство этой архитектуры: при отказе одного процессора происходит отказ того канала, на котором этот процессор находится.

Рис. 1.18 *Рис. 1.19*

Однако на этой схеме (рис. 1.19) не отражена самая главная особенность систем типа loo2D, а именно - перекрестная перепроверка состояния соседнего канала с помощью диагно-

стических цепей, а также встроенная способность контроля и управления выходом всей схемы **каждым каналом в отдельности.** А ведь именно это свойство превращает архитектуру 1oo2 в сочетание архитектур 1oo2 и 2oo2, то есть в архитектуру 1oo2D (рис. 1.20).

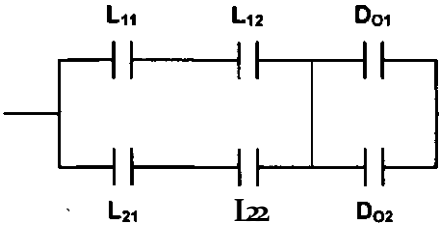


Рис. L20

Эта схема дает ясное представление, что в действительности мы имеем дело с архитектурой 1oo2D, с усиленным с помощью дополнительного процессора каналом. К чему на самом деле приводит это "усиление", мы скоро увидим. А пока можно смело утверждать, что внесение второго элемента в каждое плечо схемы в два раза увеличивает вероятность отказа каждого плеча, и, соответственно, в четыре раза - вероятность отказа системы. Из рисунков 1.18 и 1.20 понятно, что архитектуру QMR "2oo4" нужно бы обозначить как-то *породственному* с архитектурой 1oo2D:

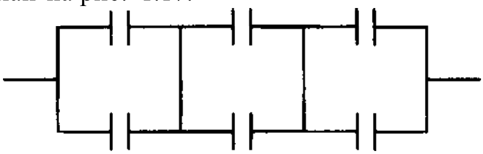
- 1oo2D (2*2),
- "2oo4", или просто
- 2*2, но уж никак не 2oo4D.

Замечание

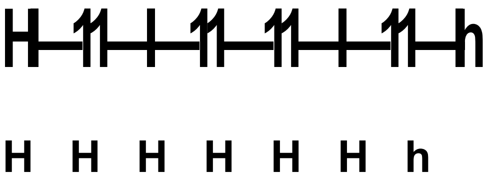
*Лучший способ проявить абсурдность некоторого утверждения - довести это утверждение до совершеннейшего абсурда. Представим, что на каждом из двух параллельных модулей мы разместили по 20 процессоров. Спрашивается: неужели кому-то пришло бы в голову определить эту архитектуру как **20 oo 40?** Напомним смысл этого обозначения:*

Для нормальной работы архитектуры из сорока имеющихся в наличии каналов необходимо не менее двадиати каналов. Но каналов-то как было два, так и осталось, и система QMR "20 из 40" по-прежнему принадлежит к семейству архитектур 1oo2.

И предпоследний казус. Доктор Бэкман не упоминает, что системы Tricon и Trident с архитектурой 2oo3 также имеют по 2 микропроцессора на каждом модуле управления. Невозможно представить, что специалист такого ранга может не знать об этом. И на самом деле логическая блок-схема центральной часуи этих систем выглядит не так, как изобразил доктор Бэкман на рис. 1.17:



а, оставаясь в рамках графической "концепции" Бэкмана, вот так:



Если быть последовательным, то по логике Бэкмана необходимо отнести эту архитектуру к классу шестиканальных систем типа 4oo6. И тогда вероятность отказа этой системы будет также пропорциональна кубу произведения A t . Если быть точным, то вероятность отказа *П - Т + 1 =* б *- 4 + 1 =* **трех** из шести каналов системы 4oo6 равна **5 • (Я** $t)^3$.

Покажем это. Вероятность опасного отказа одиночного канала в интервале времени *[0,t]* равна *At.* Для резервированных систем безопасности типа *moon (m out ofn),* вероятность отказа *(n-m+1)* каналов в интервале времени *[0,t]* в общем случае будет определяться числом различных сочетаний (п—т+1) каналов, и равна соответственно

$$C''\sim^{m+1} \cdot (A - t)^{n}\sim^{m+1} \quad _{в}$$

где $C''\sim^{т+1}$ - число сочетаний (п-ш+1) отказавших каналов из п возможных:

$$\pounds_{п-т+1} \qquad \wedge'$$

$$'' \quad \{n-m + 1У\backslash n-(n-m + 1)У \sim \{n-m + 1У\{m-1)У$$

Тогда среднее значение вероятности опасного отказа в течение временного интервала *[0,t]* определится интегрированием и усреднением по времени:

$$PFD_{moon} = \quad . \mid J\ (Л \bullet t)^{n \sim m+1} \bullet dty\ t, \text{ или}$$

$$PFD_{moon} = CI^{m+7} \bullet (Л \bullet tr^{m+1} /(n\text{-}m + 2)$$

В нашем клиническом случае это составит:

$$PFD_{4oo6} = C^{n}_{n} \sim^{m+1} \bullet (Л \bullet t)^{n \sim m+1} /(n - m + 2) -$$

$$\frac{n!}{(n\text{-}m + 1)!\text{-}(m\text{-}1)!} \quad \frac{(At)^{n \sim m+1}}{(n\text{-}m + 2)} \quad \frac{61}{(6\text{-}4 + 1)!(4\text{-}1)!} \quad \frac{(Л\text{-}t)^{6}}{(6\text{-}4 + 2)}$$

$$\frac{1 - 2\ \ 3\ \ 4 \bullet 5\ \ 6 \qquad (Л\text{-}t)^{3}}{(1\text{-}2\text{-}3)\ \ (12\ \ 3)\ \ (6\text{-}4 + 2)} \qquad \begin{matrix} з \\ (\quad) \end{matrix}$$

Несколько выше, чем для истинно четырехканальной архитектуры 2oo4, но ведь порядок все равно запредельный!

Почему же Triconex не выказывает никакого желания отнести свои трехканальные системы к архитектуре 4oo6? Да просто потому, что прекрасно понимает, что если в выражение вероятности отказа архитектуры $PFD_{2oo3} = \{A\ tf$ подставить удвоенную частоту отказа канала, то вероятность отказа так называемой системы "4oo6" составит

$$PFDuoor = [(2Я).\ t]^2 = 4\ .\ (Л.\ tf = 4\ .\ PFD_{2oo3},$$

то есть возрастет в четыре раза.

Таким образом, главное соотношение вероятностей отказа дублированных и троированных систем сохраняется и при удвоении числа элементов в канале:

$$PFD_{1oo2} : PFD_{2oo3} = PFD._{2oo4}.\ ;\ PFD._{4oo6}. = 1:3$$

Соотношение вероятностей отказа архитектур 1oo2, "2oo4", "4oo6" при прочих равных условиях составляет

$$PFD_{1oo2} : PFD._{2oo4}.\ : PFD,._{4oo6}. = 1: (1 \bullet 2^2): (3 \bullet 2^2) = 1: 4 : 12\ .$$

Таким образом, вероятность отказа архитектуры 2oo3 ("4oo6") с парой процессоров в каждом канале на порядок выше, чем для классической архитектуры 1oo2.

Небольшой комментарий.

Все, что представлено в данном разделе, представлено вовсе не для того, чтобы принизить или превознести уровень

какой-либо архитектуры. Обе модели, - и классическая loo2D, и ее модификация QMR "2oo4", - имеют исключительно высокие характеристики надежности. Но важно понимать, что ничто не возникает из ничего, и добавление новых элементов в канал, повышая уровень самодиагностики канала, в то же время никак не может уменьшить вероятность отказа, но только увеличить. И обозначить архитектуру одного-единственного модуля управления в архитектуре QMR "2oo4" как loo2D, да еще и без ограничений по времени - это неправильно. Возникает закономерный вопрос: где происходит подмена понятий?

1.14. Анатомия подмены понятий

Смысл, который скрывается за вроде бы правдоподобными рассуждениями, может ввести в заблуждение кого угодно, если не знать в точности, как работает та или иная схема. И только после детального изучения становится понятным, что "в *действительности все совсем не так, как на самом деле*

Попробуем разобраться, какую архитектуру подразумевает аббревиатура 2oo4, и внимательно рассмотрим наш случай произвольной интерпретации.

Гибридная схема "2oo4" (2*2). Структурная схема центральной части гибридной архитектуры "2oo4" выглядит следующим образом:

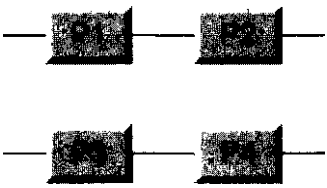


Рис. 1.21

Именно таким образом построено ядро систем loo2D, у которых ставится по два процессора на каждый из дублированных модулей управления.

Схема на рис. 1.21 совершенно точно отражает главное свойство данной архитектуры:

Отказ любого элемента канала означает отказ канала.

А поскольку канал имеет удвоенное количество элементов, то соответственно, и вероятность отказа канала по сравнению с обычной схемой резервирования удваивается. В данной работе, чтобы не смешивать архитектуру рис. 1.21 с классической архитектурой loo2D, она обозначается как loo2D (2*2) или "2oo4".

Но некоторые из особо восторженных поклонников этой схемы смело обозначают ее как архитектуру 2oo4, или того пуще - 2oo4D, и легко распространяют это обозначение на всю архитектуру системы безопасности - целиком, и без всяких кавычек. Этот простейший прием дает колоссальный эффект в увеличении надежности системы - и без малейших усилий. Посмотрим, как это делается.

Выстраивается следующая цепочка рассуждений:

1. *Данная архитектура имеет N = 4 элемента.*
2. *Отказ одного из элементов приводит к отказу всего плеча, на котором этот элемент находится, то есть выводит из работы сразу два элемента.*
3. *Система сохраняет работоспособность на оставшихся двух элементах.*
4. *Значит, для нормальной работы системы достаточно M = 2 элементов.*
5. *Таким образом, система деградирует по схеме 4-2-0.*
6. *Согласно определению, аббревиатура **MooN (M** out of N) обозначает, что для правильного функционирования системы необходимо, чтобы **M** из **N** каналов работали нормально.*

   *Если система построена на **N** каналах, и для нормальной работы системы необходимо M каналов, то это означает, что система способна пережить отказ (N — M) каналов без потери функциональности.*

   Соответственно, для отказа системы необходимо, чтобы отказали (N — M + 1) каналов.

1. *Наша система полностью соответствует этому определению: Система построена на 4 элементах, и для нормальной работы системы необходимо 2 элемента. Это означает, что система способна пережить отказ (4-2) элементов без потери функциональности.*

   Соответственно, для отказа системы необходимо, чтобы отказали (4 - 2 + 1) = 3 элемента.

8. Вывод: Система рис. 1.21 имеет архитектуру 2oo4.

Теперь, если непринужденно произвести "обратное преобразование" аббревиатуры 2oo4 в архитектуру, то удается легко интерпретировать ее уже как **четырехканальную** (хотя очевидно, что в исходной архитектуре о четырех каналах и речи нет):

1. *Как мы только что выяснили, система имеет архитектуру 2oo4.*
2. *Поскольку согласно этому определению, для нормальной работы системы достаточно двух элементов, то для отказа системы 2oo4 необходимо, чтобы отказало* $N - M + 1 = 4 - 2+1=3$ *элемента.*
3. *Вероятность отказа трех независимых элементов равняется:*

   $P2004 = Pl \quad P_2 \quad Pз = P^3 = (1-R)^3 = [1-(1-M)]^3 = (At)^3$
4. *Ч. Т.Д.*

Эта элементарная манипуляция дает возможность утверждать, что гибридная архитектура "2oo4" имеет уже не второй порядок частоты отказа, а третий. Естественно, при этом совершенно нет никакой нужды упоминать, что найденная вероятность принадлежит совсем другой, действительно *четырехканальной* архитектуре:

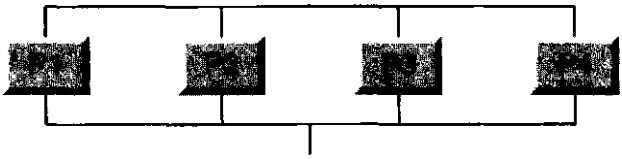


Рис. 1.22

Вот так вполне безобидный с виду ход позволяет без лишних хлопот поднять надежность системы до недосягаемой высоты. В действительности же вероятность отказа схемы 2*2 (рис. 1.21) при условии, что все элементы эквивалентны, определяется следующим соотношением:

$$P"2oo4^{ы} = (P1 + P2) \cdot (P3 + P4) = 4P^2 = 4(At)^2,$$

то есть в четыре раза превышает вероятность отказа архитектуры 1oo2.

Специфические особенности архитектуры "2oo4" подробно исследованы в настоящей работе.

Но главное свойство этой архитектуры необходимо отметить сразу:

По отношению к отказам удвоение числа элементов канала эквивалентно удвоению частоты отказа исходного элемента. А второй порядок вероятности отказа от частоты для двухканальной системы приводит к учетверенному значению вероятности отказа по отношению к системе loo2D с одним элементом в канале.

Алгоритмы самодиагностики архитектур loo2D и "2oo4" тождественны:

- Способ диагностики канала для схемы "2oo4" - сравнение результатов работы двух логических элементов.
- Способ диагностики канала для схемы loo2D - независимая диагностическая цепь.
- Способ диагностики состояния центральной части обеих архитектур - сравнение результатов диагностики каждого из каналов.

Необходимо отметить, что с помощью независимых диагностических цепей в архитектуре loo2D достигается своего рода альтернативное резервирование на основе схемной реализации.

Диагностические цепи осуществляют строго специфические функции обнаружения отказов и, соответственно, организованы гораздо более жестко по сравнению с основными процессорами.

Архитектура loo1D одного канала системы loo2D вполне может превосходить по надежности архитектуру одного канала 1oo2 системы loo2D (2*2).

На вопрос: какая из этих архитектур a priori обеспечивает более высокий уровень диагностики? - ответить однозначно невозможно. Только непосредственный опыт реализации во множестве предыдущих воплощений может придать уверенность в правильности выбора.

Именно по этой причине стандарты IEC предъявляют очень жесткие требования к полевым испытаниям систем безопасности, причем не на своем, а на чужом поле. Мы должны ясно понимать и твердо помнить, что для них таковым является наше, русское поле.

Те преимущества систем QMR, которые превозносятся энтузиастами этих систем, как то:

"The key features of the Hi Quad (Quad Modular Redundant) system are as follows:

- *Mode of Operation:*
  Unlimited Operation on a Single Channel -
  Никак не соответствует требованиям стандарта IEC 61508;
- *Rated up to TUV RC6 (SIL3)* -
  Справедливо только в конфигурации loo2D;
- *Three Times Better Safety Performance than TMR* -
  Справедливо только для обычных loo2D архитектур. Для архитектур QMR "2oo4" при прочих равных условиях все-таки несколько ниже, чем 2oo3;
- *Availability Equal to TMR (см. выше)*
- *Less Common Cause Susceptibility than TMR* -
  На то они и общие, что при прочих равных условиях производят на систему общий катастрофический эффект. Потому и сказываются в общем, то есть одинаково;
- *Lower Life Cycle Cost",* -

Эти мнимые преимущества, если и присущи системам QMR "2oo4[п]", то ровно настолько, насколько они присущи всем системам с архитектурой loo2D.

Таким образом, выводы, которые делает Бэкман в конце своей публикации, таки остаются и пребывают фактическим концом публикации:

"Conclusions: The New Quad (QMR) Architecture is a major technological enhancement in safety system performance. It provides both higher levels of safety and availability than either TMR (2oo3) or loo2D. It has significantly less susceptibility to common cause failure than TMR because of the absolute separation, isolation and operation of the redundant channels.

Because each channel has a pair of dual processors operating in the safety (2-0) mode, a dangerous undetected failure of the processors has been eliminated; and the system provides unrestricted SIL3 operation in either a simplex, selectively redundant, or fully redundant configuration.

This new architecture is highly configurable and can be used for SIL1, SIL2, and SIL3 applications. However, the most attractive advantage is a lower life cycle cost, which will enable it to be utilized effectively on both small and large safety projects.

Consequently, combining multiple process units into a single PES, in order to be cost effective, is no longer a necessity".

И соответствующий перевод:

"Выводы: Новая Quad (QMR) Architecture является главным прорывом в исполнении систем безопасности. Она обеспечивает более высокий уровень и безопасности и готовности чем TMR (2oo3) или loo2D. Она имеет значительно меньшую подверженность отказам общего порядка, чем TMR из-за абсолютного разделения, изоляции и работы резервированных каналов.

Так как каждый канал имеет пару сдвоенных процессоров в безопасном (2-0) режиме, опасные необнаруженные отказы были исключены; и система обеспечивает неограниченную по SIL3 работу как в симплексной, селективно резервированной, так и в полностью резервированной конфигурации. Эта новая архитектура является высоко конфигурируемой, и может использоваться для приложений SILl, SIL2, и SIL3.

Однако наиболее привлекательным преимуществом является более низкая стоимость жизненного цикла, которая позволяет использовать ее эффективно как в небольших, так и больших проектах.

Следовательно, сочетать несколько технологических узлов в одной программируемой электронной системе для снижения стоимости теперь нет необходимости ".

Но на этом высокохудожественном фоне в Глоссарии к статье автор скромно приводит совершенно трезвые формулировки режимов деградации рассмотренных архитек!ур:

ff2-0 Mode of operation where the dual system shuts down after the first diagnosed fault.

2-1-0 Mode of operation where the dual system shuts down after the second diagnosed fault.

3-2-0 Mode of operation where the triplicated system shuts down after the second diagnosed fault.

4-2-0 Mode of operation where the quadruplicated system shuts down after the second diagnosed fault".

Этим определениям и будем следовать.

1.15. Сертификация систем "2oo4" по стандарту IEC 61508

В настоящее время все уважающие себя производители оборудования систем безопасности должны пройти сертификацию на соответствие требованиям стандарта IEC 61508. Сертификация по стандарту IEC 61508 заставляет все расставить по своим местам, и та же архитектура "2oo4" уже занимает свое законное место - loo2D.

В подтверждение приводятся две схемы систем HIMA, которые уже идентифицированы самой же фирмой HIMA по правилам IEC 61508. На первой (рис. 1.23) представлена схема PLC H41/51-HRS с архитектурой loo2D, - та самая, что на рис. 1.10 обозначена как 2oo4. В таблице ниже схемы (рис. 1.23) поясняются действия системы при отказах:

"В том случае если данные в ДВУХ центральных модулях отличаются, и причина отказа определена программой самодиагностики, то происходит:

А) отключение ОБОИХ модулей, или работа на одном канале в течение 1 часа.

Если причина расхождения не определена, то происходит:

В) отключение ОБОИХ центральных модулей".

Конец цитаты.

И никаких четырехканальных 2oo4 и безграничных времен одноканальной работы. Та же метаморфоза произошла и с одноканальной системой H41/51-S - стандарт IEC 61508 законно требует отнести ее на вполне заслуженную позицию **loolD,** и, соответственно **RC4, SIL2** (рис. 1.24). Читаем:

"В случае отказа центрального модуля - его отключение, отключение сторожевого таймера и выходов".

Результат - ЖЕСТКИЙ ФИЗИЧЕСКИЙ ОСТАНОВ.

И никаких шестых классов и безграничной работы.

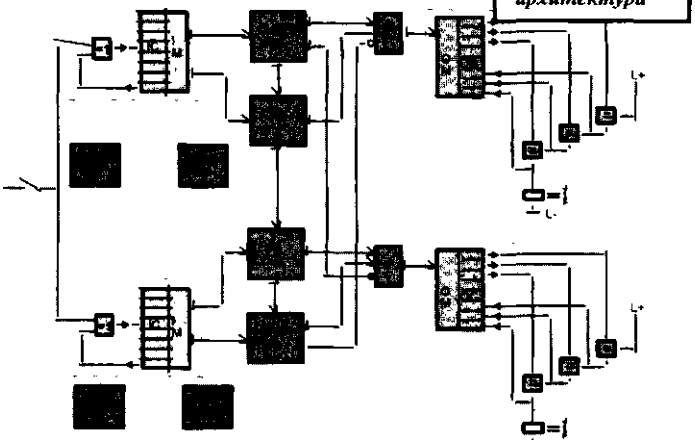
Системы безопасности фирмы HIMA по определению имеют высшие показатели надежности и безопасности, и совершенно не нуждаются в нелепых утверждениях своего превосходства. Сказать, что для перечисления систем такого класса достаточно пальцев одной руки - не сказать ничего: *ровно половина* пальцев останется без применения. Вместе с тем, безусловно, существует "тонкое расщепление" характеристик различных архитектур. И этому будет уделено достойное внимание на всем протяжении настоящей работы.

Standard IEC 61508

System Structure of the 1oo2D«Svstem. RC 6. SIL 3

Systems H41-HRS, H51-HR

Реальная архитектура



Range	Test	Reaction to Failures
0 modules	Same tests as in the 1oo1 system	Same reactions like in the 1oo1 system
Central Module (PE)	Same tests in the central modules as *in* the 1oo2D-system with one IO bus if the data in the two central modules is different- A) More than 99 % of the failures will be detected by the test routines B) The test *тыр*^y*&mX* detect a failur^>^\>^ata do differ	Display as in the 1oo2D system with one IO bus A) Switch-off of both central modules or ^ time limited single channel operation up to 1 h (defined in the user's program), depending on plant B) Switch-off of both CMs
Coupling to IO modules	Test ofUj^^><reing,	Same reaction like in the 1oo2D system with bus in the one 10
1 ^		
Действия системы в случте расхождения ДВУХ ufMtHn/irtkHkir ылЛкпей (tuiiaTgna)	6	

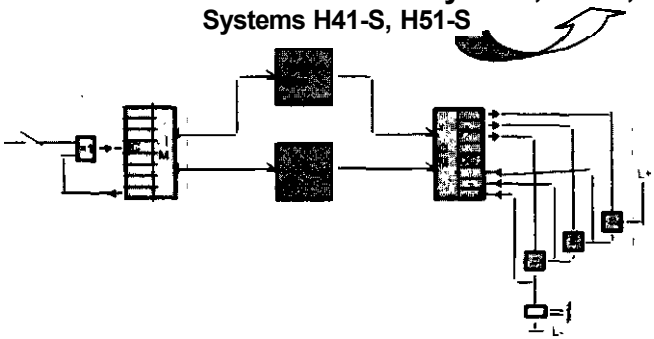
.. the safe decision.

Рис. 1.23

Standard IEC 61508

System Structure of the 1oo1D System, RC 4, SIL 2

Systems H41-S, H51-S



Range		Reaction to Failure
Input Module digital	Correct function of the module Crosstalk of the input circuits Function of the input filters	Display position of faulted module L-signal in user's program
analog	as digital, additionally Linearity of the AD converter Test of transmitter supply voltage	Processing of the defined value in the user's program
Central Module (PE)	intensive self tests Check (CRC) for static memory and read/write test for variable memory ranges. Direct and inverted memory with steady hardware comparison in background Diverse time bases, te le watch dog (switch off capabi	Switch-off of the central module, watchdog signal and outputs Display STOP on PE
Coupling to input/output modules	Test of the addressa functionality	Switch-off of the related IO modules in the subrack Display of the number of the faulted subrack
Output Modules digital	Read bapf ^Comparison with the internal Xgnal Swjfr ^pability Cr rf the channels	Display position of the faulted module Switch-off of the output module (simple failure) Switch-off of the coupling module/IO subrack (double failure)
analog	tal additionally eirity of the DA converter	

Действия системы в случае отказа ЕДИНСТВЕННОГО центрального модуля

the safe decision.

Рис. 1.24

1.16. Непрерывность контроля и защиты

Термин "Непрерывность" отсутствует в современных стандартах МЭК, однако активно используется отечественными поставщиками оборудования систем безопасности. Проследим историю его возникновения. Термин возник в результате некорректного использования понятия *Safety Availability* - Готовность, доступность, работоспособность - термин американского стандарта ANSI/ISA 84.01-96. В стандартах IEC 61508 и IEC 61511 данное понятие отсутствует. Фактически это понятие используется многими без ясного понимания того, что оно включает в себя два аспекта:

- Динамическая, или мгновенная готовность, как функция работоспособного существования технического устройства во времени. Эту функцию и называют непрерывностью.
- Стационарная готовность, как усредненная характеристика надежности за какой-то период времени.

Динамическая готовность $A(t)$ - это величина, характеризующая вероятность того, что система выполнит предопределенную функцию защиты в момент возникновения необходимости ее выполнения, в течение всего наперед заданного интервала времени.

Стационарная готовность выражается в процентах, и определяется средним временем работы до отказа $MTTF$ и средним временем восстановления после отказа *MTTR (Mean Time To Repair)* по следующей формуле:

$$Л = \frac{MTTF}{MTTF + MTTR} \quad 100\% = \frac{MTTF}{MTBF} 100\%$$

Уже Стандарт ISA 84.01-96 рекомендовал вместо стационарной готовности использовать более точное понятие "Вероятность опасного отказа выполнения требуемой функции - PFD". Тем не менее, Стационарная готовность активно используется наряду с прочими усредненными и вероятностными характеристиками технических устройств.

Стандарт IEC 61508 также использует только аналог стационарной готовности, точнее, неготовности, и определяет ее как Среднюю вероятность опасного отказа выполнения требуемой функции - *Probability offailure on demand-* PFD_{AVG} .

И используются только стационарные решения, полученные к тому же полуэмпирическим путем, а не в результате решения динамических моделей.

Важное замечание

Динамическая готовность A(t) - это попросту Надежность системы R(t) во времени:

A(t) = R(t), тогда PFD(t) = 1 - R(t).

Реальное понимание процессов, происходящих с оборудованием систем безопасности, а уж тем более исследование их возможного поведения невозможно без динамики. Тем более вполне может статься, что в реальности стационарное состояние окажется вообще недостижимым.

И все же понятие "Непрерывность" в смысле Динамической готовности практически исключено из технического обихода ввиду абсолютной бесперспективности получить его аналитическое выражение для реальных систем.

Готовность систем существенно возрастает для малых времен обнаружения неисправности. Быстрое обнаружение неисправности в современных электронных системах достигается применением автоматических процедур самотестирования и выводом подробной диагностической информации.

Однако необходимо подчеркнуть, что если отказ привел к останову процесса, то время восстановления может сильно увеличиться, поскольку запуск производства "несколько" отличается по времени от времени замены модулей.

Готовность системы защиты может быть увеличена посредством резервирования, например, при параллельной работе центральных модулей, модулей ввода-вывода, и применением нескольких сенсоров в каждой точке измерения. Резервные компоненты встраиваются в систему таким образом, что отказ одного компонента не сказывается на общем функционировании системы. Очень важным компонентом готовности является подробный вывод диагностической информации.

"Непрерывность" - динамическая готовность, - которую якобы могут обеспечить только системы 2oo3, принадлежит к одному из многочисленных мифов, созданных проводниками оборудования систем 2oo3.

Непрерывность - динамическая готовность - свойство, в равной степени присущее ВСЕМ резервированным системам типа loo2D и 2oo3. Система просто должна быть надежной.

1.17. Сравнение надежности архитектур loo2D и 2oo3

В монографии автора "*Основы построения АСУТП взрывоопасных производств*", Синтег, 2006, приводятся результаты расчетов вероятностей отказов для базовых архитектур систем безопасности - от loo1 до 2oo3. Результаты этих расчетов довольно впечатляющи. В частности, неожиданным оказался следующий результат:

При прочих равных условиях, а именно однородность и однотипность составных элементов, вероятность всех видов отказа систем типа 2oo3 в три раза выше вероятности всех видов отказа систем типа loo2D.

Данное обстоятельство объясняется тем, что вариантов отказа тройной системы в три раза больше, чем для системы loo2D. Сказанное подтверждается прямым счетом возможных вариантов отказа, и всех возможных путей к этим отказам.

В данном разделе мы рассмотрим сравнительную устойчивость архитектур loo2D и 2oo3 по отношению к ложным остановам.

В стандартах МЭК и само понятие ложного останова, и, тем более, расчеты интенсивности и вероятности ложного отказа отсутствуют.

Вероятность ложного срабатывания архитектуры loo2D. В исходном состоянии система loo2D по отношению к ложным срабатываниям работает по схеме 2oo2. Для совершения внепланового останова необходимо, чтобы оба канала дали команду на останов. Поэтому для определения частоты ложных срабатываний системы необходимо учесть последовательность развития событий.

Вероятность ложного срабатывания системы будет определяться условной вероятностью повторного отказа $P(P_{SP2}1$ **Pspi** $)$ течение времени существования первого отказа. Свершиться ложный останов может двумя путями:

- Сначала выдает ложную команду первый (условно) элемент, затем - второй.
- Сначала выдает ложную команду второй (условно) элемент, затем - первый.

Приведем эти предпосылки к символическому виду (таблица 1.1).

Таблица 1.1

Ch1	Ch2	System	Интенсивность ложных отказов
+	+	+	: -
sp		+	*SP1*
sp	*sp*	*sp*	*ASP1 'PsP2*
+	+	+	. -
+	*sp*	+	*SP2*
sp	*sp*	*sp*	*&sp2 'P$pt*

Здесь

Pgp2 = P(PSP21 Pspi) ~ ASp2 ~условная вероятность отказа второго элемента (канала) после отказа первого;

Pspi = Pspi I Psp2) Лspi ~условная вероятность отказа первого элемента (канала) после отказа второго;

г - некоторое характеристическое время существования одиночного отказа.

Следовательно, интенсивность ложных срабатываний определится выражением

$$4SP = Л_3P2'(A_SP1't) + AsP1'(Л\$P2\text{-}T) = 2\text{-}ЯSPJ'Л_{8P2} \cdot T$$

При = ^SP1 4sP

$$y1oo2D\_n2oo2\_o\ 12 \approx SP$$

Вероятность ложного срабатывания архитектуры 2оо3. В системе 2оо3 ложное срабатывание происходит по следующему элементарному алгоритму:

Команда на ложный останов может быть выдана любой парой из трех наличных элементов (каналов). А поскольку число сочетаний из 3 по 2 равно трем (1-2, 1-3, 2-3), то и частота ложных срабатываний по сравнению с системой loo 2D утраивается.

Что и подтверждается прямым счетом. Рассмотрим все возможные состояния системы 2оо3, и все возможные пути, приводящие к ложным срабатываниям (таблица 1.2).

Таблица 1.2

Ch1	Ch2	Ch3	System	Интенсивность ложных отказов
+	+	+	+	
*SP_*	+	+	+ ~ ~	; ^*SPI*
sp	*sp*	+	*sp*	^*SP1 'PsP2* = ^*SP1 '(^SP2 '*
sp	+	*1 sp*	*i sp*	5 ^*SP1 'PsP3* = *ASP1 '(A-SP3 '*
+	+	+	+	-
+		+	+	
sp	*sp*	1 +	I sp	; ^SP2 * *Psp1 ~ ^SP2 ' (A$P1 ' t)*
+	sp	j sp	*sp*	*; ^SP2 'PsP3* = *^SP2 '(ASP3 '*
+	+	+	+	
	+	sp	+	^*SP3*
sp	+			*^SP3 '^SP1 ~ ASP3 '(Asp1 't)*
+	*SP*		*sp*	*A-SP3 'PSP2 ~ ASP3 '(ASP2 't)*

Поскольку $A_{SP1} - A_{SP2} = A_{SP3} - A$,

получаем:

$AV?^3 = 6 - Alp - г$

Полученное утроенное соотношение частоты и вероятности отказов систем loo2D и 2oo3 соблюдается для всех видов отказов.

Когда знаешь правильный ответ, то сказанное объясняется довольно просто. Согласно определению,

MooN (M out of N) *- специфическая аббревиатура для обозначения и определения архитектуры систем безопасности. Данное сокращение обозначает, что для правильного функционирования системы необходимо, чтобы т из п каналов работали нормально.*

Если система построена на n каналах, и для нормальной работы системы необходимо m каналов, то это означает, что система способна пережить (n-m) отказов без потери функциональности. Соответственно, для отказа системы необходимо, чтобы отказали (n-m) + 1 каналов.

Поэтому основной характеристикой является число сочетаний по *(n-m) + 1* элементов из *n* имеющихся элементов:

$$Q_{n-m+f} \sim (n-m+1)!(m-1)!$$

Число сочетаний для системы 1оо2 равно 1, а для системы 2оо3 - трем. Соответственно вероятность отказа системы 1оо2 определяется всего одним сочетанием:

$$P_{1oo2} = P_{1-2>}$$

а системы 2оо3 - тремя:

$$P_{2oo3} = P_{f-2} + P_{из} + P_{2-3} \sim 3 \cdot P_{f-2} \cdot$$

То же соотношение соблюдается и с учетом перестановок - обе вероятности синхронно удваиваются. Именно по этим причинам конфигурация 2оо3 до последнего времени использовалась, в основном, в схемах резервирования датчиков, причем на альтернативной основе. А вот анализ достоверности их показаний возлагался собственно на PLC системы защиты.

В настоящее время появилась уникальная возможность проверки готовности полевого оборудования к выполнению функций защиты *on-line* с помощью специально выделенных автономных систем обслуживания, диагностики и управления оборудованием производства - *Plant Asset Management Systems.* **Поэтому необходимость применения таких дорогостоящих конфигураций, как 2оо3, - даже для датчиков, - отпадает.**

Яркими примерами таких систем являются *Asset Management Solutions (AMS)* фирмы Emerson, и *Plant Resource Manager (PRM)* фирмы Yokogawa Electric.

С появлением протоколов HART *(Highway Addressable Remote Transducer)* и цифровой полевой шины Fieldbus системы этого рода находят все большее применение в АСУТП, и дают колоссальный эффект выявления отклонений, сбоев и отказов полевого оборудования в оперативном режиме.

1.18. Сравнение схем деградации архитектур loo2D и 2oo3

Один из не убиенных аргументов, которых превозносится нашими перепродавцами оборудования в качестве неоспоримого преимущества, выдвигается тот, что система 2oo3 теоретически позволяет продлить свой жизненный цикл до трех шагов деградации: 3 - 2 - 1 - 0 (Характерно, что западные сторонники и пропагандисты систем 2oo3 его старательно избегают). Однако необходимо быть осведомленным, что *в конце пути придется рассчитаться*, и расплачиваться придется по гамбургскому счету.

Необходимо помнить, что ПРИНЦИП ДИАГНОСТИКИ СИСТЕМЫ 2oo3 - ГОЛОСОВАНИЕ. Поэтому после отказа одного из каналов 2 оставшихся в работе канала системы 2oo3 - ЭТО НЕ РЕЗЕРВИРОВАНИЕ, а последний рубеж, на котором система сохраняет возможность самодиагностики.

Для архитектуры loo2D, в отличие от архитектуры 2oo3, таким рубежом является одноканальная работа по схеме looID. При этом канал полностью контролируется диагностическими цепями. Если восстановление системы loo2D в течение предопределенного интервала времени не произошло, производится программно-контролируемый останов производства.

Совсем иная ситуация с переходом на одноканальную работу системы 2oo3. В случае отказа одного из двух оставшихся в работе элементов исчезает и возможность самодиагностики. И лучшее, что вы можете сделать - немедленно отключить систему, снять питание с выходов и физически остановить процесс. Причем о восстановлении исходной конфигурации в течение 1 часа не может быть и речи:

Если вы не удосужились восстановить конфигурацию 1 oo2 до исходного состояния 2oo3 в течение нескольких месяцев, смешно рассчитывать, что вы сможете это сделать из непредсказуемой конфигурации 1oo1 в течение 1 часа, тем более после только что произошедшего по неизвестной причине отказа второго процессора.

Эту особенность двухканальной работы системы 2oo3 можно отметить как схему деградации **3-2-(1-0),** чтобы подчеркнуть тот факт, что предпоследний канал скорее мертв, чем жив.

I и И)

По отношению к схеме деградации 3-2-1-0 создатели систем 2oo3 находятся в патовой ситуации:

- С одной стороны, - хочется продлить "путь к последнему приюту" до однопроцессорной работы, но тогда придется создавать уровень самодиагностики, соответствующий уровню систем 1oo1D и 1oo2D.
- А с другой, - создание этих дополнительных диагностических цепей дискредитирует саму идею голосования, как попытку обойтись малой кровью.

Если чисто гипотетически разрешить архитектуре 2oo3 деградацию до одноканальной работы, то после первого отказа система переходит на работу по схеме 1oo2, и здесь возникает совершенно курьезная ситуация:

Отказ одного из каналов архитектуры 2oo3 приводит к трехкратному уменьшению вероятности опасного отказа системы! Напрашивается детский вопрос: Так может, в таком случае и изначально система 2oo3 должна работать в двухканальном варианте? Как мы неоднократно будем иметь возможность убедиться на протяжении настоящей работы, это предложение имеет под собой серьезные основания:

Система 2oo3 в архитектурном отношении является избыточной. Действительно, если продлить разрешение для двух оставшихся каналов работать по схеме деградации 2 - 1 - 0, то вероятность повторного опасного отказа составит $P_{1oo2} = P_{2oo3} / 3$. Но, к сожалению, при этом одновременно с уменьшением вероятности опасного отказа, вероятность ложного срабатывания становится максимально возможной из всех существующих архитектур:

Для архитектуры 1oo2 вероятность ложного срабатывания в два раза выше, чем для одноканальной системы 1oo1. Тем не менее, система 2oo3 такова, какова она есть, и безопасной она может быть только при работе по схеме 3-2-0, и не нужно пытаться выжать из нее больше, чем она может дать. Схема деградации 3-2-1-0 - не более чем рекламный трюк. И не дай Бог пытаться проверить его на практике.

Необходимо ясно понимать, что два работающих канала системы 1oo2D, и два работающих канала системы 2oo3 - это две большие разницы. Для архитектуры 2oo3, два оставшихся в работе процессора после первого отказа - это не резервирование, а средство самодиагностики.

Отказ любого из них означает отказ системы и немотивированный физический останов процесса.

Именно по этой причине стандартно после первого отказа система 2oo3 переходит на работу по схеме 2-0, прямо указывая на необходимость немедленного восстановления исходной конфигурации.

Формальное "*разрешение*" одноканальной работы для архитектуры 2oo3, аттестуемой по максимальным для перерабатывающих отраслей промышленности категориям RC6 (DIN), SIL3 (IEC 61508, ISA 84.01), чревато еще более серьезными последствиями, чем изначальная установка пресловутых "*безграничных*" систем 1oo1D на объектах с уровнем требований RC6 и SIL3. Именно поэтому потенциальная *возможность* перехода от схемы 2oo3 через схему 1oo2 к схеме 1oo1 никогда не может стать даже потенциальной *реальностью.* Как только отказывает один из каналов системы 1oo2, система тут же самоустраняется, и снимает с себя всякую ответственность за ложный физический останов. Для систем с архитектурой 1oo2 единственный рациональный алгоритм действий после отказа одного из двух каналов - это полный останов:

1. Снять питание с выходов. Тем самым
2. Запустить полный **программно-неуправляемый аппаратный останов** процесса.
3. Провести автономное восстановление системы:
   - Замена отказавших модулей,
   - Автономное тестирование,
   - Запуск системы и тестирование в рабочем режиме *(on-line).*

Ровно таков алгоритм действий и одноканальной системы с самодиагностикой - 1oo ID. Поэтому применение систем 1oo2, равно как и систем 1oo1D, ограничивается всеми авторитетными надзорами классом RC4 (DIN), и интегральным уровнем безопасности SIL2 (IEC 61508, ISA 84.01-96).

Так в чем же разница между архитектурами 1oo1D и 1oo2 и полной конфигурации, и архитектурой 2oo3 после частичною отказа? И в архитектурном, и в функциональном отношении - ни в чем. Более того, схема 1oo1D в своем классическом представлении (рис. 1.25) при определенных условиях вполне может быть даже более надежной, чем схемы с дублированными процессорами (рис. 1.26 и 1.27):

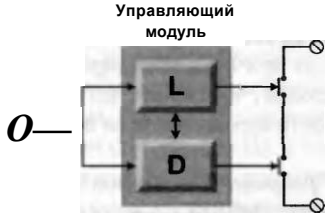


Рис. 1.25

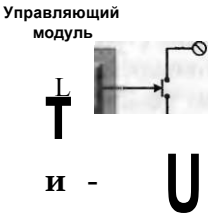


Рис. 1.26

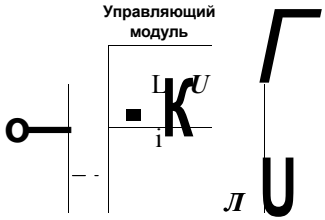


Рис. 1.27

При этом невозможно даже с определенностью отнести представленные конфигурации к какому-то определенному типу архитектуры:

- *Схема рис. 1.25 - это и архитектура loo ID, и архитектура центральной части loo2D после частичного отказа;*
- *Схема рис. 1.26 - это и архитектура loolD, и архитектура центральной части loo2D ("2oo4") после частичного отказа;*
- *Схема рис. 1.27 - это и архитектура 1oo2, и архитектура 2oo3 после частичного отказа, и даже архитектура центральной части некоторых систем loo ID (см. рис. 1.15)!*

Разница состоит в интерпретации способа диагностики:

- *В одном случае диагностическая цепь или сравнение центральных процессоров интерпретируется как средство самодиагностики, и схема обозначается как loolD.*
- *В другом случае схема интерпретируется как схема голосования, и обозначается как архитектура 1oo2.*

Но вне зависимости от интерпретации все три схемы работают совершенно одинаково:

При любом сбое в работе модуля управления питание с выходов системы снимается, и происходит физический останов процесса. TUV совершенно справедливо аттестует представленные схемы одинаково - по RC4 и SIL2.

Очевидно, что для обеих схем рис. 1.26 и 1.27 работа на одном процессоре абсолютно исключена - системы полностью теряют самоконтроль, и результат их работы становится непредсказуем.

Архитектура loo2D исторически возникла самой последней из известных систем, как результат многолетних поисков архитектуры, сочетающей

- Устойчивость архитектуры 1oo2 по отношению к опасным отказам (несрабатыванию),
- Устойчивость архитектуры 2oo2 по отношению к ложным остановам,
- И развернутой самодиагностики, и взаимной диагностики каналов.

Принцип диагностики систем loo2D - это не просто наличие индивидуальных диагностических цепей и на модулях ввода, и на модулях управления, и на выходных модулях. Если бы особенности архитектуры loo2D ограничивались только *наличием* диагностических цепей, система никогда не смогла бы подняться выше архитектуры 1oo2. Коренное отличие систем loo2D состоит в том, что перекрестная взаимопроверка каждым каналом работоспособности соседнего канала позволяет осуществить непрерывный контроль состояния соседнего капала, и в случае его отказа взять на себя управление состоянием выхода системы в целом. Именно этот принцип дает возможность сохранить полноценную работу системы на время восстановления исходной конфигурации.

Таким образом, функциональным аналогом одноканальной работы системы loo2D является двухканальная работа системы 2oo3, а не одноканальная, как могло бы показаться с первого взгляда. Причем система loo2D имеет дополнительное преимущество, которое выражается в том, что диагностическое резервирование осуществляется на альтернативной основе, то есть диагностические цепи используют жесткие схемные решения, построены на собственной элементной базе

повышенной надежности, и предназначены для выполнения исключительно специфических задач диагностики.

Специалисты TUV хорошо понимают опасность одноканальной работы - для систем любой конфигурации. Приведем выдержку из отчета TUV по сертификации одного из контроллеров фирмы Triconex. *Report-No. 968/EZ 105.03/01 "Type approval of TRICON version 9.6" от 1 сентября 2001 года, стр. 8, п. 3.2, абзац второй (отчет можно посмотреть на сайте TUV* ***www.tuv-fs.com):***

"For an application class 6 ESD system, the system is allowed to continue operation for one hour with one channel, if the other two channels have failed. This is true for applications equal or higher than class 5.

IT IS SAFER TO SHUT DOWN THE PROCESS TO THE SAFE STATE THAN TO CONTINUE OPERATION WITH ONLY ONE CHANNEL IN OPERATION FOR A PERIOD LONGER THAN THE RECOMMENDED PERIOD".

Русским языком по-английски написано:

"Для использования в качестве системы ПАЗ 6 класса, системе разрешается продолжить работу на одном канале в течение 1 часа, если другие два канала отказали. Это справедливо для объектов равных, или выше 5 класса". И далее:

"БЕЗОПАСНЕЕ ПЕРЕВЕСТИ ПРОЦЕСС В БЕЗОПАСНОЕ СОСТОЯНИЕ, ЧЕМ ПРОДОЛЖАТЬ РАБОТУ НА ОДНОМ КАНАЛЕ В ТЕЧЕНИЕ БОЛЬШЕГО ПЕРИОДА, ЧЕМ РЕКОМЕНДОВАННЫЙ ПЕРИОД". Приложение В данного отчета дает еще более жесткие рекомендации:

Уже при отказе ОДНОГО из трех плеч (legs) на входном, выходном модуле, или отказе центрального процессора^ОТЕ 1) настоятельно рекомендуется произвести замену отказавшего компонента в течение принятого в отрасли среднего времени на замену.

Однако Triconex трактует ситуацию с отказами по-своему:

" To keep the PFD within industry-acceptable guidelines, adherence with the recommended maximum operating period of 1500 hours in dual mode and 72 hours (SIL3/AK5) or 1 hour (SIL3/AK6) in single mode should be observed",

Источник цитаты - "Safety Considerations Guide, Tricon, version 9, 2001, Triconex Corporation of Invensys Company", Chapter 3 "Fault Management, Operating Modes", стр. 41:

"Для того чтобы удержать PFD в пределах, приемлемых для промышленности, нужно руководствоваться следующими правилами:

1. *Максимальный период работы на двух каналах - 1500 часов;*
2. *Одноканальная работа -*
   - *72 часа для SIL3 / АК5;*
   - *1 час дляБИЗ/АКб."*

Причем никакого обоснования этих цифр, и никаких расчетов в руководстве не приводится. К подобным рекомендациям надо подходить очень внимательно, поскольку увеличение допустимого интервала работы в неполной конфигурации выше разумных пределов приведет в лучшем случае к внеплановому останову производства.

Особенно должно насторожить, что предлагаемые правила расходятся с рекомендациями TUV. Любопытно посмотреть, что по тому же поводу рекомендует TUV для контроллера Quadlog для работы по 6 классу. Смотрим Отчет о сертификации контроллера Quadlog "*Report to the Certificate U 0012 40001 003 Safety Critical Programmable Logic Solver, Siemens Energy & Automation" от 10 апреля 2003 года, таблица 2.5.1, стр. 11-16 (можно посмотреть на сайте* www.sea.siemens.com/process/docs/MS122496CREV3_3.PDF):

"Shutdown of defective module and continued operation for a period of time defined by the manufacturers PFD calculation for a specific system or if no calculation is done, 72 hours (Note 1) and shutdown of the system /group after this time period".

II случае отказа одного из модулей:

"Отключить дефектный модуль, и продолжить работу в течение периода времени, определяемого расчетами производителя вероятности опасного отказа PFD для конкретной системы, или, если эти расчеты отсутствуют, произвести останов системы или отключение группы модулей после 72 часов".

Примечательно, что для одноканальной работы по всем классам вплоть до 6-го рекомендовано 72, а не 1 час, как для контроллера Tricon. И замечательно, что производитель сисюмы Quadlog не имеет ни малейшего желания воспользоваться лазейкой, и увеличить рекомендуемое время одноканальной работы ну, например, хотя бы при отказе входного модуля.

Просто люди ясно понимают, что разрешение на работу в неполной конфигурации в течение нескольких месяцев может стать гибельным для установки. Таким образом, обе системы при однократном частичном отказе имеют законное право:

- Продолжить работу в течение предопределенного интервала времени с выдачей соответствующего сообщения, и с ожиданием оперативного восстановления исходной конфигурации.
- Осуществить по команде оператора программно-управляемый останов процесса, если в течение предопределенного интервала времени восстановление невозможно.
- По окончанию предопределенного интервала времени самостоятельно снять питание с выходных реле, и инициировать физический останов процесса.

1.19. Оптимальность архитектуры **loo2D**

Вначале необходимо пояснить принципиальную разницу между системами 1oo2 и loo2D.

Как сказано в стандарте IEC 61508 по поводу системы 1oo2:

"Предполагается, что любое диагностическое тестирование будет только извещать об обнаруженных сбоях, и не будет изменять состояния выходов, или изменять выходное голосование

Как сказано в стандарте IEC 61508 по поводу системы loo2D:

"Для системы с расширенной диагностикой loo2D, если диагностика обнаруживает отказ в любом из каналов, процедура голосования строится таким образом, что выход системы будет контролироваться другим каналом.

Если диагностическое тестирование обнаруживает отказы в обоих каналах, или обнаруживает расхождение, которое не может быть приписано к какому-либо из каналов, то выход системы переводится в состояние останова ("безопасное" состояние).

Для того чтобы расхождение между каналами могло быть обнаружено, каждый из каналов должен иметь возможность определять состояние другого канала с помощью средств, независимых от проверяемого канала

Однако в стандарте не поясняется, что же это за средства, независимые от другого канала? В данном случае - это не просто "возможность определять состояние другого канала", а оригинальное сочетание архитектур 2oo2 и 1oo2, позволяющее использовать диагностические цепи в качестве дополнительной пары каналов, построенных на альтернативных элементах и совершенно иных схемных решениях. Оба диагностических тракта работают таким образом, что без перекрестного подтверждения соседний канал не сможет выдать команду на изменение выхода.

Поэтому символ "D" в данной архитектуре означает не просто расширенные возможности диагностики, а особым образом организованное взаимодействие управляющих и диагностических цепей, позволяющее фактически реализовать реальную квадро - систему, имея:

- Два канала обработки информации, и
- Два диагностических тракта, которые с учетом перекрестного взаимодействия фактически исполняют роль дополнительной пары каналов.

Учитывая особую значимость систем класса loo2D, приведем классические образцы реальных систем с данной архитектурой.

Система H41-HRS, H51-HRS (HI Quad) фирмы HIMA

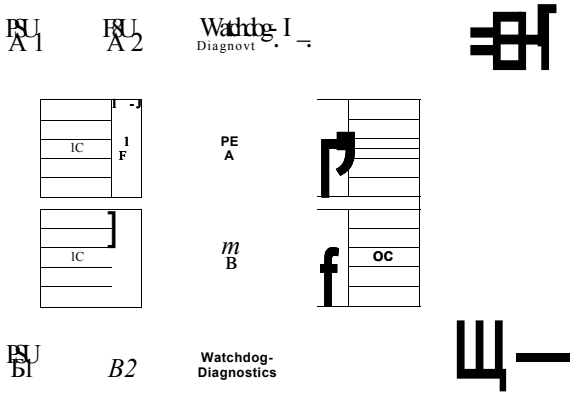


Рис. 1.28

Система QMR FSC ("2oo4D") фирмы Honeywell

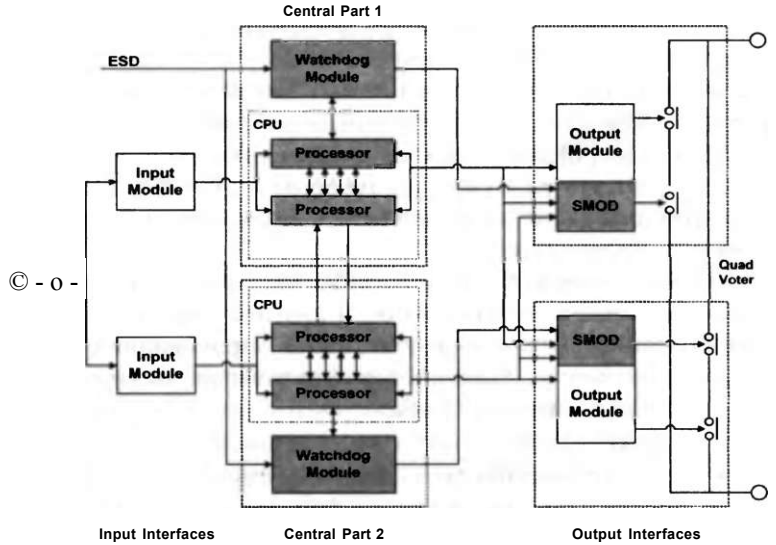


Рис. 1.29

Система QUADLOG фирмы Siemens Energy & Automation

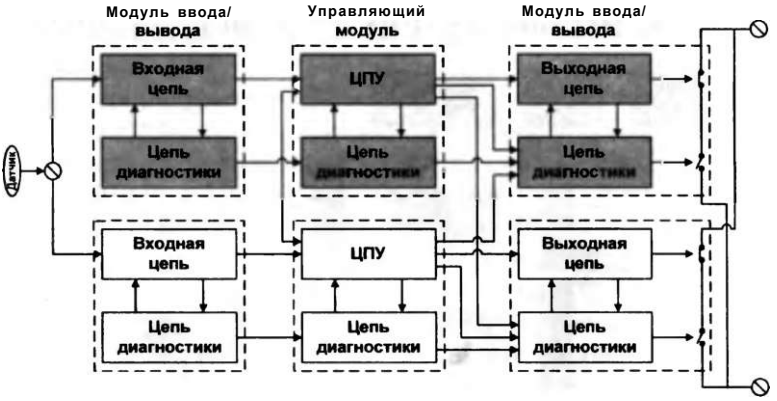


Рис. 1.30

Высокий уровень безопасности и отказоустойчивости в архитектурах loo2D достигается за счёт дублирования всех модулей - и управляющих, и ввода-вывода.

Система loo2D - это полностью резервированная архитектура с всесторонней диагностикой и дополнительным трактом безопасного отключения системы, который управляетея независимым диагностическим каналом.

Именно в системах с архитектурой loo2D параллельно работают четыре канала - два основных и два диагностических, благодаря чему достигается наивысший для программируемых электронных систем уровень безопасности и отказоустойчивости.

Система разделена на две эквивалентные подсистемы, работающие синхронно, и полностью резервирующие друг друга. В том случае, когда система диагностики обнаруживает неисправность в одной из подсистем, эта подсистема отключается, и управление не подхватывает, а **продолжает** другая подсистема. После того, как работоспособность неисправной подсистемы будет восстановлена, она включается в работу, полностью восстанавливая двойную схему резервирования архитектуры loo2D. В отличие от многих других систем управления и защиты, архитектура loo2D позволяет монтировать резервирующие друг друга подсистем на раздельных шасси, которые могут размещаться в раздельных шкафах и в разных помещениях.

Такая возможность минимизирует подверженность резервирующих друг друга подсистем общим внешним воздействиям, таким как повышение температуры или обрыв линии питания в одном из шкафов, пожар в одном из помещений и т.д. В данной архитектуре предусматривается защита выходных цепей, а также многие другие механизмы, обеспечивающие более безопасные решения, чем традиционная архитектура программируемых логических контроллеров и систем управления. В выходных каналах, как правило, используются дублирующие разнотипные элементы. Нормальный выход основного управляющего канала контроллера построен на твердотельном полупроводниковом ключе. Выходное электромагнитное реле, управляемое встроенной системой диагностики, предоставляет дополнительную возможность управления состоянием выхода. При обнаружении опасного отказа в выходном канале реле может быть автоматически обесточено, что обеспечивает безопасное отключение канала.

Высокая отказоустойчивость архитектур loo2D достигается также благодаря резервированию таких ключевых элементов системы, как источники питания и коммуникационные магистрали. Согласно технической документации, диагностика систем с архитектурой loo2D гарантирует обнаружение более 99,95% неисправностей. В целом и по вероятности всех типов отказов, и по балансу ограничений на работу в неполной конфигурации, системы loo2D явно предпочтительнее прочих архитектур.

1.20. Основные выводы сравнения

Нельзя выдавать средство диагностики - два работающих канала из трех возможных в архитектуре 2oo3, а средство повышения уровня самодиагностики, - два работающих на одной плате процессора в архитектуре 2*2 ("2oo4") - за резервирование каналов. Архитектуры "2oo4" и 2oo3 имеют столько каналов, сколько они имеют - 2 и 3. Разница между ними состоит в том, что в архитектуре 2oo3 резервные модули управл^рия являются средством диагностики, и после отказа одного модуля два оставшихся составляют последний рубеж, на котором архитектура сохраняет способность контролировать свое поведение.

Для архитектуры QMR "2oo4" отказ одного из процессоров означает отказ канала - именно это и выражено формулой 4-2-0. Эта архитектура по определению не может работать по схеме 4-3-2-1-0, ведь у нее только два канала, а не четыре. Единичный отказ процессора на одном модуле выводит из работы сразу два процессора, то есть весь канал целиком. Отказ двух процессоров, находящихся на дйух разных модулях, означает полный отказ системы. Потому-то и установлены в соответствии со стандартом IEC 61508 такие жесткие требования TUV к системе QMR HI Quad "2oo4".

Именно по этой причине архитектуры QMR "2oo4" не рассматриваются в качестве самостоятельных архитектур в стандарте IEC 61508. Эти архитектуры занимают самое достойное место в общей иерархии систем - loo2D, то есть принадлежат к тому классу систем, которые имеют самые высокие показатели по надежности и безопасности из всех ныне существующих, и без всяких натяжек.

Уникальность систем loo2D вне зависимости от числа процессоров на плате состоит совершенно в другом:

Два набора модулей управления в сочетании с двумя наборами диагностических цепей создают уникальную четырехполюсную архитектуру, которая имеет минимально возможную вероятность отказов среди всех известных на сегодня архитектур.

1.21. Протоколы Internet-мудрецов

Протокол **Ethernet** (стандарт IEEE 802.3) - наиболее распространенная технология локальных вычислительных сетей. Протокол Ethernet использует топологию типа звезда или общей шины с типом доступа *Carrier Sense Multiple Access with Collision Detection (CSMA/DC)* для управления загрузкой линий связи.

Протокол CSMA/CD изначально создавался для конторских применений, не ориентированных на работу в жестко детерминированном реальном времени. И строго говоря, он не годится для систем управления технологическими процессами, поскольку технически невозможно гарантировать точное время отклика на событие (см. рис. 1.31).

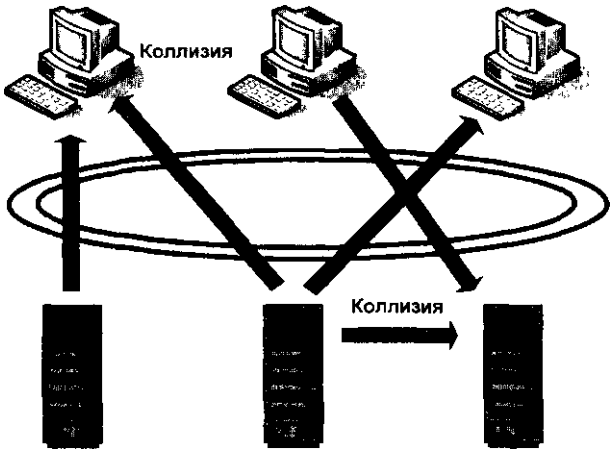


Рис. 1.28

Алгоритм работы сети на базе протокола CSMA/CD выглядит следующим образом: любая из станций может инициировать передачу данных в произвольный момент времени. Несколько сообщений, переданных в один адрес, могут вступать в противоречие друг с другом - коллизию. В таком случае выполняется повторная посылка. Соответственно, чем больше станций в сети, тем больше возникает коллизий, и тем больше времени требуется для передачи сообщений.

Гарантированного интервала времени для завершения передачи не существует.

Charles E. Spurgeon в своей книге "*Ethernet: The Definitive Guide", O'Relly and Associates*^ 2000, приводит блестящую аналогию. Он пишет, что работа протокола CSMA/CD проистекает как товарищеский ужин в темной комнате:

"Каждый из сидящих за столом должен дослушать говорящего, прежде чем заговорит сам (Carrier Sense). Как только появляется просвет в разговоре, каждый из присутствующих имеет равные шансы сказать что-нибудь (Multiple Access). Если два человека начинают говорить одновременно, они тут же обнаруживают этот факт, и прекращают разговор (Collision Detection)".

Переведем на язык Ethernet:

Каждый из интерфейсов должен дождаться того момента, когда канал освободится, и только тогда он может начать передачу. Если кто-то другой уже осуществляет передачу, то в канале появляется признак, называемый носителем *{Carrier).* Все другие интерфейсы должны ждать окончания передачи, и освобождения канала перед тем, как сделать попытку собственной передачи. Этот процесс называется *Carrier Sense.*

Все интерфейсы Ethernet равны в своей способности посылать сообщения в сеть. Никто не может иметь более высокий приоритет по отношению к кому-либо другому. Именно это подразумевает множественный доступ *(Multiple Access).*

Поскольку прохождение сигнала по сети требует времени, первый бит переданного пакета не может достичь всех узлов одновременно. Следовательно, вполне реальной становится ситуация, когда два интерфейса решают, что сеть свободна, и начинают передачу в одно время.

Когда это происходит, Ethernet распознает "коллизию" *(или "ситуацию" в понимании Льва Давидовича Ландау),* оста-

навливает передачу, и проводит ее повторно. Называется все это *Collision Detect.* Протокол CSMA/CD сконструирован для прямого доступа к общему каналу так, чтобы все станции имели возможность воспользоваться сетью. После каждой передачи очередного пакета, станции используют протокол CSMA/CD для определения, какая из станций воспользуется каналом следующей.

IP - Internet Protocol. Сетевой протокол. Данные путешествуют по сети IP в форме пакетов. Каждый пакет состоит из заголовка (источник, получатель, и информация о самих данных), и собственно самого сообщения.

TCP/IP (Transmission Control Protocol / Internet Protocol). Базовый протокол Интернета TCP отвечает за предоставление данных для передаваемых пакетов, и сборки их в пункте назначения. Протокол IP отвечает за доставку пакетов от источника к получателю. Когда TCP и IP встраиваются в приложения более высокого уровня, такие как HTTP, FTP, Telnet и т.д., то термином TCP/IP обобщается весь набор этих протоколов. Условная схема передачи сообщения иллюстрируется на диаграмме рис. 1.32.

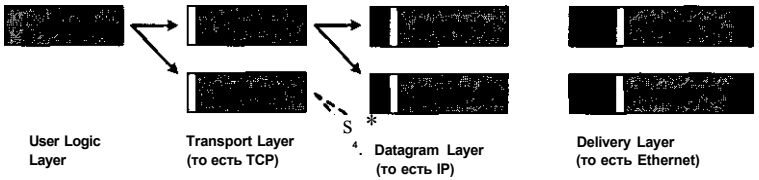


Рис. 1.32

Хотя протокол TCP/IP обычно ассоциируется с сетью Интернет, он может использоваться и в локальных сетях (ЛВС). В этом случае при невысокой загруженности магистрали он обеспечивает приемлемую скорость передачи данных.

Однако в последнее время протокол TCP/IP стал использоваться в качестве транспортного протокола для обмена информацией между узлами гибридных систем автоматизированного управления технологическими процессами.

Общий цикл сканирования сети. Для того чтобы доступ к ресурсам сети осуществлялся корректно, все сетевые интерфейсы должны иметь возможность отвечать на события в течение вполне определенного интервала времени.

Цикл сканирования складывается из времени получения сигнала и времени выдачи управляющего воздействия. Этот временной отрезок называется общим циклом сканирования *cncTQMu(round trip time).*

Максимально возможная длительность цикла сканирования должна быть жестко ограничена с тем, чтобы каждый узел сети гарантированно получал и выдавал сообщения в течение заданного интервала времени.

Чем больше некоторый сегмент сети, тем больше времени требуется для передачи сообщений. Общее требование к конфигурации сети состоит в том, что заданный цикл работы сети должен соблюдаться при любых обстоятельствах, независимо от размера и сочетания сегментов. Руководства по конфигурации определяют правила комбинации сегментов с повторителями *(repeaters),* чтобы соблюсти временные ограничения для сети в целом.

Если спецификации по длине и комбинации сегментов не соблюдаются, синхронизация сети нарушается, компьютеры не могут общаться в требуемых временных пределах, и могут вообще прекратить взаимодействие.

Более сложные сети, построенные на разнородных сетевых ресурсах, строятся в соответствии с правилами построения мультисегментных конфигураций по стандарту Ethernet. Эти правила включают ограничения на общее количество сегментов и повторителей, которое может быть в сети для соблюдения временных ограничений на цикл сканирования.

Протокол с эстафетной передачей ISO 8802-4/IEEE 802.4. Передача эстафеты осуществляется по следующим правилам (рис. 1.33):

- Только одна станция может инициировать передачу.
- В станции может находиться только один *Token* (Жетон, Эстафета).
- Каждая станция может начать передачу в соответствии с циклом сканирования сети, например, раз в секунду.
- Таким образом, возможность появления коллизий исключена - *Token* пробегает по всем станциям сети за 1 секунду.
- Гарантируется односекундный отклик на событие.

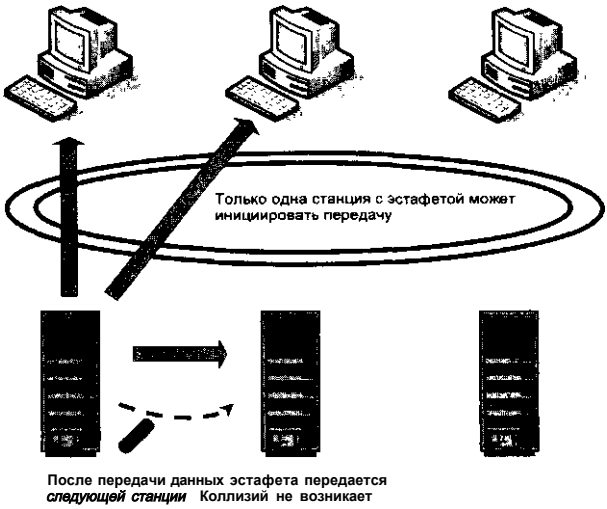


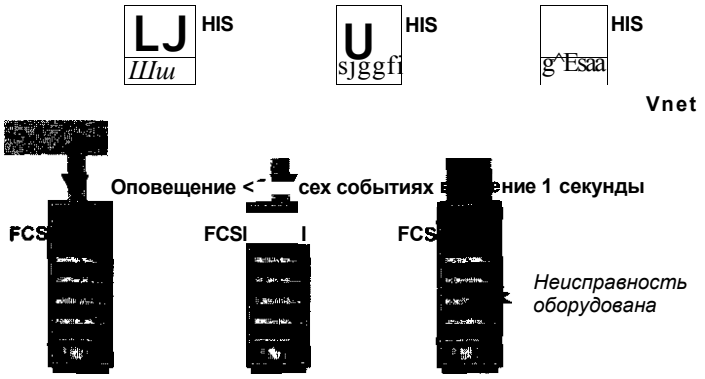
Рис. 1.33

Существует яркий пример многолетнего успешного применения этого протокола. В системах семейства Centum фирмы Йокогава используется протокол Vnet (ISO 8802-4/IEEE 802.4) с эстафетной передачей сообщений. Centum гарантирует односекундный цикл взаимодействия всех станций системы (см. рис. 1.34, 1.35).

Коммуникационный протокол Vnet. Детерминированный протокол с эстафетной передачей систем семейства Centum, соответствующий стандарту ISO 8802-4/IEEE 802.4, носит название Vnet. Для уменьшения нагрузки на сеть используется метод управления по событиям. Передаче подлежат тэги и данные. Пакеты данных не подвергаются компрессии, поэтому упрощается программное обеспечение, и соответственно возрастает его надежность.

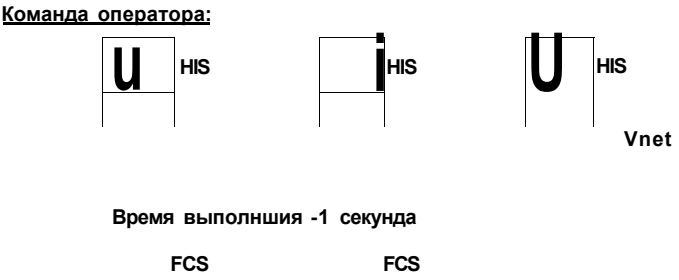
Во многих гибридных системах управления используются различные модификации протокола Ethernet на основе *Carrier Sense Multiple Access with Collision Detection (CSMA/CD),* соответствующие стандарту ISO 8802-3/IEEE 802.3. Сущность его сводится к тому, что каждый узел сети отслеживает загрузку линии, и осуществляет передачу только тогда, когда определяет, что линия свободна.

Если из-за того, что другой узел также требует линию для передачи, возникает коллизия, то оба узла прекращают передачу. Чтобы избежать повторной коллизии оба пережидают некоторое произвольное количество времени перед следующей попыткой передачи.



J K *Превышение предела по температуре*

Рис. 1.34

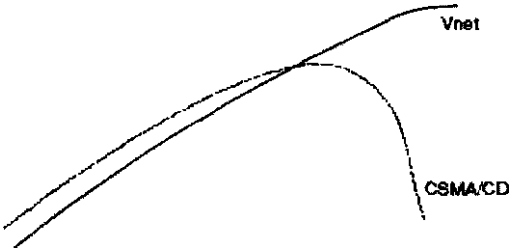


Закрытие отсекателя •

Рис. 1.35

В результате нагрузка на сеть возрастает, а реальная пропускная способность по сравнению с потенциальной пропускной способностью существенно уменьшается (см. рис. 1.36).

Верхний предел пропускной способности сети



Информационная нагрузка на сеть

Рис. 1.36

Чтобы уменьшить нагрузку на сеть, используется компрессия данных. Однако компрессия и декодирование в свою очередь увеличивает нагрузку процессоров. Это естественно сказывается на надежности и собственно самих данных, и человеко-машинного интерфейса, и станций управления.

Протоколы Ethernet (CSMA/CD) и его интернетовские надстройки типа TCP/IP вполне применимы для офисных приложений, когда вероятность коллизий невелика. Но для систем управления технологическими процессами, где предъявляются жесткие требования к циклу сканирования и безусловному выполнению функций реального времени, исследование ограничений на их применение в реальных приложениях должно быть проведено очень тщательно.

Поэтому когда преподносится, что некая гибридная система с сетевым протоколом Ethernet TCP/IP способна включать 100 контроллеров, 60 рабочих станций, 30,000 сигналов ввода-вывода и 50,000 архивируемых тэгов, но не говорится, каков при этом гарантированный цикл сканирования всей этой прорвы оборудования и информации, остается только руками развести.

Сравнительные характеристики протоколов Vnet (ISO 8802-4/IEEE 802.4) и Ethernet (CSMA/CD - ISO 8802-3/IEEE 802.3) приведены в таблице 1.3.

Таблица 13

Сравнение характеристик протокола Vnet (ISO 8802-4/IEEE 802.4) и Ethernet (CSMA/CD - ISO 8802-3/IEEE 802.3)

Item	ISO 8802-4/IEEE 802.4 (Vnet)	ISO 8802-3/IEEE 802.3 (CSMA/CD & TCP/IP)
Possibility of access competition	• None	• Large
Response	• Response time is Deterministic. • Retry time is of Millisecond order	• Response time is not Deterministic. • Retry time is of Second order
Communi-cation perform-ance	•High. • Uses only three layers of ISO/OSI model (Open System Interconnection)	• Lower than Vnet. • Ethernet based on CSMA/CD uses full seven Layers of ISO/OSI model
Dual redundant bus control	• Bus communication card perform control. • Each bus used Alternately	• CPU performs the control. • Each bus is inde-pendent (In some cases, each bus has a different IP address)
Standard compatibility	• Conforms to ISO 8802-4 / IEEE 802.4	• Conforms to ISO 8802-3 / IEEE 802.3. • There is no dual redundant Standard
Maintain-ability	Can support the follow-ing functions: • On-line FCS addition • FCS start and stop • Crash-dump function	Many competitors' sys-terns cannot support the functions listed in the left column

1.22. Номенклатура современных систем управления и защиты

ПЛК - Программируемые логические контроллеры *(PLC - Programmable Logic Controllers).* Компактные технические устройства, изначально предназначавшиеся исключительно для логического управления дискретными процессами и операциями в машиностроении, автомобилестроении, на складском оборудовании. С развитием микроэлектроники стали применяться и для управления непрерывными процессами.

Человеко-машинный интерфейс *(HMI - Human Machine Interface).* Пакеты специального программного обеспечения, представляющие собой средства опосредованного взаимодействия оператора и технологического процесса.

Гибридные системы *(Hybrid systems).* Системы, занимающие по своим характеристикам промежуточное положение между ПЛК и РСУ. Возникли в результате развития ПЛК, и во многом сохранили их достоинства и недостатки. По преимуществу предназначены для применения в процессах, сочетающих большое количество дискретных операций с непрерывным управлением в таких отраслях промышленности, как фармацевтика, цементная, пищевая промышленность, водоподготовка и т.д.

СКАДА - Системы сбора данных и оперативно диспетчерского управления *(SCADA - Supervisory Control and Data Acquisition).* Специализированные программно-технические средства, изначально предназначавшиеся исключительно для сбора информации и слежения за состоянием оборудования на значительном удалении средствами телеметрии (например, на магистральных трубопроводах). Кроме сбора информации от ПЛК, обеспечивают и человеко-машинный интерфейс HMI - PLC.

Неприятной особенностью СКАДА систем является то, что в отличие от РСУ, конфигурирование собственно контроллера и интерфейса взаимодействия с оператором (HMI) производится раздельно, и в разных программных средах со всеми проблемами избыточных тэгов, отладки и согласования баз данных. С развитием микроэлектроники СКАДА системы в составе гибридных систем стали претендо-

вать на место РСУ в управлении технологическими процессами. Вот он, классический гибрид:

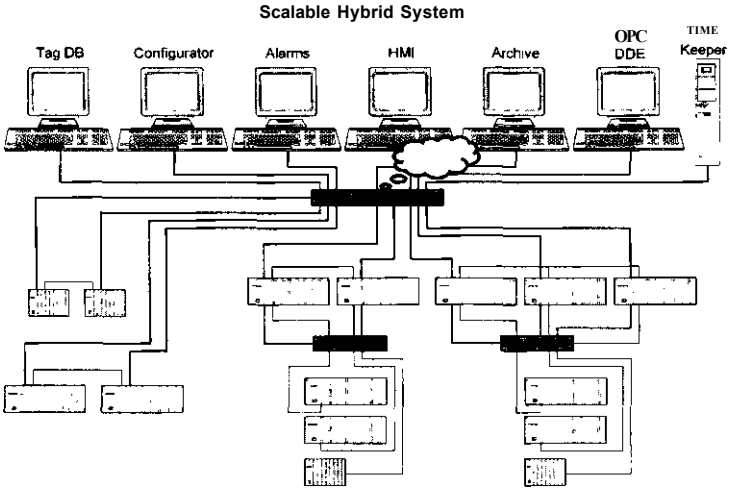


Рис. 1.37

Примечание

Необходимо обратить внимание, что вся деятельность системы происходит через одну точку - ту самую, из которой пар идет. Вообще звезды и коммутаторы ~ это патологически врожденные качества данных архитектур (рис. 1.38).

Причина состоит в том, что все гибридные архитектуры выросли из так называемых SCADA систем - систем, состоящих из набора контроллеров и серверов с человеческим лицом - человеко-машинным *интерфейсом.* Но этот подход имеет и гораздо более серьезные причины для беспокойства, чем корявость архитектуры и недетерминированная производительность.

Рассмотрим последний пример (рис. 1.39). Большей каши из гейтвеев, эрэсов, писиаев, мультидропов и прочей чепухи и представить себе невозможно. И это при том, что еще не показаны хабы и роутеры! Однако утверждается, что этот ухабистый путь и есть магистральный путь открытой архитектуры в АСУТП. В данном случае необходимо обратить внимание на поставленную на рис. 1.39 кривую стрелку справа, направленную в центр системы.

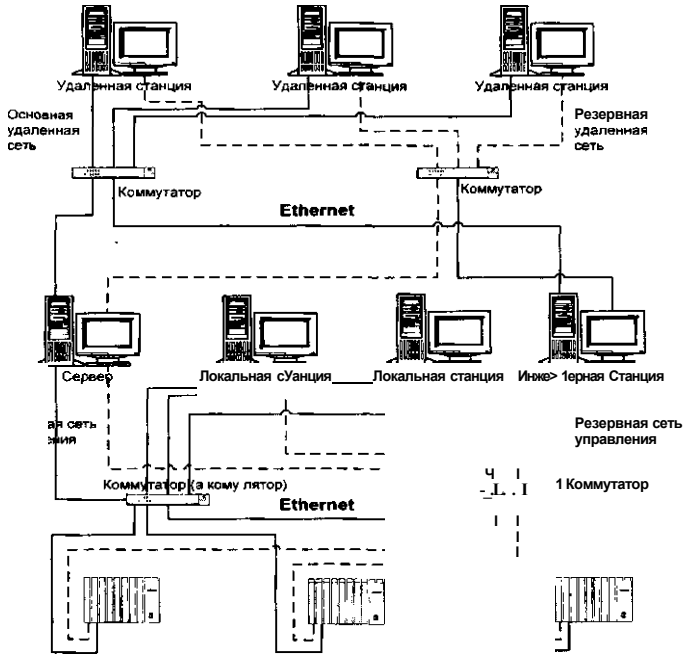


Рис. 1.38

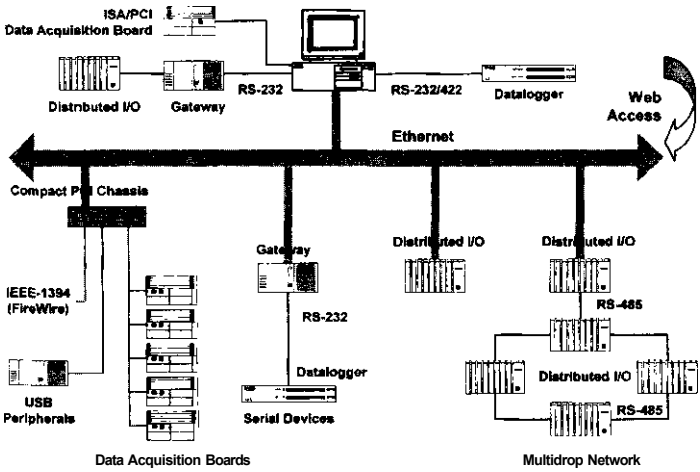


Рис. 1.28

Мы наблюдаем НЕПОСРЕДСТВЕННЫЙ WEB-ACCESS ко ВСЕМ ИНФОРМАЦИОННЫМ ПОТОКАМ И РЕСУРСАМ СИСТЕМЫ - от контроллера до сервера.

По прогнозам многих авторитетных специалистов, которые являются экспертами в решении проблем информационной безопасности, промышленные сети будут атаковать всё новые поколения вирусов, способных незаметно проникать в сети предприятий, и надолго оставаться в них совершенно незамеченными. Как бы в насмешку над гибридными системами, появились новые типы гибридных вирусов, поведение которых в корне отличается от традиционных вирусов. Это так называемые полиморфные вирусы, использующие машинно-независимые способы инфицирования и распространения, и способные приносить разрушительный ущерб. Они успешно преодолевают системы защиты прошлого поколения, поэтому для защиты от них необходима комплексная многоуровневая защита, прежде всего на шлюзах Интернет, серверах и рабочих станциях систем управления. В отличие от традиционных вирусов, которые требовали действий оператора для их активизации, гибридные вирусы распространяются автоматически, сами, выискивая слабые места в сетях и информационно-управляющих системах без участия человека.

РСУ - Распределенные системы управления *(DCS - Distributed Control Systems).* Системы управления на базе специальной вычислительной техники, предназначенные для использования исключительно в технологических процессах. Строятся на основе отказоустойчивой высоконадежной вычислительной техники промышленного исполнения для долговременной круглосуточной эксплуатации на технологических объектах, для которых последствия отказа представляют серьезную угрозу для оборудования, для жизни и здоровья людей. Традиционно РСУ ассоциируются с управлением непрерывными технологическими процессами, но реально они обеспечивают весь спектр задач управления - от чисто дискретного до программно-логического управления периодическими процессами и рецептурами.

Приведем пример классической РСУ (см. рис. 1.40). Система имеет распределенную архитектуру на уже известной нам детерминированной общей шине Vnet.

Какой разительный контраст со скадоподобными гибридами, со всеми их роутерами, серверами и хабами, и архитектурами типа звезда!..

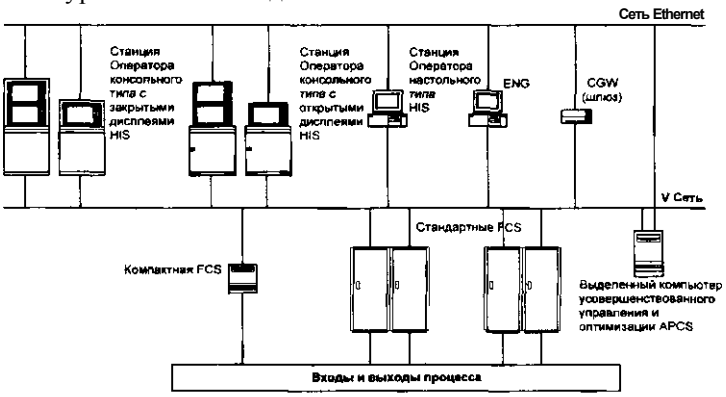


Рис. 1.40

1,23. Открытые системы

Производители PLC/HMI и гибридных систем пророчат и приветствуют применение Ethernet-протокола на всех уровнях информационно-управляющих систем - от контроллеров до корпоративных сетей - как олицетворение глобальной ОТКРЫТОСТИ. Желание вполне понятно по опыту Интернета - тотальный контроль, от которого никуда, никому, и никогда не укрыться.

Внимательный взгляд на рисунок 1.40 мог бы заметить, что представленная система также использует протокол Ethernet. Однако есть принципиальная разница: сеть Ethernet проживает **вовне** системы, и система вполне может обойтись и без нее. Внутри системы используются собственные уникальные высокоскоростные шины с детерминированными протоколами. Только с учетом этого обстоятельства и будем в дальнейшем понимать термин "Открытая система":

Открытая система - это система, способная в рамках предопределенных условий к расширению и развитию, и имеющая контролируемый внешний интерфейс, проходящий по границе системы.

Причем для расширения и развития системы допускается использовать только разрешенное оборудование и программное обеспечение. Наиболее серьезные производители гибридных систем, как, например, фирма Эмерсон, также заявляют, что для нормальной работы системы DeltaV необходимо использовать только лицензированное фирмой оборудование, включая персональные компьютеры. И это правильно.

Если бы еще удалось полностью отказаться от использования в АСУТП самой "открытой", и уже фактически ставшей единственно возможной средой обитания - операционной среды Windows, и вернуться к ОС РВ хотя бы типа UNIX, - все и вовсе стало бы на свои места.

1.24. Адекватность начальных условий

Заказчик системы должен получить ясные ответы на следующие вопросы:

- Есть ли у поставщика, разработчика, проектировщика опыт практической реализации подобных проектов?
- Есть ли вообще опыт работы предлагаемого оборудования на объектах аналогичного класса? Каковы результаты?
- Способен ли разработчик системы провести предварительное обследование производства и дать конкретные рекомендации по повышению безопасности процесса?
- Каковы минимальные требования к архитектуре системы (включая требования по модернизации полевого оборудования), чтобы система удовлетворяла необходимому уровню безопасности?
- Каковы должны быть конкретные значения вероятностей отказа элементов, составляющих систему, чтобы результирующие характеристики системы соответствовали требуемому уровню безопасности?

Ибо как показано на рис. 1.2, наибольшее количество ошибок проекта предопределяется именно начальными условиями - на стадии подготовки исходной спецификации оборудования и функций системы.

Между тем понятие предпроектного обследования производства как-то незаметно уходит, а может, и совсем уже ушло

из жизни. А ведь именно на стадиях "Формирование требований к АСУТП", "Разработка концепции АСУТП" и стадии "Разработка Технического задания" даже в стесненных денежных обстоятельствах определяются поэтапные меры по модернизации производства.

Чем больше усилий вложено в тщательный анализ процесса на предпроектных стадиях, тем меньше изменений придется вносить во время проектирования и разработки, при пуско-наладке, и дальнейшей эксплуатации и обслуживании АСУТП.

1.25. Требования МЭК к полевым испытаниям системы

В данной работе неоднократно подчеркивается, что для того чтобы система считалась прошедшей полевые испытания, стандарты IEC 61508 (Часть 7, п. В.5.4) и IEC 61511 (Часть 4) требуют, что должны быть выполнены следующие условия *(For field experience to apply, the following requirements must have been fulfilled):*

- 10 систем в различных приложениях.
- Неизменная спецификация.
- 10^5 рабочих часов (11,42 года, или по году на систему) и, как минимум, 1 год сервисного обслуживания.

Сведения о том, что система прошла испытания на практике, должны быть предоставлены в виде документов изготовителем или поставщиком системы.

Эта документация должна содержать, как минимум

- Точное предназначение системы и ее компонентов, включая контроль версии оборудования;
- Послужной список системы с указанием потребителей и даты внедрения;
- Время эксплуатации;
- Процедуры для выбора систем под конкретные приложения и варианты применения;
- Процедуры для выявления отказов, их регистрации, а также их устранения.

Тщательное и точное соблюдение этих жестких требований должно быть обязательным условием при выборе конкретного генподрядчика и поставщика оборудования.

1.26. Требования МЭК к испытаниям компонентов программного обеспечения

Программное обеспечение не ломается, однако подвержено систематическим ошибкам, поэтому компонентам программного обеспечения или программным модулям можно доверять только в том случае, если они уже проверены на практике на соответствие требуемому уровню интегральной безопасности. В особенности для комплексных компонент системы с многочисленными функциями (например, операционные системы), необходимо знать, какие из этих функций действительно были проверены на практике.

Если для определения отказов оборудования предусмотрена процедура самотестирования, но отказы оборудования не имитировались в процессе пуско-наладки, и не отрабатывались во время эксплуатации, то никто не может утверждать, что функции обнаружения неисправностей проверены на практике.

Для исключения необходимости расширенной перепроверки или перепроектирования системных программных модулей при каждом новом применении, должны быть выполнены нижеследующие требования, которые позволят удостовериться, что программные модули и компоненты оборудования свободны от систематических ошибок конструкции и/или от оперативных отказов. Для проверки программного обеспечения стандарты IEC 61508 (часть 7, C.2.10) и IEC 61511 (часть 4) требуют:

- 10 систем в различных приложениях.
- Неизменная спецификация.
- Вероятность неопасных отказов в течение года 10^{-5} с доверительной вероятностью 99,9%.
- Отсутствие опасных отказов.

Для проверки того, что компонент или модуль программного обеспечения отвечает всем этим критериям, следующие позиции должны быть документированы *(must be documented)*:

- Точная идентификация системы и ее компонентов, включая контроль версии программного обеспечения и соответствующего оборудования;
- Послужной список системы с указанием потребителей и даты внедрения;
- Время эксплуатации;

- Процедуры для выбора системы под конкретные применения,
  и варианты применения;
- Процедуры для выявления отказов, их регистрации, и их устранения.

1.27. Степень доверия к заявленному уровню интегральной безопасности

При выборе приемлемой системы безопасности часто рассматривается только часть системы - собственно программируемый контроллер, да и то лишь его центральная часть, и совершенно упускается из виду надежность всего контура безопасности, начиная от датчика, и заканчивая исполнительным элементом. Стандарты IEC 61508 и IEC 61511 предписывают рассматривать систему безопасности комплексно, целиком. Причем подчеркивается, что в общей структуре отказов существенную долю отказов несут именно полевые устройства. Поэтому при создании систем безопасности основной упор должен делаться на модернизацию и резервирование специального полевого оборудования с возможностью оперативной диагностики в режиме *on-line* на основе протоколов HART и Fieldbus. Главное, что необходимо предусматривать при создании, и обеспечивать при эксплуатации систем безопасности - это возможность оперативной диагностики и тестирования, как в ручном, так и в автоматическом режиме. Увеличение частоты тестирования за счет использования систем оперативного обслуживания полевого оборудования - один из ключевых факторов повышения надежности системы.

Полевое оборудование сертифицируется на допуск для применения в системах безопасности наравне с ПЛК. При этом основной упор делается на уровень самодиагностики. Использование протоколов типа HART и Fieldbus позволяет создать самостоятельную подсистему обслуживания полевого оборудования, независимую от РСУ и ПАЗ. Это решение при грамотном применении способно на порядки повысить уверенность в дееспособности полевого оборудования.

Однако необходимо помнить, что смысл имеет только ВЕСЬ КОНТУР безопасности. Датчик - это всего лишь один из компонентов контура.

Надо просчитать SIL для всего контура, и затем для ВСЕХ критических функций безопасности при конкретной конфигурации системы. Общий уровень SIL для комбинации из трех групп компонентов:

- Датчики,
- Логические контроллеры,
- И клапаны

совсем не обязательно будет соответствовать желанному уровню SIL3. Сводный SIL должен просчитываться для каждого конкретного случая.

Строго говоря, априорно заданное значение интегрального уровня безопасности для любого из компонентов систем безопасности противоречит самому определению данного понятия стандартами МЭК.

Пример из стандарта ANSI/ISA 84.01-1996. В целом высококачественный стандарт американского общества приборостроителей ANSI / ISA 84.01-1996 приводит диаграмму А.1 *(Приложение А, секция А.3, стр.50).*

При этом на диаграмме (см. рис. 1.41) заранее и без всякого обоснования рядом со схемами (слева) приводятся конкретные значения уровня интегральной безопасности SIL.

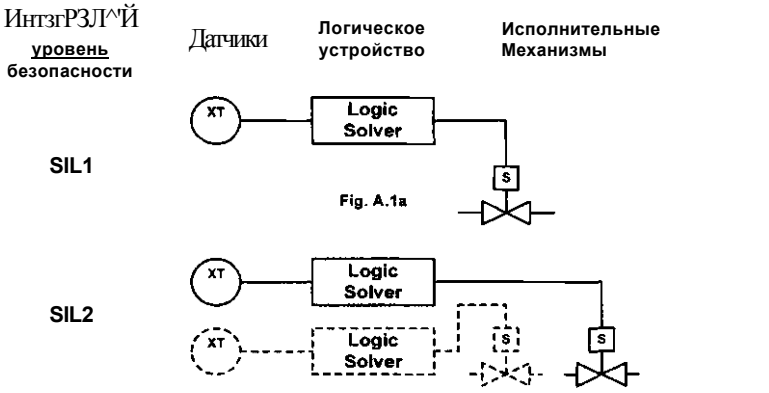
Как мы могли убедиться при рассмотрении нашего примера, априорное задание уровня безопасности, принятое только на основе *количества* оборудования, совершенно некорректно, и способно ввести в заблуждение.

И хотя эта диаграмма в стандарте имеет подзаголовок *"Example only" - "Только для примера*" - она активно используется дилетантами от автоматизации в качестве конкретной рекомендации авторитетного зарубежного стандарта.

К детальному обсуждению этого важнейшего аспекта применимости электронных средств в промышленности мы будем постоянно возвращаться в последующих главах настоящего руководства.

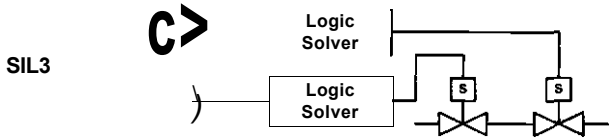
Интегральный уровень безопасности может определяться только в реальной конфигурации оборудования. Технические характеристики отдельных устройств должны содержать не абстрактное значение SIL, взятое с потолка, а исходные данные по частоте опасных и безопасных отказов, на основе которых и будет определен интегральный уровень безопасности оборудования **в конкретном приложении.**

В этой связи очень важно понимать следующее: когда поставщик импортного оборудования гордо заявляет, что его система имеет сертификат TUV на работу по уровню SIL3 (а какой же еще?!), то вы должны ясно понимать, что в данном случае речь идет вовсе не о "системе", а всего лишь о разрозненном наборе устройств или модулей для данного брэнда - по одной штуке каждого типа.



Замечание 1: Датчики, исполнительные механизмы и ПЛК могут быть дублированы в соответствии с требованиями непрерывного обеспечения безопасности.

Fig. A.1b



Замечание 2: Работа двух идентичных однонанальных систем может и не совпадать с работой одной многоканальной системы по уровню обеспечиваемой безопасности.

Fig. A.1c

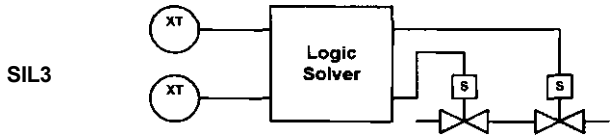


Fig. A.1d

Рис. 1.28

Кроме модулей, проверке и сертификации подлежит программное обеспечение на минимально необходимой для этого конфигурации системы, и соответствующая системная документация. В лучшем случае вы получаете следующие документы:

- Certificate,
- List of approved modules,
- Safety Reference Manual,

в чем легко убедиться, если набрать http://www.tuv-fs.com /plclist.htm, и выбрать любую из представленных в таблице *"List of Type Approved Programmable Electronic Systems (PES, PLCs)"* торговых марок. Повторяю: именно торговых марок, брэндов, шильдиков, а вовсе не некую базовую, или потенциально возможную, или какую-то еще систему, а тем более уж никак не какую-либо конкретную конфигурацию. Поэтому для нашего потребителя речь может идти только о потенциальной возможности того разрозненного оборудования, которое проходит под данным брендом, соответствовать заявленному уровню. Более того, очень полезно обратить внимание на ремарку, набранную самым мелким шрифтом, и на которую никто не обращает внимания:

Remark

There are considerable restrictions on the use of the PES in safety related applications, especially for the timing restrictions after faults have been detected. These timing restrictions are depending on calculations or applications. Refer to the detailed test reports of the respective TIJV test institute.

Зная это, перепродавцы продолжают предлагать индивидуальные устройства, будь то контроллеры или полевые устройства, как сертифицированные на определенный уровень SIL продукты. Те производители и поставщики, которые дорожат своей репутацией, даже после всеобъемлющего тестирования в испытательных лабораториях рекомендуют применять новые устройства только в некритичных приложениях, чтобы и пользователь, и производитель могли выявить все ошибки, не обнаруженные в лабораторных условиях. Применение совершенно новых, нигде не испытанных технических устройств только на основе эффектных презентаций - большой риск. И пусть эти устройства испытываются где-нибудь в другом месте, но не на наших технологических объектах.

Глава 2

СОВРЕМЕННАЯ КОНЦЕПЦИЯ АВТОМАТИЗАЦИИ

2.1. Термины и определения

Терминология стандартов Международной Электротехнической Комиссии IEC 61508 и IEC 61511 чрезвычайно усложнена (например, вместо общепринятого понятия "Надежность" используется понятие "Полноты, цельности, целостности безопасности"), но она необходима для их понимания. Впрочем, есть и обратные примеры:

Вместо нечетко определенного термина "Готовность", который к тому же имеет несколько толкований, используется конкретный термин "Вероятность опасного отказа", как дополнение к готовности.

Но так как ряд общепринятых и традиционных терминов и понятий продолжают активно использоваться, в настоящей работе они сохранены.

2.2. Оборудование и устройства

Функциональный узел *(Functional Unit).* Сущность *(entity)* оборудования или программного обеспечения, или и того, и другого, способная следовать определенной цели *(вот он - IEC 61508 во всей своей красе!).*

Контролируемое оборудование (IEC 61508) *(Equipment Under Control - EUC).* Машины, оборудование, аппараты или установки, предназначенные для производства, переработки, транспортировки, медицины и других видов деятельности.

Система (IEC 61508) *(System).* Набор взаимосвязанных в соответствии с конструкцией элементов, каждый из которых

может быть системой (подсистемой), которая может быть управляющей или управляемой системой, и может включать оборудование, программное обеспечение, и "человеческий фактор".

Логическая система *(Logic System).* Часть системы, которая выполняет логические функции, но не включает в себя сенсоры и исполнительные элементы. Стандарт IEC 61508 включает в это понятие следующие системы:

- Электрические логические системы - для электромеханической технологии;
- Электронные логические системы - для электронной технологии;
- Программируемые электронные логические системы - для программируемой электронной технологии.

Программируемый логический контроллер - ПЛК *(Programmable Logic Controller - PLC)* - комплекс электронных и программных компонент и средств, включая модули ввода-вывода, предназначенный для выполнения логических функций; то есть та часть системы безопасности, которая выполняет логические функции, за исключением сенсоров и исполнительных элементов (формулировка ISA 84.01-96).

Синонимы:

- Логическое решающее устройство *(Logic Solver)*$_9$ или просто Логическое устройство,
- Логическая система *(Logic system).*

Полевые устройства *(Field device).* В стандарте IEC 61508 данный термин отсутствует. Формулировка ISA 84.01:

Оборудование, подключенное со стороны поля (установки, процесса) к терминальным панелям ввода-вывода системы. К этому оборудованию относятся:

- Сенсоры ("датчики") и конечные исполнительные устройства, а также обвязка данных устройств,
- Средства взаимодействия с оператором технологического процесса, которые физически подключены к терминалам ввода-вывода системы (локальные панели, извещатели, и т.д.).

Программируемая электроника *(Programmable Electronic - PE).* Термин IEC 61508. Базируется на компьютерной технологии, и может состоять из оборудования, программного обеспечения, входных и выходных узлов. Данный термин по-

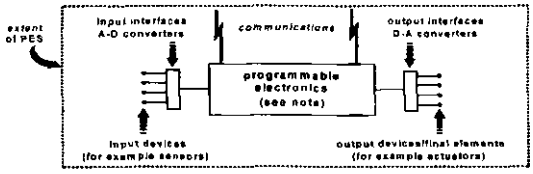
крывает микроэлектронные устройства, построенные на одном или нескольких центральных процессорах, собственной памяти, и т.д.

Примеры:

- Микропроцессоры;
- Микроконтроллеры;
- Программируемые контроллеры;
- Программируемые логические контроллеры;
- Другие микропроцессорные устройства (смарт - сенсоры, трансмиттеры, электропневмопозиционеры).

2.3. Системы

Программируемая электронная система *(Programmable Electronic System - PES).* Программируемая электронная система определяется стандартом IEC 61508 как Система, предназначенная для управления, защиты или слежения, построенная на основе одного или нескольких электронных устройств, включая все элементы системы: источники питания, сенсоры и другие входные устройства, магистрали данных и другие средства коммуникации, исполнительные устройства, и другие выходные устройства (см. рис. 2.1).



a) Basic PES structure

НИЗИН"

<4 PEi I 1

4ZHZP

b) Single PES with single programmable electronic device (le one PES com prised of a single channel of programmable electronics}

c> Single PES with dual program mable electronic devices linked In s serial manner (for example Intelligent sensor end programmable controller)

d) Single RES with dual programmable electronic devices but with shared sensors and final elements (le one PES comprised of two channels of programmable electronics)

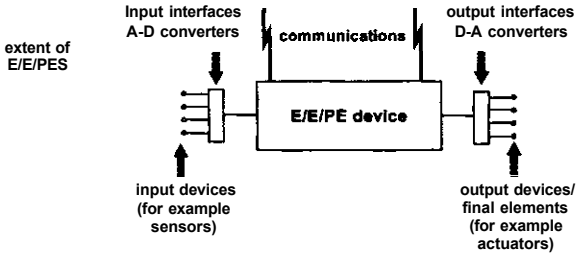
NOTE The programmable electronics are shown centrally located but could exist at several pieces in the PES

Рис. 2.1

Дополнительно введено расширенное определение:
Электрическая / Электронная / Программируемая электронная система *(Electrical / Electronic / Programmable Electronic System E / E / PES),* которое, впрочем, нисколько не отличается от предыдущего.
Электрическая / Электронная / Программируемая электронная система (см. рис. 2.2) определяется стандартом IEC 61508 как

Система, предназначенная для управления, защиты или слежения, построенная на основе одного или нескольких электронных устройств, включая все элементы системы:

- Источники питания;
- Сенсоры и другие входные устройства;
- Магистрали данных и другие средства коммуникации;
- Исполнительные устройства, и другие выходные устройства.



NOTE The E/E/PE device я shown centrally located but such dev›ce<8) could exist at several places in the E/E/PES

Рис. 2.2

Примечание

Стандарт ANSI/ISA 84.01-96 НЕ ВКЛЮЧАЕТ полевое оборудование в понятие "Электрическая / Электронная / Программируемая электронная система".

Система управления оборудованием (IEC 61508) *(EUC control system).* Система, отвечающая за получение сигналов от процесса или оператора и генерирующая выходные сигналы, заставляющие установку работать требуемым образом.

Архитектура *(.Architecture).* Специфическая конфигурация элементов оборудования и программного обеспечения системы.

Модуль *(Module).* Компонент, или целостный набор взаимосвязанных компонент, которые составляют идентифицируемый элемент, устройство, прибор, или часть оборудования. Модуль может быть отключен, перемещен как единое целое, или заменен. Модуль имеет присущие ему рабочие характеристики, которые могут быть проверены как индивидуальные характеристики данного устройства.

Можно сравнить наше определение модуля с как всегда необыкновенным определением стандарта IEC 61508-4, п.3.3.6:

Module *- routine, discrete component or a functional set of encapsulated routines or discrete components belonging together.*

Программный модуль *(Software module).* Информационная структура, состоящая из процедур и/или объявлений данных, которая может взаимодействовать с другими аналогичными структурами.

Канал *(Channel).* Элемент, или группа элементов, которая независимо, самостоятельно выполняет предопределенную функцию. Данный термин может использоваться как для обозначения комплектной системы, так и части системы. Например, двухканальная конфигурация состоит из двух самостоятельных каналов, независимо выполняющих одну и ту же функцию. Элементы внутри канала могут включать модули ввода-вывода, логические устройства, сенсоры, исполнительные устройства.

Альтернативность *(Diversity).* Различие средств для выполнения определенной функции.

Резервирование, избыточность *(Redundancy).* Технический прием, основанный на использовании нескольких систем, каналов, компонентов, или элементов систем для выполнения одних и тех же функций. Резервирование может быть выполнено на идентичных элементах **(однородное резервирование),** или на других, отличных элементах **(альтернативное резервирование).**

И, как всегда, феноменальная формулировка IEC 61508:

Средства в дополнение к уже достаточным средствам, предназначенные для выполнения функциональным узлом тре-

буемой функции, или для данных, представляющих информацию.

Система безопасности *(Safety Instrumented System - SIS; Safety Related System - SRS).* Стандарт ANSI / ISA 84.01-96 определяет Систему безопасности термином "*Safety Instrumented System - SIS",* что в буквальном переводе означает: "Оборудованная под безопасность система". Стандарт ANSI / ISA 84.01-96 определяет Систему безопасности SIS как "Систему, состоящую из сенсоров, логических решающих устройств и конечных (исполнительных) элементов, предназначенную для перевода процесса в безопасное состояние при возникновении нарушений предопределенных условий".

В стандарте IEC 61508 вводится новый термин "*Safety Related System - SRS",* что, по всей видимости, означает "Имеющую отношение к безопасности", или "предназначенную для защиты" систему. Эти вычурные термины используются в современных западных стандартах безопасности в качестве общего определения для всего спектра систем противоаварийной защиты, безопасного останова, систем логического управления и защиты, и т.д. Стандарт IEC 61508 определяет "имеющую отношение к безопасности систему" *(SRS)* как систему, предназначенную для:

1. Осуществления требуемых функций безопасности, необходимых для достижения или поддержания безопасного состояния технологического объекта;
2. Достижения необходимой полноты, целостности *(safety integrity)* для требуемых функций безопасности.

Стандарт IEC 61511 уже в своем названии возвращается к термину *"Safety Instrumented System",* и определяет Систему безопасности как "Систему, оснащенную соответствующим полевым оборудованием, используемую для выполнения одной или нескольких функций безопасности. Система безопасности состоит из сенсоров, логических решающих устройств, и конечных (исполнительных) элементов".

Обобщая предыдущее, будем считать по определению (см. рис. 2.3), что Система безопасности состоит из:

- Сенсоров,
- Логических устройств,
- Исполнительных элементов,
- И, вообще говоря, *контингента.*

И предназначена система безопасности для:

- Автоматического перевода технологического процесса в безопасное состояние при нарушении предопределенных условий;
- Разрешения на продолжение нормальной работы технологического процесса при отсутствии нарушения предопределенных условий;
- Осуществления действий, направленных на предотвращение и устранение технологических нарушений.

Таким образом, привычный термин ПАЗ далее будет использоваться только в вышеозначенном контексте, то есть в совокупности с полевым оборудованием и всеми интерфейсами. А термины:

- ПАЗ,
- Система ПАЗ,
- Система безопасности (СБ),
- Система защиты,

будем считать составляющими общую группу терминов для систем обеспечения безопасности.

Определение системы безопасности

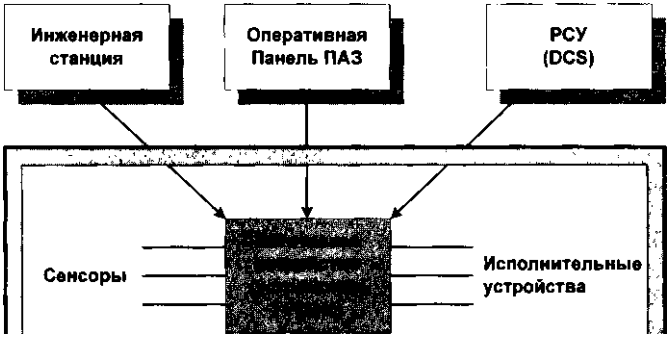


Рис. 2.3

2.4. Безопасность и риск

Угроза *(Harm).* Физическое воздействие или потеря здоровья людьми, обусловленные впрямую или косвенно результатом разрушения оборудования, или в результате воздействия опасных веществ.

Опасность, риск сбоя *(Hazard).* В данном контексте - это физические или химические условия, потенциально представляющие угрозу для людей или оборудования.

Опасная ситуация *(Hazardous situation).* Обстоятельства, в которых человек подвергается опасности.

Опасное событие *(Hazardous event).* Опасная ситуация, приводящая к угрозе.

Риск *(Risk).* Сочетание вероятности появления угрозы, и серьезности этой угрозы.

Допустимый риск *(Tolerable risk).* Приемлемый в данных обстоятельствах и социальных условиях уровень риска.

Остаточный риск *(Residual risk).* Уровень риска, оставшийся после принятия мер защиты.

Безопасность *(Safety).* Свобода от неприемлемого риска.

Безопасное состояние *(Safe state).* Безопасным состоянием называется такое **предопределенное состояние,** в которое система может быть переведена из своего рабочего состояния, и в котором потенциал опасности меньше, чем в исходном состоянии.

Абсолютно безопасным состоянием является такое состояние, в котором вкладываемая и имеющаяся энергия системы наименьшая.

Таково авторское определение. Стандарт IEC 61508, часть 4, дает совершенно бестолковое тавтологическое определение: *Состояние контролируемого оборудования, при котором безопасность достигается.* См. IEC 61508-4, п. 3.1.10: "*State of the EUC when safety is achieved*".

Функциональная безопасность *(Functional safety).* Для ряда производств отказ системы управления может привести к останову технологического процесса и потере продукции, но при этом отказ не представляет опасности для оборудования и персонала.

Понятие функциональной безопасности возникает в том случае, когда искусственно созданные или естественные нарушения технологического процесса способны привести к авариям, разрушению технологического оборудования, человеческим жертвам.

Функциональная безопасность определяется как часть общих мер безопасности, которая находится в зависимости от правильности работы системы безопасности в ответ на изменения на процессе. Требование функциональности определяется, как **способность системы безопасности переводить процесс в безопасное состояние при наличии отклонений.** Считается, что функциональная безопасность обеспечивается, если

1. Каждая специфицированная функция защиты выполняется, и
2. Достигается требуемое качество исполнения каждой функции защиты.

Причем даже если система безопасна, некоторая степень риска не исключается: считается, что система имеет требуемую безопасность, если степень риска не выше заранее определенного уровня риска.

Функция безопасности *(Safety function = Safety loop).* Функция, реализованная системой безопасности или иными средствами снижения риска, которая предназначена для достижения или поддержания безопасного состояния контролируемого оборудования *(EUC)* по отношению к определенному опасному событию. Функции безопасности реализуются посредством контуров безопасности (защиты).

Жизненный цикл системы безопасности *{Safety lifecycle).* Фазы существования системы безопасности, начиная от стадии концептуального проектирования, и до списания системы.

Надежность *(Reliability).* **В IEC 61508 данное понятие отсутствует.** Но, судя по формулировке, оно соответствует понятию IEC *"Safety Integrity".*

В терминах ISA 84.01-96, **Надежность** определяется как вероятность того, что система (включая и человека) будет выполнять требуемые функции при всех предопределенных условиях в течение установленного интервала времени.

Часто надежность характеризуется непосредственно временем, в течение которого система защиты способна выполнять требуемые функции защиты технологического процесса.

Характеристики, которые учитываются при определении понятия "Надежность", принимаются усредненными, и включают:

- Среднее время работы до отказа *MTTF (Mean Time To Failure).*
- Среднее время между отказами *MTBF (Mean Time Between Failure).*
- Средняя вероятность отказа выполнения требуемой функции PFD_{AVG} **В течение межповерочного интервала.**
- Средняя интенсивность (частота) опасных отказов в час $PFH_{AVG} = X_{AVG}$.
- Среднее время восстановления системы *MTTR.*
- Фактор снижения риска $RRF = 1/PFH_{AVG}$.

Ограничение по времени, в течение которого можно требовать соблюдения определенных характеристик надежности системы, является важнейшим условием.

Однако наш ГОСТ 27.002-89 "*Надежность в технике. Основные понятия. Термины и определения*" дает определение надежности, в котором ограничение по времени отсутствует:

"Свойство объекта **сохранять во времени** в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования. *(Свойство сохранять и выполнять во время обслуживания, хранения и транспортирования - это круто знай наших!)*

Важное замечание

Надежность системы не связана напрямую с безопасностью системы: ненадежные системы являются безопасными, если каждый отдельный отказ ***всегда*** *переводит объект в так называемое "безопасное" состояние, то есть приводит к останову процесса.*

Целостность, полнота безопасности *(Safety integrity)* - термин IEC 61508. Вероятность того, что система безопасности *удовлетворительно (?! - так и формулируется стандартом IEC)* выполняет требуемые функции безопасности по всем предопределенным условиям в течение установленного интервала времени. В ISA 84.01-96 данное понятие соответствует понятию "*Reliability*" - надежности (см. определение Надежности).

При определении целостности ВСЕ причины отказов, - и случайные отказы оборудования, и систематические отказы, которые ведут к небезопасному состоянию, - должны быть учтены. Например, отказы оборудования, отказы, наведенные программным обеспечением, отказы вследствие электромагнитного воздействия.

Некоторые из подобных отказов, в частности случайные отказы оборудования, поддаются количественной оценке с помощью таких показателей, как:

1. Вероятность (интенсивность) опасных отказов в час *(Probability, Intensity of failure per hour)* PFH_{AVG} , или *A>AVG•*
2. Вероятность опасного отказа выполнения требуемой функции в течение предопределенного межповерочного интервала - интервала автономного функционального тестирования (например, 1год) - *Probability of failure on demand* PFD_{AVG}.

Первый показатель используется в том случае, когда необходимо определить характеристику способности системы к осуществлению **непрерывного контроля и защиты** объекта, то есть без привязки к конкретному временному межповерочному интервалу. Второй показатель используется, как усредненная мера готовности системы обеспечить защиту (останов) процесса в течение предопределенного интервала межповерочного тестирования.

Полнота безопасности системы зависит от очень многих факторов. Некоторые, как например, человеческий фактор, не поддаются количественной оценке, но могут быть только качественно оценены.

В общем виде **Целостность, полнота безопасности** оценивается как состоящая из двух компонент:

1. Аппаратная целостность безопасности;
2. Систематическая целостность безопасности.

И данное определение наиболее полно соответствует понятию надежности выполнения системой функций безопасности.

Примечание

К сожалению, очень трудно дать количественные оценки вероятности и частоты систематических отказов. И совершенно невозможно предугадать надежность человека даже в обычных для него обстоятельствах.

Аппаратная целостность безопасности *(Hardware safety integrity).* Термин IEC 61508. Часть интегральной безопасности системы, относящаяся к случайным опасным отказам оборудования.

Систематическая целостность безопасности *(Systematic safety integrity).* Термин IEC 61508. Часть интегральной безопасности системы, относящаяся к систематическим опасным отказам. Систематическая целостность безопасности, в отличие от аппаратной целостности, как правило, не может быть оценена количественно.

Программная целостность безопасности *(Software safety integrity).* Термин IEC 61508. Показатель, который означает степень доверия к тому, что программное обеспечение в программируемой электронной системе выполняет функции безопасности при всех предопределенных условиях в течение установленного интервала времени.

Интегральный уровень безопасности SIL *(Safety Integrity Level - SIL, - термин ISA 84.01-96, IEC 61508).*

Дискретная величина от единицы до четырех, предназначенная для определения уровня требований к интегральной безопасности, целостности функций безопасности, реализуемых системой безопасности. Иными словами, SIL является мерой, определяющей степень безопасности самой системы безопасности.

Спецификация требований безопасности *(Safety Requirements Specification).* Важнейший документ, необходимый для создания системы - и АСУТП в целом, и системы безопасности в отдельности.

Непосредственный отечественный аналог - Техническое задание на создание АСУТП. В контексте стандарта IEC, спе-

цификация должна содержать ВСЕ требования, которым должна соответствовать система безопасности. Спецификация подразделяется на:

1. Спецификацию требований к функциям безопасности,
2. Спецификацию требований к интегральной безопасности - комплексной надежности системы безопасности.

Спецификация требований к функциям безопасности *(Safety Functions Requirements Specification).*

Определяет требования к функциям безопасности, которые должны выполняться системой безопасности, и содержит точное и детальное представление функций безопасности в виде текстов, таблиц, блок-схем, матриц (таблиц решений), логических диаграмм и т.д., обеспечивающих ясное описание функций системы - контуров управления и защиты.

Спецификация требований к интегральной безопасности *(Safety Integrity Requirements Specification).*

Определяет требования к интегральной безопасности - надежности системы безопасности, с которой должны выполняться функции системы безопасности, и содержит детальное представление данных изготовителя и разработчика системы в виде текстов, таблиц, блок-схем, расчетов и т.д., обеспечивающих ясное представление о надежности системы.

Режим работы *(Mode of operation - IEC 61508).* Режим, в котором будет использоваться система безопасности в зависимости от частоты запросов к системе на обеспечение безопасности.

Различают два режима работы системы безопасности:

1. **Режим низких требований безопасности** *(Low demand mode of operation),* когда частота запросов на выполнение системой безопасности функций защиты НЕ БОЛЬШЕ, чем один раз в год, и не превышает частоту проведения процедур диагностического тестирования более чем в два раза.
2. **Режим высоких требований безопасности** *(High demand mode of operation),* когда частота запросов на выполнение системой безопасности функций защиты БОЛЬШЕ, чем один раз в год, или превышает частоту проведения процедур диагностического тестирования более чем в два раза.

Целевая мера отказов *(Target failure measure).* Целевая мера вероятности опасных отказов, которая должна быть достигнута по отношению к требованиям интегральной безопасности (НАДЕЖНОСТИ). Количественно определяется следующими показателями:

Вероятность опасного отказа выполнения требуемой функции *(Probability offailure on demand* PFD_{AVG}*)* - для режима низких требований.

Вероятность (интенсивность) опасных отказов в час *(Probability (Intensity) offailure per hour* PFH_{AVG} , или A_{avg}) - для режима высоких, или непрерывных требований. Конкретные значения этих показателей регламентируются таблицами 2.1 и 2.2 *(соответствующие таблицы 2 и 3 из пункта 7.6.2.9 стандарта IEC 61508).*

Таблица 2.1

Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	> 10~^{5} to < 10^{u}
3	> 10"^{4} to < 1Cl^{3}
2	> 10"^{3} to < 10"^{2}
1	> 10"^{2} to < 10~^{1}

Таблица 2.2

Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	> 10"^{9} to < 10"^{8}
3	> 10"^{8} to < 10"^{7}
2	> 10"^{7} to < 10"^{6}
1	> 10 ^{6} to < 10"^{5}

Межповерочный интервал, интервал межповерочного тестирования *(prove Test Interval) - TI или* **Т,.** Временной межповерочный интервал периодического **автономного** *(off-line)* функционального тестирования, который служит для выявления сбоев и отказов с целью проверки и восстановления исходной функциональности и надежности системы.

Примечание

В формулировке стандарта IEC 61508 слово "off-line" отсутствует. Однако, исходя из контекста и дальнейшего использования, оно как бы "подразумевается".

Интервал диагностического тестирования *(Diagnostic test interval).* Временной интервал **оперативного** *(on-line)* функционального тестирования с целью выявления сбоев системы безопасности, имеющих **специфицированный** уровень диагностического охвата.

Примечание

В формулировке стандарта IEC 61508 слово "on-line" в данном случае присутствует.

Интенсивность отказов *Я (Fault rate).* Измеряется в количестве отказов, отнесенном к одному часу работы системы *(отказ/час, или просто 1/час).*

Среднее время между отказами - *MTBF* *(Mean Time Between Failures).* В стандарте IEC 61508-4 не определяется. В предположении *Я* = ***Const***, *MTBF* наряду с *MTTF* определяется как величина, обратная к *Я* .

Данный показатель является статистическим представлением потенциальной возможности отказа компонента, устройства или системы в течение определенного интервала времени. Данная величина практически всегда вычисляется на основе теоретических предпосылок. К сожалению, это часто приводит к совершенно нереальным значениям. Иногда *MTBF* отражает данные, полученные в результате тестирования при искусственном ускорении темпа жизни оборудования в более жестких условиях. В редчайших случаях *MTBF* может быть представлено на основе статистики реальных отказов.

В силу того, что реальные условия на процессе могут сильно отличаться от лабораторных, а полная, законченная статистика отказов никому не известна, то главным принципом отбора был и остается естественный отбор - применять только зарекомендовавшее себя на практике оборудование.

Среднее время работы до отказа - ***MTTF*** *(Mean Time To Failure).* В стандарте IEC 61508-4 не определяется. В отечественной практике соответствует понятию "Среднее время наработки на отказ".

Определяется, как Среднее время от запуска работоспособной системы до момента отказа. Строго говоря, понятие *MTTF* должно применяться только для тех компонент оборудования, которые не подлежат восстановлению, в то время как понятие *MTBF* - для тех компонент, которые могут быть заменены (восстановлены) и возвращены в работу.

Но на практике *MTTF* обычно участвует в определении Среднего времени работы между отказами *MTBF* в сочетании со Средним временем восстановления после отказа *MTTR (Mean Time To Restore, Repair):*

$$MTBF = MTTF + MTTR$$

Поскольку *MTTR* по сравнению с *MTTF* достаточно мало, то в обоснованных случаях считается, что $MTBF \sim MTTF$.

В самом общем виде *MTTF* определяется как

$$MTTF = \frac{Total\_system(s)\_operation\_time}{Total\_number\_of\_failures}$$

Важно правильно понимать смысл этого показателя. Часто считается, что *MTTF* определяет среднее, или даже гарантированное время безотказной работы устройства. Покажем, что, к сожалению, это не так.

Классическое проявление случайных отказов описывается экспоненциальным законом распределения надежности:

$$R(t) = e^{-t/MTTF}$$

При $t = MTTF$ надежность устройства составит

$$R(t) = e^{-MTTF/MTTF} = e^{-1} = 0.367879 \sim 37\%$$

Этот результат можно интерпретировать несколькими способами:

1. Для единичного устройства это означает, что вероятность того, что устройство останется в работе по истечению *MTTF* составляет всего лишь 37%.
2. Для группы однотипных устройств это означает, что только 37% из них переживут рубеж *MTTF.*
3. Можно также сказать, что устройство проработает в течение *MTTF* с 37% уровнем доверия.

Пусть, например, для датчика *Л = 1.0 *10^5 1/час.* Это означает, что *MTTF -11.4 лет.*

Но посмотрим, каково будет количество отказов для п = *1000 датчиков в течение 1 года:*

n-A-t = n t/MTTF = 1000 1/11.4 = 87.60 « 88 *отказов за год.*

Если не производить восстановление и замену, то через 10 лет в работе останется лишь

Exp (-10/11.4) =41.6% = 416 датчиков.

Среднее время восстановления ***MTTR*** *(Mean Time To Restore).* Складывается из интервала времени, в начале которого было обнаружено, что система безопасности находится в неработоспособном состоянии, времени определения причины отказа, времени восстановления работоспособности, и времени автономного тестирования.

Это значение в высшей степени зависит от обстоятельств и условий, в которых работает система. Система, которая работает без минимального набора необходимых запасных частей, будет иметь невероятное время восстановления.

В расчетах стандарта IEC 61508 *MTTR* принимается в интервале от 8 до 24 часов.

Частота восстановления *ju (Repair rate, restoration rate).* Определяется как чисто формальная величина, обратная к *MTTR:*

{1 = 1/ MTTR

Средняя вероятность (интенсивность) опасных отказов в час $PFH_{AVG} = A_{avg}$ *(Probability, Intensity of failure per hour).*

Величина, характеризующая частоту опасных отказов в час. Применяется для характеристики высокого уровня требований к системе безопасности. См. Режим высоких требований безопасности.

Примечание

В предварительной версии стандарта IEC 61508 данная характеристика имела вполне оправданное название "Интенсивность, частота", и обозначалась как A_{avg}. *Однако в окончательной версии она обозначена как* PFH_{AVG}, *хотя по всем канонам вероятность - величина безразмерная.*

Фактор снижения риска *RRF* *(Risk Reduction Factorj.* Величина, обратная интенсивности опасного отказа при высоком уровне требований:

$RRF = 1/PFH.$

Готовность *(Safety Availability - термин ISA 84.01-96).*

Важное замечание

Фактически, это понятие часто используется без ясного понимания того, что оно включает в себя два аспекта:

- *Динамическая, или как ее еще называют, мгновенная готовность, как функция времени существования того технического устройства, к которому оно относится, и*
- *Стационарная готовность, как усредненная характеристика надежности за какой-то период времени.*

Стандарты ISA 84.01-96 и IEC 61508 используют только Стационарную готовность, точнее, Неготовность, и определяют ее как **Среднюю вероятность опасного отказа выполнения требуемой функции** *Probability offailure on demand* - PFD_{AVG} , то есть пользуются только стационарными решениями, полученными к тому же полуэмпирическим путем, а не в результате решения динамических моделей.

Важное замечание

Реальное понимание процессов, происходящих с оборудованием систем безопасности, а уж тем более исследование их поведения невозможно без динамики. Ведь вполне может статься, что в реальности стационарное состояние окажется вообще недостижимым. Исследование поведение базовых архитектур систем безопасности на основе динамических моделей Маркова требует специальной подготовки.

Динамическая готовность - это величина, характеризующая вероятность того, что система выполнит предопределенную функцию защиты в момент возникновения необходимости ее выполнения в течение наперед заданного интервала времени. Динамическая готовность *A(t)* - это надежность *R(t)* во времени:

$A(t) = R(t),$

тогда

$PFD(t) = 1-R(t).$

Стационарная готовность выражается в процентах, и определяется средним временем работы до отказа *MTTF* и средним временем восстановления после отказа *MTTR* по следующей формуле:

$$a = \frac{MTTF}{MTTF + MTTR} \qquad 100\% = \frac{MTBF}{MTBF} \cdot 100\%$$

Готовность систем существенно возрастает для малых времен обнаружения неисправности. Быстрое обнаружение неисправности в современных электронных системах достигается применением автоматических процедур оперативного тестирования и выводом подробной диагностической информации.

Однако необходимо подчеркнуть, что если отказ привел к останову процесса, то время восстановления может сильно увеличиться, поскольку запуск производства "несколько" отличается по времени от времени замены модулей.

Готовность системы защиты может быть увеличена посредством резервирования, например, при параллельной работе центральных устройств, модулей ввода-вывода, и применением нескольких сенсоров в каждой точке измерения.

Резервированные элементы встраиваются в систему таким образом, чтобы отказ отдельного элемента не сказывался на общей функциональности системы. Очень важным компонентом готовности является подробный вывод диагностической информации.

Уже стандарт ISA 84.01-96 рекомендовал вместо готовности использовать более точное понятие "*Вероятность опасного отказа выполнения требуемой функции -PFD*

В IEC 61508 понятие готовности вообще отсутствует. Вероятность опасного отказа выполнения требуемой функции *(Probability offailure on demand - PFD).* Величина, характеризующая вероятность того, что система не выполнит предопределенную функцию защиты в момент возникновения необходимости ее выполнения.

По сути j*PFD* - это усредненная по времени вероятность НЕГОТОВНОСТИ системы защиты в самый нужный момент. Для системы безопасности по каждой функции безопасности она определяется как сумма

$$PFD_{AVG} = PFD_{SE} + PFD_{LS} + PFD_{FE}$$, где

I $pfd_{AV(}$ - Средняя вероятность отказа выполнения требуемой функции защиты,

I *PFDse* - Средняя вероятность отказа выполнения требуемой функции связной группы сенсоров и входного интерфейса (входных модулей),

I *PFDls* - Средняя вероятность отказа выполнения требуемой функции самого логического устройства,

I PFD_{FE} - Средняя вероятность отказа выполнения требуемой функции выходного интерфейса (выходных каналов) и группы конечных (исполнительных) элементов.

Вероятностное определение стационарной готовности *(Safety Availability)* выражается как

$(1\text{-}PFD_{AVG})100\%$.

Кроме всего прочего, данный показатель зависит от состояния самого технологического процесса, полевого оборудования, системы защиты и ее компонентов, интервала тестирования, и от того, насколько часто возникает потребность в выполнении функций защиты.

MooN *(M out ofN).* Специфическая аббревиатура для обозначения и определения архитектуры систем безопасности. Данное сокращение обозначает, что для правильного функционирования системы необходимо, чтобы *M* из *N* каналов работали нормально. Если система построена на *N* каналах, и для нормальной работы системы необходимо M каналов, то это означает, что система способна пережить *(N - M)* отказов без потери функциональности. Соответственно для отказа системы необходимо, чтобы отказали (N - M + 1) каналов.

MooND *(M out ofN with Diagnostic).* В данном контексте символ *D* добавляется к мнемонике архитектуры в двух случаях:

- Для архитектуры **loo1D,** символизируя во множестве случаев наличие обыкновенного сторожевого таймера;
- Для выделения архитектуры **loo2D,** которая имеет принципиальные отличия от архитектуры **1oo2,** определяемые не только наличием диагностических цепей, но особой спецификой архитектуры.

Причем зачастую между архитектурами 1oo1 и 1oo1D не делается никаких различий, и обе аббревиатуры используются равноправно, ибо действия обеих систем в случае отказа совпадают: система отключается, и происходит физический останов процесса. А вот между системами 1oo2 и 1oo2D существует принципиальная разница. Как сказано в стандарте IEC 61508 по поводу системы 1oo2:

Предполагается, что диагностическое самотестирование системы 1oo2 способно только извещать о сбоях, но при этом не производит никаких изменений состояния выходных сигналов. Как сказано в стандарте IEC 61508 по поводу системы 1oo2D:

Для системы с расширенной диагностикой 1oo2D, если диагностика обнаруживает отказ в любом из каналов, процедура голосования строится таким образом, что выход системы будет контролироваться другим каналом. Если диагностическое тестирование обнаруживает отказы в обоих каналах, или обнаруживает расхождение, которое не может быть приписано к какому-либо из каналов, то выход системы переводится в состояние останова ("безопасное" состояние). Для того чтобы расхождение между элементами (каналами) могло быть обнаружено, каждый из элементов должен иметь возможность определять состояние другого элемента с помощью средств, независимых от проверяемого элемента.

Однако ни в одном из западных стандартов не поясняется, что в случае с архитектурой 1oo2D символ D - это не просто "возможность определять состояние другого элемента", а оригинальное сочетание архитектур 2oo2 и 1oo2, позволяющее использовать диагностические цепи в качестве **дополнительной пары каналов, построенных на альтернативных элементах и совершенно иных схемных решениях.** Оба диагностических тракта работают таким образом, что без перекрестного подтверждения соседний канал не сможет выдать команду на изменение выхода. Поэтому символ "D" в данной архитектуре означает не просто расширенные возможности диагностики, а особым образом организованное взаимодействие управляющих и диагностических цепей, позволяющее фактически реализовать **квадро - систему,** имея:

- Два канала обработки информации,
- Два диагностических канала.

2.5. Сбои и отказы

Сбой *(Fault).* Ненормальная ситуация, которая может привести к снижению или потере способности функционального узла к выполнению предопределенной функции, то есть к отказу.

Отказобезопасность *(Fail-safe - ISA 84.01-96).* Способность системы к переходу в предопределенное безопасное состояние **в случае своего собственного отказа.**

Важное замечание

Для систем безопасности на опасных технологических процессах в данное определение вкладывается не сразу осознаваемый, но крайне неприятный смысл: в случае так называемого безопасного отказа системы безопасности процесс переводится в "безопасное состояние", которое, по сути, является состоянием немотивированного, ложного останова процесса.

Устойчивость к сбоям, Отказоустойчивость *(Fault tolerance).*

IEC 61508: Способность функционального узла продолжать выполнение требуемой функции в присутствии сбоев и ошибок.

ISA 84.01-96 в очередной раз дает абсолютно точное определение: Встроенная способность системы обеспечивать непрерывное и корректное выполнение предопределенных функций в присутствии ограниченного количества программных и аппаратных сбоев.

Примечание

Следует иметь в виду, что понятия Резервирование и Отказоустойчивость несколько отличаются одно от другого:

- *Системы с резервированием имеют самостоятельно выделенные дублированные (или более того) элементы, а также ручные или автоматические средства для выявления отказов и переключения на резервные элементы.*
- *Комплектные отказоустойчивые модули или системы имеют внутренне резервированные (параллельные) компоненты и встроенную логику для выявления и обхода неисправностей без негативного воздействия на выходы.*

Отказ *(Failure).* Прекращение способности функционального узла к выполнению предопределенной функции. Отказ должен определяться системой, иметь возможность исправления или замены *on-line* без воздействия на функциональность системы как до, так и после восстановления (замены).

Случайный отказ оборудования (.*Random hardware failure).* Отказ, проявляющийся в произвольный момент времени, приводящий к запуску одного или более механизмов скачкообразной деградации оборудования. Реальные условия работы оборудования приводят к тому, что элементы системы отказывают по разным механизмам отказа и в произвольные моменты времени. Поэтому **оценить можно всего лишь частоту отказов, но не конкретные моменты их появления.**

Систематический отказ *(Systematic failure).* Отказ, проявляющийся вполне определенным образом по определенной причине, от которой можно избавиться только изменением конструкции, технологических процедур, документации, или других определяющих факторов. Систематические отказы иногда могут быть устранены путем моделирования причин и условий отказа. Однако профилактическое обслуживание без внесения радикальных изменений, как правило, не устраняет первопричины отказа.

В стандарте IEC 61508 приводятся следующие примеры причин систематических отказов:

- Ошибки спецификации.
- Ошибки конструкции, технологии производства оборудования, пуско-наладки, условий эксплуатации.
- Ошибки проекта, разработки, программного обеспечения.

Главная разница между случайными и систематическими отказами заключается в следующем:

- Частота отказов системы, возникающая в результате случайных отказов элементов оборудования, в отличие от систематических отказов, как это ни парадоксально, может быть предсказана с приемлемой точностью.
- Систематические отказы системы, которые появились вследствие случайных отказов оборудования, также можно оценить. Но отказы системы, которые возникли в результате систематических ошибок, очень сложно оценить статистически, поэтому наличие и проявление

систематических отказов трудно предсказать - они детерминированы.

Следующие два определения настолько важны, что приведем их формулировки из стандарта IEC 61508, Part 4 "*Definitions and abbreviations",* Стр. 41, целиком:

"3.6.7. Dangerous failure

Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state

NOTE - Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure ***is less likely*** *to lead to the overall dangerous or fail-to-function state".*

"3.6.8. Safe failure

Failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state

NOTE - Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a safe hardware failure ***is less likely*** *to result in an erroneous shutdown ".*

И перевод:

Опасный отказ *(Dangerous failure).* Отказ, который имеет потенциал привести систему безопасности к опасному состоянию, или к неспособности осуществлять функции защиты.

Замечание создателей стандарта

Будет или не будет реализован этот потенциал, может зависеть от архитектуры каналов системы. В системах с несколькими каналами для увеличения безопасности **менее похоже** *(?! - так и написано - is less likely, - Ю. Ф.),* что опасный отказ оборудования приведет к общему опасному состоянию, или к неспособности осуществлять функции защиты.

"Безопасный" отказ *(Safe failure).* Отказ, который не имеет потенциала привести систему безопасности к опасному состоянию, или к неспособности осуществлять функции безопасности.

Замечание создателей стандарта

Будет или нет, реализован этот потенциал, может зависеть от архитектуры каналов системы. В системах с несколькими каналами для увеличения безопасности **менее похоже** *(так и написано - is less likely, - Ю.Ф.),* что безопасный отказ оборудования приведет к ошибочному останову.

Важное замечание

За этой, вроде бы успокаивающей и обтекаемой формулировкой кроется крайне опасный смысл, который не сразу обнаруживается. Гораздо "более похоже", что "безопасный" отказ в лучшем случае будет означать ложный останов производства. Можно сказать, что Safe failure - это самый неудачный термин стандартов МЭК для тех, кто использует оборудование и системы безопасности. ***Фактически он означает самоустранение - "безопасность" самой системы безопасности от технологического процесса.***

Ложное срабатывание *(Spurious trip, nuisance trip, false shut down).* Ложное, беспричинное срабатывание блокировки, или немотивированный останов процесса по причинам, не связанным с действительными событиями на процессе (см. ANSI/ISA 84.01-1996, стр. 22, п. 3.1.59).

В стандарте IEC 61508 определение ложного срабатывания отсутствует.

Ложное срабатывание может произойти по множеству причин:

- По причине отказа оборудования;
- Ошибки программного обеспечения;
- Ошибки обслуживания, неправильной калибровки;
- Отказа полевого оборудования;
- Отказа модулей ввода-вывода;
- Отказа центрального процессора;
- Электрического сбоя;
- Электромагнитной наводки и т. д.

Сбой общего порядка (общей причины) - ISA 84.01 *(Common cause fault).* Единый источник, единая первопричина, которая может привести к отказу группы элементов системы. Единый источник отказа может быть как внутренним, так и внешним по отношению к системе.

Отказ общего порядка (общей причины) - IEC 61508 *(Common cause failure).* Редчайший случай, когда определение **IEC** 61508 оказывается лучше определения **ISA** 84.01:

Отказ, который является результатом одного или нескольких событий, приводящих к **одновременному отказу двух или более отдельных каналов в многоканальной системе, приводящему к отказу системы в целом.**

Примеры общих отказов:

- Неквалифицированное обслуживание;
- Не откалиброванные единичные датчики;
- Коррозия, эрозия деталей клапанов;
- Забивка импульсных линий;
- Неблагоприятные условия окружающей среды;
- Перебои электроэнергии;
- Электромагнитное воздействие и т.д.

Замечание

Как мы видим, основные причины отказов, которые оказывают общее катастрофическое воздействие на систему безопасности, это:

- *Люди. Вне конкуренции.*
- *Полевое оборудование.*
- *Энергообеспечение.*

Причины разных отказов существенным образом пересекаются и, как правило, вызывают их нарастание. Экономия на подготовке квалифицированного персонала, на модернизации полевого оборудования с использованием современных средств оперативной диагностики *(Plant Asset Management%* на резервировании ключевых компонентов системы, на источниках бесперебойного электропитания и кондиционировании рабочей среды сводит на ноль любые затраты на суперсовременное основное оборудование АСУТП.

Ошибка *{Error).* Расхождение между вычисленным, наблюдаемым или измеренным значением или условием, и правильным, специфицированным, или теоретически ожидаемым значением или условием.

Человеческая ошибка *(Human error).* Человеческое действие или бездействие, которое может привести к негативным результатам.

Вскрытый сбой, или отказ

(Detected\ Revealed\ Overt fault).

Определение IEC 61508: По отношению к оборудованию - это ошибки, которые могут быть классифицированы как определенные, объявленные, проявленные, выявленные с помощью диагностических тестов, поверочного тестирования, вмешательства оператора.

(Во время нормальной эксплуатации, или во время физической инспекции и ручного тестирования).

Определение ISA 84.01: Ошибки, которые могут быть классифицированы как определенные, объявленные, проявленные.

Скрытый сбой, или отказ

{Undetected, Unrevealed, Covert fault).

Определение IEC 61508:

По отношению к оборудованию - это ошибки, которые могут быть классифицированы как скрытые, не проявленные, не определенные, не выявленные с помощью диагностических тестов, поверочного тестирования, вмешательства оператора. (Во время нормальной эксплуатации, или во время физической инспекции и ручного тестирования).

Определение ISA 84.01: Ошибки, которые могут быть классифицированы как неопределенные, необъявленные, не проявленные.

Останов по отключению питания *(De-energize to trip).*

Определение ISA 84.01 (в IEC 61508 отсутствует):

Отключение источника питания (электроэнергия, воздух КИП), приводящее к переводу процесса в безопасное состояние по физически предопределенной последовательности операций. Предполагается, что в нормальных условиях выходные цепи системы защиты запитывают выходные устройства.

Останов по включению питания *(Energize to trip).* Включение источника питания (электроэнергия, воздух КИП), приводящее к переводу процесса в безопасное состояние по физически предопределенной последовательности операций. Предполагается, что в нормальных условиях выходные цепи системы защиты не запитывают выходные устройства.

Запрос, потребность *(Demand).* Условие, или событие, которое требует от системы защиты предпринять соответствующие действия, направленные на предотвращение опасного события - как от появления, так и от распространения последствий опасного события.

Степень диагностического охвата *(Diagnostic coverage).* Доля уменьшения вероятности опасного отказа оборудования в результате автоматического диагностического тестирования.

Согласно ISA 84.01-96 определяется, как отношение количества обнаруживаемых средствами диагностики системы защиты сбоев к общему количеству сбоев.

Согласно IEC 61508 - доля уменьшения вероятности опасных отказов за счет автоматического диагностического тестирования. Определяется отношением суммарной частоты обнаруженных опасных отказов к общему количеству опасных отказов:

$$= \qquad \text{где} \quad A_D=A_{DD}+A_{SD}.$$

Повышение степени диагностического охвата *DC* имеет первостепенное значение для систем управления и защиты технологических процессов. В современных системах *DC* может достигать уровня 99,95%.

Деблокировка, байпас, обход блокировки *(Bypassing)* - термин ISA 84.01. Действие по временному отключению функции защиты в системе. Осуществляется по инициативе обслуживающего или оперативного персонала с целью диагностики, определения неисправности системы, технического обслуживания и ремонта.

Принудительное изменение состояния входов-выходов *(Forcing).* Функция системы, которая дает возможность изменить состояние входов-выходов системы в обход прикладного программного обеспечения.

Функциональное тестирование *(Functional testing).* Периодически проводимые проверки работоспособности технического и программного обеспечения системы на соответствие Спецификации требований безопасности.

Аппаратная реализация *(Hard-wired).* Схемные решения; работа оборудования без применения программных средств.

Предупредительное обслуживание *(Preventive maintenance).* Практика технического обслуживания, при которой оборудование обслуживается в соответствии с фиксированным графиком по рекомендациям производителя оборудования или на основе накопленного опыта работы и статистики отказов.

Доля (фракция) безопасных отказов *(Safe Failure Fraction - SFF).* Стандартом IEC 61508 не определяется. Доля безопасных отказов устройства или подсистемы определяется как отношение суммы средней частоты безопасных отказов и обнаруженных опасных отказов к средней общей частоте отказов устройства или подсистемы:

$$SFF = \frac{X^{S} + Z^{PP}}{Z^{S} + Z^{OP} + Z_{Л_{ои}}} - \frac{Z^{S} + X^{PP}}{S^{S} + I^{D}} - \frac{Z + X^{PP}}{}$$

Замена в реальном времени *(On-line repair).* Замена отказавших элементов оборудования *on-line* без отключения системы безопасности, и без потери функциональности.

Замена не должна воздействовать на остальные элементы системы. Резервные компоненты должны уже находиться на своих рабочих местах или, в крайнем случае, на специально выделенных местах для размещения резервных компонентов.

Динамическое тестирование *(Dynamic testing).* Демонстрация работоспособности программного обеспечения и/или оборудования с тем, чтобы удостовериться в правильности и отсутствии неправильных действий.

Независимое отделение, департамент *(Independent department).*Отделение (департамент) предприятия, существующее отдельно и независимо от подразделений, отвечающих за действия, которые предпринимаются во время какой-либо фазы, или в целом на жизненном пути электрической / электронной / программируемой электронной системы *(E/E/PES%* предметом деятельности которого является оценка или подтверждение функциональной безопасности.

Независимая организация *(Independent organization).* Организация, существующая отдельно и независимо и в руководстве, и по другим ресурсам от организаций, отвечающих за действия, которые предпринимаются во время какой-либо фазы, или **в** целом на жизненном пути электрической / электронной / программируемой электронной системы *(E/E/PES),* предметом деятельности которой является оценка или подтверждение функциональной безопасности. Непосредственный отечественный аналог - *Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор).*

2.6. Обозначения и сокращения

МЭК	Международная электротехническая комиссия	IEC	International electro technical commission
дин	Немецкие промышленные нормы	DIN	Deutche Industri Normen
TUV	Немецкая ассоциация технического надзора	TUV	Technischer UberwachungsVerein (Technical Inspection , Association)
ANSI	Американский институт стандартизации	ANSI	American national standard institute
ISA !	Американское общество приборостроителей	ISA	Instrument society of , America
NPD	Норвежский нефтяной директорат	NPD	Norwegian Petroleum ; Directorate
SINTEF I	Фонд научных и промышленных , исследований, Норвегия	SINTEF	Foundation of Scientific and Industrial Research
OREDA	Справочник данных о надежности, Норвегия	OREDA	Offshore Reliability Data Handbook
NORSOK	Норвежская организация стандартов нефтяной промышленности	NORSOK	Norwegian Oil Industry Standards ; Organization
NUREG	Комиссия по ядерному регулированию	NUREG	Nuclear Regulatory Commission

КИП и СА	**Контрольно-измерительные приборы и средства автоматизации**		**Instrumentation**
АСУТП	**Автоматизированная система управления технологическими процессами**	**ACS PCS PAS**	**Automated Control System Process Control System Process Automation System**
ТП	**Оборудование технологического процесса, находящееся под контролем**	**EUC**	**Equipment under control (IEC 61508) = Process (IEC 61511)**
РСУ	**Распределенная система управления**	**DCS BPCS EUCCS**	**Distributed control system Basic process control system (ISA 84.01) EUC control system (IEC 61508)**
ПАЗ СБ	**Система противоаварийной защиты - Система защиты Система безопасного останова Система останова процесса Высоко интегрированная система защиты Оборудованная под безопасность система - Система безопасности; Предназначенная для защиты система**	**ESD SSD PSD HIPS SIS SRS**	**Emergency shutdown system Safety shutdown system Process shutdown system High integrity protection system Safety instrumented system (DIN, ISA) Safety related system (IEC)**
E/E/PES PES	**Электрическая / Электронная / Программируемая электронная система Программируемая**	**E/E/PES PES**	**Electrical / Electronic / Programmable electronic system Programmable**

SS&SSS			
	электронная система		electronic system
ппо	Прикладное программное обеспечение	~~	Application software
CCF	Отказы общей причины, общего происхождения	CCF	Common Cause Failure
SFF	Доля безопасных отказов	SFF	Safe failure fraction
SIF	Функция безопасности	SIF	Safety instrumented function
СУПБ	Система управления промышленной безопасностью	PSM	Process safety management
RMP	Программа управления рисками	RMP	Risk management program
EPA	Агентство по охране окружающей среды	EPA	Environmental
OSHA	Управление по ТБ и охране труда	OSHA	Occupational safety and health administration
FMEA	Анализ эффектов режимов отказов	FMEA	Failure Modes Effect Analysis
FMEDA	Анализ режимов, эффектов и диагностики отказов	FMEDA	Failure Modes, Effects and Diagnostic Analj^sis
HAZOP	Исследование опасности и работоспособности	HAZOP	Hazard and operability study
HAZID	Идентификация отказов	HAZID	Hazard identification
HSE	Британская инспекция охраны здоровья	HSE	Health Safety Executive
РИА	Анализ опасности процесса	PHA	Process hazard analysis
QRA	Количественная оценка риска и надежности	QRA	Quantitative risk and reliability assessment

ЩШШШШШ	*МШШШШШ "ШшШШШШШШШШ^*		
FTA	**Анализ дерева отказов**	**FTA**	**Fault tree analysis**
СТБ ! тз	**Спецификация требований к безопасности**	**SRS**	**Safety requirements specification**
ALARP :	**Настолько низкий [показатель, уровень требований], насколько это оправдано практикой**	**ALARP**	**As low as is reasonably practicable**
MTTF	**Среднее время работы до отказа**	**MTTF**	**Mean time to failure**
MTBF	**Среднее время между отказами**	**MTBF**	**Mean time between failures**
MTTR ;	**Среднее время восстановления работоспособности**	**MTTR**	**Mean time to repair**
PFH № :	**Вероятность (интенсивность, частота) опасных отказов в час**	**PFH W**	**Probability (intensity) . of dangerous failures per hour**
PFD	**Средняя вероятность отказа выполнения требуемой функции (отказа на запрос)**	**PFD**	**Average probability to fail on demand - Average probability of dangerous event upon request**
RRF	**Фактор снижения риска**	**RRF**	**Risk reduction factor • = 1/PFH**
FIT	**$1.0*10^{-9}$ отказов в час**	**FIT**	**$1.0*10^{-9}$ failures per hour**

SIL	Интегральный уровень безопасности	SIL	Safety integrity level (ISA, IEC)
АК RC	Классы требований Безопасности	АК RC	AnforderurgsKlasse (DIN V 19250) = Requirements Class (DIN VVDE 0801)
HART	Комбинированный цифро-аналоговый протокол	HART	High Addressable Remote Transducer
HCF	Ассоциация протокола HART	HCF	HART Communication Foundation
HIS	Решения по интерфейсу HART	HIS	HART Interface Solutions
FF	Ассоциация Fieldbus	FF	Foundation Fieldbus
УОП	Управление оборудованием предприятия	PAM	Plant Asset Management
МРП	Менеджер ресурсов предприятия	PRM	Plant Resource Manager (Yokogawa Electric)
СОП	Система обслуживания поля (полевого оборудования)	AMS	Asset Management Solutions (Emerson)

2.7. Современная концепция безопасности

Потенциальная опасность систем управления и противоаварийной защиты состоит в возможности отказов, что является органическим свойством этих систем.

Безопасные системы управления и противоаварийной защиты должны разрабатываться таким образом, чтобы отказ любого компонента этих систем и все мыслимые последствия такого отказа не вызывали опасной ситуации на технологическом объекте.

Современная концепция безопасности состоит в том, что международные стандарты безопасности рассматривают систему безопасности комплексно, в целом, с учетом резервирования всех компонентов системы защиты, включая измерительные и исполнительные устройства, и самое главное:

- **Для конкретной конфигурации оборудования и программного обеспечения;**
- **В зависимости от конкретного применения;**
- **В процессе реального жизненного цикла системы.**

Стандарты безопасности определяют классы требований, а также общие меры по достижению этих требований в зависимости от предопределенной степени риска.

Только вся совокупность стандартов устанавливает возможные мероприятия, определяемые в соответствии с их эффективностью, возможным временем их реализации и дополнительными затратами на аппаратное и программное обеспечение.

Ошибки, проявляющиеся до запуска системы. Ошибки, проявляющиеся до запуска системы, должны рассматриваться совместно с мерами по их предотвращению. Это могут быть, например, ошибки технического задания, ошибки в постановке задачи, ошибки программирования, ошибки изготовления и т.д.

Ошибки, появляющиеся после запуска системы. Ошибки, появляющиеся после запуска системы, должны рассматриваться совместно с мерами по устранению неисправностей, например, дефектов оборудования, ошибок управления, экстремальных внешних воздействий и т.д.

Неисправности технических средств могут быть вызваны следующими причинами:

- Случайные отказы аппаратуры, например, одиночные отказы.
- Многократные отказы из-за накопления ошибок.
- Систематические ошибки в конструкции или при изготовлении оборудования.
- Неблагоприятные условия эксплуатации.
- Неквалифицированное техническое обслуживание.

Меры по предотвращению отказов. Из сказанного следует, что меры по предотвращению отказов должны быть направлены на выявление и предотвращение следующих негативных воздействий и нарушений работы системы:

- Систематические отказы технического и программного обеспечения,
- Ошибочные действия операторов,
- Ошибки обслуживания,
- Отказы из-за неблагоприятных условий эксплуатации и окружающей среды.

К числу методов, используемых в системах безопасности для уменьшения ущерба и снижения риска, относятся:

- Модернизация и замена полевого оборудования;
- Применение систем противоаварийной защиты;
- Усовершенствование системы управления процессом;
- Разработка дополнительных или более подробных процедур тренинга персонала по эксплуатации и техобслуживанию;
- Использование специального оборудования для снижения негативных последствий: взрывозащитных стен, пены, резервуаров с водой и систем для сброса давления;
- Изменение технологического процесса, в том числе технологической схемы или даже расположения оборудования;
- Повышение механической целостности оборудования;
- Увеличение частоты испытаний критических компонентов;
- Применение специальных средств оперативного контроля и тестирования полевого оборудования - *Plant Asset Management Systems* - с использованием возможностей протоколов HART и Fieldbus.

2.8. Электротехническая комиссия, Германия

Стандарт DIN V 19250 "Фундаментальные аспекты безопасности, рассматриваемые для связанного с безопасностью оборудования измерения и управления". В Германии методика определения риска описывается в стандарте DIN V 19250 "*Fundamental Safety Aspects To Be Considered For Measurement And Control Protective Equipment*Стандарт устанавливает концепцию систем безопасности, разработанных таким образом, чтобы соответствовать требованиям установленных классов *(Requirements Class - RC),* начиная с Класса 1 (RC1) и до Класса 8 (RC8). Ранее использовалось обозначение А К - *Anfonderungs Klasse.*

Выбор класса зависит от уровня риска конкретного процесса. Стандарт предписывает учитывать опасные факторы, свойственные технологическим процессам, и определять уровень допуска требуемой системы, связанной с безопасностью. Диаграмма рисков стандарта представлена на рис. 2.4.

Параметры риска

ОПОСЛЕДСТВИЯ АВАРИИ;
51 - Незначительные травмы
52 - Серьезные травмы одного или нескольких человек, смерть одного человека
53 - Смерть нескольких человек
S4 - Катастрофические последствия большие человеческие потери

^ЧАСТОТА И ВРЕМЯ НАХОЖДЕНИЯ В ОПАСНОЙ ЗОНЕ;
A1 - От редкого до относительно частого
A2 - Частое или постоянное

^ВОЗМОЖНОСТЬ ИЗБЕЖАТЬ ОПАСНОСТЬ;
G1 - Возможно при определенных обстоятельствах
G2 - Невозможно

ОВЕРОЯТНОСТЬ НЕЖЕЛАТЕЛЬНОГО СОБЫТИЯ;
W1 - Крайне низкая
W2 - Низкая
W3 - Высокая

Диаграмма рисков по стандарту DIN V 19250

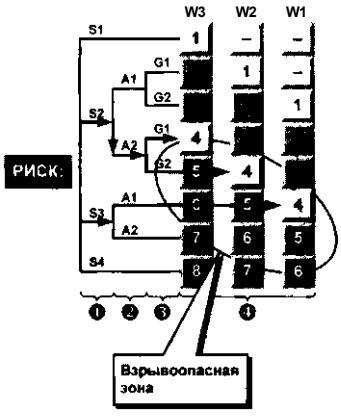


Рис. 2.4

Параметры риска по стандарту DIN V 19250 (см. рис. 2.4):

Травматизм

51 - Незначительные травмы

52 — Серьёзные травмы одного или нескольких человек, смерть одного человека

53 - Смерть нескольких человек

54 – Катастрофические последствия, большие человеческие потери.

Продолжительность нахождения в опасной зоне

A1 - От редкого до относительно частого

A2 - Частое или постоянное.

Предотвращение опасности

G1 - Возможно при определённых обстоятельствах

G2 - Невозможно.

Вероятность нежелательного события

W1 - Крайне низкая

W2 Низкая

W3 - Высокая.

Стандарт DIN V VDE 0801 "Принципы для компьютеров в системах, связанных с безопасностью". Стандарт DIN V VDE 0801 *Principles For Computers In Safety Related Systems "* устанавливает следующие аспекты при оценке программируемых электронных систем *(Programmable Electronic Systems-PES):*

- Проектирование;
- Конфигурирование (прикладной уровень);
- Внедрение и интегрирование в процесс;
- Аттестация.

Каждый из этих аспектов подвергается проверке конкретными методами. Результаты тщательно анализируются и документируются независимыми специалистами.

Таким образом, стандарт DIN V VDE 0801 предоставляет средства для определения соответствия PES определенным классам стандарта DIN V 19250.

DIN V VDE 0801:

- Предназначен для процессов, которые связаны с опасной химией, взрывоопасными и горючими жидкостями и газами;
- Требует исходного анализа опасности процесса за последние пять лет;
- Определяет требуемые измерения для проверки соответствия классам требований;
- Повторный анализ опасности должен производиться каждые пять лет;
- Требует разработки процедур безопасного управления и обслуживания;
- Допуск к работам имеет только персонал, прошедший обучение правилам безопасности, и сдавший экзамены на допуск;
- Должна быть выполнена проверка безопасности при предварительном пуске нового, или модифицированного процесса;
- Должны выполняться периодические инспекции и тестирование оборудования, а также проверки знаний ТБ.

Документирование:

- Должна быть разработана письменная процедура внесения каких-либо изменений в опасный процесс.
- Каждый инцидент должен быть расследован и записан в отчет.
- Каждые 3 года должен выполняться технический аудит.

Определение требуемого класса безопасности по стандарту DIN V 19250. Поскольку программируемые электронные системы все более широко используются в системах безопасности, возникает необходимость определить, соответствует ли данная система данной области применения и требуемому классу стандарта DIN V 19250.

Одной из наиболее известных организаций в области сертификации систем безопасности является Ассоциация Технического Надзора TUV, Германия.

Ассоциация Технического Надзора TUV. Ассоциация Технического Надзора TUV проводит сертификацию функциональной безопасности оборудования систем управления и защиты с присвоением соответствующей категории. TUV также проводит независимую сертификацию по стандартам третьей стороны, и использует для оценки систем противоаварийной защиты всю имеющуюся систему международных стандартов: DIN, IEC, ANSI, UL и т.д. (TUV не пишет собственных стандартов). Сегодня TUV присваивает уровень интегральной безопасности SIL по стандартам ANSI/ISA 84.01-96, IEC 61508, IEC 61511:

- Проводит сертификацию систем безопасности на соответствие определенным классам требований.
- Определяет ограничения и рекомендации на каждый тип систем безопасности.

TUV имеет представительства в 140 странах мира, и насчитывает около 10,000 сотрудников. За годы своего существования ассоциация провела сертификацию более 24000 изделий и 12000 систем. Сертификат TUV признан в десятках стран мира как допуск на отдельные компоненты систем, и систем в целом для защиты опасных производств.

2.9. Стандарты безопасности США

Стандарт ANSI/ISA 84.01-96 "Применение оборудованных под безопасность систем для технологических процессов". Стандарт ANSI/ISA 84.01 "*Application of Safety Instrumented Systems for the Process Industries*" - американский стандарт систем безопасности для технологических процессов. В разработке стандарта принимали участие более 100 промышленных компаний. Стандарт является результатом согласия между производителями и потребителями систем безопасности. В стандарте используются собственные уровни допуска систем безопасности SIL, но в то же время поддерживаются взаимосвязи стандарта DIN V 19250.

Стандарт НЕ рассматривает сенсоры и исполнительные элементы как составную часть программируемых электронных систем *(PES).* Вместе с тем, стандарт вводит понятие Системы безопасности *(Safety Instrumented System - SIS),* которое объединяет все составные элементы оборудова-

ния, участвующие в обеспечении безопасности - от сенсоров до исполнительных элементов, включая модули ввода-вывода, интерфейсы пользователя системы, источники энергии и собственно логические устройства.

В отличие от стандарта общего назначения IEC 61508, Стандарт 84.01-96 не включает в себя наивысший класс допуска SIL4. Комитет S84 не считает областью действия программируемых электронных систем защиту от катастроф.

Дополнительно используется **Технический отчет** безопасного технического допуска dTR84.02 - ISA TR84.0.02 *"Safety Instrumented Systems (SIS) - Safety Integrity Level (SIL) Evaluation Techniques"* (Оборудованные под безопасность системы - Техника оценки интегрального уровня безопасности), разработанный подкомиссией ISA (SP84.02).

Стандарт ANSI/ISA 84.01-96 впервые вводит понятие **Модели жизненного цикла системы безопасности** (см. рис. 2.5).

2.10. Общие методы анализа рисков

Технический отчет dTR84.02 представляет основные методики анализа рисков для систем безопасности, позволяющие получить ответ на главный вопрос: будет ли система в состоянии выполнить предопределенные функции, когда в этом возникнет необходимость.

Три методики:

- Метод логических блок-диаграмм
- Анализ дерева отказов
- Марковский анализ.

Марковский анализ назван в честь великого русского математика Андрея Андреевича Маркова (1856 - 1922 г.). Ученик знаменитого Чебышева — создателя русской школы теории вероятностей, давшего доказательство закона больших чисел, поражающее своей красотой и элементарностью. Марков ~ Академик Петербургской академии наук, автор пионерских работ по математическому анализу, дифференциальным уравнениям, теории чисел, теории вероятностей, многие из которых сохраняют свою актуальность до сих пор. Маркову принадлежит обобщение закона больших чисел на случай ***зависимых*** *случайных величин.*

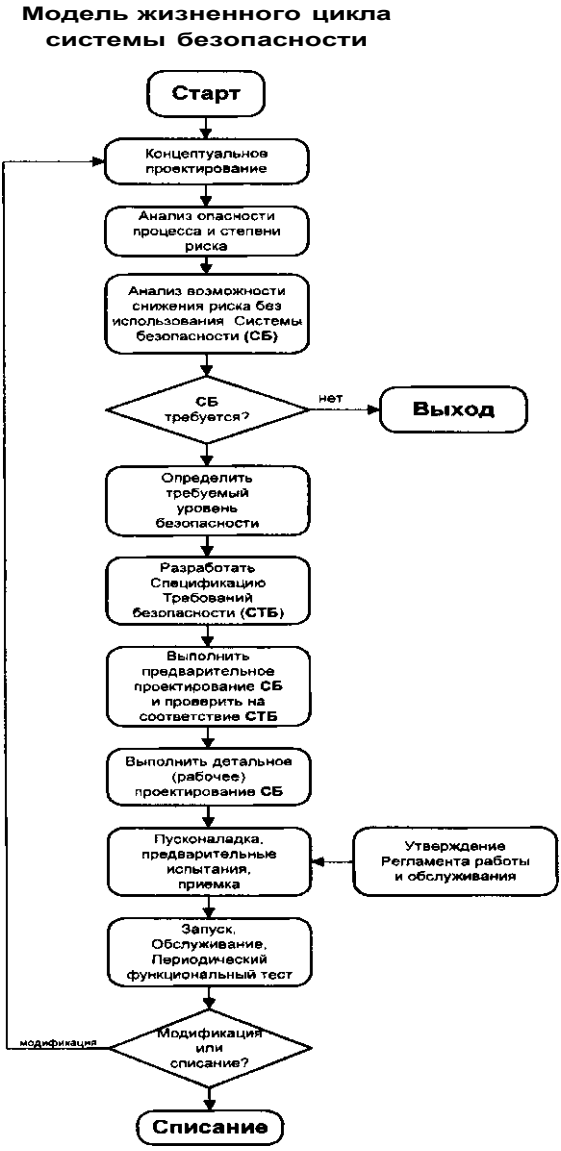

Модель жизненного цикла системы безопасности
Старт
Концептуальное проектирование
Анализ опасности процесса и степени риска
Анализ возможности снижения риска без использования Системы безопасности (СБ)
СБ требуется?
нет
Выход
Определить требуемый уровень безопасности
Разработать Спецификацию Требований безопасности (СТБ)
Выполнить предварительное проектирование СБ и проверить на соответствие СТБ
Выполнить детальное (рабочее) проектирование СБ
Пусконаладка, предварительные испытания, приемка
Утверждение Регламента работы и обслуживания
Запуск, Обслуживание, Периодический функциональный тест
Модификация или списание?
модификация
Списание

Рис. 2.5

Первый шаг.

Для каждой из перечисленных методик первым шагом является определение интенсивности отказов для каждого элемента, модуля, или комплектной подсистемы. Многие поставщики предоставляют эти данные с большой неохотой. Отказ от предоставления данных о надежности оборудования и, что не менее важно, методик расчета параметров надежности, должен породить сомнения в добросовестности поставщика оборудования.

Для метода логических блок-диаграмм следующим шагом будет объединение (логическое сложение и умножение) вероятностей отказов отдельных компонентов. Однако и этот метод может оказаться не совсем простым, если в составе анализируемой цепочки компонентов оказывается конкретная конфигурация из нескольких логических устройств, нескольких сенсоров и нескольких исполнительных устройств, завязанных в единую физическую и логическую последовательность.

Конкретные примеры расчетов приведены в стандарте IEC 61508. По результатам этих расчетов производится сравнение полученных вероятностей с требуемыми для определенного класса значениями (таблица 2.3).

Таблица 2.3

Интегральный уровень безопасности (SIL)

SIL	Допустимая вероятность опасного отказа pfd_{avg}	Требуемая надежность (стационарная готовность) $(1 \sim PFD_{avg})$	Вероятность (частота) опасных отказов (1/час) $PF^{\wedge}avg\,(^{\wedge}AVG)$	Фактор снижения риска (годы) $RRF = 1/PFH_{AVG}$
1	от 10^{-2} до 10^{-1}	90% - 99%	от 10^{-6} до 10^{-5} >	От 10 до 100 лет
2	от 10^{-3} до 10^{-2}	99% - 99.9%	от 10^{-7} до 10^{-6}	От 100 до 1000 лет
3	от 10^ до $1СГ^{3}$ <	99.9% - 99.99%	от $КГ^{8}$ до $1(Г^{7}$ |	От 1000 до 10000 лет
4 !	Менее 1СГ*	Более 99 99%	Менее $1СГ^{8}$!	Более 10000 лет

В случае метода анализа дерева отказов следующим шагом будет создание диаграммы дерева отказов. Анализ дерева отказов - это специальная техника, которая используется для анализа и идентификации условий и факторов, вызывающих появление определенного нежелательного события.

Дерево отказов имеет одно головное нежелательное событие - аварию или инцидент, которое обуславливается набором нижестоящих событий - ошибок или отказов. Эти причинно-следственные цепи называют сценариями.

Для связи между событиями в узлах деревьев используются операции "И" и "ИЛИ". Операция "И" означает, что вышестоящее событие возникает при одновременном наступлении подлежащих событий. Операция "ИЛИ" означает, что вышестоящее событие может произойти при возникновении одного из подлежащих событий. Собственно анализ дерева заключается в определении причин и их комбинаций, которые приводят к появлению головного события.

На первом этапе - это качественный анализ. Но если вероятности появления базовых событий известны, то вероятность головного события может быть вычислена по правилам булевой алгебры. Существуют программные средства генерации и обсчета деревьев.

И так же, как и в первом случае, по результатам расчетов производится сравнение полученной сводной вероятности отказа с требуемыми значениями (таблица 2.3).

Наиболее точным является **Марковский анализ.** Метод заключается в разработке диаграммы состояний и переходов Марковского процесса. В диаграмму состояний и переходов включаются все мыслимые состояния процесса, которые могут возникнуть вследствие отказа любого из компонентов процесса, включая состояния полного останова, и задаются интенсивности перехода системы из одного состояние в другое. По диаграмме формируется система дифференциальных уравнений, и в результате ее решения определяются вероятности нахождения процесса в определенных состояниях **как функции времени.** Естественно, что полученная Марковская модель допускает и статические решения в зависимости от предопределенных начальных условий.

Все другие методы оценки вероятностей отказов системы позволяют производить **только** статические расчеты.

Всеобъемлющий учет всех факторов, влияющих на надежность и безопасность, делает Марковский анализ лучшим, но одновременно и самым сложным и трудоемким с математической (и не только) точки зрения методом предсказания надежности и безопасности системы. И так же, как и в первом случае, по результатам расчетов производится сравнение полученных значений вероятности отказа с требуемыми значениями таблицы 2.3, и определяется общий уровень безопасности процесса.

Из сказанного следует, что самым простым является метод логических блок-схем, который дает наиболее консервативную оценку опасности процесса, и обычно используется в качестве первого приближения для оценки требуемого уровня безопасности.

Метод анализа дерева отказов рассматривается многими как возможный компромисс между простотой метода логических блок-схем, и полнотой Маковского анализа для вычислений общего уровня безопасности.

Марковский анализ проводится экспертами по промышленной безопасности, и используется ими не только для определения существующего уровня опасности, но и для перепроектирования системы безопасности с целью снижения этого уровня.

Технический отчёт обеспечивает сравнение различных архитектур программируемых электронных систем. Технический отчёт определяет уровень допуска по интенсивности отказов, по наработке на отказ, по требуемой степени диагностики, по требуемой периодичности тестирования.

2.11. Методы анализа риска и опасных факторов в США

Перед конкретным применением стандарта 84.01-96 требуется провести специальное обследование опасности технологического процесса. В Соединенных Штатах существуют нормы управления безопасностью процесса **PSM** *(Process Safety Management),* управления по технике безопасности и охране труда **OSHA** *(Occupational Safety and Health Administration),* и программы управления рисками **RMP** *(Risk Management Program)* агентства по защите окружающей среды *EPA (Environment Protection Agency).*

Эти нормы требуют проведения анализа опасности процесса PHA *(Process Hazards Analysis)* для идентификации потенциально опасных факторов в ходе эксплуатации технологического процесса, и для разработки мер, необходимых для защиты персонала, населения и окружающей среды.

Объем проведения PHA может меняться от простейшего классификационного анализа до всестороннего исследования опасности и работоспособности **HAZOP** *(Hazard and Operability Study).* Процедура **HAZOP** представляет собой систематическую и методическую проверку технологического процесса, в ходе которой команда, представленная различными специалистами, идентифицирует опасные факторы и проблемы эксплуатации, способные стать причиной аварии. Процедура **HAZOP** обеспечивает приоритетный базис для внедрения стратегий снижения риска, таких как системы безопасности SIS *(Safety Instrumented System).*

Если в результате анализа опасности процесса *(Process Hazards Analysis - PHA)* выясняется, что механическая целостность оборудования и стандартное управление процессом недостаточны для снижения потенциальной опасности, то утверждается, что необходима система защиты. Она состоит из измерительных приборов и органов управления (в общем случае - резервированных), устанавливаемых с целью уменьшения опасности или перевода процесса в безопасное состояние в случае нарушения нормального хода технологического процесса, либо сбоя самой системы защиты. Если в ходе анализа опасности процесса выявляется, что необходима система безопасности, в соответствии с требованиями стандарта ANSI/ISA 84.01-96 задается целевой уровень допуска безопасности SIL.

В отличие от уникальной попытки МЭК формализовать методы выбора архитектуры систем безопасности, в США задание SIL является по преимуществу корпоративным решением, основанным на философии управления риском, и исходя из допустимого риска. Нормы по безопасности предписывают, чтобы процедура задания SIL проводилась тщательно и документировалась полностью.

По завершению процедуры HAZOP определяется серьезность и вероятность возникновения связанных с данным процессом рисков.

Серьезность риска оценивается по степени ожидаемого воздействия и последствиям, к которым относятся:

- Последствия на территории установки;
- Травмы или смерть производственного персонала;
- Ущерб оборудованию;
- Последствия за пределами установки;
- Воздействие на население, в том числе травмы и смерть;
- Ущерб собственности;
- Воздействие на окружающую среду;
- Выброс опасных химических веществ;
- Загрязнение воздуха, почвы и водных источников;
- Ущерб в экологически чувствительных зонах.

Степень риска - это оценка вероятности наступления неблагоприятного события. Степень риска классифицируется как высокая, средняя или низкая, и часто основывается на опыте самой компании или ее конкурентов.

Для преобразования данных HAZOP в SIL используются различные методы - от принятия корпоративного решения по всем установкам системы безопасности до более точных методик, таких как диаграмма риска стандарта IEC 61508, заимствованная из немецкого стандарта DIN V 19250.

2.12. Российские нормы анализа рисков и последствий отказов

За последние годы появилась группа очень добротных отечественных нормативных документов по анализу рисков и оценке последствий отказов:

- РД 03-418-01 *"Методические указания по проведению анализа риска опасных производственных объектов",* основанные на анализе деревьев отказов и событий.
- ГОСТ 27.310-95 *"Анализ видов, последствий и критичности отказов*

РД 03-418-01 дает вполне определенные рекомендации:

Пункт 5.2: "При выборе и применении методов анализа риска рекомендуется придерживаться следующих требований:

- *Метод должен быть научно обоснован и должен соответствовать рассматриваемым опасностям;*

- *Метод должен давать результаты в виде, позволяющем лучше понять формы реализации опасностей и наметить пути снижения риска;*
- *Метод должен быть повторяемым и проверяемым ".*

Пункт 5.3: "На стадии идентификации опасностей рекомендуется использовать один или несколько из перечисленных ниже методов анализа риска:

- *"Что будет, если... ? ";*
- *Проверочный лист;*
- *Анализ опасности и работоспособности;*
- *Анализ вида и последствий отказов;*
- *Анализ дерева отказов;*
- *Анализ дерева событий*

Приводятся конкретные показатели по уровню и критичности последствий отказа, аналогичные тем, что используются на западе.

Критерии отказов по тяжести последствий:

- Катастрофический отказ - приводит к смерти людей, существенному ущербу имуществу, наносит невосполнимый ущерб окружающей среде;
- Критический / Некритический отказ - угрожает / не угрожает жизни людей, приводит / не приводит к существенному ущербу имуществу, окружающей среде;
- Отказ с пренебрежимо малыми последствиями - отказ, не относящийся по своим последствиям ни к одной из первых трех категорий.

Категории (критичность) отказов:

- "А" - Обязателен количественный анализ риска, или требуются особые меры обеспечения безопасности;
- "В" - Желателен количественный анализ риска, или требуется принятие определенных мер безопасности;
- "С" - Рекомендуется проведение качественного анализа опасностей или принятие некоторых мер безопасности;
- "Д" - Анализ и принятие специальных (дополнительных) мер безопасности не требуется.

Возможные сочетания этих показателей приводятся в таблице 2.4.

Таблица 2.4

Частота возникновения отказа, 1/год		Тяжесть последствий отказов			
		катастрофический отказ	критический отказ	некритический отказ	отказ с пренебрежимо малыми последствиями
Частый отказ	> 1				с
Вероятный отказ	1 - КГ^2			в	с
Возможный отказ	10^2-КГ^4		в	в	с
Редкий отказ	КГ^4-10*	А	в	с	д
Практически невероятный отказ	<10*	В	с	с	д

Из представленных категорий и критериев тяжести отказов следует, что взрывоопасные объекты нефтегазодобывающей, химической, нефтехимической и нефтеперерабатывающей промышленности прочно занимают ячейки, выделенные серым цветом, поэтому **количественный анализ риска для них обязателен.**

Существенное замечание

Необходимо понимать, что при всей внешней стройности метод на основе анализа дерева отказов и событий имеет существенные ограничения:

- *Лишь одно нежелательное событие может быть корневым. Соответственно, для каждого типа отказа нужно создавать свое дерево. Пример - дерево опасных отказов (несрабатывание), и дерево ложных отказов - немотивированный останов.*
- *Модель статична. Поэтому вероятность проявления нежелательного события представляет собой суперпозицию отказов, возникшую в некий абстрактный срез времени.*
- *Базовые отказы имеют неприятное свойство концентрироваться и, как правило, взаимосвязаны самым непредсказуемым образом. Классическое дерево не имеет горизонтальных и перекрестных связей, и не может представить взаимную коррелированность отказов на разных ветвях.*

- *Дерево по определению не имеет циклов и, соответственно, не позволяет моделировать системы с восстановлением после отказа - обратного хода нет.*

И самый важный аспект - высокая зависимость результативности метода от компетентности исследователя. Он должен досконально знать свойства того объекта, который исследуется. Иначе какие-то из возможных комбинаций отказов будут пропущены, и результат анализа во многом потеряет смысл.

2.13. Международные стандарты безопасности

Уровни защиты. На рис. 2.6 показано, как различные уровни защиты используются для снижения неприемлемого риска до приемлемого уровня.

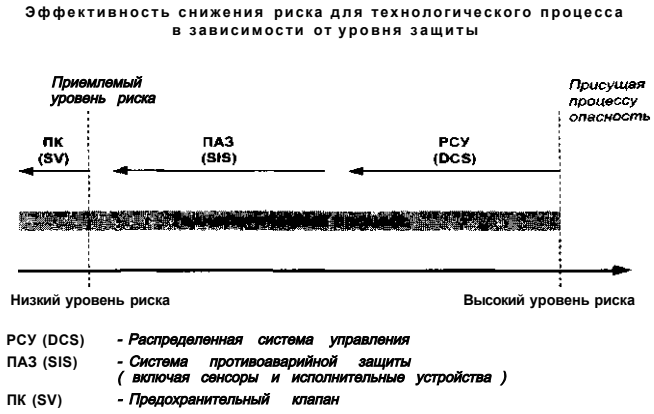


Рис. 2.6

Величина снижения риска для каждого уровня зависит от конкретной природы фактора риска, и влияния уровня защиты на данный фактор. В общем случае фактор снижения риска может быть определен как степень, в которой снижается производственный риск по сравнению с ситуацией при отсутствии системы безопасности. Естественно, что при определении подходящей комбинации уровней защиты для снижения факторов риска необходимо учитывать и экономическую целесообразность.

Факторы, влияющие на надежность системы защиты. При определении необходимой конфигурации системы защиты в состав анализируемого оборудования включаются измерительные приборы и органы управления, ответственные за перевод процесса в безопасное состояние в случае отказа. Надежность системы защиты зависит от следующих факторов:

1. Тип установленных измерительных приборов и управляющих устройств.
2. Степень резервирования основных компонентов системы:
   - Центральных процессоров,
   - Плат ввода-вывода,
   - Сетевых плат,
   - Источников питания,
   - Измерительных и исполнительных устройств.
3. Тип и частота отказов компонентов.
4. Уровень диагностического обеспечения.
5. Частота проведения тестовых испытаний и проверок.

2.14. Стандарт IEC 61508 Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью"

(Functional Safety of Electrical /Electronic /Programmable Electronic Safety Related Systems)

Стандарт Международной Электротехнической Комиссии *(International Electrotechnical Commission)* IEC 61508 - "Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью" - это международный стандарт, разработанный для определения систем безопасности *(Safety Related Systems - SRS)* общего вида.

Стандарт может использоваться для любых отраслей промыгиленности, где имеется необходимость в использовании программируемых систем безопасности. Дата официального утверждения стандарта - 2000 год.

В целом стандарт довольно сложен для восприятия не только из-за своего огромного объема (более 400 страниц убористого текста на двух языках - английском и французском), но и чрезвычайно усложненной и запутанной терминологии.

Стандарт определяет концепцию **Модели жизненного цикла системы безопасности,** аналогичную ISA 84.01-96 (см. рис. 2.7 - 2.9).

Общая схема модели жизненного цикла, которую воспроизводит и структура самого стандарта IEC 61508, приведена в первой главе настоящей работы "Постановка задач автоматизации", рис. 1.7.

Модель жизненного цикла системы устанавливает, что уровень допуска системы не ограничивается изначальным уровнем допуска входящих в нее устройств, включая датчики и исполнительные механизмы.

Уровень допуска системы, точно так же, как и уровень допуска человека, должен определяться и подтверждаться для всех стадий и этапов на всем жизненном пути:

- Зарождение идеи;
- Предварительное обследование и оценка;
- Проектирование;
- Эксплуатация;
- Испытания, проверка и техобслуживание.

Стандарт представляет безопасность как "свободу от неприемлемого риска". Иными словами, абсолютной безопасности достичь невозможно, можно только снизить риск до приемлемого уровня.

Стандарт определяет **4 уровня интегральной безопасности** *(Safety Integrity Level - SIL)* в зависимости от конкретной вероятности отказа выполнения требуемой функции *(Probability of Failure on Demand - PFD):*

УРОВНИ безопасного допуска SIL по стандарту IEC 61508

4	-	Защита от общей катастрофы
3	-	Защита обслуживающего персонала и населения
2	_	Защита оборудования и продукции, защита от травматизма
1	-	Защита оборудования и продукции

Модель жизненного цикла электрической, электронной, программируемой электронной системы безопасности (E/E/PES)

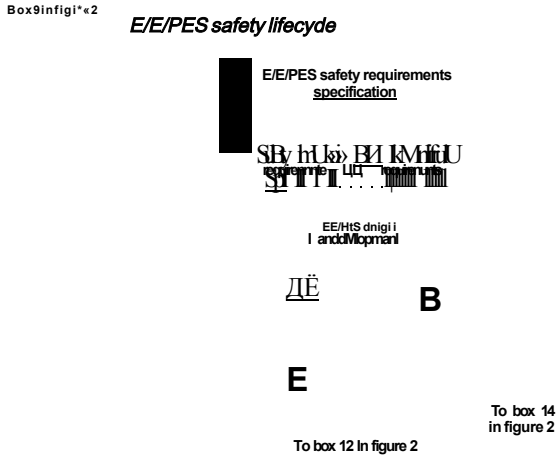


Рис. 2.7

Модель жизненного цикла программного обеспечения

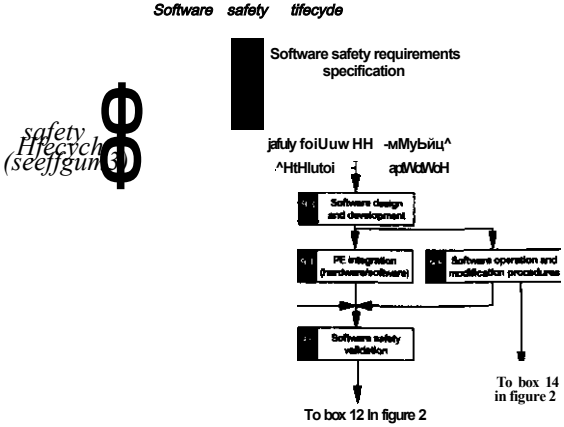


Рис. 2.8

Взаимодействие моделей жизненного цикла электрической, электронной, программируемой электронной системы безопасности (E/E/PES) и программного обеспечения

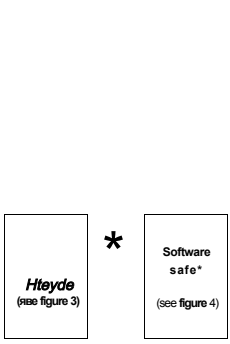


Рис. 2.9

При этом необходимо понимать, что, например, принятие уровня допуска SIL1 означает, что уровень опасности процесса и ограничения на экономические потери при отказе системы защиты низки настолько, что системе разрешается 10% отказов выполнения функций защиты (см. таблицу 2.3).

Соответственно, 90% надежность будет означать, что из каждых десяти случаев превышения, например, уровня в емкости, в одном случае из этих десяти произойдет переполнение емкости.

Фактор снижения риска также нуждается в правильной интерпретации. Например, увеличение фактора снижения риска до 100 и более лет при уровне допуска SIL2 вовсе не означает, что данная конкретная система способна проработать без опасных отказов и ложных срабатываний эту самую сотню лет. Данное значение означает, что из сотни одновременно работающих систем одна система в течение одного года приведет процесс к опасному отказу.

В конечном итоге, задание уровня допуска SIL основывается на требуемой величине снижения риска, определяемой в ходе анализа опасности процесса.

Конечно, каждое предприятие вольно самостоятельно принимать решения, и устанавливать свои требования к системам безопасности на основе собственной технической поли-

тики. Однако современные стандарты безопасности устанавливают и требуют от предприятий соответствия предписаниям, выработанным на основе опыта эксплуатации и анализа причин аварий большого числа взрывопожароопасных производств. Сказанное означает, что в любом случае выбор уровня интегральной безопасности и соответствующей ему системы защиты должен быть тщательно проанализирован, обоснован и точно документирован. Диаграмма рисков и уровни допуска стандарта IEC 61508 представлены на рис. 2.10.

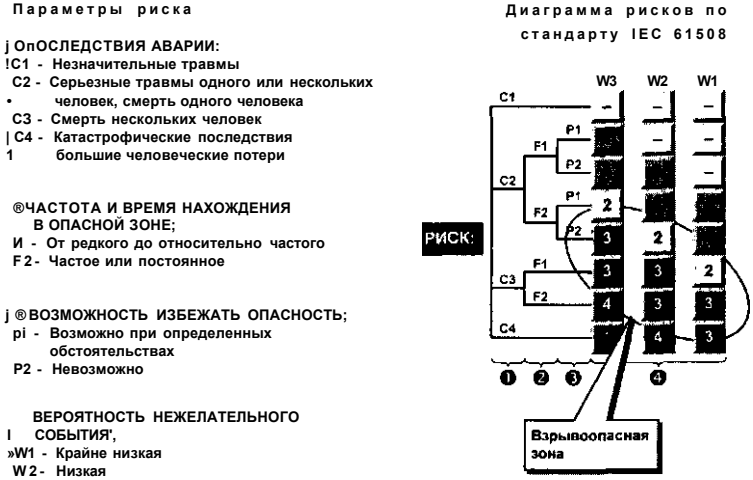


Рис. 2.10

Важное дополнение

Стандарт определяет требования к профессиональной подготовке и квалификации специалистов, определяющих уровень требований к системам безопасности для конкретного процесса.

В отличие от всех предыдущих стандартов безопасности, стандарт IEC 61508 предусматривает непосредственное участие технологического персонала в обеспечении функций безопасности. Вместе с тем, в стандарте делается оговорка, что конкретные требования к технологическому и обслуживающему персоналу должны устанавливаться в отраслевых

стандартах *(и в стандартах предприятия - Ю.Ф.),* которые должны разрабатываться с учетом общей методологии безопасности, определяемой данным стандартом.
В самом общем виде, стандарт IEC 61508:

1. Определяет Модель развития системы безопасности.
2. Определяет два подхода к системам безопасности:
   - Системы, обеспечивающие защиту и непрерывность контроля по средней частоте опасных отказов, и
   - Системы, обеспечивающие защиту и контроль по средней вероятности опасного отказа в течение предопределенного интервала времени.
3. Определяет концепцию безопасного *допуска.*
4. Устанавливает 4 уровня безопасного допуска (SIL).

Структура и параметры риска стандарта IEC 61508 заимствованы запросто и без церемоний из немецкого стандарта DIN 19250. При этом структуры диаграмм параметров риска для DIN и IEC полностью совпадают (сравните рис. 2.4 и 2.10).

Параметры риска по стандарту IEC 61508 (см. рис. **2.10):**

Травматизм

C1	**Незначительные травмы**
C2	**Серьёзные травмы одного или нескольких человек, смерть одного человека**
C3	**Смерть нескольких человек**
C4	**Катастрофические последствия, большие человеческие потери.**

Продолжительность нахождения в опасной зоне

F1	-	**От редкого до относительно частого**
F2	-	**Частое или постоянное.**

Предотвращение опасности

P1	-	**Возможно при определённых обстоятельствах**
P2	-	**Невозможно.**

Вероятность нежелательного события

W1 - Крайне низкая

W2 Низкая

W3 - Высокая.

2.15. Стандарт IEC 61511 "Функциональная безопасность: Оборудованные под безопасность системы для перерабатывающего сектора промышленности"

Стандарт IEC 61511 "*Functional Safety: Safety Instrumented Systems for the Process Industry Sector*" - это международный стандарт, разработанный для совместного использования с IEC *61508.*

В дополнение к стандарту IEC 61508, который определяет общие требования безопасности, в 2004 году МЭК приняла стандарт безопасности технологических процессов IEC 61511.

Стандарт IEC 61508 изначально предназначался для производителей и поставщиков оборудования.

Стандарт IEC 61511 предназначен для проектировщиков систем безопасности, специалистов по их интегрированию в процесс - разработчиков, и **пользователей** систем управления производственными и технологическими процессами.

Стандарту IEC 61511 должны соответствовать системы безопасности, предназначенные для защиты технологических процессов в нефтяной, газовой, химической, нефтехимической и других отраслях промышленности.

Сенсоры, логические устройства и исполнительные элементы стандартом IEC 61511 также рассматриваются как составные элементы системы безопасности.

Стандарт также рассматривает интерфейсы с другими уровнями контроля и управления на соответствие общим требованиям безопасности производства и даже человеческого сообщества (см. рис. 2.11).

Аналогично стандарту IEC 61508, стандарт IEC 61511 определяет две главных концепции, которые лежат в основе его практического применения:

1. **Жизненный цикл системы безопасности;**
2. **Интегральный уровень безопасности.**

Концепция уровней защиты согласно IEC 61511

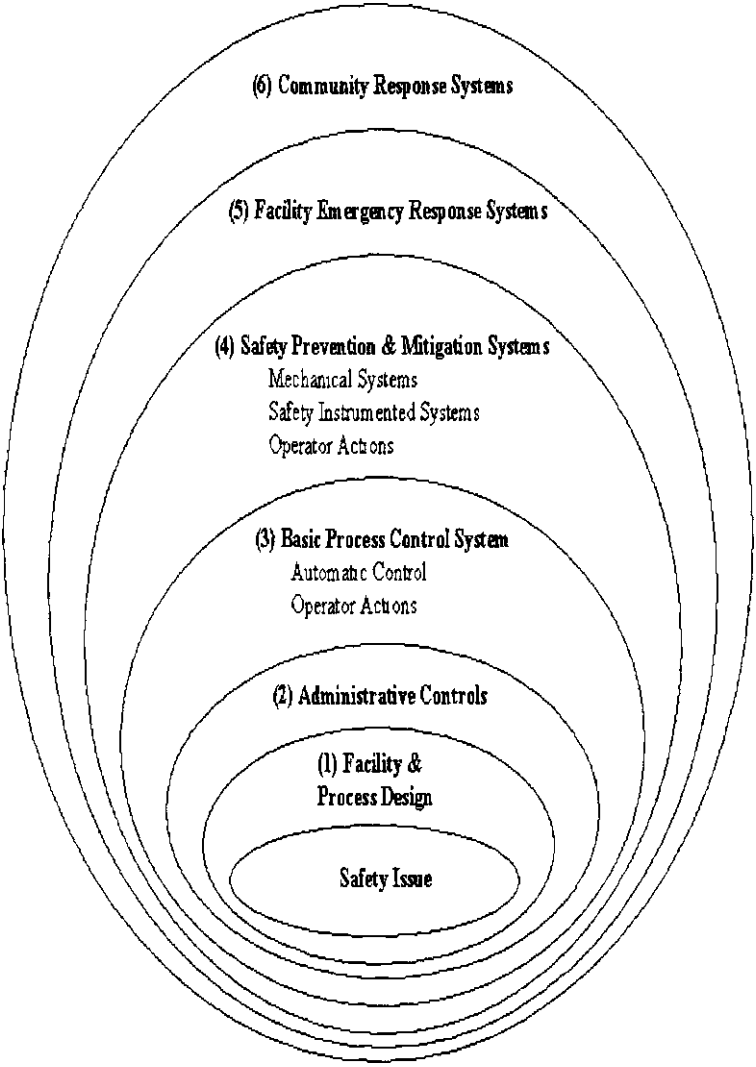


Рис. 2.11

Стандарт охватывает полный жизненный цикл системы:

- Проектирование;
- Сборка;
- Внедрение;
- Эксплуатация;
- Обслуживание;
- Модификация;
- Списание системы.

При рассмотрении жизненного цикла системы:

- Количественно оцениваются риски технологического процесса,
- Определяются требования к системе безопасности, включающей сенсоры и исполнительные элементы,
- Рассматриваются и проектируются уровни управления и защиты и, наконец,
- Определяется архитектура системы безопасности, обеспечивающая защиту от рисков процесса.

Так же, как и стандарт IEC 61508, стандарт IEC 61511 имеет 4 уровня интегрального допуска.

Но в отличие от стандарта общего назначения IEC 61508, **стандарт IEC 61511 не рекомендует рассматривать катастрофические процессы, соответствующие наивысшему уровню требований SIL4, в качестве области применения программируемых электронных систем.**

Идентификация интегрального уровня безопасности SIL. Позиция автора. Уровень допуска системы безопасности может рассматриваться как статистическое представление соответствия системы заданному интегральному уровню безопасности.

При этом необходимо ясно понимать, что данные требования относятся изначально к каждой **отдельной функции,** включающей в себя и сенсоры, и логические устройства, и исполнительные элементы. Некорректно утверждать, что отдельная единица оборудования имеет некий собственный интегральный уровень безопасности.

Некоторый компонент оборудования системы может быть одобрен на применение по определенному уровню SIL, но наличие сертификата составляет всего лишь незначительную часть общих усилий по безопасности, поскольку на соответст-

вие требуемому уровню должны быть проверены значения вероятностей отказа **всех комплексных критических** функций **в конкретном приложении.** И только потом могут быть определены значения интегральных показателей надежности всего программно-технического комплекса системы.

Система только тогда способна достичь требуемого уровня интегральной безопасности, когда весь технологический цикл был рассмотрен на соответствие данному уровню.

Необходимо удостовериться и закрепить документально, что:

- Архитектура системы соответствует спецификации;
- Все компоненты системы находятся на своих местах и правильно работают;
- Функции системы реализованы в соответствии с Техническим заданием;
- Документация разработана в соответствии с проектом.

Только в таком случае может появиться уверенность, что SIL действительно является интегральным показателем созданной системы, и учитывает все жизненно необходимые факторы:

- Уровень допуска и отдельных устройств, и системы в целом;
- Описание и идентификация возможных отказов, и отказов общего происхождения;
- Процедуры предварительных и периодических испытаний;
- Требования к эксплуатации;
- Метрологическое обеспечение;
- Диагностика и техническое обслуживание;
- Обучение и квалификация персонала.

Глава 3

АРХИТЕКТУРА СИСТЕМ УПРАВЛЕНИЯ И ЗАЩИТЫ

3.1. Безопасные ПЛК

Безопасные программируемые логические контроллеры (ПЛК) - это техника специального назначения, которая используется для обеспечения задач безопасности и критического управления в системах автоматизации. Эти контроллеры являются центральным компонентом систем безопасности, и предназначены для выявления потенциально опасных технологических ситуаций, и предотвращения их дальнейшего развития. В том случае, если подобная ситуация все-таки возникает, система безопасности программируется таким образом, чтобы автоматически перевести процесс в безопасное состояние.

Существуют серьезные ограничения на использование ПЛК, в особенности при временных ограничениях на восстановление работоспособности после сбоя. ПЛК общего назначения, не имеющие специального допуска на применение в системах защиты, не могут использоваться в критичных по отношению к безопасности приложениях.

Рассмотрим разницу между безопасным ПЛК и обычным, и зададимся вопросом: почему обычные ПЛК не могут использоваться для реализации функций защиты и критичного по отношению к безопасности управления. Доктор William M. Goble, лидер независимой группы экспертов Exida, чей авторитет котируется в профессиональном мире уж никак не ниже пресловутого TUV, в статье *"Conventional PLC vs. Safety PLC", Exida, 2000,* указывает на принципиальную разницу между обычными и безопасными ПЛК.

Безопасные программируемые логические контроллеры специально спроектированы для достижения двух важнейших целей:

- Обеспечение безотказности за счет достаточного уровня резервирования и, если отказа все же не удается избежать,
- Отказ должен сказываться на процессе только предсказуемым, безопасным образом.

Для того чтобы наделить системы данным набором качеств, предпринимается ряд специальных проектных решений. Безопасные ПЛК имеют изощренную внутрисистемную аппаратную и программную диагностику, которая позволяет программно-техническому комплексу с большой степенью достоверности определять собственную нештатную работу:

- Безопасные ПЛК имеют специальные средства для проверки правильности и надежности программного обеспечения.
- Безопасные ПЛК по определению используют резервирование, которое позволяет поддерживать безопасность технологического процесса даже при отказе части оборудования.
- Безопасные ПЛК имеют дополнительные средства защиты операций чтения и записи по каналам связи.

Однако доктор Goble не упоминает о самом важном качестве систем безопасности, ядро которых составляют безопасные ПЛК:

Системы, предназначенные для выполнения задач управления и защиты технологических процессов, - <u>это детерминированные системы</u>, то есть такие системы, которые должны обеспечивать реакцию на событие в течение известного предопределенного интервала времени при любых обстоятельствах.

Все элементы системы - от сенсора до исполнительного механизма - должны обеспечивать не абстрактное "математически" ожидаемое, а точно известное время реакции.

Сказанное означает, что детерминированная система должна обладать значительной аппаратной и функциональной избыточностью по всем компонентам системы: процессоры, память, шины данных, количество каналов ввода-вывода, частота сканирования каналов и программ, и т. д.

Промышленные сети также должны подчиняться этим требованиям: характеристикой промышленной сети должно быть гарантированное время реакции на событие, а не средняя скорость передачи.

Для недетерминированных систем собственные вычислительные ресурсы и средства коммуникации могут внести непредсказуемые задержки в силу различных внешних и внутренних причин:

- Обработка асинхронных прерываний извне.
- Отсутствие реальной многозадачности и неумение работать по приоритетам.
- Ожидание освобождения общего ресурса (процессор, память, драйвер...).
- Использование устройств с непредсказуемым временем реакции (позиционирование жесткого диска) и тому подобное.

То, что недетерминированные системы не способны обеспечить заданное время реакции даже при отсутствии внешних причин, на своей шкуре испытано всеми пользователями Windows. Вам остается только с изумлением наблюдать, как система - и модель, и воплощение абсолютной власти - живет своей внутренней и очень насыщенной жизнью, которая к вам не имеет абсолютно никакого отношения. А ваши действия ей только мешают, и воспринимаются не иначе, как досадная необходимость чистить зубы. Воистину монумент бесконечному снобизму и авантюризму ее создателей. Но ради мирового информационного захвата и не такое сделаешь.

Детерминированное, предсказуемое поведение системы неразрывно связано с понятием **жесткого реального времени. В** жесткой системе:

- **Опоздания не допускаются ни при каких обстоятельствах.**
- **Опоздание считается катастрофическим сбоем.**
- **Цена опоздания очень велика.**

Таким образом, системы безопасности в целом и безопасные **ПЛК** в частности, должны обеспечивать **гарантированное время реакции на события.** Это требование предполагает жесткий временной цикл работы системы, рассчитанный на самую неблагоприятную ситуацию по событиям.

Еще одним важным отличием безопасных ПЛК является **независимая сертификация** этих систем третьими организациями на предмет их соответствия требованиям безопасности и надежности по международным стандартам.

Дополнительные требования предъявляются к проектированию, изготовлению и тестированию данных ПЛК. Независимые эксперты третьей стороны, такие как Exida, TUV или Корпорация совместной инспекции производства, США *(Factory Mutual Research Corporation - FM%* обеспечивают проверку качества разработки, конструкции и заводских процедур тестирования безопасных ПЛК. Тщательный анализ применяемых схемных решений и диагностического программного обеспечения, полное тестирование оборудования с искусственным внесением всех мыслимых отказов позволяет определить и выявить более 99% потенциально опасных отказов компонентов системы. Чтобы понять, каким образом может отказать каждый компонент системы, как система способна выявить эти отказы, и как система реагирует на отказы, при конструировании проводится анализ режимов отказов, эффектов и диагностики отказов *(Failure Modes, Effects and Diagnostic Analysis* - FMEDA). Эксперты FM, Exida или TUV **персонально** выполняют процедуры тестирования отказов как часть процесса сертификации.

При испытаниях системного программного обеспечения проводится расширенный анализ и тестирование, включающее проверку операционных систем реального времени, многозадачного взаимодействия и прерываний. Все критические данные сохраняются в резервной памяти и проверяются перед использованием на соответствие спецификациям.

Для прикладного программного обеспечения ПЛК также разработаны международные стандарты (IEC 61131). Эти стандарты требуют использования специальных приемов и средств программирования для снижения сложности при реализации алгоритмов. Во время разработки прикладного программного обеспечения используются дополнительные средства тестирования. Для проверки целостности данных при тестировании также используется внесение ошибок в исходные данные. Спроектированное программное обеспечение и проведенное тестирование подробно документируются с тем, чтобы инспекторы могли понять работу системы.

Безусловно, между обычными ПЛК и ПЛК, предназначенными для решения задач безопасности, есть много общего. Например,

- И те, и другие могут опрашивать входы, производить вычисления и выдавать управляющие воздействия,
- И те, и другие имеют модули ввода-вывода, которые позволяют им интерпретировать ситуацию на процессе и воздействовать на исполнительные элементы,
- И те, и другие имеют интерфейсное и сетевое оборудование.

Но существенным является другое:

- Обычные ПЛК изначально не спроектированы как отказоустойчивые и безопасные системы.
- Обычные ПЛК не гарантируют детерминированного поведения системы.

И в этом состоит фундаментальная разница.

Появление международных стандартов безопасности, определяющих особые требования к проектированию, производству и конкретной реализации безопасных ПЛК, связано с всё большим усложнением технологических процессов, и соответствующим увеличением количества и масштабов аварий на производстве. Все, что способно снизить уровень этих требований, рассматривается как проявление легкомыслия и с профессиональной, и с социальной точки зрения, и с позиции коммерческих интересов.

3.2. Структура отказов базовых архитектур систем безопасности

Системы безопасности по своей природе являются пассивными. Поэтому в режиме *on-line* выявить все виды отказов с помощью одной внутрисистемной диагностики невозможно. Опасный отказ может существовать абсолютно необнаруженным до тех пор, пока система неактивна. Система безопасности может отказать одним из двух способов:

Во-первых, она может вызвать или инициировать ложный, немотивированный останов, и остановить производство, в то время как фактически ничего опасного не произошло. Если выходные цепи спроектированы таким образом, что в нормальных рабочих условиях реле находятся под напряже-

нием и контакты замкнуты, то в случае отказа системы защиты электропитание с контактов снимается, и они размыкаются, вызывая останов процесса. Некоторые люди называют подобную ситуацию "безопасным" отказом.

Во-вторых, система защиты может отказать прямо противоположным способом, то есть НЕ выполнить функцию защиты, в то время как это действительно требуется со стороны процесса. Примером подобной ситуации являются реле с залипшими контактами, которые не могут разомкнуться для правильного срабатывания блокировки, либо заклинивший исполнительный механизм отсекателя. Подобные отказы называют опасными отказами.

3.3. Архитектура lool
(рис. 3.1)

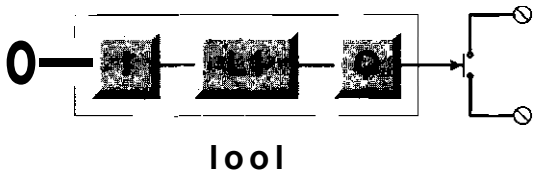


Рис. 3.1

Резервирование отсутствует, поэтому система lool имеет присущую ей проблему общего порядка:

Если какой-либо из единичных элементов в цепи отказывает, то и вся система перестает работать. Питание с реле снимается, вызывая размыкание контактов, и происходит жесткий, программно-неконтролируемый, физический ("безопасный") останов.

Прежде чем рассмотреть разницу между показателями надежности и безопасности одноканальной системы и системами более высокого порядка, введем два определения:

1. Если входной сигнал не подвергается никакому анализу, то любой дребезг контакта приводит к ложному сигналу на срабатывание блокировки. Обозначим вероятность ложного срабатывания для одноканальной системы в течение 1 года как $p_{\$}$:

$$PГ = Ps$$

2. Если выходные контакты залипли, возникает опасный отказ, который можно выявить только после деблокировки и последующего тестирования. Либо, что самое неприятное, после того, как блокировка в нужный момент не сработала.

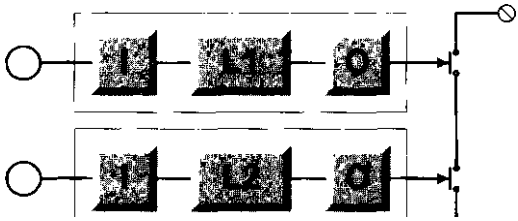
   Обозначим вероятность опасного отказа в течение одного года как p_D:

   $$P\Gamma = Po \bullet$$

Примечание:

Во всех последующих примерах предполагается, что реле под нагрузкой имеют замкнутые контакты.

3.4. Архитектура 1oo2
(рис. **3.2)**



1oo2

Рис. 3.2

Данная конфигурация означает, что **ложный останов** произойдет в том случае, если контакты любого из двух последовательных реле разомкнуться.

Поскольку по сравнению с системой lool данная система имеет удвоенное количество оборудования, **вероятность ложного срабатывания удваивается,** и составляет

$$PT^2 = 2 \quad p_s$$

Опасный отказ произойдет только в том случае, если оба канала откажут одноврёменно. Для независимых событий вероятность отказа обоих каналов одноврёменно будет определяться как квадрат вероятности опасного отказа одноканальной системы:

$$pГ = P^2o$$

Поскольку данная вероятность довольно мала, система 1oo2 обладает высокой степенью безопасности.

Однако частота ложных срабатываний по сравнению с одноканальной системой удваивается.

3.5. Архитектура 2oo2

(рис. 3.3)

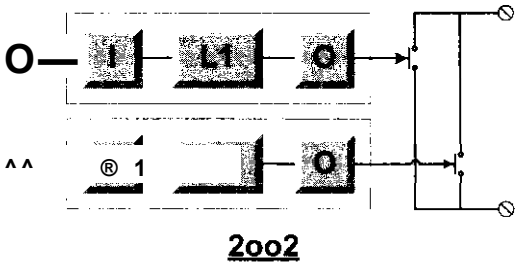


Рис. 3.3

Система 2oo2 имеет два набора контактов, установленных параллельно. Для того чтобы произошел **ложный останов,** оба канала должны осуществить ложный останов одноврёменно. Поэтому для независимых событий вероятность одновременного ложного срабатывания обоих каналов определяется произведением вероятностей:

$$P_S^{002} = P_S' P_S = P^2 S$$

Эта вероятность чрезвычайно мала, но вероятность несрабатывания оказывается очень высокой:

Для **опасного отказа** достаточно, чтобы отказал один из двух каналов. И поскольку данная система имеет удвоенное количество оборудования, то **вероятность опасного отказа (несрабатывания) удваивается:**

$$pГ^2 = 2_{P\,o}$$

Таким образом, как это ни парадоксально, но система 2oo2 уступает по безопасности одноканальной системе 1oo1 в два раза.

3.6. Архитектура 2оо3
(рис. 3.4)

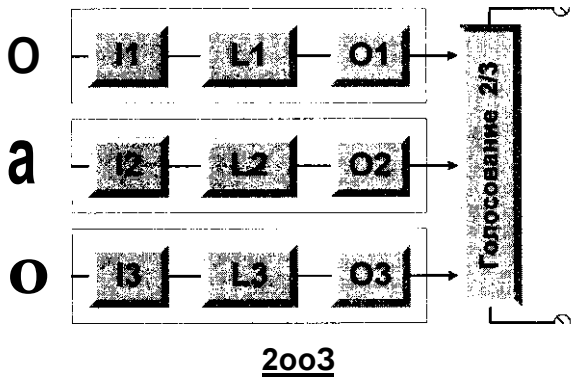


Рис. 3.4

Система со специфической архитектурой на базе трех попарно *"голосующих" в* порядке 1-2, 1-3, 2-3 элементов. Система считается работоспособной, если результаты работы любых двух элементов совпадают. В чистом виде (без общих отказов - Common Cause Failures, IEC 61508) вероятность всех типов отказа архитектуры 2оо3 в ТРИ РАЗА ВЫШЕ, чем для системы 1оо2. Это обстоятельство объясняется довольно просто:

Без учета перестановок существует только одно сочетание для отказа системы 1оо2 - это комбинация (1-2).
Для системы 2оо3 таких сочетаний три:

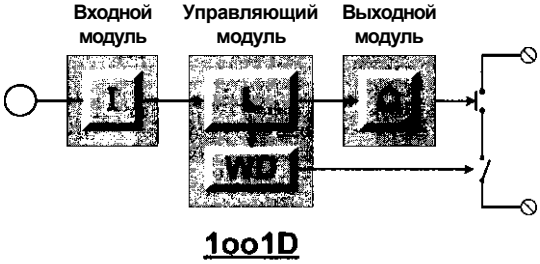
(1-2), (1-3), (2-3)

С учетом перестановок оба набора сочетаний синхронно удваиваются, соответственно удваивается и частота отказов, сохраняя общее соотношение вероятностей отказа

P1oo2/P2003=1/3

Расчеты показывают, что и в целом, то есть с учетом *плия ни я* отказов общего *порядка конфигурация* 2оо3 *имеет* меньшую надежность в сравнении с архитектурой 1оо2D (см. IKC 61508, Part 6).

3.7. **Основные архитектуры промышленных систем безопасности. Архитектура 1oo1D**
(рис. 3.5, рис. 3.6)



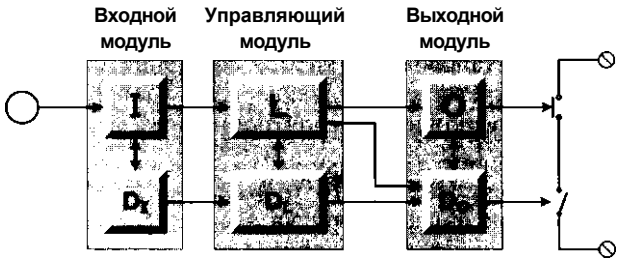
1oo1D

Рис. 3.5

В простейшем варианте в эту архитектуру добавляется дополнительный электронный ключ, управляемый диагностической цепью.

В качестве средства диагностики выступает обычный сторожевой таймер *(Watchdog).* В том случае, когда диагностика обнаруживает опасный отказ, ключ может снять питание с выхода, преобразуя опасный отказ в почти "безопасный". Суффикс "D" в данном случае отражает расширенные возможности самодиагностики, внесенные в канал.

В стандартной конфигурации данная архитектура имеет дополнительные диагностические цепи и на модулях ввода-вывода:



1oo1P

Рис. 3.6

3.8. Архитектура 1oo1D - расширенный вариант (рис. 3.7, рис. 3.8)

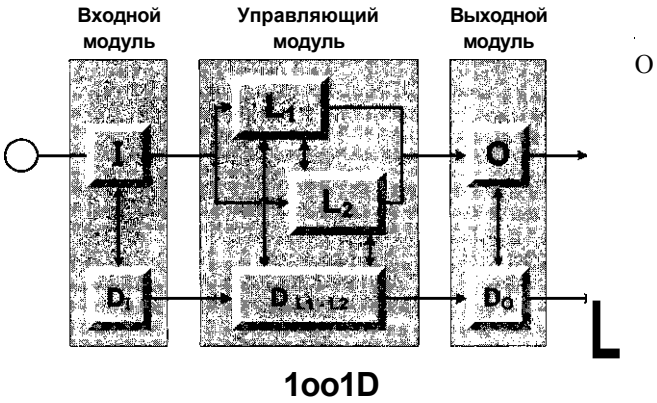


Рис. *3.7*

Стандартная архитектура 1oo1D дополняется вводом еще одного процессора в основной канал системы. Расширенный вариант конфигурации 1oo1D предоставляет недорогую возможность увеличения уровня самодиагностики.

Тонкость состоит в том, что это - воистину одноканальиая система, поскольку оба процессора находятся на одном модуле, и восстановлению в режиме *on-line* по отдельности не подлежат.

Степень диагностического охвата по сравнению с предыдущим вариантом (рис. 3.6) увеличивается, однако после обнаружения отказа одного из процессоров не остается ничего другого, как снять питание с выходных реле, и совершить незапланированный останов.

Существует более продуманный и гибкий вариант одноканальной системы, когда центральные процессоры и диагноегические цепи полностью дублируются, и размещаются на отдельных управляющих модулях (рис. 3.8).

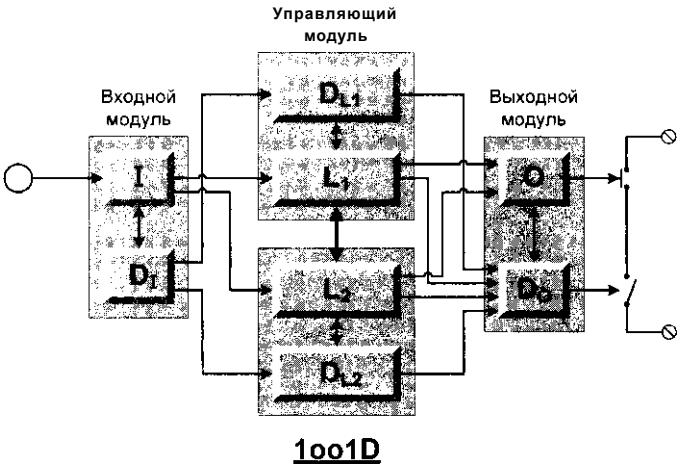


Рис. 3.8

Примечание

Это может быть, например, один из вариантов архитектуры системы противоаварийной защиты Quadlog, который использует фирма Siemens Energy & Automation.

В отличие от "чисто" одноканальной системы, данный расширенный вариант потенциально позволяет произвести замену отказавшего модуля управления в режиме *on-line,* либо провести программно-управляемый останов.

Но поскольку входная и выходная цепи не резервированы, система по определению относится к классу 1oo1D.

Таким образом, все без исключения модификации систем с архитектурой 1oo1D, включая и последнюю, аттестуются по классу RC4 и уровню SIL2.

3.9. Архитектура looID - "горячее" резервирование (рис. 3.9)

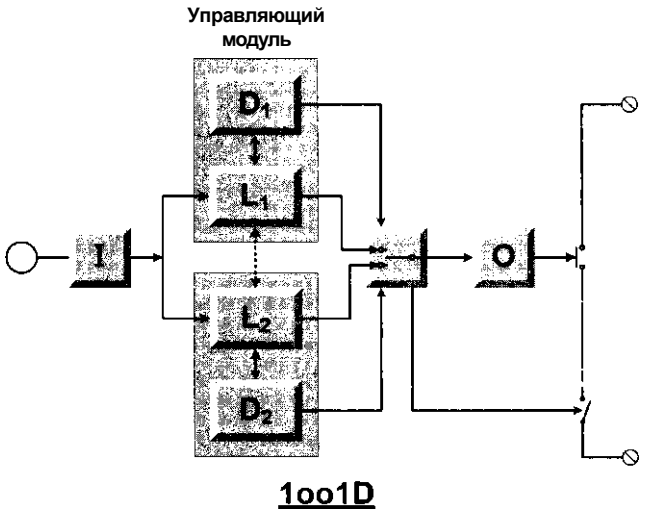


Рис. 3.9

В эту архитектуру добавлен дополнительный электронный ключ, управляемый диагностическими цепями управляющих модулей.

В качестве средства диагностики каждого канала выступает обычный сторожевой таймер. Ключ периодически переключается в соседнее положение - так подтверждается функциональность резервного канала.

Дополнительно может использоваться сравнение процессоров. Если на момент переключения резервный канал оказывается неработоспособен, то и вся система считается неспособной к выполнению функций защиты.

В случае какого-либо отклонения от штатной работы питание с выходных цепей снимается, и происходит незапланированный останов процесса.

Все без исключения модификации систем с архитектурой looID включая и последнюю, аттестуются по RC4 и S1L2.

3.10. Архитектура 2oo2 (рис. 3.10, рис. 3.11)

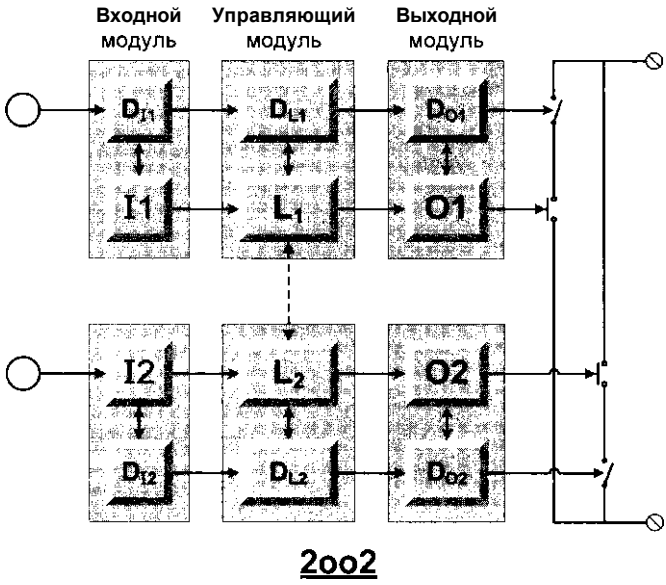


Рис. 3.10

Следует обратить внимание на то обстоятельство, что наличие диагностических цепей и межпроцессорного взаимодействия не превращает архитектуру 2oo2 в архитектуру 2oo2D, поскольку данное обстоятельство только повышает уровень самодиагностики, но никак не меняет принцип действия системы. Именно по этой причине архитектуру 1oo1D часто не выделяют особо из семейства 1oo1, и если это не вызывает недоразумений, помечают просто как систему 1oo1. Вот что просто, доходчиво, русским языком по-английски говорит об архитектуре 2oo2 стандарт IEC 61508 (Part 6, Annex B, пункт B.2.2.3, стр. 55):

"This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that ***any diagnostic testing*** *would only report the faults found and would not change any output states or change the output voting*

"Эта архитектура состоит из двух каналов, соединенных параллельно, так что оба канала должны выполнить функцию безопасности, чтобы она смогла иметь место. Предполагается, что ***любое диагностическое тестирование*** *будет только извещать об обнаруженных сбоях и не будет изменять состояния выходов или изменять выходное голосование*

Чтобы произвести **аварийный останов,** оба канала должны дать команду на аварийный останов. Для того чтобы произошел **ложный останов,** оба канала должны осуществить ложный останов одновременно. Чтобы произошел **опасный отказ** - несрабатывание в нужный момент, - достаточно, чтобы отказал любой из каналов.

С оответственно, **вероятность опасного отказа системы 2oo2 н два раза выше, чем у системы 1oo1.**

По этой причине в чистом виде системы 2oo2 для защиты технологических объектов не применяются. Однако, как мы увидим далее при рассмотрении архитектуры 1oo2D, резкое снижение вероятности ложных остановов архитектуры 2oo2 использовано в архитектуре 1oo2D остроумным сочетанием преимуществ систем 1oo2 и 2oo2.

Все системы с архитектурой 2oo2 аттестуются по классу RC4 и уровню SIL2.

Важно понимать, что количество процессоров на одном управляющем модуле никак не может изменить архитектуру системы. В представленной ниже схеме (рис. 3.11) на каждом управляющем модуле PE A и PE B размещено по два процессора, - PSU A1 и PSU A2, PSU B1 и PSU B2. Кроме того, добавлены диагностические цепи и межпроцессорное взаимодействие, однако архитектура системы остается неизменной - 2oo2.

Источник информации рис. 3.11:

"Comparison of Programmable Electronic Safety-Related System Architectures10 January, 2003. Anton A. Frederickson, Dr. Independent Consultant, Member of Safety Users Group Network. Авторская графика намеренно сохранена в неприкосновенности.

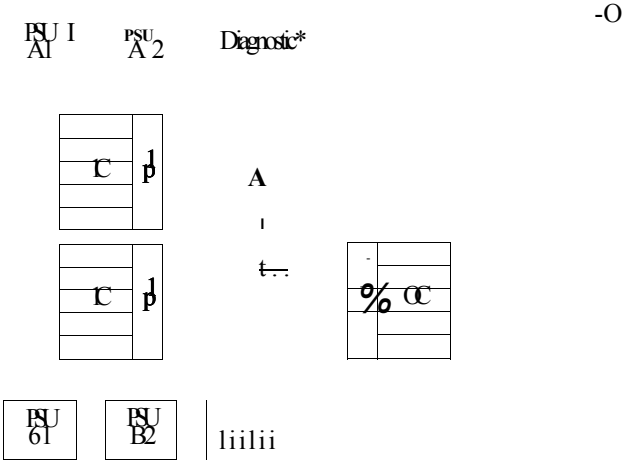


FIGURE 4-4 Dual PE with Dual I/O, External Watchdogs, Interprocessor Communication and lool Shutdown Logic

Рис. 3.11

3.11. Архитектура 1oo2

Важно понимать разницу между системами 1oo2 и loo2D.

Чтобы сразу внести определенность, приведем схему системы 1oo2 (рис. 3.12), которая часто помечается как система с архитектурой loo2D, однако таковой не является.

В очередной раз необходимо обратить внимание, что, несмотря на то, что в представленной на рис. 3.12 схеме на каждом управляющем модуле PE A и PE B размещено по два процессора - PSU A1 и PSU A2, PSU B1 и PSU B2, и, кроме того, добавлены диагностические цепи и межпроцессорное взаимодействие, -

Архитектура системы остается неизменной - 1oo2.

Примечание

Некоторые вообще умудряются отнести эту систему к архитектуре 2oo4, и даже более того -к ни кому не ведомой архитектуре 2oo4D.

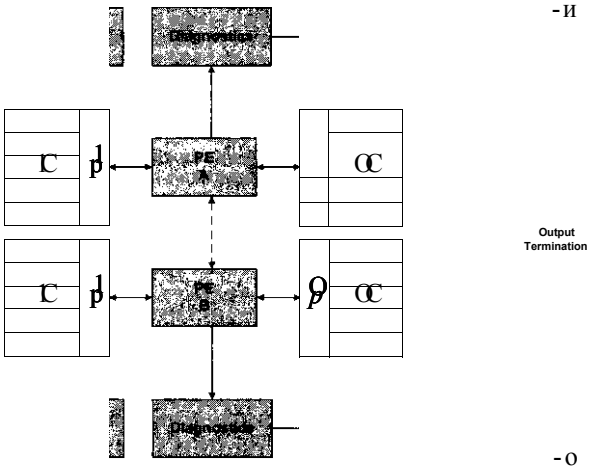


FIGURE 4-3 Dual PE with Dual I/O, Interprocessor Communication and 1oo2 Shutdown Logic

Рис. 3.12

Источник информации рис. 3А2:
"Comparison of Programmable Electronic Safety-Related System Architectures", 10 January, 2003. Anton A. Frederickson, Dr. Independent Consultant, Member of Safety Users Group Network.

Несмотря на то, что система имеет по два процессора и сторожевой таймер на каждом из двух управляющих модулей, а также может осуществлять межпроцессорное взаимодействие, тем не менее, эта схема классифицируется как система с архитектурой 1oo2.

Вот что простым и доходчивым русским языком, по-английски говорит об архитектуре 1oo2 стандарт IEC 61508 (Part 6, Annex B, пункт B.2.2.2, стр. 53):

"This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand. It is assumed that ***any diagnostic testing*** *would only report the faults found and would not change any output states or change the output voting*

И означает это буквально следующее:

"Архитектура состоит из двух каналов, соединенных параллельно, так что любой из каналов может обработать

функцию безопасности. Таким образом, должен произойти опасный отказ в обоих каналах, чтобы система не смогла осуществить функцию защиты. Предполагается, чшо ***любое диагностическое тестирование*** *будет только извещать об обнаруженных сбоях, и не будет изменять состояния выходов, или изменять выходное голосование*

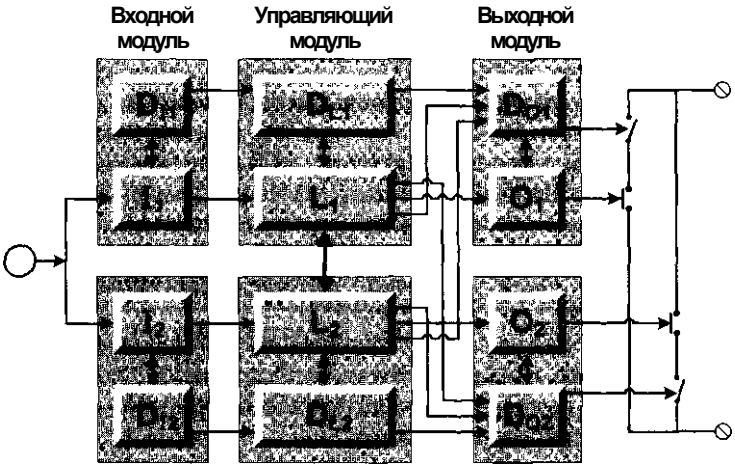
Таким образом, ни количество процессоров на одном управляющем модуле, ни наличие диагностических цепей, ни межпроцессорное взаимодействие НЕ ЯВЛЯЕТСЯ отличительным признаком системы loo2D, и не переводит автоматически систему 1oo2 в систему loo2D:
В случае отказа любого из каналов питание с выходных реле снимается, и процесс останавливается.
Поэтому все без исключения модификации систем с архитектурой 1oo2 аттестуются по RC4 и SIL2.

Наша цель состоит в том, чтобы построить такую архитектуру, которая позволяла бы блокировать ошибочные действия соседнего канала, и давала бы возможность производить восстановление исходной конфигурации системы в реальном времени. Для превращения архитектуры 1oo2 в архитектуру loo2D должна измениться логика управления выходом системы. Для архитектуры loo2D в случае отказа одного из каналов должен быть выбор:

1. Осуществить восстановление системы в течение предопределенного интервала времени, или
2. Произвести программно-управляемый останов.

В конце концов, было найдено решение, которое позволяет сочетать устойчивость архитектуры 2oo2 по отношению к ложным остановам, и устойчивость архитектуры 1oo2 по отношению к опасным отказам (несрабатыванию в нужный момент). Решение проблемы состоит в той специфической организации взаимодействия управляющих, входных, выходных модулей, и, главное, диагностических цепей обоих каналов, которая получила название **четырехполюсной архитектуры loo2D.** Несколько позже будет представлена система с архитектурой 2oo3, для которой в случае отказа одного из трех управляющих модулей также существует возможность восстановления в реальном времени.
А теперь - loo2D.

3.12. Архитектура 1oo2D - Классический вариант (рис. 3.13)



1 o o 2 P

Рис. 3.13

Данная архитектура построена на остроумном сочетании преимуществ систем 1oo2 и 2oo2. Система состоит из двух самостоятельных наборов оборудования (каналов). Каждый из каналов содержит:

- Входные модули
- Логическое устройство - управляющий модуль
- Выходные модули
- Диагностические цепи на каждом модуле.

Вот что говорит стандарт IEC 61508-6 об архитектуре 1oo2D (Annex B, пункт B.2.2.4, стр. 57):

"This architecture consists of two channels connected in parallel During normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel

If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel".
Итак:

"Эта архитектура состоит из двух каналов, соединенных параллельно. Во время нормальной работы необходимо, чтобы оба канала выдали команду на выполнение функции безопасности, чтобы она смогла осуществиться. Кроме того, если диагностическое тестирование обнаруживает сбой в любом из каналов, процедура голосования строится таким образом, что общее состояние выхода будет определяться другим каналом.

Если диагностическое тестирование обнаруживает сбои в обоих каналах, или обнаруживает расхождение, которое не может быть приписано к какому-либо из каналов, то выход системы переводится в состояние останова ("безопасное" состояние). Для того чтобы расхождение между каналами могло быть обнаружено, каждый из каналов должен иметь возможность определять состояние другого канала с помощью средств, независимых от проверяемого канала".

Однако в стандарте не поясняется:

Что же это за средства, независимые от другого канала?

В данном случае - это не просто "возможность определять состояние другого канала", а оригинальное сочетание архитектур **2oo2** и **1oo2,** позволяющее использовать диагностические цепи в качестве дополнительной пары каналов, построенных на альтернативных элементах и совершенно иных схемных решениях. Оба диагностических канала работают таким образом, что без перекрестного подтверждения соседний канал не сможет выдать команду на изменение выхода.

Поэтому символ "D" в архитектуре loo2D означает не просто расширенные возможности диагностики, а особым образом организованное взаимодействие управляющих и диагностических цепей, позволяющее фактически реализовать реальную квадро - систему, имея:

- **Два канала обработки информации, и**
- **Два диагностических канала.**

3.13. Логика работы системы loo2D

В норме для минимизации ложных срабатываний система работает по схеме **2oo2.** Если диагностика обнаруживает отказ, то отключает выходную цепь данного канала, и система продолжает работу по схеме **loolD.** Система остается работоспособной, поскольку второй канал поддерживает общую нагрузку на выходе.

Каждый канал имеет сторожевой таймер, который служит вторичным средством отключения выходов. В данной архитектуре используется межпроцессорное взаимодействие каналов для сравнения входных данных, результатов вычислений, и выходных данных.

Все системы с архитектурой loo2D аттестуются по классу RC6 и уровню SIL3.

Из всех рассмотренных до сих пор систем только системы с архитектурой loo2D имеют законное право на восстановление в режиме *on-line.* Однако необходимо помнить, что для соответствия всего контура защиты требуемому классу необходимо учитывать не только категорию PLC, но и надежность, и степень резервирования, и уровень диагностики полевого оборудования.

Системы loo2D предоставляют исключительно высокий уровень диагностики. Это фактически означает, что в применении дублированных процессоров на модулях управления непосредственной необходимости нет.

Тем не менее, системы с дублированными процессорами на каждом управляющем модуле существуют (см. рис. 3.14).

Источник информации - тот же:

"Comparison of Programmable Electronic Safety-Related System Architectures", 10 January, 2003. Anton A. Frederickson, Dr. Independent Consultant, Member of Safety Users Group Network. Авторская графика намеренно сохранена в неприкосновенности.

3.14. **Важный** пример архитектуры **loo2D** (рис. 3.14)

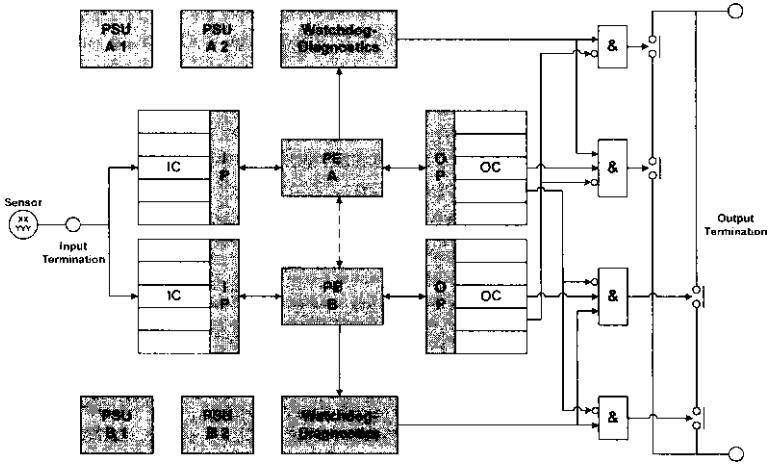


FIGURE 4-5 Dual PE with Dual I/O, External Watchdogs, Interprocessor Communication and 1oo2D Shutdown Logic

Рис. 3.14

В очередной раз необходимо обратить внимание на то обстоятельство, что наличие двух процессоров на одном управляющем модуле не меняет архитектуру системы.

Но вокруг систем с удвоенным количеством процессоров на каждом управляющем модуле образовано такое количество недоразумений и мистификаций, что необходимо подробно представить и логику работы, и место данной архитектуры в общем ряду систем безопасности.

Главное недоразумение, которое связано с системами этого рода, и на котором необходимо остановиться, заключается в следующем:

Архитектуру loo2D с дублированными процессорами на модулях управления некоторые энтузиасты этих систем смело определяют как архитектуру 2oo4, и даже 2oo4D.

3.15. Архитектура loo2D - модификация 2*2 ("2oo4")

Так же, как и для архитектур looID, 2oo2 и 1oo2, существуют модификации архитектур loo2D с дублированными процессорами в каждом управляющем модуле (рис. 3.15).

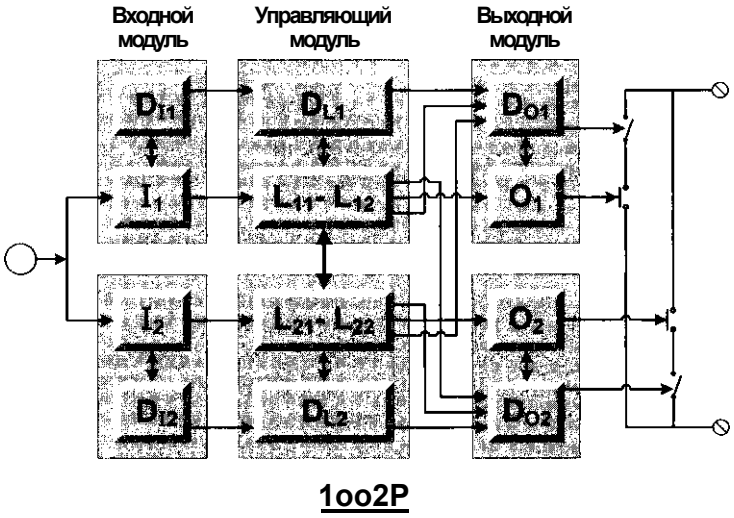


Рис. 3.15

Центральная часть системы построена по принципу 2*2, то есть каждый из двух управляющих модулей содержит по 2 микропроцессора. В случае расхождения в работе какой-либо пары микропроцессоров, данный канал выключается из работы, и система продолжает работу по одноканальной схеме looID.

Исходная конфигурация системы может быть восстановлена в течение предопределенного интервала в реальном времени. Если по каким-либо причинам замена дефектного модуля не может быть произведена, то в течение предопределенного интервала времени система имеет возможность произвести программно-управляемый останов процесса.

Архитектуру loo2D с дублированными процессорами на модулях управления некоторые энтузиасты этих систем смело определяют как архитектуру 2oo4, и даже 2oo4D.

Замечание 1

Подобные рассуждения затрагивают только центральную часть системы - модули управления. Степень резервирования модулей ввода-вывода и полевого оборудования обычно даже не упоминается. А если и упоминается, то и шины ввода-вывода, и входные и выходные модули сами авторы концепции 2oo4 определяют все же как схемы с архитектурой 1oo2.

*Внимательно посмотрим на схему рис.3.15. На самом деле центральная часть этой системы работает по принципу 2*2жаждая пара процессоров находится на одном модуле, и на выходы системы воздействует модуль, а не индивидуальный процессор.*

Необходимо помнить, что по определению, под каналом понимается элемент, или группа элементов, способных самостоятельно выполнять предопределенную функцию.

Поэтому даже если бы центральная часть этой системы действительно реализовала архитектуру 2oo4 (для чего требуется разместить процессоры на четырех модулях управления), общеизвестно, что итоговая конфигурация определяется наиболее слабым звеном, в том числе и в архитектурном отношении, и даже в этом случае система определялась бы как система 1oo2.

Замечание 2

Четверка в коде архитектуры подразумевает существование не только схемы 2oo4, но и схем 3oo4, и 1oo4, но об этом благоразумно не упоминается, поскольку архитектура "2oo4" по схемам деградации 3oo4 и 1oo4 работать не может.

Замечание 3

Работа центральной части системы "2oo4" в случае отказа одного из процессоров эквивалентна работе на одном канале по схеме loolD, и в этом смысле полностью эквивалентна логике работы системы loo2D при отказе одного из процессоров.

*Сравнивая структуру отказов архитектур 2*2 ("2oo4"), 2oo3 и loo2D, мы видим, что стандартно все они имеют одинаковые схемы деградации:*

- *4-2-0 (останов процесса после второго обнаруженного отказа);*

- *3-2-0 (останов процесса после второго обнаруженного отказа);*
- *2-1-0 (останов процесса после второго обнаруженного отказа).*

Причем все три представленные архитектуры могут находиться в составе одной функции безопасности - едином контуре защиты:

- *Архитектура 2оо3 - в конфигурации датчиков,*
- *Архитектура 1оо2 - в конфигурации модулей ввода-вывода и исполнительных механизмов,*
- *Архитектура loo2D ("2оо4 ") - в конфигурации управляющих модулей.*

Приведенные соображения не дают повода для сомнений: **Очевидно, что в конфигурации 2*2 реализована схема loo2D.**

Пара микропроцессоров используется только для самодиагностики модуля управления, и только пара синхронно работающих микропроцессоров модуля управления формирует работоспособный канал. Каждый из каналов работает по схеме **loolD:**

Канал отключается после первой же обнаруженной ошибки, и управление выходом системы полностью переходит к оставшемуся в работе каналу.

Поэтому необходимо интерпретировать данную схему как двухканальную схему loo2D, понимая под кодом D специфический способ взаимной диагностики каналов и управления выходом системы.

Системы **loo2D** по определению имеют лучшую архитектуру из всех существующих, и не нуждаются ни в каких дополнительных рекламных трюках:

Все модификации архитектуры loo2D аттестуются по классу RC6 и уровню SIL3.

3.16. Внимание к деталям

Даже у самых известных исследователей и специалистов по промышленной безопасности случаются нелепые ошибки и совершенно курьезные случаи при определении типа архитектуры. В своей в целом содержательной статье

"How Diagnostic Coverage Improves Safety in Programmable Electronic Systems", ISA Transactions, Vol 36, No. 4, The Netherlands: Amsterdam, Elsevier Science B. V. 1998.
William M. Goble, Eindhoven University of Technology, Eindhoven, the Netherlands.
Julia V. Bukowski, Department of Electrical and Computer Engineering Villanova University, Villanova, PA.
Prof. Dr. Ir. A. C. Brombacher, Faculty of Mechanical Engineering Eindhoven University of Technology, Eindhoven, the Netherlands,

под сопроводительным текстом:
"Когда оба набора электроники компонуются вместе, создается ***четырехканальная*** *архитектура loo2D (Figure 4)",*
эти крупнейшие западные специалисты приводят следующую схему:

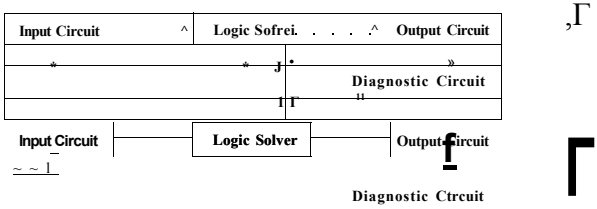


Figure 4.1oo2D Architecture with Interprocessor Communication.

Рис. 3.16

Удивительно, что авторы такого ранга допускают такие ошибки, но вопреки подписи, на данной схеме представлена вовсе не архитектура loo2D, да к тому же еще и **"четырехканальная",** и даже не архитектура 1oo2, а архитектура 2oo2!
(сравните с рис. 3.10 и рис. 3.11).

3Л7. Классические архитектуры 2oo3

TMR - *Triple Modular Redundancy* - системы со специфической архитектурой на базе трех "голосующих" в порядке A-B, A-C, B-C процессоров. Как сказано в стандарте IEC 61508 (Part 6, Annex B, пункт B.2.2.5, стр. 59):

"This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only one channel gives a different result which disagrees with the other two channels. It is assumed that ***any diagnostic testing would only report the faults found*** *and would not change any output states or change the output voting". -*

"Эта архитектура состоит из трех каналов, соединенных параллельно, с голосованием по принципу большинства таким образом, что состояние выхода не меняется, если только один канал дает результат, отличный от двух других каналов. Предполагается, что ***любое диагностическое тестирование будет только извещать об обнаруженных сбоях,*** *и не будет изменять состояния выходов, или изменять выходное голосование*

Коротко и ясно. Но следует обратить внимание на последнюю сентенцию. Мы с ней уже встречались, когда приводили цитаты стандарта IEC 61508 для систем с архитектурами 2002 и 1oo2, также не имеющих признака диагностики D.

В отличие от архитектур 1oo2, 2oo2 и 2oo3, системы loo2D имеют принципиально иную логику взаимодействия диагностических и управляющих цепей, чем простое сравнение состояния процессоров. И даже оказавшись в одиночестве, одиночный канал системы loo2D имеет право контролировать общий выход системы в течение предопределенного интервала времени.

Как мы уже подробно исследовали в главе *"Постановка задач автоматизации*двухканальная работа архитектуры 2003 полностью эквивалентна одноканальной работе архитектуры loo2D по схеме loolD.

Поэтому одноканальная работа голосующей архитектуры 2oo3 по схеме 1oo1 на взрывоопасных производствах невозможна - результат непредсказуем, ведь системе 1oo1 просто не с кем и не за кого голосовать.

Примеры классических систем типа 2оо3 - Tricon фирмы Triconex (Invensys), и August (Triguard) фирмы ABB. Архитектура этих систем представлена на рис. 3.17. Расчеты показывают, что в целом эта конфигурация даже с учетом влияния отказов общего порядка имеет меньшую надежность в сравнении с конфигурацией loo2D. А без учета влияния общих отказов **вероятность всех типов отказа архитектуры 2оо3 в ТРИ РАЗА ВЫШЕ, чем архитектуры loo2D** (см. IEC 61508, Part 6, Annex B, Tables B.2-B.5, B1 O-B. 13).

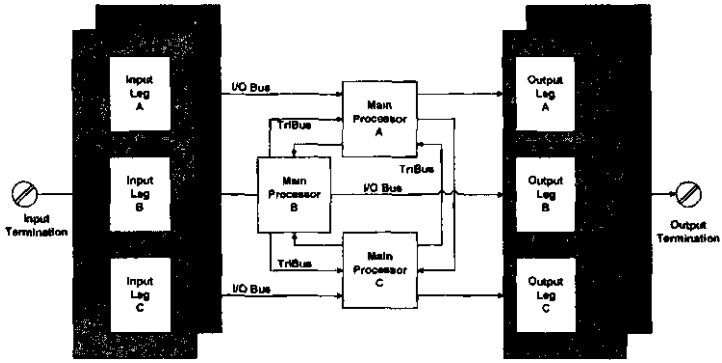


Рис. 5.77

Причем необходимо обратить самое пристальное внимание на то, что эти **расчеты МЭК относятся только к центральной части** системы, изображенной на рис. 3.17, действительно имеющей тройное модульное резервирование. Для модулей ввода-вывода ситуация серьезней - все три сегмента (Legs A, B, C) находятся на ОДНОЙ плате. Более того, все модули ввода-вывода используют мультиплексирование по 8, 16, 32 и даже 64 точкам ввода-вывода.

Существуют модификации систем с архитектурой 2оо3, которые имеют по 2 микропроцессора на каждом модуле управления, например, системы Tricon и Trident. Если в выражение вероятности отказа архитектуры 2оо3 $P_{2oo3} = (Л\ if$ подставить удвоенную частоту отказа канала, то вероятность отказа архитектуры 2оо3 ("4оо6") составит:

$P_{4oo6}'A(2Л)\quad t¥ = 4.(A\quad t)^2 = 4\text{-}P_{2oo3y}$

то есть возрастет в четыре раза.

Таким образом, главное соотношение вероятностей отказа дублированных и троированных архитектур сохраняется и при удвоении числа элементов в канале:

$PFDi. \quad 'PFD_{2OO3}=PFD_{\cdot 2OO4}.:PFD_{\cdot 4OO1R} \quad = 1:3$

Соотношение вероятностей отказа архитектур 1оо2 и 2оо3, "2оо4" и "4оо6" **при прочих равных условиях** составляет

$(PFD_{1OO2} : PFD_{2OO3}): (PFD_{\cdot 2}$

$(1:3):(12^2 \quad :3\text{-}2^*)=>(1:3):(4:12)$

То есть вероятность отказа трех центральных модулей управления архитектуры 2оо3 ("4оо6") с парой процессоров в каждом модуле на порядок выше, чем для классической архитектуры 1оо2.

Представленная на рис. 3.17 архитектура - далеко не единственно возможная для систем 2оо3. Существуют системы с полным физическим разделением на три самостоятельные подсистемы с утроенным набором управляющих модулей и модулей ввода-вывода (например, система GMR фирмы General Electric Fanuc, - см. рис 3.18). Системы этого типа состоят из:

- *Трех самостоятельных PLC, выполняющих одну и ту же логическую программу,*
- *Выносных или удаленных блоков ввода-вывода, и*
- *Тройной шины обмена данными между выносными блоками и PLC, и PLC между собой.*

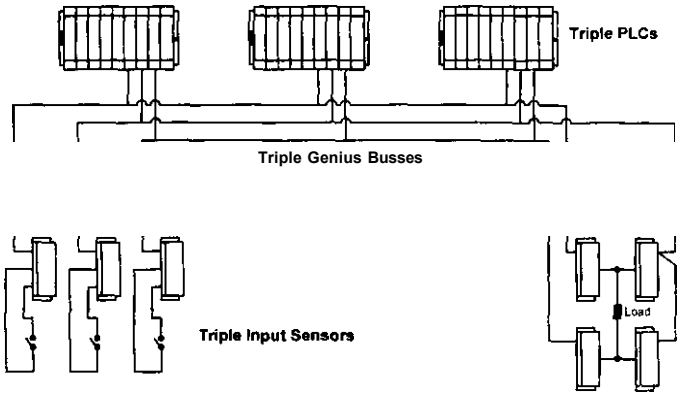


Рис. 3.18

Как видно из рисунка 3.18, архитектура 2oo3 может использоваться и для резервирования датчиков, определяющих взрывоопасность процесса, и, как правило, на альтернативной основе.

Большие системы защиты могут потребовать большее количество подсистем ввода-вывода. Например, система, представленная ниже (рис. 3.19), имеет две подсистемы ввода-вывода для шести независимых шин данных и восемнадцати контроллеров.

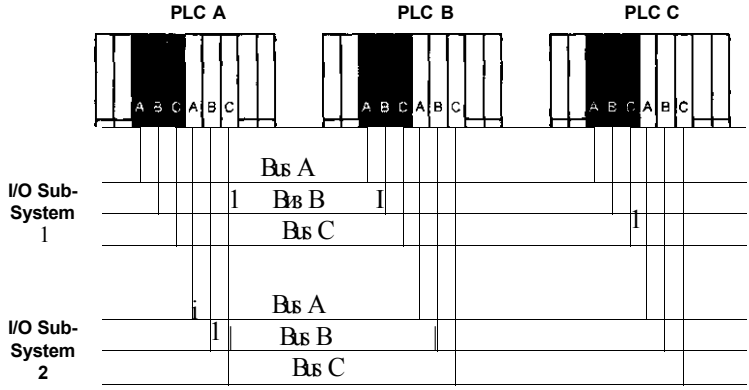


Рис. 3.19

- *Можно только догадываться, сколько это решение может стоить.*

В нескольких следующих разделах приводится краткое, и по возможности максимально формальное описание ярких представителей контроллеров для систем безопасности, имеющих базовые архитектуры 1oo1D и 1oo2D:

- Системы Quadlog фирмы Siemens Energy & Automation.
- Семейство контроллеров фирмы HIMA.
- Система QMR FSC фирмы Honeywell.
- Контроллеры семейства Pro Safe фирмы Yokogawa Electric.

3.18. Системы семейства QUADLOG (Siemens Energy&Automation)

Система критического управления и обеспечения безопасности технологических процессов QUADLOG предназначена для создания приложений, предъявляющих особенно высокие требования к надёжности, отказоустойчивости и безопасности: системы противоаварийной защиты (ПАЗ), системы пожаро - и газобезопасности, системы управления критическими процессами.

Система QUADLOG может быть непосредственно интегрирована с распределённой системой управления технологическим процессом в составе АСУТП.

В отличие от обычных контроллеров и систем управления, в архитектуру QUADLOG на всех уровнях встроены аппаратные и программные механизмы, обеспечивающие безопасность, надёжность и отказоустойчивость, которые необходимы в самых ответственных приложениях.

Система QUADLOG неоднократно проходила независимую международную сертификацию, подтвердившую её наивысший для программируемых электронных систем управления уровень безопасности. Аппаратура QUADLOG предназначена для многолетней безаварийной эксплуатации и эффективного решения критических задач управления и защиты в самых жёстких производственных условиях.

Технологическая эффективность QUADLOG получила широкое признание на промышленных предприятиях во всём мире. Технические возможности QUADLOG подтверждены всеми ведущими международными и многими национальными сертификационными органами:

- Сертификат TUV для систем обеспечения безопасности уровня АК 6.
- Сертификат IEC 61508 для систем обеспечения интегрального уровня безопасности SIL3.
- Сертификат соответствия стандартам и требованиям СС.
- Аттестат FM для использования во взрывоопасных зонах класса I, раздел 2.
- Аттестат CSA для использования во взрывоопасных зонах класса I, раздел 2.

- Сертификат ABS.
- Сертификат UL 508.
- Сертификат Госстандарта России на средство измерения.
- Разрешение на применение Ростехнадзора России.
- Сертификат пожарной безопасности Государственной Противопожарной Службы МВД России.

Данные сертификаты подтверждают соответствие системы QUADLOG жестким промышленным стандартам и требованиям различных отраслей промышленности.

3.19. Архитектура QUADLOG looID - RC4, SIL2 (рис. 3.20)

Системная архитектура QUADLOG looID аттестована на соответствие уровню безопасности SIL2 в соответствии со стандартом IEC 61508, а также классу требований RC4 по DIN. Этот вариант архитектуры соответствует наиболее простой структуре системы. Высокие показатели безопасности обеспечиваются всесторонней независимой системой диагностики, которая позволяет переводить объект в безопасное состояние в случае выхода из строя основных элементов системы. В данной архитектуре предусмотрены дублированные схемы управляющих модулей, защита выходных цепей и другие механизмы, обеспечивающие существенно более безопасные решения, чем традиционная архитектура программируемых логических контроллеров и систем управления. В выходных каналах QUADLOG используются дублирующие разнотипные элементы. Нормальный выход основного управляющего канала контроллера построен на твердотельном полупроводниковом ключе. Выходное электромагнитное реле, управляемое встроенной системой диагностики, предоставляет дополнительную возможность управления состоянием выхода. При обнаружении опасного отказа в выходном канале реле может быть автоматически обесточено, что обеспечивает безопасное отключение системы. Высокая отказоустойчивость архитектуры QUADLOG looID достигается также благодаря резервированию таких ключевых элементов системы, как источники питания и коммуникационные магистрали.

Для дополнительного повышения отказоустойчивости в рамках данной архитектуры в системе могут быть установлены резервированные управляющие модули (см. рис. 3.20, средняя схема).

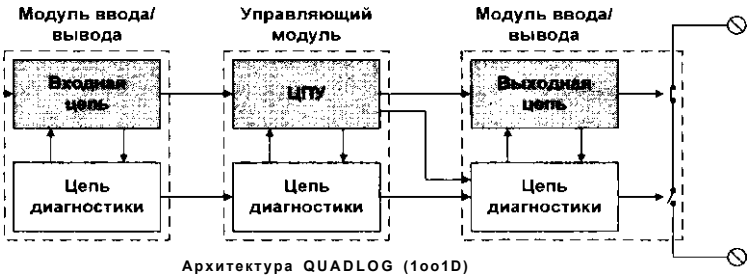
3.20. Архитектура QUADLOG loo2D - RC6, SIL3 (рис. 3.20)

Архитектура QUADLOG loo2D аттестована на соответствие уровням безопасности SIL3 и RC6. Она обеспечивает высочайший уровень безопасности и отказоустойчивости.

Архитектура loo2D включает все основные возможности архитектуры looID. Высокий уровень безопасности и отказоустойчивости в архитектуре loo2D достигается за счёт дублирования всех модулей - и управляющих, и ввода-вывода. Система loo2D - полностью резервированная архитектура с всесторонней диагностикой и дополнительным трактом безопасного отключения системы, который управляется независимым диагностическим каналом каждого модуля. Далеко не самоочевидное обстоятельство, но в системах QUADLOG с архитектурой loo2D параллельно работают четыре канала - два основных и два диагностических, благодаря чему достигается наивысший для программируемых электронных систем уровень безопасности и отказоустойчивости.

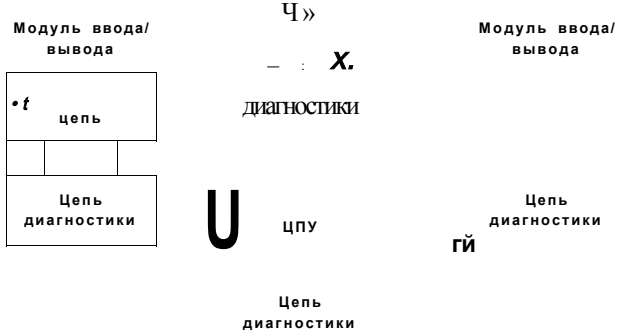
Вся система разделена на две эквивалентные подсистемы, резервирующие друг друга. В том случае, когда система диагностики обнаруживает неисправность в одной из подсистем, эта подсистема отключается, и контроль и управление поддерживается другой подсистемой.

После того, как работоспособность неисправной подсистемы будет восстановлена, она включается в работу, полностью восстанавливая двойную схему резервирования архитектуры loo2D. Данная архитектура также отличается большой общей стабильностью и устойчивостью к внешним неблагоприятным воздействиям общего характера.

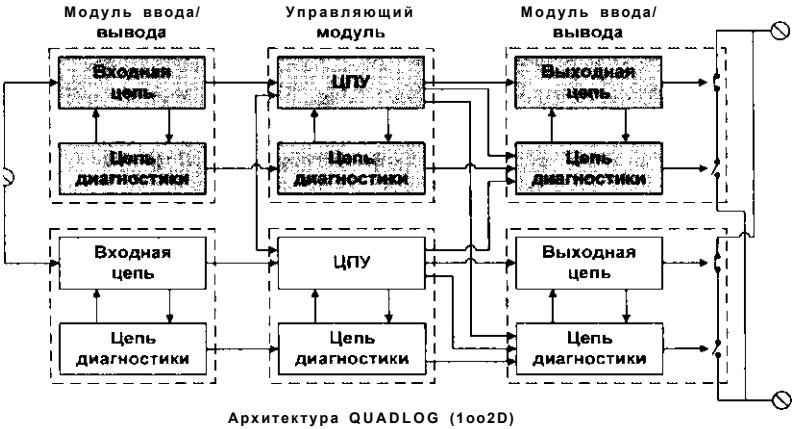


Архитектура QUADLOG (1oo1D)

Управляющий модуль



Архитектура QUADLOG (1oo1D) с резервированием управляющего модуля



Архитектура QUADLOG (1oo2D)

Рис. 3.20

Архитектура QUADLOG loo2D позволяет монтировать резервирующие друг друга подсистемы на раздельных шасси, которые могут размещаться в раздельных шкафах и в разных помещениях. Такая возможность минимизирует подверженность резервирующих друг друга подсистем общим внешним воздействиям, таким как повышение температуры или обрыв линии питания в одном из шкафов, пожар в одном из помещений и др.

Полная и всесторонняя диагностика. Полная и всесторонняя система встроенной диагностики QUADLOG испытана и сертифицирована независимыми центрами сертификации, которые подтвердили её высокий уровень. Быстрая, исчерпывающая диагностика обеспечивает безопасность систем, высокий коэффициент готовности, а также существенно облегчает и ускоряет монтажные и пусковые работы. Система диагностики QUADLOG охватывает более 99.5% возможных нарушений в работе и отказов. ***Сертифицированная безопасность***. Для того чтобы систему можно было использовать в приложениях, критичных с точки зрения безопасности, система диагностики должна обнаруживать любые внутренние эксплуатационные сбои, которые могут помешать перевести технологическую установку в безопасное состояние. Диагностика должна также гарантировать безопасное поведение системы, и оповещение обслуживающего персонала о произошедшем сбое. Система диагностики QUADLOG полностью соответствует этим требованиям, независимо от типа используемой архитектуры.

Высокий коэффициент готовности. Высокая готовность системы зависит от её способности раннего обнаружения сбоев, и точной реакции на них для предотвращения возможности возникновения больших проблем.

Диагностическая информация снабжается временной меткой и сохраняется в точке обнаружения (управляющем модуле или модуле ввода-вывода). QUADLOG осуществляет диагностику не только внутренних цепей, но и внешних сигналов. Для этого с переменными ввода-вывода связывается диагностический параметр качества сигнала. Значение этого параметра характеризует достоверность данных, получаемых системой по внешним сигнальным линиям.

Диагностическая информация модуля ввода-вывода передается в модуль управления и объединяется с данными самодиагностики модуля управления. Модуль управления поддерживает базу актуальной диагностической информации и архив диагностических сообщений.

Доступ к диагностической информации QUADLOG может быть предоставлен потребителям различного типа: операторским и инженерным станциям, контроллерам, системам управления и другим устройствам. Программное обеспечение интерфейса оператора QUADLOG включает функции и утилиты опроса, сигнализации и архивирования сообщений системной диагностики.

Устройства сторонних производителей, такие, как системы управления технологическим процессом, могут беспрепятственно получать всю диагностику QUADLOG, используя последовательный интерфейс, протокол MODBUS, а также через DDE или OPC-сервер.

Ускоренный ввод в эксплуатацию, всесторонняя диагностика QUADLOG позволяет ускорить установку, монтаж и ввод в эксплуатацию новых систем, обеспечивая автоматическую диагностическую проверку дефектов внешних электрических соединений и внутренних программных и аппаратных сбоев системы. Модули ввода-вывода проводят проверку правильности подключения полевой шины.

Надежность. Высокий уровень надёжности и отказоустойчивости QUADLOG стал возможным благодаря мощным защитным механизмам, заложенным в основу архитектуры и конструкции QUADLOG, обеспечивающим превосходную устойчивость к жестким промышленным условиям. Защитные механизмы предусмотрены и встроены в систему QUADLOG с самого начала ее разработки.

Их надёжность и эффективность была проверена во время всесторонних интенсивных испытаний специальной группой инженеров Siemens Moore, а также во многих независимых лабораториях.

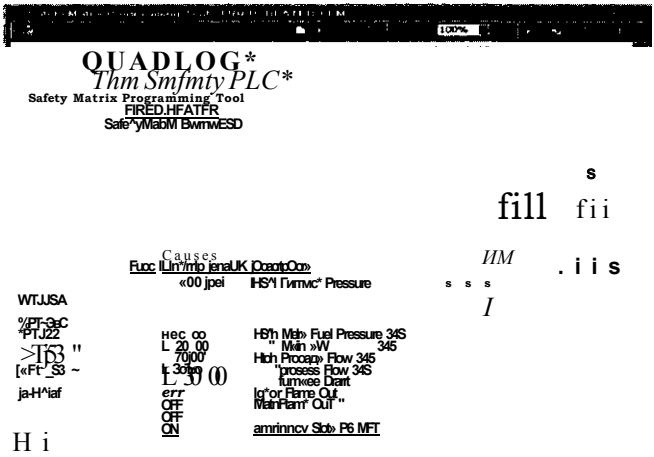
Конфигурационное программное обеспечение. Конфигурирование QUADLOG для выполнения функций конкретного приложения осуществляется с помощью конфигурационного программного обеспечения **4-mation™.**

Это программное обеспечение основано на открытом международном стандарте IEC 61131-3 и позволяет использовать любой из стандартных языков программирования (функциональные блоки, релейная логика, последовательные функциональные схемы, структурированный текст) в единой базе данных модуля управления.

Другие возможности 4-mation:

- Конфигурирование осуществляется без этапа компиляции, что обеспечивает мгновенную проверку правильности синтаксиса, существенно сокращая количество ошибок и исправлений.
- Механизм управления версиями и утилита сравнения конфигураций упрощают управление изменениями при разработке приложений.
- Функции защиты приложения от несанкционированного доступа и изменения, такие как административный пароль, пароли операторов, средства управления доступом и аппаратный защитный переключатель.
- Принудительная установка значений сигналов ввода-вывода с целью тестирования работы системы и внешнего оборудования сопровождается установкой предупредительных флагов и формированием списка таких сигналов.
- Возможность редактирования конфигурации и базы данных в режиме *on-line* существенно упрощает отладку и устранение ошибок.
- Для адресации внешних сигналов и внутренних переменных конфигурации используются имена тэгов, а не аппаратные адреса, что упрощает разработку и последующее обслуживание приложений.
- Конфигурация приложения хранится в графическом виде в энергонезависимой памяти QUADLOG.
- Возможность конфигурирования QUADLOG и РСУ APACS+ с помощью единого инструмента существенно сокращает время обучения персонала и разработки приложений.
- Существует встроенный механизм оперативных диагностических сообщений и их регистрации для быстрого поиска ошибок.

Матрица безопасности.



Матрица безопасности QUADLOG *(Safety Matrix)* - это инструментальное программное средство, которое предназначено для описания и документирования стратегии безопасности в виде таблицы, связывающей события технологического процесса, и реакцию на эти события со стороны системы безопасности.

Матрица безопасности QUADLOG используется совместно с пакетом конфигурирования 4-mation и позволяет существенно упростить конфигурирование приложений в части описания основных функций безопасности. Данный пакет инструментальных средств также служит средством проверки правильности созданной логики обеспечения безопасности. В период эксплуатации системы безопасности матрица безопасности обеспечивает оперативный мониторинг состояния объекта и возможность временного отключения функций безопасности на период обслуживания и тестирования. Матрица безопасности:

- Обеспечивает четкое и ясное документирование приложения, облегчая тем самым его разработку и анализ.
- Упрощает отслеживание документации.
- Облегчает разработку приложения благодаря автоматическому преобразованию стратегии из матрицы в конфигурацию приложения.

- Формирует адекватное документирование, требуя предварительного изменения матрицы при внесении изменений конфигурации.

Эмулятор QUADLOG *(Control Simulator)* позволяет осуществить полностью автономную разработку, моделирование и тестирование конфигурации, а также обучение персонала, не используя оборудование QUADLOG. Эта возможность существенно ускоряет разработку и проверку приложений, и уменьшает расходы на обучение.

Интерфейс оператора. В состав стандартного набора инструментальных средств QUADLOG входит программное обеспечение операторского интерфейса **Process Suite® Vision,** позволяющее создавать видеокадры технологического процесса. Интерфейс Vision представляет собой полную, безопасную и масштабируемую оболочку операторского интерфейса, и содержит мощные и разнообразные функции, существенно ускоряющие разработку приложений.

Запись последовательности событий. QUADLOG предоставляет механизм записи последовательности изменений внешних сигналов *(Sequence Of Events Recording - SOER)* с высоким временным разрешением для высокоточной фиксации, последующего анализа и диагностики событий на технологической установке, приведших к её останову, а также событий, произошедших непосредственно до и после останова. При реализации данной функции QUADLOG обеспечивает довольно высокое временное разрешение - 3 мс.
Это разрешение не зависит от частоты сканирования контроллера. Для просмотра событий, записанных с высоким разрешением, используется специализированная утилита интегрированного инструментального пакета **Process Suite® - SOER Viewer.**

Прямая интеграция с системами управления технологическим процессом. Промышленные и корпоративные стандарты содержат требования независимости функционирования систем обеспечения безопасности (системы противоаварийной защиты, пожарообнаружения, контроль загазованности и др.) и основной системы управления технологическим процессом. В то же время хорошо интегрированная система автоматизации требует эффективной коммуникации между всеми составляющими её подсистемами.

Система QUADLOG напрямую интегрируется в распределённые системы управления технологическими процессами APACS+ производства Siemens Energy & Automation и PCS7 производства Siemens Automation & Drives (рис. 3.21).

Распределённая система управления APACS+
Система обеспечения безопасности QUADLOG

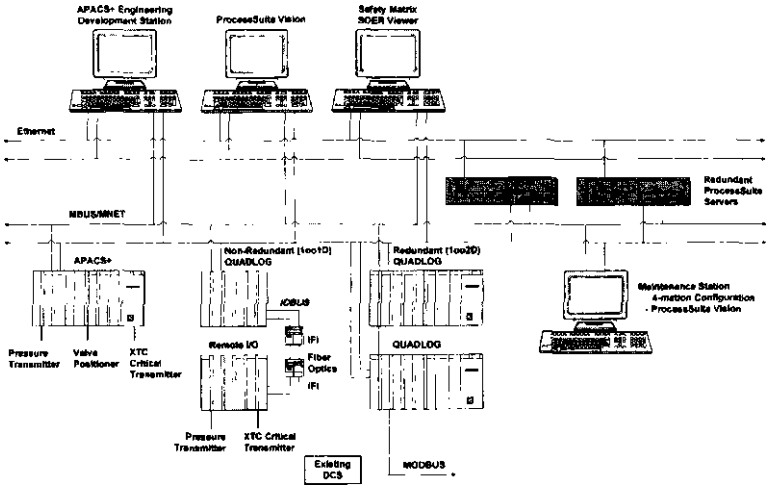


Рис. 3.21

Благодаря поддержке широкого спектра промышленных коммуникационных стандартов (OPC, MODBUS, DDE и др.), а также доступности прикладных интерфейсов программирования, QUADLOG легко интегрируется с распределёнными системами управления и промышленными контроллерами других производителей.

Встроенная мощная и гибкая система защиты коммуникаций QUADLOG позволяет гарантировать независимость, надёжность и полную безопасность его работы с любым оборудованием, обеспечивая выполнение требований всех международных и национальных стандартов, регламентирующих использование систем автоматизации и обеспечение безопасности технологических процессов.

3.21. Концепция фирмы HIMA
(рис. 3.22)

Программируемые электронные системы HIMA серий H41q и H51q состоят из модулей для основных блоков системы, расположенных в 19-дюймовом несущем каркасе, а также из модулей для цифровых и аналоговых сигналов ввода-вывода, которые могут быть выносными, или также расположены в 19-дюймовом несущем каркасе.

Система H41-HRS, H51-HRS (HI Quad) фирмы HIMA

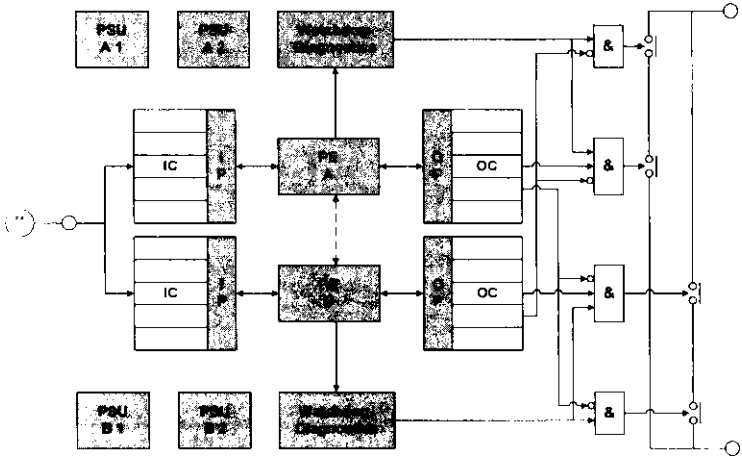


Рис. 3.22

Для конфигурирования, контроля, управления и документирования в программируемой электронной системе (PES) HIMA используется персональный компьютер с системой программирования ELOP II.

Ввод пользовательской программы и перевод в машинный код можно производить в отдельном ПК, не подключенном к программируемой электронной системе. Для загрузки, тестирования и контроля конфигурации, ПК соединяется с системой через последовательный порт напрямую, или через системную шину.

Безопасность и готовность. PES HIMA предназначены для использования по классу безопасности вплоть до 6 (деление по классам стандарта DIN V 19250) и могут обеспечивать высокую готовность. В зависимости от требуемого уровня безопасности и готовности системы HIMA могут поставляться в одно- или двукратном резервированном исполнении модулей в центральном блоке и блоках ввода-вывода. Резервные модули служат для повышения готовности, т.к. в случае неисправности дефектный модуль автоматически отключается, и в работе остается резервный модуль.

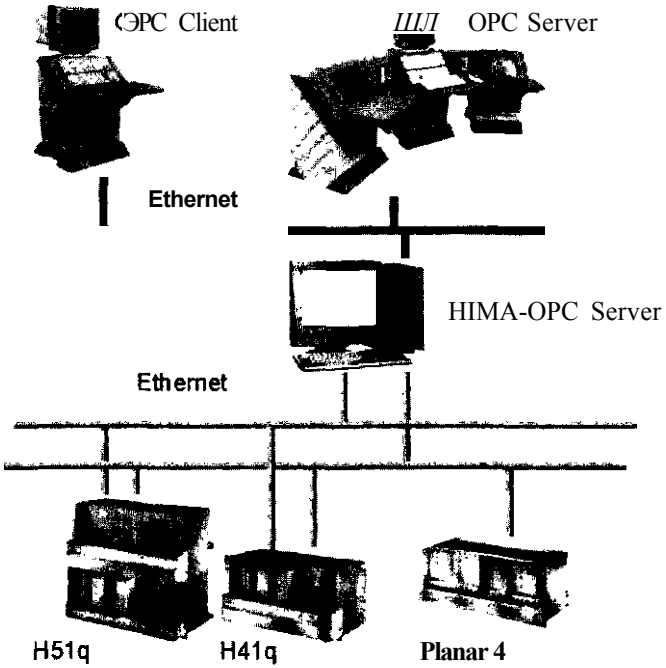


Рис. 3.23

Примечание

Система PLANAR4 - Requirement Class 7, SIL4.

HIMA имеет уникальную систему Planar 4, имеющую высшую аттестацию TUV: Safety-related modules, tested on DIN V19250 and IEC 61508. Certified for use up to AK7 (DIN V 19250) and SIL4 (IEC 61508).

Аварийное отключение. В случае возникновения неисправностей установка должна быть переведена в безопасное состояние. Безопасное состояние комплекса определяется как состояние минимального энергетического уровня на всех выходах.

В зависимости от установленного типа реакции на неисправность используются различные способы отключения.

Если в связи с возникновением неисправности в системе H51q-HRS требуется централизованное выключение, отключается сторожевой таймер контроля времени (WD) соответствующего центрального модуля.

Ethernet. Как можно видеть, система строится на протоколе Ethernet. Поэтому все замечания, высказанные ранее по отношению к этому недетерминированному протоколу, в равной степени относятся и к системам данного семейства.

Программный продукт *SILense*. Фирма HIMA обладает полным пакетом средств конфигурирования своих систем, таким как ELOP II. Но что действительно делает подход HIMA универсальным - это пакет ***SILense***, позволяющий производить расчеты надежности проектируемой системы безопасности в **конкретном применении.** Это полностью соответствует рекомендациям МЭК, и находится в согласии с отечественным ГОСТом 34.602 на создание АС.

Пакет первым получил сертификат TUV на право проведения расчетов надежности - как отдельных контуров защиты, так и системы безопасности в целом в полном соответствии со стандартом IEC 61508. И в полном соответствии с требованиями МЭК, расчеты проводятся не только для центральной части системы - контроллера, но для всего контура безопасности, включая датчики и исполнительные устройства. Пакет имеет обширную библиотеку по параметрам надежности сертифицированного оборудования систем безопасности для подавляющего большинства фирм-изготовителей полевого оборудования. При появлении нового оборудования библиотека может быть дополнена. Возможности пакета таковы, что для него требуется отдельное представление.

Конкретные особенности пакета будут подробно рассмотрены в главе "*Проектная оценка надежности системы "*

3.22. Система QMR FSC фирмы Honeywell

Архитектуру, полностью аналогичную архитектуре контроллеров HIMA серий H41q и H51q, имеет система QMR FSC ("2oo4D") фирмы Honeywell (рис. 3.24):

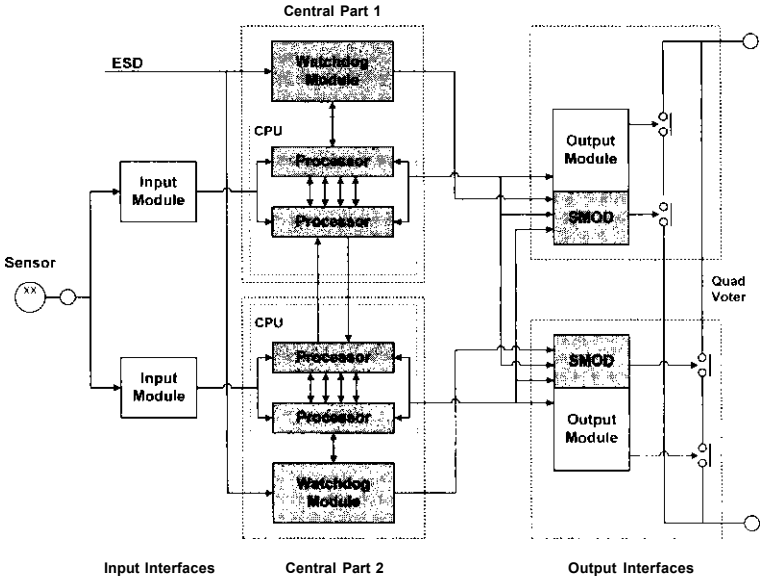


Рис. 3.24

3.23. Системы семейства ProSafe (Yokogawa Electric)

ProSafe - это целое семейство систем автоматической противоаварийной защиты. Семейство реализует различные пути обеспечения безопасности как технически, так и организационно. При необходимости может выполнять задачи, не относящиеся к критическим процессам и противоаварийной защите. Все это достигается как за счет использования современных технологий программирования, так и за счет использования современных полупроводниковых технологий.

На сегодняшний день определяются три платформы систем противоаварийной защиты:

- ProSafe-DSP
- ProSafe-PLC
- ProSafe-RS,

которые отвечают международным нормам IEC 61508 и 61511, предъявляемым к системам требуемого класса.

Система ProSafe-DSP применяется для самых опасных технологических процессов. Это один из немногих существующих контроллеров, аттестованных TUV по 6-7 **классу DIN и 4 уровню SIL.**

Радикальным отличием ProSafe-DSP является отсутствие системного и диагностического программного обеспечения. Вместо этого используется уникальная аппаратная технология встроенного схемного самотестирования для всех элементов системы ПАЗ. Полупроводниковая технология, используемая в ProSafe-DSP, основывается на ферритовой логике, определяющей принцип встроенного самотестирования и отказоустойчивости, Основным элементом ферритовой логики является кольцеобразный сердечник с обмоткой, который выполняет как логические функции (И, ИЛИ, НЕТ), так и выступает в роли гальванического изолятора.

ProSafe-PLC -^это полный аналог системы Quadlog, выпускаемой фирмой Йокогава под своей торговой маркой.

ProSafe-PLC отвечает наиболее широкому диапазону интегрального уровня безопасности согласно международному стандарту IEC 61508 и критерию работоспособности: для сводного уровня безопасности. ProSafe-PLC обеспечивает диапазон SIL 1...3, и RC 1...6 по DIN.

ProSafe-PLC состоит из ряда модулей, к которым относятся модули управления критическими технологическими процессами и модули ввода-вывода. В различных конфигурациях системы ProSafe-PLC эти устройства работают селективным и гибким образом. Даже в архитектуре loo ID система обеспечивает уникальную защиту выходных сигналов. Разнообразие маршрутов сдвоенных сигналов в ProSafe-PLC, объединенных с функциями сравнения между контроллерами, составляет основу конфигурации loolD в ProSafe-PLC. Символ D в данном случае означает, что в системе ПАЗ используется программа самодиагностики для каждого модуля ввода-вывода на основе эталонной информации, а также для аварийного останова технологического процесса.

Такая конфигурация 1oo1D с одним или сдвоенным управляющим модулем соответствует RC4 и SIL2.

Для создания полностью отказоустойчивой архитектуры системы ПАЗ за основу взята полностью резервированная конфигурация 1oo1D. В резервированном варианте возникает четырехполюсная архитектура 1oo2D (рис. 3.25).

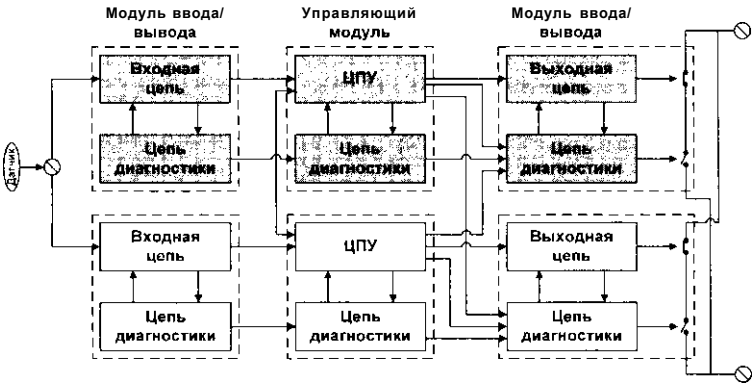


Рис. 3.25

Система 1oo2D ProSafe-PLC при обнаружении отказа переходит в конфигурацию 1oo1D, и продолжает свою работу без останова технологического процесса. Техническое обслуживание для восстановления первоначальной архитектуры этой системы допускается в режиме *on-line* без останова технологического процесса.

Структура 1oo2D ProSafe-PLC требует минимального объема аппаратных средств, обеспечивая при этом параллельное объединение защищенных выходных сигналов.

Конфигурация 1oo2D в соответствии с IEC61508 и ANSI/ISA 84.01-96 позволяет выполнить подключение резервных датчиков и приводов исполнительных устройств эффективным по стоимости способом без применения дополнительных аппаратных средств.

Полностью резервированная конфигурация 1oo2D соответствует DIN RC 5-6 и SIL3. Рисунок 3.26 отображает место каждой из систем в классификациях SIL (ANSI/ISA/IEC) и RC (DIN).

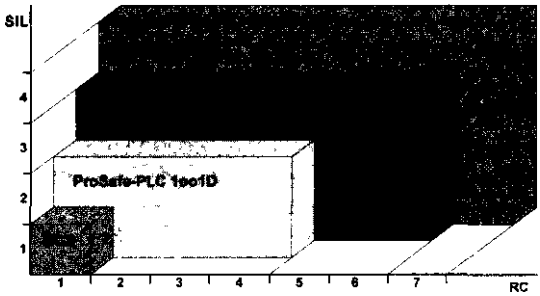


Рис. 3.26

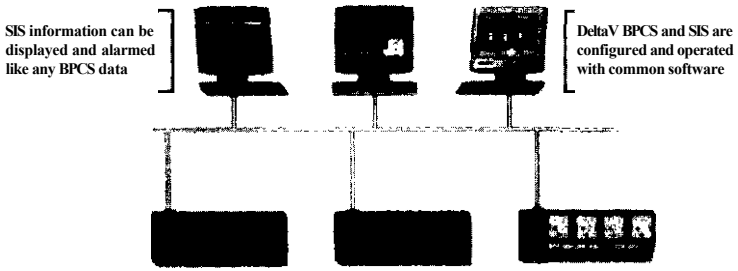
В марте 2005 года фирма Yokogawa Electric Corporation получила сертификат TUV на соответствие стандартам IEC 61508 и IEC 61511 для своей новой системы **ProSafe-RS,** и на право ее применения в приложениях SIL3.

ProSafe-RS реализует концепцию, которая уже давно стала привычной: система управления и система защиты строится на едином программно-техническом и информационно-управляющем поле, включая промышленные сети и человеко-машинный интерфейс. Преимущества очевидны:

- Однородная архитектура,
- Единая среда разработки,
- Интегрированная среда взаимодействия оператора с процессом.

Примечание

Аналогичный подход использует система DeltaV SIS:



Единственное, что нужно тщательно планировать и отслеживать, - это загрузку недетерминированного протокола Ethernet, на котором построено все семейство систем DeltaV.

Унификация на базе проверенной на практике системы Centum CS 3000 с архитектурой "Дублирование + Резервирование" *(та самая 2*2 - "Pair & Spare),* первооткрывателем которой без всякого шума была именно Yokogawa, и открыла возможность универсального построения единой системы безопасности, поэтому дискуссии на уровне Mloo2D?/"2oo4?", "TMR7/QMR?" - просто потеряли свою актуальность.

С помощью этой знаменательной для всех автоматизированных систем управления архитектуры обеспечивается:

- Реальная интеграция РСУ и ПАЗ;
- Простая, очевидная архитектура, естественная конструкция системы;
- Высокая готовность за счет резервирования;
- Резервированные двухпроцессорные модули управления и резервированные модули ввода-вывода
- Резервированная связь модулей управления и ввода-вывода
- Резервированная детерминированная системная шина Vnet.
- Одновременное функционирование и техобслуживание.

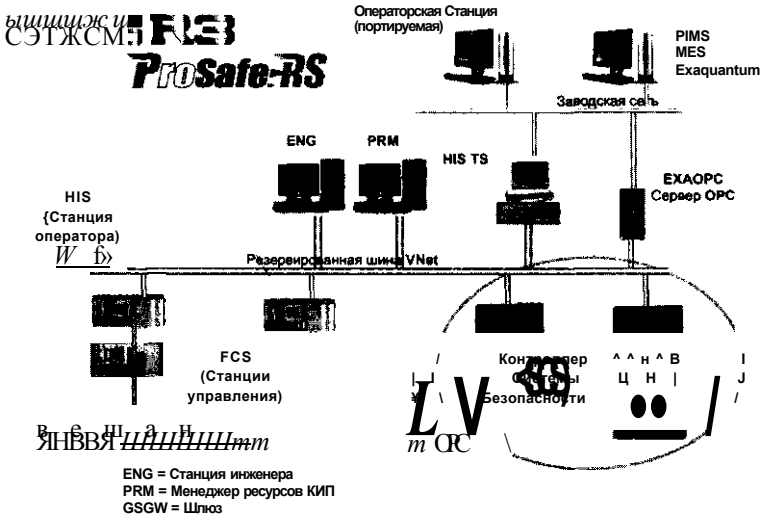


Рис. 3.30

Важное замечание

Еще раз: TUV и здесь утверждает, что уровень SIL3 достигается в нерезервированной модульной конфигурации. Необходимо твердо помнить и понимать, что это эффектное заявление не имеет под собой никаких практических оснований. Для современных непрерывных крупнотоннажных производств никак не может быть принято наивное понимание промышленной безопасности в духе IEC и TUV как способности системы в ответ на любой чих остановить производство. Применение одноканальных систем на нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производствах строго исключается. Необходимо отдавать себе отчет, что высшая степень готовности достигается только в резервированной системе.

Функция SOE (Регистрация Последовательности Событий) имеет **стандартное разрешение 1 миллисекунда.**
В перечень регистрируемых событий входит в том числе:

- Стандартный контроль линии
- Обнаружение короткого замыкания
- Обнаружение обрыва линии.

Реальная интеграция РСУ и ПАЗ. Для объединения РСУ и системы ПАЗ не требуется никаких вычурных компоновок и специальных схем связи.

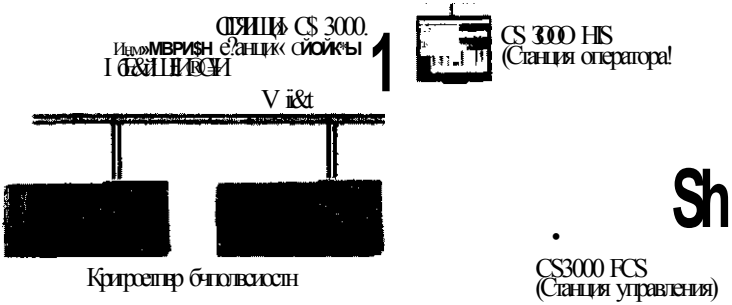


Рис. 3.28

Безопасный обмен данными между контроллерами Системы безопасности (SCS), Станциями управления (FCS) и Станциями оператора (HIS) по детерминированной промышленной шине Vnet системы Centum CS 3000.

Безопасность связи по протоколу Vnet подтверждена TUV.

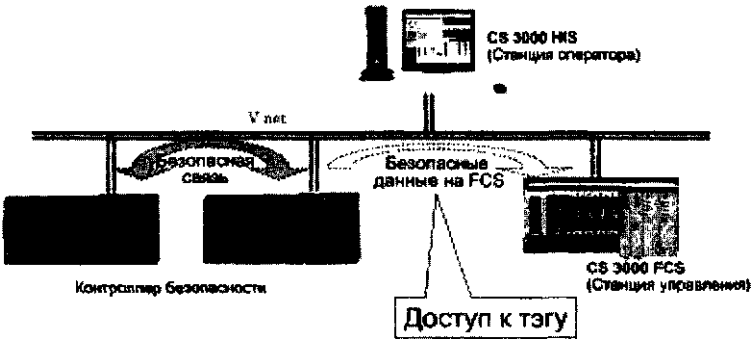


Рис. 3.29

Одно окно. Доступ (естественно, с учетом ограничений) к тэгам со станции оператора (HIS) открыт в обе стороны:

- И к данным РСУ,
- И к данным контролеров системы безопасности (SCS).

Таким образом, со станции оператора обеспечивается интегрированный контроль всей иерархии окошек системы:

- Мнемосхемы;
- Лицевые панели приборов (контуров);
- Тренды-графики;
- Состояние системы;
- Предупредительная и предаварийная сигнализация;
- SOE (последовательность событий) и т.д.

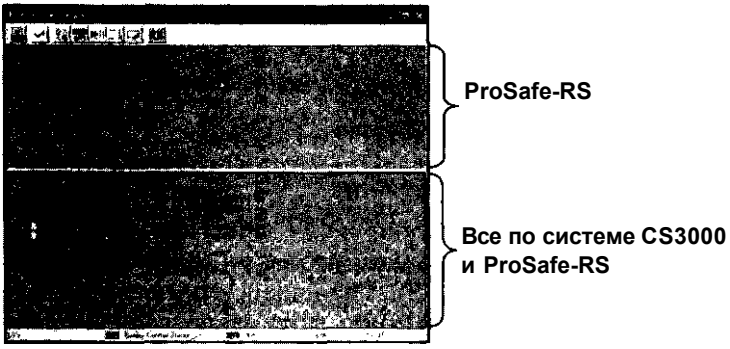


Рис. 3.30

Инструментарий инжиниринга:

- Функциональная блок-схема, лестничная (релейная) схема, структурированный текст;
- Конфигурирование системы и ввода-вывода;
- Тестирование (моделирующие программы для контроллера безопасности);
- Самодокументирование;
- Управление версиями системного и прикладного программного обеспечения.

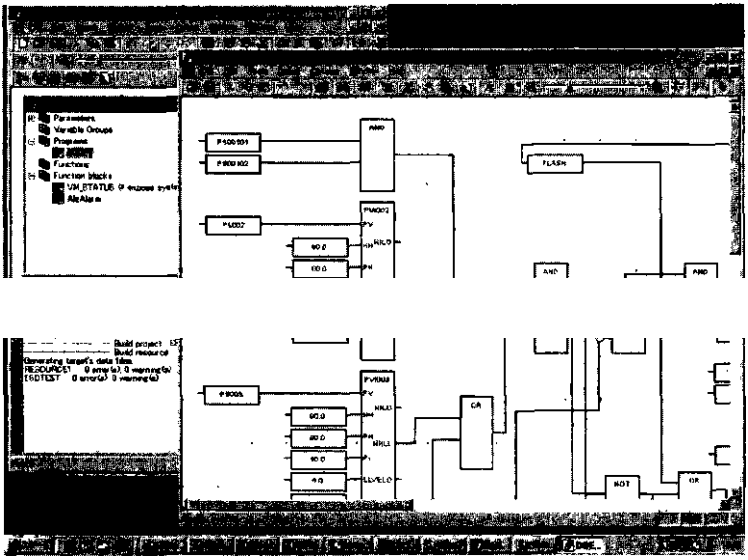


Рис. 3.31

Техобслуживание. Инженерная Станция:

- Отображение состояния логики
- Отображение состояния системы и программа просмотра диалога диагностики
- Программа просмотра SOE (протокол последовательности событий)
- Принудительные переменные (Вход, Выход, Логические переменные)
- Оперативное изменение логики (утверждено TUV).

Действия при отказах

Fault location	Cause	Structure	Actions	Fault level
CPU module	Hardware failure CPU node fault Software fault	Single	CPU stops All output modules output the output value on fault detection (All output shutdown)	Critical fault
		Dual-redundant	CPU on fault side stops The control is continued by switching the control nght	Minor fault
Input module	Hardware failure	Single	Input value on fad detection is set to all input channels of the modules and data status changed to BAD	Major fault
		Dual-redundant	The control is continued by switching the control right	Minor fault
Input channel	Failure of Hardware for individual channel Fault on field side	Single (*2)	Input value on fault detection is set to failed input channels and data status changed to BAD	Major fault
		Dual-redundant г3)	When a fault is on the field side the same action as the single structure is performed	Mapr fault
			Others except for the above case, the control is continued by switching the control right	Minor fault
Output module	Hardware failure	Single	Output of all output channels on the module becomes 0 and is put in output disable state, and data status changes into BAD state	Major fault
		Dual-redundant ГЗ)	The control is continued by switching the control nght	Minor fault
Output channel	Failure of Hardware for individual channel Fault on field side	Single	When output shutoff switch works (*1) Output of ail output channels on the module becomes 0 and is put in output disable state, and data status changes into BAD state	Major fault
			Others except for the above case Output value on fault detection is set to physical data of this channel and is put in output disable state, and data status changes into BAD state	Major fault
		Dual-redundant	When a fault is on a field side the same actions as the single structure are performed	Major fault
			When faults other than the above case the control is continued by switching the control nght	Minor fault

*1 The following faults are shown which against shutdown of at! output of the modules is performed with Output Shutoff Switch A dangerous fault like the inside of module ts fixed at ON and faults which requires the protection of modules including an over air rent caused by a short circuit on the field However, whether the output shutoff switch is operated against dangerous faults like the fixing at ON is specified with 1IO Parameter Builder as the setting of channels of the output modules

°2 When the modules have a single structure

*3 When the modules have a dual-redundant structure

Уникальные особенности создания приложений:

- Унифицированная архитектура (одно общее окно);
- Полностью дублированная и резервированная *("pair & spare" - 2*2)* архитектура;
- Автоматическая доступность сигнализаций процесса и системных сигнализаций на станции оператора (HIS);
- Автономное тестирование;
- Оперативное внесение изменений (утверждено TUV).

Единый поставщик. Соответственно,

- Ограниченное количество запасных модулей;
- Меньшая стоимость техобслуживания;
- Менее продолжительное обучение операторов;
- Унифицированная архитектура упрощает построение единой системы РСУ + ПАЗ.

Цикл контроллера **системы безопасности** (SCS):

От 50 мс до 1 сек, с шагом 10 мс

Период опроса для функции исполнения прикладной логики

1) Сбор входных данных + Диагностика
2) Безопасная связь от других SCS
3) Исполнение программы
4) Безопасная связь с другими SCS
5) Запись выходных данных + Диагностика.

Масштабируемость. Полномасштабная сеть:

- РСУ и ПАЗ имеют в общем пользовании все возможности детерминированной шины Vnet
- РСУ и ПАЗ интегрированы по сети Vnet, но физически (на уровне обособленных стоек) и функционально разделены.

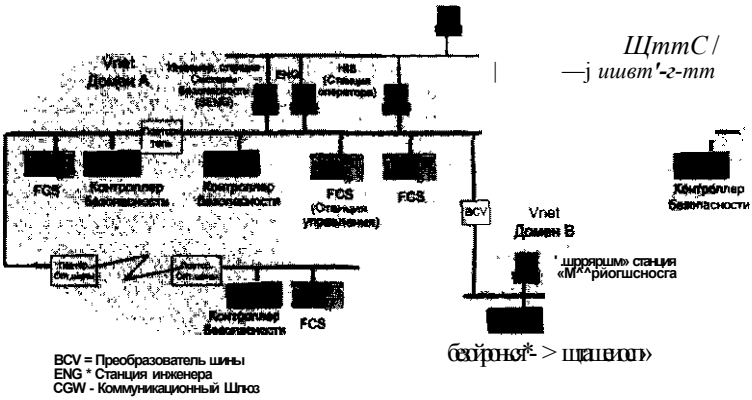


Рис. 3.32

Основные характеристики системы ProSafe-RS:

- Уровень безопасности SIL 3;
- Гарантированное время реакции системы (такое же, как и время опроса - 50 мс, то есть 20 раз в секунду);
- Безопасная связь между станциями управления и защиты (между контроллерами);
- Общий доступ к информации для управляющих приложений и приложений безопасности;
- Легко масштабируемая архитектура;
- Гибкость для различных конфигураций (распределенная или централизованная);
- Определения короткого замыкания/разрыва цепи для каналов подключения КИП;
- Соответствие языкам стандарта IEC 61131-3;
- Функции SOE (Регистрация Последовательности Событий);
- Функции сигнализации процесса;
- Функции автономного и самотестирования.

Таким образом, Yokogawa обладает уникальным спектром систем обеспечения безопасности:

- ProSafe-SLS обеспечивает неограниченную по времени поддержку для высшего уровня требований безопасности SIL4;
- ProSafe-PLC. Полный аналог хорошо проверенного на практике семейства систем типа Quadlog;
- ProSafe-RS. Проверенная многолетней практикой основного оборудования систем семейства Centum дублированная и резервированная *("pair & spare" = 2*2)* архитектура. Нет замечаний.

Глава 4

ОБЩИЕ ТРЕБОВАНИЯ ПРИ СОЗДАНИИ АСУТП

4.1. Положение наших предприятий на нормативном поле

Жизненно важный аспект создания безопасных АСУТП - это формализация самого процесса создания АСУТП, то есть определение процедур проведения проектных работ и определение состава и содержания проектной и рабочей документации. Надо отдать должное создателям отечественных ГОСТов для автоматизированных систем: эти ГОСТы и по сей день сохраняют свою актуальность. Вместе с тем, необходимость корректировки отечественных нормативных документов существует.

ПБ 09-540-03. Едва ли не единственным отечественным документом, определяющим технические и организационные условия практической автоматизации технологических процессов, являются ПБ 09-540-03 "Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств". Однако этот в целом добротный документ, который носит универсальный характер для подавляющего большинства технологических процессов, имеет ряд пробелов и неточностей. В особенности это касается вопросов применения современных средств управления и защиты технологических процессов.

Отсутствие определений для основных терминов и понятий. В отличие от предыдущего издания Правил - ПБ 09-170-97, в котором присутствовало Приложение 3 "Термины и определения, принятые в Правилах", новая редакция ПБ 09-540-03 вообще не содержит этого приложения. В результате в Правилах продолжают использоваться самые разнообразные словосочетания, допускающие произвольную интерпретацию.

В некоторых случаях это делает невозможным и без того непростое понимание положений ПБ в части АСУТП вообще, а систем ПАЗ в особенности. Достаточно привести всего лишь один характерный пример.

Пункт 3.10 ПБ 09-540-03 утверждает:

"Для взрывоопасных технологических процессов предусматриваются системы противоаварийной автоматической защиты, предупреждающие возникновение аварийной ситуации ***при отклонении от предусмотренных регламентом предельно допустимых значений параметров процесса во всех режимах работы*** *и обеспечивающие безопасную остановку или перевод процесса в безопасное состояние по заданной программе"*

Спрашивается, какие меры можно успеть предпринять, если предельно допустимые значения отличаются от критических только на величину ошибки измерительного канала, а критическое значение - это такое значение, при котором возможен взрыв или разгерметизация (см. Таблицу 3 в ПБ 09-170-97 - *как уже сказано, в ПБ 09-540-03 таблица определений вообще отсутствует).*

Авторское определение возможных и граничных значений технологических параметров, сопровождаемое графическим изображением соответствующих сигнализаций и блокировок, приводится далее в таблицах 4.4 - 4.8.

Кроме того, в таблицы 4.7 и 4.8 введена классификация технологических ситуаций с четким разграничением таких важных понятий, как "Инцидент" и простое "Нарушение" - как состояние, не приводящее к срабатыванию системы противоаварийной защиты.

Федеральный закон №116 *"О промышленной безопасности опасных производственных объектов"* вводит следующее понятие *Инцидента:*

"Инцидент - отказ или повреждение технических устройств, применяемых на опасном производственном объекте, ***отклонение от режима технологического процесса, нарушение положений настоящего Федерального закона, других федеральных законов и иных нормативных правовых актов Российской Федерации****, а также нормативных технических документов, устанавливающих правша ведения работ на опасном производственном объекте".*

В данной формулировке понятие "*отклонение от режима технологического процесса"* допускает самое широкое толкование. И со стороны контролирующих органов грех этим не воспользоваться. Под отклонением от режима при необходимости легко понимается **любое отклонение от режима,** то есть любой выход за предписанные регламентом значения, в первую очередь - в зону предупредительных значений.

На этом фоне уникально смотрится довесок "*нарушение положений настоящего Федерального закона, других федеральных законов и иных нормативных правовых актов Российской Федерации",* которое уже и не нарушение законов, а просто инцидент!

Формулировка закона в максимально возможной степени усилена по отношению к непосредственному исполнителю - аппаратчику, начальнику смены, дежурному слесарю КИП, и в максимально возможной степени ослаблена по отношению к лицам, ратующим и ответственным за создание режима безопасности производства. Пункт 2.9 ПБ 09-540-03 вводит непосредственно в данный контекст новый поворот: "*Расследование инцидентов во взрывопожароопасных производствах, **анализ причин опасных отклонений от норм технологического режима** и контроля над соблюдением этих норм осуществляются в соответствии с требованиями руководящих документов Госгортехнадзора России*

Определение понятия "*Опасное отклонение от норм"* в ПБ, естественно, отсутствует. Единственный, но полностью аналогичный по силе воздействия случай словесных манипуляций с опасностью - это потрясающее определение ПБ 09-170-97, Приложение 3: "*Опасное значение параметра - значение параметра, вышедшее за пределы регламентированного, и **приближающееся** (?!) к предельно допустимому значению".*

Причем в самом тексте ПБ 09-170-97 *"опасное значение параметра"* использовано только единожды - в пункте 3.1.12 (в новых ПБ 09-540-03 - в пункте 4.1.12). По этому определению выходит, что значение параметра, вышедшее за пределы регламентированного, но ***постоянное, или удаляющееся*** от предельно допустимого значения, опасным уже не является. Все эти недоразумения надо поправить. Необходимо избавиться от опасных отклонений, и дать строгие определения состояний.

Предаварийная ситуация *- ситуация, при которой отклонение от норм технологического режима, или состояние оборудования приводит к выходу за предаварийные граничные значения (предаварийные уставки), и вызывает срабатывание системы противоаварийной защиты, предотвращая развитие аварийной ситуации. Ложное срабатывание системы противоаварийной защиты также относится к категории предаварийной ситуации.*

Тогда **Инцидент** в Федеральном законе будет исчерпан следующим определением:

Инцидент - предаварийная ситуация, *отказ или повреждение технических устройств, применяемых на опасном производственном объекте, не приведшие к аварии.*

А нарушение нормативных технических документов, устанавливающих правила ведения работ на опасном производственном объекте, не приведшее к инциденту или аварии - это именно нарушение нормативных технических документов. И не более того.

Упомянутое всуе "*нарушение положений настоящего Федерального закона, федеральных законов",* и ещё каких-то *"иных нормативных правовых актов Российской Федерации"* из категории **технологических инцидентов** строго исключается. *(Видимо авторы закона как-то подзабыли, что кроме российских законов в России существует всего лишь один вид "иных нормативных правовых актов"-указы президента).*

Таким образом, любое изменение параметров технологического процесса за пределами предупредительных граничных значений (предупредительных уставок), не выходящее за пределы предаварийных граничных значений (предаварийных уставок), и не приводящее к срабатыванию системы противоаварийной защиты, ИНЦИДЕНТОМ НЕ ЯВЛЯЕТСЯ.

Для строгого разграничения этих промежуточных состояний между регламентированным и предаварийным состоянием процесса необходимо ввести понятие **"Нарушение":**

Нарушение норм технологического режима (технологическое нарушение) - технологическая ситуация, при которой нарушение предупредительных уставок **не приводит к выходу за предаварийные уставки,** и, соответственно, **не вызывает срабатывание системы противоаварийной защиты.**

А для разбора технологических нарушений никакого участия надзорных и федеральных органов не требуется - вполне достаточно заводского и цехового уровня.

Стандарт предприятия на проектирование, разработку, внедрение, эксплуатацию и сопровождение АСУТП. Безусловно, в конечном итоге должен существовать самостоятельный комплекс согласованных нормативных документов, определяющих все аспекты создания АСУТП, включая особые требования к автоматизации взрывоопасных производств. А пока его нет, предприятия в максимально возможной степени должны использовать существующую отечественную нормативную базу. В контексте обсуждаемой темы это можно сделать, приняв **Стандарт предприятия на проектирование, разработку, внедрение, эксплуатацию и сопровождение АСУТП (СТП).** В составе этого стандарта необходимо определить:

- Состав, распределение работ и ответственность всех участников проекта создания АСУТП;
- Состав и конкретное содержание проектной и рабочей документации технического и рабочего (технорабочего) проектов АСУТП с учетом специфических требований конкретных производств.

Авторский опыт показывает, что защита предприятия от недобросовестных проектировщиков и разработчиков АСУТП будет существенным образом укреплена, если в СТП будут включены образцовые документы стадий, определяющих начало и завершение проекта создания АСУТП:

- Отработанный на опыте практической реализации на технологических объектах аналогичного класса образец "Технического задания на создание АСУТП", и
- Образец "Программы и методики испытаний" с полным комплектом документов, необходимых при оформлении и утверждении результатов предварительных, опытных и приемочных испытаний системы.

Более того, у предприятия есть все права потребовать от генподрядчика подтверждения проектной надежности системы в виде конкретных расчетов параметров надежности для конкретного применения на взрывоопасном производстве. За последние годы успели появиться вполне добротные документы по анализу рисков и оценке последствий отказов:

- РД 03-418-01 "Методические указания по проведению анализа риска опасных производственных объектов", основанные на анализе деревьев отказов и событий, и
- ГОСТ 27.310-95 "Анализ видов, последствий и критичности отказов".

В РД 03-418-01 приводятся конкретные показатели по уровню и критичности последствий отказов, аналогичные тем, что используются на западе.

Из представленных категорий и критериев тяжести отказов следует, что взрывоопасные объекты нефтегазодобывающей, химической, нефтехимической и нефтеперерабатывающей промышленности прочно занимают положение, для которого *количественный анализ риска обязателен.*

4.2. Оптимистические выводы

Отсутствие вразумительных нормативных документов в области промышленной автоматизации приводит к полнейшей профанации, когда умение повторять всего лишь одно магическое слово "TUV" открывает все пути на взрывоопасное производство.

На этом фоне исключительно достойное впечатление производит система советских ГОСТов по созданию автоматизированных систем:

- ГОСТ 34.003-90 ИТ. Автоматизированные системы. Термины и определения.
- ГОСТ 24.104-85 ЕСС АСУ. Автоматизированные системы управления. Общие требования.
- ГОСТ 34.201-89 ИТ. Виды, комплектность и обозначение документов при создании автоматизированных систем.
- ГОСТ 34.601-90 ЕСС АСУ. Автоматизированные системы. Стадии создания.
- ГОСТ 34.602-89 ИТ. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
- ГОСТ 34.603-92 ИТ. Виды испытаний автоматизированных систем *(один из наших лучших ГОСТов по автоматизации).*

Основы этих соразмерных и согласованных документов были заложены еще в семидесятых годах людьми исключительно компетентными, с вполне организованными мозгами.
В двух следующих главах настоящей работы:

- "Состав и содержание работ по созданию АСУТП" и
- "Состав и содержание документации проекта АСУТП",

в максимально возможной степени использованы положительные результаты, достигнутые авторами наших ГОСТов. Поразительно, но даже по истечению десятилетий эти документы во многом сохраняют свою актуальность.

Вместе с тем, никак нельзя обойти главный вопрос нормативного обеспечения автоматизации технологических процессов: **Должен существовать самостоятельный комплекс согласованных нормативных документов, определяющих все аспекты создания АСУТП, включая особые требования к автоматизации взрывоопасных производств.** В противном случае наши предприятия так и будут находиться в подвешенном состоянии между устаревшими отечественными требованиями и отвлеченными западными стандартами.

Существенная, и наиболее трудоемкая доля положений этого будущего комплекса рассматривается, изучается, и предлагается в настоящей работе. Далее в настоящей главе:

- В таблицах 4.1-4.8 дается полная система терминов и понятий, которые в обязательном порядке должны входить в основание общей системы требований при создании АСУТП, и без однозначного определения которых построение предсказуемой АСУТП невозможно.
- В разделах 4.3-4.7 приводятся области разделения ответственности для участников проекта создания АСУТП.
- В разделах 4.8-4.19 приводятся скорректированные пункты раздела VI ПБ 09-540-03 "*Системы контроля, управления, сигнализации и противоаварийной автоматической защиты технологических процессов*", и предлагаются новые положения, отражающие авторское понимание той части требований к созданию АСУТП, которая должна присутствовать в нормативной документации на проектирование, разработку, внедрение, эксплуатацию и обслуживание АСУТП.

Таблица 4.1

Обозначения и сокращения

Термин	Определение термина
КИП и А	Совокупность контрольно-измерительных приборов и исполнительных устройств, предназначенных для выполнения информационных, управляющих, и функций защиты технологического процесса
СА	Средства автоматизации, включающие в себя пневматические, электрические, электронные, полевые и щитовые приборы, исполнительные устройства, а также распределенные системы управления (РСУ) и средства противоаварийной защиты (ПАЗ)
АСУТП	Автоматизированная система управления технологическим процессом, предназначенная для реализации информационных, управляющих, и функций защиты технологического процесса в автоматическом и автоматизированном режиме Организационно АСУТП состоит из 1. Персонала,и 2. Комплекса технических и программных средств, предназначенных для автоматизации его (персонала) деятельности. Структурно и функционально АСУТП взрывоопасного производства включает в себя два взаимосвязанных компонента. 1. РСУ, 2 ПАЗ
АС	Автоматизированная система, Система. *В контексте настоящей работы - Синонимы АСУТП*
РСУ	Распределенная система управления технологическим процессом, построенная на средствах измерения, вычислительной технике и исполнительных устройствах
ПАЗ	Система противоаварийной защиты - система безопасности технологического процесса, построенная на средствах измерения, вычислительной технике и исполнительных устройствах
СБ	Система безопасности. В узком смысле - Система противоаварийной защиты
ПЛК	Программируемый логический контроллер
ППО	Прикладное программное обеспечение, разработанное применительно к РСУ и ПАЗ для реализации функций контроля, управления и защиты конкретного технологического процесса

Таблица 4.2

Определение стадий и этапов создания АСУТП

Термин	Определение термина
Процесс создания АСУТП	Совокупность работ от формирования исходных требований к Системе до ее ввода в промышленную эксплуатацию. Подразделяется на стадии и этапы
Стадия создания АСУТП	Одна из частей создания АСУТП, установленная нормативными документами и заканчивающаяся выпуском документации на Систему, содержащей описание полной в рамках заданных требований модели Системы на заданном для данной стадии уровне
Этап создания АСУТП	Часть стадии создания АСУТП, выделенная по соображениям единства работ и завершающего результата, или исходя из специализации исполнителей
Техническое задание на создание АСУТП	Документ, оформленный в установленном порядке, определяющий цели создания Системы, требования к Системе и основные исходные данные, необходимые для ее разработки, а также план-график создания АСУТП
Технический проект автоматизированной системы	Комплект проектных документов на АС, разрабатываемый на стадии "Технический проект", утвержденный в установленном порядке, содержащий основные проектные решения по Системе в целом, ее функциям и всем видам обеспечения, достаточный для разработки Рабочей документации на АС
Рабочая документация на автоматизированную систему	Комплект проектных документов, разрабатываемый на стадии "Рабочая документация", и содержащий взаимоувязанные решения по Системе в целом, ее функциям и всем видам обеспечения, достаточный для комплектации, монтажа, наладки и функционирования, проверки и обеспечения работоспособности АС Создается Разработчиком АСУТП
Проектно-сметная документация на АСУТП	Часть рабочей документации, разрабатываемая для выполнения строительных, монтажных, электротехнических, санитарно-технических и других работ, связанных с созданием АСУТП. Выполняется Проектной организацией
Эксплуатационная документация	Часть рабочей документации на АСУТП, предназначенная для эксплуатации АСУТП, и определяющая правила действия персонала и пользователей АСУТП при ее функционировании, проверке и обеспечении ее работоспособности. Выполняется Разработчиком АСУТП и Проектной организацией, по принадлежности
Рабочий, Технорабочий проект автоматизированной системы	Комплект проектных документов на АС, утвержденный в установленном порядке, и содержащий решения по Системе в объеме технического проекта и рабочей документации на АС

Таблица 4.3

Организации, участвующие в процессе создания АСУТП

Термин	Определение термина
Организация - Разработчик процесса	Организация, осуществляющая разработку исходных данных на проектирование технологического процесса, основанных на научно-исследовательских и опытных работах
Проектная организация	Организация - разработчик проекта для данного технологического объекта, или проектная организация, имеющая лицензию на проектирование данных или аналогичных по типу и по категории взрывоопасности технологических объектов
Организация - Заказчик	Организация, для которой создается проект АСУТП, и которая обеспечивает финансирование, организацию и приемку работ, и эксплуатацию объекта автоматизации
Организация - Генпроектировщик (генподрядчик) АСУТП	Организация, являющаяся главным подрядчиком всех работ по проекту создания АСУТП. Для выполнения проекта генпроектировщик может привлекать различных субподрядчиков-поставщиков, разработчиков, проектировщиков и т. д.
Организации - Проектировщики	Проектировщики различных частей проекта, связанных с созданием АСУТП
Организация - Разработчик АСУТП	Организация, которая осуществляет работы по созданию АСУТП, предоставляя Организации-заказчику совокупность научно-технических услуг на разных стадиях и этапах создания, а также разрабатывая и поставляя программные и технические средства АСУТП
Организация - Поставщик	Организация, которая поставляет программные и технические средства различных частей проекта создания АСУТП
Организации строительные, монтажные, наладочные и другие	Организация, которые выполняют соответствующие работы в смежных частях проекта - проведение строительных, электротехнических, монтажных и других работ, связанных с созданием и внедрением АСУТП

Таблица 4.4

Определение регламентированных граничных значений и типов сигнализации

Термин	Определение термина
Уставка	Регламентированное граничное или заданное значение некоторой переменной величины. В данном контексте - граничное значение технологической переменной, технологического параметра
Уставки предупредительные	Установленные регламентом граничные значения параметров, при нарушении которых выдается предупредительная сигнализация.
Предупредительная сигнализация	Сигнализация, срабатывающая при нарушении предупредительной уставки параметра технологического процесса
Уставки предаварийные	Установленные регламентом граничные значения параметров, нарушение которых вызывает срабатывание системы ПАЗ, и выдается предаварийная сигнализация
Предаварийная сигнализация	Сигнализация, срабатывающая при нарушении предаварийной уставки параметра технологического процесса
Уставки критические	Установленные регламентом граничные значения одного или нескольких взаимосвязанных параметров, при которых возникает непосредственная угроза аварии - взрыва, или разгерметизации технологического оборудования

Таблица 4.5

Определение **способа** управления **объектом**

Термин	Определение термина
Автоматическое управление	Управление технологическим процессом, его частью (стадией), или осуществление отдельных функций управления без непосредственного участия человека
Автоматизированное управление	Управление технологическим процессом, его частью (стадией), или осуществление отдельных функций управления при непосредственном участии человека

Таблица 4.6

Определение возможных значений технологических параметров

Термин	Определение термина
1	2
Регламентированные (установленные) значения параметров технологического процесса	Совокупность установленных регламентом значений параметров технологического процесса, при которых технологический процесс может безопасно протекать в заданном направлении
Предупредительные (допустимые) значения технологических параметров	Значения параметров технологического процесса, выходящие за предупредительные уставки, но находящиеся в пределах предаварийных уставок, и не вызывающие срабатывание системы противоаварийной защиты
Предаварийные (опасные) значения технологических параметров	Значения параметров технологического процесса, выходящие за пределы предаварийных уставок, и вызывающие срабатывание системы противоаварийной защиты
Аварийные (критические) значения параметров	Значения одного или нескольких взаимосвязанных параметров, выходящие за пределы аварийных (критических) уставок, при которых возникает непосредственная угроза аварии - взрыва, или разгерметизации технологического оборудования

Примечание

Значения, выходящие за шкалу прибора, связанные с коротким замыканием или обрывом измерительной цепи, или с нарушением калибровки измерительного канала, обрабатываются посредством самотестирования, оперативного и технического обслуживания АСУТП, поэтому в контексте технологических нарушений не рассматриваются.

Таблица 4.7

Определение технологических ситуаций

Термин	Определение термина
1	2
Авария	Разрушение сооружений и/или технических устройств, применяемых на опасном производственном объекте, неконтролируемый взрыв и/или выброс опасных веществ (ФЗ №116)
Аварийная ситуация	Ситуация, когда произошла авария, и возможен дальнейший ход ее развития
Предаварийная ситуация	Ситуация, при которой нарушение технологического режима, или состояние оборудования приводит к выходу за предаварийные уставки, и вызывает срабатывание системы противоаварийной защиты, предотвращая развитие аварийной ситуации. **Ложное срабатывание системы ПАЗ также относится к категории предаварийной ситуации**
Инцидент	**Предаварийная ситуация,** отказ или повреждение технических устройств, применяемых на опасном производственном объекте, не приведшие к аварии
Нарушение норм технологического режима	Ситуация, при которой нарушение предупредительных уставок не приводит к выходу за предаварийные уставки, и не вызывает срабатывание системы противоаварийной защиты
Ложное срабатывание системы противоаварийной защиты	Беспричинное срабатывание системы противоаварийной защиты, вызвавшее немотивированный останов всего производства, или его части по причинам, не связанным с действительными событиями на процессе

Сводная таблица определения значений технологических параметров, уставок системы ПАЗ и типов сигнализации РСУ *Таблица 4.<*

Возможные значения параметров	Папе	ПАЗ		Твзшологичес- *ятяжумщк*	Тип сигнализации	
Аварийные ^шитические] значения				**Аварийная ситуация**		
Прсдатрийные (опасны^ значение				**Инцидент**	сигнализации	**н н**
Предупредительные (допустимые) значения				**Нарушен****	**Предупредительная сигнализации**	**н**
Рвтаиишгнроваииы* анемия	С У	V		*Шрт*		
Предупредительные Допустимые) значения				**Нарушение**	**Предупредительная ^игналшация**	**L**
Предаваркиные {впаснь<е) значения	**е**		*Ш Ж*	Инцидент	Прадапарииная сигнализация	**U -**
Аварийные |»Фиппчеех»е) значения				**Аварийная! ситуация**		

НРШГшкапы

Предзоариинная

Предзварийнзя

TFK1 **3**

В следующих разделах представлены положения, которые, по мнению автора, должны присутствовать в нормативных документах, определяющих общие требования к автоматизации взрывоопасных производств. При этом ряд безупречных положений и ПБ 09-540-03, и других отечественных нормативных документов по созданию автоматизированных систем, безусловно, должен быть сохранен.

4.3. **Схемы организации проекта**

Представленные в данном разделе схемы организации и взаимодействия участников выполнения проекта создания АСУТП (рис. 4.1 - 4.3), может быть, и не имеют прямого отношения к каждому непосредственному исполнителю, однако без ясного понимания своей роли и места в проекте для каждого из участников построить работающую систему невозможно.

Схема организации Проекта 1

Заказчик

Организации строительные, монтажные и наладочные

Проектировщик **Разработчик** **Поставщик**

Рис. 4.1

Примечание

Согласно ГОСТ 34.601-90 "Автоматизированные Системы. Стадии созданияв зависимости от условий создания АСУТП возможны различные совмещения функций Заказчика, Разработчика, Проектировщика, Поставщика и других организаций, участвующих в работах по созданию АСУТП.

Схема организации Проекта 2

Рис. 4.2

Схема организации Проекта 3

Рис. 4.3

4.4. Распределение ответственности при создании АСУТП

Система управления промышленной безопасностью. Первостепенное значение имеют требования ПБ 09-540-03 по созданию системы управления промышленной безопасностью. В частности, согласно Пункту 1.4 ПБ:

"В целях организации работы по предупреждению аварий и производственного травматизма организации, имеющие в своем составе взрывопожароопасные объекты, разрабатывают систему стандартов предприятия по управлению промышленной безопасностью, и обеспечивают их эффективное функционирование и актуализацию". Кроме того, согласно Пункту 1.5 ПБ, "Организации, осуществляющие проектную деятельность, а также деятельность по монтажу, ремонту оборудования и сооружений, обучению персонала, разрабатывают и обеспечивают эффективное функционирование и актуализацию **системы стандартов предприятия по обеспечению качества. Системы качества организаций должны предусматривать наличие стандартов по обеспечению безопасного ведения работ".**

Таким образом, Организация-заказчик не только должна сама обеспечить эти требования Правил, но и вправе потребовать от организаций, участвующих в создании, проектировании, обучении, реконструкции, модернизации взрывоопасных технологических объектов соответствия стандартам предприятия по обеспечению безопасности.

Кроме того, Заказчик должен иметь Стандарт предприятия, который устанавливает порядок проектирования, разработки, внедрения, сопровождения и эксплуатации комплекса технических и программных средств АСУТП для реконструируемых и вновь строящихся производств.

Согласно ГОСТ 34.601- 90, пункт 2.2, стадии и этапы, выполняемые организациями-участниками работ по созданию автоматизированных систем, устанавливаются во взаимных Договорах и В Техническом задании.

В следующих пунктах определяется конкретная ответственность каждого из участников проекта создания АСУТП. Соответственно определен ряд новых положений. Некоторые из положений ПБ сохранены, но скорректированы.

4.5. Ответственность Разработчика процесса

Замечание

Ответственность разработчика процесса непосредственно к нашей теме не относится и приводится только для полноты изложения.

Регламентированные значения параметров, определяющих взрывоопасность процесса, допустимый диапазон их изменений, организация проведения процесса (аппаратурное оформление и конструкция технологических аппаратов, фазовое состояние обращающихся веществ, гидродинамические режимы и т.п.), а также регламентированные значения параметров, определяющих взрывоопасность процесса, допустимый диапазон их изменения, устанавливаются *Разработчиком* процесса на основании данных о критических значениях параметров. Согласно п. 3.4.1 Правил, условия взрывопожаробезопасного проведения отдельного технологического процесса или его стадий, *устанавливаемые Разработчиком процесса,* обеспечиваются:

- Рациональным подбором взаимодействующих компонентов, исходя из условия максимального снижения или исключения образования взрывопожароопасных смесей или продуктов;
- Выбором рациональных режимов дозирования компонентов, предотвращением возможности отклонения их соотношений от регламентированных значений и образования взрывоопасных концентраций в системе;
- Рациональным выбором гидродинамических (способов и режима перемещения среды и смешения компонентов, напора и скорости потока) и теплообменных (теплового напора, коэффициента теплопередачи, поверхности теплообмена и т.п.) характеристик процесса, а также геометрических характеристик аппаратов и т.п.;
- Применением компонентов в фазовом состоянии, затрудняющем или исключающем образование взрывоопасной смеси;
- Выбором значений параметров состояния технологической среды (состава, давления, температуры), снижающих ее взрывопожароопасность.

Согласно п. 6.3.14 Правил взрывобезопасности, перечень контролируемых параметров, определяющих взрывоопасность процесса в каждом конкретном случае, определяется именно Разработчиком процесса.

4.6. Ответственность Проектной организации

Ответственность *Проектной организации* заключается в выборе рациональных условий взрывобезопасности технологической системы, которые согласно п. 3.4.2 Правил обеспечиваются:

- Рациональным выбором технологической системы с минимально возможными относительными энергетическими потенциалами входящих в нее технологических блоков, которые определяются на стадии проектирования;
- Разделением отдельных технологических операций на ряд процессов или стадий (смешение компонентов в несколько стадий, разделение процессов на реакционные и массообменные и т.п.) или совмещением нескольких процессов в одну технологическую операцию (реакционный с реакционным, реакционный с массообменным и т.д.), позволяющим снизить уровень взрывоопасности;
- Введением в технологическую систему дополнительного процесса или стадии с целью предотвращения образования взрывопожароопасной среды на последующих операциях (очистка от примесей, способных образовывать взрывопожароопасные смеси или повышать степень опасности среды на последующих стадиях, и т.п.);
- Надежным энергообеспечением.

Ответственность за разделы проекта и технологического регламента, содержащие перечень и описание последовательности срабатывания блокировок, значения предаварийных и предупредительных уставок несет *Проектная организация.*

С учетом п. 6.3.6 ПБ, *Проектной организацией* в проектной документации, технологических регламентах и перечнях блокировок для объектов с технологическими блоками всех категорий взрывоопасности наряду с уставками срабатывания

системы защиты должны указываться критические значения параметров, при которых возникает непосредственная угроза взрыва или разгерметизации технологического оборудования.

Регламентирование способов и средств, исключающих выход параметров за регламентированные граничные значения *(по мотивам пункта 3.4 ПБ).* Способы и средства, исключающие выход параметров за регламентированные граничные значения, приводятся в исходных данных на проектирование *Разработчиком процесса*, и устанавливаются в проектной документации и технологическом регламенте *Проектной организацией.*

Разработка последовательности срабатывания системы защиты. Согласно п. 5.6.2 ПБ, выбор методов и средств, разработка последовательности срабатывания системы защиты, локализации и предотвращения аварий по результатам анализа возможного развития аварийных ситуаций, и с учетом особенностей технологического процесса и категории взрывоопасности технологических блоков, входящих в объект, определяются *Проектной организацией* в проектной документации и в технологическом регламенте.

4.7. Ответственность Разработчика АСУТП

Для взрывоопасных технологических процессов всех категорий взрывоопасности должны предусматриваться системы противоаварийной защиты, предупреждающие возникновение аварийной ситуации на процессе, и обеспечивающие программно-управляемый перевод процесса в безопасное состояние по предопределенной последовательности операций, либо безопасный аппаратный останов.

Технические характеристики распределенной системы управления (РСУ) и противоаварийной защиты (ПАЗ) должны соответствовать скорости изменения значений параметров процесса в требуемом диапазоне (класс точности приборов, инерционность систем измерения, диапазон измерения и т.п.).

Системы противоаварийной защиты, как правило, включаются в общую автоматизированную систему управления технологическим процессом (АСУТП). Однако формирование сигналов для ее срабатывания должно базироваться не на *"регламентированных предельно допустимых значениях па-*

*раметров, определяемых свойствами обращающихся веществ и характером процесса*как сказано в пункте 3.11 ПБ, а на предусмотренных регламентом **предаварийных** граничных значениях. Технические и алгоритмические решения для эффективного управления и защиты технологических процессов на объектах с технологическими блоками всех категорий взрывоопасности разрабатываются и обосновываются Разработчиком АСУТП по согласованию с Организацией-заказчиком на основе проектной документации, и Технического задания на создание АСУТП.

4.8. Ответственность Организации-заказчика АСУТП

Организация-заказчик несет ответственность за подготовку и предоставление исходных данных на разработку проекта автоматизации, проверку соответствия технических решений Техническому заданию на создание АСУТП, приемку технического и рабочего (технорабочего) проектов, эксплуатацию и обслуживание АСУТП в соответствии с технологическим регламентом, проектной и эксплуатационной документацией.

4.9. Проведение конкурса (тендера) по выбору оборудования АСУТП

Выбор конкретного поставщика оборудования и программных средств РСУ и ПАЗ, а также разработчика АСУТП должен осуществляться на конкурсной основе с участием нескольких (как правило, 3 ± 1) поставщиков и разработчиков. Конкурс (тендер) на создание АСУТП проводит организация-заказчик.

При выборе генпроектировщика, разработчика, поставщика необходимо иметь дело с такими организациями, которые могут выполнить весь спектр работ в своей зоне ответственности, подтвержденный на аналогичных производствах, и ориентироваться на долговременное сотрудничество.

Важно остановить свой выбор на компании, имеющей многолетнюю устойчиво положительную репутацию на отечественном и мировом рынке автоматизации в нефтегазодобывающей, химической, нефтехимической и нефтеперерабатывающей отрасли, и способной предложить оборудование и

услуги, соответствующие уровню предъявляемых требований и по технике, и по опыту выполнения аналогичных проектов, и по экономической привлекательности предложения.

4.10. Общие требования к РСУ

РСУ должна обеспечивать:

- Автоматизированный сбор и первичную обработку технологической информации.
- Контроль состояния технологического процесса, сигнализацию при выходе технологических показателей за установленные границы.
- Автоматизированное управление технологическим процессом.
- Представление информации на операторских станциях в виде графиков, мнемосхем, гистограмм, таблиц и т.п.
- Автоматическую обработку, регистрацию и хранение текущей информации, вычисление усредненных, интегральных и удельных показателей.
- Формирование отчетов и рабочих (режимных) листов по утвержденной форме за определённый период времени, и вывод их на печать по расписанию и по требованию.
- Получение данных ПАЗ, и регистрацию ее срабатывания.
- Передачу данных в общезаводскую сеть.
- Защиту баз данных и программного обеспечения от несанкционированного доступа.
- Диагностику и выдачу сообщений по отказам всех элементов комплекса технических средств - с точностью до модуля.

Сигнализация состояния технологического процесса.

На станциях технолога-оператора должна быть предусмотрена сигнализация нарушений предупредительных и предаварийных уставок, выражаемая звуком и изменением цвета. Предупредительная и предаварийная сигнализация параметров, определяющих взрывоопасность технологического процесса, должна предусматриваться для объектов с технологическими блоками всех категорий взрывоопасности.

В обязательном порядке должна предусматриваться регистрация времени появления и исчезновения сигнализации.

Защита от ошибок персонала. Все действия персонала по взаимодействию с РСУ должны быть защищены от возможных ошибок. РСУ должна исполнять только те действия, которые описаны в документации на систему. Любые ошибочные действия персонала по управлению процессом должны игнорироваться, если они отличаются от объявленных в документации, или не соответствуют уровню полномочий персонала, и регистрироваться в журнале событий.

4.10. Общие требования к системе ПАЗ

Методы и средства защиты технологических объектов выбираются на основе анализа опасностей и условий возникновения и развития предаварийных и аварийных ситуаций, особенностей технологических процессов и аппаратурного оформления.

Система безопасности (ПАЗ) должна обеспечивать:

- Сбор аналоговой и дискретной информации от датчиков технологических параметров, и дискретных параметров состояния исполнительных механизмов, а также дискретных параметров ДВК, ПДК, и состояния аварийной вентиляции.
- Выделение достоверной входной информации.
- Анализ и логическую обработку входной информации.
- Автоматическую выдачу сигналов двухпозиционного управления на исполнительные механизмы.
- Дистанционное управление исполнительными механизмами со станции технолога-оператора РСУ при условии санкционированного доступа, либо со специальной оперативной панели ПАЗ.
- Передачу оперативной информации от системы ПАЗ в РСУ для сигнализации, регистрации и архивирования (отклонение параметров, срабатывание исполнительных механизмов ПАЗ, и т.п.).
- Выделение первопричины останова технологического процесса.
- Самодиагностику состояния технических средств системы ПАЗ.

Выбор конкретного поставщика системы защиты. Выбор архитектуры системы безопасности и ее элементов осуществляется исходя из категории взрывоопасности технологического объекта, а также требований по эксплуатации, обслуживанию и ремонту в течение всего межремонтного пробега технологического объекта. Выбор конкретного поставщика оборудования системы ПАЗ организация-заказчик осуществляет по результатам конкурса (тендера).

Особенности объектов III категории взрывоопасности. Для объектов III категории взрывоопасности функции защиты технологического процесса могут быть реализованы на стандартных **контроллерах** РСУ при выполнении следующих условий:

- Система защиты реализована на физически выделенных из РСУ (но не из АСУТП) технических средствах;
- Система защиты имеет резервирование по всем основным компонентам:
  - Модули ввода-вывода;
  - Платы контроллеров;
  - Сетевые интерфейсы;
  - Источники питания.

Резервирование датчиков и исполнительных элементов. Надежность выполнения функций измерения и защиты для переменных, определяющих взрывоопасность процесса, на взрывоопасных объектах обеспечивается:

- Использованием полевого оборудования, имеющего специальный допуск на применение в системах, обеспечивающих безопасность процесса;
- Установкой дополнительных датчиков в соответствии с категорией взрывоопасности и типом технологического процесса;
- Установкой дополнительных исполнительных элементов;
- Наличием системы автоматизированного обслуживания полевого оборудования - *Plant Asset Management System;*
- Контролем значений технологически связанных параметров.

В системах ПАЗ запрещается мультиплексирование входных параметров, определяющих взрывоопасность процесса.

Значения уставок системы защиты. Находятся под ответственностью *Проектной организации.* Значения уставок срабатывания системы защиты определяются с учетом погрешностей измерительных устройств, быстродействия системы, возможной скорости изменения параметров, и категории взрывоопасности технологического блока. Значения уставок определяются *Проектной организацией* и приводятся в проектной документации (технологическом регламенте).

Надежность и время срабатывания систем безопасности. Надежность и время срабатывания систем противоаварийной защиты обосновываются Разработчиком АСУТП на основе требований технологической части проекта. При этом учитывается категория взрывоопасности технологических блоков, входящих в объект, и время развития возможной аварии. Время срабатывания системы защиты должно быть гарантированно меньше времени, необходимого для перехода параметра от предаварийного до критического значения. Надежность систем безопасности должна обеспечивается:

- Аппаратурным резервированием необходимого типа;
- Информационной, функциональной и временной избыточностью;
- Наличием систем оперативной и автономной диагностики.

Достаточность резервирования и его тип определяются и утверждаются на специальном совещании по безопасности с участием Проектной организации, Разработчика АСУТП и Организации-заказчика.

Резервирование электропитания. Электропитание оборудования АСУТП, включая и полевое оборудование КИПиА, должно обеспечиваться от двух независимых источников. На случай отключения основных источников электроэнергии в качестве третьего независимого источника должен быть предусмотрен источник бесперебойного питания (UPS), способный обеспечить электропитанием полевое оборудование КИПиА и основное оборудование РСУ и ПАЗ, чтобы произвести перевод технологического объекта в безопасное состояние в течение наперед заданного интервала времени.

4.12. Эксплуатационные ограничения

Запрещение на ведение технологических процессов и работу оборудования с неисправными или отключенными системами контроля, управления и защиты. Согласно **ПБ** 09-540-03 п. 6.9.2, запрещается ведение технологических процессов всех категорий взрывоопасности, а также работа оборудования с неисправными или отключенными системами контроля, управления и защиты.

Кратковременное отключение защиты. Допускается в исключительных случаях для непрерывных процессов по **письменному распоряжению *главного инженера данного производства / установки*** (вместо руководителя предприятия по п. 6.9.3 ПБ) кратковременное отключение защиты по отдельному параметру, и только в дневную смену. При этом разрабатываются организационно-технические мероприятия и план организации работ, обеспечивающие безопасность технологического процесса и производства работ. Продолжительность отключения должна определяться планом организации работ.

Если деблокирование параметров ПАЗ производится через РСУ, то проведение этой операции допускается только с инженерной станции РСУ, и только для специально определенного персонала. При этом на РСУ должна производиться регистрация:

- *Шифра (позиции) точки ввода-вывода деблокированного сигнала;*
- *Времени отключения;*
- *Времени восстановления.*

Также по ключу / паролю регистрируется работник, непосредственно проводивший данную операцию.

Установка деблокирующих ключей. На объектах с блоками всех категорий взрывоопасности для обеспечения пуска, останова, регламентных переключений оборудования, а также оперативного технического обслуживания системы защиты допускается установка деблокирующих ключей в физических и программных схемах системы противоаварийной защиты. Однако количество таких ключей *должно быть не минимальным*, как сказано в пункте 6.3.12 ПБ, а таким, что бы было обеспечено выполнение перечисленных функций.

При этом должна предусматриваться регистрация всех случаев изменения состояния деблокирующих ключей, времени начала, окончания, а также регистрацию работника, осуществившего эти операции.

Замена элементов АСУТП. На период замены элементов АСУТП предусматриваются меры и средства, обеспечивающие безопасное проведение процесса в ручном режиме. В технологическом регламенте и инструкциях определяются стадии процесса или отдельные параметры, управление которыми в ручном режиме не допускается (п. 6.9.4).

Запрещение на использование приборов, устройств и других элементов, отработавших свой назначенный срок службы:

Согласно п. 6.9.5 ПБ 09-540-03, для объектов с технологическими блоками всех категорий взрывоопасности в системах контроля, управления и ПАЗ запрещается использовать приборы, устройства и другие элементы, отработавшие свой назначенный срок службы.

4.13. Индикация и сигнализация на оперативных панелях и в РСУ

Дополнительные оперативные панели ПАЗ. Кроме средств визуализации РСУ, для систем ПАЗ необходимо предусматривать панели, которые оснащаются средствами для оперативной выдачи команд управления блокирующими устройствами, операциями пуска-останова, и сигнализацией состояния блокировок, исполнительных органов и источников энергопитания.

Световая и звуковая сигнализация о загазованности воздушной среды. Во взрывоопасных помещениях и снаружи перед входными дверями предусматривается световая и звуковая сигнализация о загазованности воздушной среды.

Для контроля загазованности в производственных помещениях, рабочей зоне открытых наружных установок должны устанавливаться средства автоматического газового анализа с сигнализацией предельно допустимых концентраций.

Все случаи загазованности должны фиксироваться в АСУТП *(а не просто регистрироваться приборами, как сказано в пункте 6.4.1 ПБ 09-540-03).*

4.14. Требования к метрологическому обеспечению

Метрологическое обеспечение измерительных систем (ИС) должно удовлетворять требованиям закона Российской Федерации №4871-1 "Об обеспечении единства измерений", ГОСТов и правил по метрологии.

Метрологическое обеспечение измерительных систем должно соответствовать ГОСТ Р 8.596-2002 ГСИ. *"Метрологическое Обеспечение измерительных систем. Основные положения*Должны быть предоставлены следующие сведения и документы:

- Назначение ИС, и сведения об ее использовании в сфере (или вне сферы) Государственного метрологического контроля и надзора;
- Сертификат об утверждении типа ИС, описание типа ИС, методику поверки, - если они используются в сфере Государственного метрологического контроля и надзора;
- Сведения об измеряемых величинах и их характеристиках;
- Перечни измерительных каналов и нормы их погрешностей;
- Условия измерений;
- Условия метрологического обслуживания.

Все методики измерения, используемые в сфере государственного метрологического контроля и надзора, должны быть аттестованы.

В спецификацию оборудования АСУТП должны быть включены специальные технические и программные для калибровки измерительных каналов. Для измерительных каналов ИС должны быть представлены инструкции по поверке (калибровке), утвержденные в установленном порядке. Все метрологические характеристики измерительных и управляющих модулей должны быть представлены фирмой-изготовителем в документации на технические и программные средства. Для подтверждения выбранных метрологических характеристик согласно ГОСТ 8.009-84 *"Нормирование и использование метрологических характеристик средств измерений* испытания СИ и ИС должны проводиться по ПР 50.2.009-94 ГСИ *"Порядок проведения испытаний и утвер-*

ждения типа средств измерений". Пределы значений погрешности измерительных каналов не должны превышать норм технологического регламента. Измерительные каналы системы могут использоваться для целей контроля параметров только после их калибровки на объекте эксплуатации.

4.15. Международный подход к системе классификации рисков

Проблема соответствия отечественных категорий взрывоопасности международным классам и уровням безопасности. На первый взгляд, методика МЭК оценки интегрального уровня безопасности SIL через вероятность отказа системы безопасности никак не связана с методикой расчета категории взрывоопасности через потенциал взрывоопасности технологического блока (ПБ 09-540-03, Приложение 1). Тем не менее, решение существует.

Ключом к решению является уже упоминавшаяся в главе "Современная концепция безопасности" диаграмма рисков по немецким стандартам DIN V 19250 и DIN V VDE 0801. Классификация DIN класса требований к системе защиты по уровню опасности технологического процесса построена с глубоким пониманием существа проблемы, и заслуживает серьезного отношения. Стандарт DIN V 19250 устанавливает иерархию систем безопасности, соответствующих требованиям установленных классов АК *(AnforderungsKlasse),* начиная с АК 1, и заканчивая АК 8 (соответствующее английское сокращение - *Requirements Class -RC).* Стандарт рассматривает следующие факторы риска, свойственные технологическим процессам:

- Последствия аварии S,, / = 1,...4;
- Интенсивность (частота и время) нахождения в опасной зоне ***Aj, j = 1,2 ;***
- Возможность избежать опасность G_m, *m = 1,2;*
- Вероятность нежелательного события W_n, *n -1,...3* .

и на их основе определяет уровень допуска для системы, связанной с безопасностью (диаграмма рисков представлена на рис. 4.4).

Итоговый класс требований к системе безопасности определяется целочисленной функцией:

$$RC = RC(S,, A_{ff} G_m, W_n)$$

Легко убедиться, что создатели стандарта IEC 61508 без церемоний воспользовались диаграммой рисков DIN V 19250, поменяв на ней несколько букв, и сократив число классов (уровней) безопасности вдвое (см. рис. 4.5).

Параметры риска

10 ПОСЛЕДСТВИЯ АВАРИИ:
|S1 - Незначительные травмы
S2 - Серьезные травмы одного или нескольких человек, смерть одного человека
|S3 - Смерть нескольких человек
S4 - Катастрофические последствия
| большие человеческие потери

ФЧАСТОТА И ВРЕМЯ НАХОЖДЕНИЯ

A1 - От редкого до относительно частого
A2 - Частое или постоянное

ІФ ВОЗМОЖНОСТЬ ИЗБЕЖАТЬ ОПАСНОСТЬ;
f G1 - Возможно при определенных
| обстоятельствах
1 G2- Невозможно

^ВЕРОЯТНОСТЬ НЕЖЕЛАТЕЛЬНОГО
*** СОБЫТИЯ:**
- Крайне низкая
fW2 - Низкая
|W3 - Высокая

Диаграмма рисков по стандарту DIN V 19250

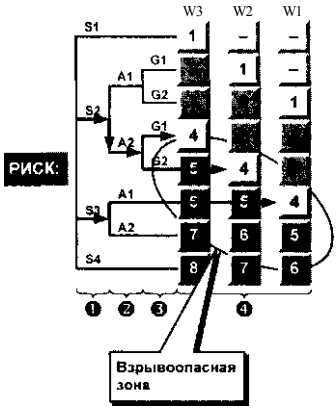


Рис. 4.4

В первую очередь обращает на себя внимание то обстоятельство, что 3 критических пути к наиболее простым одноканальным системам защиты 1oo1D класса RC 4 (на рис.4.4 отмечены стрелками) на самом деле приводят к постоянному существованию между двумя фатальными угрозами - S2 и S3:

- Серьезные травмы одного или нескольких человек, смерть одного человека.
- Смерть нескольких человек.

Из этого следует, что взрывоопасные процессы нефтегазодобывающих, нефтехимических и нефтеперерабатывающих производств не могут относиться к классу требований ниже RC4 - возможны человеческие жертвы в случае аварии.

Следовательно, при выборе системы защиты **для взрывоопасных объектов с блоками I и II категорий взрывоопасности необходимо ориентироваться на системы НЕ НИЖЕ 5-ГО КЛАССА,** а единственной степенью свободы является выбор из архитектур **1oo2D** или **2oo3.**

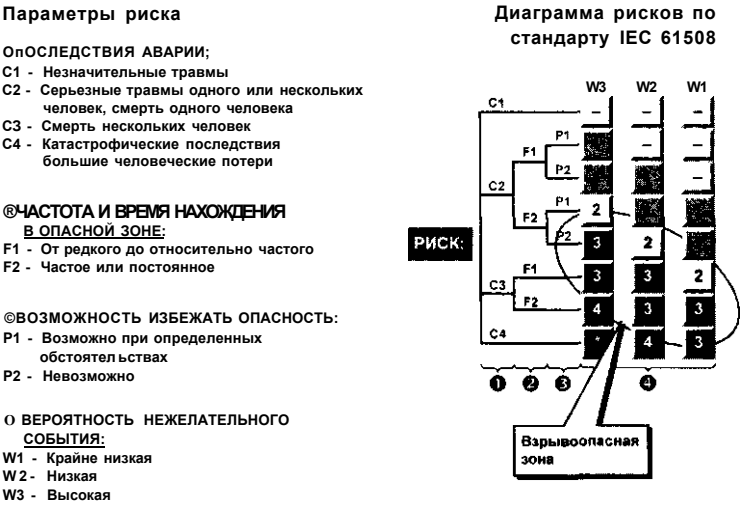


Рис. 4.5

Согласно диаграмме рисков по стандарту IEC 61508 (рис. 4.5), классам требований RC 5-6 стандарта DIN V 19250 ссоответствует уровень требований SIL 3.

Далее приводится результат анализа соответствия отечественных категорий взрывоопасности и

- Классов требований (Requirement Class - RC, AnforderungsKlasse - АК) по немецким стандартам DIN;
- Уровней безопасного допуска (Safety Integrity Level - SIL) по американским стандартам ISA;
- Уровней безопасного допуска SIL по стандартам Международной электротехнической комиссии (IEC).

Приводится Диаграмма соответствия, отражающая авторское понимание проблемы.

4.16» Диаграмма соответствия отечественных категорий взрывоопасности международным классам и уровням безопасности

Из диаграммы риска следует, что подавляющее большинство технологических процессов нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств относится к 4-6 классу требований по DIN V 19250, V VDE 0801 и 2-3 уровню SIL (IEC 61508, ISA 84.01-96) - возможны человеческие жертвы в случае аварии.

Таким образом, мы приходим к принципиально важному результату, а именно:

Классы RC 4 - 5 - 6 соответствуют нашим III - II -1 категориям взрывоопасности. Соответственно,
Уровень безопасности SIL 2 соответствует III категории взрывоопасности.
Уровень безопасности SIL 3 соответствует I - II категориям взрывоопасности.

Дополнительным подтверждением корректности нашего соответствия категорий **II-I** классам **RC 5-6** является принадлежность пары **RC 5-6** к одному общему уровню интегральной безопасности **SIL3.**

Примечание

Характерно, что несмотря на фактическую отмену стандарта DIN V 19250 и объявленный переход на стандарты Международной электротехнической комиссии IEC 61508 и 61511, в Германии продолжают пользоваться привычной классификацией АК и RC.

Полученные результаты сведены воедино в виде Диаграммы соответствия стандартов России, Германии, США и стандартов МЭК (см. таблицу 4.9).

Рекомендации по выбору конкретной архитектуры систем управления и защиты для взрывоопасных объектов приводятся в Таблице 4.10.

Строгое соблюдение жестких требований безопасности должно быть непременным условием построения АСУТП непрерывных взрывоопасных технологических процессов нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств.

Таблица 4.9

Соответствие отечественных категорий взрывоопасности зарубежным классам и уровням безопасности

		90	99,0 |	99,9 |	99,99 | 99,999 |
		0,1	0,01 |	0,001	0,0001 | 0,00001 |

Таблица 4.10

Применение различных архитектур систем безопасности в зависимости от категории взрывоопасности

Категория взрыво-опасности	RC	SIL	Архитектура системы	Пояснение
1m	4	2	Нерезервированные (1оо1) или резервированные (1оо2) входы	Периодическое тестирование входов. Входы могут быть аналоговыми или дискретными
			ПЛК 1оо1D, или Стандартные контроллеры РСУ	ПЛК с двумя центральными процессорами или резервированными модулями управления, Или (по согласованию с технадзором) - выделенное резервированное оборудование РСУ
			Нерезервированные (1оо1) выходы	Периодическое тестирование выходов
II	5	3	Резервированные (1оо2) входы	Оперативное тестирование входов Входы могут быть аналоговыми или дискретными
			Архитектуры ПЛК 1оо2D,2оо3	Полностью резервированные (дублированные, троированные) системы
			Нерезервированные (1оо1) выходы	Оперативное тестирование выходов
1	6	3	Резервированные (1оо2 или 2оо3) входы	Оперативное тестирование входов Голосующие входы - аналоговые
			Архитектуры ПЛК 1оо2D, 2оо3	Полностью резервированные (дублированные, троированные) системы
		J .	Резервированные (1оо2) выходы	Оперативное тестирование выходов

4.17. Механизмы деградации систем безопасности и действия при отказах

Для ряда технологических процессов собственно сама процедура аварийного останова может представлять значительную опасность, и должна проводиться по точно определенной последовательности операций с контролем исполнения всех промежуточных команд и действий.

В подобных случаях уменьшение уровня безопасности процесса, произошедшее за счет кратковременной одноканальной работы, должно быть компенсировано за счет дополнительных мер.

Например, во время восстановления исходной конфигурации процесс контролируется технологическим персоналом с особой тщательностью, и при первых признаках опасности переводится в безопасное состояние.

В таблице 4.11 представлены механизмы деградации различных архитектур промышленных систем безопасности, и допустимые действия при частичном или полном отказе системы, - по мнению TUV. В таблице ясно виден водораздел между двумя категориями систем:

1. **1oo2D и 2oo3 - 5 - 6 класс**
2. **Все остальное - 4 класс.**

Как мы помним, согласно IEC 61508 представленные ограничения относятся не только к центральной части системы - ПЛК, но к целостным функциям безопасности, включая и полевое оборудование.

Разработчик системы безопасности должен быть осведомлен о существующих ограничениях на применение конкретных архитектур систем безопасности, в особенности в тех случаях, когда немотивированные остановы процесса не только нежелательны, но и представляют серьезную опасность.

Знание особенностей работы той или иной архитектуры систем безопасности в сочетании с пониманием требований безопасности технологического процесса позволяет сделать правильный выбор, обеспечить необходимый запас времени на восстановление системы, и избежать экономических по-iepb.

Таблица 4.11

Механизмы деградации промышленных систем безопасности и действия при отказах

Исходная структура Системы (нормальное состояние)	Структура и действие Системы при наличии единичного отказа оборудования	Структура и действие Системы при наличии двух отказов оборудования	Сертификация TUV и категория взрывоопасности
2oo3	1oo2, Восстановление исходной конфигурации с ограничением по времени, либо программно-управляемый останов	Аппаратный останов процесса	Аттестована по: 5-6 классу DIN, 3 уровню SIL 1, II категория взрывоопасности
1oo2D	1oo1D, Восстановление исходной конфигурации с ограничением по времени, либо программно-управляемый останов	Аппаратный останов процесса	Аттестована по: 5-6 классу DIN, 3 уровню SIL 1, II категория взрывоопасности
1oo1D	Аппаратный останов процесса		Аттестована по: 4 классу D1N, 2 уровню SIL III категория взрывоопасности
1oo2	Аппаратный останов процесса		Аттестована по 4 классу DIN, 2 уровню SIL III категория взрывоопасности

4.18. Временные ограничения на применение ПЛК

Стандарты DIN V 19250, IEC 61508, ISA 84.01 не предписывают каких либо конкретных рекомендаций по допустимому времени пребывания систем безопасности в неполной конфигурации в случае частичной потери оборудования.

Поэтому максимально разрешенный интервал одноканальной работы должен в каждом конкретном случае определяться индивидуально - в зависимости от специфики конкретного процесса. TUV устанавливает нижеследующие ограничения на применение различных архитектур программируемых логических контроллеров в неполной конфигурации.

III категория взрывоопасности - 4 класс требований RC, **уровень SIL2.** При использовании дублированных центральных процессоров, модулей ввода-вывода, сетевых интерфейсов, источников питания разрешается использовать расширенный вариант системы 1oo1D. При отказе одного из центральных процессоров - немедленный аппаратный останов процесса. В настоящей работе предлагается следующий далее альтернативный вариант.

Для объектов III категории взрывоопасности функции защиты технологического процесса могут быть реализованы на **стандартных контроллерах РСУ** при выполнении следующих условий:

1. Система защиты построена на физически выделенных из РСУ (но не из состава АСУТП!) технических средствах (выделенные стойки ПАЗ);
2. Система защиты имеет резервирование по всем основным компонентам:
   - Модули ввода-вывода;
   - Платы контроллеров;
   - Сетевые интерфейсы;
   - Источники питания.

Данное техническое решение в обязательном порядке согласовывается с территориальным органом Ростехнадзора при оформлении Технического задания на создание АСУТП.

I и II категория взрывоопасности - 5 и 6 класс требований RC, **SIL3.** Стандарты общего назначения IEC 61508, DIN 19250 и DIN 0801 не дают конкретных значений или рекомендаций по времени работы в неполной конфигурации для

случаев обнаружения отказов в системе, и последовавшей в результате этого отказа деградации системы. Максимальный интервал времени одноканальной работы для резервированных систем, который устанавливает TOV в своих общих рекомендациях "*Product Independent Conditions and Restrictions",* www.tuv-fs.com /plcgen4.htm, если оперативного восстановления исходной конфигурации системы не произведено, таков:

- Для уровня требований АК5 (II категория взрывоопасности по предлагаемой в данной работе классификации) в одноканальном режиме работы - останов после 72 часов работы в контролируемом режиме, то есть под наблюдением *(supervised operation).*
- Для уровня требований АК6 (I категория взрывоопасности по предлагаемой в данной работе классификации) в одноканальном режиме работы - останов после 1 часа работы в контролируемом режиме, то есть под наблюдением *(supervised operation).*

При этом подчеркивается, что в одноканальном варианте работа системы возможна только в режиме под наблюдением.

Вместе с тем к каждой системе TUV подходит индивидуально (см. например, отчет TUV U 0012 40001 003, стр.11-15):

Для 5 и 6 класса требований (объекты I и II категории взрывоопасности - Ю. Ф.) - восстановление системы в течение интервала времени, определенного для конкретной системы на основе представленных производителем данных о вероятности опасного отказа, либо программно-контролируемый останов не более чем через 72 часа.

Максимальный интервал времени работы в неполной конфигурации для системы 2оо3, который устанавливает TUV для 5-6 класса требований (отчет TUV 968/EZ 105.03/01, стр.8):

При отказе одного канала — восстановление конкретной системы в течение заданного для нее производителем оборудования интервала времени, при отказе двух каналов - останов процесса через 1 час.

Таким образом, общее правило состоит в следующем:

Постоянная одноканальная работа системы защиты для объектов I и II категории взрывоопасности запрещена.

Сказанное означает, что для объектов **I и II категории взрывоопасности** при частичной потере исходной конфигурации программно-управляемая защита процесса возможна только для архитектур **2oo3 и 1oo2D,** причем с резервированием сенсоров и исполнительных устройств, определяющих безопасность процесса.

Время восстановления работоспособности системы безопасности после ее полного отказа с последующим остановом процесса. Стандартами DIN, ISA, IEC никак не регламентируется, хотя стандарт IEC 61508 оперирует интервалом 8-24 часа. TUV также не дает никаких конкретных рекомендаций. Исходя из реальных возможностей по времени:

- Определения причин отказа системы защиты,
- Времени замены дефектных компонентов системы защиты,
- Времени на пробный запуск и тестирование системы,

предлагается определить в качестве ориентира для объектов всех категорий взрывоопасности интервал в 8 часов на восстановление готовности системы безопасности к выполнению своих функций, и к запуску технологического процесса.

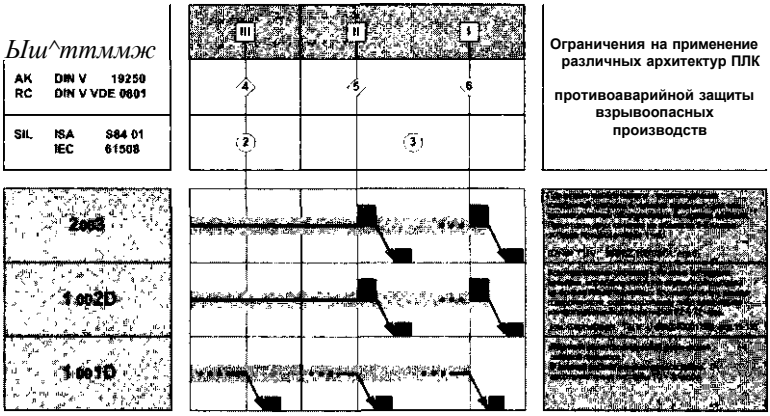
Авторское понимание ограничений TUV на применение различных архитектур программируемых логических контроллеров в сочетании с предложенным взаимно однозначным соответствием классов и уровней допуска отечественным категориям взрывоопасности (таблица 4.9) представлено в таблице 4.12. Еще раз: очень важно понимать принципиальную, границу, разделяющую 1oo1D и системы с архитектурами 1oo2D и 2oo3:

- Для одноканальных систем частичный отказ означает одновременно жесткий физический останов процесса.
- Системы с резервированием позволяют в случае частичного отказа провести оперативную замену отказавшего модуля, либо произвести программно-управляемый останов процесса.

Данное качество резервированных систем является определяющим при выборе архитектуры систем управления и защиты непрерывных технологических процессов для нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств.

Таблица 4.12

Ограничения на применение различных архитектур промышленных систем противоаварийной защиты для взрывоопасных производств



Важное замечание

Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор) при выдаче Разрешений на применение технических устройств для создания автоматизированных систем управления и противоаварийной защиты не делает подразделения по категориям взрывоопасности объекта.

Таким образом, Разрешение Ростехнадзора подразумевает право на применение технических устройств на объектах всех категорий взрывоопасности.

Поэтому технические решения по выбору конкретной архитектуры систем защиты и управления для данного технологического объекта должны быть обоснованы в Техническом задании на создание АСУТП.

Техническое задание на создание АСУТП в обязательном порядке согласовывается с территориальным органом Ростехнадзора. *И самое главное:*

Вне зависимости от наличия и содержания западных сертификатов, разрешение Ростехнадзора имеет безоговорочный приоритет.

4.19. Резервирование полевого оборудования

Все сказанное по поводу резервирования центральной части систем безопасности - ПЛК - в полной мере относится и к полевому оборудованию. Согласно IEC 61508, минимальная смысловая единица системы управления и защиты - функция, или контур безопасности. Под контуром безопасности (*<Safety Loop)* в самом тривиальном случае понимается цепочка элементарного контура управления и защиты:

Сенсор - ПЛК - Исполнительное устройство.

Становится понятным, почему системы безопасности с не резервированными сенсорами и исполнительными устройствами аттестуются TUV не выше 4 класса защиты DIN, и 2 уровня безопасности SIL независимо от архитектуры ПЛК, то есть имеют право на существование только на объектах III категории взрывоопасности.

Поэтому нет особого смысла на объектах III категории взрывоопасности с одним сенсором и одним исполнительным устройством в каждом канале ставить специализированные системы loo2D или 2oo3. В данном случае вполне можно обойтись резервированным оборудованием того же типа, которое используется для реализации функций РСУ.

Таким образом, для объектов III категории взрывоопасности функции защиты технологического процесса могут быть реализованы на стандартных контроллерах РСУ при выполнении следующих условий:

- Система защиты реализована на специально выделенных аппаратных средствах;
- Система защиты имеет резервирование по всем основным компонентам:
  - Модули ввода-вывода
  - Платы контроллера
  - Сетевые интерфейсы
  - Источники питания.

Как и все решения, связанные с применением технических устройств на взрывоопасных объектах, данное техническое решение в обязательном порядке согласовывается с территориальным органом Ростехнадзора при оформлении Технического задания на создание АСУТП.

4.20. Выбор архитектуры систем безопасности

Архитектура системы оказывает основное влияние на общий уровень безопасности. Архитектура также определяет надежность системы. Ниже приводятся некоторые решения, которые необходимо сделать при определении архитектуры:

- Выбор идентичного или альтернативного резервирования для сенсоров, логических решающих устройств, и исполнительных элементов;
- Выбор избыточности для источников и блоков питания;
- Выбор компонентов интерфейса оператора (например, станция технолога-оператора, оперативные панели системы противоаварийной защиты, кнопки, извещатели) и метод взаимосвязи с системой защиты;
- Выбор сопряжений между системой защиты и другими системами, например, РСУ, и метод доступа (например, "*только чтение" яш "чтение /запись").*

Архитектуры, которые могут удовлетворять требованиям взрывобезопасности различного уровня, включают нижеследующие конфигурации.

Для объектов III категории взрывоопасности (SIL2 и RC4) от системы требуется наличие самодиагностики, сторожевого таймера. Дополнительно не исключается возможность резервирования сенсоров, и с одним конечным управляющим устройством.

Приемлемый вариант по согласованию с территориальным органом Ростехнадзора - выделенное резервированное оборудование РСУ с резервированием модулей ввода-вывода, модулей управления, сетевых плат, источников питания.

Для объектов I и II категории взрывоопасности (SIL3 и RC 5-6) классический выбор - системы защиты с архитектурами loo2D и 2oo3 с дублированием сенсоров и управляющих устройств.

Для объектов всех категорий взрывоопасности настоятельно рекомендуется применение системы обслуживания полевого оборудования - *Plant Asset Management System.* Для объектов I и II категории взрывоопасности это должно быть обязательное требование.

Существует множество поставщиков оборудования, "инжиниринговых" фирм, собственных разработчиков предприятия, которые способны заложить контроллер, который, судя по рекламным проспектам, выставкам и презентациям, вроде бы вполне отвечает требованиям безопасности. Но при этом не поясняется, что под безопасностью, понимается, в том числе, и ложное срабатывание.

Например, одноканальная система может 10 раз в месяц останавливать процесс по ложной причине, и отвечать требуемому классу безопасности, обеспечивая "безаварийный", ничем не контролируемый физический останов. И при этом мгновенно перезапускаться и демонстрировать потрясающую "готовность" к новому останову процесса! Более того, стереотип мышления, навязанный неуемной дилетантской или преднамеренной рекламой достоинств ПЛК, приводит к тому, что заказчик совершенно упускает из виду, либо оставляет "на потом" решение вопросов, которые как раз-то и являются первостепенными - **модернизация полевого оборудования.** Важно понимать следующее:

Надежность и готовность системы безопасности означают, что система может находиться в режиме *on-line*, будучи устойчивой к одному или нескольким отказам, и при этом сохраняет способность производить необходимые действия для безопасного **программно-управляемого останова** процесса, - в то время как отказ элемента системы будет идентифицирован, и будет произведена замена дефектного оборудования. При выборе конкретной архитектуры системы безопасности разработчик должен определить полноту диагностического охвата, промежутки времени между испытаниями, резервирование и т.п. и оценить **конкретную конфигурацию оборудования с обязательным учетом полевой части системы** на соответствие требуемому уровню безопасности.

Хорошо спроектированные системы для решения критических задач безопасности находят **баланс между безопасностью и надежностью** посредством выбора адекватного резервирования, и высоким уровнем диагностики полевого оборудования и программируемых логических устройств. Целостность системы после запуска обеспечивается правильным выбором частоты и глубины тестирования.

Но самое главное - квалифицированным персоналом.

4.21. Западные документы специального допуска

Хотя во всех европейских странах и на американском рынке применение программируемых электронных систем в качестве систем противоаварийной защиты жестко регламентировано существующими национальными и международными стандартами, и требует специальной сертификации для определения допуска к применению, тем не менее, возможность их применения для конкретного технологического процесса должна быть тщательно проверена. Жесткие требования связаны со спецификой электронной техники, которая обеспечивает функциональные преимущества перед щитовыми и релейными схемами, но имеет гораздо более высокую цену отказа. От поставщиков западного оборудования систем ПАЗ необходимо требовать документы, подтверждающие право использования на аналогичных технологических объектах с учетом категории взрывоопасности:

- Сертификат безопасности TUV, определяющий **предварительный** уровень допуска на систему безопасности по стандарту 1EC 61508;
- Технический отчет TUV, определяющий технические требования при проектировании, программировании и эксплуатации для заданной конфигурации системы;
- Руководство по безопасности *(Safety Manual).*

Еще раз укажем, что очень важно понимать следующее:

Когда поставщик импортного оборудования гордо заявляет, что его "система" имеет сертификат TUV на работу по уровню SIL3 (а какой же еще?!), то вы должны ясно понимать, что в данном случае речь идет всего лишь о разрозненном наборе модулей для данного брэнда - по одной штуке каждого типа. Кроме модулей, проверке и сертификации подлежит программное обеспечение на минимально необходимой для этого конфигурации системы, и соответствующая системная документация.

В лучшем случае вы получаете следующие документы:

- *Certificate,*
- *List of approved modules,*
- *Safety Reference Manual.*

Вы сами можете в этом легко убедиться, если наберете http://www.tuv-fs.com/plclist.htm, и выберете любую из пред-

ставленных торговых марок. Повторяю: именно торговых марок, брэндов, шильдиков, а вовсе не некую базовую, или потенциально возможную, или какую-то еще систему, а тем более уж никак не какую-либо конкретную конфигурацию. Да и вообще у ТЮФа ни о какой конфигурации и речи нет. Поэтому для нашего потребителя речь может идти только о **потенциальной** возможности того разрозненного оборудования, которое проходит под данным брендом, соответствовать заявленному уровню. И все. Поэтому от генподрядчика должны быть затребованы дополнительные данные, подтверждающие право использования данной конфигурации оборудования на данном технологическом объекте:

- Послужной список практической реализации системы с указанием потребителей, даты внедрения, и периода эксплуатации каждой из систем;
- Процедуры для выбора системы под конкретные применения, и варианты применения;
- Процедуры для выявления отказов, их регистрации, и устранения.

При закупке импортного оборудования наличие сертификата на право использования данного оборудования на объектах того или иного класса взрывоопасности **теоретически** позволяет использовать это оборудование как законченное изделие, удовлетворяющее определенному уровню требований, поскольку предварительные расчеты, испытания и проверки проведены, и доступны для потребителя. Кроме того, заказчик может быть уверен, что предоставленные данные по надежности системы были проверены независимой третьей стороной. Однако важно помнить, что требования IEC 61508 установлены для всего контура безопасности - от датчика до клапана, и степень соответствия этим требованиям должна быть проверена для каждого конкретного применения.

Наиболее значимым документом сертифицированной продукции является Технический отчет *(Safety Manual)*. Данный отчет содержит важнейшую информацию от ограничений на использование до описания всех уровней самодиагностики, а также статистические данные по надежности - по интенсивности отказов и среднему времени наработки на отказ. Дополнительно, в отчете даются конкретные рекомендации по периодичности тестирования элементов системы.

Заданный класс требований может повлиять на выбор типа и количества сенсоров и исполнительных устройств - для контроля критических параметров эти устройства должны быть зарезервированы. При условии, что основные проектные решения по резервированию датчиков и исполнительных механизмов, а также по схемам блокировок уже сделаны проектной организацией, выбор контроллеров для системы безопасности может показаться не слишком сложным.

Например, в США задание класса требований вообще является закулисным, или, как у них принято говорить, "корпоративным" решением, то есть результатом внутренней договоренности. Может быть потому США и имеют по данным межправительственной организации ООН по экономическому сотрудничеству и развитию (OECD) самый высокий в мире уровень аварийности на своих предприятиях.

Лучше, если система защиты и ее конфигурация будет выбираться не в приватных кабинетах, а на специальном совещании с участием технических специалистов Генпроектировщика, Поставщика, Разработчика, Заказчика и Проектной организации. При определении класса требований должны приниматься в расчет все аспекты безопасности технологического процесса, в том числе такие, как:

- Допустимое время реакции системы;
- Требования к надежности оборудования;
- Уровень оперативной и автономной диагностики;
- Состав и содержание документации;
- Опыт применения на объектах аналогичного класса.

4.22. Простейшая процедура предварительного выбора

Простейшая процедура предварительного выбора требуемой системы безопасности заключается в следующем:

- В соответствии с категорией взрывоопасности объекта и с учетом временных ограничений на работу в неполной конфигурации определить по таблицам 4.9-4.12 соответствующий класс требований и интегральный уровень безопасности системы.
- При выборе поставщика зарубежных систем безопасности проверить наличие сертификата TUV на требуемый класс системы, и Технического отчета.

- Выбирать тех поставщиков и разработчиков, которые имеют достаточный опыт и репутацию в проектировании систем безопасности.
- Для обеспечения интегрального уровня безопасности система защиты должна быть построена соразмерно, то есть иметь не только резервирование необходимого типа для основного оборудования АСУТП, но также и для сенсоров, и для исполнительных элементов, определяющих безопасность процесса.

При выборе зарубежного поставщика оборудования взаимосвязь между отечественной Категорией взрывоопасности, классом RC и уровнем SIL чрезвычайно важна, и не должна упускаться:

Представленное в таблице 4.9 соответствие предназначено в качестве основы для адекватного выбора сертифицированного оборудования эффективных систем безопасности.

Вместе с тем, необходимо отдавать себе отчет, что выбор, сделанный таким тривиальным путем, можно сказать, на глазок, серьезно ослабляет уверенность в адекватности выбора.

В работе с потенциальным поставщиком и разработчиком заказчик имеет полное право воспользоваться поддержкой отечественных нормативных документов, и сослаться на требования ГОСТ 34.601, 34.602, ГОСТ 24.701, и потребовать подтверждения заявленных характеристик надежности **в виде конкретных расчетов параметров надежности для конкретного применения.**

За последние годы появились наши вполне добротные документы по анализу рисков и оценке последствий отказов:

- РД 03-418-01 *"Методические указания по проведению анализа риска опасных производственных объектов",* основанные на анализе деревьев отказов и событий.
- ГОСТ 27.310-95 *"Анализ видов, последствий и критичности отказов".*

Западные поставщики, а тем более, отечественные эксклюзивные и авторизованные перекупщики - люди весьма искушенные, и моментально понимают, с кем имеют дело.

Если заказчик ДО ЗАКЛЮЧЕНИЯ КОНТРАКТА проявляет свою компетентность, и твердо настаивает на выполнении базовой системы требований, без выполнения которых дальнейшее продвижение невозможно, а именно:

- Оборудование системы должно иметь документальное подтверждение соответствия стандартам IEC 61508 и IEC 61511;
- Система должна соответствовать требованиям российских ГОСТов 34.201, 34.601, 34.602, 34.603, РД 50-34.698, норм и правил на создание автоматизированных систем;
- Система должна соответствовать требованиям Правил взрывобезопасности по обеспечению промышленной безопасности ПБ 09-540-03;
- Система должна соответствовать требованиям Стандартов предприятия по обеспечению промышленной безопасности и Стандарта предприятия на создание АСУТП;
- Система должна соответствовать требованиям Технического задания на создание АСУТП;
- Система должна иметь стандартную техническую и проектную документацию не только на английском, но и на русском языке, - то будьте уверены - так оно и будет.

4.23. **Ведущие производители промышленных систем безопасности**

Ниже приводятся списки производителей программируемых электронных систем, имеющих разрешения TUV на применение определенных моделей PLC для целей защиты технологических процессов.

Ведущие фирмы-производители систем класса loo2D:

- ABB
- HIMA
- Honeywell
- Siemens Energy & Automation
- Yokogawa.

Фирмы-производители систем класса 2oo3:

- ABB
- GE-Fanuc
- ICS
- Triconex.

Текущий перечень производителей сертифицированного TUV оборудования систем безопасности можно посмотреть на сайтах http://www.tuvasi.com, http://www.tuv-fs.com

Замечание 1

Информация на сайтах TUV обновляется достаточно редко, и может не соответствовать реальному статусу оборудования. Согласно требованиям стандартов МЭК, TUV Rheinland отмечает продукцию, соответствующую IEC 61508 "Functional Safety of E/E/PE safety-related systems", следующим знаком:

Замечание 2

*Необходимо внимательно проверять методики расчета вероятностей отказов в технической документации изготовителей и поставщиков оборудования и программного обеспечения систем безопасности. Например, в руководствах фирмы GE Fanuc Automation "Genius Modular Redundancy. Users Manual (February 2002)", Appendix F "PFD Calculations*и *"Genius Modular Redundancy for Fire and Gas Applications", Appendix B "PFD Calculations" вместо соотношений для расчета вероятности опасного отказа системы 2oo3 приведены соотношения для системы loo2D!*

Кроме того, в расчетах использовано значение для интервала функционального (межповерочного) тестирования T_t = голько 6 месяцев, и нет расчетов для одного года, двух лет, 10 лет, как это рекомендовано стандартом МЭК. Надо ли напоминать, что искусственное сокращение интервала T_t с одного года до полугодия приводит к снижению вероятности опасного отказа в ДВА РАЗА, то есть к искусственному завышению характеристик надежности системы.

Притом, что на западе стандартный интервал между остановами на капремонт измеряется 2-4 годами (рекорд - 12(!) нет для одной из этиленовых установок).

Кроме того, параметр /? - доля общих отказов - принят в расчетах равным 1%, тогда как МЭК рассматривает диапазон от 1 до 10%, а для необнаруженных общих отказов - до 20%. Примеров подобных ухищрений можно привести множество.

Представитель фирмы HIMA J.Borcsok в *документе "Safety Consideration", 2003,* приводит результаты расчетов вероятности отказа для различных конфигураций контроллеров HIMA в совокупности с полевым оборудованием. При этом во всех расчетах принимается, что все датчики имеют конфигурацию 2oo3, а клапаны - 1oo2. При всем уважении к авторитету фирмы HIMA, интересно было бы посмотреть: много ли в США или Германии таких систем.

Замечание 3

Ко всем подкрепляющим аргументам, исходящим от заинтересованного лица, надо относиться с известной осторожностью. Как правило, используется испытанный прием:

Данные, полученные в одних условиях, применяются для подкрепления утверждений в собственных обстоятельствах, но при этом, естественно, не упоминается, что обстоятельства поменялись. Поэтому необходимо критически относиться к сведениям из проспектов поставщиков систем безопасности, и всегда понимать, что ***фактический уровень допуска конкретной конфигурации оборудования*** *и формальное соответствие последним международным стандартам - 1EC 61508, IEC 61511 - это далеко не одно и то же. Применение технических устройств только на основе эффектных презентаций - большой риск. И пусть эти устройства испытываются где-нибудь в другом месте, но не на наших взрывоопасных объектах.*

К сожалению, сертификаты не гарантируют соответствие фактических характеристик заявленным характеристикам оборудования. В стандартах IEC 61508 и 61511 прямо указывается на необходимость опыта непосредственного применения конкретных систем безопасности в течение достаточного интервала времени на различных процессах как одного из решающих условий выбора. В особенности это касается комплексных компонент системы с многочисленными функциями. Заказчик должен знать, какие из этих функций действительно были проверены на практике. Если отказы оборудования не имитировались в процессе пуско-наладки и не отраба-

тывались во время эксплуатации, то невозможно утверждать, что эти функции на самом деле будут выполнены.

В заключение еще раз приведем чрезвычайно жесткие требования стандартов МЭК к полевым испытаниям оборудования и программного обеспечения систем безопасности. Эти требования настолько важны, что должны в обязательном порядке присутствовать в наших нормативных документах.

Стандарты IEC 61508 (Часть 7, п. В.5.4) и IEC 61511 (Часть 4) требуют: Для того чтобы система считалась прошедшей полевые испытания, должны быть выполнены следующие требования *(For field experience to apply, the following requirements must have been fulfilled):*

- Неизменная спецификация.
- 10 систем в различных приложениях.
- отработанных рабочих часов (11,42 года) и, как минимум, 1 год сервисного обслуживания.

Сведения о том, что система прошла испытания на практике, должны быть предоставлены в виде документов изготовителем или поставщиком системы. Эта документация должна содержать, как минимум:

- Точное предназначение системы и ее компонентов, включая контроль версии оборудования;
- Послужной список системы с указанием потребителей и даты внедрения;
- Время эксплуатации;
- Процедуры для выбора системы и ее компонент, и процедуры, достаточные для проверки;
- Процедуры для выявления отказов, их регистрации, а также их устранения.

В части проверки программного обеспечения Стандарты IEC 61508 (часть 7, С.2.10) и IEC 61511 (часть 4) требуют:

Программное обеспечение не ломается, однако подвержено систематическим ошибкам, поэтому компонентам программного обеспечения или программным модулям можно доверять, если они уже проверены на соответствие требуемому уровню интегральной безопасности. Например, если для определения отказов оборудования предусмотрена процедура самотестирования, но отказы оборудования не имитировались в процессе пуско-наладки и не отрабатывались во время эксплуатации, то невозможно утверждать, что функции обнару-

жения неисправностей проверены на практике. Для исключения расширенной перепроверки или перепроектирования системных программных модулей при каждом новом применении, должны быть выполнены следующие требования, которые позволят удостовериться, что программные модули свободны от систематических ошибок проектирования и от опасных отказов. Программное обеспечение должно отвечать следующим жестким критериям:

- Неизменная спецификация.
- 10 систем в различных приложениях.
- Вероятность неопасных отказов в течение года 10^{-5} с доверительной вероятностью 99,9%.
- Отсутствие опасных отказов.

Для проверки того, что компонент или модуль программного обеспечения отвечает всем этим критериям, следующие позиции должны быть документированы *(must be documented):*

- Точная идентификация системы и ее компонентов, включая контроль версии и программного обеспечения, и оборудования;
- Послужной список системы с указанием потребителей и даты внедрения;
- Время эксплуатации;
- Процедуры для выбора системы под конкретные применения, и варианты применения;
- Процедуры для выявления отказов, их регистрации и устранения.

Замечание 4

Полевое оборудование сертифицируется на допуск к применению в системах безопасности наравне с ПЛК. При этом основной упор делается на уровень самодиагностики. Использование протоколов типа HART и Fieldbus позволяет создать самостоятельную систему обслуживания полевого оборудования, независимую от РСУ и ПАЗ. Это решение на порядки повышает надежность и готовность полевого оборудования. Однако необходимо помнить, что смысл имеет только ВЕСЬ КОНТУР безопасности, и общий SIL для комбинации из многих элементов - датчики, барьеры, логические контроллеры, клапаны - должен просчитываться для каждой конкретной функции (контура).

Глава 5

СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ АСУТП

5.1. Стандарты предприятия по управлению промышленной безопасностью

Первостепенное значение имеют требования ПБ 09-540-03 по созданию на взрывоопасных производствах системы управления промышленной безопасностью. Согласно Пункту 1.4 ПБ: "В целях организации работы по предупреждению аварий и производственного травматизма **организации, имеющие в своем составе взрывопожароопасные объекты, разрабатывают систему стандартов предприятия по управлению промышленной безопасностью, и обеспечивают их эффективное функционирование и актуализацию".**

Более того, согласно Пункту 1.5 ПБ: "Организации, осуществляющие проектную деятельность, а также деятельность по монтажу, ремонту оборудования и сооружений, обучению персонала, разрабатывают и обеспечивают эффективное функционирование и актуализацию **Системы стандартов предприятия по обеспечению качества. Системы качества организаций должны предусматривать наличие стандартов по обеспечению безопасного ведения работ".**

Таким образом, промышленное предприятие не только само должно обеспечить требования Правил, но и вправе потребовать от организаций, участвующих в создании, проектировании, обучении, реконструкции, модернизации взрывоопасных технологических объектов соответствия Стандартам предприятия по обеспечению промышленной безопасности, и по созданию безопасных систем управления и защиты.

Прежде всего, промышленное предприятие должно иметь собственную концепцию создания и развития безопасных средств автоматизации. Эта концепция должна быть оформлена в виде комплекса стандартов предприятия (СТП) в приложении к системам управления и защиты взрывоопасных технологических процессов. Ядро этого комплекса стандартов составляют четыре документа, представленные в четырех главах настоящей работы:

- **"Состав и содержание работ по созданию АСУТП"**
- **"Состав и содержание документации проекта АСУТП"**
- **"Техническое задание на создание АСУТП"**
- **"Программа и методика испытаний".**

Объединяющая роль этого комплекса должна быть отведена **Стандарту предприятия "На проектирование, разработку, внедрение, эксплуатацию и сопровождение АСУТП",** определяющему общие организационно-технические мероприятия по созданию и эксплуатации автоматизированных систем управления и защиты технологических процессов.

ПОРЯДОК ВЫПОЛНЕНИЯ ПРОЕКТА

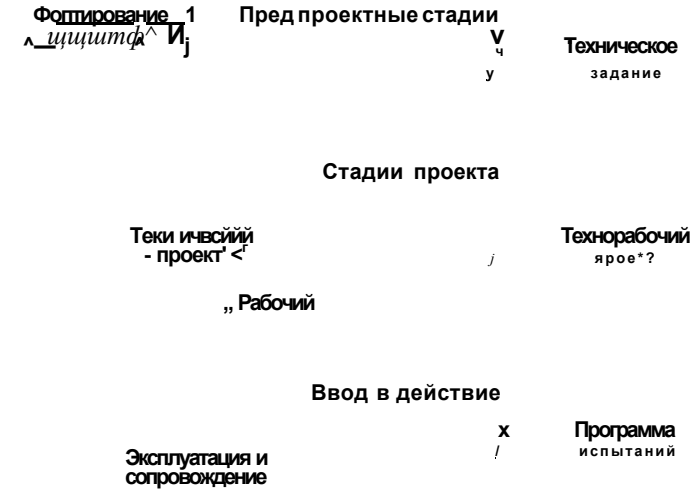


Рис. 5.7

5.2. Стадии и этапы создания АСУТП

Согласно ГОСТ 34.601-90 *"Автоматизированные Системы. Стадии создания",* процесс создания АСУТП представляет собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания Системы, соответствующей заданным требованиям.

Стадии и этапы создания АСУТП выделяются как части процесса создания по соображениям рационального планирования и организации работ, заканчивающихся заданным результатом. ГОСТ 34.601-90 рекомендует нижеследующую последовательность стадий и этапов работ по созданию АСУТП.

Стадия "Формирование требований к АСУТП" включает в себя выполнение следующих этапов:

- Обследование объекта и обоснование необходимости создания АСУТП;
- Формирование требований Заказчика к АСУТП;
- Оформление Отчета о выполненной работе, и Заявки на разработку АСУТП.

На этапе "Обследование объекта и обоснование необходимости создания АСУТП" в общем случае проводится:

- *Сбор данных об объекте автоматизации;*
- *Оценка качества функционирования объекта автоматизации;*
- *Выявление проблем, решение которых возможно средствами автоматизации;*
- *Оценка технико-экономической целесообразности создания АСУТП.*

На этапе "Формирование требований Заказчика к АСУТП" проводится:

- *Подготовка исходных данных для формирования требований к АСУТП (характеристика объекта автоматизации, описание требований к системе, допустимые затраты на разработку, ввод в действие и эксплуатацию, эффект, ожидаемый от системы, условия создания и функционирования системы);*
- *Формулирование и оформление требований Заказчика к АСУТП*

На этапе "Оформление Отчета о выполненной работе, и Заявки на разработку АСУТП" производится:

- *Оформление Отчета о выполненных работах на данной стадии;*
- *Оформление Заявки на разработку АСУТП (тактико-технического задания) или другого заменяющего его документа с аналогичным содержанием.*

Стадия "Разработка концепции АСУТП" заключается в выполнении следующих этапов:

- Изучение объекта автоматизации;
- Проведение необходимых научно-исследовательских работ;
- Разработка вариантов концепции АСУТП и выбор варианта концепции АСУТП в соответствии с требованиями Заказчика.

По завершению стадии оформляется отчет.

На этапе "Изучение объекта автоматизации" и

На этапе "Проведение необходимых научно - исследовательских работ" организация-разработчик проводит:

- *Детальное изучение объекта автоматизации и необходимые научно-исследовательские работы, связанные с поиском путей и оценкой возможности реализации требований Заказчика;*
- *Оформление и утверждение отчетов.*

На этапе "Разработка вариантов концепции АСУТП и выбор варианта концепции АСУТП в соответствии с требованиями Заказчика" в общем случае проводится:

- *Разработка альтернативных вариантов концепции АСУТП и планов их реализации;*
- *Оценка необходимых ресурсов на их реализацию и функционирование;*
- *Оценка преимуществ и недостатков каждого варианта;*
- *Сопоставление требований Заказчика и характеристик предлагаемой системы, и выбор наилучшего варианта;*
- *Определение порядка оценки качества и условий приемки системы;*
- *Оценка эффектов, получаемых от системы.*

Стадия "Техническое задание" заключается в единственном, но чрезвычайно ответственном этапе:

- Разработка и утверждение Технического задания на создание АСУТП.

На этапе "Разработка и утверждение Технического задания на создание АСУТП" проводится:

- *Разработка, оформление, согласование и утверждение Технического задания на создание АСУТП, а при необходимости, нескольких технических заданий на части АСУТП.*

Стадия "Эскизный проект" состоит из следующих этапов:

- Разработка предварительных проектных решений по Системе и ее частям;
- Разработка документации на АСУТП и ее части.

На этапе "Разработка предварительных проектных решений по Системе и ее частям" определяются:

- *Функции АСУТП;*
- *Функции и цели подсистем;*
- *Состав программных комплексов и отдельных задач;*
- *Концепция информационной базы, ее укрупненная структура;*
- *Функции системы управления;*
- *Состав комплекса технических средств;*
- *Функции и параметры основных программных средств и ресурсов АСУТП.*

На этапе "Разработка документации на АСУТП и ее части" проводится:

- *Разработка, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых проектных решений, и достаточном для выполнения работ по созданию АСУТП.*

Стадия "Технический проект" состоит из следующих этапов:

- Разработка проектных решений по Системе и ее частям;
- Разработка документации на АСУТП и ее части;
- Разработка и оформление документации на поставку

изделий для комплектования АСУТП и технических требований (технических заданий) на их разработку;

- Разработка заданий на проектирование в смежных частях проекта.

На этапе "Разработка проектных решений по Системе и ее частям" производится разработка общих решений:

- *По Системе и ее частям;*
- *По функционально-алгоритмической структуре Системы;*
- *По функциям персонала и организационной структуре;*
- *По структуре технических средств;*
- *По алгоритмам решения задач и применяемым языкам;*
- *По организации и ведению информационной базы;*
- *По Системе классификации и кодирования информации;*
- *По программному обеспечению.*

На этапе "Разработка документации на АСУТП и ее части" проводится:

- *Разработка, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых проектных решений и достаточном для дальнейшего выполнения работ по созданию АСУТП.*

На этапе "Разработка и оформление документации на поставку изделий для комплектования АСУТП и технических требований (технических заданий) на их разработку" проводится:

- *Подготовка и оформление документации на поставку изделий для комплектования АСУТП;*
- *Определение технических требований или составление ТЗ на разработку несерийных изделий.*

На этапе "Разработка заданий на проектирование в смежных частях проекта" осуществляется:

- *Разработка, оформление, согласование и утверждение заданий на проектирование в смежных частях проекта для проведения строительных, электротехнических, санитарно-технических и*

других подготовительных работ, связанных с созданием АСУТП.

Стадия "Рабочий проект (Рабочая документация)" включает в себя следующие этапы:

- Разработка рабочей документации на АСУТП и ее части;
- Разработка и конфигурация программного обеспечения.

На этапе "Разработка рабочей документации на АСУТП и ее части" осуществляется:

- *Разработка рабочей документации, содержащей все необходимые и достаточные сведения для обеспечения выполнения работ по вводу АСУТП в действие и для её эксплуатации, а также для сохранения уровня эксплуатационных характеристик системы в соответствии с принятыми проектными решениями;*
- *Оформление, согласование и утверждение рабочей документации на АСУТП.*

На этапе "Разработка и конфигурация программного обеспечения" проводится:

- *Разработка прикладного программного обеспечения;*
- *Выбор, адаптация и привязка программных средств, разработка программной документации.*

Стадия "Ввод в действие" состоит из следующих этапов:

- Подготовка объекта автоматизации к вводу АСУТП в действие;
- Подготовка персонала;
- Комплектация АСУТП поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями);
- Строительно-монтажные работы;
- Пусконаладочные работы;
- Проведение Предварительных испытаний;
- Проведение Опытной эксплуатации;
- Проведение Приемочных испытаний.

На этапе "Подготовка объекта автоматизации к вводу АСУТП в действие" проводятся работы по организационной подготовке объекта автоматизации к вводу АСУТП в действие, в том числе:

- *Реализация проектных решений по организационной структуре АСУТП;*
- *Обеспечение подразделений объекта управления инструктивно-методическими материалами.*

На этапе "Подготовка персонала" проводится:

- *Обучение персонала, и*
- *Проверка его способности обеспечить функционирование АСУТП.*

На этапе "Комплектация АСУТП поставляемыми изделиями" обеспечивается:

- *Получение комплектующих изделий серийного и единичного производства, материалов и монтажных изделий;*
- *Проводится входной контроль их качества.*

На этапе "Строительно-монтажные работы" проводится:

- *Выполнение работ по строительству специализированных зданий (помещений) для размещения технических средств и персонала АСУТП;*
- *Сооружение кабельных каналов;*
- *Выполнение работ по монтажу технических средств и линий связи;*
- *Испытание смонтированных технических средств;*
- *Сдача технических средств для проведения пусконаладочных работ.*

На этапе "Пусконаладочные работы" проводится:

- *Автономная наладка технических средств;*
- *Загрузка системного и прикладного программного обеспечения;*
- *Комплексная наладка всех средств системы.*

На этапе "Проведение Предварительных испытаний" осуществляются:

- *Испытания АСУТП на работоспособность и соответствие Техническому заданию и в соответствии с Программой предварительных испытаний;*

- *Устранение неисправностей и внесение изменений в документацию на АСУТП в соответствии с Протоколом испытаний;*
- *Оформление Акта о приемке АСУТП в Опытную эксплуатацию.*

На этапе "Проведение Опытной эксплуатации" проводят:

- *Опытная эксплуатация АСУТП;*
- *Анализ результатов Опытной эксплуатации АСУТП;*
- *Доработка (при необходимости) программного обеспечения АСУТП;*
- *Дополнительная наладка технических средств АСУТП;*
- *Доработка проектной документации;*
- *Оформление Акта о завершении Опытной эксплуатации.*

На этапе "Проведение Приемочных испытаний" проводятся:

- *Испытания на соответствие Техническому заданию и в соответствии с Программой приемочных испытаний;*
- *Анализ результатов испытаний АСУТП и устранение недостатков, выявленных при испытаниях;*
- *Оформление Протокола и Отчета по каждому объекту испытаний, определенному Программой испытаний;*
- *Оформление Акта о приемке АСУТП в Постоянную (промышленную) эксплуатацию.*

Стадия "Сопровождение АСУТП" включает в себя:

- Выполнение работ в соответствии с гарантийными обязательствами;
- Послегарантийное обслуживание.

На этапе "Выполнение работ в соответствии с гарантийными обязательствами" осуществляются:

- *Работы по устранению недостатков, выявленных при эксплуатации АСУТП в течение установленных гарантийных сроков;*
- *Внесение необходимых изменений в документацию на АСУТП.*

На этапе "Послегарантийное обслуживание" осуществляется:

- *Анализ функционирования системы;*
- *Выявление отклонений фактических эксплуатационных характеристик АСУТП от проектных значений;*
- *Установление причин этих отклонений;*
- *Устранение выявленных недостатков и обеспечение стабильности эксплуатационных характеристик АСУТП;*
- *Внесение необходимых изменений в документацию на АСУТП.*

5.3. Степени свободы при создании АСУТП

Согласно стандарту ГОСТ **34.601-90 "***Автоматизированные Системы. Стадии создания",* пункт 2.2:
"Стадии и этапы, выполняемые организациями-участниками работ по созданию АСУТП, устанавливаются во взаимных Договорах и в Техническом задании на создание АСУТП".
Согласно тому же пункту 2.2, допускается:

- Исключать стадию "Эскизный проект";
- Исключать отдельные этапы работ на всех стадиях;
- Объединять стадии "Технический проект" и "Рабочая документация" в одну стадию - "Технорабочий проект".

Кроме того, в зависимости от специфики создаваемых АС и условий их создания допускается:

- Выполнять отдельные этапы работ до завершения предшествующих стадий;
- Параллельное во времени выполнение этапов работ;
- Включение новых этапов работ.

В соответствии с предоставленными правами, устанавливаются следующие решения по составу проектных работ на создание АСУТП:

1. **Стадия "Эскизный проект" - исключается.**
2. **Предпочтительным вариантом выполнения проекта считается одностадийный "Технорабочий проект".**

3. С учетом специфики процесса создания АСУТП произведено:
- **Исключение отдельных этапов работ;**
- **Включение новых этапов работ.**

Согласно пункту 1.**4** ГОСТ 34.601-90, конкретный состав и правила выполнения работ определяются в соответствующей документации тех организаций, которые участвуют в создании конкретной АСУТП. Роль Заказчика в определении этих правил всегда должна быть определяющей.

Тщательное проведение предпроектных стадий:
- Предварительное обследование объекта автоматизации, формирование исходных требований к АСУТП,
- Разработка концепции АСУТП,
- Разработка Технического задания, -

имеет решающее значение для успеха всего проекта создания АСУТП. Согласно существующим оценкам, около половины всех ошибок вносится в еще не существующую систему именно на этапе предварительного специфицирования.

Согласно РД 50-34.698-90 МЕТОДИЧЕСКИЕ УКАЗАНИЯ. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. "*Автоматизированные Системы. Требования к содержанию документов", Приложение 1*, рекомендуется нижеследующее содержание документов, разрабатываемых на предпроектных стадиях.

5.4. Стадия "Формирование требований к АСУТП"

Выполняется Заказчиком совместно с Разработчиком Системы. В результате выполнения данной стадии оформляются:
- Отчет по ГОСТ 7.32-2001 *"Отчет о научно-технической работе";*
- Заявка на разработку АСУТП.

Основная часть отчета содержит следующие разделы:
1) Характеристика объекта и результатов его функционирования;
2) Описание существующих средств автоматизации, и информационно-управляющей системы;
3) Описание недостатков существующих средств автоматизации и информационно-управляющей системы;

4) Описание требований к средствам измерений автоматизируемого технологического процесса;
5) Обоснование необходимости совершенствования существующих средств автоматизации и информационно-управляющей системы объекта;
6) Цели, критерии и ограничения создания АСУТП;
7) Функции и задачи создаваемой АСУТП;
8) Ожидаемые технико-экономические результаты создания АСУТП;
9) Выводы и предложения.

Рекомендуется следующее содержание разделов:

1) В разделе "Характеристика объекта и результатов его функционирования" описывают задачи развития, требования к объему, номенклатуре и качеству результатов функционирования, а также характер взаимодействия объекта с внешней средой. При определении фактических показателей определяют тенденции их изменения во времени.
2) Раздел "Описание существующих средств автоматизации и информационно-управляющей системы" содержит описание функциональной и информационной структуры системы, качественных и количественных характеристик, раскрывающих взаимодействие ее компонентов в процессе функционирования.
3) В разделе "Описание недостатков существующих средств автоматизации и информационно-управляющей системы" приводят результаты диагностического анализа, при котором оценивают качество функционирования и организационно-технический уровень системы, выявляют недостатки в организации информационных и управляющих процессов, и определяют степень их влияния на качество функционирования системы.
4) В разделе "Описание требований к средствам измерений автоматизируемого технологического процесса" необходимо определить:
   - Какие измерения следует проводить и с какой точностью;
   - Дать рекомендации по выбору соответствующего контрольного, измерительного и испытательного оборудования, способного обеспечить необходимую точность и сходимость измерений.

5) В разделе "Обоснование необходимости совершенствования существующих средств автоматизации и информационно-управляющей системы объекта" при анализе соответствия показателей функционирования объекта предъявляемым требованиям оценивают степень соответствия прогнозируемых показателей и требуемых, и выявляют необходимость совершенствования информационно-управляющей системы путем создания АСУТП *(согласие есть продукт при полном непротивлении сторон — красиво излагают).*
6) Раздел "Цели, критерии и ограничения создания АСУТП" содержит:
   - Формулировку производственно-хозяйственных, научно-технических и экономических целей и критериев создания АСУТП;
   - Характеристику ограничений по созданию АСУТП.
7) Раздел "Функции и задачи создаваемой АСУТП" содержит:
   - Обоснование выбора перечня автоматизированных функций и комплексов задач с указанием очередности внедрения;
   - Требования к характеристикам реализации функций и задач в соответствии с действующими нормативно-техническими документами, определяющими общие технические требования к АСУТП конкретного вида;
   - Дополнительные требования, учитывающие специфику АСУТП.
8) Раздел "Ожидаемые технико-экономические результаты создания АСУТП" содержит:
   - Определение всех трех источников, трех составных частей экономической эффективности, получаемых в результате создания АСУТП (экономия производственных ресурсов, улучшение качества продукции, повышение производительности труда), и оценку ожидаемых изменений основных технико-экономических и социальных показателей производственно-хозяйственной деятельности объекта. Например, показателей по номенклатуре и объему производства, себестоимости продукции, рентабельности, отчислениям в фонды экономического стимулирования;

- Оценку ожидаемых затрат на создание и эксплуатацию АСУТП с распределением их по очередям создания АСУТП и с разбивкой по годам;
- Ожидаемые обобщающие показатели экономической эффективности АСУТП.

9) Раздел "Выводы и предложения" рекомендуется разделять на подразделы:
   - Подраздел "Выводы о производственно-хозяйственной необходимости и технико-экономической целесообразности создания АСУТП" содержит:
     - Сопоставление ожидаемых результатов создания АСУТП с заданными целями и критериями создания АСУТП (по целевым показателям и нормативным требованиям);
     - Принципиальное решение вопроса о создании АСУТП (положительное или отрицательное, то есть погодить).
   - Подраздел "Предложения по совершенствованию организации и технологии процесса деятельности" содержит предложения по совершенствованию:
     - Производственно-хозяйственной деятельности;
     - Организационной и функциональной структуры системы;
     - Методов деятельности;
     - Видов обеспечения АСУТП.
   - Подраздел "Рекомендации по созданию АСУТП" содержит рекомендации:
     - По виду создаваемой АСУТП и ее совместимости с другими АСУТП;
     - По организационной и функциональной структуре создаваемой АСУТП;
     - По составу и характеристикам подсистем и видов обеспечения АСУТП;
     - По организации использования имеющихся, и по приобретению дополнительных средств вычислительной техники;
     - По рациональной организации разработки и внедрения АСУТП;
     - По определению основных и дополнительных,

внешних и внутренних источников, видов и объемов финансирования и материального обеспечения разработки АСУТП;
- По обеспечению производственных условий создания АСУТП;
- Другие рекомендации по созданию АСУТП.

Заявка на разработку АСУТП составляется Заказчиком в произвольной форме и содержит:
- Предложения организации-заказчика к организации-разработчику на проведение работ по созданию АСУТП;
- Требования Заказчика к Системе;
- Условия и ресурсы на создание АСУТП.

5.5. Стадия "Разработка концепции АСУТП"

Выполняется Разработчиком Системы с участием Заказчика.

Стадия подразумевает:
- Детальное обследование объекта автоматизации;
- Анализ и оценку адекватности требований Заказчика;
- Разработку альтернативных вариантов построения АСУТП, и
- Выбор наиболее предпочтительного варианта построения АСУТП.

Обновление технических средств КИПиА может проводиться поэтапно:
- 1-й этап - внедрение современного оборудования РСУ и ПАЗ с использованием существующего полевого КИП и электропневмо - и пневмоэлектрических преобразователей, и
- 2-й этап - замена/устаревшего оборудования КИП на электронную технику.

В конечном итоге архитектура АСУТП должна представлять собой следующее:
- Полевой КИП на современной электронной технике;
- Контроллеры РСУ и ПАЗ, связанные с рабочими станциями промышленного исполнения;
- Квалифицированный персонал.

В обязательном порядке должна предусматриваться связь с заводской локальной и с корпоративной вычислительной сетью.

Выбор конкретного поставщика средств автоматизации вообще, и системы управления и защиты в частности должен осуществляться на конкурсной основе с участием нескольких, как правило, 3 ± 1 поставщиков.

Согласно рекомендациям профессора Э.Л. **Ицковича, Институт Проблем Управления РАН,** при проведении тендеров (конкурсов) и при сравнении различных программно-технических комплексов необходимо исходить из учета следующих критериев:

- Технический уровень оборудования и программного обеспечения;
- Уровень обеспечения требуемой надежности;
- Уровень полноты программных средств и простота конфигурирования;
- Степень защиты от проникновения в систему;
- Опыт применения данного оборудования на аналогичных объектах;
- Уровень доверия к поставщику оборудования и программного обеспечения;
- Способность поставщика оборудования взять на себя роль Разработчика, то есть выполнить весь спектр работ по созданию АСУТП - от обследования технологического объекта до внедрения;
- Адекватность цены и предлагаемых средств и услуг.

Процедура выбора конкретного поставщика для конкретного объекта состоит из выполнения следующих шагов:

- Определение технических требований к составу и качеству оборудования, программного обеспечения и услуг;
- Анализ рынка АСУТП, и выбор поставщиков, участвующих в конкурсе;
- Рассылка требований;
- Получение технической и коммерческой информации, и её анализ;
- Составление сводных таблиц для сопоставления предложений;

- Организация группы экспертов из представителей заинтересованных служб предприятия;
- Определение критериев оценки предложений и их ранжирование;
- Индивидуальная работа экспертов над полученными данными;
- Составление сводных таблиц с экспертными оценками;
- Ранжирование потенциальных поставщиков в соответствии с полученными средневзвешенными показателями;
- Утверждение результатов и окончательный выбор поставщика.

По окончанию данной стадии разрабатывается отчет. В основной части отчета приводят:

- Описание результатов обследования объекта автоматизации;
- Описание и оценку преимуществ и недостатков разработанных альтернативных вариантов концепции создания АСУТП;
- Сопоставительный анализ требований к АСУТП и вариантов построения АСУТП;
- Обоснование выбора наиболее рационального варианта концепции, и описание предлагаемой АСУТП;
- Ожидаемые результаты и эффективность реализации выбранного варианта концепции АСУТП;
- Ориентировочный план реализации выбранного варианта построения АСУТП;
- Оценка затрат на реализацию проекта создания АСУТП.

Важное замечание

Для хорошо проработанных объектов автоматизации и для объектов, уже имеющих в своем составе действующие АСУТП, процесс модернизации АСУТП может быть начат непосредственно со стадии Технического задания, минуя стадии "Формирование требований к АСУТП" и "Разработка концепции АСУТП". **Однако проведение конкурса и в этом случае строго рекомендуется.**

5.6. Стадия "Техническое задание на создание АСУТП"

Результатом выполнения двух предыдущих этапов является разработка и оформление **Технического задания на АСУТП** в соответствии с ГОСТ 34.602-89, которое является основой для выполнения работ по техническому и рабочему (технорабочему) проектированию, а также при подготовке к вводу Системы в действие.

Техническое задание на создание АСУТП создается Разработчиком АСУТП при непосредственном участии Организации-заказчика. Согласно ГОСТ 34.602-89, Техническое задание должно состоять из следующих разделов:

1. Общие сведения
1.1. Полное наименование Системы
1.2. Шифр темы
1.3. Наименование Организаций - разработчиков, проектировщиков, заказчика, и их реквизиты
1.4. Перечень документов, на основании которых создается Система
1.5. Сроки выполнения работ
1.6. Источники и порядок финансирования
1.7. Порядок оформления и предъявления заказчику результатов работы
2. Назначение и цели создания Системы
2.1. Назначение Системы
2.2. Цели создания Системы
3. Характеристика объекта автоматизации
4. Требования к Системе
4.1. Требования к Системе в целом
4.1.1. Требования к структуре и функционированию Системы
4.1.2. Требования к численности и квалификации персонала
4.1.3. Требования к показателям назначения
4.1.4. Требования к надёжности
4.1.5. Требования безопасности
4.1.6. Требования по эргономике и технической эстетике
4.1.7. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению

8. Требования к документированию
9. Источники разработки
10. ПРИЛОЖЕНИЯ
И. СОСТАВЛЕНО
12. СОГЛАСОВАНО

Согласно ГОСТ 34.601-90, пункт 2.2, стадии и этапы, выполняемые организациями-участниками работ по созданию автоматизированной системы, устанавливаются во взаимных договорах и в Техническом задании.

Согласно ГОСТ 34.201-89, пункт 2.1, в Техническом задании на Систему должен быть определен "Перечень наименований разрабатываемых документов и их комплектность на Систему и ее части". В любом случае перечень проектной документации должен быть строго определен в Договоре между Разработчиком и Заказчиком на разработку Рабочего проекта и рабочей документации (технорабочего) проекта. Тогда в Техническом задании достаточно указать ссылку на этот договор. В общем случае согласно РД 50-34.698-90,

"Содержание каждого документа, разрабатываемого при проектировании АС согласно ГОСТ 34.201-89, определяет Разработчик в зависимости от объекта проектирования (система, подсистема и т.д.)". Однако во избежание недоразумений содержание документов и формы таблиц всегда должны быть согласованы с Заказчиком.

Согласно ГОСТ 34.003-90 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. *"Автоматизированные системы. Термины и определения",* Техническое задание в обязательном порядке должно содержать предварительный План-график работ по созданию АСУТП.

Техническое задание на создание АСУТП для объектов всех категорий взрывоопасности согласовывается с региональным представителем Ростехнадзора, как независимой контролирующей организацией третьей стороны, осуществляющей надзор над промышленной безопасностью.

Кроме того, для вновь строящихся производств Техническое задание на создание АСУТП для объектов всех категорий взрывоопасности должно быть согласовано с Проектной организацией.

Техническое задание на создание АСУТП утверждается руководителем / главным инженером предприятия-заказчика и

руководителем / техническим директором организации - разработчика Системы.

Изменения или дополнения к Техническому заданию оформляются в виде Протокола или Дополнения к ТЗ, согласовываются с технадзором, и утверждаются Заказчиком и Разработчиком Системы. С этого момента Протокол или Дополнение к ТЗ становятся неотъемлемой частью Технического задания на Систему.

Неформальное отношение к определению исходных требований к Системе в Техническом задании оказывает решающее воздействие на конечный результат всей работы. В главе "Техническое задание на создание АСУТП" воспроизводится образец Технического задания, отработанный на практике целого ряда успешно реализованных проектов.

5.7. Состав и содержание работ по созданию АСУТП

Разработка АСУТП и ввод в действие осуществляются в соответствии с ГОСТ 34.601-90 "*Автоматизированные Системы. Стадии создания*

В соответствии с правами, предоставленными ГОСТ 34.601-90 *"Автоматизированные системы. Стадии создания*пункт 2.2, **стадия "Эскизный проект" исключается.**

Стадии создания АСУТП, этапы и содержание работ по ним, а также распределение работ и сроки выполнения указываются в согласованном Плане-графике работ к Договору на создание АСУТП с обязательным отражением промежуточных этапов. В зависимости от специфики объекта автоматизации, могут быть заключены несколько самостоятельных, но взаимоувязанных по срокам выполнения договоров:

- Договор на Поставку оборудования РСУ, ПАЗ и КИП;
- Договор на Разработку технорабочего проекта;
  Договор на "инжиниринг". Речь в этом договоре, в частности, идет о следующем:
  - Конфигурирование станций управления (контроллеров);
  - Конфигурирование модулей ввода-вывода;
  - Написание пользовательских программ управления;
  - Конфигурирование операторских станций;

- Конфигурирование обзорных экранов;
- Конфигурирование мнемосхем;
- Конфигурирование групповых и индивидуальных графиков (трендов);
- Конфигурирование отчетов (рапортов);
- Шефмонтаж основного оборудования системы;
- Автономная наладка системы;
- Комплексная наладка системы;
- Разработка инструкции оператора процесса;
- Обучение оперативного персонала;
- Проведение предварительных испытаний и т.д.

В некоторых случаях могут быть заключены самостоятельные договора на обучение, на шефмонтаж и пусконаладку системы.

5.8. Первое техническое совещание

После заключения Договора на создание АСУТП проводится первое техническое (организационное) совещание с участием Заказчика, Проектной организации, Разработчика системы и Поставщика оборудования для окончательного согласования и уточнения спецификаций и характеристик Системы.

На этом этапе согласовываются функции Системы управления, включая контуры управления, контроля, сервисные функции Системы, функции Системы противоаварийной защиты, включая блокировки, сигнализацию, отчеты по событиям. Согласовываются объемы работ, которые необходимо выполнить каждому из участников проекта создания АСУТП, сроки выполнения работ, определяются ответственные лица и способы взаимодействия.

5.9. Исходные данные для создания АСУТП

В идеале, на первом техническом совещании Разработчику должна быть предоставлена следующая документация, которая потребуется для выполнения проекта:

- Пояснительная записка технологической части проекта;
- Копия Технологического регламента;

- Монтажно-технологические схемы с КИПовской обвязкой;
- Перечень КИПовскнх позиций с указанием уровней входных и выходных сигналов, пределов сигнализации и блокировок;
- Инструкции по эксплуатации, пуску и останову технологического процесса;
- Описание алгоритмов управления и противоаварийной защиты;
- Описание алгоритмов связного, последовательного и логического управления;
- Логические схемы управления и противоаварийной защиты;
- Принципиальные схемы управления силовым оборудованием;
- Схемы электроснабжения технологического объекта;
- Документация строительной части помещений управления;
- Спецификация полевого оборудования;
- Схемы подключения внешних проводок от полевого оборудования до кроссовых шкафов в помещениях управления;
- Планы размещения существующего оборудования средств автоматизации в помещениях управления.

5.10. Разработка Технического проекта

На основании исходных данных Разработчик выполняет Технический проект на РСУ и ПАЗ в соответствии с требованиями Технического задания.

В Техническом проекте должны быть, в частности, представлены следующие документы:

- Планы расположения технических средств АСУТП;
- Архитектура РСУ и ПАЗ;
- Чертежи конструкций оборудования Системы, включая конструкцию консольных пультов и шкафов;
- Схемы компоновки Системы;
- Схемы размещения и подключения барьеров искробезопасности;

- Расчеты потребляемой мощности и теплоотдачи;
- Схемы заземления;
- Схемы кроссового оборудования;
- Кабельный журнал для подключения кроссовых шкафов к РСУ и ПАЗ;
- Перечни параметров РСУ и ПАЗ;
- Перечни контуров управления и защиты;
- Описание автоматизируемых функций управления и защиты.

5.11. Рассмотрение Технического проекта

В соответствии с календарным планом проводится техническое совещание для рассмотрения Технического проекта, на котором окончательно уточняются требования Заказчика к Прикладному ("математическому") программному обеспечению (ППО). Все замечания Заказчика к Техническому проекту и требования к прикладному программному обеспечению должны быть учтены Разработчиком при разработке Рабочего проекта и конфигурации системы.

На данном этапе в соответствии с ГОСТ 34.601-90 *"Автоматизированные системы. Стадии создания",* Проектная организация совместно с Заказчиком осуществляют разработку, оформление, согласование и утверждение Заданий на проектирование в смежных частях проекта автоматизации для проведения строительных, электротехнических, санитарно-технических и других подготовительных работ, связанных с созданием Системы.

Согласно ГОСТ 34.201-89, п. 1.3.1, табл. 2, *"Виды документов, разрабатываемых на стадиях Технического проекта и Рабочей документации, имеющих отношение к проектно-сметным, выполняются проектной организацией".*

5.12. Рабочий проект (Рабочая документация)

Конфигурация функций управления и защиты. Разработка, конфигурация, загрузка, тестирование и отладка функций управления и защиты, а также конфигурация РСУ и ПАЗ в целом, выполняются Разработчиком. Копии прикладного программного обеспечения передаются Заказчику на магнитных /

оптических / электронных носителях на стадии сдачи Рабочего проекта.

Конфигурация функций представления информации. В объем конфигурации входят:

- Разработка и конфигурация мнемосхем технологического процесса с контурами контроля и управления;
- Конфигурация отображения параметров, находящихся в состоянии сигнализации, или блокировки;
- Разработка и конфигурация трендов (графиков изменения параметров во времени);
- Конфигурация архивов;
- Генерация и вывод технологических отчетов и режимных листов;
- Генерация и вывод системных отчетов, хронологических перечней технологических и системных событий;
- Определение и конфигурация данных для внешних информационных сетей (корпоративная сеть и заводская ЛВС).

Параллельно с конфигурацией Системы должны вестись курсы обучения специалистов Заказчика, причем практические занятия должны включать реальные задачи управления и защиты объекта автоматизации Заказчика на реальной Системе. Приемку Рабочего проекта целесообразно планировать сразу после курса обучения.

Приемка Рабочего проекта. В состав Рабочего проекта входят все скорректированные разделы Технического проекта. Разработчик АСУТП должен выполнить рабочий проект на РСУ и ПАЗ, и представить заказчику для согласования и приемки. В Рабочем проекте должны быть представлены следующие документы:

- Документация по общесистемным решениям (ОР)
- Документация на техническое обеспечение (ТО)
- Документация на информационное обеспечение (ИО)
- Документация на стандартное программное обеспечение (ПО)
- Документация на прикладное программное обеспечение (МО)
- Документация организационного обеспечения (ОО).

Следующая глава "Состав и содержание документации проекта АСУТП" содержит подробные методические указания по составу документации Технического и Рабочего (Технорабочего) проекта:

В большинстве случаев и по срокам, и по деньгам предпочтительно объединение стадий технического проектирования и рабочей документации в одну стадию - единый Технорабочий проект.

После приемки Рабочего (технорабочего) проекта и сконфигурированной Системы, оборудование передается Заказчику для монтажа. Вместе с тем, с целью сокращения сроков создания и запуска АСУТП монтаж и пусконаладка могут производиться параллельно с выполнением проектных работ.

5.13. Взаимодействие и ответственность подразделений, участвующих в процессе создания АСУТП

На всех этапах создания АСУТП непосредственным Заказчиком является одно из структурных подразделений предприятия, для которого создается АСУТП. Исполнителями при разработке и внедрении АСУТП являются специализированные организации, выполняющие работы по Договору с Заказчиком.

На стадии **"Формирование требований к АСУТП"** Заказчик несет ответственность за:

- Обеспечение и организацию процедуры обследования объекта автоматизации;
- Формирование требований к АСУТП, включая оценку ожидаемых технико-экономических результатов создания АСУТП;
- Оформление отчета, и Заявки на разработку АСУТП.

Стадия **"Формирование требований к АСУТП"** выполняется Заказчиком при участии потенциального Разработчика Системы. **Ответственность за результат выполнения стадии в целом возлагается на Заказчика.**

Стадия **"Разработка концепции АСУТП"** выполняется Разработчиком при участи Заказчика Системы. **Ответственность за результат выполнения стадии возлагается на Разработчика.**

По согласованию между Разработчиком и Заказчиком, процесс создания АСУТП может быть начат непосредственно со стадии Технического задания, минуя две предварительные стадии.

Стадия **"Техническое задание на создание АСУТП"** выполняется Разработчиком по Договору с Заказчиком Системы, и при непосредственном участии Заказчика. **Ответственность за результат выполнения стадии ТЗ возлагается на Разработчика АСУТП.**

Техническое задание после согласования с Проектной организацией, региональным представителем Ростехнадзора, и утверждения руководителем (или техническим директором) организации-разработчика, и руководителем (или главным инженером) предприятия-заказчика становится основой для выполнения работ по техническому и рабочему (технорабочему) проектированию, а также при пусконаладочных работах, приемо-сдаточных испытаниях, и запуске Системы в эксплуатацию.

Ответственность за проектирование на стадиях Технического проекта и Рабочей документации АСУТП, или единого Технорабочего проекта возлагается на Разработчика.

Разработку, оформление, согласование и утверждение "Заданий на проектирование" в смежных частях проекта для проведения строительных, электротехнических, санитарно-технических и других подготовительных работ, связанных с созданием АСУТП, осуществляют Проектная организация совместно с Заказчиком Системы.

Ответственность за выполнение проектно-сметной документации несет Проектная организация.

5.14. Состав работ и ответственность при подготовке к вводу АСУТП в действие

Заказчик на стадиях разработки и внедрения АСУТП несет ответственность за выполнение следующих мероприятий:

- Формирование или расширение подразделения эксплуатации и обслуживания АСУТП;
- Согласование Технического задания, приемку Техни-

ческого проекта и Рабочей документации в соответствии с Планом-графиком работ по созданию АСУТП;
- Организацию работ по замене существующих средств КИПиА, а также работ по монтажу и пуско-наладке средств КИПиА;
- Организацию строительно-монтажных работ, связанных с переоборудованием помещений управления (операторных), и с установкой средств вычислительной техники;
- Обеспечение и организацию работ по поверке (калибровке) измерительных каналов;
- Организацию проведения комплексной наладки Системы;
- Организацию предварительных и приёмочных испытаний Системы;
- Обеспечение обслуживания Системы с момента её сдачи в Опытную эксплуатацию;
- Регистрацию сбоев и отказов средств вычислительной техники и КИПиА в Рабочем журнале;
- Представление Разработчику необходимых данных на всех стадиях создания Системы, и нормальных условий для работы специалистов Разработчика на площадке Заказчика.
- Организацию обучения технологического персонала и специалистов подразделения АСУТП объекта автоматизации.

Поставщик оборудования несет ответственность за:
- Соответствие поставляемого оборудования спецификации Договора на поставку;
- Наличие и предоставление Заказчику соответствующих сертификатов и инструкций:
  - Сертификаты Госстандарта России об утверждении типа средств измерений;
  - Разрешения Госгортехнадзора (Ростехнадзора) на применение оборудования;
  - Методики поверки для СИ, для которых нет общегосударственных стандартов;
  - Инструкции по техническому обслуживанию, эксплуатации и монтажу **на русском языке.**

- Осуществление поставки оборудования Системы на склад Заказчика в соответствии с договорными обязательствами;
- Гарантийное обслуживание оборудования и поставку запасных частей.

Разработчик АСУТП несет ответственность за своевременное и качественное выполнение следующих мероприятий:

- Наличие действующих лицензий на право проведения работ по проектированию и разработке АСУТП;
- Качественное исполнение документации Технического и Рабочего (технорабочего) проектов;
- Проведение обучения технологического персонала и специалистов подразделения АСУТП объекта автоматизации.
- Синхронное выполнение проектных работ со сроками поставки технических средств АСУТП, включая и полевое оборудование;
- Синхронное выполнение проектных работ с планом строительных работ, монтажа оборудования КИП и средств вычислительной техники;
- Проверку состояния технических средств АСУТП и качества поверки (калибровки) измерительных каналов;
- Проведение комплексной наладки Системы;
- Своевременное проведение предварительных и приёмочных испытаний Системы;
- Своевременный ввод Системы в промышленную эксплуатацию.

5.15. Монтаж и пуско-наладка

Монтаж и пусконаладка. Работы по монтажу и пусконаладке РСУ, ПАЗ и полевого оборудования на площадке Заказчика выполняются специализированными организациями. Рекомендуется привлекать специалистов Разработчика и Поставщика оборудования на шефмонтаж. С целью сокращения неоправданных простоев технологического оборудования во время наладочных работ по Системе, наладка может выпол-

няться по позициям, по аппаратам, или по технологическим узлам. На этапах монтажа и пуско-наладки проводятся работы по сборке, наладке и настройке основного оборудования и программного обеспечения АСУТП:

- Монтаж оборудования РСУ, ПАЗ и полевого оборудования;
- Прокладка, расключение и маркировка кабельных соединений;
- Обеспечение заземления;
- Подача электропитания;
- Загрузка базового программного обеспечения;
- Системное и функциональное тестирование;
- Прозвонка сигнальных кабелей;
- Настройка измерительных каналов;
- Установка прикладного программного обеспечения;
- Проверка и настройка прикладного программного обеспечения.

Безопасность работ по монтажу, наладке, регулировке и испытанию. На проведение работ во взрывоопасных зонах оформляются наряды-допуски, разрабатываются меры, обеспечивающие безопасность проведения работ.

5.16. Поверка и калибровка измерительных каналов

После наладки измерительные каналы подвергаются поверке или калибровке. Поверка или калибровка измерительных каналов должны проводиться Государственной метрологической службой, или метрологической службой Заказчика в зависимости от назначения измерительной системы, и сведений об ее использовании в сфере, или вне сферы государственного метрологического контроля и надзора.

5.17. Порядок контроля и приемки

На стадии "Ввод в действие" ГОСТ 34.601-90 "*Стадии создания*" устанавливает следующие этапы испытаний:

- Предварительные испытания;
- Опытная эксплуатация;
- Приемочные испытания.

Замечание

В противоречие с ГОСТ 34.601, в целом весьма добротный ГОСТ 34.603-92 "Виды испытаний автоматизированных систем " определяет ***этапы*** *испытаний как* ***виды*** *испытаний.*

Для определения процедуры проведения конкретного этапа испытаний разрабатываются самостоятельные документы - Программы испытаний. По каждому этапу испытаний Программа испытаний составляется Разработчиком и утверждается Заказчиком Системы. Программа испытаний должна устанавливать необходимый и достаточный объем испытаний, обеспечивающий заданную полноту и достоверность получаемых результатов. Программа испытаний может разрабатываться на АСУТП в целом, или на части АСУТП. В качестве приложений могут включаться тесты (контрольные примеры). Предварительные испытания АСУТП проводятся для определения работоспособности АСУТП, и возможности приемки АСУТП в Опытную эксплуатацию.

Предварительные испытания проводятся после отладки и предварительного тестирования программных и технических средств системы Разработчиком Системы, и после того, как Разработчик представит официальный запрос о готовности к испытаниям. **Необходимым условием начала предварительных испытаний является:**

- Обучение эксплуатационного и оперативного персонала Заказчика методам взаимодействия с Системой;
- Рассмотрение и изучение проектной и эксплуатационной документации персоналом Заказчика.

Опытная эксплуатация АСУТП проводится с целью определения готовности АСУТП к постоянной эксплуатации, проверки готовности персонала к работе в новых условиях, и доработки и корректировки проектной документации.

Проводить Приемочные испытания без прохождения этапа Опытной эксплуатации запрещается.

Приемочные испытания АСУТП проводятся для определения соответствия АСУТП Техническому заданию на создание АСУТП, оценки успеха Опытной эксплуатации, и решения о возможности приемки АСУТП в постоянную (промышленную) эксплуатацию.

В зависимости от требований, предъявляемых к АСУТП на испытаниях, проверке или аттестации подвергается:

- Комплекс программных и технических средств;
- Эксплуатационный и оперативный (технологический) персонал;
- Эксплуатационная и рабочая документация, регламентирующая взаимодействие персонала с системой управления и защиты;
- Аттестация АСУТП в целом.

При испытаниях АСУТП проверяется:

- Соответствие разработанной АСУТП Техническому заданию на создание АСУТП;
- Качество выполнения автоматических и автоматизированных функций АСУТП **во всех режимах функционирования АСУТП;**
- Знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций **во всех режимах функционирования АСУТП** согласно ТЗ на создание АСУТП;
- Полнота содержащихся в эксплуатационной документации указании персоналу по выполнению установленных функций **во всех режимах функционирования АСУТП** согласно ТЗ на создание АСУТП;
- Количественные и качественные характеристики выполнения автоматических и автоматизированных функций АСУТП в соответствии с ТЗ;
- Другие свойства АСУТП, которым она должна соответствовать по Техническому заданию.

Испытания АСУТП следует проводить на объекте Заказчика. По согласованию между Заказчиком и Разработчиком предварительные испытания и приемку программных средств АСУТП допускается проводить на технических средствах Разработчика при условии получения достоверных результатов испытаний.

Допускается последовательное проведение испытаний и сдача АСУТП в опытную и постоянную эксплуатацию по частям при соблюдении установленной в ТЗ очередности ввода АСУТП в действие.

Предварительные испытания, Опытная эксплуатация и Приемочные испытания начинаются с приказа или распоряжения по предприятию о проведении соответствующих работ.

Предварительные испытания АСУТП.

В зависимости от взаимосвязей испытываемых в АСУТП объектов, испытания могут быть:

- Автономные;
- Комплексные.

Автономные испытания охватывают части АСУТП и проводятся по мере готовности частей АСУТП к сдаче в Опытную эксплуатацию. Комплексные испытания проводят для взаимосвязанных частей АСУТП или для АСУТП в целом.

Автономные испытания. Автономные испытания АСУТП проводятся в соответствии с **Программой автономных испытаний, разрабатываемых для каждой части АСУТП.** В программе автономных испытаний указываются:

- Перечень функций, подлежащих испытаниям;
- Описание взаимосвязей объекта испытаний с другими частями АСУТП;
- Условия, порядок и методы проведения испытаний и обработки результатов;
- Критерии приемки частей по результатам испытаний.

К Программе автономных испытаний должен прилагаться График проведения автономных испытаний. Подготовленные и согласованные тесты на этапе автономных испытаний должны обеспечивать:

- Полную проверку функций и рабочих процедур по перечню, согласованному с Заказчиком;
- Необходимую точность вычислений, установленную в тз;
- Проверку временных характеристик функций и процедур системы;
- Проверку надежности и устойчивости функционирования программных и технических средств.

В качестве исходной информации для тестов рекомендуется использовать фрагменты реальной информации с технологического объекта в объеме, достаточном для обеспечения необходимой достоверности испытаний. Результаты автономных испытаний частей АСУТП должны фиксироваться в Протоколах испытаний по каждой испытанной части. Протоколы должны содержать заключение о возможности (невозможности) допуска части АСУТП к комплексным испытаниям.

В случае если проведенные автономные испытания будут признаны недостаточными, либо будет выявлено нарушение требований по составу или содержанию документации, указанная часть АСУТП может быть возвращена на доработку, и назначен новый срок испытаний.

Комплексные испытания. Комплексные испытания АСУТП проводятся путем выполнения комплексных тестов. После завершения испытаний оформляется Акт приемки в Опытную эксплуатацию.

В программе комплексных испытаний АСУТП в целом или взаимосвязанных частей АСУТП указывается:

- Перечень объектов испытания;
- Состав предъявляемой документации;
- Описание проверяемых взаимосвязей между объектами испытаний;
- Очередность испытаний частей АСУТП;
- Порядок и методы испытаний, в том числе состав программных средств и оборудования, необходимых для проведения испытаний, включая специальные стенды.

Для проведения комплексных испытаний предъявляются:

- Программа комплексных испытаний;
- Заключение по автономным испытаниям соответствующих частей АСУТП с устранением ошибок и замечаний, выявленных при автономных испытаниях;
- Методики комплексных тестов;
- Собственно проверяемые программные и технические средства, и соответствующая им эксплуатационная документация.

Комплексный тест должен:

- Быть логически увязанным;
- Обеспечивать проверку выполнения функций частей АСУТП во всех режимах функционирования, установленных в ТЗ на АСУТП, в том числе всех связей;
- Обеспечивать проверку реакции системы на некорректную информацию и аварийные ситуации.

Результаты испытаний отражаются в Протоколах испытаний по каждому разделу испытаний, как то:

- Проверка комплектности поставки КТС и стандартной технической документации;

- Проверка комплектности разработанной проектной документации;
- Проверка функционирования КТС и системного программного обеспечения;
- Проверка функционирования прикладного программного обеспечения.

Протоколы комплексных испытаний должны содержать заключение о возможности (невозможности) приемки АСУТП в Опытную эксплуатацию, а также перечень необходимых доработок и согласованные сроки их выполнения.

После устранения недостатков проводятся повторные комплексные испытания в необходимом объеме. Работу над предварительными испытаниями завершаются оформлением Акта приемки в Опытную эксплуатацию.

Опытная эксплуатация.

Устанавливается продолжительностью **не менее двух месяцев,** и проводится в соответствии с Программой, в которой указываются:

- Условия и порядок функционирования частей Системы и Системы в целом.
- Порядок устранения недостатков, выявленных в процессе Опытной эксплуатации.
- Продолжительность Опытной эксплуатации, достаточную для проверки правильности функционирования Системы при выполнении каждой функции и готовности персонала к работе в условиях полноценного функционирования Системы.

Перед началом Опытной эксплуатации издается приказ или распоряжение "О начале опытной эксплуатации АСУТП".

Во время Опытной эксплуатации Системы ведут Рабочий журнал, в который заносят:

- Сведения о продолжительности функционирования Системы;
- Сведения об отказах, сбоях, аварийных ситуациях;
- Сведения об изменениях параметров объекта автоматизации;
- Сведения о проведенных корректировках программного обеспечения и документации;
- Сведения о наладке технических средств.

Сведения фиксируются в Журнале с указанием даты и ответственного лица. В Журнал могут быть внесены замечания оперативного персонала по эксплуатации и функционированию Системы. По результатам Опытной эксплуатации составляют **Акт о завершении** работ по проверке Системы в режиме **Опытной эксплуатации,** с заключением о возможности предъявления Системы на Приемочные испытания.

Приемочные испытания допускается проводить только на функционирующем технологическом объекте.

Приемочные испытания.

Приемочные испытания автоматизированной Системы проводят в соответствии с Программой, в которой указывают:

- Перечень объектов, выделенных в Системе для испытаний, и перечень требований, которым должны соответствовать объекты (со ссылкой на пункты ТЗ);
- Критерии приемки Системы и ее частей;
- Условия и сроки проведения испытаний;
- Технические и организационные средства для проведения испытаний;
- Фамилии лиц, ответственных за проведение испытаний;
- Методику испытаний и обработки результатов;
- Перечень оформляемой документации.

Приёмочные испытания АСУТП проводят для определения соответствия Техническому заданию и Проектной документации. Приёмочную комиссию образуют приказом или распоряжением по предприятию. В состав комиссии входят преде 1авители Заказчика, Разработчика, Поставщика оборудования, Проектной организации, монтажных и пусконаладочных организаций и органов технадзора.

Приёмочной комиссии предъявляется следующая документация:

- Техническое задание на создание АСУТП;
- Исполнительную документацию по монтажу;
- Протокол предварительных испытаний;
- Программу испытаний Системы;
- Акты метрологической аттестации измерительных каналов;
- Акт приёмки Системы в опытную эксплуатацию;

- Рабочие журналы Опытной эксплуатации Системы;
- Акт о завершении работ по проверке Системы в режиме Опытной Эксплуатации;
- Техническую документацию на Систему;
- Собственно физический комплекс программно-технических средств - АСУТП с подготовленным и обученным оперативным и эксплуатационным персоналом.

Перед предъявлением Системы на Приемочные испытания системная и техническая документация должна быть доработана по замечаниям Протокола предварительных испытаний и Акта о завершении работ по проверке Системы в режиме Опытной эксплуатации.

Приемочные испытания должны включать проверку:

- Полноты и качества реализации функций АСУТП в соответствии с Техническим Заданием на создание АСУТП;
- Выполнения каждого требования, относящегося к человеко-машинному интерфейсу Системы;
- Работы персонала в диалоговом режиме;
- Средств и методов восстановления работоспособности Системы после отказов;
- Комплектности и качества эксплуатационной документации.

Проверку полноты и качества выполнения функций АСУТП рекомендуется проводить в два этапа. На первом этапе проводят испытания отдельных функций (задач, комплексов задач). При этом проверяют выполнение требований ТЗ к функциям (задачам, комплексам задач). На втором этапе проводят проверку взаимодействия задач в системе, и выполнение требований ТЗ к системе в целом.

По согласованию с заказчиком проверка задач в зависимости от их специфики может проводиться автономно, или в составе комплекса. Объединение задач при проверке в комплексах целесообразно проводить с учетом общности используемой информации и внутренних связей.

Проверку эффективности работы персонала в диалоговом режиме проводят с учетом полноты и качества выполнения функций системы в целом.

Проверке подлежат, как минимум:

1) Полнота сообщений, директив, запросов, доступных оператору и их достаточность для эксплуатации системы;
2) Интуитивность операторского интерфейса, сложность процедур диалога, необходимость специальной подготовки;
3) Реакция системы и ее частей па ошибки оператора, и защита от несанкционированного доступа;
4) Вспомогательные диагностические средства системы.

Проверка средств восстановления работоспособности АСУТП после отказов должна включать:

1) Проверку наличия в эксплуатационной документации инструкций по восстановлению работоспособности и полноту их описания;
2) Практическую проверку рекомендованных процедур по восстановлению работоспособности;
3) Работоспособность средств резервирования и автоматического восстановления функций.

Проверку комплектности и качества эксплуатационной документации необходимо проводить путем проверки соответствия документации требованиям нормативно-технических документов и ТЗ.

Результаты испытаний объектов, предусмотренных программой испытаний, фиксируются в протоколах, содержащих следующие разделы по каждому типу испытаний:

1) Назначение испытаний и номер раздела Технического задания на создание АСУТП, по которому проводят испытание;
2) Состав технических и программных средств, используемых при испытаниях;
3) Указание методик, в соответствии с которыми проводились испытания, обработка и оценка результатов;
4) Условия проведения испытаний и характеристики исходных данных;
5) Обобщенные результаты испытаний;
6) Выводы о результатах испытаний и соответствии созданной системы или ее частей конкретному разделу требований Технического задания на создание АСУТП.

Протоколы испытаний АСУТП по всем объектам испытаний обобщаются в итоговом едином Протоколе, на основании которого делают заключение о соответствии системы требованиям Технического задания на создание АСУТП, и возможности оформления Акта приемки АСУТП в постоянную эксплуатацию. По результатам приемочных испытаний составляются и подписываются:

- Протоколы испытаний по каждому объекту испытаний;
- Итоговый Протокол испытаний о возможности оформления Акта приемки АСУТП в постоянную эксплуатацию;
- Акт о приемке Системы в постоянную (промышленную) эксплуатацию.

В завершение издается Приказ по предприятию "О вводе АСУТП в постоянную (промышленную) эксплуатацию". Допускается по решению Приемочной комиссии доработка технической документации АСУТП после ее ввода в действие. Сроки доработки указываются в итоговом Протоколе приемочных испытаний.

5.18. Ответственность при эксплуатации и техническом обслуживании АСУТП

Функционирование АСУТП должно быть рассчитано на круглосуточный режим работы, с остановкой на профилактику не чаще, чем 1 раз в год в период капитального ремонта. Эксплуатация КИП и средств автоматизации предусматривает:

- Контроль над работоспособностью, выявление и устранение неисправностей;
- Учет отказов;
- Проведение планово-предупредительных ремонтов;
- Проведение плановых поверок.

Виды, периодичность и регламент обслуживания технических средств должны быть указаны в соответствующих инструкциях по эксплуатации. Общие требования к системам контроля, управления, сигнализации и противоаварийной защиты при эксплуатации, монтаже, наладке и ремонте определяются ПБ 09-540-03 "*Общие правила взрывобезопасности*

для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств". Конкретные требования по эксплуатации КИП и СА регламентируются общезаводскими инструкциями.

Служба главного энергетика отвечает за надежное электроснабжение АСУТП от своих электроустановок, и за состояние линий связи АСУТП, проходящих по кабелям цеха связи. За эксплуатацию и обслуживание программно-технических средств АСУТП несет ответственность служба главного метролога данного производства или завода. Ответственность за эксплуатацию АСУТП и эффективность комплекса в целом несет главный инженер данного производства.

5.19. Требования к документированию

Требования к содержанию документов, разрабатываемых при создании автоматизированной Системы, установлены указаниями руководящего документа РД 50-34.698-90 МЕТОДИЧЕСКИЕ УКАЗАНИЯ. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. *"Автоматизированные системы. Требования к содержанию документов*", а также соответствующими государственными стандартами:

- Единой системы программной документации (ЕСПД);
- Единой системы конструкторской документации (ЕСКД);
- Системы проектной документации для строительства (СПДС);
- ГОСТ 34.602-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

Виды и комплектность документов регламентированы ГОСТ 34.201-89 *"Виды, комплектность и обозначение документов при создании автоматизированных систем".* Состав и содержание документов по ГОСТ 34.201-89 является общим для всех видов автоматизированных систем, и при необходимости может дополняться в зависимости от особенностей конкретно создаваемой Системы. Допускается включать в документы дополнительные разделы и сведения, объединять и исключать разделы.

Как сказано, согласно ГОСТ 34.201-89, пункт 2.1, "Перечень наименований разрабатываемых документов и их комплектность на Систему и ее части" должен быть определен в Техническом задании на Систему. В любом случае конкретный состав проектной документации должен быть строго определен в Договоре между Разработчиком и Заказчиком на разработку Рабочего (технорабочего) проекта и рабочей документации. Тогда в Техническом задании можно ограничиться ссылкой на этот договор.

В составе Технического (технорабочего) проекта разрабатывается документация по общесистемным решениям, организационному, техническому, информационному и программному обеспечению, а также проектно-сметная документация. В состав Рабочей документации входит эксплуатационная документация по информационному, программному, техническому и метрологическому обеспечению, а также проектно-сметная документация. В соответствии с ГОСТ 34.201-89, п. 1.3.1, табл. 2 "Наименование конкретных документов, разрабатываемых при проектировании системы в целом или ее части", виды документов, разрабатываемых на стадиях Технического проекта и Рабочей документации, имеющие отношение к проектно-сметным, выполняются Проектной организацией.

Стандартная техническая документация иностранных поставщиков оборудования должна представляться и на английском, и на русском языке. Вся Рабочая документация (документация Технорабочего проекта), разработанная применительно к конкретному проекту, должна быть на русском языке.

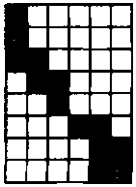
Количество экземпляров проектной и эксплуатационной документации, предоставляемой Заказчику, определяется договорами с Поставщиком оборудования и Разработчиком проекта, однако в любом случае должно быть НЕ МЕНЕЕ ТРЕХ.

5.20. План-график и распределение работ по созданию АСУТП

В заключение приводится подробный **План-график и распределение работ по созданию АСУТП** (см. таблицу 5.1).

Таблица 5.1

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители П&Е*	Зд £ а Ш	Месяц с начала работ 1 I 2 I 3 I 4 I 5 I 6 I 7 I 8 I 9 I 10 I 11 I 12 I 13 I 14 I 15 I 16 I 17 I 18 I
00	Предпроектные стадии			
01	Формирование требований к АСУТП			
02	Проведение тендера среди ведущих фирм-поставщиков			
03	Разработка и выбор концепции АСУТП			
04	Разработка ТЭО на создание АСУТП			
05	Подготовка перечня входов-выходов РСУ и ПАЗ			
06	Разработка Технического Задания на создание АСУТП			
07	Подготовка опросных листов на оборудование КИПиА			
10	Первое техническое (организационное) совещание			
11	Утверждение перечня входов-выходов РСУ и ПАЗ			
12	Утверждение опросных листов на оборудование КИПиА			
13	Утверждение спецификаций оборудования РСУ и ПАЗ			
14	Утверждение функций РСУ и ПАЗ			
15	Утверждение Плана-графика работ			

Поставщик

Завод

Служба автоматизации

Проектная организация

Отвиактитвт, •

Исполнители +

Продолжение таблицы 5.1 о

План-график и распределение работ по созданию АСУТП

Ш	Наименование этапов работы	Исполнители	Месяц с начала работ
		0s Ei За Si Пв -6 5 - 4 - 3 -2 -1	1 | 2 | з | 4 | 5 Ы 171 э| 91 ю| 111 м\ I 1311411S11в| 171 161
20	Разработка технического проекта		
21	р%>рудовани? КИПиА		
	- Планы расположения вновь монтируемых средств КИПиА		
	- Заказные спецификации средств КИПиА		
	- Заказные спецификации на кабель с расшифровкой типов		
	- Спецификаций запасных частей на средства КИПиА		
	- Заказные спецификации средств поверки и ремонта		
	- Спецификация материалов для монтажа оборудования КИПиА		
	- Деталировочные чертежи приборов		
	- Эскизы монтажа датчиков на аппаратах и трубопроводах		
	- Кабельные журналы для подключения оборудования КИПиА к кроссовым шкафам РСУ и ПАЗ		
	- Чертежи кабельной трассировки в пределах помещений управл		
	- Эскизы монтажно-технологических схем технологического процесса с привязкой средств КИПиА		
	- Перечень обогреваемых импульсных проводок		
	- Схемы электропитания, потребляемая мощность на каждом фидере с предохранителем		
	- Каталоги на средства КИПиА и кабели, с типовыми чертежами конструкций для установки приборов		
	- Перечень точек отбора проб, связанных с РСУ, составы проб		

Продолжение таблицы 5.1

План-график и распределение работ по созданию АСУТП

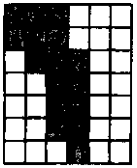
Наименование этапов работы	Исполнители	Месяц с начала работ
Проектирование технических средств АСУТП		
- План расположения технических средств АСУТП		
- Заказные спецификации технических средств РСУ и ПАЗ		
- Архитектура и конструктивные чертежи РСУ и ПАЗ		
- Схемы компоновки РСУ и ПАЗ		
- Схемы размещения и подключения барьеров РСУ и ПАЗ		
- Схемы кроссового оборудования РСУ и ПАЗ		
- Кабельные журналы для подкл крое шкафов к РСУ и ПАЗ		
- Схемы электропитания и заземления		
• Расчеты потребляемой мощности и теплоотдачи		
Проектирование поогоаммных средств АСУТП		
•Разработка функциональных схем автоматизации		
• Анализ логических схем защиты для системы ПАЗ		
- Составление перечней контуров управления		
- Составление перечней контуров защиты		
- Разработка эскизов видеограмм		
- Распределение видеограмм по рабочим местам		
- Разработка эскизов технологических отчетов		
- Описание автоматизируемых функций управления		
* Описание автоматизируемых функций защиты		

Продолжение таблицы 5.1

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		Ней Зд&пе -в -5 -4 3 2 1	I 1 I 2 | 3 | 4 I 5 | 6 | I 7 I 8 I 9 110| 11112| 1131 141 15| 16| 17116|
30	Приемка технического проекта		
31	Окончательное уточнение требований к Системе	I I I I I I I	ГГТТТ ш
32	Рассмотрение и приемка технического проекта		П Т Т Т Т Т
33	Утверждение состава и оглавлений документации рабочего проекта по принадлежности-		
	-КИПиА		
	-РСУ		
	-ПАЗ		
34	Оформление заданий на проектирование в смежных частях проекта		

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		Па 2д £а Ос -в * -4 .3 2 .1	Ы 2 | 3 Ы 5| 6| | 7| 8| 9 | ю| 11112 f 113| 14| 15| 16| 17| 16|
40	**Стадия рабочего проектирования**		
41	Корректировка докуц^ции трхничдскдгд пр-кта пф принадлежности-		
	•КИПиА -РСУ •ПАЗ		E
42	Разработка прикладного программного обеспечения РСУ		
	- Конфигурирование базы данных - Конфигурирование станций технолога-оператора - Конфигурирование мнемосхем • Конфигурирование отображения сигнализаций и блокировок - Конфигурация трендов - Конфигурация архивов - Конфигурация технологических отчетов		
	- Конфигурирование базы данных обмена с РСУ - Программирование логики ПАЗ на языке блочных диаграмм - Конфигурирование программы последовательности останова		*m*

Продолжение таблицы 5.1 о

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		По Рi За Пц	1 1 2 1 з | 4 | 5 | б | 1 7 I 6 I 9 | ю| 11112 j 11з| 14| 1511б| 17] 1в|
44	Разработка технической документации по КИПиА		
	Пояснительная записка по КИПиА, содержащая		
	- Выбор приборов и средств автоматизации		
	• Описание средств автоматизации, увязанное со схемами трубопроводной обвязки с указанием КИПиА		
	- Описание сигнализаций и блокировок		
	- Принципиальные правила монтажа		
	- Монтажно-технологические схемы технологического процесса с привязкой средств КИПиА		
	• Монтажные чертежи вновь проектируемого оборудования		
	- Схемы принципиальные электрические всех цепей с обозначением всех приборов и мест подключений		
	- Компоновочные чертежи приборов с указанием взаимного расположения,отметок,соединительных коробок и каб трасс		
	- Схемы трубопроводной обвязки с указанием КИП со всеми целями КИП		
	- Чертежи монтажа датчиков на аппаратах и трубопроводах		
	- Кабельные журналы для подключения оборудования КИПиА к кроссовым шкафам РСУ и ПАЗ		
	- Чертежи кабельной трассировки в пределах помещений управл		
	- Инструкции по эксплуатации, монтажу, проверке и ремонту КИП		

Продолжение таблицы 5.1

План-график и распределение работ по созданию АСУТП

NQ	Наименование этапов работы	Исполнители ШЕа ЗаСаОв -6 5 -4 -3 21	Месяц с начала работ | 1 [г | з | 4 | 5 | б | 111819 [io|n|i2[[13] i-^l 151 ie [17 [1в[
45	Разработка технической документации по РСУ		
	- План размещения оборудования 8 стойках		
	- Схемы и конфигурация модулей РСУ		
	- Схемы питания и заземления РСУ		
	- Кабельный журнал внутрисистемных соединений		
	- Инструкции по монтажу и наладке		
	- Полное техническое описание функций РСУ		
	- Функциональные схемы управления		
	- Схемы измерительных и управляющих контуров РСУ		
	- Описание системных и технологических событий		
	- Технологические отчеты		
	- Руководства технолога-оператора		
	- Протокол-заключение о проведении заводских испытаний фирмы-изготовителя РСУ на площадке изготовителя	d I]	ГЕ
	Полный комплект стандартных руководств пользователя по всей номенклатуре поставляемой продукции		
	-КИПиА		
	-РСУ		1
	-ПАЗ		

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		Os Es 2a £r Oc -6-5-4-3 2	1 2 3 4 5 6 I 9 j ю 1112 1 1 13 14 1S 16 17 16
46	Разработка технической документации по системе ПАЗ		
	- Чертежи компоновки системы в шкафах		И
	- Установочные чертежи		
	- Схемы и конфигурация модулей ПАЗ		
	- Схемы распределения питания внутри шкафов		
	• Схемы подключения заземления системы		
	- Кабельный журнал внутрисистемных соединений		
	- Схемы подключения каналов и внешних источников питания		
	- Инструкции по монтажу и наладке		П
	- Описание функций ПАЗ		Т Ш
	- Схемы измерительных и управляющих контуров ПАЗ		
	- Распечатка программы логического управления системы ПАЗ		
	- База данных параметров ввода-вывода и обмена с РСУ		
	• База данных программы определения первопричины останова		
	- Таблицы подключения каналов ввода-вывода к терминальным панелям и клеммным сборкам шкафов системы ПАЗ		
	- Рекомендации по регламенту эксплуатации системы ПАЗ		I I I I Ч I Ш I I I I I I I
	- Протокол-заключение о проведении заводских испытаний фирмы-изготовителя системы ПАЗ на площадке изготовителя	\ I I I I I I I	

Продолжение таблицы 5.1 **о**

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители Qa Pi Зд С* Ik - 6 5 4 - 3 - 2	Месяц с начала работ 3 4 5 6 7 8 9 10 n t2 11з 14 15 16 17 16
47	**Формирование паспорта АСУТП, включающего:**		
	- Общие сведения о входящих в АСУТ) системах - Основные характеристики систем - Комплектность и реквизиты систем - Акты приемо-сдаточных испытаний		
	Сертификаты качества отдельных компонентов систем -КИПиА -РСУ -ПАЗ		
	Гарантии изготовителя/поставщика -КИПиА -РСУ -ПАЗ		
48	Приемка рабочего проекта	ТТТТ	

Продолжение таблицы 5.1 **о**

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		Па р& ЗдfаШ -в-5^-3 2	| 1 I 2| 3 | 4 j 5| 6j | 7 | В I 9 I 1oj 11112| Il3|14|15|16|17|18|
50	Обучение		
	• Обучение по аппаратному обеспечению РСУ - Обучение по программному обеспечению РСУ - Обучение по аппаратному обеспечению ПАЗ - Обучение по программному обеспечению ПАЗ • Обучение по системе обслуживания средств КИПиА (AMS) - Обучение по эксплуатации и обслуживанию АСУТП		Н
60	Доставка оборудования на площадку:		
	Таможенная очистка, Страхование груза, Доставка оборудования на площадку. Получение оборудования, проверка комплектности по принадлежности		
	-КИПиА -РСУ -ПАЗ - Вспомогательное оборудование		m

Продолжение таблицы 5.1 **О**

План-график и распределение работ по созданию АСУТП

№	Наименование этапов работы	Исполнители	Месяц с начала работ
		Дь Ра За Са Е	1 | г | з | 4 | 5 | 6 | I 7| 8 I 9 | ю| 111 "12I 113| 14| 15| 16| 17| 18|
70	Сборка и монтаж оборудования		
71	Монтаж и пусконаладка оборудования КИПиА		
72	Сборка и монтаж оборудования РСУ		
	- Монтаж оборудования РСУ		
	- Маркировка кабелей		
	- Выполнение нестандартных кабельных соединений		
	- Подключение питания		
	- Функциональный тест, загрузка базового прогр обеспечения		
	- Прозвонка сигнальных кабелей		
	- Настройка измерительных преобразователей		
	- Установка прикладного программного обеспечения		
	- Проверка и настройка программного обеспечения		
73	Сборка и монтаж оборудования системы ПАЗ		
	- Монтаж оборудования системы ПАЗ		
	- Маркировка кабелей		
	- Выполнение нестандартных кабельных соединений		
	- Подключение питания		
	- Функциональный тест, загрузка базового прогр обеспечения		
	- Прозвонка сигнальных кабелей		
	• Настройка измерительных преобразователей		
	- Установка прикладного программного обеспечения		
	- Проверка и настройка программного обеспечения		

Окончание таблицы 5.1

План-график и распределение работ по созданию АСУТП

N8	Наименование этапов работы	Исполнители	Месяц с начала работ
		Da Ei & Qa он	ЕЛЕ 1 7 1 8 | 9 j10|11|12| 113|14|15|ie|17|181
80	Повеока. испытания и запуск Системы		
81	Повеока и калибровка измерительных каналов		
	- Утверждение методик поверки средств измерения		
	- Проведение поверки и калибровки		
82	Предварительные испытания		
	- Составление Программы предварительных испытаний		
	- Составление Методики предварительных испытаний		
	- Проведение предварительных испытаний (72 часа)		
	- Утверждение Протокола предварительных испытаний		
83	Опытная эксплуатация		
	- Составление Программы Опытной эксплуатации		
	- Подготовка Рабочего журнала опытной эксплуатации		
	- Проведение опытной эксплуатации Системы		
	• Утверждение Акта о завершении опытной эксплуатации		
84	Приемочные испытания		
	- Утверждение Программы приемочных испытаний		
	- Проведение приемочных испытаний Системы		
	- Утверждение Протокола приемочных испытаний		
	- Утверждение Акта о приемке Системы в промышленную эксплуатацию		

Глава 6

СОСТАВ И СОДЕРЖАНИЕ ДОКУМЕНТАЦИИ ПРОЕКТА АСУТП

Содержание проектной документации для автоматизированных систем (АС) по ГОСТ 34.201-89 *"Виды, комплектность и обозначение документов при создании автоматизированных систем",* и РД 50-34.698-90 *"Автоматизированные системы. Требования к содержанию документов"* является общим для всех типов автоматизированных систем. Однако процедура создания систем управления технологическими процессами обладает множеством специфических особенностей, которые никак не отражены в нормативных документах, но требуют своего адекватного воплощения в проектной документации.

Настоящее руководство распространяется на автоматизированные системы управления технологическими процессами - АСУТП, и устанавливают требования к составу и содержанию документов, которые должны разрабатываться при создании АСУТП, и построены с максимально возможным учетом существующих стандартов.

Как уже было отмечено в предыдущей главе, согласно ГОСТ 34.601-90, пункт 2.2, *"Стадии и этапы, выполняемые организациями-участниками работ по созданию автоматизированной системы, устанавливаются во взаимных договорах и в Техническом задании ".*

Согласно ГОСТ 34.201-89, пункт 2Л,

"Перечень наименований разрабатываемых документов и их комплектность на Систему и ее части должен быть определен в Техническом задании на создание автоматизированной системы "

В любом случае перечень проектной документации должен быть строго определен в Договоре между Разработчиком и Заказчиком на разработку Рабочего проекта и рабочей документации (технорабочего) проекта. Тогда в Техническом задании достаточно указать ссылку на этот договор.

Вместе с тем, согласно положению РД 50-34.698-90 *"Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов*", пункт 1.3, "*Содержание каждого документа, разрабатываемого при проектировании автоматизированных систем (АС) согласно ГОСТ 34.201-89, - запятая - определяет Разработчик в зависимости от объекта проектирования (система, подсистема и т.д.)".*

Поэтому если Заказчик предпочитает установить единый подход к документальному оформлению своих проектов по автоматизации вне зависимости от конкретного разработчика, он вполне может узаконить свои требования в собственных Стандартах предприятия на создание АСУТП, и жестко определить и состав, и содержание документации проекта АСУТП.

Две стадии проекта создания АСУТП выделяются особо -

- Стадия формализации и утверждения требований к системе - стадия "Техническое задание на создание АСУТП", и
- Стадия "Ввод в действие".

Важность этих стадий, по мнению автора работы такова, что две следующих главы настоящего руководства целиком посвящены представлению документов, которые, как альфа и омега олицетворяют собой всю эпопею проекта создания АСУТП - от замысла до результата:

- Глава "Техническое задание на создание АСУТП", которое во многом, если не сказать во всем, предопределяет конечный результат, и
- Глава "Программа и методика испытаний", в которой под этим многозначным определением представлена процедура достойного прохождения испытаний, и реальный комплект документов и правил, которые необходимо создать и выполнить для законного оформления результата.

6.1. Общие положения

Требования к содержанию и оформлению документов, разрабатываемых при создании автоматизированных систем, установлены:

- Стандартом РД 50-34.698-90 "Требования к содержанию документов", а также
- Государственными стандартами Единой системы программной документации (ЕСПД),
- Стандартами Единой системы конструкторской документации (ЕСКД), и
- Стандартами Системы проектной документации для строительства (СПДС).

Виды и комплектность документов регламентированы ГОСТ 34.201 *"Виды, комплектность и обозначение документов при создании автоматизированных систем*Согласно этому ГОСТу, содержание документов является общим для всех видов АС и при необходимости может дополняться в зависимости от особенностей создаваемой АС. Допускается включать в документы дополнительные разделы и сведения, объединять и исключать разделы.

Общее требование, которое необходимо сразу установить в Техническом задании, состоит в следующем:

Стандартная техническая документация иностранных производителей оборудования должна представляться и на английском, и на русском языке. Вся Рабочая документация (Технорабочий проект), разработанная применительно к конкретному проекту, должна быть на русском языке. Количество экземпляров стандартной, проектной и эксплуатационной документации, предоставляемой Заказчику, определяется договорами с Поставщиком оборудования и Разработчиком проекта, однако в любом случае должно быть НЕ МЕНЕЕ ТРЕХ.

6.2. Исключение, изменение и включение стадий выполнения проекта

Согласно ГОСТ 34.601, пункт 2.2, допускается:

- Исключать стадию "Эскизный проект";
- Исключать отдельные этапы работ на всех стадиях;

- Объединять стадии "Технический проект" и "Рабочая документация" в одну стадию - "Технорабочий проект".

Кроме того, в зависимости от специфики создаваемой АС, и условий создания допускается:

1) Выполнять отдельные этапы работ до завершения предшествующих стадий;
2) Параллельное во времени выполнение этапов работ;
3) Включение новых этапов работ.

В соответствии с предоставленными правами, устанавливаются следующие решения по составу проектных работ на создание АСУТП:

1. Стадия "Эскизный проект" - исключается.
2. Предпочтительным способом выполнения проекта является одностадийный "Технорабочий проект".
3. С учетом специфики процесса создания АСУТП произведено:
   - Исключение отдельных этапов работ, и соответствующих документов.
   - Изменение названий отдельных этапов работ, и названий соответствующих документов.
   - Включение новых этапов работ и новых документов.

6.3. Требования к содержанию документов по Общесистемным решениям

Документы, помеченные знаком *, после необходимой корректировки переходят в состав Рабочей документации из Технического проекта, либо создаются непосредственно в процессе разработки единого Технорабочего проекта.

6.4. Документ "Ведомость проекта" * (ТП)

Ведомость содержит перечень всех документов, разработанных на данной стадии создания АСУТП. Документ следует выполнять по ГОСТ 2.106 ЕСКД "*Текстовые документы*". Наименования разделов и подразделов записываются в графах "Обозначение" и "Наименование" в виде заголовков и выделяются подчеркиванием.

6.5. Документ "Пояснительная записка к проекту" * (П2)

Документ содержит следующие разделы:

- Общие положения;
- Описание процесса деятельности;
- Основные технические решения;
- Мероприятия по подготовке объекта автоматизации к вводу системы в действие.

В разделе "Общие положения" приводится:

1) Наименование АСУТП, и наименования документов, их номера и дату утверждения, на основании которых ведется проектирование АСУТП;
2) Перечень организаций, участвующих в разработке системы, сроки выполнения стадий;
3) Цели, назначение и области использования АСУТП;
4) Подтверждение соответствия проектных решений действующим нормам и правилам техники безопасности, пожаро - и взрывобезопасности;
5) Сведения об использованных при проектировании нормативно-технических документах;
6) Сведения о НИР, передовом опыте, изобретениях, использованных при разработке проекта;
7) Очередность создания системы и объем каждой очереди.

В разделе **"Описание процесса деятельности"** отражается состав процедур (операций) с учетом обеспечения взаимосвязи и совместимости процессов автоматизированной к неавтоматизированной деятельности, формируются требования к организации работ в условиях функционирования АСУТП.

В разделе **"Основные технические решения"** приводятся:

1) Решения по структуре системы, подсистем, средствам и способам связи для информационного обмена между компонентами системы, подсистем:
2) Решения по взаимосвязям АСУТП со смежными системами, обеспечению ее совместимости;
3) Решения по режимам функционирования, диагностированию работы системы;
4) Решения по численности, квалификации и функциям персонала АСУТП, режимам его работы, порядку взаимодействия;

5) Сведения об обеспечении заданных в Техническом задании (ТЗ) потребительских характеристик системы (подсистем), определяющих ее качество;
6) Состав функций и комплексов задач, реализуемых системой (подсистемой);
7) Решения по комплексу технических средств, его размещению на объекте;
8) Решения по составу информации, объему, способам ее организации, видам машинных носителей, входным и выходным документам и сообщениям, последовательности обработки информации и другим компонентам;
9) Решения по составу программных средств, языкам деятельности, алгоритмам процедур и операций и методам их реализации.

В разделе приводятся в виде иллюстраций другие документы, которые допускается включать по ГОСТ 34.201.

В разделе **"Мероприятия по подготовке объекта автоматизации к вводу системы в действие"** приводятся:

1) Мероприятия по приведению информации к виду, пригодному для обработки средствами АСУТП;
2) Мероприятия по обучению и проверке квалификации персонала;
3) Мероприятия по созданию необходимых подразделений и рабочих мест;
4) Мероприятия по изменению объекта автоматизации;
5) Другие мероприятия, исходящие из специфических особенностей объекта автоматизации.

6.6. Документ "Описание автоматизируемых функций" *(ПЗ)

Документ "Описание автоматизируемых функций" содержит следующие разделы:

- Исходные данные;
- Цели АСУТП и автоматизированные функции;
- Характеристика функциональной структуры;
- Типовые решения.

В разделе **"Исходные данные"** приводится:

1) Перечень исходных материалов и документов, использованных при разработке функциональной части проекта АСУТП;
2) Особенности объекта управления, влияющие на проектные решения по автоматизированным функциям;
3) Данные о системах управления, взаимосвязанных с разрабатываемой АСУТП, и сведения об информации, которой она должна обмениваться с абонентами и другими системами;
4) Описание информационной модели объекта вместе с его системой управления.

В разделе **"Цели АСУТП и автоматизированные функции"** приводится описание автоматизированных функций, направленных на достижение установленных целей.

Раздел **"Характеристика функциональной структуры"** содержит:

1) Перечень подсистем АСУТП с указанием функций и (или) задач, реализуемых в каждой подсистеме;
2) Описание процесса выполнения функций (при необходимости);
3) Необходимые пояснения к разделению автоматизированных функций на действия (операции), выполняемые техническими средствами и человеком;
4) Требования к временному регламенту и характеристикам процесса реализации автоматизированных функций (точности, надежности и т.п.) и решения задач.

В разделе **"Типовые решения"** приводится перечень типовых решений с указанием функций, задач, комплексов задач, для выполнения которых они применены.

6.7. Документ "Описание постановки задач (комплекса задач)" *(П4)

Документ содержит следующие разделы:

- Характеристики комплекса задач;
- Выходная информация;
- Входная информация.

В разделе **"Характеристики комплекса задач"** приводится:

1) Назначение комплекса задач;
2) Перечень объектов (технологических объектов управления, подразделений предприятия и т. п.), при управлении которыми решается данный комплекс задач;
3) Периодичность и продолжительность решения;
4) Условия, при которых прекращается решение комплекса задач автоматизированным способом;
5) Связи данного комплекса задач с другими комплексами (задачами) АСУТП;
6) Должности лиц и наименования подразделений, определяющих условия и временные характеристики конкретного решения задачи (если они не определены общим алгоритмом функционирования системы);
7) Распределение действий между персоналом и техническими средствами при различных ситуациях решения комплекса задач.

Раздел **"Выходная информация"** содержит:

1) Перечень и описание выходных сообщений;
2) Перечень и описание имеющих самостоятельное, смысловое значение структурных единиц информации выходных сообщений (показателей, реквизитов и их совокупностей, сигналов управления) или ссылку на документы, содержащие эти данные.

В описании по каждому выходному сообщению следует указывать:

1) Идентификатор;
2) Форму представления сообщения (документ, видеокадр, сигнал управления) и требования к ней;
3) Периодичность выдачи;
4) Сроки выдачи и допустимое время задержки решения;
5) Получателей и назначение выходной информации.

В описании по каждой структурной единице информации следует указывать:

1) Наименование;
2) Идентификатор выходного сообщения, содержащего структурную единицу информации;
3) Требования к точности и надежности вычисления.

Раздел **"Входная информация"** должен содержать:

1) Перечень и описание входных сообщений (идентификатор, форму представления, сроки и частоту поступления);
2) Перечень и описание структурных единиц информации входных сообщений или ссылку на документы, содержащие эти данные.

В описании по каждой структурной единице информации входных сообщений следует указывать:

1) Наименование;
2) Требуемую точность;
3) Источник информации (документ, видеокадр, устройство, кодограмма, информационная база на машинных носителях);
4) Идентификатор источника информации.

6.8. Документ "Общее описание системы" (ПД)

Документ содержит следующие разделы:

- Назначение системы;
- Описание системы;
- Описание взаимосвязей АСУТП с другими системами;
- Описание подсистем.

В разделе **"Назначение системы"** указывается:

1) Вид деятельности, для автоматизации которой предназначена система;
2) Перечень объектов автоматизации, на которых используется система;
3) Перечень функций, реализуемых системой.

В разделе **"Описание системы"** указывается:

1) Структура системы и назначение ее частей;
2) Сведения об АСУТП в целом и ее частях, необходимые для обеспечения эксплуатации системы;
3) Описание функционирования системы и ее частей.

В разделе **"Описание взаимосвязей АСУТП с другими системами"** приводится:

1) Перечень систем, с которыми взаимодействует АСУТП;
2) Описание связей между системами;
3) Описание регламента связей;

4) Описание взаимосвязей АСУТП с подразделениями объекта автоматизации.

В разделе **"Описание подсистем"** приводится:

1) Структура подсистем, и назначение их частей;
2) Сведения о подсистемах и их частях, необходимые для обеспечения их функционирования;
3) Описание функционирования подсистем и их частей.

6.9. Документ "Программа и методика испытаний (компонентов, комплексов средств автоматизации, подсистем, систем)" (ПМ)

Программа и методика испытаний системы предназначена для:

- Определения предмета испытаний;
- Определения порядка испытаний;
- Методов контроля;
- Проверки проектных решений;
- Определения качества выполненных работ;
- Подтверждения показателей качества функционирования системы (подсистемы);
- Проверки соответствия системы требованиям промышленной безопасности и Технического задания;
- Определения продолжительности и режима испытаний.

Документ "Программа и методика испытаний (ПМ)" создается Разработчиком системы в составе документации рабочего (технорабочего) проекта. На стадии "Ввод в действие" на основе проектной "Программы и методики испытаний (ПМ)" вначале создается "Программа предварительных испытаний", а по окончанию опытной эксплуатации - "Программа приемочных испытаний" системы.

Согласно РД 50-34.698-90, пункт 2.14.3, **эти Программы испытаний должны содержать перечни конкретных проверок (решаемых задач), которые следует проводить для подтверждения выполнения требований ТЗ, со ссылками на соответствующие методики (разделы методик) испытаний.** Соответственно, базовый перечень проверок системы, подлежащих включению в конкретные программы испытаний для подтверждения соответствия требованиям Технического

задания, должен быть определен в проектном документе "Программа и методика испытаний (ПМ)". Этот перечень проверок должен включать определение и описание следующих проверок и соответствующих методик:

1. Проверка комплектности комплекса технических средств и стандартной технической документации;
2. Проверка состава и содержания документации технорабочего проекта;
3. Автономная проверка готовности комплекса технических средств;
4. Метрологическая поверка измерительных каналов;
5. Проверка отказоустойчивости и функций самодиагностики системы;
6. Проверка реализации функций АСУТП на соответствие требованиям Технического задания;
7. Проверка квалификации и уровня подготовки оперативного (технологического) и эксплуатационного (обслуживающего) персонала для работы в условиях функционирования АСУТП.

Описание методов испытаний системы по отдельным показателям рекомендуется располагать в той же последовательности, в которой эти показатели расположены в перечне проверок.

Методики испытаний разрабатываются с использованием типовых методик испытаний. Отдельные положения типовых методик могут уточняться и конкретизироваться в зависимости от особенностей системы и условий проведения испытаний. Согласно РД 50-34.698-90, пункт 2.14.17, содержание разделов методик испытаний также определяет Разработчик. Документ **"Программа** и **методика** испытаний" содержит разделы:

- Объект испытаний;
- Цель испытаний;
- Общие положения;
- Объем испытаний;
- Условия и порядок проведения испытаний;
- Материально-техническое обеспечение испытаний;
- Метрологическое обеспечение испытаний;
- Отчетность.

В документ включаются приложения.

В зависимости от особенностей систем допускается объединять или исключать отдельные разделы при условии изложения их содержания в других разделах программы испытаний, а также включать в нее дополнительные разделы.

В разделе **"Объект испытаний"** указывается:

1) Полное наименование системы, обозначение;
2) Комплектность испытательной системы.

В разделе **"Цель испытаний"** указываются конкретные цели и задачи, которые должны быть разрешены в процессе испытаний.

В разделе **"Общие положения"** указывается:

1) Перечень руководящих документов, на основании которых проводятся испытания;
2) Место и продолжительность испытаний;
3) Организации, участвующие в испытаниях;
4) Перечень ранее проведенных испытаний;
5) Перечень предъявляемых на испытания документов, откорректированных по результатам ранее проведенных испытаний.

В разделе **"Объем испытаний"** указывается:

1) Перечень этапов испытаний, состав и описание проверок на каждом этапе, а также количественные и качественные характеристики, подлежащие оценке;
2) Последовательность проведения и режима испытаний;
3) Требования по испытаниям программных средств;
4) Перечень работ, проводимых после завершения испытаний, требования к ним, объем и порядок проведения.

В разделе **"Условия и порядок проведения испытаний"** задаются:

1) Условия проведения испытаний;
2) Условия начала и завершения отдельных этапов испытаний;
3) Имеющиеся ограничения в условиях проведения испытаний;
4) Требования к техническому обслуживанию системы;
5) Меры, обеспечивающие безопасность и безаварийность проведения испытаний;
6) Порядок взаимодействия организаций, участвующих в испытаниях;

7) Порядок привлечения экспертов для исследования возможных повреждений в процессе проведения испытаний;
8) Требования к персоналу, проводящему испытания, и порядок его допуска к испытаниям.

В разделе **"Материально-техническое обеспечение испытаний"** указывается конкретные виды материально-технического обеспечения с распределением задач и обязанностей организации, участвующих в испытаниях.

В разделе **"Метрологическое обеспечение испытаний"** приводится перечень мероприятий по метрологическому обеспечению испытаний с распределением задач и ответственности организаций, участвующих в испытаниях.

В разделе **"Отчетность"** приводится перечень отчетных документов, которые должны оформляться в процессе испытаний и по их завершению, с указанием организаций и предприятий, разрабатывающих, согласующих и утверждающих их, и сроки оформления этих документов. В обязательном порядке должно быть обеспечено наличие следующих документов:

- *Сертификаты Госстандарта России об утверждении типа средств измерений;*
- *Разрешения Ростехнадзора России на применение оборудования;*
- *Методики поверки для СИ, для которых нет общегосударственных стандартов;*
- *Сертификаты о калибровке измерительных каналов системы;*
- *Инструкции по монтажу, эксплуатации и техническому обслуживанию* ***на русском языке.***

К отчетным документам для конкретных программ испытаний по конкретному этапу испытаний относятся Протоколы и Отчеты о результатах испытаний, а также Акт о готовности или неготовности системы к дальнейшим испытаниям.

В приложения к "Программе и методике испытаний" включаются перечни методик испытаний, математических соотношений и комплексных проверок, применяемых для оценки характеристик системы. Методики испытаний разрабатываются на основе типовых методик испытаний, и методик изготовителя оборудования, сертифицированных Госстандартом. При этом отдельные положения типовых методик испы-

таний могут уточняться и конкретизироваться в разрабатываемых методиках конкретных испытаний в зависимости от особенности системы, и условий проведения испытаний. Содержание разделов методик устанавливает Разработчик.

Тщательное и подробное проведение испытаний имеет исключительное значение для определения жизнеспособности Системы. В главе "*Программа и методика испытаний*" приводится авторский вариант документа рабочего (технорабочего) проекта "Программа и методика испытаний", а также полный комплект документов, необходимых для проведения и оформления предварительных и приемочных испытаний.

6.10. Документ "Ведомость эксплуатационных документов" (ЭД)

Документ содержит перечень эксплуатационных документов согласно ГОСТ 34.201. Ведомость заполняется по разделам - частям проекта на автоматизированную систему.

6.11. Документ "Паспорт" (ПС)

Документ содержит следующие разделы:

- Общие сведения о АСУТП;
- Основные характеристики АСУТП;
- Комплектность АСУТП;
- Свидетельство (Акт) о приемке АСУТП;
- Гарантии изготовителя (поставщика);
- Сведения о рекламациях.

В разделе **"Общие сведения об АСУТП"** указывается наименование АСУТП, ее обозначение, присвоенное разработчиком, наименование предприятия - поставщика, и другие сведения о АСУТП в целом.

В разделе **"Основные характеристики АСУТП"** должны быть приведены:

1) Сведения о составе функций, реализуемых АСУТП, в том числе измерительных и управляющих;
2) Описание принципа функционирования АСУТП;
3) Общий регламент и режимы функционирования АСУТП и сведения о возможности изменения режимов ее работы;

4) Сведения о совместимости АСУТП с другими системами.

В разделе **"Комплектность АСУТП"** указываются все непосредственно входящие в состав АСУТП комплексы технических и программных средств, отдельные средства, в том числе носители данных и эксплуатационные документы.

В разделе **"Свидетельство о приемке АСУТП"** приводится дата подписания Акта о приемке АСУТП в промышленную эксплуатацию и фамилии лиц, подписавших акт.

В разделе **"Гарантии изготовителя"** приводятся сроки гарантии на АСУТП в целом и на ее отдельные части, если эти сроки не совпадают со сроками гарантии АСУТП в целом.

В разделе **"Сведения о рекламациях"** регистрируются все предъявленные рекламации, их краткое содержание и меры, принятые по рекламациям.

6.12. Документ "Формуляр" (ФО)

Документ содержит следующие разделы:

- Общие сведения о АСУТП;
- Основные характеристики АСУТП;
- Комплектность АСУТП;
- Свидетельство (Акт) о приемке АСУТП;
- Гарантийные обязательства;
- Сведения о состоянии АСУТП;
- Сведения о рекламациях.

В разделе "Общие сведения **о АСУТП"** указывается:

- Наименование АСУТП;
- Шифр АСУТП;
- Наименование разработчика;
- Дата сдачи АСУТП в эксплуатацию;
- Общие указания персоналу по эксплуатации АСУТП;
- Требования по ведению формуляра и о месте его хранения, в том числе перечень технической документации, с которой должен быть ознакомлен персонал.

В разделе **"Основные характеристики АСУТП"** указываются:

1) Перечень реализуемых функций;

2) Количественные и качественные характеристики АСУТП и ее частей;
3) Описание принципов функционирования АСУТП, регламент и режимы функционирования;
4) Сведения о взаимодействии АСУТП с другими системами.

В разделе **"Комплектность АСУТП"** приводится:

1) Перечень технических и программных средств, в том числе носителей данных;
2) Перечень эксплуатационных документов.

В разделе **"Свидетельство о приемке АСУТП"** указываются:

1) Даты подписания актов о приемке АСУТП и ее частей в промышленную эксплуатацию;
2) Фамилии председателей комиссий, осуществлявших приемку АСУТП.

В разделе **"Гарантийные обязательства"** указываются:

1) Гарантийные обязательства разработчиков АСУТП по системе в целом и частям, имеющим разные гарантийные сроки;
2) Перечень технических средств АСУТП, имеющих гарантийные сроки службы меньше гарантийных сроков для системы.

В разделе **"Сведения о состоянии АСУТП"** указываются:

1) Сведения о неисправностях, в том числе дату, время, характер, причину возникновения и лицах, устранивших неисправность;
2) Замечания по эксплуатации и аварийным ситуациям, принятые меры;
3) Сведения о проведении проверок измерительных устройств и точностных характеристиках измерительных каналов;
4) Сведения о ремонте технических средств и изменениях в программном обеспечении с указанием основания, даты и содержания изменения;
5) Сведения о выполнении регламентных (профилактических) работ и их результатах.

В разделе **"Сведения о рекламациях"** указываются сведения о рекламациях с указанием номера, даты, краткого содержа-

ния рекламационного акта, а также сведения об устранении замечаний, указанных в акте.

Примечание

Формуляр отличается от Паспорта только наличием пункта "Сведения о состоянии АСУТП". Согласно устоявшейся практике, эти сведения указываются в оперативных технологических журналах, журналах по эксплуатации, обслуживанию и ремонту для каждого типа оборудования. Параллельное ведение сводных документов в целом для системы, которая по определению состоит из самого разнообразного оборудования, оказывается избыточным. ***Поэтому данный документ можно признать необязательным.***

6.13. Документ "Проектная оценка надежности системы" * (Б1)

Документ содержит следующие разделы:

- Введение;
- Исходные данные;
- Методика расчета;
- Расчет показателей надежности;
- Анализ результатов расчета.

В разделе **"Введение"** указывается:

1) Назначение расчета надежности системы;
2) Перечень оцениваемых показателей надежности;
3) Состав учитываемых при расчете факторов, а также принятые допущения и ограничения.

В разделе **"Исходные данные"** приводятся:

1) Данные о надежности (паспортные и справочные) элементов АСУТП, учитываемые при расчете надежности системы;
2) Данные о режимах и условиях функционирования элементов АСУТП;
3) Сведения об организационных формах, режимах и параметрах эксплуатации АСУТП.

В разделе **"Методика расчета"** указывается обоснование выбора методики расчета и нормативно-технический документ, согласно которого проводится расчет. Или краткое описание методики расчета, и ссылки на первоисточники.

В разделе **"Расчет показателей надежности"** указываются:

1) Структуры надежности компонентов АСУТП (комплекса технических средств, программного обеспечения и персонала) по всем оцениваемым функциям или функциональным подсистемам АСУТП;
2) Необходимые вычисления;
3) Результаты расчета.

В разделе **"Анализ результатов расчета"** указываются:

1) Итоговые данные расчета по каждой оцениваемой функции (функциональной подсистеме) АСУТП и каждому нормируемому показателю надежности;
2) Выводы о достаточности или недостаточности полученного уровня надежности АСУТП по каждой оцениваемой функции (функциональной подсистеме) АСУТП и, при необходимости, рекомендации по повышению надежности.

При оценке надежности АСУТП трудно учесть уровень надежности программного обеспечения, и уровень надежности действий персонала АСУТП. Поэтому в документе "Проектная оценка надежности системы", как правило, указываются сведения по оценке надежности АСУТП только с учетом надежности комплекса технических средств.

Понятие надежности тесно связано с понятием критичности отказов. За последние годы появилась группа добротных отечественных нормативных документов по анализу рисков и оценке последствий отказов, в частности:

- РД 03-418-01 *"Методические указания по проведению анализа риска опасных производственных объектов* основанные на анализе деревьев отказов и событий.
- ГОСТ 27.310-95 "*Анализ видов, последствий и критичности отказов".*

Согласно РД 03-418-01, исходя из категории отказов по тяжести последствий и критичности отказов, взрывоопасные объекты нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств **по критичности отказов относятся к Категории "А",** что означает, что обязателен **количественный** анализ риска, или требуются особые меры обеспечения безопасности. Таким образом,

Проектная оценка надежности оборудования систем управления и защиты для взрывоопасных объектов должна

сочетаться с **количественным** анализом критических функций (контуров) безопасности.

Необходимость документа "Проектная оценка надежности системы" определяется категорией взрывоопасности объекта автоматизации.

Согласно РД 03-418-01, для технологических объектов с блоками I и II категории взрывоопасности документ "Проектная оценка надежности системы" является обязательным.

Надежность систем управления и защиты для объектов всех категорий взрывоопасности должны обеспечивать следующие системные качества и свойства:

1. Аппаратурное резервирование;
2. Временная, информационная и функциональная избыточность;
3. Системы оперативной и функциональной диагностики.

Достаточность резервирования и его тип в общем случае обосновываются Разработчиком АСУТП, и согласовываются с Заказчиком, Ростехнадзором и Проектной организацией в соответствии с нормативными документами, с учетом особенностей технологического объекта и рекомендаций, представленных в настоящей работе.

6.14. Требования к содержанию документов с решениями по Техническому обеспечению

Принципиальное изменение:

Пункт 4.1.1 "Схема автоматизации" исходного стандарта РД 50-34.698-90 перенесен из группы документов по Техническому обеспечению в группу документов по Прикладному программному обеспечению и озаглавлен "Функциональные схемы автоматизации".

Согласно ГОСТ 34.201-89, "Схема автоматизации" отнесена к документации Технического обеспечения, и содержит она невесть что (кто бы объяснил, что все это значит):

"4.1 Схема автоматизации

4.LL Схема автоматизации содержит:

1) упрощенное изображение объекта или его части, для которой составлена схема;

2) средства технического обеспечения, участвующие в процессе, отображенном на схеме, за исключением вспо-

могательных устройств и аппаратуры (источники питания реле, магнитные пускатели);

3) функциональные связи между средствами технического обеспечения;

4) внешние функциональные связи средств технического обеспечения с другими техническими средствами;

5) таблицу примененных в схеме условных обозначений, не предусмотренных действующими стандартами.

4.1.2. На схеме допускаются необходимые текстовые пояснения".

Первое, что необходимо сделать, это узаконить понятие **Функциональная схема автоматизации -** термин общепринятый, и понятный в среде разработчиков АСУТП.

Функциональные схемы автоматизации создаются разработчиком АСУТП на стадии предварительного (технического) проектирования АСУТП, и являются промежуточным документом между монтажно-технологическими схемами, и тем, что обычно называют мнемосхемами, то есть это - графические изображения стратегии управления и защиты, реализованной в АСУТП - и в РСУ, и в ПАЗ.

Функциональные схемы автоматизации освобождены от изображения всего, что не относится непосредственно к функциям АСУТП:

- Технологических линий, не используемых при реализации функций управления и защиты в АСУТП;
- Приборов по месту;
- Первичных измерительных элементов;
- Предохранительных клапанов;
- Преобразователей входных и выходных сигналов;
- Клапанных сборок;
- Задвижек, не связанных с АСУТП;
- И т. д.

Как правило, на функциональных схемах изображаются связи и блоки, реализующие функции усовершенствованного управления в РСУ, которые отсутствуют на монтажно-технологических схемах.

Как правило, на тех же функциональных схемах изображаются связи и блоки, реализующие функции противоаварийной защиты в системе ПАЗ.

Сказанное означает, что "Функциональные схемы автоматизации" относятся к прикладному программному обеспечению, а именно - к алгоритмическому, но никак не к техническому.

Функциональные схемы автоматизации разрабатываются специалистами АСУТП - разработчиками АСУТП, и входят в состав документов, содержащих решения по реализации алгоритмов управления и ПАЗ:

- Краткое описание технологического процесса;
- Цели управления;
- Стратегия управления;
- Алгоритм решения;
- Результаты решения;
- Функциональная схема автоматизации;
- Блок-схема управления / логики;
- Детальная конфигурация;
- Диаграммы контуров управления и ПАЗ *(Loop Diagrams)*.

Все эти документы создаются Разработчиком АСУТП.

Следующие четыре документа переходят в Рабочую документацию из Технического проекта после внесения всех необходимых дополнений и корректировок, либо непосредственно создаются как документы Технорабочего проекта.

6.15. Документ "Описание комплекса технических средств" * (П9)

Документ содержит следующие разделы:

- Общие положения;
- Структура комплекса технических средств;
- Средства вычислительной техники;
- Аппаратура передачи данных.

В разделе **"Общие положения"** приводятся исходные данные, использованные при проектировании технического обеспечения АСУТП.

В разделе **"Структура комплекса технических средств"** приводится:

1) Обоснование выбора структуры комплекса технических средств (КТС). В том числе - технические реше-

ния по обмену данными с техническими средствами других АСУТП, и по использованию технических средств ограниченного применения (в соответствии с перечнями, утвержденными в установленном порядке).

2) Описание функционирования КТС, в том числе в пусковых и аварийных режимах;
3) Описание размещения КТС на объектах и на производственных площадках с учетом выполнения требований техники безопасности, а также с учетом соблюдения условий эксплуатации данных технических средств;
4) Обоснование применения, и технические требования к оборудованию, предусмотренному в утвержденных проектах и сметах на строительство или реконструкцию предприятий, и изготовляемому в индивидуальном порядке промышленными предприятиями, или строительно-монтажными организациями по заказным спецификациям и чертежам проектных организаций как применяемые в силу особых технических решений в проекте;
5) Обоснование методов защиты технических средств от механических, тепловых, электромагнитных и других воздействий, защиты данных, в том числе от несанкционированного доступа к ним, и обеспечения заданной достоверности данных в процессе функционирования КТС;
6) Результаты проектной оценки надежности КТС.

В разделе **"Средства вычислительной техники"** приводится:

1) Обоснование и описание основных решений по выбору оборудования РСУ и ПАЗ;
2) Обоснование и описание основных решений по выбору типов периферийных технических средств, в том числе средств получения, контроля, подготовки, сбора, регистрации, хранения и отображения информации;
3) Описание структурной схемы технических средств, размещенных в ЦПУ и на удаленных рабочих местах;
4) Результаты расчета или расчет числа технических средств и потребности в носителях данных;

5) Обоснование численности персонала, обеспечивающего функционирование технических средств;
6) Технические решения по оснащению рабочих мест персонала, включая описание рабочих мест и расчет площадей;
7) Описание особенностей функционирования технических средств в пусковом, нормальном и аварийном режимах.

В разделе **"Аппаратура передачи данных"** приводится:

1) Обоснование и описание решений по выбору средств телеобработки и передачи данных, в том числе решения по выбору каналов связи, и результаты расчета (при необходимости расчет) их числа;
2) Решения по выбору технических средств, обеспечивающих сопряжения с каналами связи, в том числе результаты расчета (или расчет) их потребности;
3) Требования к арендуемым каналам связи;
4) Сведения о размещении абонентов и объемно-временных характеристиках передаваемых данных;
5) Основные показатели надежности, достоверности и других технических характеристик средств телеобработки и передачи данных.

6.16. Документ "План расположения оборудования АСУТП на объекте" * (С7)

План расположения оборудования должен показывать размещение средств технического обеспечения АСУТП на площадке.

План расположения средств технического обеспечения, выполняемый при разработке технического проекта, должен определять расположение пунктов управления и средств технического обеспечения, требующих специальных помещений или отдельных площадей для размещения.

Документ допускается включать в раздел "Структура комплекса технических средств" документа "Описание комплекса технических средств".

6.17. Документ "Схема структурная комплекса технических средств" * (С1)

Документ содержит состав комплекса технических средств и связи между этими техническими средствами или группами технических средств, объединенными по каким-либо логическим признакам (например, совместному выполнению отдельных или нескольких функций, одинаковому назначению и т. д.).

При выполнении схем допускается:

1) Указывать основные характеристики технических средств;
2) Представлять структуру КТС АСУТП несколькими схемами, первой из которых является укрупненная схема КТС АСУТП в целом.

6.18. Документ "Спецификация оборудования" * (В4)

Документ "Спецификация оборудования" должен быть составлен в соответствии с требованиями ГОСТ 21.110-95 СПДС "*Правша выполнения спецификации оборудования, изделий и материалов*"

При использовании в проекте технических средств, для заказа которых требуется заполнение опросных листов, приложение последних к проекту обязательно. При использовании технических средств, имеющих ограничения на применение в соответствии с перечнями, утвержденными в установленном порядке, необходимо приложить к проекту копии документов о согласовании поставки этих средств.

6.19. Документ "Планы расположения оборудования и проводок в ЦПУ" (С8)

План расположения оборудования и проводок должен показывать планы и разрезы помещений, на которых должно быть указано размещение средств технического обеспечения Системы. Документ допускается включать в раздел "Структура комплекса технических средств" документа "Описание комплекса технических средств".

6.20. Документ "Чертеж общего вида системных шкафов и установки технических средств" (ВО)

Данный документ содержит следующие разделы:

- Легенда адресации устройств;
- Общий вид системных шкафов с установкой технических средств;
- Общий вид шасси системы, терминальных панелей и их конфигурация.

На чертежах допускаются необходимые текстовые пояснения. В ряде случаев "Таблицу соединений и подключений (С6)" документа РД 50-34.698-90 удобно разделить на два нижеследующих документа.

6.21. Документ "Таблица внутрисистемных соединений и подключений" (С6.1)

Данный документ содержит таблицу внутренних соединений основного оборудования системы системными кабелями.

6.22. Документ "Таблица соединений кросс - система" (С6.2)

Данный документ содержит таблицу соединения системного оборудования с кроссовыми шкафами и другими промежуточными клеммниками.

Далее вводится дополнительный, отсутствующий в ГОСТ 34.201-89 и РД 50-34.698-90 документ, определяющий схемы питания и заземления.

6.23. Документ "Схемы питания и заземления" (СЮ)

Данный документ содержит следующие разделы:

- Структурная схема расключения питания 220V AC;
- Блоки питания и клеммники расключения 24V DC;
- Таблицы расключения питания 220V AC;
- Таблицы расключения питания 24V DC;
- Схемы заземления системы.

Примечание

При составлении Спецификации оборудования системы для объектов I и II категорий взрывоопасности в обязательном порядке необходимо предусмотреть систему бесперебойного электропитания основного оборудования Системы и питания цепей полевого КИП.

Еще один принципиальный момент:

Конкретизируется содержание документа 4.16 "Схема принципиальная" из РД 50-34.698-90 как документа, содержащего принципиальное графическое изображение прохождения сигналов по каналу Поле - Система - Поле:

6.24. Документ "Схемы электрические принципиальные контуров измерения, регулирования, сигнализации и блокировок" (Loop Diagrams) (СБ)

Содержат изображение последовательности прохождения сигнала от датчика до системы с указанием и маркировкой соединительных коробок, кабелей, кросса и барьеров искробезопасности; а также в обратной последовательности — от системы до исполнительного механизма.

Учитывая особую актуальность и, в то же время, новизну диаграмм контуров для многих отечественных разработчиков и пользователей, на следующих страницах воспроизводятся несколько образцов (таблицы 6.1-6.5).

Воспроизведены стандарты диаграмм, разработанные экспертами Инженерного центра ЗАО "Компания СЗМА" (трест "Севзапмонтажавтоматика"), г. Санкт-Петербург.

Аналогичные диаграммы используют и ведущие западные проектировщики и разработчики систем автоматизации.

Диаграмма стандартного контура регулирования уровня *Таблица 6.1*

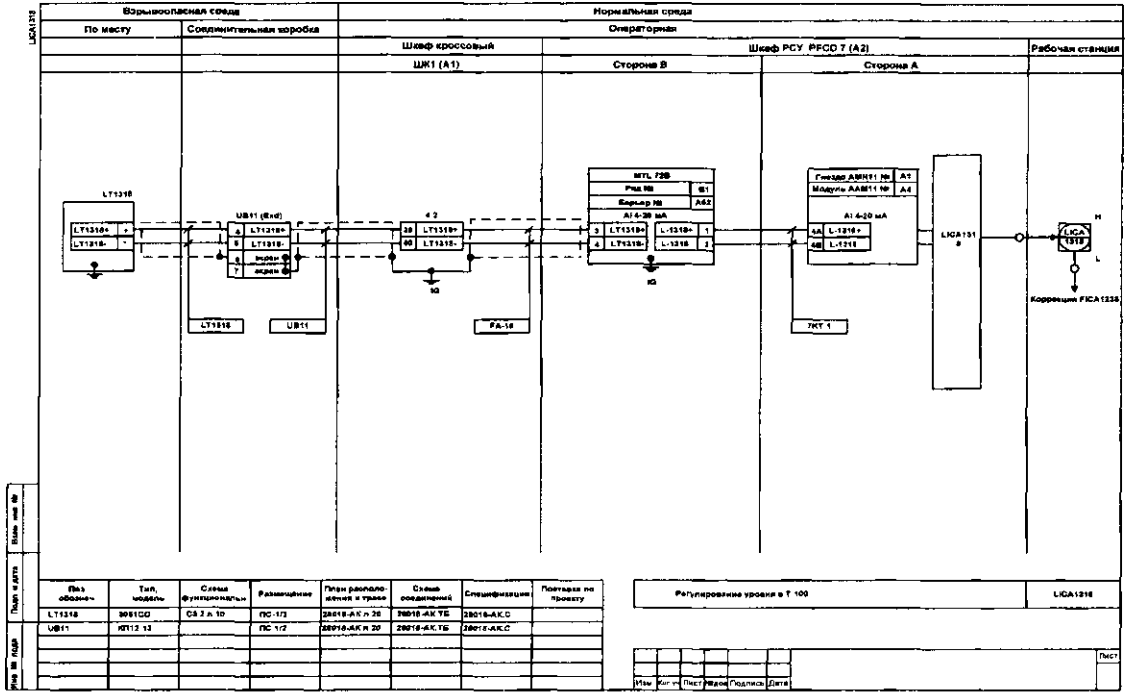


Диаграмма каскадного ПИД-регулятора давления *Таблица 6.2*

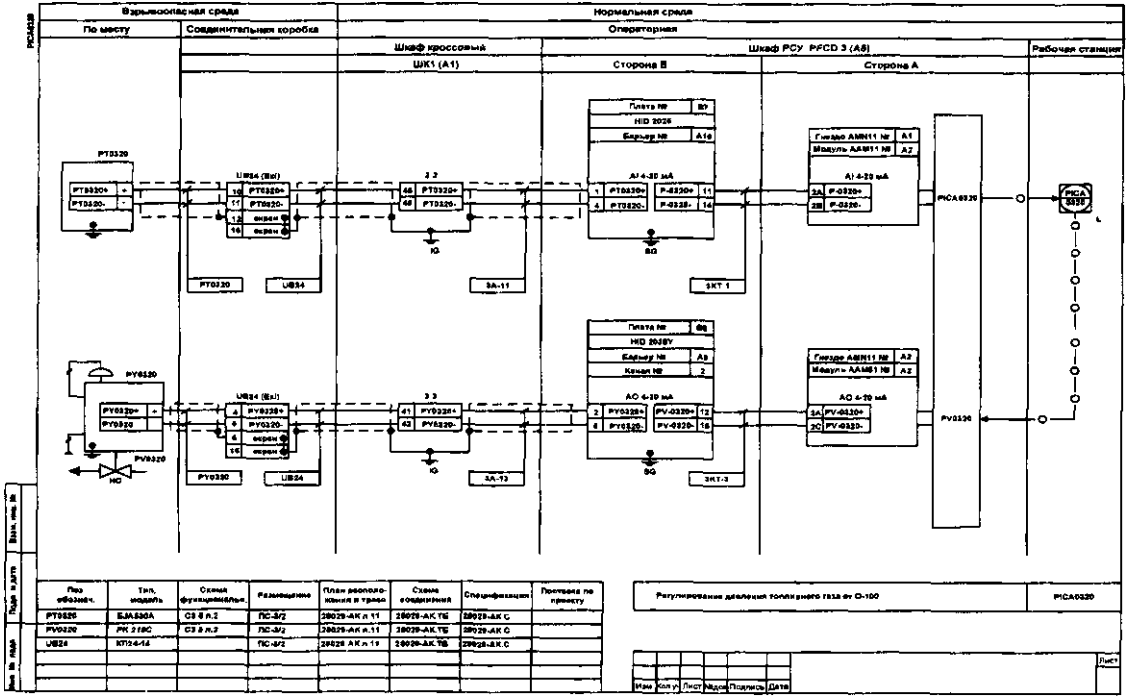
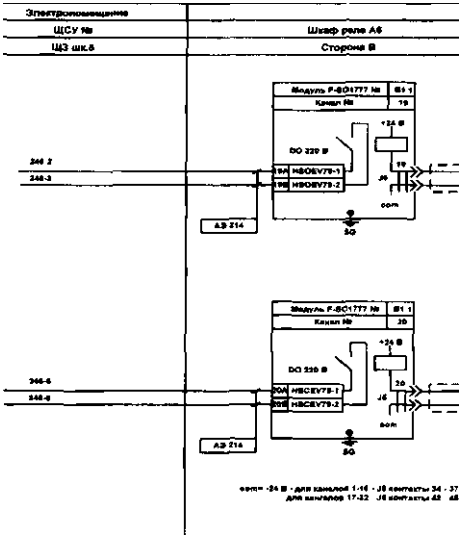


Диаграмма контура управления приводом электрозадвижки *Таблица 6.3*



Шкаф РСУ PFCD 3 <A8

Рабочая станция

Гекрс AMN2 H

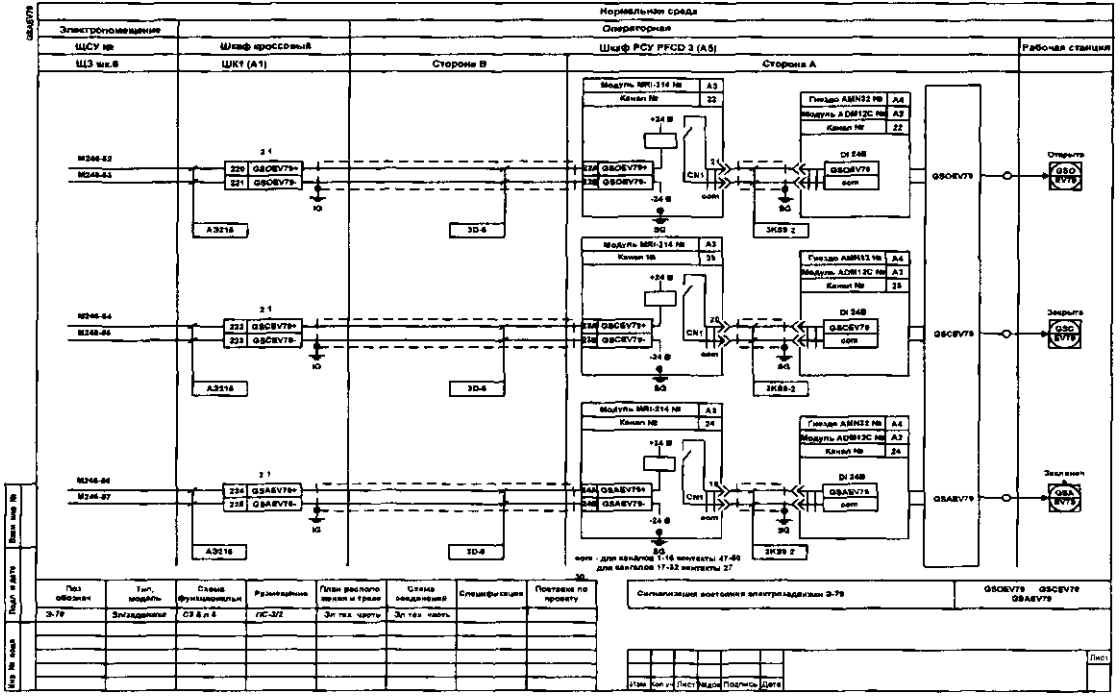
III

ЖлйИ I

модуль лоанс I

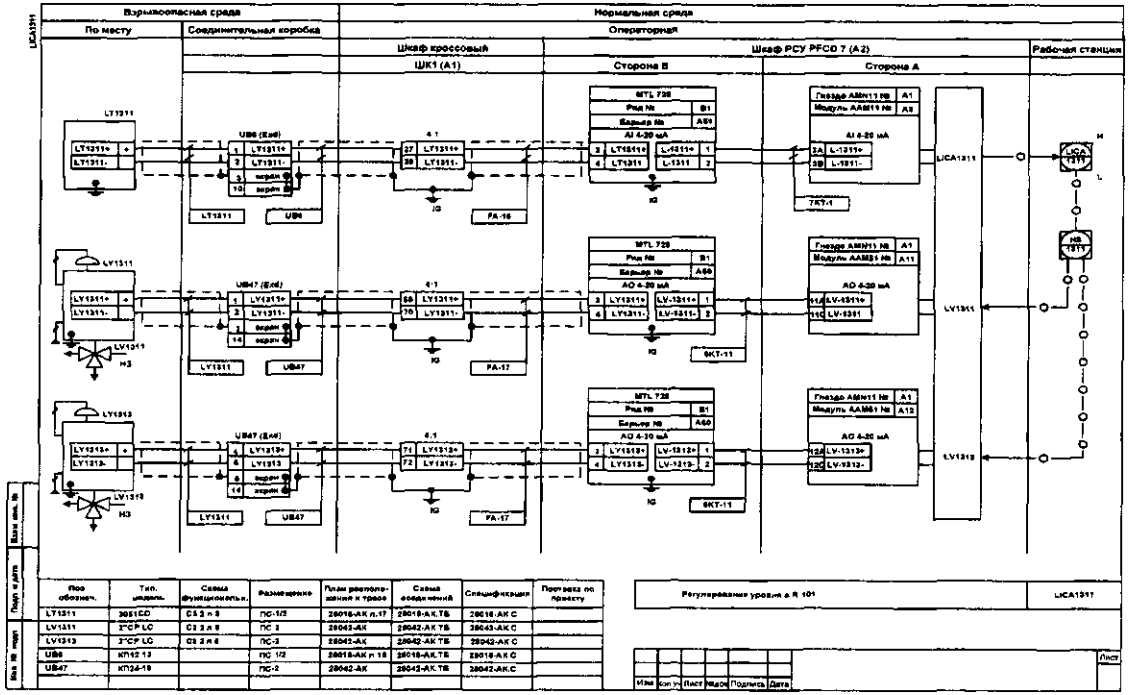
Лист «ДП Подпись Да»

Диаграмма сигнализации состояния электрозадвижки *Таблица 6.4*



ІЛ

Диаграмма контура управления с двумя выходными сигналами *Таблица 6.5*



6,25. Документ "Инструкция по эксплуатации и обслуживанию КТС" (ИЭ)

Документ содержит следующие разделы:

- Общие указания;
- Меры безопасности;
- Порядок работы;
- Проверка правильности функционирования;
- Обслуживание и замена модулей и плат;
- Указания о действиях в разных режимах.

В разделе **"Общие указания"** указываются:

1) Вид оборудования, для которого составлена инструкция;
2) Наименование функций АСУТП, реализуемых на данном оборудовании;
3) Регламент и режимы работы оборудования по реализации функций;
4) Перечень эксплуатационных документов, которыми должен дополнительно руководствоваться персонал при эксплуатации данного оборудования.

В разделе **"Меры безопасности"** перечисляются правила безопасности, которые необходимо соблюдать во время подготовки оборудования к работе и при его эксплуатации.

В разделе **"Порядок работы"** указываются:

1) Состав и квалификацию персонала, допускаемого к эксплуатации оборудования;
2) Порядок проверки знаний персонала и допуска его к работе;
3) Описание работ и последовательность их выполнения.

В разделе **"Проверка правильности функционирования"** приводится содержание, краткие методики основных проверок оборудования, и правильность выполнение функций системы.

В разделе **"Обслуживание и замена модулей и плат"** описываются процедуры обслуживания оборудования системы, как в автономном, так и в оперативном (рабочем) режиме.

В разделе **"Указания о действиях в разных режимах"** перечисляются действия персонала при нормальном режиме работы, предаварийном состоянии объекта, при отключении оборудования, при пуске и останове технологического процесса.

Примечание

Следующие два документа:
С4 "Схема соединения внешних проводок", и
С5 "Схема подключения внешних проводок"
Технического обеспечения разрабатываются Проектной организацией.

6.26. Документ "Схема соединения внешних проводок" (С4)

На схемах указываются:

1) Электрические провода и кабели, импульсные, командные, питающие, дренажные трубопроводы, защитные трубы, короба и металлорукава (с указанием их номера, типа, длины и, при необходимости, мест подсоединения), прокладываемые вне щитов и кроссовых шкафов;
2) Отборные устройства, чувствительные элементы, регулирующие органы и т. п., встраиваемые в технологическое оборудование и трубопроводы с указанием номеров их позиций по спецификации оборудования и номеров чертежей их установки;
3) Приборы, регуляторы, исполнительные механизмы и т. п., устанавливаемые вне щитов с указанием номеров их позиций по спецификации оборудования, и номеров чертежей их установки;
4) Щиты и пульты с указанием их наименований и обозначения таблиц соединений, таблиц подключений;
5) Устройства защитного заземления щитов, приборов и других электроприемников, выполненные согласно действующей нормативно-технической документации;
6) Технические характеристики кабелей, проводов, соединительных и разветвительных коробок, труб, арматур и т. п., предусмотренных данной схемой и необходимое их число;
7) Таблицу примененных в схеме условных обозначений, не предусмотренных действующими стандартами.

На схемах допускается указывать другие виды технических средств и давать текстовые пояснения.

6.27. Документ "Схема подключения внешних проводок" (С5)

Представляет собой таблицы электрических соединений полевого КИПиА с кроссовым оборудованием РСУ и системы ПАЗ. На схемах указываются вводные устройства (сборки коммутационных зажимов, штепсельные разъемы и т. п.) шкафов, щитов, пультов, соединительных коробок, и подключаемые к ним кабели и провода, а также другие виды технических средств.

Схемы подключения (С5) допускается не выполнять, если эти подключения показаны на схемах соединения внешних проводок (С4).

6.28. Требования к содержанию документов с решениями по Информационному обеспечению

Документы, помеченные звездочкой, включаются в рабочую документацию из технического проекта после внесения необходимых дополнений и корректировок.

6.29. Документ "Перечень входных и выходных сигналов РСУ" *(В1)

Документ содержит следующие разделы:

- Перечень входных сигналов РСУ;
- Перечень выходных сигналов РСУ.

В разделе **"Перечень входных сигналов** РСУ" указываются:

1) Для аналогового сигнала - наименование измеряемой величины, единицы измерения, диапазон изменения, предаварийные и предупредительные уставки, требования к точности и периодичности измерения, тип сигнала;
2) Для дискретного сигнала - наименование, периодичность, смысловое значение сигнала.

Раздел "Перечень выходных сигналов РСУ" содержит перечень выходных сигналов с указанием их наименований, единиц измерения и диапазонов изменения.

Замечание

В ряде случаев удобно делать группировку сигналов по контурам управления или защиты в едином перечне сигналов входа-выхода.

6.30. **Документ "Перечень входных и выходных сигналов ПАЗ" *(B2)**

Документ содержит перечни входных и выходных сигналов с указанием их наименований, единиц измерения и диапазонов изменения:

- Перечень входных сигналов системы ПАЗ;
- Перечень выходных сигналов системы ПАЗ.

Состав характеристик аналогичен перечням сигналов РСУ.

6.31. **Документ** "Перечень **сигналов взаимообмена** РСУ-ПАЗ" (B10)

Содержит перечень сигналов (переменных) взаимодействия системы управления с системой ПАЗ с указанием их наименований, назначения, единиц измерения и диапазонов изменения.

Образец упрощенной формы документов B1 и B2, который удобно использовать при подготовке Технического задания, приводится в таблице 6.6. Ту же форму можно использовать и для документа B10.

На стадии технического проектирования необходимо использовать подробные формы Перечней. Пример формы, разработанной специалистами Инженерного центра ЗАО "Компания СЗМА", приведен в таблице 6.7.

На предпроектных стадиях, в особенности - при подготовке Технического задания и бюджетных оценок, удобно использовать Сводные таблицы сигналов входа-выхода - таблица 6.8 (авторство фирмы Иокогава Электрик, Россия).

Упрощенная форма Таблицы сигналов входа-выхода АСУТП *Таблица 6.6*

№	Код кон-тура	Пози-ция КИП	Наименование параметра	Шкала		£д. изм.	Тип сигна-ла	Предупредительная Сигнализация		Предаварийная Сигнализация	
				мин	ма КС			L	H	LL	HH
1	2	3	4	5	6	7	8	9	10	11	12

Подробная форма перечня сигналов входа-выхода

Таблица 6.7

№ позиции	Переменная	Значения переменной							Шкала датчика		Ед. измер.	Тип сигнала		Функции системы управления									Примечание
		Блокировка		Сигнализация				Номин.	Диапазон	Тип		I/O	Ex	Контроллер				Станция оператора					
		LL	HH	LL	L	H	HH							P I/O	Тип клав.	Тип рег.	БЛК	Инд.	Сигн.	ДУ	Исп.	Нрав.	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Секция полимеризации и дегазации																							
FE 1101	Расход [illegible] в реактор R 101				100				0–2685	L	кг/ч	AI	O					+	L		+	/H	
FV 1101	[illegible]								0–100		%	AO	I		Ручн.			+					
FE 1102	Расход [illegible]				250				0–3400	L	кг/ч	AI	I					+	L		+	+ L	[illegible]
FV 1102	[illegible]								0–100		%	AO	I		FC			+		+			
FE 1103	Расход [illegible]				30	90			0–100	L	%	AI	I					+	L H			+	[illegible]
FE 1104	[illegible]				30	90			0–100	L	%	AI	I						L/H			L H	[illegible]
PE 1105	[illegible]					93.31		110	0–120	L	кПа	AI	I			R		+	H		+	+/H	
FE 12	[illegible]								0–100		%	AO	I		FO			+		+			[illegible]
FV 2432	[illegible]								0–100		%	AO	I		FO			+		+			
PE 1203	[illegible]					8			0–120	L	кПа	AI	I						H		+	+/H	
PE 1108	Контроль давления в [illegible]					133			0–40	L	кПа	AI	I					+	H		+	+/H	
TE 112	[illegible]					120		82	0–200	L	°C	AI	I			R		+	H		+	+/H	[illegible]
TE 1122	[illegible]					125		120	0–200	L	°C	AI	I			R		+	H		+	+/H	[illegible]
FV 1108	[illegible]								0–100		%	AO	I		FC			+		+			
TE 1179	[illegible]					130		125	0–200	L	C	AI	I			R		+	H		+	+ H	
FV 1204	[illegible]								0–100		%	AO	I		FO			+		+			
FV 1108	[illegible]								0–100		%	AO	I		FC			+		+			
TE 1118	[illegible]					134		124	0–250	L	C	AI	I			R		+	H		+	/H	[illegible]
TE 1137	[illegible]					160		129	0–250	L	°C	AI	I					+	H		+	+/H	
TE 1138	[illegible]					160		121	0–250	L	°C	AI	I			R		+	H		+	+/H	[illegible]
FV 1124	[illegible]								0–100		%	AO	I		FO			+		+			
FV 1108	[illegible]								0–100		%	AO	I		FC			+	H	+			
TE 1135	[illegible]					160		129	0–250	L	°C	AI	I					+	H		+	+/H	
TE 1136	[illegible]					160		129	0–250	L	°C	AI	I					+	H		+	+/H	
TE 113	[illegible]					160		129	0–250	L	C	AI	I			R		+	H		+	+/H	[illegible]
TE 1140	[illegible]					170		137	0–250	L	°C	AI	I					+	H		+	+/H	
TE 1142	[illegible]					180		125	0–250	L	°C	AI	I			R		+	H		+	+/H	[illegible]
FV 1142A	[illegible]								0–100		%	AO	I		FO			+		+			
FV 1142B	[illegible]								0–100		%	AO	I		FC			+		+			
TE 1143	[illegible]					170		137	0–250	L	°C	AI	I					+	H		+	+/H	
TE 1144	[illegible]					170		137	0–250	L	°C	AI	I					+	H		+	+/H	

Форма Сводной таблицы сигналов входа-выхода *Таблица 6.8*

ПОЯСНЕНИЯ / Clarification
STD - Стандартные вх/вых / Standard I/O
I.S - Искробезопасные вх/вых / I/O are connected via safety barriers

		ВХОД УПРАВЛЕНИЯ/ CONTROL INPUT					ВЫХОД УПРАВЛ! CONTROL OUTPUT		ВХОД НАБЛЮДЕНИЯ / MONITORING INPUT					ДИСКРЕТНЫЙ ВХОД STATUS INPUT		ДИСКРЕТНЫМ ВЫХОД STATUS OUTPUT	
НАИМЕНОВАНИЕ БЛОКА {АГРЕГАТАyUNTT NAME		4 2 0 mA	1-5 V ОС	Термо-пара Т/С	Тврмо-сопр-е/ RTD	Имп. •ход/ Pulse	4-20mA		4-20 mA	1-5 V ОС	Термо-пара ТЮ	Термо-оопр-е/ RTD	Иил •ход/ Pulse	Сухой контакт Dry Contact	Вход репе Relay Input	Сухой юитакт Dry Contact	Выход реле Relay Output
Блок 1/ Unit 1	STD																
	IS.																
Ьлок2/илй2	STD																
	IS																
Блок 3 / Unit 3	STO																
	IS																
Итого/ Sub-Tola*																	
Резерв/ Spare 5%																	
ВСЕГО /TOTAL																	

Для входа реле указать номинал сигнала / For relay input select from the following.
220VAC.0.1A 110VAC.01A 24VDC.0.1A Прочие / Other

Для выхода реле указать номинал сигнала I For re/ay output select from the following:
220VAC.01A 110V AC,0.1 A 24VDC.01A Прочие/Other

6.32. Документ "Описание информационного обеспечения системы" *(П5)

Документ содержит следующие разделы:

- Состав информационного обеспечения;
- Организация информационного обеспечения;
- Организация сбора и передачи информации;
- Организация информационной базы;
- Человеко-машинный интерфейс.

В разделе **"Состав информационного обеспечения"** указывается наименование и назначение всех баз данных и наборов данных.

В разделе **"Организация информационного обеспечения"** приводятся:

1) Принципы организации информационного обеспечения системы;
2) Обоснование выбора носителей данных и принципы распределения информации по типам носителей;
3) Описание принятых видов и методов контроля в маршрутах обработки данных при создании и функционировании информационных баз с указанием требований, на соответствие которым проводится контроль;
4) Описание решений, обеспечивающих информационную совместимость АСУТП с другими системами управления по источникам, потребителям информации, по сопряжению применяемых классификаторов, по использованию в АСУТП унифицированных систем документации.

В разделе **"Организация сбора и передачи информации"** приводится:

1) Перечень источников и носителей информации с указанием интенсивности и объема потоков информации, включая заводскую ЛВС, корпоративную сеть, и т.д.;
2) Описание общих требований к организации сбора, передачи, контроля и корректировки информации.

В разделе **"Организация информационной базы"** приводятся следующие описания:

1) Описание принципов построения информационной базы, характеристики ее состава и объема;

2) Описание структуры информационной базы на уровне баз данных с описанием характера взаимосвязей баз данных и с указанием функций АСУТП, при реализации которых используют каждую базу данных, и характеристики данных, содержащихся в каждой базе данных.

В разделе **"Человеко-машинный интерфейс"** определяются принципы построения интерфейса, приводятся характеристики состава и объема структурных единиц информации, определяющих взаимодействие технолога-оператора с Системой.

6.33. Документ "Описание организации информационной базы" *(П6)

Документ **"Описание организации баз данных"** содержит следующие разделы:

- Логическая структура;
- Физическая структура;
- Организация ведения информационной базы данных.

В разделе **"Логическая структура"** приводится описание состава данных, их форматов и взаимосвязей между данными.

В разделе **"Физическая структура"** приводится описание избранного варианта расположения данных на конкретных машинных носителях.

При описании структуры информационной базы должны быть приведены перечни баз данных и массивов исторических данных (архивов), и логические связи между ними.

Для массивов исторических данных указывается логическая структура внутри массива или дается ссылка на документ **"Описание массивов исторических данных (архивов)".**

При описании структуры информационной базы приводится перечень документов и других информационных сообщений, использование которых предусмотрено в системе, с указанием автоматизируемых функций, при реализации которых формируется или используется данный документ.

Если эта информация приведена в документах **"Перечень входных и выходных сигналов",** можно сослаться на эти документы.

В разделе **"Организация ведения информационной базы"** приводится:

- Последовательность процедур при создании и обслуживании базы;
- Регламент выполнения этих процедур;
- Средства защиты базы от разрушения и несанкционированного доступа с указанием связей между массивами баз данных и массивами входной информации.

6.34. Документ "Описание систем классификации и кодирования" * (П7)

Документ содержит перечень применяемых в Системе зарегистрированных классификаторов всех категорий по каждому классифицируемому объекту, описание метода кодирования, структуры и длины кода, указания о системе классификации и другие сведения по усмотрению разработчика.

Примечание

Принятый в 1985 году ГОСТ 21.404-85 "Обозначения условные приборов и средств автоматизации в схемах" во многом не соответствует общемировой практике графической и символьной кодировки параметров АСУТП в приложении к современным системам управления и защиты технологических процессов.

Полное описание системы идентификации оборудования КИП и А, контуров и параметров РСУ и ПАЗ, сформированное в основных положениях на основе общепризнанной международной практики - стандарт ANSI/ISA S5.1-1984 "Instrumentation Symbols and Identification", - а также исходя из собственного опыта, и опыта работы ведущих западных фирм-разработчиков оборудования и систем управления, дано в главе ***"Система идентификации параметров АСУТП".***

6.35. Документ "Описание массивов исторических данных (архивов)" *(П8)

Документ содержит общее описание организации долговременного хранения исторических данных.

По каждому архиву документ содержит:

- Наименование архива;
- Обозначение архива;
- Наименование носителей информации;

- Перечень реквизитов в порядке их следования в записях архива с указанием обозначения, диапазона изменения, логических и семантических связей с другими реквизитами и другими записями архива;
- Частота архивирования (регулярная, по событиям и т.д.);
- Количество записей и общий объем архива;
- Другие характеристики архива (при необходимости).

6.36. Документ "Альбом документов и видеокадров" *(С9)

В документе должен быть приведен полный комплект **фактических** документов и видеоизображений АСУТП в соответствии с организационно-технологической структурой объекта автоматизации, и даны необходимые пояснения.

6.37. Документ "Состав выходных данных (сигнализаций, сообщений)" (В8)

Документ содержит полный набор образцов выходных данных с указанием их наименований, кодовых обозначений и реквизитов, а также наименований и кодовых обозначений документов или сообщений, содержащих эти данные:

- Предупредительная и предаварийная сигнализация;
- Сообщения оператору процесса;
- Системные сообщения.

6.38. Документ "Каталог баз данных" (В7)

Каталог базы данных содержит распечатку баз данных для всех структурных единиц системы:

- Инженерная станция:
  - Распечатка базы данных станции.
- Станции технолога-оператора:
  - Распечатка базы данных станции.
- Станции управления / Контроллеры:
  - Распечатка базы данных ввода-вывода,
  - Обмена с системой ПАЗ.

- Система ПАЗ:
  - Распечатка базы данных ввода-вывода;
  - Распечатка базы данных параметров обмена с РСУ;
  - Определения первопричины останова.

6.39. Документ "Инструкция по формированию и ведению базы данных" (И4)

Документ "Инструкция по формированию и ведению базы данных" содержит следующие разделы:

- Правила подготовки данных
- Порядок и средства заполнения базы данных
- Процедуры изменения и контроля базы данных
- Порядок и средства восстановления базы данных.

В разделе **"Правила подготовки данных"** приводится порядок отбора информации для включения в базу данных, правила подготовки и кодирования информации, формы ее представления и правила заполнения этих форм, порядок внесения изменений.

В разделе **"Порядок и средства заполнения базы данных"** приводится состав технических средств, правила, порядок, последовательность и описание процедур, используемых при заполнении базы данных, включая перенос данных на машинные носители информации.

В разделе **"Процедуры изменения и контроля базы данных"** приводится состав и последовательность выполнения процедур по контролю и изменению содержания базы данных.

В разделе **"Порядок и средства восстановления базы данных"** приводится описание средств защиты базы от разрушения и несанкционированного доступа, а также правила, средства и порядок проведения процедур по копированию и восстановлению базы данных.

6.40. Требования к содержанию документов с решениями по Стандартному программному обеспечению

Следующий документ переходит в состав Рабочей документации из Технического проекта после внесения всех необходимых дополнений и корректировок.

6.41. Документ "Описание стандартного программного обеспечения" * (ПА)

Документ содержит стандартную документацию фирмы-изготовителя на стандартное программное обеспечение: описания используемых пакетов программного обеспечения, их структуры и функций.

Документ содержит следующие разделы:

- Операционная система / системы;
- Структура программного обеспечения;
- Функции частей программного обеспечения.

Во вводной части приводится основные сведения о техническом, информационном и других видах обеспечения АСУТП, необходимые для разработки программного обеспечения, или ссылку на соответствующие документы проекта.

В разделе **"Операционная система "** указываются:

1) Наименование, обозначение и краткую характеристику каждой из выбранных операционных систем, версий, в рамках которых будут выполняться разрабатываемые программы, с обоснованием выбора и указанием источников, где дано подробное описание выбранной версии;
2) Наименование руководства, в соответствии с которым должна осуществляться генерация выбранного варианта операционной системы;
3) Требования к варианту генерации выбранной версии операционной системы.

В разделе **"Структура программного обеспечения"** приводится перечень частей программного обеспечения с указанием их взаимосвязей и обоснованием выделения каждой из них:

- Инженерная станция;
- Станция оператора;
- Станция управления / Контроллер;
- Система ПАЗ;
- Взаимообмен РСУ - система ПАЗ;
- Взаимообмен с ЛВС.

Для **Инженерной станции** определяются и описываются функции проектирования системы.

1) **Среда проектирования:**
   Описываются варианты состава оборудования, необходимые для проведения процедуры проектирования.
2) **Процедура проектирования Системы:**
   - Определение основных параметров и характеристик системы;
   - Разработка структуры системы;
   - Детальная разработка;
   - Генерация системы;
   - Автономное тестирование;
   - Проверка на реальном объекте.
3) **Стандартные функции проектирования:**
   - Представление дерева базы данных;
   - Функции построителя Системы;
   - Проверка достоверности и непротиворечивости базы данных;
   - Редактирование конфигурации;
   - Выполнение функций самодокументирования;
   - Загрузка базы данных в соответствующие Станции управления / Контроллеры и в Станции технолога-оператора;
   - Сохранение параметров настройки;
   - Функции печати всех данных и частей проекта;
   - Функции обслуживания Системы.

Для **станции Оператора (человеко-машинный интерфейс)** определяются принципы построения интерфейса, приводятся характеристики состава и объема структурных единиц информации, определяющих взаимодействие технолога-оператора с Системой:

1) **Окна общего обзора**
   Предназначены для контроля над работой всего производства в целом и для получения доступа к более подробным окнам.
2) **Графические окна (Мнемосхемы)**
   Относятся к наиболее важным типам операционных панелей. Представляют графическое изображение основного технологического оборудования, средств КИПиА, и отображают структуру алгоритмов управления и защиты, и их состояние.

3) **Окна группы приборов**
   Представляют и описывают состояние лицевых панелей группы приборов.
4) **Окна настройки**
   Описывают параметры конкретного устройства / прибора / регулятора и дают возможность его настройки.
5) **Окна сообщений и сигнализаций**
   Отражают в хронологическом порядке сообщения, предупредительную и предаварийную сигнализацию процесса.
6) **Окна регистрации хода процесса (тренды)**
   Отображают данные о ходе процесса во времени:
   - Окно группы трендов,
   - Окно одиночного тренда.

Для **Станции управления / для Контроллера / системы ПАЗ** определяются:

1) Принципы построения;
2) Функции локального (регулярного) управления;
3) Функции усовершенствованного (связного) управления;
4) Функции логического управления;
5) Функции противоаварийной защиты;
6) Вычислительные функции;
7) Характеристики состава и объема структурных единиц.

В разделе **"Функции частей программного обеспечения"** приводится назначение, и описание функций для каждой части программного обеспечения.

Изменение в структуре РД 50-34.698-90:

*Документ Организационного обеспечения "**Методика (технология) автоматизированного проектирования (И1)**" исходного стандарта РД 50-34.698-90 совершенно не относится к Организационному обеспечению, но точно согласуется с функциями стандартного программного обеспечения. Поэтому он перенесен в данный раздел документации "Стандартное программное обеспечение" в качестве нижеследующего самостоятельного документа.*

6.42. Документ "Методы и средства разработки (конфигурирования)" (И1)

Документ "Методы и средства разработки (конфигурирования)" содержит следующие разделы:

- Общие положения;
- Методика конфигурирования;
- Исходные данные;
- Проектные процедуры;
- Проверка достоверности (непротиворечивости) базы данных;
- Описание функций самодокументирования.

Кроме того, документ **"Методы и средства разработки (конфигурирования)"** может быть дополнен специфическими разделами, характерными для конкретного объекта автоматизации.

В разделе **"Общие положения"** указывается класс объектов, на которые распространена методика, состав специалистов-пользователей, требования и ограничения на условия применения.

В разделе **"Методика конфигурирования"** указывается состав и назначение процедур и операций конфигурирования, и порядок их взаимодействия.

В разделе **"Исходные данные"** определяется состав, порядок выбора, представления и формирования массивов используемой информации, перечень элементов, описывающих предметную область, критерии оценки исходных данных.

В разделе **"Проектные процедуры"** по каждой проектной процедуре (процедуре, операции конфигурирования) указывается состав нормативно-справочных входных данных, правила доступа к ним, порядок выполнения процедуры, состав и форму выходных сообщений.

В разделе **"Проверка достоверности (непротиворечивости) базы данных"** описываются процедуры автоматической проверки сконфигурированной базы данных на отсутствие ошибок и непротиворечивость.

В разделе **"Описание функций самодокументирования"** описываются функции, обеспечивающие сохранение, дублирование и печать всех *данных* проекта.

В документ вводится дополнительный раздел **"Методы и средства разработки программного обеспечения". В** данном разделе приводится перечень методов программирования и средств разработки программного обеспечения АСУТП с указанием частей программного обеспечения, при разработке которых следует использовать соответствующие методы и средства.

Для реализации функций АСУТП должны использоваться современные средства конфигурирования и визуального программирования, ориентированные на прикладных инженеров и технологов. **В** соответствии со стандартом **IEC 61131-3,** используются следующие средства технологического программирования:

1. **Function Block Diagrams -**
   Графический язык функциональных блоков;
2. **Sequential Function Chart -**
   Функциональные схемы для описания последовательности операций.

Для разработки систем противоаварийной защиты дополнительно предусматривается механизм описания логических (релейных) схем:

3. **Ladder Logic Diagrams -**
   Графические средства описания логических (релейных) схем.

Для разработки прикладных программ, в частности, технологических и технико-экономических расчётов, используется

4. **Проблемно-ориентированный язык**
   (Структурированный текст).

6.43. Требования к содержанию документов с решениями по Прикладному программному обеспечению

Нижеследующий документ включается в Рабочую документацию из Технического проекта после внесения всех необходимых дополнений и корректировок, либо создается непосредственно как документ Техноработчего проекта.

Замечание

Не слишком корректный термин ГОСТ 34.201, РД 50-34,698, ГОСТ 34.603 "Математическое обеспечение " заменен на "Прикладное программное обеспечение "

6.44. Документ "Описание и логические схемы алгоритмов" * (ПБ)

Описания алгоритмов группируются в соответствии с организационной и функциональной структурой объекта автоматизации:

1) Рабочее место технолога-оператора;
2) Технологический узел / блок;
3) Процедура / Алгоритм.

Документ **"Описание и логические схемы алгоритмов"** в зависимости от специфики АСУТП допускается разрабатывать как документ **"Описание алгоритмов",** или как документ **"Логические схемы алгоритмов".**

По каждому алгоритму документ **"Описание алгоритмов"** содержит разделы:

- Краткое описание технологического процесса;
- Цели управления;
- Стратегия управления (математическое описание);
- Алгоритм решения;
- Результаты решения;
- Функциональная схема автоматизации;
- Блок-схема управления или защиты;
- Детальная конфигурация.

В разделе **"Краткое описание технологического процесса"** приводятся краткие сведения о технологическом процессе (объекте автоматизации), при управлении которым используется данный алгоритм.

В разделе **"Цели управления"** приводится:

1) Назначение алгоритма;
2) Обозначение документа "Описание алгоритма", с которым связан данный алгоритм (при необходимости);
3) Ограничения на возможность и условия применения алгоритма и характеристики качества решения (точность, время решения и т.д.);
4) Общие требования к входным и выходным данным (форматам, кодам и т. д.), обеспечивающие правильность работы алгоритма.

В разделе **"Стратегия управления (Математическое описание)"** приводится:

1) Перечень принятых допущений и оценки соответствия принятой стратегии управления реальному процессу в различных режимах и условиях работы (например, стационарные режимы, режимы пуска и останова агрегатов, аварийные ситуации и т. д.);
2) Математическое описание процесса;
3) Сведения о научно-исследовательских работах, если они использованы для разработки алгоритма.

В разделе **"Алгоритм решения"** следует приводить:

1) Пошаговое описание логики алгоритма и способа формирования результатов решения с указанием последовательности выполнения функциональных блоков или шагов, расчетных или логических формул, используемых в алгоритме;
2) Правила контроля достоверности входных данных и вычислений;
3) Описание связей между частями и операциями алгоритма;
4) Ссылки на соответствующие схемы автоматизации и блок-схемы;
5) Распечатку детальной конфигурации функциональных блоков, либо текста программы.

Алгоритмом должны быть предусмотрены все ситуации, которые могут возникнуть в процессе решения задачи.

При изложении алгоритма следует использовать условные обозначения реквизитов, сигналов, граф, строк со ссылкой на соответствующие массивы и перечни сигналов.

В расчетных соотношениях (формулах) должны быть использованы обозначения реквизитов, приведенные при описании в других разделах документа.

Алгоритм представляется одним из следующих способов:

1) Графический, в виде схемы;
2) Табличный;
3) Текстовый;
4) Смешанный графический или табличный с текстовой частью.

Способ представления алгоритма выбирает Разработчик, исходя из сущности алгоритма, своей собственной сущности, и возможности её формального описания.

При этом указываются контрольные соотношения, которые позволяют выявить ошибки, допущенные в процессе счета, и решение о необходимости отклонений от нормального процесса вычислений (продолжении работы по одному из вариантов алгоритма).

В разделе **"Результаты решения"** следует приводить перечень массивов или сигналов, формируемых в результате реализации алгоритма, в том числе:

1) Массивы информации или сигналов, формируемые для выдачи управляющих воздействий и выходных сообщений (документов, видеокадров, сигналов управления и т. д.);
2) Массивы информации, сохраняемой для решения данной и других задач.

По каждому массиву приводится:

1) Наименование, обозначение, максимальное число записей;
2) Перечень наименований и обозначений реквизитов и (или) выходных переменных, используемых для формирования выходных сообщений или ссылку на массивы, содержащие эти данные.

6.45. Документ "Функциональные схемы автоматизации (P&IDs)" *(СЗ)

Документ **"Функциональные схемы автоматизации"** содержит схемы технологического процесса с киповской обвязкой, на которых указаны все средства автоматизации, имеющие отношение к проектируемой системе управления и защиты.

Примечание

Этот документ перенесен в данный раздел из группы документов по Техническому обеспечению - "Схема автоматизации" исходного стандарта РД50-34.698-90, пункт 4.1.1 (см. пояснение в разделе "Техническое обеспечение").

Далее следуют вновь введенные альбомы схем, отражающие непосредственную реализацию алгоритмов системы

управления и противоаварийной защиты. В современных системах эти документы возникают как результат выполнения функций самодокументирования. Им присвоены коды С11, С12 и С13.

6.46. Документ "Блок-схемы алгоритмов РСУ" (СИ)

Документ "Блок-схемы алгоритмов управления" отражает компьютерную реализацию алгоритмов управления в виде:

- Диаграмм функциональных блоков *(Function Block Diagrams),*
- На проблемно-ориентированном языке высокого уровня, или в виде
- Структурированного текста *(Structural Text).*

6.47. Документ "Блок-схемы алгоритмов ПАЗ" (С12)

Документ "Блок-схемы алгоритмов системы ПАЗ" содержит схемы алгоритмов противоаварийной защиты:

- На языке лестничных диаграмм *(Ladder Logic Diagrams),*
- На языке функциональных блоков *(Function Block Diagrams),*
- В виде таблиц решений *(Safety Matrix).*

6.48. Документ "Детальная конфигурация функциональных блоков" (С13)

Документ "Детальная конфигурация функциональных блоков" содержит распечатки сгруппированных по схемам детальных конфигураций функциональных блоков в порядке из выполнения.

Документы:

- Функциональные схемы автоматизации (СЗ),
- Блок-схемы алгоритмов РСУ (СП),
- Блок-схемы алгоритмов ПАЗ (С 12),
- Детальная конфигурация функциональных блоков (С13)

допускается давать в виде единых приложений.

6.49. Требования к содержанию документов с решениями по Организационному обеспечению

Следующие два документа включаются в Рабочую документацию из Технического проекта после внесения всех необходимых дополнений и корректировок, либо создаются непосредственно как документы Технорабочего проекта.

6.50. Документ "Описание организационной структуры" *(ПВ)

Документ содержит следующие разделы:

- Изменения в организационной структуре управления объектом;
- Организация подразделений;
- Реорганизация существующих подразделений управления.

В разделе **"Изменения в организационной структуре управления объектом"** указываются:

1) Проектные решения по изменению организационной структуры управления объектом и их обоснование;
2) Описание изменений во взаимосвязях между подразделениями.

В разделе **"Организация подразделений"** приводится:

1) Описание организационной структуры и функций подразделений, создаваемых с целью обеспечения функционирования АСУТП;
2) Описание регламента работ;
3) Перечень категорий работников и число штатных единиц.

В разделе **"Реорганизация существующих подразделений управления"** приводятся описания изменений, обусловленных созданием АСУТП, которые необходимо осуществить в каждом из действующих подразделений управления объектом:

- В организационной структуре;
- В функциях подразделений;
- В регламенте работы;
- В составе персонала подразделений.

Документ "Описание организационной структуры" формируется Разработчиком системы по согласованию с Заказчиком.

6.51. Документ "Схема организационной структуры" *(СО)

Схема организационной структуры содержит:

1) Состав подразделений и должностных лиц, обеспечивающих функционирование АСУТП, а также использующих при принятии решения информацию, полученную от АСУТП;
2) Основные функции и связи между подразделениями и отдельными должностными лицами, указанными на схеме, и их подчиненность.

Схему организационной структуры определяет Заказчик по рекомендациям Разработчика.

Документ "Организационного обеспечения" **"Методика (технология) автоматизированного проектирования (И1)"** исходного стандарта РД 50-34.698-90 перенесен в раздел "Стандартное программное обеспечение" в качестве самостоятельного документа **"Методы и средства разработки (конфигурирования) (И1)",** как совершенно не относящийся к организационному обеспечению, но точно согласующийся с функциями стандартного программного обеспечения.

6.52. Документ "Технологическая инструкция" (И2)

Технологические инструкции непосредственно в состав документации технорабочего проекта АСУТП не входят. Технологические инструкции составляются и корректируются технологическим персоналом производства с учетом функций АСУТП, и утверждаются главным инженером предприятия.

Скорректированный с учетом внедрения АСУТП технологический регламент согласовывается с проектной организацией, и утверждаются главным инженером предприятия.

6.53. Документ "Руководство пользователя" (И3)

Документ содержит следующие разделы:

- Введение;
- Назначение и условия применения;
- Подготовка к работе;
- Описание операций;

- Аварийные ситуации;
- Рекомендации по освоению.

В разделе **"Введение"** указываются:

1) Область применения;
2) Краткое описание возможностей;
3) Уровень подготовки пользователя;
4) Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю.

В разделе **"Назначение и условия применения"** указываются:

1) Виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации;
2) Условия, при соблюдении которых обеспечивается примене-ние средств автоматизации в соответствии с назначением (например, конфигурация технических средств, операционная среда и общесистемные программные средства, входная информация, носители данных, база данных, требования к подготовке специалистов и т. п.).

В разделе **"Подготовка к работе"** указывается:

1) Состав и содержание дистрибутивного носителя данных;
2) Порядок загрузки данных и программ;
3) Порядок проверки работоспособности.

В разделе **"Описание операций"** приводится:

1) Описание всех выполняемых функций, задач, комплексов задач, процедур;
2) Описание операций обработки данных, необходимых для выполнения функций, задач, процедур.

Для каждой операции обработки данных указываются:

1) Наименование операции;
2) Условия, при которых возможно выполнение операции;
3) Подготовительные действия;
4) Основные действия в требуемой последовательности;
5) Заключительные действия;
6) Ресурсы, расходуемые на операцию.

В описании действий допускаются ссылки на файлы подсказок.

В разделе **"Аварийные ситуации"** указываются:

1) Действия в случае отказа технических средств;
2) Действия по восстановлению программ и данных при обнару-жении ошибок в данных;
3) Действия в случае обнаружения несанкционированного вмешательства в данные;
4) Действия в других аварийных ситуациях.

В разделе **"Рекомендации по освоению"** указываются рекомендации по освоению и эксплуатации, включая описание контрольного примера, правила его запуска и выполнения.

6.54. Сводные таблицы состава документации и распределения работ по стадиям и этапам создания АСУТП

Состав документации и распределение работ на предпроектных стадиях. Первая из таблиц 6.9 содержит состав документации, создаваемой на предпроектных стадиях.

По взаимному согласованию между Разработчиком и Заказчиком процесс создания АСУТП может быть начат непосредственно со стадии Технического задания, минуя стадии 0.1 "Формирование требований к АСУТП" и 0.2 "Разработка концепции АСУТП".

Состав документации и распределение работ по выполнению технического и рабочего (технорабочего) проектов АСУТП. Таблица 6.10 содержит состав документации технического и рабочего (технорабочего) проекта создания АСУТП. Представленный в таблице 6.10 состав проектной и эксплуатационной документации построен с максимально возможным учетом рекомендаций ГОСТ 34.201-89, ГОСТ 34.601-90, ГОСТ 34.602-89, ГОСТ 34.603-92, и РД 50-34.698-90. Кроме того, в таблицах представлен вариант распределения работ и ответственности за результаты работы. Состав документации является строго рекомендуемым, тогда как представленное распределение работ нужно рассматривать как справочное.

Пояснение

Раз и навсегда заданное распределение работ установить нереально в силу специфических особенностей каждого конкретного проекта. Так, например, в роли Разработчика может выступать собственная служба АСУТП или КИП

предприятия. А может и сторонняя организация, которая одновременно является и Поставщиком оборудования.

В таблицах 6.9 и 6.10 приняты следующие обозначения:	
Стадии проекта:	
ПП	Предпроектные стадии
ТП	Технический проект
РД	Рабочая документация
Часть проекта:	
ОР	Общесистемные решения
ТО	Решения по Техническому обеспечению
ИО	Решения по Информационному обеспечению
ПО	Решения по Стандартному программному обеспечению
МО	Решения по Прикладному программному обеспечению
0 0	Решения по Организационному обеспечению
Участники проекта:	
©	Участник работ по стадии
е	Ответственный за стадию и документ

Таблица 6.9

СОСТАВ ДОКУМЕНТАЦИИ ПРЕДПРОЕКТНЫХ СТАДИИ

ПРЕДПРОЕКТНЫЕ СТАДИИ

Документ	Стадия создания	Наименование документа	Код документа	Часть проекта	Генпроектировщик	Проектировщик1	Проектировщик2	Заказ-		Служба автоматизации	Генпод	Разработчик	Разработч*к2		Распределение работ между участниками проекта
0.1	**ПП**	**Фоомиоование требований к АСУТП**	**ФТ**	-						©	©				**Факультативная стадия**
011		*Обследование объекта и обоснование необходимости создания АСУТП*						©		©	©				
012		*Формирование требований Заказчика к АСУТП*						©		©					
013		*Оформление отчета о выполненной работе и заявки на разработку АСУТП*								©	©				
0.2	**ПП**	**Разпабогка конаепиии АСУТП**	**КО**	-				©		©					
021		*Изучение объекта автоматизации*								©	©				
022		*Проведение необходимых научно-исследовательских работ*						©		©	©				
023		*Разработка вариантов концепции АСУТП и выработка концепции АСУТП*						©		©	©				
02.4		*Оформление отчета*						©		©					
0.3	**ПП**	**Техническое задание**	**ТЗ**					©		©		© I			Обязательная стадия
031		*Разработка и утверждение Технического задания на создание АСУТП*													

Таблица 6.10

СОСТАВ ДОКУМЕНТАЦИИ И РАСПРЕДЕЛЕНИЕ РАБОТ ПО ВЫПОЛНЕНИЮ ТЕХНИЧЕСКОГО И РАБОЧЕГО ПРОЕКТОВ СОЗДАНИЯ АСУП1

ОБЩЕСИСТЕМНЫЕ РЕШЕНИЯ

Распределение работ между участниками проекта

Документ	Стадия создания	Наименование документа	Код документа	Часть проекта	Гемпроектировщик	Проектировщик	Проектировщик*2	Заказ		Служба автоматизации	Генподрядчик	Разработчик	Разработчик2		Примечание
1.1	ТП	ведомость проекта	ТП	ОР								©			
12	ТП	Пояснительная записка	П2	ОР								©			
13	ТП	Описание автоматизируемых функций	П3	ОР								©			
	777	*Описание постановки задач (комплекса задач)*	П4	ОР											
14	РД	Общее описание системы	ПД	ОР							•	©			
15	РД	Программа и методика испытаний	ПМ	ОР				©		©	•				
16	РД	Ведомость эксплуатационных документов	ЭД	ОР							•	©			
1.7	РД	Паспорт	ПС	ОР							е	©			
18	РД	Формуляр	ФО	ОР							®	©			
19	ТП.РД	Проектная оценка надежности системы	Б1	ОР								©			Обязательна для объектов I и Н категории

Продолжение таблицы 6.10

СОСТАВ ДОКУМЕНТАЦИИ И РАСПРЕДЕЛЕНИЕ РАБОТ ПО ВЫПОЛНЕНИЮ ТЕХНИЧЕСКОГО И РАБОЧЕГО ПРОЕКТОВ СОЗДАНИЯ АСУТП

2	ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ				Распределение работ между участниками проекта										
Документ	Стадия создания		Код документа	Часть проекта	Генпроектировщик	Проектироа ЦИК1	Проектировщик2	Зажм-		Служба автоматизации	Генподрядчик	Разработчик!	Разработчик		
2.1	ТП	Описание комплекса технических средств	П9	ТО							●				
2.2	ТП	План расположения оборудования АС на объекте	С7	ТО				©			●				В ГОСТ* 34 301 План расположения и проводок Допускается включать в П9 Допускается включать в
2.3	ТП.РД	Схема структурная комплекса технических средств	С1	ТО				©		©	ф				
2.4	ТП.РД	Спецификация оборудования	В4	ТО				©		©	ф				
2.5	РД	Планы расположения оборудования и проводок в ЦПУ	С8	ТО				©		©	ф	©			8 ГОСТа: План расположения Допускается включать в
2.6	РД	Чертеж общего вида системных шкафов и установки технических средств	ВО	ТО							ф	©			В ГОСТа Чертеж общего
2.7	РД	Таблица внутрисистемных соединений и подключении	Св.1	ТО							ф	©			
2.8	РД	Таблица соединений Кросс-Система	С6.2	ТО							ф	©			подключений" (Сб)
2.9	РД	Схемы питания и заземления	СЮ	ТО	©			©		©	ф	©			Вновь ваал документ
2.10	РД	Схемы электрические принципиальные *контуров измерения,* регулирования, сигнализации и блокировок	СБ	ТО	©						ф	©			В ГОСТе: Схема *принципмтьния*
2.11	РД	Инструкция по эксплуатации и обслуживанию КТС	ИЭ	ТО							ф	©			
2.12	РД	Схемы соединения внешних проводок	С4	ТО	*						©	©			
2.13	РД	Схемы подключения внешних проводок	Сб	ТО	ф						©	©			Разрабатывает проектная организация

Продолжение таблицы 6.10

СОСТАВ ДОКУМЕНТАЦИИ И РАСПРЕДЕЛЕНИЕ РАБОТ ПО ВЫПОЛНЕНИЮ ТЕХНИЧЕСКОГО И РАБОЧЕГО ПРОЕКТОВ СОЗДАНИЯ АСУТП

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Документ	Стадия создания	Наименование документа	Код документа	Часть проекта	Распределение работ между участникам* проекта: Генпроеетировщик	Проектировщик	Прое* тмровщик2	Заказ-		Служба автоматизации	Гентадрядчик	Разработчик	Разработчик		
3.1	ТП	Перечень входных и выходных сигналов РСУ	В1	ИО	©			©		©	●	O			В ГОСТ». "Перечень
3.2	ТП	Перечень входных и выходных сигналов системы ПАЗ	В2	ИО	©			©		©	●	©			S ГОСТе "Перечень выход-ных сигналов (документов)"
3.3	ТП	Перечень сигналов взаимообмена РСУ - ПАЗ	В10	ИО	©			©		©	●	©			
3.4	ТП	Описание информационного обеспечения системы	П5	ИО							●		©		
3.5	ТП	Описание организации информационной базы	П6	ИО							●		©		
3.6	ТП	Описание систем классификации и кодирования	П7	ИО						©	●	©	©		
3.7	ТП	Описание массивов исторических данных (архивов)	П8	ИО				©		©	●		©		В ГОСТе "Описание
3.8	ТП, РД	Альбом документов и видеокадров	С9	ИО				©		©	•		©		В ГОСТе "Чертеж формы документа {видеокадре}"
3.9	РД	Состав выходных данных (сигнализаций, сообщений)	88	ИО				©		©	●		©		В ГОСТе "Состав выходных оамных (сообщений)"
3.10	РД	Каталог базы данных	В7	ИО							•		©		
3.11	РД	Инструкция по формированию и ведению базы данных	И4	ИО							●		©		

Продолжение таблицы 378.10

СОСТАВ ДОКУМЕНТАЦИИ И РАСПРЕДЕЛЕНИЕ РАБОТ ПО ВЫПОЛНЕНИЮ ТЕХНИЧЕСКОГО И РАБОЧЕГО ПРОЕКТОВ СОЗДАНИЯ АСУТП

СТАНДАРТНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Документ	Стадия создания	Наименование документа	Код документа	Часть проекте	Распределение работ между участниками проекта: Генпроектировщик	Проектировщик1	Проектировщик2	Заказчик		Служба автоматизации	Генподрядчик	Разработчик	Разработчик	
4.1	ТП	**Описание стандартного программного обеспечения**	ПА	ПО									©	**В ГОСТ"- "Описание**
41.1		*Операционные системы*												
4 1.2		*Структура программного обеспечения*												
4.1.3		*Функции частей программного обеспечения*												
4.2	РД	**Методы и средства разработки (конфигурирования)**	И1	ПО									©	**Документ перенесен из Разделав "Организационное обеспечение" - Пункт в 3**

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Документ	Стадия создания	Наименование документа	Код документа	Часть проекта	Распределение работ между участниками проекта: Генпроектиро-	тировщик1	Проектировщик2	Заказ		Служба автоматизации	Генподрядчик	Разработчик1	Разработчик	
5.1	ТП	**Описание и логические схемы алгоритмов**	ПБ	МО				©		©	*	©	©	**В ГОСТе. "Описание алгоритмов (проектных процедур)" Перенесено из ТО Прежнее название - "Схема автоматизации"**
5.2	ТП	**Функциональные схемы автоматизации (P&IDs)**	С3	МО	©	©	©	©		©	*	©		
5.3	РП	**Блок-схемы алгоритмов РСУ**	С11	МО								©	©	**вновь введенный документ**
5.4	РП	**Блок-схемы алгоритмов ПАЗ**	С12	МО								©	©	
5.5	РП	**Детальная конфигурация функциональных блоков**	С13	МО									©	

Окончание таблицы 6.10

СОСТАВ ДОКУМЕНТАЦИИ И РАСПРЕДЕЛЕНИЕ РАБОТ ПО ВЫПОЛНЕНИЮ ТЕХНИЧЕСКОГО И РАБОЧЕГО ПРОЕКТОВ СОЗДАНИЯ АСУТП

6	ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ				Распределение работ между участниками проекта									
Документ	Стадия создания	Наименование документа	код документа	Часть проекта	*Генпро-*ектиро-вщик	*Проех-*тирое ЦИК1	*Проек-*тироеши к2	Заказ-чик		*Служба* автома тизации	Генпод-рядчик	Разра ботчик!	Разра-ботки к2	
6.1	ТП	Описание организационной структуры	п в	0 0				©		©	*			
6.2	ТП	Схема организационной структуры	со	0 0				©		©	●			
6.3	*РД*	*Методика автоматизированного проектирования*	*И1*	0 0									©	
6.4	РД	Технологическая инструкция	И2	0 0						©	©			
6.5	РД	Руководство пользователя	ИЗ	0 0								©	©	

Перенесено из ОР Может входить в документ ПВ

Документ перенесем е *Раздел 4 "Стандартно»* обеспечение* *под номером 4.2*

Разрабатывается технологическим персоналом завода Изменения технологического регламента согласовываются с проектной организацией

6.55. Образцы Приложений к Договору на разработку технорабочего проекта

В заключение приводятся образцы основных приложений к Договору на разработку технорабочего проекта (ТРП) (таблицы 6.11 -6.14).

Таблица 6.11

Приложение №

К Договору №

От_____2010 г.

К А Л Е Н Д А Р Н Ы Й П Л А Н
Разработка технического задания и технорабочего проекта
АСУТП

№	Наименование этапа работ	Срок выполнения с начала работ
1-ый Этап		**6 недель**
1.	Разработка и согласование Технического задания на создание АСУТП	
2-ой Этап		**12 недель**
2.	Общесистемная проектная документация (утверждаемая часть)	
3-ий Этап		**20 недель**
3.	Рабочие чертежи для производства монтажных работ	
4-ый Этап		**26 недель**
4.	Эксплутационная документация	
5.	Программа и методика испытаний	

Таблица 6.12

Приложение №
К Договору №
От_____2010 г.

РАСЧЕТ СТОИМОСТИ РАБОТ

Разработка технического задания и технорабочего проекта АСУТП и ПАЗ

№	Наименование этапа работ	Продолжительность выполнения В человеко-днях	Стоимость включая НДС
1	Разработка и согласование Технического задания на создание АСУТП		
2	Общесистемная проектная документация (утверждаемая часть)		
3.	Рабочие чертежи для производства монтажных работ		
4	Эксплутационная документация		
5.	Программа и методика испытаний		

ЗАКАЗЧИК'
Генеральный директор

2010 г.

ИСПОЛНИТЕЛЬ:
Генеральный директор

2010 г.

Таблица 6.13

Приложение №
К Договору №
От_____2010 г.

З А Д А Н И Е
на разработку технорабочего проекта АСУТП

1	Наименование и местоположение предприятия-заказчика и объекта проектирования	Название места, организации и производства
2	Основание для проектирования	Решение Протокола Технического совещания Заказчика № от 2010 года
3	Сроки проектирования	2010-2012 годы
4	Производственное, хозяйственное кооперирование, энергообеспечение	От существующих сетей и объектов Заказчика
5	Режим работы	Непрерывный, в течение 8000 часов в год с одним остановом на капитальный ремонт
6	Требования к механизации и автоматизации	Предусмотрена автоматизация технологических процессов с использованием микропроцессорной техники
7	Выделение очередей проектирования	В соответствии с календарным планом
8	Стадия проектирования	Технорабочий проект
9	Сроки выполнения проекта	В соответствии с календарным планом к договору
10	Исходные данные	Монтажно-технологические схемы с киповской обвязкой; Опросные листы КИП и А; Спецификация оборудования (отечественной поставки); Перечень сигнализаций и блокировок, Схемы внешних электрических соединений, Планы помещений управления, межсистемной связи, серверной аппаратуры, UPS;

		Описание технологического процесса; Перечень входов-выходов; Описание логических последовательностей управления и блокировок, Проектная документация на шкафы кроссовые, шкафы барьеров, шкаф релейный; Схемы соединений соединительных коробок; Кабельный журнал; Спецификации на поставляемое оборудование КИП и А, РСУ и ПАЗ с указанием моделей и фирм поставщиков.
11	Состав и порядок разработки документации технорабочего проекта	Разработка технорабочего проекта производится в соответствии с требованиями ГОСТ 34 601-90 "Автоматизированные системы. Стадии создания", РД 50-34.698-90 "Автоматизированные системы. Требования к содержанию документов". Разработка проектной документации осуществляется с учетом контроля системы качества ISO 9001-2000. Состав и содержание рабочего проекта должны быть выполнены в соответствии с пунктом 4 СНиП 11-01-95.
12	Наименование Заказчика	Наименование организации-заказчика
13	Наименование Генпроектировщика	Наименование Проектной организации
14	Проектные организации, принимающие участие в проектировании	Наименования проектных организаций
15	Наименование Генподрядчика по АСУТП	Наименование организации-разработчика АСУТП
16	Особые условия проектирования и строительства	16.1. При проектировании применяется технологическое оборудование, система управления, полевой КИП и другое оборудование, закупленное по контракту на поставку оборудования. 16.2. Рабочий проект АСУТП должен быть выполнен в соответствии с российскими стандартами, нормами и правилами. В состав основных технических решений для согласования включить перечень отступлений от действующих российских стандартов, норм и правил.

Представленный в предыдущих разделах и в таблицах 6.9 и 6.10 состав проектной документации построен с максимально возможным учетом рекомендаций ГОСТ 34.201-89, ГОСТ 34.601-90, ГОСТ 34.602-89, ГОСТ 34.603-92, и РД 50-34.698-90. Во многих случаях вполне достаточным является более компактный комплект документации технорабочего проекта, приведенный в таблице 6.14.

Таблица 6.14

Приложение №

К Договору №

От_____2010 г.

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ТЕХНОРАБОЧЕГО ПРОЕКТА

Номер тома	Код документа	Наименование	Примечание
1		**Проектная документация:**	
	СП	**Состав проекта**	
	П2	Пояснительная записка	
	пз	**Описание автоматизируемых функций**	
	П4	**Описание постановки задач**	Доп. вкл в П2 или ПЗ
	П9	Описание комплекса технических средств	
	С1	Схема структурная комплекса технических средств	Доп. вкл в П9
	С8	План расположения оборудования и проводок в ЦПУ	Доп. вкл. в П9
	С7	План расположения оборудования АС на объекте	Доп вкл в П9
	В4	**Спецификация оборудования системы**	
	В1	**Перечень входных и выходных сигналов РСУ**	
	В2	**Перечень входных и выходных сигналов ПАЗ**	
	В12	**Перечень сигналов взаимообмена РСУ и ПАЗ**	

Номер тома	Код документа	Наименование	Примечание
	П5	Описание информационного обеспечения системы	
	П6	Описание организации информационной базы	
	П7	Описание систем классификации и кодирования	
	П8	Описание массива исторических данных (архивов)	
	ПА	Описание стандартного программного обеспечения	
	ПВ	Описание организационной структуры	
	СО	Схема организационной структуры	Доп. вкл. в ПВ
	СЗ	Функциональная схема автоматизации	
	ПБ 1.1	Описание алгоритмов (проектных процедур) РСУ	
	ПБ 2 1	Описание алгоритмов (проектных процедур) ПАЗ	
	Б1	Проектная оценка надежности системы	
2		**Рабочие чертежи:**	
	СБ	Схемы электрические принципиальные	
	ВО	Чертежи общего вида системных шкафов и установки технических средств	
	Сб 1	Таблица внутрисистемных соединений и подключений	
	Сб 2	Таблица соединений кросс-система	
	СЮ	Схемы питания и заземления	
	ПБ 1 2	Логические схемы РСУ	
	ПБ.2.2	Логические схемы ПАЗ	

Номер тома	Код документа	Наименование	Примечание
	С13	Детальная конфигурация функциональных блоков	
	С4	*Схемы соединения внешних проводок*	*Гэнпроектировщик*
	С5	*Схемы подключения внешних проводок*	*Генпроектировщик*
	С11	Кабельный журнал	
3		**Эксплуатационная документация:**	
	ЭД	Ведомость эксплуатационных документов	
	ПС	Паспорт	
	ФО	Формуляр	
	ПД	Общее описание системы	
	ИЭ	Инструкция по эксплуатации и обслуживанию КТС	
	С9	Альбом документов и видеокадров	
	В8	Состав выходных данных (сигнализаций, сообщений)	Доп вкл. в С9
	В7	Каталог баз данных	
	И4	Инструкция по формированию и ведению базы данных	
	И1	Методика (технология) автоматизированного проектирования	
	ИВ	Руководство пользователя (Инструкция оператора)	
	И2	*Технологическая инструкция*	Генлроектировщик, *Заказчик*
4	**ПМ**	**Программа и методика испытаний**	

Глава 7

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА СОЗДАНИЕ АСУТП

В настоящей главе представлен отработанный в нескольких десятках успешных проектов полный авторский текст Технического задания на создание АСУТП.

Документ полностью соответствует требованиям ГОСТ 34.602-89 "*Комплекс стандартов на АС. Техническое задание на создание автоматизированной системы*

Для привязки текста Технического задания к конкретному технологическому объекту достаточно сделать подстановку собственных атрибутов и сведений об объекте автоматизации. Вместе с тем, необходимо очень тщательно поработать над Приложениями к Техническому заданию, определяющими и особенности объекта автоматизации, и его информационную и функциональную мощность, и график выполнения проекта, и состав проектной документации.

7.1. Титульный лист

УТВЕРЖДАЮ:
Руководитель
Организации-разработчика
/ /
" " 2010 г.

УТВЕРЖДАЮ:
Руководитель
Предприятия-заказчика
/ /
2010 г.

Автоматизированная система управления технологическим процессом производства АВС
ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА СОЗДАНИЕ АСУТП

Код предприятия.425790.*Трехзначный номер ТЗ*

Действуете "____"_____2010г.

СОГЛАСОВАНО:
Директор
производства / завода
Предприятия-заказчика
/ /
" "_____2010 г.

СОГЛАСОВАНО:
Технический директор
Проектной
организации
/ /
"_____2010 г.

СОГЛАСОВАНО:
Зам. главного инженера
По метрологии и КИП
Предприятия-заказчика
/ /
" "_____2010 г.

СОГЛАСОВАНО:
Руководитель
территориального органа
Ростехнадзора
/ /
" "_____2010 г.

7.2. Общие сведения

Полное наименование Системы:

"Автоматизированная система управления технологическим процессом условного производства АВС".

Краткое наименование Системы:

АСУТП *АВС*, в дальнейшем - **Система.**

Шифр темы:

Код и;?едя/?шшшя.425790.Трехзначный *номер ТЗ*

Наименование организаций Заказчика, Разработчика, Проектной организации и их реквизиты.

Проектная организация:

Наименование организации
Технический директор -
тел.:
факс:
Руководитель проекта -
тел.:
E-mail:

Организация-разработчик:

Наименование организации
Технический директор -
тел.:
факс:
Руководитель проекта -
тел.:
E-mail:

Организация-заказчик:

Наименование организации
Главный инженер производства -
тел.:
факс:
Руководитель проекта -
тел.:
E-mail:

Основание для разработки АСУТП. Основанием для разработки АСУТП, состоящей из распределенной системы управления (РСУ) и системы противоаварийной защиты (ПАЗ), является решение Протокола технического совещания от 26.02.2010 года, утвержденного генеральным директором предприятия, а также Договор на разработку Технорабочего проекта с фирмой *XYZ № YNF-1234/02 от 26.08.2010 года.*

В качестве исходных данных использованы:

- Спецификация оборудования по Договору на поставку оборудования *YNF-1234/01 от 26.08.2010 г.*
- Проектная документация, выполненная Проектной организацией.
- ГОСТ 34.602-89 "*Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы ".*

Сроки выполнения работ:

- Начало работы - "_____"_____2010 г.
- Окончание работы- "_____"_____2012 г.

Источники и порядок финансирования. *Работа финансируется Заказчиком с использованием целевого кредита* ***Сбербанка России.***

Порядок оформления и предъявления Заказчику результатов работы. Материалы технорабочего проекта АСУТП в составе, соответствующем:

1. ГОСТ 34.201-89 *"Виды, комплектность и обозначение документов при создании автоматизированных систем*[99]*;*
2. Стандарту предприятия на [11]*Порядок разработки, внедрения, сопровождения и эксплуатации автоматизированных систем управления технологическими процессами*
3. Перечню документации технорабочего проекта в соответствии с договором *YNF-1234/02* (приведен в Приложении 6 к настоящему ТЗ),

разрабатываются и оформляются Разработчиком, согласовываются с Проектной организацией в соответствии с этапами Календарного плана, определенного Договором на разработку Технорабочего проекта, и предъявляются Заказчику для утверждения и приемки.

Разработанная система внедряется и сдается Заказчику в соответствии с:

1. ГОСТ 24.104-85 ЕСС АСУ "*Автоматизированные системы управления. Общие требования",* и
2. ГОСТ 34.603-92 *"Виды испытаний автоматизированных систем ".*

Стадии и этапы работы должны быть оформлены и представлены в следующем порядке:

- Разработка и утверждение окончательной Спецификации оборудования. Утверждается Протоколом в течение 1 месяца после начала работ;
- Документация технорабочего проекта принимается и утверждается Заказчиком через____месяцев после начала работ;
- Шеф-монтажные и пусконаладочные работы с началом через____и окончанием через____месяцев после начала работ;
- Завершение оформляется Актом завершения пусконаладочных работ и предъявлением Системы на испытательный **предгарантийный 72-часовой пробег** в присутствии специалистов Заказчика и Разработчика.
- Завершение предварительных испытаний Системы оформляется совместным Актом приемки в опытную эксплуатацию;
- Опытная эксплуатация продолжительностью **не менее 2 месяцев** завершается приемочными испытаниями и Актом ввода в постоянную (промышленную) эксплуатацию через____месяцев после начала работ.

Согласованный со всеми участниками проекта План-график выполнения работ приведен в Приложении 5.

Требования к Системе управления и защиты, установленные настоящим Техническим заданием, не должны ограничивать Разработчика Системы в поиске и реализации наиболее эффективных технических и технико-экономических решений.

Изменения к данному Техническому заданию оформляются в виде Протокола или Дополнения к ТЗ, согласовываются с региональным управлением Ростехнадзора, и подписываются Заказчиком и Разработчиком Системы. С этого момента Протокол или Дополнение к ТЗ становятся неотъемлемой частью Технического задания на Систему.

7.3. Назначение и цели создания Системы

Назначение Системы. АСУТП предназначена:

- Для целевого применения как законченное изделие под определенный объект автоматизации - производство АВС;
- Для стабилизации заданных режимов технологического процесса путем контроля технологических параметров, визуального представления, и выдачи управляющих воздействий на исполнительные механизмы, как в автоматическом режиме, так и в результате действий технолога - оператора;
- Для определения аварийных ситуаций на технологических узлах путем опроса подключенных к Системе датчиков в автоматическом режиме, анализа измеренных значений, и переключения технологических узлов в безопасное состояние путем выдачи управляющих воздействий на исполнительные механизмы в автоматическом режиме, или по инициативе оперативного персонала.

Цели создания Системы. Целями создания АСУТП являются:

- Стабилизация эксплуатационных показателей технологического оборудования и режимных параметров технологического процесса;
- Увеличение выхода товарной продукции;
- Уменьшение материальных и энергетических затрат;
- Выбор рациональных технологических режимов с учетом показаний промышленных анализаторов, установленных на потоках, и оперативной корректировки режима по данным лабораторных анализов;
- Улучшение качественных показателей конечной продукции;
- Предотвращение аварийных ситуаций.

Ключевым критерием качества работы АСУТП является стабильность заданных характеристик технологического процесса с учетом противоаварийной защиты для всех стадий ісинологического процесса.

Кроме того, предполагается, что достижение вышеозначенных целей должно способствовать улучшению экологиче-

ской обстановки за счет уменьшения загрязненности промышленных стоков и выброса вредных веществ в атмосферу. В целом, внедрение АСУТП должно обеспечивать достижение главной цели политики предприятия в области качества:

Получение стабильной прибыли за счет производства конкурентоспособной продукции, удовлетворяющей требованиям потребителей.

7.4. Характеристика объекта автоматизации

Производство АБС состоит из технологических блоков, относящихся к I и II категории взрывоопасности.

Технологические процессы производства АВС характеризуется большим числом переменных состояния и управления, сложной корреляцией технологических параметров, воздействием на объект многочисленных возмущений, связанных как с плановыми переключениями технологических аппаратов, так и с присутствием неконтролируемых примесей; применением токсичных, пожаро - и взрывоопасных продуктов, что в совокупности предъявляет повышенные требования к АСУТП.

Технологические процессы являются непрерывными. Однако для выпуска продукции различных марок существует необходимость переключения аппаратов и конфигурации различных вариантов технологических схем, поэтому АСУТП должна иметь возможность осуществления программно-логического управления по предопределенным регламентированным последовательностям операций.

И т.д.

Основные характеристики системы приводятся в приложениях:

- *Краткое описание технологического процесса дано в Приложении 1 к настоящему Техническому заданию.*
- *Структурная схема технологического процесса приведена в Приложении 2.*
- *Исходный перечень входов-выходов РСУ приведен в Приложении 3-1.*
- *Исходный перечень входов-выходов ПАЗ приведен в Приложении 3-2.*

- *Сводный перечень входов-выходов РСУ приведен в Приложении 3-3.*
- *Сводный перечень входов-выходов ПАЗ приведен в Приложении 3-4.*
- *Структурная схема АСУТП приведена в Приложении 4.*
- *Проектный План-график выполнения работ приведен в Приложении 5.*
- *Перечень документации технорабочего проекта в рамках договора на разработку технорабочего проекта приведен в Приложении 6.*

7.5. Требования к Системе

Требования к Системе в целом. Разрабатываемая АСУТП должна соответствовать ГОСТ 24.104-85 ЕСС АСУ *"Автоматизированные системы управления. Общие требования"* с учетом требований, изложенных в данном разделе.

Требования к структуре и функционированию Системы. По функциональным признакам структура АСУТП подразделяется на следующие категории:

- Распределенная система управления (в дальнейшем РСУ), базирующаяся на специализированной микропроцессорной технике, предназначенной для управления технологическим процессом совместно с оперативным персоналом в режиме реального времени, и предоставления информации в виде технологических данных, трендов, отчетов в заводскую ЛВС - директору завода, главному инженеру, диспетчеру, главным специалистам, начальникам технологических цехов;
- Система противоаварийной защиты (в дальнейшем ПАЗ), базирующаяся на специализированной микропроцессорной технике повышенной надежности, предназначенной для предотвращения аварийных ситуаций, и автоматического перевода технологического процесса в безопасное состояние при возникновении предаварийных ситуаций;
- Периферийное оборудование - понятие, объединяющее датчики, анализаторы, преобразователи и исполнительные механизмы, а также электрические и другие

приводы, установленные как непосредственно на технологическом оборудовании, так и в специальных помещениях, и подключенные к РСУ и ПАЗ.

АСУТП должна быть ориентирована на работу в жестком реальном времени, и быть предсказуемой, то есть обеспечивать выполнение всех функций с заданной периодичностью и точно в назначенный срок.

Должна быть обеспечена надежная защита АСУТП:

- От несанкционированного доступа;
- От разрушения или останова работы программного обеспечения в результате некорректных действий оператора технологического процесса;
- От проникновения в Систему вирусов.

Должна быть обеспечена возможность полного исключения на использование станции оператора в качестве персонального компьютера для непроизводственных целей, выходящих за рамки инструкций технолога-оператора.

Для удобства восприятия информации и выработки соответствующих стереотипов у технолога-оператора, вся технологическая информация должна быть организована иерархически, воспроизводя организационную структуру производства в естественной для технологического персонала форме:

- Производство / Цех
- Отделение
- Технологический узел
- Контур (параметр).

Должна быть возможность управления технологическим процессом с любого рабочего места оператора-технолога в данном помещении управления - операторной.

В составе программного обеспечения Системы должен быть набор программных модулей - функциональных блоков, позволяющих осуществлять контроль и управление технологическими объектами различных классов. Система должна иметь возможность оперативного конфигурирования прикладного программного обеспечения на отдельной инженерной станции без нарушения работоспособности Системы.

Конфигурирование и настройка Системы под конкретный объект управления должна производиться в человеко-машинной интерактивной среде, обученными работе с Системой специалистами. АСУТП должна иметь гибкую структуру,

обеспечивать модификацию алгоритмов решения задач и наборов участвующих в них переменных, конфигурирование схем регулирования и управления.

Работа распределенной системы управления не должна влиять на работу системы противоаварийной защиты - как в нормальном режиме работы, так и в случае нарушения своей работоспособности.

В Системе должны иметься аппаратные и аппаратно-программные средства диагностики сетей, станций, блоков и модулей.

Пуск и останов технологических установок будет производиться технологическим персоналом в автоматизированном режиме с помощью дистанционного управления под контролем АСУТП.

Система противоаварийной защиты должна строиться на автономно функционирующих средствах микропроцессорной техники, измерительных датчиках и исполнительных механизмах, и обеспечивать гарантированную реализацию алгоритмов защиты технологического процесса в предаварийных ситуациях.

Технические средства РСУ и ПАЗ должны быть резервированы. При выходе из строя какого-либо из модулей (блоков) должен происходить автоматический переход на резервный модуль (блок) с регистрацией и выдачей соответствующего сообщения. Должна быть предусмотрена возможность замены неисправных модулей в оперативном режиме работы РСУ и системы ПАЗ.

АСУТП должна иметь программные и аппаратные средства для подключения к локальной вычислительной сети производства (завода), а также к единой ("корпоративной") сети предприятия.

Гарантийный срок на оборудование систем РСУ и ПАЗ должен быть не менее 1 года с учётом срока хранения и при соблюдении Заказчиком условий хранения, монтажа и эксплуатации, оговоренных настоящим ТЗ, проектной и эксплуатационной документацией.

Требования к численности и квалификации персонала. Персонал автоматизированной системы в соответствии с ролью, выполняемой им в процессе функционирования Системы, делится на 2 основные категории:

1) Оперативный (технологический) персонал;
2) Эксплуатационный (обслуживающий) персонал.

К оперативному персоналу относятся лица, непосредственно участвующие в принятии решений по управлению технологическим процессом и в выполнении функций защиты. В данном случае - это аппаратчики, начальники смен и технологических установок, технологи и начальники цехов.

Количество и квалификация технологического персонала определяется действующим штатным расписанием.

Внедрение Системы не повлияет на численность технологического персонала, однако потребует от него специальной подготовки.

К эксплуатационному (обслуживающему) персоналу относятся лица, обеспечивающие нормальные условия функционирования Системы в соответствии с Инструкциями по эксплуатации и обслуживанию, и выполняющие работы по техническому обслуживанию Системы.

Предполагается, что обслуживающий персонал подразделения АСУТП будет состоять как минимум из следующих категорий работников, прошедших соответствующее обучение:

- Начальник сектора АСУТП
- Ведущий инженер-электроник
- Ведущий инженер-программист
- Инженер-электроник
- Инженер-программист
- Сменный инженер.

Примечание

По согласованию с администрацией предприятия численность и состав персонала сектора АСУТП может быть оставлен в соответствии с существующим штатным расписанием.

Перед вводом Системы в эксплуатацию технологический и эксплуатационный персонал должен пройти соответствующее обучение.

Помимо персонала АСУТП, работу Системы обеспечивает также ремонтный персонал, непосредственно в функционировании Системы не участвующий, однако способный выполнить ремонт отказавших технических средств.

Требования к показателям назначения. Оборудование РСУ и ПАЗ должно иметь модульную архитектуру, предусматривающую возможность расширения и развития функций АСУТП.

Программное обеспечение АСУТП должно иметь гибкую структуру, давать возможность легко адаптироваться к изменениям характеристик технологических процессов, обеспечивать модификацию алгоритмов решения задач и наборов участвующих в них переменных, переконфигурирование схем регулирования и управления.

Система ПАЗ должна обеспечивать функции противоаварийной защиты по заданным в технологическом регламенте алгоритмам, и иметь возможность переконфигурации при изменении алгоритмов защиты технологического процесса.

На стадии подготовки спецификаций проекта необходимо предусмотреть достаточные резервы по оперативной и дисковой памяти, а также по быстродействию микропроцессорных устройств и промышленных сетей, которые (резервы) потребуются для развития функций Системы.

Как РСУ, так и система ПАЗ, должны иметь 10% резерв по информационным и управляющим каналам.

Требования к надёжности. Показатели надежности Системы должны отвечать требованиям ГОСТ 24.701-86 ЕСС АСУ "Надежность автоматизированных систем управления. Основные положения". Обеспечение необходимого уровня надежности требует проведения специального комплекса работ, выполняемых на разных стадиях создания и эксплуатации АСУТП.

При решении вопросов обеспечения требуемого уровня надежности АСУТП необходимо учитывать следующие особенности:

1) АСУТП является многофункциональной Системой, функции которой имеют различную значимость и, соответственно, характеризуются разным уровнем требований к надежности их выполнения;
2) В работе АСУТП участвуют различные виды обеспечения, в том числе и так называемый "человеческий фактор", который может в существенной степени влиять на уровень надежности АСУТП;

3) В состав АСУТП входит большое количество разнородных элементов (включая технологический и эксплуатационный персонал). При этом в выполнении одной функции АСУТП обычно участвуют несколько различных элементов, а один и тот же элемент может участвовать в выполнении нескольких функций Системы.

Поэтому при решении вопросов, связанных с надежностью АСУТП, количественное описание, анализ, оценка и обеспечение надежности необходимо проводить **по каэвдой функции АСУТП в отдельности. В** обоснованных случаях необходимо использовать анализ возможности возникновения в Системе аварийных ситуаций, ведущих к значительным техническим, экономическим или социальным потерям вследствие аварии объекта управления или автоматизированного комплекса в целом.

Уровень надежности АСУТП в существенной степени зависит от следующих *основных* факторов:

1) Состав и уровень надежности используемых технических средств, их взаимодействие и взаимосвязь в структуре комплекса технических средств АСУТП;
2) Состав и уровень надежности используемых программных средств, их содержание, взаимосвязь и взаимодействие в структуре программного обеспечения АСУТП;
3) Уровень квалификации, организации работы, и уровень надежности технологического, эксплуатационного и обслуживающего персонала;
4) Рациональность распределения задач, решаемых Системой, между КТС, программным обеспечением, и персоналом;
5) Режимы и организационные формы эксплуатации КТС АСУТП;
6) Степень использования различных видов резервирования (структурного, информационного, алгоритмического, функционального, временного и др.);
7) Степень использования методов и средств технической диагностики;
8) Реальные условия функционирования АСУТП.

Пояснение

Свойства информационного, математического, лингвистического, правового обеспечения АСУТП влияют на надежность АСУТП косвенно - через функционирование технических и программных средств, действия технологического и эксплуатационного персонала, поэтому при решении вопросов, связанных с надежностью АСУТП, отдельно не учитываются.

При анализе надежности АСУТП необходимо учитывать, что элементы, входящие в состав какой-либо функциональной подсистемы, должны решать задачи взаимной компенсации нарушений нормальной работы, сводить к минимуму их неблагоприятные последствия, и предотвращать переход этих нарушений в отказы выполнения соответствующих функций:

1) Программное обеспечение функциональной подсистемы должно предотвращать возникновение отказов в выполнении функций АСУТП при отказах технических средств функциональной подсистемы и при ошибках персонала, участвующего в выполнении этой функции, либо должно обеспечить перевод отказов, ведущих к большим потерям, в отказы, сопряженные с малыми потерями;
2) Технические средства функциональной подсистемы должны не допускать перехода определенных нарушений в работе программного обеспечения и персонала в отказ выполнения функции АСУТП, либо минимизировать последствия отказа;
3) Технологический и эксплуатационный персонал должен принимать активные меры к недопущению отказов в работе функциональной подсистемы при отказах технических средств или при выявлении ошибок в программном обеспечении, либо к снижению потерь от таких отказов.

Выбор состава показателей надежности АСУТП необходимо производить на основе установленного данным Техническим заданием перечня функций Системы, видов их отказов, и перечня аварийных ситуаций, для которых регламентируют требования к надежности. Исходными данными для определения обоснованных требований к надежности АСУТП являются:

1) Виды и критерии отказов по всем рассматриваемым функциям АСУТП;
2) Уровень эффективности по всем функциям Системы и величины ущербов по всем видам отказов;
3) Состав персонала, технических и программных элементов, участвующих в выполнении каждой функции Системы;
4) Возможные пути повышения надежности для каждой функции АСУТП, и связанные с ним затраты;
5) Величины ущербов, связанные с возникновением в АСУТП аварийных ситуаций;
6) Возможные пути снижения опасности возникновения аварийных ситуаций, и связанные с ними затраты.

Требования по обеспечению надежности АСУТП должны определяться путем сопоставления потерь, связанных с отказами АСУТП в выполнении функций и с возникновением аварийных ситуаций, и затрат, связанных с обеспечением и повышением надежности АСУТП, включая удорожание оборудования.

Надежность технических средств и программного обеспечения, предназначенных для реализации каждой из функций Системы, должна обеспечивать в совокупности выполнение указанных требований по надежности функций Системы в целом.

Необходимый уровень надежности конкретной АСУТП должен обеспечиваться специальным комплексом работ, проводимых на всех этапах создания и функционирования Системы. К обязательным работам по обеспечению надежности АСУТП, которые следует выполнять в процессе создания АСУТП, относятся:

1) Анализ состава и содержания функций разрабатываемой АСУТП;
2) Определение конкретного содержания понятия ОТКАЗ, и критериев отказа по каждому виду отказов для всех функций Системы;
3) Определение конкретного содержания понятия АВАРИЙНАЯ СИТУАЦИЯ для данной Системы и критериев аварийной ситуации по каждой из рассматриваемых ситуаций;
4) Анализ аварийных ситуаций в АСУТП;

5) Выбор состава показателей надежности по всем функциям АСУТП, указанным в Техническом задании на АСУТП и, при необходимости, по всем аварийным ситуациям и определение требований к уровню их значений;
6) Выбор методов оценки надежности АСУТП на различных стадиях ее создания и функционирования;
7) Проведение проектной оценки надежности АСУТП при разработке технического (технорабочего) проекта Системы. Общий порядок оценки надежности автоматизированных систем приведен в разделе 4 ГОСТа 24.701-86;
8) Определение режимов и параметров технической эксплуатации АСУТП.

НАДЕЖНОСТЬ СИСТЕМ ПАЗ должна обеспечиваться:

1. АППАРАТУРНЫМ РЕЗЕРВИРОВАНИЕМ:
   - Модулей центрального процессора; (управляющих модулей);
   - Модулей ввода вывода;
   - Промышленных сетей;
   - Источников питания.
2. ВРЕМЕННОЙ, АЛГОРИТМИЧЕСКОЙ, ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ ИЗБЫТОЧНОСТЬЮ, и
3. НАЛИЧИЕМ СРЕДСТВ ОПЕРАТИВНОЙ И АВТОНОМНОЙ ДИАГНОСТИКИ.

Далее приводятся основные меры и показатели, которые необходимо предусмотреть для обеспечения надежности комплекса технических средств и программного обеспечения:

- РСУ и система ПАЗ должны иметь средства бесперебойного питания, чтобы функции контроля и защиты выполнялись при любых сбоях энергоснабжения. Система бесперебойного электропитания должна обеспечивать функционирование РСУ, ПАЗ и полевого оборудования КИП и А в течение 30 минут после аварийного отключения электроэнергии;
- Структура комплекса технических средств должна предусматривать возможность запитывания РСУ и системы ПАЗ от двух независимых вводов через один

источник бесперебойного питания, имеющего возможность автоматического включения резерва;

- После снятия условий защитных блокировок включение исполнительных механизмов должно выполняться технологическим персоналом дистанционно с рабочего места технолога-оператора (при условии санкционированного доступа к органам управления);
- Как РСУ, так и система ПАЗ должны иметь в своем составе аппаратно-программные средства самодиагностики, позволяющие фиксировать отказы оборудования Системы с точностью до модуля, и передавать о них сообщения на рабочие станции и для архивирования;
- Для РСУ и системы ПАЗ должно быть предусмотрено резервирование необходимого типа (дублированные контроллеры, дублированные платы ввода-вывода, дублированные блоки питания, дублированная шина системы);
- Все промышленные сети в составе АСУТП должны быть резервированы.

Согласно ПБ 09-540-03, п. 6.3.2,

Для взрывоопасных технологических объектов системы контроля, управления и ПАЗ должны проходить комплексное опробование по специальным программам. Серийно выпускаемые приборы проходят специальную отбраковку по результатам стендовых испытаний на предприятиях-изготовителях приборов (с соответствующей отметкой в паспортах).

На все поставляемые технические средства в документации должен быть указан назначенный срок службы, или назначенный ресурс. Средний срок службы Системы в целом - не менее 10 лет с учетом проведения восстановительных работ

Требования безопасности. Потенциальная опасность технологического процесса в широком смысле заложена в целом в самом производстве. Технологические процессы данного производства характеризуются применением токсичных, пожаро - и взрывоопасных продуктов, что в совокупности предъявляет жесткие требования к АСУТП.

В связи с этим используемые в составе АСУТП технические средства, устанавливаемые непосредственно на технологических установках, по защищенности от воздействия окружающей среды должны иметь взрывозащищённое исполнение, соответствующее категории взрывоопасности технологического объекта и применяемым на производстве продуктам.

Остальные технические средства, устанавливаемые в помещениях управления - нормального исполнения. Для технологических процессов, которые требуют обеспечения взрывозащиты объекта автоматизации, все каналы ввода-вывода должны быть оснащены взрывозащитой типа "искробезопасная электрическая цепь".

РСУ и система ПАЗ должны разрабатываться с учётом требований безопасности, определённых ПБ 09-540-03 "Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств", а также специфических требований промышленной безопасности предприятия.

В частности, согласно ПБ 09-540-03, пункт 6.9.2, запрещается ведение технологических процессов и работа оборудования с неисправными или отключенными системами контроля, управления и ПАЗ. Согласно пункту 6.10.3 тех же Правил, при снятии средств контроля, управления и ПАЗ, связи и оповещения для ремонта, наладки или поверки, **должна производиться немедленная замена снятых средств на идентичные по всем параметрам.** Соответственно, АСУТП должна иметь программные и технические средства регистрации и безаварийной обработки этих ситуаций.

Технические средства АСУТП должны соответствовать требованиям "*Правил устройства электроустановок*". Все внешние элементы технических средств АСУТП, находящиеся под напряжением, должны иметь защиту от случайного прикосновения человека, а сами технические средства иметь защитное заземление в соответствии с требованиями "*Правил устройства электроустановок* и ГОСТ 12.1.030 ССБТ "*Защитное заземление, зануление*

В помещениях управления должны быть предусмотрены автономные контуры заземления, не связанные гальванически с контурами заземления каких-либо других производственных помещений, а так же с нейтралью трехфазной сети.

Сопротивление заземляющего устройства между корпусом любой части оборудования Системы и землей (грунтом) не должно превышать 4 Ом в любое время года. В общем случае должны быть предусмотрены два контура заземления для оборудования РСУ и ПАЗ:

- Контур защитного заземления с сопротивлением не более 4 Ом;
- При наличии искробезопасных цепей с пассивными барьерами Зенера - контур "чистого" заземления с сопротивлением не более 1 Ом.

Технические средства должны быть установлены так, чтобы обеспечивалась безопасность при их монтаже, наладке, эксплуатации, техническом обслуживании и ремонте.

На применение трубопроводной арматуры, средств защиты, а также средств измерения, связи и автоматизации, изготовляемых на территории России, должны быть представлены Разрешения на применение Ростехнадзора или его территориальных органов. Для ввозимых из-за рубежа - разрешение Ростехнадзора на их применение.

Также должны быть представлены Разрешения Ростехнадзора на применение средств защиты оборудования (предохранительные клапаны, мембранные предохранительные устройства), а также всех элементов, задействованных в системах противоаварийной автоматической защиты.

Комфортные условия работы персонала должны соответствовать действующим санитарным нормам по СанПиН 2.2.2/2.4.1340-03 *"Гигиенические требования к персональным электронным вычислительным машинам и организации работы. Санитарно - эпидемиологические правила и нормативы "*

Уровни шума и звуковой мощности в местах расположения персонала не должны превышать значений, установленных ГОСТом 12.1.003 ССБТ *"Шум. Общие требования безопасности*и санитарными нормами. При этом должны быть учтены уровни шумов и звуковой мощности, создаваемые всеми источниками.

Требования безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств Системы должны быть приведены в Документации на технические средства.

Общие требования по технике безопасности при эксплуатации АСУТП должны устанавливаться специальным разделом инструкции по эксплуатации Системы.

Требования по эргономике и технической эстетике. Взаимодействие человека с Системой осуществляется через рабочее место технолога-оператора, оборудованное операторской станцией, в состав которой входят цветные графические терминалы, алфавитно-цифровая и функциональная клавиатура, и печатающие устройства. Общие эргономические требования, регламентирующие организацию рабочего места, взаимное расположение средств связи в пределах рабочего места - по СанПиН 2.2.2/2.4.1340-03.

Станции технолога оператора должны быть оснащены функциональной клавиатурой, обеспечивающей возможность прямого выбора необходимого фрагмента информации путем однократного прикосновения к элементу клавиатуры с надписью на русском языке.

Отображение информации на экранах дисплеев должно обеспечивать получение для каждой зоны контроля и управления полной характеристики текущего состояния, архивных данных технологического процесса и оборудования в виде, наиболее удобном для восприятия в конкретной ситуации.

Размеры экрана должны быть **не менее 21 дюйма** по диагонали. Фрагменты изображения не должны быть перенасыщены информацией и разнообразием цветовой гаммы.

Предупредительная и предаварийная сигнализация должна сопровождаться мерцанием и изменением цвета цифровых значений переменных на экране дисплея, а также звуковой сигнализацией, квитируемой технологическим персоналом.

Уровни освещённости рабочих мест персонала должны соответствовать характеру и условиям труда. Должна быть предусмотрена защита от слепящего действия света и отражения (бликов).

Компоновка технических средств Системы должна быть рациональной, как с точки зрения монтажных связей между ними, так и удобства их эксплуатации и обслуживания.

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению. Функционирование Системы должно быть рассчитано на круглосуточный режим работы, с остановкой на профилактику не чаще, чем 1 раз в год в период капитального ремонта.

Виды, периодичность и регламент обслуживания технических средств должны быть указаны в соответствующих инструкциях по эксплуатации.

Основные технические средства РСУ и ПАЗ будут размещаться в помещениях управления. Помещения, в которых должны располагаться данные технические средства, должны отвечать требованиям Инструкций по проектированию зданий и помещений для ЭВМ.

В соответствии с ГОСТом 21552-84 "*Средства вычислительной техники. Общие технические требования, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение"* и ГОСТом 12.1.005-88 ССБТ *"Общие санитарно гигиенические требования к воздуху рабочей зоны",* для нормального функционирования вычислительной техники в этих помещениях должны быть обеспечены следующие условия:

- Температура окружающего воздуха (20 ± 5) °С;
- Относительная влажность окружающего воздуха (60 ± 15)%;
- Атмосферное давление от 84 до 107 кПа (680-800 мм. рт. ст.);
- Запыленность воздуха в помещении - не более 1мг / куб. м при размере частиц не более 3 мкм;
- Напряженность внешнего электрического поля должна быть не более 0.3 V/**М**;
- Напряженность внешнего магнитного поля должна быть не более 5.0 А/м;
- Частота вибрации должна быть не более 25 Гц при амплитуде смещений не более 0.1 мм.

В воздухе помещений не должно быть агрессивных веществ, вызывающих коррозию. Необходимо обеспечить контроль температуры, относительной влажности и атмосферного давления в помещениях постоянного пребывания оперативного и обслуживающего персонала.

Вводы переменного напряжения должны осуществляться через фильтры подавления помех. Нормально допустимые и предельно допустимые значения установившегося отклонения напряжения на выводах приемников электрической энергии равны соответственно ±5 и ±10 % от номинального напряжения электрической сети по ГОСТ 21128 (номинальное напряжение).

Действующее значение напряжения 220V ± 5% (предельно ± 10%), частота 50 ± 0,2 Гц (предельно ± 0,4 Гц), коэффициент несинусоидальности - нормально до 8 % и предельно - до 12% (ГОСТ 13109-97).

Оборудование Системы должно быть обеспечено комплектом ЗИП на весь гарантийный срок. В течение всего срока службы Системы комплект ЗИП должен пополняться в соответствии с условиями договора на сервисное обслуживание.

Требования к защите информации от несанкционированного доступа. Защита информации и вычислительного процесса является исключительно важным элементом сохранения работоспособности Системы. Система должна автоматически вести Журнал учета пользователей, записи которого должны содержать полную информацию о работе и действиях пользователей Системы. Эти данные должны быть защищены от возможного вмешательства и изменения после их регистрации. Функция защиты информации и межсетевые интерфейсы должны обеспечить контроль и управление доступом к системе. Эти функции должны быть включены в набор системных средств управления и контроля, включая функции обеспечения межсетевого взаимодействия.

Возможности по обеспечению защиты информации в Системе должны включать, как минимум, следующее:

- Должна использоваться концепция работы с Системой только зарегистрированных пользователей, исключающая возможность несанкционированного доступа;
- Каждый пользователь (оператор или прикладная программа с использованием межсетевого интерфейса) получает доступ в Систему только с использованием пароля.

Для индивидуальных пользователей должны быть установлены различные уровни доступа, контролируемые Системой.

Каждый пользователь должен иметь собственный набор разрешенных действий для просмотра или изменения данных и информационно-управляющих функций.

К ним относятся, в частности, следующие виды защиты и ограничений доступа к данным и функциям Системы:

- Обеспечение защиты информации в процессе работы;
- Ограничение доступа для технолога-оператора;
- Ограничение возможностей изменения или модификации данных технологом-оператором;
- Ограничение доступа к выполнению инженерных функций;
- Ограничения на добавление, удаление, изменение, модификацию данных;
- Протоколирование событий с начала и до завершения работы технолога-оператора с Системой, и их распечатка независимо от успешности выполнения этих операций.

Требования по сохранности информации при авариях. Временный отказ технических средств или потеря электропитания не должны приводить к разрушению накопленной или усредненной во времени информации, и к потере текущих выходов на регулирующие органы.

Требования к средствам защиты от внешних воздействий. Технические средства Системы должны быть устойчивы к воздействиям температуры и влажности окружающего воздуха по группе В1 ГОСТ 12977-84 "*Изделия ГСП. Общие технические условия", таблица 1 "Температура и влажность окружающей среды. Места размещения при эксплуатации*и к воздействию механических факторов по группе L2 ГОСТ 12977-84, *таблица 3 "Места размещения, защищенные от существенных вибраций'*\ а для вычислительной техники - по группе 3 ГОСТ 21552-84 *"Средства вычислительной техники. Общие технические требования, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение".*

Группа 3 ГОСТ 21552-84 ограничивает изменение климатических условий следующим диапазоном:

- Температура окружающего воздуха от +5 до +40 °С;
- Относительная влажность окружающего воздуха от 40 до 90% при температуре +30 °С;

- Атмосферное давление от 84 до 107 кПа (680 - 800 мм. рт. ст.).

Для устройств связи с объектом, располагаемых непосредственно у технологических аппаратов, должны быть обеспечены условия взрывопожаробезопасности.

Должна предусматриваться защита технических средств от внешних электрических и магнитных полей, а также помех по цепям питания. Для этих целей в Системе должны применяться специальные аппаратные и схемные решения:

- Гальваническая развязка технических средств от технологического оборудования;
- Информация от двухпозиционных датчиков должна проходить через узлы защиты от "дребезга" контактов и узлы защиты от перенапряжений;
- Применение экранированных пар для передачи электрических сигналов;
- Фильтрация помех по цепям питания;
- Гальваническая развязка между территориально - распределёнными техническими средствами;
- Применение микропроцессорной элементной базы с повышенной помехозащищенностью.

Требования к патентной чистоте. Разрабатываемая Система не предназначается на экспорт, поэтому ограничения по патентной чистоте не накладываются. Однако Заказчику необходимо помнить, что в настоящее время авторские права фирм-изготовителей оборудования и разработчиков программного обеспечения охраняются не только международным, но и Российским законодательством, поэтому и оборудование, и программное обеспечение Системы как целиком, так и в какой-либо её части, может применяться только для целевого использования, определенного Договорами с Генподрядчиком, Поставщиком оборудования или Разработчиком Системы, и не может быть передано третьей стороне без письменного разрешения Генподрядчика, Поставщика оборудования или Разработчика программного обеспечения.

Требования к стандартизации и унификации. Разрабатываемая Система должна быть универсальной, обеспечивать возможность её использования на широком классе объектов управления и соответствовать достигнутому мировому уров-

ню в области создания АСУТП по функциональному развитию, удобству эксплуатации и обслуживания.

Ввиду полного *служебного* несоответствия отечественного ГОСТ 21.404-85 "Обозначения условные приборов и средств автоматизации в схемах" современным требованиям, при кодировке позиций КИПиА, а также при разработке функциональных схем автоматизации и соответствующих им мнемосхем следует придерживаться общепризнанных зарубежных стандартов, прежде всего - ANSI/ISA-S5.1-1984 '*Instrumentation Symbols and Identification".*

7.6. Требования к функциям, реализуемым Системой

Перечень задач РСУ **и требования к качеству их выполнения.** В соответствии с ГОСТ 24.104-85 ЕСС АСУ "Автоматизированные системы управления. Общие требования" РСУ должна обеспечивать:

1. Автоматизированный сбор и первичную обработку технологической информации;
2. Автоматический контроль состояния технологического процесса, предупредительную сигнализацию при выходе технологических показателей за установленные границы;
3. Управление технологическим процессом в реальном масштабе времени;
4. Представление информации в удобном для восприятия и анализа виде на цветных графических операторских станциях в виде графиков, мнемосхем, гистограмм, таблиц и т.п.
5. Автоматическую обработку, регистрацию и хранение поступающей производственной информации, вычисление усредненных, интегральных и удельных показателей;
6. Автоматическое формирование отчетов и рабочих (режимных) листов по утвержденной форме за определённый период времени, и вывод их на печать по расписанию и по требованию;
7. Получение информации от системы противоаварийной защиты, сигнализацию и регистрацию срабатывания системы ПАЗ;

8. Контроль над работоспособным состоянием средств РСУ и ПАЗ, включая входные и выходные цепи полевого оборудования;
9. Подготовку исходных данных для расчета материальных и энергетических балансов по производству, расчетов расходных норм по сырью, реагентам, энергетике;
10. Автоматизированную передачу данных в общезаводскую сеть и единую ("корпоративную") сеть предприятия;
11. Защиту баз данных и программного обеспечения от несанкционированного доступа;
12. Диагностику и выдачу сообщений по отказам всех элементов комплекса технических средств с точностью до модуля.

Сбор и первичная обработка информации включает в себя опрос аналоговых и дискретных датчиков, ввод инициативных сигналов изменения состояния оборудования, числоимпульсных сигналов интегрирующих счетчиков, масштабирование и перевод в действительные значения в соответствии с градуировочными характеристиками аналоговых измерительных элементов, фильтрацию сигналов от высокочастотных помех и выбросов.

Период опроса аналоговых датчиков должен подбираться индивидуально, а для особо важных переменных - **быть в пределах одной секунды.**

Регулирование и программно-логическое управление должны включать в себя проверку входного сигнала на достоверность, формирование управляющего воздействия, и выдачу управляющего воздействия на исполнительный механизм с частотой до одного раза в секунду.

Для функции управления должна быть обеспечена реализация основных законов регулирования *(ПИД, Соотношение, Упреждение и т.д.).* В каждом контуре должна быть предусмотрена возможность дистанционного ("ручного") управления со станций технолога-оператора, а также безударный переход с режима ручного управления на автоматическое управление, и наоборот.

Для оперативного персонала, имеющего соответствующие права доступа, должна быть предусмотрена возможность

настройки параметров Системы управления со станций технолога-оператора.

Отказ любого элемента технических средств РСУ не должен приводить к изменению положения или состояния исполнительных механизмов.

Функции отображения информации должны по запросу оператора обеспечить вывод на экран рабочей станции оперативной информации о текущем состоянии технологического процесса и оборудования, представляемой в виде мнемосхем, графиков, гистограмм и таблиц. Время реакции Системы на вызов нового изображения **- не более чем 2.5 секунды.** Оперативная информация с процесса на каждом вызванном изображении должна обновляться с частотой **до 1** раза **в секунду.**

Погрешности преобразования при вводе сигналов и пересчете введенных кодов в действительные значения не должны превышать 0,1% диапазона шкалы датчиков.

Для обеспечения связи технолога-оператора с процессом и Системой должны быть предусмотрены два типа запросов: прямой и последовательный, реализуемый с помощью перелистывания.

Тип представления информации в каждом фрагменте изображения (мнемосхема, график, таблица) определяется непосредственно, т.е. путем однократного нажатия на соответствующую кнопку на функциональной клавиатуре, а также по выбору из меню.

Все действия оператора по взаимодействию с Системой должны быть защищены от возможных ошибок. Система должна исполнять только те действия, которые описаны в документации на Систему. Любые случайные или ошибочные действия персонала по управлению процессом должны игнорироваться, если они отличаются от объявленных в документации, или не соответствуют уровню полномочий персонала для исполнения действий. В любом случае все действия персонала должны диагностироваться и архивироваться.

Для ретроспективного анализа хода процесса должно быть предусмотрено архивирование данных. Для дискретных параметров должно регистрироваться точное время изменения сигнала.

Автоматический контроль состояния технологического процесса должен подразумевать проверку нарушений преду-

предительных и предаварийных значений технологических переменных. На станциях технолога-оператора должна быть предусмотрена сигнализация нарушений, выражаемая звуком и изменением цвета.

Подготовка исходных данных для расчётов включает в себя определение средних значений переменных, а также вычисление нарастающих итогов и суммарных значений за определённые интервалы времени. Процедуры расчета накопленных значений должны быть устойчивы к отсутствию данных при выходе из строя датчиков или оборудования вычислительного комплекса.

Расчёт технологических и технико-экономических показателей (ТЭП), предусматривающий определение комплексных показателей, характеризующих эффективность технологического процесса, а также расчёты материальных балансов, фактических расходных показателей, общих и удельных материальных и энергетических затрат *{расходных норм),* технологической себестоимости целевых продуктов и отклонений фактических ТЭП от плановых должны реализовываться на средствах заводской ЛВС.

АСУТП должна обеспечивать подготовку всех необходимых данных и их последующую передачу в заводскую ЛВС по запросу или по расписанию.

Для всех фоновых расчётных задач должна быть обеспечена возможность повторного запуска без разрушения информации базы данных и изменения даты и времени последнего расчёта, выполненного в соответствии с периодичностью их запуска. Средства автоматизированного составления документов должны предусматривать возможность генерации и модификации отчетов без перепрограммирования. На станциях технолога-оператора должны печататься следующие виды отчетов:

- Рабочий (режимный) лист технолога-оператора (1 раз в смену);
- Рапорт нарушений предупредительных и предаварийных границ, а также действий оперативного персонала (1 раз в смену или по требованию);
- Архивная информация выбранных параметров в виде таблиц или графиков за выбранное время (по требованию).

Все документы должны печататься **в утвержденной форме,** и должны сопровождаться календарной датой и временем, которые соответствуют периоду печати.

Доступ к информации со стороны рабочих станций Системы ориентирован на использование технологическим персоналом, и поэтому должен обеспечивать представление различных категорий оперативных данных, а также ввод данных в Систему наиболее простым и естественным способом.

Аппаратура и программная поддержка должны обеспечивать начальную загрузку, высокоскоростной обмен данными между отдельными элементами Системы, и управление выполнением задач на удалённых устройствах. Скорость обмена данными между различными узлами Системы должна быть достаточной для выполнения требований, предъявляемых к функциям Системы.

Сопровождение информационного и программного обеспечения выполняется с помощью программных средств, ориентированных на обслуживающий персонал АСУТП. Средства разработки должны обеспечивать возможность создания и конфигурирования информационно-управляющих функций Системы, редактирования, визуализации и **самодокументирования.**

Перечень задач системы ПАЗ и требования к качеству их выполнения.

Система ПАЗ должна обеспечивать:

1. Автоматизированный сбор аналоговой и дискретной информации от датчиков технологических параметров и параметров состояния исполнительных механизмов, а также дискретных параметров ДВК, ПДК, состояния аварийной вентиляции;
2. Выделение достоверной входной информации;
3. Анализ и логическую обработку входной информации;
4. Автоматическую выдачу сигналов двухпозиционного управления на исполнительные механизмы;
5. Дистанционное ("ручное") управление исполнительными механизмами при условии санкционированного доступа;
6. Определение первопричины срабатывания системы защиты и останова технологического процесса;

7. Передачу оперативной информации от системы ПАЗ в РСУ для сигнализации, регистрации и архивирования (отклонения параметров, срабатывание исполнительных механизмов ПАЗ, реакция на действия персонала и т.п.);
8. Оперативную и автономную диагностику технических средств системы ПАЗ, и идентификацию неисправностей с точностью до модуля (блока).

7.7. Требования к видам обеспечения

Требования к Информационному обеспечению. Информационное обеспечение АСУТП включает в себя следующие категории данных:

- Текущие значения технологических переменных, поступающих в систему в результате опроса датчиков и первичной переработки информации;
- Усреднённые или сглаженные за определенные периоды времени значения переменных;
- Границы переменных различных уровней, настройки алгоритмов управления, информация привязки программного обеспечения к конкретному объекту;
- Тексты программ и загрузочные модули.

Для обмена информацией в рамках распределённой Системы должна быть создана база данных, обеспечивающая доступ к данным с локальных элементов сети, которыми являются:

- Периферийные микропроцессорные устройства - подсистемы управления или контроллеры;
- Многофункциональные операторские станции - рабочие места технологического персонала;
- Инженерная станция.

Для удобства работы технологов-операторов с большими объемами разнообразной информации, и для выработки соответствующих стереотипов взаимодействия с Системой, Информационное обеспечение Системы должно быть структурировано, и иметь иерархическую организацию.

Должны быть предусмотрены следующие стандартные операционные панели (*видеоизображения, кадры, окна):*

1. **Панели общего обзора**
   Предназначены для контроля над работой всего производства в целом и для получения доступа к более подробным панелям при возникновении такой необходимости.
2. **Мнемосхемы**
   Относятся к наиболее важным типам операционных панелей. Представляют собой графическое изображение основного технологического оборудования, средств КИПиА, и отображают структуру алгоритмов управления и защиты, и их состояние.
3. **Панели группы приборов**
   Представляют и описывают состояние лицевых панелей 8 - 1 2 приборов.
4. **Панели настройки**
   Описывают параметры конкретного устройства / прибора / регулятора и предоставляют возможность его настройки.
5. **Панели сигналов тревоги**
   Отражают в хронологическом порядке предупредительную и предаварийную сигнализацию процесса.
6. **Панели регистрации хода процесса (тренды)**
   Должны быть предусмотрены 2 вида панелей для графического отображения данных о ходе процесса во времени:
   - Панель группы из 6 - 12 трендов,
   - Панель одиночного тренда.

Технологу-оператору должны быть представлены простые и естественные способы вызова и ввода данных для различных панелей, как то:

- Кнопка на функциональной клавиатуре;
- Указание элемента на экране;
- Выбор из меню;
- Ввод данных через соответствующую зону на экране.

Информационное обеспечение системы ПАЗ состоит из следующих категорий данных:

- Текущие значения входных аналоговых параметров;
- Текущие значения входных дискретных параметров;
- Программы логической обработки событий;

- Дискретные управляющие параметры;
- Параметры связи и взаимообмена с РСУ.

Все категории данных информационного обеспечения системы ПАЗ не должны теряться при авариях электропитания и отказе блоков и модулей системы ПАЗ.

Все настроечные константы, информация привязки, алгоритмы решения задач и тексты программ должны храниться на дублирующих носителях и обновляться при внесении изменений в Систему.

Требования к Лингвистическому обеспечению. Для реализации функций АСУТП должны использоваться современные средства конфигурирования и визуального программирования, ориентированные на специалистов-разработчиков АСУТП.

Эти средства позволяют существенно минимизировать время разработки, и придают исключительную наглядность алгоритмам переработки информации и управления.

Ввиду отсутствия отечественных нормативных документов, в качестве их прототипа необходимо использовать разработанный Международной Электротехнической Комиссией (МЭК) стандарт **IEC 61131-3,** регламентирующий полноту и синтаксис языков технологического программирования.

В соответствии с этим стандартом Система должна иметь, как минимум, следующие средства технологического программирования:

1. *Function Block Diagrams* - Графический язык функциональных блоков;
2. *Sequential Function Chart* - Функциональные схемы для описания последовательности операций.

Для разработки систем противоаварийной защиты дополнительно предусматривается:

3. *Ladder Logic Diagrams* - Графические средства описания логических схем.

Для разработки прикладных программ, в частности, технологических и технико-экономических расчётов, должен быть предусмотрен

4. Проблемно-ориентированный язык высокого уровня, позволяющий:
   - Создавать новые задачи,
   - Оперативно их корректировать,

- Сохранять результаты решения задач в базе данных,
- Организовывать запуск задач по запросу и по времени
  с соответствующими приоритетами.

Непременное условие:

Вся представленная на экранах мониторов и в печатных отчетах смысловая и текстовая информация для технологического и эксплуатационного персонала, как то:

- Описатели технологических переменных,
- Сообщения и инструкции оператору,
- Диалоги,
- Названия полей в меню и т.д., -

должна быть на русском языке.

Исключением, по взаимному согласию между Поставщиком, Разработчиком и Заказчиком могут быть шифры КИПовских позиций (так называемые тэги), коды ошибок, служебные сообщения.

Требования к **стандартному** Программному **обеспечению.** Для реализации задач распределённой Системы должно использоваться специализированное программное обеспечение, функционирующее в среде многозадачной операционной системы реального времени.

Характеристики программного обеспечения должны удовлетворять требованиям по выполнению функций, указанных в предыдущих разделах.

Сетевые программные средства, обеспечивающие объединение подсистем управления, операторских станций и средств архивирования данных в единую Систему, должны реализовывать загрузку и управление запуском задач, обеспечивать обмен между задачами и базами данных, и предоставлять доступ к периферийным устройствам.

Система управления должна иметь возможность оперативного конфигурирования прикладного программного обеспечения в процессе функционирования АСУТП.

Все ошибочные ситуации, возникающие при работе программ, должны диагностироваться, сопровождаться сообщениями, и не должны вызывать нарушений в работе Системы.

Требования к прикладному программному ("математическому") обеспечению. Математическое обеспечение Системы должно обеспечивать реализацию перечисленных в данном ТЗ функций, а также выполнение операций конфигурирования, программирования, управления базами данных и документирования.

Прикладное программное обеспечение АСУТП должно обеспечить реализацию требуемых алгоритмов контроля, регулирования и защиты, отображения информации, сигнализации и архивирования данных.

Алгоритмы управления должны иметь возможность переконфигурирования, и реализовываться через библиотечные блочные структуры.

Требования к Техническому обеспечению. Комплекс 1ехнических средств РСУ и системы ПАЗ должен быть достаточен для реализации определенных данным ТЗ функций, и строиться на базе следующих специализированных программно-технических комплексов:

- Средства КИПиА, в том числе датчики, исполнительные механизмы, электронные микропроцессорные регуляторы и поточные анализаторы качества;
- Периферийные микропроцессорные устройства - подсистемы управления, или контроллеры;
- Многофункциональные операторские и инженерные станции;
- Средства архивирования данных;
- Сетевое оборудование;
- Специализированные микропроцессорные контроллеры системы ПАЗ;
- Средства метрологической поверки оборудования.

Система измерений должна строиться на базе электронных датчиков расхода, давления, уровня, температуры, перепада давления, интегрирующих счетчиков, анализаторов качества и состава.

Средства измерений расходов, давлений, уровней и перепадов давлений должны иметь стандартные сигналы диапазона 4-20 мА.

Для реализации сбора и обработки информации в составе иодсистем управления должны быть предусмотрены модули:

- Ввода сигналов 4-20шА;

- Ввода сигналов 4-20шА со встроенными барьерами искрозащиты;
- Входа милливольтовых сигналов со встроенными барьерами искрозащиты;
- Ввода дискретных сигналов;
- Ввода по протоколу RS-422/RS-485 от периферийных микропроцессорных устройств.

Вывод управляющих воздействий, рассчитанных по законам регулирования, должен осуществляться через модули вывода аналоговых токовых сигналов на электропневмопозиционеры, установленные на пневматических исполнительных механизмах.

Вывод дискретных управляющих воздействий и блокировок для управления электрооборудованием выполняется через модули вывода дискретных сигналов.

Требования к Метрологическому обеспечению. Метрологическое обеспечение измерительных систем (ИС) должно удовлетворять требованиям Закона Российской федерации "Об обеспечении единства измерений", ГОСТов и Правил по метрологии.

Метрологическое обеспечение измерительных систем должны соответствовать ГОСТ Р 8.596-2002. ГСИ. "Метрологическое Обеспечение измерительных систем. Основные положения". Должны быть предоставлены следующие сведения и документы:

- Назначение ИС, и сведения об ее использовании в сфере (или вне сферы) Государственного метрологического контроля и надзора;
- Сертификат об утверждении типа ИС, описание типа ИС, методику поверки, - если они используются в сфере Государственного метрологического контроля и надзора;
- Сведения об измеряемых величинах и их характеристиках;
- Перечни измерительных каналов и нормы их погрешностей;
- Условия измерений;
- Условия метрологического обслуживания.

Средства измерения (СИ), входящие в систему контроля, управления и ПАЗ должны иметь сертификат об утверждении типа СИ, описание типа СИ, методику поверки.

В спецификацию оборудования АСУТП должны быть включены специальные технические и программные для калибровки измерительных каналов.

Значения контролируемых параметров (технологического процесса, технологического оборудования) должны быть выражены в соответствии с ГОСТ 8.417-2002 "ГСИ. Единицы величин".

Метрологическое Обслуживание РСУ и системы ПАЗ должно обеспечивать возможность как поэлементной (покомпонентной), так и комплектной поверки или калибровки измерительных каналов.

В номенклатуру контролируемых параметров входят расходы жидкостей, газов и пара, температура, давление, уровень, концентрация и т.д.

Для измерения хозучетных расходов методом переменного перепада давления, следует руководствоваться **ГОСТ 8.563-97 ГСИ "***Измерение расхода и количества жидкостей и газов методом переменного перепада давления*

Все методики измерения, используемые в сфере государственного метрологического контроля и надзора, должны быть аттестованы.

При поверке и калибровке каналов РСУ и ПАЗ должна быть предоставлена возможность доступа ко всем элементам Системы для подключения образцовых приборов (калибраторов).

Для измерительных каналов ИС должны быть представлены рекомендации (инструкции) по поверке (калибровке) ИК, утвержденные в установленном порядке.

Все метрологические характеристики измерительных и управляющих модулей должны быть представлены фирмой-изготовителем в документации на технические и программные средства. Пределы допускаемых значений погрешности измерительных каналов не должны превышать норм Технологического Регламента.

Значения диапазонов измерений и допускаемые приведенные погрешности должны быть определяющими при выборе оборудования и фирмы-поставщика.

Для подтверждения выбранных метрологических характеристик согласно **ГОСТ 8.009-84** "*Нормирование и использование метрологических характеристик средств измерений* испытания СИ и ИС должны проводиться по **ПР 50.2.009-94 ГСИ** "*Порядок проведения испытаний и утверждения типа средств измерений* ".

Измерительные каналы Системы должны комплектоваться техническими средствами измерения, прошедшими государственные приемочные испытания в порядке, установленном ПР 50.2.009-94.

Для технических средств, участвующих в процессе измерения контролируемых параметров должны быть обеспечены соответствующие условия эксплуатации (температура, влажность). Должен быть обеспечен контроль условий их эксплуатации в помещениях управления.

Измерительные каналы Системы могут использоваться для целей контроля параметров только после их калибровки на объекте эксплуатации. Калибровка измерительных каналов ИС проводится в соответствии с установленным на Предприятии порядком.

Требования к Организационному обеспечению. Организационное обеспечение АСУТП должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей по эксплуатации Системы.

Организационное обеспечение должно включать требования по численности и квалификации персонала АСУТП и КИПиА, инструкции по каждому виду деятельности, и точное определение выполняемых функций.

Инструкции Организационного обеспечения для технологического персонала должны определять его действия при эксплуатации АСУТП как в нормальном режиме, так **и** при отказах технических средств.

7.8. Состав и содержание работ по созданию АСУТП

Разработка АСУТП и ввод в действие осуществляются в соответствии с ГОСТ 34.601-90 *"Автоматизированные Системы. Стадии создания "*.

Стадии создания АСУТП, этапы и содержание работ по ним, а также организации-исполнители и сроки выполнения

указываются в Плане-графике работ с отражением нижеследующих этапов.

Первое техническое совещание. После заключения Договора на разработку ТРП проводится первое техническое (организационное) совещание с участием Заказчика, проектной организации, Разработчика системы и Поставщика оборудования для окончательного согласования и уточнения спецификаций и характеристик Системы.

На этом этапе согласовываются функции системы управления, включая контуры управления, контроля, сервисные функции системы, функции системы противоаварийной защиты, включая блокировки, сигнализацию, отчеты по событиям.

Согласовываются объемы работ, которые необходимо выполнить каждому из участников проекта создания АСУТП, сроки выполнения работ, определяются ответственные лица и способы взаимодействия.

Обработка исходных данных. Следующая документация, которая потребуется для выполнения проекта, должна быть предоставлена Разработчику на первом техническом совещании:

- Пояснительная записка технологической части проекта;
- Копия Технологического регламента;
- Монтажно-технологические схемы с КИПовской обвязкой;
- Перечень КИПовских позиций с указанием уровней входных и выходных сигналов, пределов сигнализации и блокировок;
- Инструкции по эксплуатации, пуску и останову технологического процесса;
- Описание алгоритмов управления и ПАЗ;
- Описание алгоритмов связного, последовательного и логического управления;
- Логические схемы управления и противоаварийной защиты;
- Принципиальные схемы управления силовым оборудованием;
- Схемы электроснабжения средств автоматизации и помещений управления;

- Документация строительной части помещений управления;
- Спецификация полевого оборудования;
- Схемы подключения внешних проводок от полевого оборудования до кроссовых шкафов в помещениях управления;
- Планы размещения существующего оборудования в помещениях управления.

Выполнение рабочего (технорабочего) проекта РСУ и ПАЗ. Разработчик должен выполнить Технорабочий проект на РСУ и ПАЗ, и представить Заказчику для согласования в сроки, определенные Договором на разработку проекта.

В технорабочем проекте должны быть представлены следующие виды документации:

- Документация по общесистемным решениям (ОР);
- Документация на техническое обеспечение (ТО);
- Документация на информационное обеспечение (ИО);
- Документация на прикладное ("математическое") программное обеспечение (МО);
- Документация на стандартное программное обеспечение (ПО);
- Документация организационного обеспечения (ОО).

Разработчик Системы должен решить вопросы рационального распределения входных и выходных сигналов по модулям ввода-вывода согласно технологическим узлам для удобства при монтаже и эксплуатации, а также для минимизации времени обработки контуров управления и ПАЗ.

Законное требование:

Если аппаратная часть Системы и стандартное программное обеспечение будут изготавливаться или разрабатываться за рубежом, Разработчик должен обеспечить Заказчика стандартной технической документацией и на английском, и на русском языке.

Обучение персонала Заказчика. Специалисты Заказчика должны пройти обучение в учебном центре Разработчика системы или Поставщика оборудования.

Конфигурация функций контроля и управления. Разработка, конфигурация, загрузка, тестирование и отладка функций контроля и управления, а также конфигурация РСУ и

ПАЗ в целом, выполняются Разработчиком системы. Прикладное программное обеспечение передается Заказчику на магнитных носителях на стадии сдачи рабочей документации.

Конфигурация функций предоставления информации. Весь объем работ по конфигурации функций предоставления информации выполняется Разработчиком, дополнительные затраты специалистов Заказчика не требуются.

Параллельно с конфигурацией Системы будут вестись курсы обучения специалистов Заказчика, причем практические занятия будут включать реальные конфигурационные задачи на реальной Системе.

В объем конфигурации функций отображения входят:

- Разработка и конфигурация изображений (мнемосхем) участков технологического процесса с КИПовской обвязкой и контурами управления;
- Конфигурация отображения параметров, находящихся в состоянии сигнализации или блокировок;
- Разработка и конфигурация трендов (графиков изменения параметров во времени);
- Конфигурация архивов и баз данных, технологических констант;
- Генерация и вывод технологических отчетов и режимных листов;
- Генерация и вывод системных отчетов, хронологических перечней технологических и системных событий.

Шефмонтаж и пусконаладка. Для непосредственного выполнения монтажных и наладочных работ привлекаются специализированные монтажно-наладочные организации.

Услуги по шефмонтажу и пуско-наладке РСУ и ПАЗ, производимые на площадке Заказчика, будут выполнены специалистами Разработчика и Поставщика оборудования.

С целью сокращения неоправданных простоев технологического оборудования во время наладочных работ, наладка может выполняться по-позиционно, по-аппаратно, или по технологическим узлам. В любом случае решение по наиболее приемлемому варианту зависит от Заказчика.

После наладки измерительные каналы подвергаются поверке или калибровке. Поверка или калибровка измерительных каналов ИС должны проводиться Государственной метрологической службой или метрологической службой пред-

приятия Заказчика в зависимости от назначения ИС, и сведений об ее использовании в сфере или вне сферы государственного метрологического контроля и надзора.

Пуск АСУТП в эксплуатацию. Каждый канал контроля, управления, сигнализации и блокировки отлаживается и настраивается в индивидуальном порядке в соответствии с Программой и методикой испытаний.

После завершения наладочных работ по всем контурам и сервисным функциям, вся Система целиком, включая управление и ПАЗ, в автоматическом режиме будет поставлена на испытательный **предгарантийный пробег** (Предварительные испытания), который заключается в беспрерывной и безотказной работе **в течение** 72-х **часов** в присутствии специалистов Разработчика и Заказчика.

После успешного завершения предварительных испытаний подписывается совместный Акт о сдаче АСУТП в Опытную эксплуатацию.

Гарантийный срок. Гарантийный срок должен составлять **не менее 12 месяцев** с момента пуска Системы в промышленную эксплуатацию, но не более **18 месяцев** со дня поставки оборудования на склад Заказчика в зависимости от того, что наступит ранее.

В течение гарантийного срока специалисты Разработчика по первому требованию Заказчика должны прибывать на площадку Заказчика для устранения неполадок и отказов, или для предоставления квалифицированных консультаций.

7.9. **Порядок контроля и приемки**

Ввод в действие разрабатываемой АСУТП осуществляется в соответствии с требованиями ГОСТ 34.601-90 ЕСС АСУ *"Автоматизированные системы. Стадии создания"* и ГОСТ 34.603-92 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. *"Виды испытаний автоматизированных систем"*.

Для автоматизированной системы устанавливаются следующие этапы испытаний:

- Предварительные испытания;
- Опытная эксплуатация;
- Приемочные испытания.

Программы всех этапов испытаний составляются Разработчиком на основании документа технорабочего проекта "Программа и методика испытаний (ПМ)^{П}, и утверждаются Заказчиком.

Программы испытаний должны предусматривать следующие виды проверок:

1. Проверка комплектности комплекса технических средств и стандартной технической документации;
2. Проверка состава и содержания документации технорабочего проекта;
3. Автономная проверка готовности комплекса технических средств;
4. Метрологическая поверка измерительных каналов;
5. Проверка отказоустойчивости и функций самодиагностики системы;
6. Проверка реализации функций АСУТП на соответствие требованиям Технического задания;
7. Проверка квалификации и уровня подготовки оперативного (технологического) и эксплуатационного (обслуживающего) персонала для работы в условиях функционирования АСУТП.

По результатам этапов испытаний оформляются отчетные документы. К отчетным документам относятся Протоколы и Отчеты о результатах испытаний. В приложения должны включаться перечни методик испытаний. Согласно РД 50-34.698-90, пункт 2.14.17, содержание разделов методик устанавливает Разработчик.

Отчетные документы подписываются членами комиссии (членами рабочих групп, сформированных из членов комиссии), и утверждаются председателем комиссии.

Предварительные испытания Системы проводятся для определения ее работоспособности и возможности приемки Системы в Опытную эксплуатацию. Предварительные испытания организует Заказчик, и проводит их совместно с Разработчиком.

Предварительные испытания могут быть:

- Автономные;
- Комплексные.

Результаты испытаний по различным этапам испытаний отражаются в Протоколах испытаний и соответствующих Отчетах.

В сводном Протоколе испытаний приводится заключение о возможности приемки системы в Опытную эксплуатацию, а также перечень необходимых доработок и сроки их выполнения. Работа завершается оформлением **Акта приемки в Опытную эксплуатацию.**

Опытная эксплуатация проводится в соответствии с Программой, в которой указываются:

1) Условия и порядок функционирования частей Системы, и Системы в целом;
2) Порядок устранения недостатков, выявленных в процессе Опытной эксплуатации;
3) Продолжительность Опытной эксплуатации, достаточную для проверки правильности функционирования Системы при выполнении каждой функции и готовности персонала к работе в условиях полноценного функционирования Системы.

Продолжительность Опытной эксплуатации - не менее двух месяцев. Во время Опытной эксплуатации Системы ведут Рабочий журнал, в который заносят:

1) Сведения о продолжительности функционирования Системы;
2) Сведения об отказах, сбоях, аварийных ситуациях;
3) Сведения об изменениях параметров объекта автоматизации;
4) Сведения о проведенных корректировках программного обеспечения и документации;
5) Сведения о наладке технических средств.

Сведения фиксируют в Журнале с указанием даты и ответственного лица. В Журнал могут быть внесены замечания персонала об удобстве эксплуатации Системы. По результатам Опытной эксплуатации составляют Акт о завершении работ по проверке Системы в режиме Опытной эксплуатации, с заключением о возможности предъявления Системы на Приемочные испытания.

Приемочные испытания должны включать проверку:

1) Полноты и качества реализации функций при регламентированных и предаварийных значениях параметров объекта автоматизации, и в других условиях функционирования АСУТП, указанных в Техническом задании;

2) Выполнения каждого требования, относящегося к интерфейсу Системы;
3) Работы персонала в диалоговом режиме;
4) Средств и методов восстановления работоспособности Системы после отказов;
5) Комплектности и качества эксплуатационной документации.

Приемочные испытания автоматизированной системы проводят в соответствии с Программой испытаний, в которой указывают:

1) Перечень объектов, выделенных в Системе для испытаний, и перечень требований, которым должны соответствовать объекты со ссылкой на конкретные пункты ТЗ;
2) Критерии приемки Системы и ее частей;
3) Условия и сроки проведения испытаний;
4) Средства для проведения испытаний;
5) Фамилии лиц, ответственных за проведение испытаний;
6) Методики испытаний и обработки результатов;
7) Перечень оформляемой документации (протоколы и отчеты).

Приёмочные испытания АСУТП проводят для определения соответствия Техническому заданию и документации проекта.

Приёмочную комиссию образуют приказом по предприятию. В состав комиссии входят представители Заказчика, Разработчика, и представители технадзора.

Согласно ГОСТ 34.603-92, Приёмочной комиссии должна быть предъявлена следующая документация:

1. Техническое задание на создание АСУТП;
2. Исполнительная документация по монтажу;
3. Протокол предварительных испытаний;
4. Программа испытаний;
5. Акт приёмки Системы в опытную эксплуатацию;
6. Рабочие журналы опытной эксплуатации Системы;
7. Акт о завершении работ по проверке Системы в режиме опытной эксплуатации;
8. Техническая и проектная документация на Систему.

Перед предъявлением Системы на приемочные испытания должна быть доработана техническая и проектная документация по замечаниям Протокола предварительных испытаний, и Акта о завершении работ по проверке Системы в режиме Опытной эксплуатации.

Согласно ГОСТ 34.603-92, пункт 4.10, протоколы отдельных проверок обобщаются в едином итоговом Протоколе, на основании которого делается заключение о возможности оформления Акта приемки АСУТП в постоянную (промышленную) эксплуатацию.

Допускается по решению Приемочной комиссии доработка технической документации Системы после ее ввода в действие. Сроки доработки указываются в Протоколе приемочных испытаний.

Результаты приемочных испытаний оформляются:

1. Итоговым Протоколом испытаний;
2. Актом о приемке АСУТП в промышленную эксплуатацию, и
3. Издается приказ "О вводе АСУТП в промышленную эксплуатацию".

7.10. Требования к составу и содержанию работ по подготовке объекта к вводу АСУТП в действие

Заказчик на стадии разработки и внедрения АСУТП должен обеспечить выполнение следующих мероприятий:

- Формирование подразделение обслуживания АСУТП;
- Приемку Технического проекта и Рабочей документации в соответствии с Техническим заданием и Планом-графиком работ по созданию АСУТП;
- Организацию работы по замене существующих средств КИПиА, а также работы по монтажу и пусконаладке средств КИПиА;
- Организацию строительно-монтажных работ по реконструкции помещений операторных и монтажу средств вычислительной техники;
- Обеспечение и организацию работ по поверке (калибровке) измерительных каналов;
- Организацию проведения комплексной наладки Системы;

- Организацию предварительных и приёмочных испытаний Системы;
- Обеспечение обслуживание Системы с момента её сдачи в Опытную эксплуатацию;
- Регистрацию сбоев и отказов оборудования КИПиА и вычислительной техники в рабочем журнале;
- Представление Разработчику необходимых данных на всех стадиях создания Системы, и нормальные условия работы.
- Организацию обучения технологического персонала и специалистов подразделения АСУТП объекта автоматизации.

Разработчик совместно с Заказчиком должен обеспечить выполнение следующих мероприятий:

- Наличие действующих лицензий на право проведения работ по проектированию и разработке АСУТП;
- Качественное исполнение документации Технического и Рабочего (технорабочего) проектов;
- Проведение обучения технологического персонала и специалистов подразделения АСУТП объекта автоматизации.
- Синхронное выполнение проектных работ со сроками поставки технических средств АСУТП, включая и полевое оборудование;
- Синхронное выполнение проектных работ с планом строительных работ, монтажа оборудования КИП и средств вычислительной техники;
- Проверку состояния технических средств АСУТП и качества поверки (калибровки) измерительных каналов;
- Проведение комплексной наладки Системы;
- Своевременное проведение предварительных и приёмочных испытаний Системы;
- Своевременный ввод Системы в промышленную эксплуатацию.

7.11. Требования к документированию

Требования к содержанию документов, разрабатываемых при создании автоматизированной системы, установлены указаниями РД 50-34.698-90 "*Автоматизированные системы. Требования к содержанию документов*", а также соответствующими государственными стандартами:

- Единой системы программной документации (ЕСПД);
- Единой системы конструкторской документации (ЕСКД);
- Системы проектной документации для строительства (СПДС);
- ГОСТ 34.602-89 "Техническое задание на создание автоматизированной системы".

Виды и комплектность документов регламентированы ГОСТ 34.201-89 *"Виды, комплектность и обозначение документов при создании автоматизированных систем*

Содержание документов является общим для всех видов автоматизированных систем и, при необходимости, может дополняться Разработчиком в зависимости от особенностей конкретно создаваемой Системы. Допускается включать в документы дополнительные разделы и сведения, объединять и исключать разделы.

В составе технорабочего проекта разрабатывается документация по общесистемным решениям, организационному, техническому, информационному и программному обеспечению, а также проектно-сметная документация. В состав эксплуатационной документации входит документация по информационному, программному, техническому и метрологическому обеспечению, а также проектно-сметная документация. В соответствии с ГОСТ 34.201-89, п. 1.3.1, табл. 2, виды документов, разрабатываемых на стадиях Технического проекта и Рабочей документации и имеющих отношение к проектно-сметным, выполняются Проектной организацией.

Вся рабочая документация, разработанная применительно к данному конкретному проекту, должна быть на русском языке. Стандартная техническая документация иностранных фирм должна быть представлена **и на английском, и на русском языках.**

Количество экземпляров проектной и эксплуатационной документации, предоставляемой Заказчику, определяется Договорами с Поставщиком оборудования и Разработчиком проекта, однако в любом случае должно быть НЕ МЕНЕЕ ЧЕТЫРЕХ. Перечень документации технорабочего проекта представлен в Приложении 6.

7.12. Источники разработки

Настоящее ТЗ разработано на основании следующих стандартов и нормативных документов:

1. Закон РФ №4871-1 "Об обеспечении единства измерений".
2. СТП 7.3-03-2008 СТАНДАРТ ПРЕДПРИЯТИЯ. Порядок разработки, внедрения, сопровождения и эксплуатации автоматизированных систем управления технологическими процессами.
3. ГОСТ 34.003-90 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Термины и определения.
4. ГОСТ 24.104-85 ЕСС АСУ. Автоматизированные системы управления. Общие требования.
5. ГОСТ 34.201-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды, комплектность и обозначение документов при создании автоматизированных систем.
6. ГОСТ 34.601-90 ЕСС АСУ. Автоматизированные системы. Стадии создания.
7. ГОСТ 34.602-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
8. РД 50-34.698-90 МЕТОДИЧЕСКИЕ УКАЗАНИЯ. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Требования к содержанию документов.
9. ГОСТ 21.404-85 Автоматизация технологических процессов. Обозначения условные приборов и средств автоматизации в схемах.
10. IEC 1131-3 : 1) Function Block Diagrams;
    2) Sequential Function Chart;
    3) Ladder Logic Diagrams.
11. ANSI / ISA-S5.1-1984 Instrumentation Symbols and Identification.

12. ГОСТ 34.603-92 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды испытаний автоматизированных систем.
13. ПБ 09-540-03 Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств.
14. ГОСТ 24.701-86 ЕСС АСУ. Надёжность автоматизированных систем управления. Основные положения.
15. ГОСТ 21552-84 СВТ. Общие технические требования, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение.
16. ПУЭ, Правила устройства электроустановок. 7-е издание.
17. ГОСТ 12.2.070-81 Правила техники безопасности электрических цепей.
18. ГОСТ 13109-97 Нормы качества электрической энергии в системах электроснабжения общего назначения.
19. ГОСТ 21128-84 Системы электроснабжения, сети, источники, преобразователи и приемники электрической энергии. Номинальные напряжения до ЮООв.
20. ГОСТ 12.1.030-81 ССБТ. Защитное заземление, зануление.
21. ГОСТ 25861-83 Машины вычислительные и системы обработки данных. Требования электрической и механической безопасности и методы испытаний.
22. ГОСТ 12.1.005-88 ССБТ Общие санитарно-гигиенические требования к воздуху рабочей зоны.
23. ГОСТ 12.0.003-74 ССБТ Опасные и вредные производственные факторы.
24. ГОСТ 12.1.003-83 ССБТ. Шум. Общие требования безопасности.
25. ГОСТ 21958-76 Общие эргономические требования к расположению рабочих мест.
26. ГОСТ 22269-76 Система "Человек-машина". Рабочее место оператора. Взаимное расположение элементов рабочего места. Общие эргономические требования.
27. СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронным вычислительным машинам и организации работы. Санитарно - эпидемиологические правила и нормативы.
28. ГОСТ 12977-84 Изделия ГСП. Общие технические условия.

29. СН 512-78 Инструкция по проектированию зданий и помещений для электронно-вычислительных машин.
30. ГОСТ Р 8.596-2002 ГСИ Метрологическое обеспечение измерительных систем. Основные положения.
31. МИ 2439-97 Метрологические характеристики измерительных систем. Номенклатура. Принципы регламентации, определения и контроля.
32. МИ 2441-97 Испытания для целей утверждения типа измерительных систем. Общие требования.
33. ПР 50.2.009-94 ГСИ. Порядок проведения испытаний и утверждения типа средств измерений.
34. ГОСТ 8.009-84 ГСИ. Нормируемые метрологические характеристики средств измерений.
35. ГОСТ 8.417-02 ГСИ. Единицы величин.
36. СНиП 3.05.07-85 Системы автоматизации.
37. ГОСТ 8.563-97 ГСИ. Измерение расхода и количества жидкостей и газов методом переменного перепада давления.

7.13. Приложения

Приложение 1:	Краткое описание технологического процесса.
Приложение 2:	Структурная схема технологического процесса.
Приложение 3:	Перечни входов-выходов.
Приложение 3-1:	Перечень входов-выходов РСУ.
Приложение 3-2:	Перечень входов-выходов ПАЗ.
Приложение 3-3:	Сводный перечень входов-выходов РСУ.
Приложение 3-4:	Сводный перечень входов-выходов ПАЗ.
Приложение 4:	Структурная схема АСУТП.
Приложение 5:	Предварительный план-график работ по созданию АСУТП.
Приложение 6:	Перечень документации технорабочего проекта.

7.14. Составлено:

Должность	Ф.И.О.	Подпись	Дата

От Заказчика:

От Разработчика:

7.15. Согласовано:

Должность	Ф.И.О.	Подпись	Дата

От Заказчика:

От Разработчика:

От Проектной организации:

Глава 8

ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ АСУТП

Глава условно разделена на две части.

В первой, основной части (разделы 8.1-8.14) приводится документ **"Программа и методика испытаний (ПМ)",** разработанный с максимально возможным учетом отечественной нормативной базы.

Во второй части (разделы 8.15-8.18), приводится образец Программы и методики испытаний **на площадке поставщика системы.** Данный вид испытаний никак не оговаривается отечественными нормативными документами. Однако значимость этого вида испытаний чрезвычайно высока: это означает, что заранее в договоре с поставщиком (разработчиком) системы предполагается, что система будет разрабатываться не на коленке заказчика, а вполне предсказуемым порядком.

Как таковой документ "Программа и методика испытаний (ПМ)" создается Разработчиком системы в составе документации рабочего (технорабочего) проекта. На основе проектной "Программы и методики испытаний" создается Программа предварительных, а по окончанию опытной эксплуатации - Программа приемочных испытаний системы. Эти Программы испытаний должны содержать Перечни и описания конкретных проверок, которые следует проводить по каждому пункту Перечня для подтверждения выполнения требований Технического задания, со ссылками на соответствующие разделы и пункты Технического задания.

Методики испытаний разрабатываются с использованием типовых методик испытаний. При этом отдельные положения типовых методик испытаний могут уточняться и конкретизироваться в разрабатываемых методиках в зависимости от кон-

кретных особенностей системы и условий проведения испытаний. Согласно РД 50-34.698-90, пункт 2.14.17, содержание разделов методик также устанавливает разработчик.

Документ проекта "Программа и методика испытаний (ПМ)" разумно начать с подтверждения целей Технического задания, ради достижения которых создается система.

8.1. Назначение, цели создания, и функции АСУТП

АСУТП предназначена для:

- Целевого применения как законченное изделие под определенный объект автоматизации;
- Стабилизации заданных режимов технологического процесса путем измерения значений технологических параметров, их обработки, визуального представления, и выдачи управляющих воздействий в режиме реального времени на исполнительные механизмы, как в автоматическом режиме, так и в результате действий технолога-оператора;
- Анализа состояния технологического процесса, выявление предаварийных ситуаций и предотвращение аварий путем переключения технологических узлов в безопасное состояние, как в автоматическом режиме, так и по инициативе оперативного персонала;
- Обеспечения административно-технического персонала завода необходимой информацией с технологического процесса для решения задач контроля, учета, анализа, планирования и управления производственной деятельностью.

Целями создания АСУТП являются:

- Обеспечение надежной и безаварийной работы производства;
- Стабилизация эксплуатационных показателей технологического оборудования и режимных параметров технологического процесса;
- Увеличение выхода товарной продукции;
- Уменьшение материальных и энергетических затрат;
- Снижение непроизводительных потерь человеческих, материально - технических и топливно-энергетических ресурсов, сокращение эксплуатационных расходов;

- Выбор рациональных технологических режимов с учетом показаний промышленных анализаторов, установленных на потоках, и оперативной корректировки стратегии управления по данным лабораторных анализов;
- Улучшение качественных показателей конечной продукции;
- Предотвращение аварийных ситуаций;
- Автоматическая и автоматизированная диагностика оборудования АСУТП.

Функции управления технологическим процессом реализуются посредством распределенной системы управления (РСУ). Функции противоаварийной защиты реализуются посредством специализированной системы противоаварийной защиты - системы ПАЗ.

Состав программно-технического комплекса.

В качестве программно-технического комплекса АСУТП используются специализированные средства управления и противоаварийной защиты, сертифицированные Госстандартом как средства измерения, и разрешенные Федеральной службой по экологическому, технологическому и атомному надзору (Ростехнадзор) для применения на взрывоопасных производствах.

Перечень документов, на основании которых создается Система. Система создается на основании следующих документов:

1. Техническое задание на создание АСУТП;
2. Договор YNF-1234/01 на поставку оборудования АСУТП;
3. Договор YNF-1234/02 на разработку Технорабочего проекта АСУТП;
4. Договор YNF-1234/03 на разработку и внедрение АСУТП ("инжиниринг").

Структура АСУТП. Структура АСУТП разделяется на следующие категории:

- Распределенная система управления (в дальнейшем РСУ), базирующаяся на специализированной микропроцессорной технике, предназначенная для управления технологическим процессом в режиме реального времени и предоставления информации в заводскую

ЛВС (директору завода, диспетчеру, главным специалистам завода).

- Система противоаварийной защиты (в дальнейшем ПАЗ), базирующаяся на специализированной микропроцессорной технике повышенной надежности, предназначенной для автоматического перевода технологического процесса в безопасное состояние при возникновении аварийных ситуаций.
- Периферийное оборудование - понятие, объединяющее датчики, анализаторы, преобразователи и исполнительные механизмы, а также электрические и другие приводы, установленные как непосредственно на технологическом оборудовании, так и в специальных помещениях, и подключенные к РСУ и ПАЗ.

Верхний уровень АСУТП представлен автоматизированными рабочими местами оператора-технолога. На верхнем уровне реализуются следующие функции:

- Визуализация состояния технологических объектов управления в реальном масштабе времени;
- Задание требуемых режимов технологического процесса и ввод данных;
- Сигнализация отклонений технологического процесса от регламентных значений;
- Визуализация данных об истории процесса;
- Печать сообщений о нарушениях и технологических режимов;
- Регистрация в базе данных предыстории значений технологических переменных во времени;
- Регистрация в базе данных сообщений о системных и технологических нарушениях;
- Регистрация в базе данных действий оперативного персонала;
- Формирование и печать отчетных документов.

Требования к функциям АСУТП.

РСУ должна обеспечивать:

1. Автоматизированный сбор и первичную обработку технологической информации.
2. Автоматический контроль состояния технологического процесса, предупредительную и предаварийную

сигнализацию при выходе технологических параметров за установленные границы.

3. Управление технологическим процессом в реальном масштабе времени.
4. Представление информации в удобном для восприятия и анализа виде на операторских станциях в виде графиков, мнемосхем, гистограмм, таблиц.
5. Автоматическую обработку, регистрацию и хранение поступающей производственной информации, вычисление усредненных и интегральных показателей.
6. Автоматическое формирование отчетов и рабочих (режимных) листов по утвержденной форме за определённый период времени, и вывод их на печать по расписанию и по требованию.
7. Получение информации от системы ПАЗ и регистрацию срабатывания системы ПАЗ.
8. Контроль над работоспособным состоянием технических средств РСУ и ПАЗ.
9. Автоматизированную передачу данных в общезаводскую сеть.
10. Защиту баз данных и программного обеспечения от несанкционированного доступа.
11. Диагностику и выдачу сообщений по отказам всех элементов комплекса технических средств с точностью до модуля.

Система ПАЗ должна обеспечивать:

1. Автоматизированный сбор аналоговой и дискретной информации от датчиков технологических параметров и параметров состояния исполнительных механизмов, а также дискретных параметров ДВК, ПДК, состояния аварийной вентиляции.
2. Выделение достоверной входной информации.
3. Анализ и логическую обработку входной информации.
4. Автоматическую выдачу сигналов двухпозиционного управления на исполнительные механизмы.
5. Дистанционное ("ручное") управление исполнительными механизмами при условии санкционированного доступа.
6. Определение первопричины срабатывания системы защиты и останова технологического процесса.

7. Передачу оперативной информации от системы ПАЗ в РСУ для сигнализации, регистрации и архивирования (отклонения параметров, срабатывание исполнительных механизмов ПАЗ, реакция на действия персонала и т.п.).
8. Оперативную и автономную диагностику технических средств системы ПАЗ, и идентификацию неисправностей с точностью до модуля (блока).

8.2. Объект испытаний

Объектом испытаний является комплекс технических и программных средств АСУТП конкретного производства (указать, какого).

8.3. Цель испытаний

Цель испытаний состоит в следующем:

- Проверка соответствия состава, функций и эксплуатационных характеристик АСУТП Техническому заданию, проектной и эксплуатационной документации;
- Проверка функционирования программно - технического комплекса АСУТП в реальных условиях эксплуатации на действующем технологическом объекте;
- Проверка квалификации и готовности оперативного и эксплуатационного персонала к работе и обслуживанию АСУТП;
- Приемка АСУТП в опытную (затем, по окончанию опытной - промышленную) эксплуатацию.

8.4. Объем испытаний

Программа испытаний должна предусматривать Перечень и описание проверок, которые необходимо провести для принятия обоснованного решения о готовности системы:

1. Проверка спецификации комплекса технических средств и стандартной технической документации;
2. Проверка состава и содержания документации техно-рабочего проекта;

3. Автономная проверка готовности комплекса технических средств;
4. Метрологическая поверка измерительных каналов;
5. Проверка отказоустойчивости и функций самодиагностики системы;
6. Проверка реализации функций АСУТП на соответствие требованиям Технического задания;
7. Проверка квалификации и уровня подготовки оперативного (технологического) и эксплуатационного (обслуживающего) персонала для работы в условиях функционирования АСУТП.

8.5. Условия и порядок проведения испытаний

Подготовка и организация испытаний осуществляется Приемочной комиссией, образованной приказом по предприятию в составе:

- Представители Заказчика;
- Представители Разработчика АСУТП,
- Представители Поставщика оборудования;
- Представители Проектной организации;
- Представители монтажных и пуско-наладочных организаций;
- Представители органов технадзора.

Испытания АСУТП проводятся для определения соответствия Техническому заданию и проектной документации. Приёмочной комиссии представляется следующая документация:

- Техническое задание на создание АСУТП;
- Исполнительная документация по монтажу;
- Протокол предварительных испытаний;
- Программа испытаний Системы;
- Акты метрологической аттестации измерительных каналов;
- Техническая и проектная документация на Систему;
- Собственно физический комплекс программно-технических средств АСУТП вместе с подготовленным и обученным оперативным и эксплуатационным персоналом.

Кроме того, по окончанию опытной эксплуатации предъявляются:

- Акт приёмки Системы в опытную эксплуатацию;
- Рабочие журналы Опытной эксплуатации Системы;
- Акт о завершении работ по проверке Системы в режиме Опытной эксплуатации.

Перед проведением испытаний все участники должны быть ознакомлены с Программой испытаний, порядком проведения и оформления результатов испытаний.

Приемочные испытания должны проводиться на действующем технологическом объекте.

Для предупреждения несчастных случаев и электрических повреждений технических средств при монтаже, включении, тестировании, проверке, эксплуатации, регламентных работах необходимо обеспечить выполнение следующих условий:

- Работы производить только при наличии технической документации, и в соответствии с технической документацией;
- При выполнении монтажных работ подсоединять и отсоединять компоненты, модули, блоки и другие составные части системы разрешается только при отключенном электропитании;
- Для проверки требований ТЗ по оперативному резервированию и самодиагностике во время испытаний системы разрешается производить операции отключения, переключения и замены модулей при включенном электропитании;
- Запрещается производить любые монтажные и ремонтные работы в процессе испытаний;
- Используемые в процессе испытаний образцовые средства измерений должны быть поверены;
- Применяемый в процессе настройки и эксплуатации инструмент должен соответствовать требованиям электробезопасности.

Члены комиссии и рабочих групп, эксплуатационный и технический персонал, принимающие участие в испытаниях, должны быть проинструктированы о порядке действий в случае возникновения аварийной ситуации на объекте.

8.6. Материально-техническое обеспечение испытаний

Проект Программы испытаний разрабатывается Разработчиком АСУТП на основе проектной "Программы и методики испытаний (ПМ)". После согласования с техническими специалистами Заказчика Программа испытаний утверждается Техническим директором организации-разработчика и Главным инженером предприятия Заказчика. Ответственность за полноту и порядок проведения испытаний несет Разработчик АСУТП. Заказчик на время проведения испытаний должен обеспечить организацию испытаний и условия для работы комиссии, удовлетворяющие требованиям безопасности, предоставить необходимое сервисное оборудование и инструмент.

Во время проведения предварительных испытаний и до передачи системы в опытную эксплуатацию техническое обслуживание программно-технического комплекса обеспечивается Разработчиком системы и Поставщиком оборудования по принадлежности, и при участии Заказчика.

8.7. Метрологическое обеспечение испытаний

Измерительные каналы подвергаются поверке или калибровке после наладки. Поверка или калибровка измерительных каналов измерительных систем (ИС) должны проводиться государственной метрологической службой, или метрологической службой предприятия Заказчика в зависимости от назначения ИС, и сведения об ее использовании в сфере или вне сферы государственного метрологического контроля и надзора.

Метрологическое обеспечение измерительных систем должно соответствовать ГОСТ Р 8.596-2002 "*Метрологическое обеспечение измерительных систем. Основные положения*

В технической документации на Систему должны быть представлены следующие сведения и документы:

- Назначение ИС, и сведения об ее использовании в сфере (или вне сферы) государственного метрологического контроля и надзора;
- Сертификат об утверждении типа ИС, описание типа ИС, методика поверки, - если они используются в

сфере Государственного метрологического контроля и надзора;
- Сведения об измеряемых величинах и их характеристиках;
- Перечни измерительных каналов и нормы их погрешностей;
- Условия измерений;
- Условия метрологического обслуживания.

Согласно Техническому заданию, в спецификацию оборудования АСУТП должны быть включены специальные технические и программные средства для калибровки измерительных каналов.

Значения контролируемых параметров технологического процесса и технологического оборудования должны быть выражены в соответствии с ГОСТ 8.417-2002 ГСИ. "*Единицы величин*".

Метрологическое обслуживание РСУ и системы ПАЗ должно обеспечивать возможность как поэлементной (покомпонентной), так и комплектной поверки или калибровки измерительных каналов. В номенклатуру контролируемых параметров входят расходы жидкостей, газов и пара, температура, давление, уровень, концентрация и т.д. Для измерения хозучетных расходов методом переменного перепада давления, следует руководствоваться ГОСТ 8.563-97 ГСИ "*Измерение расхода и количества жидкостей и газов методом переменного перепада давления*".

Все методики измерения, используемые в сфере государственного метрологического контроля и надзора, должны быть аттестованы.

При поверке и калибровке каналов РСУ и ПАЗ должна быть предоставлена возможность доступа ко всем элементам Системы для подключения образцовых приборов (калибраторов).

Для измерительных каналов ИС должны быть представлены инструкции по поверке (калибровке), утвержденные в установленном порядке. Все метрологические характеристики измерительных и управляющих модулей должны быть представлены фирмой-изготовителем в документации на технические и программные средства. Пределы допускаемых значений погрешности измерительных каналов не должны превышать норм технологического регламента.

Для подтверждения выбранных метрологических характеристик согласно ГОСТ 8.009-84 "*Нормирование и использование метрологических характеристик средств измерений* испытания СИ и ИС должны проводиться по ПР 50.2.009-94 ГСИ "*Порядок проведения испытаний и утверждения типа средств измерений*Измерительные каналы Системы должны комплектоваться техническими средствами измерения, прошедшими государственные приемочные испытания в порядке, установленном ПР 50.2.009-94.

8.8. Оформление результатов испытаний

По результатам каждого этапа испытаний оформляются отчетные документы. К отчетным документам относятся Протоколы и Отчеты о результатах проверок. В приложения к отчетным документам включается перечень ссылок на стандартные методики, или описание конкретных методик испытаний. Отчетные документы подписываются членами комиссии (членами рабочих групп), и утверждаются Председателем комиссии. Протоколы испытаний по всем пунктам Перечня проверок Программы испытаний обобщаются **в едином итоговом Протоколе,** на основании которого делается заключение о возможности или невозможности оформления Акта приемки АСУТП в опытную (промышленную) эксплуатацию.

Допускается по решению Приемочной комиссии доработка технической документации после ввода Системы в действие. Сроки доработки указываются в итоговом Протоколе испытаний.

8.9. Процедура (методика) испытаний

1. Проверка спецификации комплекса технических средств и стандартной технической документации.

Изначальная Спецификация оборудования приводится в Приложении к Договору на поставку оборудования. Окончательно согласованный состав комплекса технических средств АСУТП приводится в документе проекта "Спецификация оборудования (В4)". Проверка состава и комплектности Системы, состава ЗИП и контрольно-диагностического оборудования осуществляется путем сравнения фактически смонтированного оборудования КТС со Спецификацией, технической и про-

ектной документацией. Важнейшее требование, соблюдение которого должно быть непременным условием при заключении контрактов с западными фирмами и их посредниками:

Стандартная техническая документация изготовителя оборудования должна быть представлена и на английском, и на русском языке.

Количество экземпляров документации, предоставляемой Заказчику, определяется Договорами с Поставщиком оборудования и Разработчиком проекта, однако в любом случае должно быть НЕ МЕНЕЕ ТРЕХ.

2. Проверка состава и содержания документации технорабочего проекта.

Состав документации технорабочего проекта на АСУТП приведен в документах:

- Контрактный перечень приведен в Приложении к Договору на разработку технорабочего проекта;
- Окончательно согласованный перечень приведен в документе "Ведомость (состав) проекта (ТП)".

Проверка проводится с целью определения соответствия и качества документации для осуществления эксплуатации и технического обслуживания КТС и АСУТП в целом. И так же, как и для стандартной технической документации изготовителя, важнейшим требованием, которое должно быть выставлено еще перед подписанием каких-либо контрактов с иностранными поставщиками и разработчиками проектной документации, является **Представление проектной документации на русском языке.**

3. Автономная проверка готовности комплекса технических средств.

Проверка выполнения требований готовности АСУТП к опытной (промышленной) эксплуатации включает:

1) Проверку правильности и качества проектного монтажа и внутренних соединений РСУ и ПАЗ;
2) Проверку правильности проектного монтажа и подключения полевого оборудования к кроссовым шкафам;
3) Проверку проектного электроснабжения КТС;
4) Проверку проектного контура заземления КТС.

Проверка осуществляется на основании проектной и эксплуатационной документации на Систему:

- Планы расположения оборудования и проводок в ЦПУ **(С8);**
- Чертеж общего вида системных шкафов и установки технических средств (ВО);
- Таблица внутрисистемных соединений и подключений **(С6.1);**
- Таблица соединений кросс-система (С6.2);
- Схемы питания и заземления (С 10);
- Схемы электрические принципиальные контуров измерения, регулирования, сигнализации и блокировок **(СБ).**

3.1. Проверка правильности и качества проектного монтажа и внутренних соединений РСУ и ПАЗ осуществляется на основании соответствующих Актов выполнения монтажных работ, и сравнения выполненного монтажа с проектной "Таблицей внутрисистемных соединений и подключений".

3.2. Проверка правильности проектного монтажа и подключения полевого оборудования к кроссовым шкафам АСУТП.

Производится на основании Акта выполнения монтажа и наладки КИПиА, и сравнения с проектной документацией.

3.3. Проверка проектного электроснабжения КТС производится путем проверки соответствия подключения технических средств к сети основного и резервного электроснабжения, и схем подключения, представленных в технической документации на КТС АСУТП "Схемы питания и заземления (С 10)".

Фактическая проверка осуществляется на основании Акта о выполнении электротехнических работ путем поочередного отключения источников основного и резервного электроснабжения (одновременное отключение обоих источников не допускается).

3.4. Проверка проектного контура заземления КТС должна подтверждаться Актом проверки соответствия параметров контура заземления требованиям проекта и технической документации на КТС.

Проверка выполнения требований к электрической безопасности Системы. Проверка производится в соответствии с действующими правилами и нормами для электроснабжения и контура заземления, а также по наличию сертифика-

тов электрической безопасности на компоненты КТС (электрические цепи шкафов КТС, дисплеи рабочих станций и др.).

Проводится проверка соответствия электротехнических изделий комплекса технических средств требованиям "Правил устройства электроустановок". Защитное заземление КТС должно быть выполнено по ГОСТ 12.1.030 "*Электробезопасностъ. Защитное заземление. Зануление*

Все внешние части оборудования, находящиеся под напряжением свыше 42V по отношению к корпусу, должны иметь защиту от случайного прикосновения во время эксплуатации в штатных режимах работы. Изоляция электрически несвязанных цепей относительно корпуса и между собой при температуре +25 °С и относительной влажности до 80%, должна выдерживать в течение 1 минуты действие испытательного напряжения синусоидальной формы тока промышленной частоты:

- Между цепями с напряжением 40V - 250V;
- Между цепями с напряжением 250V - 1500V.

4. Метрологическая поверка измерительных каналов.

Метрологические характеристики датчиков и модулей ввода-вывода аналоговых сигналов определяются на основании данных фирм-изготовителей.

Метрологическая аттестация измерительных каналов Системы проводится по окончанию наладки системы по следующим типам параметров: давление, температура, расход, уровень жидкости, концентрация.

Метрологические характеристики измерительных каналов фиксируются в Актах и Протоколах метрологической поверки, представляемых Заказчиком.

5. Проверка отказоустойчивости и функций самодиагностики системы.

Данный вид проверки является одним из важнейших для взрывоопасных процессов.

Проверяется:

- Автоматический контроль и самодиагностика работоспособности программно-технического комплекса;
- Сохранение работоспособности КТС при сбоях и отказах, и восстановление исходной конфигурации оборудования в реальном времени.

5.1. Проверка отказоустойчивости и самодиагностики КТС.

Проверка функций самодиагностики программно-технического комплекса производится имитацией отказа на любом произвольно выбранном элементе оборудования.

Например:

1) Снимается питание с одного или нескольких модулей контроллера;
2) Имитируется обрыв линии связи;
3) Имитируется неисправность какой-либо части системы (контроллер, блок питания, модуль ввода-вывода, и т.д.);
4) При возникновении неисправности, которую можно имитировать путем отключения какого-либо элемента, система должна выдать соответствующее сообщение оператору процесса, сопровождаемое звуковой сигнализацией, регистрацией на принтере сообщений и сигнализаций, и записью в архив.
5) После снятия искусственных неисправностей должны исчезнуть соответствующие сообщения с экрана диаг-,ностики.

Перед проверкой отказоустойчивости и самодиагностики производится вызов стандартного системного окна *(System Status Overview).* На рабочей станции должно отображаться состояние всех компонентов Системы. Это состояние сопоставляется с фактическим состоянием компонентов Системы.

Все компоненты Системы должны отображаться в соответствии с их фактическим состоянием.

Поблочная проверка отказоустойчивости проводится после того, когда все блоки и модули Системы установлены, смонтированы и запитаны.

Испытания проводятся в нижеследующем порядке.

5.2. Тестирование системы бесперебойного электропитания.

Тестирование автомата включения резерва (АВР):

При поданном питании по 1-й и 2-й линии отключить питание с 1-й линии. При этом АВР должен переключиться на резервную линию питания. При переключении АВР источник бесперебойного питания (ИБП) должен обеспечивать непрерывное питание шкафов и операторских станций АСУТП.

Опять подключить 1-ю линию питания, АВР не должен изменить своего положения. При поданном питании по 1-й и 2-й линии отключить питание со 2-й линии и провести аналогичные проверки.

Тестирование отключения питания с 1-й и 2-й линии ввода:

Отключить питание с 1-й и 2-й линии. В этом случае ИБП должен обеспечить непрерывное питание шкафов, операторских станций АСУТП и цепей полевого оборудования от встроенных и внешних батарей.

При условии полной зарядки батарей все оборудование АСУТП (станции технолога-оператора, контроллеры РСУ и ПАЗ, **полевой КИП) должны сохранять работоспособность в течение 30 минут за счет источника бесперебойного электропитания.**

По окончанию проверки восстановить питание на ИБП.

Тестирование байпасной линии:

Включить байпасную линию питания АСУТП и отключить напряжение на 1-ми 2-м вводах АВР.

Контролировать работоспособность АСУТП. В этом случае питание шкафов и операторских станций должно осуществляться от байпасной линии (3-я линия питания). Подать питание на ИБП.

5.3. Проверка переключения резервированной системной шины данных:

1) Отключить одну из шин переводом переключателя в положение *Disable*, наблюдать при этом за отображением состояния шины на операторской станции и по месту.

   Необходимо убедиться, что обмен информации между контроллерами и операторскими станциями АСУТП не нарушается, а на контроллере и операторских станциях отображается истинное состояние каждой шины;
2) После включения первой шины произвести аналогичную процедуру со второй шиной.

Операции по обоим пунктам провести последовательно на каждом контроллере.

5.4. Проверка переключения резервированных модулей управления и защиты:

1) Остановить один из процессоров (модулей управления), и наблюдать за отображением его состояния на операторской станции и в стойке. Убедиться, что обмен информации между контроллером и операторскими станциями АСУТП не нарушается, а на контроллере и операторской станции отображается истинное состояние каждого процессора;
2) Восстановить работоспособность отключенного модуля управления, затем отключить второй модуль и провести аналогичные проверки.

Операции по обоим пунктам провести последовательно на каждом контроллере.

5.5. Проверка резервированных блоков питания контроллеров РСУ **и ПАЗ.** Проводится в следующем порядке:

1) Отключить 1-й блок питания контроллера. При этом наблюдать состояние блоков питания на операторской станции и в стойке. Необходимо убедиться, что обмен информации между контроллером и операторскими станциями АСУТП не нарушается, а на контроллере и операторской станции отображается истинное состояние каждого блока питания;
2) Включить 1-й блок питания;
3) Отключить 2-й блок питания, и провести аналогичные проверки;
4) Включить 2-ой блок питания.

Операции по этим пунктам провести последовательно на каждом контроллере.

5.6. Проверка резервированных блоков питания 24 VDC шкафов РСУ и ПАЗ. Проводится в следующем порядке:

1) Отключить один из блоков питания 24 VDC;
2) Проверить получение информации по аналоговым сигналам, подключенным через барьеры искробезопасности, и по дискретным сигналам данного шкафа на операторской станции;
3) Включить 1-й блок питания;
4) Отключить 2-й блок питания, провести аналогичные проверки.

Операции по пунктам 1)-4) провести последовательно в каждом шкафу РСУ и ПАЗ.

5.7. Проверка резервированных блоков питания шкафа реле. Проводится в следующем порядке:

1) Отключить один из блоков питания 24 VDC;
2) Проверить получение информации по дискретным сигналам шкафа реле на операторской станции;
3) Включить 1-й блок питания;
4) Отключить 2-й блок питания и провести аналогичные проверки.

5.8. Проверка выполнения требований к безопасности и сохранности информации в Системе при сбоях и отказах Системы.

После наведения искусственных сбоев в Системе (скачки или перерывы в электроснабжении и т.п.) и их последующей ликвидации, производится проверка того, что:

- Рабочие станции и контроллеры автоматически перезапускаются и продолжают нормально функционировать;
- Все исполнительные механизмы в зависимости от предопределенных условий сохраняют свое текущее положение, либо переходят в предопределенное состояние.

Тестирование сохранности базы данных при отключении операторской станции:

1) Отключить на несколько минут операторскую станцию;
2) Включить операторскую станцию и проконтролировать сохранность базы данных.

Операции по обоим пунктам провести последовательно для каждой операторской станции.

Система должна обеспечивать сохранность баз данных технологических параметров и программного обеспечения при сбоях и отказах Системы на всех уровнях управления.

Проверка резервирования и сохранности информации при отказе зеркального диска операторской станции проводится последовательным отключением и подключением каждого из резервированных дисков, и проверкой сохранения работоспособности рабочей станции.

Резервные копии базы данных и программного обеспечения Системы должны храниться на сменных оптических / магнитных носителях. Проверка производится путем контроля наличия резервных файлов на различных носителях, и **совпадения текущих версий.**

5.9. **Проверка быстродействия Системы.** Проверяются характеристики быстродействия Системы в соответствии с требованиями Технического задания:

- Цикл опроса аналоговых параметров с технологических объектов управления - не более 1 сек;
- Выдача команд управления на исполнительные механизмы - не более 1 сек;
- Выявление технологических нарушений и изменений состояния (сигнализация отклонения параметров, изменение состояния исполнительных механизмов, включение или отключение устройств и т.п.) - не более 1 сек;
- Отображение нового кадра - не более 2 сек;
- Обновление значений постоянно индицируемых параметров - не реже одного раза в 1 сек.

5.10. **Проверка выполнения требований к защите Системы ог несанкционированного доступа.** Защита Системы от несанкционированного доступа осуществляется путем регистрации пользователей в Системе по личному коду и паролю доступа в соответствии с инструкцией "Руководства пользователя (ИЗ)".

После входа пользователя в приложение, доступ к любой защищенной функции будет предоставляться путем сравнения пароля оператора и уровня доступа со значением, определенным для данной функции.

При использовании неправильного кода и пароля пользователь не должен получать доступа к Системе, при этом чолжно появляться сообщение об отсутствии доступа к Сис-1сме.

Факт попытки несанкционированного проникновения и Систему фиксироваться в защищенном от доступа оперативного персонала системном Протоколе.

Доступ к конфигурации контроллера должен защищаться специальными программными, техническими и организационными средствами:

- Физическая изоляция инженерной станции;
- Разрешение доступа к инженерной станции только строго определенному кругу лиц;
- Пароли и физические ключи.

6. Проверка реализации функций АСУТП.

Испытания включают:

- Проверку входов-выходов;
- Проверку информационных функций;
- Проверку выполнения управляющих функций;
- Проверку функций противоаварийной защиты с имитацией причин срабатывания защиты и отслеживанием результатов срабатывания;
- Проверку выполнения требований к условиям эксплуатации, техническому обслуживанию и ремонту Системы.

Проверка выполнения функций Системы осуществляется в соответствии с технической и проектной документацией:

- Перечень входных и выходных сигналов РСУ (В1);
- Перечень входных и выходных сигналов системы ПАЗ **(В2);**
- Схемы электрические принципиальные контуров; измерения, регулирования, сигнализации и блокировок *(Loop Diagrams)* (СБ);
- Описание информационного обеспечения системы (П5);
- Описание организации информационной базы (П6);
- Описание систем классификации и кодирования (П7);
- Описание массивов исторических данных (архивов) (П8);
- Альбом документов и видеокадров (С9);
- Состав выходных данных (сигнализаций, сообщений) (В8);
- Каталог баз данных (В7);
- Инструкция по формированию и ведению базы данных (И4);
- Описание и логические схемы алгоритмов (ПБ);
- Функциональные схемы автоматизации (СЗ);
- Блок-схемы алгоритмов РСУ (С 11);
- Блок-схемы алгоритмов ПАЗ (С 12);

- Инструкция по эксплуатации и обслуживанию КТС (ИЭ).

Результат проверок оформляются одним или несколькими Отчетами и Протоколом.

6.1. Проверка входов-выходов.

Проверка аналоговых входных сигналов 4-20 тА.

Входы-выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

1) Проверка диапазона измерения с использованием задатчика тока по пяти точкам (таблица 8.1):

Таблица 8.1

Значение тока шА	Точка диапазона измерения %
4	0
8	25
12	50
16	75
20	100

Непосредственно на клеммах полевого оборудования последовательно задается задатчиком/калибратором 5 значений аналогового сигнала (0%, 25%, 50%, 75%, 100%) и проверяется отображение соответствующего значения на станции оператора. Показания калибратора и показаний датчика на станции оператора должны соответствовать друг другу.

2) Имитация обрыва цепи датчика, и проверка соответствующей сигнализации;
3) Имитация нарушения верхней предупредительной границы, и проверка выдачи предупредительного сообщения;
4) Имитация нарушения верхней предаварийной границы диапазона измерения, и проверка выдачи предаварийного сообщения;
5) Имитация нарушения нижней предупредительной границы, и проверка выдачи предупредительного сообщения;

6) Имитация нарушения нижней предаварийной границы диапазона измерения, и проверка выдачи предаварийного сообщения.

Проверка дискретных входов.

Входы»выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно таблицам расключения входов-выходов;
- Правильности настроек сигнализации;
- Правильности графического представления.

Тестирование проводится с использованием следующей процедуры:

1) Проверить правильность идентификации входного сигнала;
2) Начальное условие - входная цепь контура разомкнута;
3) Проверить на экране статус входного сигнала и подтвердить правильность представления для разомкнутой цепи по месту;
4) Замкнуть цепь входа;
5) Проверить на экране статус входного сигнала и подтвердить правильность для закрытой цепи по месту;
6) Разомкнуть цепь входа;
7) Проверить на экране статус входного сигнала и подтвердить правильность для разомкнутой цепи по месту;
8) Проверить сигнализацию.

Проверка дискретных выходных каналов.

Входы-выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (то есть управляю-

щие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц (если используется).

Тестирование проводится с использованием следующей процедуры:

1) Проверить правильность идентификатора выходного сигнала;
2) Проверить наличие в соответствующей блокировке;
3) Начальное условие - на операторской консоли выход отключен (OFF);
4) Проверить выходные контакты и подтвердить правильность состояния выхода - OFF (то есть открытой цепи);
5) Установить выход на операторской консоли в состояние ON (включить);
6) Проверить выходные контакты и подтвердить правильность состояния выхода - ON (то есть закрытой цепи);
7) Установить выход на операторской консоли в состояние OFF (выключить);
8) Проверить выходные контакты и подтвердить правильность поля состояния выхода - OFF (то есть открытой цепи).

Проверка аналоговых выходов.

Входы-выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению входов-выходов;
- Правильности функционирования и принадлежности (управляющие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Тестирование проводится с использованием нижеследующей процедуры:

1) Проверить правильность диапазона физических единиц и их обозначения;
2) Начальное условие - цепь выхода разомкнута;
3) Проверить на экране статус выхода и подтвердить правильность сигнализации открытого контура;
4) Проверить, чтобы в цепи выходов было установлено правильное значение для выходного сигнала контура 0%;
5) Установить выходной сигнал контура 0%, 25%, 50%, 75% и 100%. Проверяется работоспособность сигнализаций:
   - Высокий-высокий (HH) и высокий (H);
   - Низкий-низкий (LL) и низкий (L);
   - Разомкнуть цепь выхода и проверить соответствующую сигнализацию.

6.2. Проверка информационных функций.

Проверяются следующие функции:

1) Автоматическое с заданной периодичностью (а также по вызову) измерение, регистрация, отображение и архивирование текущих значений технологических параметров;
2) Автоматическая сигнализация отклонений технологических параметров от установленных предупредительных и предаварийных пределов;
3) Автоматическое ведение трендов технологических параметров;
4) Автоматическое ведение протоколов изменений состояния устройств, отклонений и нарушений технологического процесса, и действий оперативно-технического персонала.

Проверка функций измерения и контроля:

1) Проверяется наличие значений аналоговых сигналов на мнемосхемах в соответствии с Перечнями входных и выходных сигналов (B1) и (B2), и Альбомом документов и видеокадров (C9);
2) Проверяется соответствие числового значения параметра на экране станции оператора фактическому значению измеряемого технологического параметра.

Проверка осуществляется сличением фактического и воспроизведенного на экране рабочей станции значения техноло-

гического параметра. В процессе проверки функций измерения осуществляется проверка достоверности измерения параметров.

Выход параметра за предупредительные и предаварийные границы должен сопровождаться появлением соответствующего сообщения, и изменением цвета в поле отображения параметра. Недостоверные и неподтвержденные параметры и сигналы состояния отображаются мерцанием поля.

Проверка предупредительных и предаварийных сигнализаций и сообщений. Осуществляется имитацией нарушения предупредительного и предаварийного порога, и контролем над автоматическим выводом соответствующих сообщений в информационную строку на мнемосхеме, протоколированием в базе данных и на выделенном для регистрации событий и сигнализаций принтере.

Проверка выполнения функции сигнализации выполняется по изменению состояния датчиков на соответствующей мнемосхеме при реальном изменении состояния, или путем простого замыкания соответствующих клемм на модуле ввода-вывода.

Проверка функций регистрации выполняется путем (типа "посредством") просмотра протоколов и графиков технологических переменных во времени.

Проверка функции автоматического отображения информации. Проводится путём вызова на экран рабочей станции видеокадров:

1) Мнемосхем технологического процесса;
2) Графиков изменения технологических параметров во времени (трендов);
3) Технологических сводок о режимах работы объекта;
4) Диагностики состояния блоков и модулей КТС;
5) Протокола действий технолога-оператора;
6) Рабочих (режимных) листов.

Проверка выполняется путем наблюдения за автоматическим обновлением при изменении значений параметров.

6.3. Проверка выполнения управляющих функций.

Стандартное ПИД - регулирование заключается в изменении управляющего выходного сигнала в случае расхождения между значением технологической переменной PV и заданным значением SV, введенным оператором.

Входы-выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (то есть управляющие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Тестирование проводится с использованием следующей процедуры:

1) Проверить правильность диапазона физических единиц входа и их описания;
2) Начальное условие - режим контура MANUAL (ручной), цепь входов разомкнута, установить контрольную точку 0% диапазона, выходные сигналы контура 0%;
3) Проверить работу контура (то есть проверить статусы открытый/закрытый, обратный/прямой);
4) Проверить, чтобы в цепи выходов было установлено правильное значение для выходного сигнала контура 0%;
5) Проверить сигнализацию обрыва аналогового входа;
6) Подать на вход сигналы следующих значений: 4мА, 8мА, 12мА, 16мА и 20мА;
7) По каждому уровню входного сигнала подтвердить правильность соответствующего значения физической единицы и то, что любая сигнализация срабатывает при правильном значении (делается посредством проверки пределов сигнализации в конфигурации);
8) Проверить следующие сигнализации:
    - Высокий-высокий (HH) и высокий (H);
    - Низкий-низкий (LL) и низкий (L);
    - Сигнализация о превышении допустимого отклонения от задания;
    - Разомкнуть цепь входа и проверить сигнализацию обрыва;

- Разомкнуть цепь выхода и проверить сигнализацию обрыва.

9) Ввести значение больше 100% и проверить, что срабатывает сигнализация, указывающая на превышение диапазона значений;
10) Установить выходной сигнал контура в 0%, 25%, 50%, 75% и 100%;
11) Разомкнуть цепь выхода и проверить сигнализацию;
12) Установить входной сигнал в 50%, и выходной в 50%. Установить задание в 75%. Перевести контур в режим AUTO (автоматический) и проверить, что нарастание / понижение выходного сигнала происходит в соответствии с заданием.

6.4. Проверка выполнения функций противоаварийной защиты.

Проверка функций ПАЗ выполняется путём принудительного изменения значений параметров, или имитацией их изменения:

1) Для всех аналоговых входных параметров, связанных с алгоритмами противоаварийной защиты, имитируется ситуация перехода предаварийных границ, а для дискретных сигналов имитируется переключение, соответствующее нарушению.
   При этом должно происходить срабатывание соответствующих исполнительных механизмов в соответствии с документом "Блок-схемы алгоритмов ПАЗ (С 12)". Одновременно проверяются функции отображения данных ситуаций на станциях операторов;
2) Функция определения первопричины срабатывания блокировок проверяется путем имитации в минимально возможный промежуток времени нескольких предаварийных событий;
3) Проверяется возможность перевода исполнительных механизмов из положения, соответствующего сработавшей блокировке, в исходное положение при условии, что входные параметры блокировки находятся в допустимых пределах;
4) С инженерной станции проверяется возможность отключения входных блокирующих сигналов (деблокировка) от алгоритма защиты. В зависимости от уровня

допуска оперативного персонала к функциям обслуживания системы проверяется возможность или невозможность деблокировки технологических параметров со станций технолога-оператора.

Одновременно проверяются функции сигнализации всех событий на станциях технолога-оператора и их регистрация в системных протоколах.

Перечень сигналов системы ПАЗ и логика её работы должны соответствовать проектной документации. Исходные данные для проверки:

- Перечень входных и выходных сигналов ПАЗ (В2);
- Схемы контуров (СБ);
- Блок-схемы алгоритмов ПАЗ (С 12).

6.5. Проверка выполнения требований к условиям эксплуатации, техническому обслуживанию и ремонту Системы.

Проверяется выполнение требований раздела Технического задания к условиям эксплуатации, техническому обслуживанию и ремонту Системы.

Проверка помехозащищенности и устойчивости технических средств к воздействию внешних факторов (температура и влажность окружающего воздуха, электромагнитные воздействия, вибрация и т.д.) выполняется путем оценки работоспособности Системы в реальных производственных условиях в процессе её наладки и эксплуатации.

7. Проверка квалификации и уровня подготовки оперативного (технологического) и эксплуатационного (обслуживающего) персонала для работы в условиях функционирования АСУТП.

Комиссия в процессе испытаний проверяет навыки персонала по взаимодействию с Системой.

Комиссия должна оценить квалификацию оперативного технологического и эксплуатационного (обслуживающего) персонала АСУТП, проверить журналы прохождения инструктажей, наличие удостоверений и допусков к работе с Системой.

При необходимости комиссия уточняет и согласовывает состав и порядок выполнения работ по гарантийному и сервисному обслуживанию АСУТП.

8.10. Содержание организационно-распорядительных документов

1. **Акт завершения работ.**
   Документ содержит:
   1) Наименование завершенной работы;
   2) Список представителей организации-разработчика, и организации-заказчика, составивших Акт;
   3) Дату завершения работ;
   4) Наименование документов, на основании которых проводилась работа;
   5) Основные результаты завершенной работы;
   6) Заключение о результатах завершенной работы.
2. **Акт приемки в опытную эксплуатацию.**
   Документ содержит:
   1) Наименование объекта автоматизации;
   2) Наименование АСУТП (или ее части), принимаемой в опытную эксплуатацию;
   3) Наименование документа, на основании которого разработана АСУТП;
   4) Состав Приемочной комиссии и основание для ее работы (наименование, номер и дату утверждения документа, на основании которого создана комиссия);
   5) Период времени работы комиссии;
   6) Наименование Организации-разработчика, Организаций-соисполнителей и Организации заказчика;
   7) Состав функций АСУТП (или ее части), принимаемых в опытную эксплуатацию;
   8) Перечень составляющих технического, программного, информационного и организационного обеспечений, проверяемых в процессе опытной эксплуатации;
   9) Перечень документов, предъявляемых комиссии;
   10) Оценку соответствия АСУТП Техническому заданию на ее создание;
   11) Основные результаты приемки в опытную эксплуатацию;
   12) Решение комиссии о принятии АСУТП в опытную эксплуатацию.

3. Акт приемки в промышленную эксплуатацию.

После всех перенесенных испытаний составляется Акт приемки системы в промышленную эксплуатацию, который должен содержать:

1) Наименование объекта автоматизации и АСУТП, принимаемой в промышленную эксплуатацию;
2) Сведения о статусе и составе Приемочной комиссии, и основание для ее работы;
3) Период работы комиссии;
4) Наименования организаций Заказчика, Проектной организации, Разработчика, Поставщика оборудования;
5) Наименования документов, на основании которых разработана АСУТП;
6) Состав АСУТП и реализуемых функций;
7) Перечень составляющих технического, программного, информационного и организационного обеспечений, принимаемых в промышленную эксплуатацию;
8) Перечень документов (Актов и Протоколов предварительных испытаний и опытной эксплуатации), представленных комиссии;
9) Оценку соответствия Системы техническому заданию, проектной и технической документации;
10) Оценку результатов испытаний Системы;
11) Решение комиссии о приеме или не приеме Системы в промышленную эксплуатацию;
12) Рекомендации комиссии по доработке Системы.

К "Акту приемки в промышленную эксплуатацию" прилагают:

1) Программу и протоколы испытаний;
2) Протоколы заседания комиссии;
3) Акты приемки в промышленную эксплуатацию принятых ранее частей АСУТП;
4) Перечень технических средств, которые использовала комиссия при приемке АСУТП;
5) Справку о применении в АСУТП унифицированных форм документов и классификаторов.

По усмотрению комиссии допускается включать в Приложения дополнительные документы.

4. План-график работ.

Документ устанавливает перечень работ, сроки выполнения и исполнителей работ, связанных с созданием АСУТП. Для каждой работы, включенной в перечень, План-график содержит:

1) Наименование работы;
2) Дату начала и окончания работы;
3) Наименование подразделения-участника работы;
4) Фамилию и должность ответственного исполнителя;
5) Форму представления результатов работы.

5. Приказ о проведении работ.

В зависимости от этапа работ по созданию АСУТП установлены следующие документы:

1) Приказ о готовности объекта автоматизации к проведению строительно-монтажных работ;
2) Приказ о готовности объекта автоматизации к проведению наладочных работ;
3) Приказ о начале опытной эксплуатации АСУТП (ее частей);
4) Приказ о вводе АСУТП в промышленную эксплуатацию (ее частей).

Документ **"Приказ о готовности объекта автоматизации к проведению строительно-монтажных работ"** содержит:

1) Сообщение о готовности объекта автоматизации к проведению строительно-монтажных работ;
2) Определение зоны строительства и монтажа;
3) Порядок допуска к проведению работ;
4) Список представителей организации-заказчика, ответственных за проведение работ и сохранность смонтированного оборудования;
5) Список ответственных представителей строительных и монтажных организаций, проводящих работы.

Документ **"Приказ о готовности объекта автоматизации к проведению наладочных работ"** содержит:

1) Сообщение о готовности объекта автоматизации к проведению наладочных работ;
2) Перечень технических средств АСУТП, подлежащих наладке;
3) Указание о порядке проведения наладочных работ;

4) Порядок допуска к проведению наладочных работ;
5) Список представителей организации-заказчика, ответственных за обеспечение проведения наладочных работ;
6) Список ответственных представителей организаций, выполняющих наладочные работы;
7) Указания о порядке устранения ошибок монтажа и лицах, ответственных за выполнения этих работ.

Документ **"Приказ о начале опытной эксплуатации АСУТП"** (или ее частей) содержит:

1) Наименование АСУТП в целом или ее частей, проходящей опытную эксплуатацию;
2) Наименование организации разработчика, организаций-соисполнителей;
3) Сроки проведения опытной эксплуатации;
4) Список должностных лиц организации-заказчика и организации-разработчика, ответственных за проведение опытной эксплуатации;
5) Перечень подразделений организации-заказчика, участвующих в проведении опытной эксплуатации.

Документ **"Приказ о вводе АСУТП** (или ее частей) **в промышленную эксплуатацию"** должен содержать:

1) Состав функций АСУТП или ее частей, технических **и** программных средств, принимаемых в промышленную эксплуатацию;
2) Список должностных лиц и перечень подразделений организации-заказчика, ответственных за работу АСУТП;
3) Порядок и сроки введения новых форм документов (при необходимости);
4) Порядок и сроки перевода персонала на работу в **условиях** функционирования АСУТП.

Приказ о составе приемочной комиссии.

Документ содержит:

1) Наименование принимаемой АСУТП (в целом или ее і частей);
2) Сведения о составе комиссии;
3) Основание для организации комиссии;
4) Наименование Организации-заказчика;
5) Наименование Организации-разработчика;

6) Наименования организаций-соисполнителей;
7) Назначение и цели работы комиссии;
8) Сроки начала и завершения работы комиссии;
9) Указание о форме завершения работы комиссии.

6. Протокол испытаний.

Документ содержит:

1) Наименование объекта испытаний;
2) Список должностных лиц, проводивших испытания;
3) Цель испытаний;
4) Дата и продолжительность испытаний;
5) Перечень разделов и пунктов "Технического задания на создание АСУТП", на соответствие которым проведены испытания;
6) Перечень пунктов проверки из "Программы испытаний", по которым проведены испытания;
7) Сведения о результатах испытаний;
8) Сведения об отказах, сбоях и аварийных ситуациях, возникающих при испытаниях;
9) Сведения о корректировках параметров объекта испытания и технической документации.

7. Протокол согласования.

Документ содержит:

1) Перечень рассмотренных отклонений с указанием документа, отклонения от которого являются предметом согласования;
2) Перечень должностных лиц, составивших протокол;
3) Обоснование принятых отклонений от проектных решений;
4) Перечень согласованных отклонений и сроки внесения необходимых изменений в техническую документацию.

Далее приводятся типовые формы документов, необходимых при оформлении, утверждении результатов испытаний и при приемке АСУТП в опытную и постоянную (промышленную) эксплуатацию, а также образцы Протоколов, Отчетов и Актов, оформляемых при проведении испытаний.

8.11. Типовая форма Протокола организационного заседания комиссии

ПРОТОКОЛ
Организационного заседания комиссии

Место проведения Дата

1. В соответствии с

(наименование, номер и дата документа)

комиссия приступила к работе в следующем составе:

Председатель комиссии:

(должность, ф.и.о.)

Члены комиссии:

(должность, ф.и.о.)

2. Программа работы комиссии.

3. График проведения испытаний (таблица 8.2).

4. Определение состава рабочих групп.

Председатель комиссии:
(Ф. И. О.) (Подпись) (Дата)
Секретарь комиссии:
(Ф. И. О.) (Подпись) (Дата)

Таблица 8.2

Типовая форма Графика проведения испытаний

Наименование работы	Дата		Наименование подразделения-участника работы	Фамилия и должность ответственного исполнителя	Форма представления результатов работы
	Начало	Окончание			

8.12. Типовая форма Протокола предварительных (или приемочных) испытаний

ПРОТОКОЛ
Проведения предварительных (приемочных) испытаний АСУТП

Место проведения Дата

1) Наименование объекта испытаний;
2) Список должностных лиц, проводивших испытания;
3) Цель испытаний;
4) Сведения о продолжительности испытаний;
5) Перечень разделов и пунктов "Технического задания на создание АСУТП", на соответствие которым проведены испытания;
6) Перечень разделов из "Программы испытаний", по которым проведены испытания;
7) Сведения о результатах испытаний;
8) Сведения об отказах, сбоях и аварийных ситуациях, возникающих при испытаниях;
9) Сведения о корректировках параметров объекта испытания и технической документации;
10) Выводы.

Ответственные члены комиссии:

(Ф. И. О.) (Подпись) (Дата)

Привлекаемые специалисты:

(Ф. И. О.) (Подпись) (Дата)

$.13. Образцы протоколов и отчетов по разделам Программы испытаний

ПРОТОКОЛ №1
Проверка спецификации комплекса технических средств и стандартной технической документации

Заказчик :
Исполнитель
Договор № :
Завод :

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную эксплуатацию.

Согласно Спецификации к Договору YNF-1234/01 на поставку оборудования АСУТП проведена проверка поставленного оборудования и стандартной технической документации.

Результаты проверки комплектности КТС и стандартной технической документации:

Оборудование, поставленное по накладной на прием-передачу, соответствует Спецификации к Договору YNF-1234/01. Претензии по комплектности поставки КТС и стандартной технической документации отсутствуют.

Председатель комиссии:
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:
(Ф. И. О.) (Подпись) (Дата)

ПРОТОКОЛ №2
Проверка состава и содержания документации технорабочего проекта

Заказчик
Исполнитель :
Договор № :
Завод

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Согласно Приложению № к Договору YNF-1234/02 на разработку Технорабочего проекта проведена проверка комплектности разработанной документации Технорабочего проекта на АСУТП по компонентам.

Результаты Проверки комплектности разработанной проектной документации:

Документация поставлена в полном объеме согласно Приложению № к Договору YNF-1234/02.

Претензии по комплектности разработанной документации отсутствуют.

Председатель комиссии:
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:
(Ф. И. О.) (Подпись) (Дата)

ПРОТОКОЛ №3
Проверка готовности комплекса технических средств

Заказчик :
Исполнитель :
Договор № :
Завод :

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Согласно Спецификации к Договору YNF-1234/01 и Договору YNF-1234/02 на разработку Технорабочего проекта проведена проверка готовности комплекса технических средств.

Результаты Проверки готовности КТС представлены в Отчете №3.

Претензии по готовности комплекса технических средств к опытной (промышленной) эксплуатации отсутствуют.

Председатель
комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:
(Ф. И. О.) (Подпись) (Дата)

ОТЧЕТ №3
Проверка готовности комплекса технических средств

Заказчик :
Исполнитель
Договор № :
Завод :

Данный Отчет является частью приемки АСУТП в опытную (промышленную) эксплуатацию.
Проверка готовности комплекса технических средств включает следующие проверки:

3.1 Проверку правильности и качества проектного монтажа и внутренних соединений РСУ и ПАЗ;
3.2 Проверка правильности проектного монтажа и подключения полевого оборудования к кроссовым шкафам;
3.3 Проверку проектного электроснабжения КТС;
3.4 Проверку проектного контура заземления КТС.

Результаты Проверки готовности КТС представлены в таблице 8.3.
Претензии по готовности комплекса технических средств к опытной (промышленной) эксплуатации отсутствуют.

Председатель
комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Примечание

Необходимость сопровождения каждого из Протоколов подобным Отчетом зависит от сложности и объема проводимых испытаний. Очевидно, что в ряде случаев вполне достаточно сослаться на соответствующие таблицы с результатами испытаний непосредственно из соответствующего Протокола результатов проверки.

Таблица 8.3

Перечень проверок готовности комплекса технических средств

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведения теста	Статус теста: успешно ДА / НЕТ
3.1	Проверка правильности и качества проектного монтажа и внутренних соединений РСУ и ПАЗ		
3.2	Проверка правильности проектного монтажа и подключения полевого оборудования к кроссовым шкафам		
3 3	Проверка проектного электроснабжения КТС		
3 4	Проверка проектного контура заземления КТС		

ПРОТОКОЛ №4
Метрологической поверки измерительных каналов АСУТП

Заказчик :
Исполнитель :
Договор № :
Завод

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную эксплуатацию.

Поверка измерительных каналов АСУТП проведена в соответствии со следующими нормативными документами:

- ГОСТ 8.009-84 ГСИ. *"Нормируемые метрологические характеристики средств измерений*и
- Методикой поверки МИ 2439-97 *"Метрологические характеристики измерительных систем. Номенклатура. Принципы регламентации, определения и контроля*", утвержденной ВНИИМС.

Результаты Метрологической поверки:
Все измерительные каналы поверены в объеме 100%.
Претензии к точности измерительных каналов отсутствуют.

Председатель комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:___
(Ф. И. О.) (Подпись) (Дата)

ПРОТОКОЛ №5
Проверка отказоустойчивости и функций самодиагностики системы

Заказчик :
Исполнитель :
Договор №
Завод :

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Согласно Договору YNF-1234/01 на поставку оборудования, и Договору YNF-1234/02 на разработку Технорабочего проекта проведена проверка отказоустойчивости и функций самодиагностики системы.

Результаты Проверки приведены в Отчете №5 "О проверке отказоустойчивости и функций самодиагностики системы".
Претензии по отказоустойчивости и функциям самодиагностики системы отсутствуют.

Председатель комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Примечание

Проверки составных частей системы на отказоустойчивость и обеспечение функций самодиагностики могут быть проведены индивидуально, и тогда для них могут быть оформлены самостоятельные Отчеты, либо они проверяются в составе единого пункта проверки, а результаты объединяются в единый Отчет.

ОТЧЕТ №5
Проверка отказоустойчивости и функций самодиагностики системы

Заказчик :
Исполнитель :
Договор № :
Завод :

Данный ОТЧЕТ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Перечень испытаний и их результаты приведены в таблице **8.4.**

Результаты проверки отказоустойчивости и функций самодиагностики системы:
Техническое обеспечение и системное программное обеспечение АСУТП функционируют в соответствии с заявленными в технической документации характеристиками.
Претензии по проверке отказоустойчивости и функций самодиагностики системы отсутствуют.

Председатель комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Таблица 8.4

Перечень проверки отказоустойчивости и функций самодиагностики системы

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведения теста	Статус теста: успешно ДА/НЕТ
5.1	Проверка отказоустойчивости и самодиагностики КТС		
5.2	Тестирование системы бесперебойного питания		
5.3	Проверка переключения резервированной системной шины данных		
5.4	Проверка переключения резервированных модулей управления и защиты		
5.5	Проверка резервированных блоков питания контроллеров РСУ и ПАЗ		
5.6	. Проверка резервированных блоков питания 24 VDC шкафов РСУ и ПАЗ		
5.7	Проверка резервированных блоков питания шкафа реле		
5.8	Проверка выполнения требований к безопасности и сохранности информации в Системе при сбоях и отказах Системы		
5 9	Проверка быстродействия Системы		
5.10	Проверка выполнения требований к защите Системы от несанкционированного доступа		

ПРОТОКОЛ №6
Проверка реализации функций АСУТП

Заказчик :
Исполнитель :
Договор № :
Завод :

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Результаты проверки реализации функций АСУТП приведены в Отчете №6 "О проверке реализации функций АСУТП".

Системное и прикладное программное обеспечение АСУТП функционирует в полном соответствии с Техническим заданием и с Технорабочим проектом.
Претензии по реализации функций АСУТП отсутствуют.

Председатель комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:__
(Ф. И. О.) (Подпись) (Дата)

Далее приводится пример Отчета №6 к Протоколу №6.

ОТЧЕТ №6
О проверке реализации функций АСУТП

Заказчик :
Исполнитель :
Договор № :
Завод :

Данный ОТЧЕТ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

После загрузки системного программного обеспечения и прикладного программного обеспечения проведена проверка реализации функций АСУТП в соответствии с данным этапом проверки:

6.1 Проверка входов-выходов;
6.2 Проверка информационных функций;
6.3 Проверка выполнения управляющих функций;
6.4 Проверка выполнения функций противоаварийной защиты;
6.5 Проверка выполнения требований к условиям эксплуатации, техническому обслуживанию и ремонту Системы.

Произведенные проверки и их результаты приведены в таблице 8.5.

Результаты проверки реализации функций АСУТП:
Системное и прикладное программное обеспечение АСУТП функционирует в полном соответствии с Техническим заданием и с Технорабочим проектом.
Претензии по реализации функций АСУТП отсутствуют.

Председатель комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Таблица 8.5

Перечень проверок реализации функций АСУТП

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведе-ния теста	Статус теста: успешно ДА/НЕТ
6.1	Проверка входов-выходов		
6.2	Проверка информационных функций		
6.3	Проверка выполнения управляющих функций		
6.4	Проверка выполнения функций противоаварийной защиты		
6 5	Проверка выполнения требований к условиям эксплуатации, техническому обслуживанию и ремонту Системы		

ПРОТОКОЛ №7
Проверка квалификации и уровня подготовки оперативного (технологического) и эксплуатационного (обслуживающего) персонала для работы в условиях функционирования АСУТП

Заказчик :
Исполнитель :
Договор № :
Завод

Данный ПРОТОКОЛ является частью приемки АСУТП в опытную (промышленную) эксплуатацию.

Согласно Договору YNF-1234/03 на разработку и внедрение АСУТП, предусматривающему обучение оперативного и эксплуатационного персонала, проведена проверка знаний эксплуатационной и проектной документации на АСУТП, и наличие у персонала необходимых навыков для выполнения установленных функций во всех режимах функционирования АСУТП.

Результаты Проверки знаний и навыков персонала:
Оперативный и эксплуатационный персонал АСУТП продемонстрировал наличие знаний эксплуатационной и проектной документации на АСУТП, и наличие необходимых навыков для выполнения установленных функций во всех режимах функционирования АСУТП.
Претензии по подготовке персонала для допуска к работе в условиях функционирования АСУТП отсутствуют.

Председатель
комиссии:___
(Ф. И. О.) (Подпись) (Дата)

Члены комиссии:
(Ф. И. О.) (Подпись) (Дата)

Таблица 8.6

Типовая форма Рабочего журнала регистрации замечаний, выявленных в процессе испытаний

Содержание замечаний и рекомендации	Предлагаемые мероприятия по устранению	Ответственный исполнитель	Срок исполнения		Форма отчетности	Примечание
			План	Факт		

8.14. АКТ Приемки АСУТП в опытную (промышленную) эксплуатацию

Комиссия в составе:

Председателя:
(Должность) (Ф.И.О)

И членов комиссии
От Организации - заказчика:
Главный специалист по АСУТП (Ф.И.О)

Главный инженер производства

Главный метролог производства

Главный энергетик производства

Начальник ПТО производства

От Организации - поставщика оборудования:
Технический директор (Ф.И.О)

Руководитель проекта

От Организации - разработчика АСУТП:
Технический директор (Ф.И.О)

Руководитель проекта

От Проектной организации:
Технический директор (Ф.И.О)

Руководитель проекта

От технадзора:
Представитель территориального органа Ростехнадзора .ф ' ^ q. ' '
Представитель технадзора предприятия-заказчика

действующая на основании Распоряжения № 123 от хх.хх 2010 года, составила настоящий Акт о нижеследующем:
Комиссия провела приемку АСУТП производства *ЛВС* в период с_____по_____2010 года.

Комиссии были предъявлены:

1) Технические средства АСУТП производства АВС в составе, соответствующем Спецификации к Договору YNF-1234/01 на поставку технических средств;
2) Разработанная документация согласно Договору YNF-1234/02 на разработку Технорабочего проекта;
3) Собственно разработанная автоматизированная система управления технологическим процессом АВС в соответствии с Договором на разработку и внедрение АСУТП YNF-1234/03.

АСУТП обеспечивает выполнение следующих основных функций:

- Функции сбора и первичной обработки аналоговой и дискретной информации;
- Функции визуализации;
- Функции сигнализации;
- Функции диагностики;
- Функции передачи данных;
- Функции регулирования аналоговых параметров;
- Функции управления оборудованием;
- Функции системы противоаварийной защиты;
- Функции формирования и визуализации протоколов нарушений;
- Функции формирования и вывода на печать отчетов.

Система состоит из:

- Распределенной системы управления, базирующейся на КТС системы УУУ, и предназначенной для управления технологическим процессом производства АВС в режиме реального времени, и для предоставления информации в заводскую ЛВС;
- Системы противоаварийной защиты, базирующейся на КТС системы ZZZ, и предназначенной для автоматического перевода технологического процесса в безопасное состояние при возникновении предаварийных ситуаций, и
- Полевого оборудования в соответствии с проектной спецификацией.

Комиссии предъявлена следующая документация:

1) Техническое Задание на создание АСУТП;
2) Исполнительная документация по монтажу;
3) Протокол Предварительных испытаний;
4) Программа испытаний АСУТП;
5) Техническая и проектная документация на АСУТП.

При приемке в промышленную эксплуатацию дополнительно представляются следующие документы:

6) Акт приёмки АСУТП в Опытную эксплуатацию;
7) Рабочие журналы Опытной эксплуатации АСУТП;
8) Акт о завершении работ по проверке АСУТП в режиме Опытной эксплуатации.

Перед предъявлением Системы на приемочные испытания техническая документация была доработана по замечаниям Протокола предварительных испытаний и Акта о завершении работ по проверке Системы в режиме опытной эксплуатации.

Рассмотрев представленные материалы, комиссия признала их достаточными, выполненными на уровне требований Технического задания и договорных обязательств, и сочла возможным приступить к приемке АСУТП в опытную (промышленную) эксплуатацию. Комиссия провела испытания предъявленной Системы, и установила:

1. Технические средства РСУ, ПАЗ и полевого оборудования поставлены в полном объеме согласно Спецификации к Договору YNF-1234/01;
2. Разработанная документация технорабочего проекта поставлена в полном объеме согласно Приложению №6 к Договору YNF-1234/02;
3. Техническое обеспечение, системное и прикладное программное обеспечение функционируют в соответствии с Договором на разработку и внедрение АСУТП YNF-1234/03;
4. АСУТП в целом выдержала испытания с положительным результатом.

Заключение и рекомендации комиссии:

- Наладка систем РСУ, ПАЗ и полевого оборудования АСУТП выполнена с хорошим качеством и в полном объеме.
- АСУТП в целом соответствует требованиям Технического задания и условиям Договоров:

- На поставку оборудования YNF-1234/01;
- На разработку ТРП YNF-1234/02;
- На разработку и внедрение АСУТП YNF-1234/03.

- Считать АСУТП производства АВС принятой в опытную (промышленную) эксплуатацию.
- Установить срок проведения опытной эксплуатации с по 2010 года.
- Замечания и предложения, выявленные в процессе наладки Системы, и переданные в адрес Организации-разработчика АСУТП, должны быть внесены в Техно-рабочий проект, и переданы в адрес Заказчика в срок до 01.01 2010 года.
- Замечания, требующие согласования с проектной организацией, Заказчик должен согласовать с проектной организацией и передать в срок до 01.01 2010 года в адрес Разработчика АСУТП.
- Организация-разработчик АСУТП должна внести соответствующие изменения в Техно-рабочий проект, и передать в адрес Заказчика в срок до 01.01 2010 года (до передачи АСУТП в промышленную эксплуатацию).

Приложения:

1. Программа испытаний;
2. Протоколы и Отчеты испытаний по пунктам проверок Программы испытаний;
3. Протокол результатов испытаний;
4. Акт приемки в опытную эксплуатацию;
5. Акт о завершении работ по проверке АСУТП в режиме опытной эксплуатации, с заключением о предъявлении АСУТП на приемочные испытания, либо
6. Акт о вводе АСУТП в промышленную эксплуатацию.

Председатель
комиссии:
(Ф. И. О.) (Подпись) (Дата)
Члены комиссии:
(Ф. И. О.) (Подпись) (Дата)

8.15. ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ НА ПЛОЩАДКЕ ПОСТАВЩИКА

Целью данного документа является определение процедуры проведения приемочных испытаний основного оборудования АСУТП - РСУ и ПАЗ - на площадке поставщика АСУТП в соответствии с процедурой приемки системы, изложенной в документации изготовителя оборудования РСУ и ПАЗ, и поставщика АСУТП *(указываются ссылки на конкретные документы).*

8.16. Внутреннее тестирование поставщика

Для проверки всех частей системы перед проведением приемочных испытаний в присутствии заказчика, на площадке поставщика должно быть проведено внутреннее тестирование. При этом должна тестироваться **каждая составляющая** аппаратного и программного обеспечения. Испытания будут проводиться специалистами изготовителя (разработчика) системы, контролироваться и координироваться специалистами поставщика в присутствии специалистов поставщика системы и заказчика.

Устанавливается следующий порядок взаимодействия участников испытаний:

Заказчик => Поставщик => Изготовитель (разработчик) системы.

И наоборот:

Изготовитель (разработчик) системы => Поставщик ==> Заказчик.

Таким образом, во избежание недоразумений непосредственное решение вопросов рекомендуется для тех сторон, которые имеют взаимные договоры.

Для выполнения процедур тестирования оборудование должно быть полностью смонтировано, подключено и включено в сеть.

Перечень тестов внутреннего тестирования приведен ниже.

Объем внутреннего тестирования. Процедура внутреннего тестирования должна включать в себя следующие группы испытаний в соответствии с документацией детального (технорабочего) проекта:

1. ТЕСТИРОВАНИЕ ОБОРУДОВАНИЯ:

- Проверка состава проектной документации, необходимой для проведения испытаний на площадке поставщика;
- Визуальный осмотр и контроль размеров по каждому устройству;
- Объем поставки;
- Проверка возможности легкого доступа и извлечения компонентов;
- Внешние дефекты;
- Проверка маркировок;
- Проверка монтажного соединения с внешними устройствами;
- Проверка монтажного соединения с внешними системами;
- Проверка системы вентиляции;
- Проверка источников питания системы;
- Отключение / включение питания и перезагрузка;
- Проверка цепей заземления;
- Тест приложенного напряжения;
- Тест сопротивления изоляции;
- Проверка функций системной диагностики;
- Проверка версий стандартного программного обеспечения;
- Проверка операторских станций;
- Проверка станций управления.

2. ТЕСТИРОВАНИЕ ВВОДА-ВЫВОДА.

Для каждого канала ввода-вывода проводятся следующие проверки:

- Проверка правильности монтажной разводки по терминальным панелям;
- Проверка соответствия адресов аппаратного и программного обеспечения;
- Проверка идентификаторов позиций;
- Проверка корректной установки шкал и пределов срабатывания сигнализации;
- Проверка сообщений сигнализации;
- Проверка контуров регулирования, клапанов и цепей электроприводов.

3. ТЕСТИРОВАНИЕ ОПЕРАТОРСКОГО ИНТЕРФЕЙСА И МНЕМОСХЕМ:

- Проверка контроля уровней доступа;
- Проверка работоспособности функций, определенных для операторских станций;
- Проверка расположения статических и динамических элементов, включая изменение цвета и отображение данных;
- Тестирование правильности работы мнемосхем.

Тестирование мнемосхем заключается в проверке расположения статических и динамических элементов, включая изменение цвета и отображение данных, и в тестировании правильности работы мнемосхем:

- Группы управления;
- Обзорные панели;
- Группы трендов (графики изменения параметров во времени);
- Функциональные клавиши.

4. ТЕСТИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОЙ СВЯЗИ (MODBUS) С КОНТРОЛЛЕРАМИ СИСТЕМЫ ПАЗ И С ПЛК КОМПЛЕКТНЫХ АГРЕГАТОВ:

Проверка соответствия функций связи техническим требованиям; Контроль функциональности с использованием реальных программируемых логических контроллеров системы ПАЗ и ПЛК для блоков комплектной поставки, или соответствующих имитаторов, и таблиц распределения памяти.

5. ТЕСТИРОВАНИЕ ЛОГИЧЕСКИХ СХЕМ СИСТЕМЫ ПАЗ:

Проверка логических схем противоаварийной защиты (блокировок) на соответствие проектной документации. Процедура тестирования должна выполняться с использованием панелей аппаратного моделирования ситуаций, подключенных к системе ESD.

6. ТЕСТИРОВАНИЕ КОМПЛЕКСНЫХ КОНТУРОВ (КОНТУРОВ УСОВЕРШЕНСТВОВАННОГО УПРАВЛЕНИЯ):

Проверка функционирования комплексных контуров на соответствие проектной документации. Процедура тестирования должна выполняться с использованием тестового

программного обеспечения для имитации (моделирования) сигналов ввода-вывода.

8.17. Объем испытаний в присутствии заказчика

Данный вид тестирования служит для проверки соответствия сконфигурированной АСУТП (РСУ и ПАЗ) специфическим требованиям заказчика и техническим требованиям к проекту.

Испытания проводятся специалистами изготовителя (разработчика), контролируются и координируются специалистами поставщика системы в непосредственном присутствии специалистов поставщика системы, и заказчика. Процедура тестирования в присутствии заказчика выполняется по тому же принципу, что описанная выше процедура внутреннего тестирования. Основная цель - обеспечить полноту тестирования, начиная с самого нижнего уровня для того, чтобы продемонстрировать целостность системы. Процедура тестирования составлена в соответствии с техническими требованиями к системе, которые определены проектными спецификациями.

Для регистрации результатов необходимо использовать рекомендованные формы протоколов, а сбои и возникшие проблемы должны быть зафиксированы в списке проблем, и подробно изложены в отчетах. Образцы приведены в конце данного документа (см. таблицы 8.7-8.9). Установлены следующие критерии приемки:

- ДА - Принято заказчиком;
- НЕТ - Отклонено заказчиком.

Перед повторным запуском теста должны быть скорректированы и исправлены все проблемы, ставшие причиной отклонения результатов тестирования.

8.18. Процедура (методика) испытаний

В последующих разделах данной Программы подробно рассматриваются методики тестирования для каждого конкретного теста. Перечень всех тестовых испытаний приведен в Таблице 8.7. Описание каждого тестового испытания подразделяется на три части:

- Цель и объем испытаний;

- Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке;
- Критерии приемки.

По окончанию испытаний по каждому тесту составляется отчет с результатами испытаний.

1. ТЕСТИРОВАНИЕ ОБОРУДОВАНИЯ.

Аппаратное обеспечение должно быть проверено на соответствие спецификации оборудования, которая представлена в контрактной спецификации. Процедура тестирования должна включать в себя нижеследующие тесты.

1) Проверка состава проектной документации, необходимой для проведения испытаний на площадке поставщика.

Цель и объем испытаний.

Проверка наличия проектной документации по аппаратному и программному обеспечению соответствующих версий для обеспечения приемочных испытаний.

Методика выполнения и оборудование или устройства. подлежащие проверке.

Визуальная проверка в соответствии с системной спецификацией.

Критерии приемки.

Все документы должны проверяться в соответствии с перечнем проектной документации.

2) Визуальный осмотр и контроль размеров по каждому устройству.

Цель и объем испытаний.

Визуальная проверка внешних и внутренних дефектов (например, деформации и загрязнение), а также сверка основных внешних параметров со спецификацией производителя.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

- Визуальный осмотр на наличие внешних дефектов и проведение реальных измерений внешних параметров (см. техническую документацию по оборудованию системы, руководство по инсталляции, и проектную документацию);
- Визуальный осмотр системы и расположения стоек;

- Визуальный осмотр по плотности расположения и проверка монтажа.

Критерии приемки.

Все компоненты должны проверяться согласно списку системных компонентов. Необходимо проверить внешние размеры одного компонента каждого типа.

3) Объем поставки.

Цель и объем испытаний.

Проверка комплектности системы.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Проверка объема поставки согласно контракту.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

4) Проверка возможности легкого доступа и извлечения компонентов.

Цель и объем испытаний.

Проверка возможности проведения текущего обслуживания и замены следующих модулей:

- Сменные модули (процессор, блоки питания, модули ввода-вывода и т.д.);
- Контроль просвета, допустимого для обеспечения возможности легко устанавливать и извлекать компоненты;
- Терминальные панели;
- Проверка возможности быстро подойти к терминальной панели и беспрепятственно провести техническое обслуживание или замену.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Подойти и заменить компоненты.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

5) Внешние дефекты.

Цель и объем испытаний.

Общая проверка того, что на оборудовании отсутствуют дефекты, и оно соответствует соответствующим стандартам.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Визуальный осмотр на предмет внешних дефектов

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

6) Проверка маркировок.

Цель и объем испытаний.

Проверка наличия соответствующих маркировок для модулей и компонентов:

- Стойки (бирка с указанием имени клиента);
- Кабели (тип, номер);
- Разъемы;
- Терминальные блоки;
- Монтажные рамы.

7) Проверка монтажного соединения с внешними устройствами.

Цель и объем испытаний.

Проверка того, что каждое устройство (шлюзы, коммутаторы, принтеры и т.д.) подключено в соответствии с проектной документацией.

8) Проверка монтажного соединения с внешними системами.

Цель и объем испытаний.

Проверка того, что в системе предусмотрено аппаратное соединение для последовательного канала связи с внешними системами (контроллерами комплектных агрегатов).

Методика выполнения (процедура) и оборудование или устройства> подлежащие проверке.

Визуальная проверка того, что в системе предусмотрено аппаратное обеспечение для последовательного канала связи с внешними системами.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

9) Проверка системы вентиляции.

Цель и объем испытаний.

Проверка функционирования, механической и электрической защиты.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

- Функционирование: запуск и остановка каждого вентилятора;
- Механическая защита;
- Электрическая защита.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

10) Проверка источников питания системы.

Цель и объем испытаний.

Проверка того, что каждый из компонентов можно запитать через силовой переключатель или силовой разъем.

Методика выполнения (процедура) и оборудование или устройства> подлежащие проверке.

Для станции оператора проверка проводится по следующим этапам:

a) Выключить источник электропитания одной операторской станции;
b) Проверить, отобразится ли соответствующее сообщение системной сигнализации на других операторских станциях;
c) Включить источник электропитания одной операторской станции;
d) Проверить, подключилась ли эта станция к системе;
e) Через системное меню подтвердить соответствующее сообщение сигнализации;
f) Сделать то же самое для других станций.

Для станций управления (контроллеров) проверка проводится по следующей методике:

a) Подключить один сигнал к модулю ввода аналоговых сигналов и отобразить этот сигнал на рабочей станции;
b) Вывести тренд данного контура;
c) Отключить один из источников питания;
d) Проверить, отображается ли соответствующее сообщение сигнализации;
e) Проверить, изменился ли статус резервного источника со STANDBY на CONTROL;
f) Проверить, отразилось ли это на графике выбранного параметра;

g) Включить источник электропитания;
h) Проверить, изменился ли его статус на STANDBY после восстановления;
i) Через системное меню подтвердить соответствующее сообщение сигнализации;
j) Сделать то же самое для второго источника электропитания;
к) выключить одновременно оба источника электропитания;
1) Проверить, отображается ли соответствующее сообщение сигнализации;
ш) Включить оба источника электропитания.

Методика проверки электропитания для оборудования шины ввода-вывода:

a) Подключить один вход к модулю ввода аналоговых сигналов и вызвать соответствующий временной график (тренд);
b) Отключить один из двух разъемов источников электропитания;
c) Проверить, отображается ли соответствующее сообщение сигнализации;
d) Проверить, продолжает ли гореть лампочка индикации готовности каждой из карт ввода-вывода;
e) Проверить, отразилось ли это на панели временного графика;
f) Включить разъем источника электропитания;
g) Через системное меню подтвердить соответствующее сообщение сигнализации;
h) Сделать то же самое для второго разъема источника электропитания.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

11) Отключение / включение питания и перезагрузка.

Цель и объем испытаний.

- Демонстрация того, как выключить питание всей системы в безопасном и управляемом режиме;
- Демонстрация того, как включить питание всей системы в безопасном и управляемом режиме;

- Демонстрация того, как перезагрузить системную конфигурацию.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Провести отключение питания системы в следующем порядке:

a) Отключить питание всех блоков ввода-вывода;
b) Отключить питание всех станций управления;
c) Отключить питание всех операторских станций.

Провести включение питания системы в следующем порядке:

a) Последовательно подключить питание каждой операторской станции;
b) Последовательно подключить питание каждой станции управления;
c) Последовательно подключить питание каждой интерфейсной карты.

Провести перезагрузку системной конфигурации в следующем порядке:

a) С инженерной станции выполнить полную загрузку всех операторских станций;
b) С инженерной станции выполнить автономную загрузку всех станций управления.

Критерии приемки.

По окончанию всей процедуры на операторских станциях не должно быть сообщений о каких бы то ни было отказах.

12) Проверка цепей заземления.

Цель и объем испытаний.

Проверка цепей заземления.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Визуальный осмотр в соответствии документацией проекта для проверки того, что:

a) Цепь защитного заземления внутри стоек соответствует схемам проекта;
b) В каждом блоке предусмотрена возможность подключения защитного заземления;
c) Внутренняя сеть защитного заземления не имеет контуров;
d) Подключение блока к цепи защитного заземления выполнено надлежащим образом.

Критерии приемки.

Все компоненты должны проверяться согласно документации проекта.

13) Тест приложенного напряжения.

Цель и объем испытаний.

Проверка того, что электропитание системы обеспечено сертификатом, и соответствует требованиям нормативных документов по приложенному напряжению.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Предоставление сертификатов.

Критерии приемки.

Проверка сертификатов.

14) Тест сопротивления изоляции.

Цель и объем испытаний.

Проверка того, что сертификат проверки сопротивления изоляции соответствует техническим требованиям заказчика.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Предоставление сертификатов.

Критерии приемки.

Проверка сертификатов.

15) Проверка функций системной диагностики.

Цель и объем испытаний.

Проверка следующих функций диагностики:

- Диагностика отказа источника питания;
- Диагностика ошибок связи;
- Диагностика отказа резервного модуля;
- Диагностика отказа модуля ввода-вывода;
- Диагностика системы;
- Диагностика отказа релейной платы.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Состояния, приведенные ниже, должны быть указаны на страницах диагностики операторских станций:

a) Нарушение энергоснабжения (отключение одного источника питания);

b) Ошибка связи (отказ платы коммуникационного модуля);

c) Отказ резервного модуля;
d) Отказ модуля ввода-вывода (отключение одного из модулей);
e) Моделирование отказа релейной платы.

Критерии приемки.

На страницах операторских станций, посвященных системной диагностике, должен содержаться список соответствующих системных сообщений.

16) Проверка версий стандартного программного обеспечения.

Цель и объем испытаний.

Проверка наличия всех компонентов стандартного программного обеспечения соответствующих версий.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Проверка списка компонентов стандартного программного обеспечения по спецификации системных компонентов.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

17) Проверка операторских станций.

Цель и объем испытаний.

Проверка функционирования каждой операторской станции.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Для каждой операторской станции выполняется следующая процедура:

a) Проверить, что сигнализация на клавиатуре срабатывает при генерации случайного тревожного входа;
b) Проверить работу мыши и клавиатуры посредством доступа к мнемосхеме, и изменения задания контура регулирования;
c) Проверить подключение к шине передачи данных;
d) Отключить одну из резервированных шин и проверить, что на станции воспроизводится соответствующее системное сообщение и сигнализация, и что она продолжает работать в нормальном режиме резервной шины;
e) Восстановить подключение шины и проверить, что

сброшена тревожная сигнализация, и станция продолжает работать в нормальном режиме;

f) Повторить тест для другой шины;
g) Отключить обе шины данных и проверить, что на станции воспроизводится соответствующее системное сообщение и сигнализация, что нормальная работа невозможна, и что другие операторские станции генерируют сигнализацию;
h) Восстановить оба подключения шины и проверить, что нормальная работа восстановлена;
i) Отключить шину Ethernet и проверить, что операторская станция продолжает работать в нормальном режиме;
j) Восстановить подключение Ethernet и проверить, что станция работает в нормальном режиме.

Критерии приемки.

Все компоненты должны проверяться согласно документации проекта.

18) Проверка станций управления.

Цель и объем испытаний.

Проверка работоспособности каждой из станций управления (контроллеров). Станции управления - это контроллеры, построенные на базе стопроцентного резервирования всех основных компонентов:

- Модулей управления (процессоров);
- Модулей ввода-вывода;
- Источников питания;
- Скоростных шин.

Данные тесты предназначены для проверки того, что после удаления резервного элемента, станция управления (контроллер) будет продолжать работать.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Проверка резервирования модулей управления (процессоров):

a) Проверить функцию резервирования с помощью диагностики системы;
b) Выбрать вход и выход одного процессора;
c) Передать данные на вход и измерить состояние на выходе;

d) Отключить резервный процессор и проверить, что появилось сообщение сигнализации, но функционирование контролера продолжается;
e) Подключить резервный процессор и проверить, что сообщение сигнализации сброшено, и работа не прерывается;
f) Отключить основной процессор, и проверить, что появилось сообщение сигнализации, функционирование продолжается, и что теперь вспомогательный процессор замещает основной;
g) Подключить отключенный процессор и проверить, что сообщение сигнализации сброшено, работа не прерывается, и резервный процессор продолжает работать как основной.

Проверка резервирования шины передачи данных:

a) Проверить функцию резервирования с помощью системной диагностики;
b) Выбрать один вход и выход;
c) Передать данные на вход и измерить состояние на выходе;
d) Отключить одну шину передачи данных, и проверить, что появилось сообщение сигнализации, но функционирование продолжается;
e) Восстановить подключение и проверить, что сообщение сигнализации сброшено, а работа не прерывается;
f) Повторить процедуру для другого разъема шины передачи данных;
g) Отключить обе шины передачи данных, проверить, что появилось сообщение сигнализации, и что выход находится в аварийном режиме;
h) Восстановить оба соединения и проверить, что сообщение сигнализации сброшено, и функционирование восстановлено.

Проверка резервирования скоростной шины ввода-вывода:

a) Проверить функцию резервирования с помощью системной диагностики;
b) Выбрать вход и выход одного процессора;
c) Передать данные на вход и измерить состояние на выходе;

d) Отключить одну шину ввода-вывода, проверить, что появилось сообщение сигнализации, но функционирование продолжается;
e) Восстановить подключение, и проверьте, что сообщение сигнализации сброшено, а работа не прерывается;
f) Повторите процедуру для другого разъема шины передачи данных;
g) Отключить обе шины ввода-вывода, проверить, что появилось сообщение сигнализации, и что выход находится в аварийном режиме;
h) Восстановить оба соединения и проверить, что сообщение сигнализации сброшено, и функционирование восстановлено.

Критерии приемки.

Все компоненты должны проверяться согласно спецификации системных компонентов.

Дополнительно в процедуру приемочных испытаний на площадке поставщика должно включаться следующее:

a) Тест резервирования модулей ввода-вывода должен проводиться в обязательном порядке на 100%;
b) Должно проводиться тестирование резервирования оптоволоконной коммуникационной шины;
c) Проверка обнаружения утечки на землю;
d) Проверка сигнализации отключения автоматов питания;
e) Автоматическое включение/отключение света в стойке при открытии/закрытии двери;
f) Проверка термореле и пожарной сигнализации.

2. ТЕСТИРОВАНИЕ ВВОДА-ВЫВОДА.

Данный раздел посвящен детальному рассмотрению тестов, предназначенных для проверки того, что сконфигурированные для входы-выходы соответствуют проекту. Для регистрации результатов должны использоваться протоколы испытаний.

Все отказы или возникшие проблемы должны быть подробно описаны в отчетах о проблемах и зарегистрированы в списке проблем. Все протоколы испытаний имеют табличную форму, что обеспечивает возможность испытателю подтверждать каждый этап тестирования по мере его исполнения. Поскольку каждый пункт испытаний обозначен буквами, каждая

колонка в протоколе испытаний должна быть озаглавлена соответствующей буквой, и по завершению теста эта колонка должна быть заполнена.

Входы-выходы системы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Совпадения адресации аппаратного и программного обеспечения согласно таблицам расключения;
- Правильности функционирования (управляющие контуры/клапаны/двигатели) согласно таблицам расключения ввода-вывода;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

1) Проверка правильности монтажной разводки по терминальным панелям.

Цель и объем испытаний.

Проверить, что кабели проложены в соответствии с документацией по аппаратному обеспечению и что все кабели правильно промаркированы.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

a) Разводка по терминальным панелям:
   Проверить, что все провода, подходящие к колодке, установлены и разведены таким образом, чтобы разделить входную проводку от промаркированных входных сигналов и входную проводку от промаркированных выходов.
   Разводка по клеммным колодкам в кроссовых шкафах должна производиться с учетом типа кабеля и иметь маркировку входящего многожильного кабеля. Сигналы разных уровней напряжения должны быть по возможности разделены.
b) Разводка проводов по уровням напряжения:
   Проверить, что все провода, относящиеся к разным уровням напряжения, установлены и разведены таким образом, чтобы разделить внутреннюю проводку 220V переменного напряжения и внутреннюю проводку 5-24V постоянного напряжения.
c) Проверка кабелей:

Проверить, чтобы тип, размер, длина и цвет кабеля, в соответствии с условным обозначением цветового кода проводки системных чертежей, соответствовали проектной документации;

Проверить количество кабелей по технической документации;

Проверить правильность кабельных соединений с оборудованием;

Проверить, чтобы внешняя кабельная изоляция не была повреждена, особенно в критических зонах возможного износа;

Проверить степень заполнения лотков: согласно контракту провода должны лежать максимально плотно.

Все проверки включают в себя проведение визуального осмотра в соответствии с технической документацией.

2) Тестирование индивидуальных дискретных входов.

Цель и объем испытаний.

Данный тип контура имеет единичный цифровой вход для оповещения о состоянии оборудования.

Входы-выходы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно таблицам расключения входов-выходов;
- Правильности настроек сигнализации;
- Правильности графического представления.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием следующей процедуры:

a) Проверить правильность идентификации входного сигнала;

b) Начальное условие - входная цепь контура разомкнута;

c) Проверить на экране статус входного сигнала и под-

твердить правильность представления для разомкнутой цепи по месту;

d) Замкнуть цепь входа;
e) Проверить на экране статус входного сигнала и подтвердить правильность для закрытой цепи по месту;
f) Разомкнуть цепь входа;
g) Проверить на экране статус входного сигнала и подтвердить правильность для разомкнутой цепи по месту;
h) Проверить сигнализацию.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

3) Тестирование дискретных выходных каналов.

Цель и объем испытаний.

Данный тип сигнала имеет индивидуальный цифровой выход, генерируемый блокировкой.

Входы-выходы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (документ СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (то есть управляющие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц (если используется).

Методика выполнения (проиедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием следующей процедуры:

a) Проверить правильность идентификатора выходного сигнала;
b) Проверить наличие в соответствующей блокировке;
c) Начальное условие - на операторской консоли выход отключен (OFF);
d) Проверить выходные контакты и подтвердить правильность состояния выхода - OFF (то есть открытой цепи);

e) Установить выход на операторской консоли в состояние ON (включить);
f) Проверить терминалы выходов и подтвердить правильность состояния выхода - ON (то есть закрытой цепи);
g) Установить выход на операторской консоли в состояние OFF (выключить);
h) Проверить терминалы выходов и подтвердить правильность состояния выхода - OFF (то есть открытой цепи).

Критерии приемки.

Должны быть удовлетворены все указанные условия.

4) Тестирование модулей дискретного входа.

Цель и объем испытаний.

Входы-выходы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования (то есть управляющие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Графического представления.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием следующей процедуры:

a) Проверить правильность идентификатора входного сигнала;
b) Начальное условие - цепь контура разомкнута;
c) Проверить на экране статус входного сигнала и подтвердить правильность для открытой цепи по месту;
d) Замкнуть цепь входа;
e) Проверить на экране статус входного сигнала и подтвердить правильность для закрытой цепи по месту;
f) Разомкнуть цепь входа вход;
g) Проверить на экране статус входного сигнала и подтвердить правильность функционирования для разомкнутой цепи по месту.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

5) Тестирование модулей аналогового ввода.

Цель и объем испытаний.

Стандартная индикация сигнала технологической переменной используется в том случае, когда требуются только функции отображения и сигнализации.

Входы-выходы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расключения входов-выходов;
- Правильности функционирования и принадлежности (контуры/клапаны/двигатели) согласно распределению входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием нижеследующей процедуры:

a) Проверить правильность диапазона физических единиц и их идентификации;
b) Начальное условие - цепь входа разомкнута;
c) Проверить на экране статус входа и подтвердить правильность для открытого контура на месте (то есть появляется сообщение сигнализации обрыва цепи);
d) Подать на вход сигналы следующих значений: 4mA, 12mA и 20mA;
e) По каждому уровню входного сигнала подтвердить правильность соответствующего значения физической единицы и то, что любая сигнализация срабатывает при правильном значении (это можно сделать посредством проверки пределов сигнализации в конфигурации);
f) Проверить следующие виды сигнализаций:
   - Высокий-высокий (HH) и высокий (H);
   - Низкий-низкий (LL) и низкий (L).

Примечание

Согласно данным ранее определениям, HH и LL соответствуют предаварийным значениям, а H и L — предупредительным.

g) Разомкнуть входную цепь и проверить сигнализацию обрыва цепи;

h) Ввести значение больше 100% и проверить, что срабатывает сигнализация, указывающая на превышение диапазона значений.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

6) Регуляторы ручного управления (задатчики).

Цель и объем испытаний.

Стандартные средства ручного задания используются в случае, когда необходимо средство изменения выходных сигналов, но собственно функция управления (регулирования) не требуется.

Входы-выходы должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению входов-выходов;
- Правильности функционирования и принадлежности (управляющие контуры/клапаны/двигатели) согласно таблицам расключения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц (если используется).

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием нижеследующей процедуры:

a) Проверить правильность диапазона физических единиц и их обозначения;

b) Начальное условие - цепь выхода разомкнута;

c) Проверить на экране статус выхода и подтвердить правильность сигнализации открытого контура;

d) Проверить, чтобы в цепи выходов было установлено правильное значение для выходного сигнала контура - 0%;

e) Установить выходной сигнал контура в 25%, 50%, 75% и 100%. Проверить работу сигнализаций:
   - Высокий-высокий (HH) и высокий (H);
   - Низкий-низкий (LL) и низкий (L);
   - Разомкнуть цепь входа и проверить соответствующую сигнализацию;
   - Разомкнуть цепь выхода и проверить соответствующую сигнализацию.

f) Разомкнуть цепь выхода и проверить соответствующую сигнализацию.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

7) Блоки стандартного ПИД - регулирования (регулятор типа PID-1).

Цель и объем испытаний.

Стандартное ПИД-регулирование заключается в изменении управляющего выходного сигнала в случае расхождения между технологической переменной PV и заданным значением SV, введенным оператором, или системой усовершенствованного управления.

Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно таблицам расклюючения входов-выходов;
- Правильности функционирования (то есть управляющие контуры/клапаны/двигатели) согласно таблицам расклюючения входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц (если используется).

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием следующей процедуры:

a) Проверить правильность диапазона физических единиц входа и их описания;

b) Начальное условие - режим контура MANUAL (ручной), цепь входов разомкнута, установить контроль-

ную точку 0% диапазона, выходные сигналы контура 0%;

c) Проверить работу контура (то есть проверить статусы открытый/закрытый, обратный/прямой);
d) Проверить, чтобы в цепи выходов было установлено правильное значение для выходного сигнала контура **0%;**
e) Проверить сигнализацию обрыва аналогового входа;
f) Подать на вход сигналы следующих значений: 4мА, 8м А, 12мА, 16мА и 20мА;
g) По каждому уровню входного сигнала подтвердить правильность соответствующего значения физической единицы и то, что любая сигнализация срабатывает при правильном значении (это можно сделать посредством проверки пределов сигнализации в конфигурации);
h) Проверить следующие сигнализации:
   - Высокий-высокий (HH) и высокий (H);
   - Низкий-низкий (LL) и низкий (L);
   - Сигнализация о превышении допустимого отклонения от задания;
   - Разомкнуть цепь входа и проверить сигнализацию обрыва;
   - Разомкнуть цепь выхода и проверить сигнализацию обрыва.
i) Ввести значение больше 100% и проверить, что срабатывает сигнализация, указывающая на превышение диапазона значений;
j) Установить выходной сигнал контура в 25%, 50%, 75% и 100%;
к) Разомкнуть цепь выхода и проверить сигнализацию;
1) Установить входной сигнал в 50%, и выходной в 50%. Установить задание в 75%. Перевести контур в режим AUTO (автоматический), и проверить, что нарастание / понижение выходного сигнала происходит в соответствии с требованиями.

Критерии приемки

Должны быть удовлетворены все указанные условия.

8) Блоки стандартного ПИД - регулирования с передачей значения технологической переменной на вычислительный блок (регулятор типа PID-2).

Цель и объем испытаний.

Стандартное ПИД-регулнрованне заключается в изменении управляющего выходного сигнала в случае ошибки между технологической переменной PV и заданным значением SV, введенным оператором. Кроме того, переменная процесса PV используется в вычислениях вычислительного блока.

Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению вводов-выводов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно распределению вводов-выводов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Методика выполнения (проиедура) и оборудование или устройства, подлежащие проверке

Так же, как для блоков PID-1, но с проверкой на наличие в соответствующем блоке CALCU.

9) Блоки каскадного ПИД-регулирования (регуляторы типа PID-3).

Цель и объем испытаний.

Каскадное ПИД-регулирование заключается в изменении задания вторичного ПИД-регулятора.

Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению вводов-выводов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно распределению вводов-выводов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Так же, как для блоков PID-1, но с проверкой на участие в соответствующей блокировке.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

10) Блоки стандартного ПИД - регулирования с получением значения технологической переменной из вычислительного блока (регулятор типа PID-4).

Цель и объем испытаний.

ПИД-регулирование заключается в изменении управляющего выходного сигнала в случае ошибки между технологической переменной PV и заданным значением SV, введенным оператором. Регулируемый параметр процесса рассчитывается через другой программный вычислительный блок. Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению вводов-выводов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно распределению вводов-выводов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц (если используется).

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Так же, как для блоков PID-1, но с проверкой передачи в соответствующий вычислительный блок.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

11) Блоки регулирования соотношения (RATIO).

Цель и объем испытаний.

Стандартное регулирование соотношения - это модуляция выходных управляющих сигналов в случае ошибки между связанным параметром процесса и неуправляемым потоком.

Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению входов-выходов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно распределению входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Тестирование проводится с использованием следующей процедуры:

b) Проверить правильность диапазона физических единиц входа и их описания;
c) Начальное условие - режим контура MANUAL (ручной), входные сигналы 0%, установить заданное значение в 0% диапазона, выходные сигналы контура в 0%;
d) Проверить работу контура (повысить выходной сигнал, изменить заданное значение, коэффициент усиления, смещение);
e) Проверить, чтобы цепи выходных сигналов были установлены в правильное значение для выходного сигнала контура 0%.
f) Установить режим контура AUTO (автоматический);
g) Последовательно установить входной сигнал в 0%, 25%, 50%, 75% и 100%;
h) Для каждого значения выходного сигнала удостовериться, что на выходе устанавливается правильное значение выходного сигнала;
i) Проверить, чтобы выходной сигнал нарастает или ослабевает в соответствии с заданием;
j) Проверить следующие состояния сигнализации:
    - Высокий-высокий (HH) и высокий (H);
    - Низкий-низкий (LL) и низкий (L);
    - Разомкнуть цепь входных сигналов и проверить сигнализацию обрыва;
    - Разомкнуть цепь выходных сигналов и проверить сигнализацию обрыва.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

12) Блоки регулирования с разделением зоны регулирования (SPLIT- контроллер).

Цель и объем испытаний.

Стандартное **SPLIT**-регулирование включает в себя модуляцию двух выходных сигналов с разделением диапазона в случае ошибки между переменной процесса и заданным значением. Входы-выходы контура должны тестироваться с использованием Перечней входов-выходов (В1) и (В2) и схем контуров (СБ) в целях проверки:

- Правильности адресации аппаратного и программного обеспечения согласно распределению входов-выходов;
- Правильности функционирования (контуры / клапаны / двигатели) согласно распределению входов-выходов;
- Настроек сигнализации;
- Графического представления;
- Физических единиц.

Методика выполнения (проиедура) и оборудование или устройства, подлежащие проверке.

Так же, как для блоков PID-1, но с проверкой правильности модуляции между двумя выходными сигналами через стандартный блок разделения сигналов.

Критерии приемки.

Должны быть удовлетворены все указанные условия.

3. ТЕСТИРОВАНИЕ ОПЕРАТОРСКОГО ИНТЕРФЕЙСА И МНЕМОСХЕМ.

На данном этапе подробно производятся все действия, необходимые для проверки того, что графические панели, контрольные группы, обзорные панели, изменения, отчеты и конфигурация системы соответствуют требованиям пользователя и техническим требованиям к проекту. Процедура тестирования должна включать в себя следующие тесты:

1) Тестирование мнемосхем.

Цель и объем испытаний.

Целью тестирования мнемосхем является проверка правильности представления графического отображения для оператора процесса как статических, так и динамических элементов.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

После восстановления на операторской станции соответствующей графической страницы, проверяется ее соответствие монтажно-технологическим схемам.

Критерии приемки.

Все перечисленные выше условия должны быть удовлетворены. Любые отклонения должны утверждаться инспектором заказчика.

Отдельно проверяется

2) Время вызова и обновления видеоизображений.

Цель и объем испытаний.

Проверить, что время вызова и обновления видеоизображений - не более 2-х секунд.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

После восстановления на операторской станции какой-либо графической страницы, необходимо проверить, что другая страница полностью проявится на экране не более, чем через 1 секунду

Динамически обновляемые значения должны обновляться с частотой 1 раз в секунду.

Критерии приемки.

Все перечисленные выше условия должны быть удовлетворены. **Любые отклонения должны утверждаться инспектором заказчика.**

3) Группы управления.

Цель и объем испытаний.

Целью тестирования групп управления является проверка правильности представления графического отображения для оператора процесса как статических, так и динамических элементов для контрольных групп.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Необходимо вызвать специфицированные контрольные группы и выполнить проверку на наличие требуемых изображений лицевых панелей приборов.

Критерии приемки.

В каждой группе должны содержаться требуемые изображения лицевых панелей приборов.

4) Обзорные панели.

Цель и объем испытаний.

Целью тестирования обзорных панелей является проверка правильности представления графического отображения для оператора процесса как статических, так и динамических элементов на обзорных панелях.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Необходимо вызвать специфицированные обзорные панели и выполнить проверку.

Критерии приемки.

Должны быть представлены и проверены все обзорные панели.

5) Группы трендов (графики изменения параметров во времени).

Цель и объем испытаний.

Целью тестирования трендовых групп является проверка правильности представления графического отображения для оператора процесса как статических, так и динамических элементов на графиках параметров во времени.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Необходимо вызвать определенные групповые панели изменений и выполнить проверку на наличие требуемых переменных.

Критерии приемки.

Каждая группа должна содержать специфицированные переменные.

6) Функциональные клавиши.

Цель и объем испытаний.

Целью тестирования функциональных клавиш является проверка правильности представления графического отображения для оператора процесса в соответствии с функциональным назначением каждой клавиши.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Необходимо нажать все специфицированные функциональные клавиши и проверить их функции.

Критерии приемки.

(нойства *должны* соответствовать техническим требованиям.

4. ТЕСТИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОЙ СВЯЗИ (MODBUS) С КОНТРОЛЛЕРАМИ СИСТЕМЫ ПАЗ И С ПЛК КОМПЛЕКТНЫХ АГРЕГАТОВ.

Цель и объем испытаний.

Часть технологического оборудования имеет собственные программируемые логические контроллеры, предназначенные для управления и защиты конкретных агрегатов, таких как:

- Компрессоров;
- Пневмотранспорта;
- Связи с поточными хроматографами;
- Системы газообнаружения и пожаротушения.

В данном разделе подробно рассматриваются тесты, предназначенные для проверки связи с ПЛК системы ПАЗ, а также с ПЛК устройств и агрегатов через последовательные каналы, и передачи параметров, которые должны конфигурироваться в соответствии с требованиями пользователя и техническими требованиями к проекту. Тестирование должно проводиться с использованием программируемых логических контроллеров, поставляемых и сконфигурированного поставщиками данного комплектного оборудования, и специального стенда для моделирования ситуации, которую нельзя создать в случае отсутствия на момент проверки связи агрегата (блока) комплектной поставки.

Испытание последовательной связи осуществляется на производственном участке поставщика РСУ.

Поставщик агрегата комплектной поставки отправляет на площадку поставщика РСУ главную стойку ПЛК со всем оборудованием, необходимым для испытаний последовательного протокола обмена данными между АСУТП и данным ПЛК:

- Сконфигурированный ПЛК;
- Локальная панель управления агрегатом (блоком) комплектной поставки;
- Коммуникационные платы;
- Блоки питания.

Методика выполнения (процедура) и оборудование или устройства. подлежащие проверке.

Тест, указанный выше, проводится следующим образом:

- Проверить связь по каждой линии;
- Проверить работоспособность резервирования:

  Удалить сетевую плату №2 из гнезда, и проверить на панели представления индикацию аварийного состояния и проверить целостность данных. Изменить данные, как указано выше, и проверить соответствующее изменение в месте назначения;

  Установить сетевую плату №2 и удалить плату №1. Повторить процедуру проверки целостности данных.
- Проверить соответствие передаваемых данных (Memory Map) по каждой линии.

Критерии приемки.

- Система связи сконфигурирована правильно;
- Сконфигурированы все сигналы, указанные в таблицах распределения памяти;
- Все передаваемые данные воспроизводятся правильно.

Полноценная проверка возможна только в случае наличия соответствующего PLC от поставщика агрегата.

При отсутствии PLC во время проведения приемочных испытаний, сигналы, передаваемые с помощью ПЛК, должны моделироваться посредством функции тестирования РСУ или основной системы ПАЗ.

5. ТЕСТИРОВАНИЕ ЛОГИЧЕСКИХ СХЕМ СИСТЕМЫ ПАЗ.

В данном разделе подробно рассматриваются тесты, предназначенные для проверки того, что блокировки, сконфигурированные для системы, соответствуют требованиям пользователя и техническим требованиям к проекту.

Процедура тестирования должна выполняться с использованием панелей аппаратного моделирования ситуаций, подключенных к системе ПАЗ.

Блокировка - непрерывно работающая логика, которая позволяет предотвратить возникновение аварийных ситуаций.

Блокировки, как правило, работают независимо от других приложений, однако в системе должна существовать возможность установки деблокирующих ключей.

Цель и объем испытаний.

Данные тесты позволяют проверить функционирование блокировок в соответствии с требованиями спецификаций конечного пользователя посредством систематического создания аварийных условий и проверкой статуса выходных сигналов. Данные тесты не следует проводить одновременно с другими видами испытаний.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Функционирование этих логических схем должно проверяться посредством симулирования входных сигналов системы при максимально полной конфигурации и посредством мониторинга статуса-значения выходных сигналов.

Данный тест должен выполняться с помощью панелей аппаратного моделирования, подключенных к включенным вводам-выводам.

Кроме проверки поведения логической схемы данный тест позволит проконтролировать функционирование операторского интерфейса, связанного с логическими схемами блокировок (последовательность зарегистрированных событий, сигнализации и т.д.).

Критерии приемки.

Логические схемы блокировок должны соответствовать проектной спецификации.

6. ТЕСТИРОВАНИЕ КОМПЛЕКСНЫХ КОНТУРОВ (КОНТУРОВ УСОВЕРШЕНСТВОВАННОГО УПРАВЛЕНИЯ).

В данном разделе подробно рассматриваются тесты, предназначенные для проверки того, что комплексные контуры, сконфигурированные для системы, удовлетворяют требованиям пользователя и техническим требованиям к проекту.

Процедура тестирования должна выполняться с использованием программного обеспечения по тестированию для моделирования ввода-вывода на месте.

Цель и объем испытаний.

В результате данных тестов проверяется работа комплексных контуров согласно спецификации требований пользователей. В ходе данных тестов не следует сочетать их с каким-либо другим приложением.

Методика выполнения (процедура) и оборудование или устройства, подлежащие проверке.

Должна использоваться следующая общая процедура тестирования:

- По спецификации комплексных контуров продумайте вероятное поведение контура.
- Проверить поведение контура в какой-либо возможной ситуации.
- Отметить проверенные компоненты контура в спецификациях с указанием фамилий специалистов, проводивших испытания, и даты.
- После того, как один контур будет полностью протестирован, проставить на соответствующей странице фамилии и дату.
- Повторить процедуру для каждого элемента контура.

Критерии приемки.

Характеристики контуров должны соответствовать проектной спецификации.

Таблица 8.7

Перечень тестовых испытаний

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведе-ния теста	Статус теста: успешно ДА/НЕТ
1.	ТЕСТИРОВАНИЕ ОБОРУДОВАНИЯ		
1.1	. Проверка состава проектной документации, необходимой для проведения испытаний на площадке поставщика		
1.2	Визуальный осмотр и контроль размеров по каждому устройству		
1.3	Объем поставки		
1.4	Проверка возможности легкого доступа и извлечения компонентов		
1.5	Внешние дефекты		
1.6	Проверка маркировок		
1 7	Проверка монтажного соедине-ния с внешними устройствами		
1.8	Проверка соединения и совместимости внешних систем		
1.9	Проверка системы вентиляции		
1 10	Проверка источников питания системы		

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведе-ния теста	Статус теста успешно і ДА/НЕТ
1.11	Отключение / включение питания и перезагрузка		
1.12	Проверка цепей заземления	»	
1.13	Тест приложенного напряжения		
1.14	Тест сопротивления изоляции		
1.15	Проверка функций системной диагностики	:	
1.16	; Проверка версий стандартного программного обеспечения		
1.17	Проверка операторских станций		
1.18	Проверка станций управления		

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата проведе-ния теста	Статус теста: успешно ДА/НЕТ
2.	**ТЕСТИРОВАНИЕ ВВОДА-ВЫВОДА**		
2.1	**Проверка правильности монтажной разводки по терминальным панелям**	.	
2.2	**Тестирование индивидуальных дискретных входов**		
2.3	**Тестирование дискретных выходных каналов**		
2.4	**Тестирование модулей дискретного входа**		
2.5	**Тестирование модулей аналогового входа**		
2.6	**Регуляторы ручного управления (за датчики)**		
2.7	**Блоки стандартного ПИД - регулирования (регулятор типа РЮ-1)**		
2.8	**Блоки стандартного ПИД - регулирования с передачей значения технологической переменной на вычислительный блок (регулятор типа PID-2)**	.	

Наименование теста	Дата проведе-ния теста	Статус теста, успешно ДА / НЕТ
Блоки каскадного ПИД - регулирования (регулятор типа PID-3)		
Блоки стандартного ПИД - регулирования с получением значения технологической переменной из вычислительного блока (регулятор типа PID-4)		
Блоки регулирования соотношения (RATIO)		
* Блоки регулирования 5 с разделением зоны ; регулирования , (SPLIT - контроллер)		
ТЕСТИРОВАНИЕ : ОПЕРАТОРСКОГО , ИНТЕРФЕЙСА И МНЕМОСХЕМ		
Тестирование мнемосхем		
Время вызова и обновления видеоизображений		
Группы управления		

Ссылка На раздел Программы и методики испытаний	Наименование теста	Дата ; проведе-ния теста	, Статус теста: успешно ДА/НЕТ
3.4	Обзорные панели		
3.5	Группы трендов (графики изменения параметров во времени)	; ;	
3.6	Функциональные клавиши		
4.	ТЕСТИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОЙ СВЯЗИ (MODBUS) С КОНТРОЛЛЕРАМИ СИСТЕМЫ ПАЗ И С ПЛК КОМПЛЕКТНЫХ АГРЕГАТОВ		
5.	ТЕСТИРОВАНИЕ ЛОГИЧЕСКИХ СХЕМ СИСТЕМЫ ПАЗ		
6.	ТЕСТИРОВАНИЕ КОМПЛЕКСНЫХ КОНТУРОВ (КОНТУРОВ УСОВЕРШЕНСТ-ВОВАННОГО УПРАВЛЕНИЯ)	.	

Таблица 8.8

Перечень отчетов о проблемах тестирования

Номер Отчета	Дата	Название	Статус
		:	

Таблица 8.9

Форма отчета о проблемах тестирования

Номер отчета	Ссылка на раздел Программы и методики испытаний	Дата	Описание

Описание проблемы:

Предпринятые действия:

Дата проведения теста	Успешно / Безуспешно	Подпись непосредственных исполнителей	Подпись ответственного лица

Глава 9

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ

9.1. Жизненный цикл системы безопасности

Началом жизненного цикла и основой проекта системы безопасности является **разработка Спецификации требований к системе безопасности.**

Спецификация требований состоит из:

- Функциональных требований безопасности;
- Интегральных требований безопасности.

Функциональные требования безопасности определяют:

- Логику и действия, которые должна выполнить система безопасности, и
- События на технологическом процессе, которые инициируют эти действия.

Эти требования также должны включать в себя такие позиции, как описание процедуры ручного останова, действия при исчезновении питания, и т.д.

Интегральные требования безопасности определяют:

- Интегральный уровень безопасности (SIL), и
- Исполнение системы безопасности, требуемое для осуществления функций защиты.

Интегральные требования безопасности включают:

- Требуемый интегральный уровень безопасности для каждой функции защиты;
- Требования к диагностике;
- Требования к обслуживанию и тестированию;
- Требования к надежности для исключения ложных срабатываний.

Особые требования. Часть требований оговаривается особо:

- Логическое устройство защиты должно быть обособлено от РСУ;
- Сенсоры системы безопасности должны быть отделены от сенсоров РСУ;
- Для всех главных компонент системы безопасности, включая датчики и исполнительные устройства, поставщик должен предоставить:
  - Данные по среднему времени наработки на отказ,
  - Данные по интенсивности появления выявленных отказов.
- Каждое полевое устройство должно иметь свою собственную линию связи с модулем ввода-вывода;
- Рекомендуется использование "интеллектуальных" датчиков, исполнительных устройств и протоколов HART и Fieldbus, чем обеспечивается расширенный уровень диагностики и тестовых испытаний полевого оборудования, и что приводит к радикальному повышению надежности системы. Однако **требование индивидуальных каналов взаимосвязи с полевым оборудованием системы защиты пока сохраняется;**
- Для объектов I и II категории взрывоопасное™ (по классификации, предложенной в настоящем руководстве, это 5-6 класс DIN, третий уровень SIL) использование одного запорно-регулирующего клапана и для РСУ, и для ПАЗ запрещается;
- Операторский интерфейс, в отличие от инженерного, не должен давать возможности изменить прикладное программное обеспечение системы безопасности;
- Если требуется проведение процедуры тестирования ПАЗ в рабочем, функционирующем состоянии *on-line,* тестовые процедуры должны быть встроены в систему безопасности при проектировании;
- Для обслуживания полевых устройств рекомендуется применение специальной выделенной системы обслуживания КИП - *Plant Asset Management System* - системы управления оборудованием производства.

9.2. Отказы общего порядка (общей причины)

Отказы общего порядка могут быть вызваны каким-либо единственным, нерезервированным компонентом системы, или общими систематическими ошибками в резервированных компонентах.

Некоторые из причин общих отказов включают:

- Ошибки спецификации;
- Ошибки проектирования оборудования;
- Дефекты при изготовлении оборудования;
- Ошибки программирования;
- Групповые линии связи с полевыми устройствами;
- Ошибки проектирования человеко-машинного интерфейса;
- Неблагоприятные условия окружающей среды (температура, влажность, давление, вибрация, коррозия);
- Отсутствие резервирования (единственные источники энергии, единичные полевые устройства, и т.п.);
- Ненадлежащая эксплуатация и техническое обслуживание.

Для уменьшения вероятности отказов общего порядка или систематических ошибок могут использоваться следующие методы:

- Резервирование;
- Разделение на подсистемы;
- Тестирование и проверка.

Функционально разделенные подсистемы ПАЗ могут использовать однотипное оборудование:

- интерфейс оператора,
- инженерный интерфейс,

поскольку эти подсистемы, как правило, требуют физического разделения

- источников питания,
- логического решающего устройства,
- модулей ввода-вывода,

и позволяют выполнять независимое тестирование или модификацию.

9.3. Ложные срабатывания

Ложные срабатывания и остановы процесса не только приносят убытки, но и в большинстве случаев представляют значительную опасность. Опыт показывает, что на процессах с большим количеством ложных сигналов технологический персонал теряет бдительность и реагирует на предупреждения с опозданием, или вовсе не реагирует на действительно аварийную ситуацию.

Примеры предпосылок для ложного срабатывания:

- Неправильная калибровка датчика;
- Нормально закрытые контакты имеют неожиданно высокое сопротивление;
- Отказ модуля ввода-вывода;
- Отказ микропроцессора;
- Отказ какого-либо электронного компонента полевого устройства.

Большое количество ложных событий связано со **сбоями питания** - электропитания и обеспечения киповским воздухом. Отсутствие резервных источников питания - ведущая причина ложных срабатываний. Например, потеря воздуха КИП - это всегда критическое событие на производстве, поскольку приводит не просто к ложному срабатыванию, но к аварийной ситуации. Другая частая причина ложных срабатываний - **оперативное техническое обслуживание в реальном времени,** - калибровка, тестирование полевых приборов, замена неисправных модулей, переключение кабеля и т.д.

9.4. Отказы полевых устройств

Многие общие причины сбоя систем защиты из-за отказа полевых устройств можно избежать с помощью правильно организованного резервирования. Примером такого решения может быть установка дополнительных сенсоров с другим принципом действия, или даже приборов других изготовителей. Для контроля критичных параметров могут быть использованы следующие варианты:

- Два аналоговых сенсора,
- Два дискретных сенсора (реле), или
- По одному каждого типа.

Однако надо иметь в виду, что если выбран третий вариант - одно аналоговое устройство и одно дискретное устройство, - то по сравнению с двумя однотипными устройствами теряется преимущество непрерывного сравнения сигналов. Правильность работы дискретного устройства может быть проверена с помощью тестирования, или в случае изменения состояния со стороны процесса. Если выбраны два различных аналоговых устройства, то их показания можно сравнивать непрерывно. Это сравнение значительно минимизирует среднее время обнаружения отказа, и таким образом обеспечивает более качественную защиту и повышает надежность системы.

Итак, следующие меры, относящиеся к полевым устройствам, способствуют повышению безопасности:

- Непрерывное сравнение показаний резервированных устройств в течение всего времени работы системы, приводящее к сигналу тревоги или останову процесса в случае слишком большого расхождения;
- Сравнение измеренных значений критических по отношению к безопасности параметров и других взаимосвязанных переменных процесса с последующей сигнализацией оператору процесса;
- При каждом предаварийном останове процесса - программный контроль показаний сенсоров на согласованность с предполагаемыми условиями останова. При этом должен осуществляться контроль над срабатыванием и положением клапанов по концевым выключателям;
- И непременное условие - сигнализация оператору процесса при любом нарушении регламентной процедуры останова технологического процесса;
- Все данные, которые поступают в РСУ из системы защиты, должны использоваться и отображаться на операторских станциях только по своему действительному, фактическому значению, и не должны подвергаться какой-либо дополнительной обработке или "интерпретации";
- Обязательное извещение оператора технологического процесса в случае, если исполнительный элемент системы защиты не выполнил команду переключения в течение предопределенного интервала времени;

- Обязательное извещение оператора технологического процесса в случае, если полевое устройство самопроизвольно изменило свое состояние без команды от системы защиты;
- Отслеживание данных оборудования по среднему времени наработки на отказ - MTTF, и между отказами - MTBF;
- Периодическое тестирование позиций, долгое время находящихся в неизменном состоянии;
- Идентификация, сигнализация и регистрация на РСУ всех событий, происходящих с системой защиты.

9.5. Резервирование как средство противодействия сбоям

Как сказано, система защиты может отказать одним из следующих способов:

"Безопасный" отказ - ложное срабатывание - возникает в том случае, когда система защиты функционирует, и от системы не требуется производить каких-либо действий по обеспечению безопасности, однако система производит беспричинный, немотивированный, неоправданный останов процесса, хотя на процессе никаких отклонений от регламента не произошло.

Опасный отказ - опасное НЕ срабатывание - возникает в том случае, когда система защиты не функционирует, или ее функции подавлены, хотя внешне это никак не проявляется. В результате система НЕ производит останова процесса, хотя это требуется. Отказы такого рода определяются только автономным тестированием.

Другой, очень перспективный вариант - тестирование в оперативном режиме путем частичного открытия-закрытия отсечных клапанов с помощью специальных систем обслуживания полевого оборудования.

Замечание

Приведенные далее рекомендации по резервированию одинаково относятся ко всем компонентам системы безопасности:

- *Сенсорам;*
- *Исполнительным элементам;*
- *Логическим устройствам.*

9.6. Общие рекомендации по выбору архитектуры

1. Одноканальные системы 1oo1 - ненадежны и небезопасны. Единственный промышленный вариант данной категории, сертифицированный по классу RC4 и SIL2 - система 1oo1D.
   В общем случае, необходимо избегать одноканальных систем для задач защиты и критичного управления - даже для объектов III категории взрывоопасности.
2. Дублированные системы с голосующей архитектурой "один отказ из двух возможных" (1oo2) могут быть безопасны, но имеют высокую интенсивность ложных срабатываний, то есть необоснованных остановов процесса:
   - Частота НЕ срабатывания (вероятность отказа выполнения требуемой функции - PFD) уменьшается (повышается безопасность), но зато
   - Интенсивность ложных срабатываний и, соответственно, беспричинных, немотивированных остановов по сравнению с архитектурой 1oo1 УДВАИВАЕТСЯ.
3. Дублированные системы с голосующей архитектурой "два отказа из двух возможных" - 2oo2 - имеют повышенную опасность:
   - Частота НЕ срабатывания, и риск возникновения аварийных ситуаций по причине НЕ срабатывания (вероятность отказа выполнения требуемой функции - PFD) по сравнению с архитектурой 1oo1 УДВАИВАЕТСЯ.
   - Однако уменьшается интенсивность и вероятность ложного срабатывания, и, соответственно, беспричинного останова процесса.
4. Системы 1oo2D, сочетающие достоинства систем 1oo2 и 2oo2, а также системы с тройным модульным резервированием 2oo3 с голосующей архитектурой "два отказа из трех возможных" обеспечивают приемлемый баланс безопасности и надежности.

   Системы 1oo2D и 2oo3 аттестуются по классам RC 5-6 и уровню безопасности SIL3.

9.7. Резервирование - однородное и альтернативное

Резервирование (избыточность) используется, чтобы обеспечить расширенную безопасность и увеличить устойчивость к отказам. Разработчик должен определить требования избыточности, чтобы достигнуть требуемого уровня безопасности и надежности для всех компонентов ПАЗ, включая сенсоры, логические решающие устройства, и конечные управляющие элементы.

Избыточность должна рассматриваться как применительно к аппаратным средствам, так и к программному обеспечению. Резервирование является эффективным средством борьбы с отказами общего порядка, общей причины - **с отказами единичных элементов системы** *(Common Cause Failure - CCF).* Устранение или уменьшение влияния источника сбоев, или использование резервирования на альтернативных аппаратных средствах, - методы, способные устранить отказы общего порядка.

При **альтернативном резервировании** используется другая технология, конструкция, другое системное программное обеспечение, прикладное программное обеспечение, чтобы уменьшить вероятность отказов общего порядка.

Альтернативное резервирование не должно использоваться в тех случаях, когда это связано с использованием компонентов с более низкой надежностью, которая не удовлетворяет системным требованиям по надежности.

Меры, которые могут использоваться для альтернативного резервирования, включают, но не ограничиваются следующими приемами:

- Использование различных типов измерений (например, давление и температура), когда известно соотношение между ними;
- Использование других технологий измерения той же самой переменной (например, диафрагма и вихревой расходомер);
- Использование различных типов контроллеров для каждого канала резервирования;
- Использование географического разделения (например, альтернативные маршруты для линий связи).

Типичные аспекты проектирования, при рассмотрении которых может быть использовано альтернативное резервирование, состоят в следующем:

- Аппаратные средства;
- Производители;
- Компоненты системы;
- Операционные системы;
- Каналы связи;
- Стандартное и прикладное программное обеспечение.

9.8. Разделение и распределение функций АСУТП

Разделение функций между РСУ и ПАЗ способно существенно уменьшить вероятность того, что обе функции АСУТП - и управляющие, и функции защиты станут недоступными одновременно, и что невнимательные или неквалифицированные действия персонала повлияют на выполнение функций защиты. Функциональное разделение РСУ и ПАЗ дает дополнительное преимущество за счет уменьшения вероятности систематических ошибок и влияния общих дефектов - показатель, особенно важный в приложениях I и II категории взрывоопасности для SIL3 и RC5-6.

Существует четыре области, где разделение функций особенно необходимо для удовлетворения требований функциональной безопасности АСУТП:

1) Полевые приборы (сенсоры);
2) Конечные исполнительные устройства;
3) Логические решающие устройства;
4) Связь между РСУ и ПАЗ.

Для каждой из этих четырех областей должен быть определен и обеспечен необходимый уровень требований безопасности.

9.9. Сенсоры

Объекты III категории взрывоопасности. Для объектов III категории взрывоопасности (SIL2 и RC4), как правило, чтобы обеспечить требуемый уровень безопасности, необходимо разделение функций и, соответственно, сенсоров между РСУ и ПАЗ.

Объекты I и II категории взрывоопасности. Для объектов I и II категории взрывоопасности (SIL3 и RC5-6), чтобы обеспечить требуемый уровень безопасности, необходимо полное разделение функций и, соответственно, сенсоров между РСУ и ПАЗ.

Некоторые рекомендации при выборе сенсоров:

- В общем случае аналоговые устройства предпочтительные дискретных;
- Там, где это оправдано, и где это возможно, нужно использовать резервирование или альтернативные способы получения данных, дублирующих свидетельство об одном и том же нерегламентированном событии;
- Устройства, которые выбраны в качестве альтернативных, должны иметь достаточную надежность, чтобы можно было считаться и с их показаниями;
- Каждый сенсор, определяющий безопасность процесса, должен иметь свою собственную (не групповую) связь с контроллером;
- Необходимо тщательно взвесить использование устройств, которые являются совершенно новыми в эксплуатационной истории завода;
- Сенсоры (трансмиттеры) должны иметь сертификацию на право использования в системах защиты данного класса.

9.10. Регулирующие и отсечные клапаны

Объекты III категории взрывоопасности. Для объектов III категории взрывоопасности (SIL2 и RC4) единственный запорно-регулирующий клапан может быть использован как для РСУ, так и ПАЗ, если соблюдены требования безопасности, то есть не возникает противоречия при выполнении функций управления и защиты.

Объекты I и II категории взрывоопасности. Для объектов I и II категории взрывоопасности (SIL3 и RC5-6) необходимо полное разделение функций и, соответственно, установка собственных клапанов РСУ и ПАЗ, чтобы обеспечить требуемый уровень безопасности.

Дополнительный запорно-регулирующий клапан может быть использован как для РСУ, так и ПАЗ, если соблюдены

требования безопасности, то есть исключены противоречия при выполнении функций управления и защиты. При использовании дополнительных клапанов, сигнализаторы положения этих клапанов могут быть подключены как к ПАЗ, так и РСУ, поскольку данная связь с РСУ не нарушает работу системы ПАЗ.

Исполнительные устройства должны иметь сертификаты на право использования в системах защиты данного класса.

Дополнительные условия, которые учитываются для определения требований к клапанам:

- Требования по времени отсечки;
- Надежность клапана;
- Возможные варианты отказов клапана.

Возможности диагностики существенно повышаются при применении "интеллектуальных" исполнительных элементов.

9.11. Логические решающие устройства (контроллеры)

Объекты III категории взрывоопасности. Для объектов III категории взрывоопасности (SIL2 и RC4), как правило, производится разделение функций РСУ и ПАЗ. Для объектов III категории взрывоопасности (SIL2 и RC4) по согласованию с территориальным органом технадзора для системы ПАЗ может быть использовано то же оборудование, что и для РСУ при условии, что система защиты обособлена от РСУ, и имеет необходимое резервирование:

- Модулей ввода-вывода;
- Центральных процессоров;
- Дублированные промышленные сети;
- Резервированные источники питания.

Существуют успешные примеры подобного применения однородного оборудования и программного обеспечения для реализации функций и управления, и защиты.

Авторское отступление. Centum. Фирма Йокогава является автором концепции распределенных систем управления. В 1975 году этой фирмой была выпущена первая в мире РСУ. И с тех пор, невзирая на все дешевые конфигурации типа одиозных ПЛК + СКАДА, или их новомодные и разнородные гибриды, фирма едва ли не в единственном

числе сохраняет приверженность уже ставшей классической концепции РСУ.

Первая из систем семейства Centum - Centum V - вышла в свет в 1982 году, и сразу привлекла внимание специалистов своей уникальной архитектурой с полным резервированием ВСЕХ компонентов системы:

- Шин управления;
- Шин ввода-вывода;
- Сетевых интерфейсов;
- Модулей ввода-вывода;
- Шин связи с модулями ввода-вывода;
- Источников питания;
- Станций управления.

При этом станция управления уже тогда имела уникальную четырехпроцессорную архитектуру 2*2 - ту самую, которую с таким энтузиазмом сегодня превозносят сторонники систем "2оо4"(см. рис.9.1). За прошедшие годы система прошла серьезный путь технических усовершенствований, но базовая концепция распределенных систем управления сохраняется: Система рассчитана на работу в жестком реальном времени, то есть ВСЕ ЗАЯВЛЕННЫЕ ХАРАКТЕРИСТИКИ СИСТЕМЫ обеспечиваются не "*по возможности*", а при любых обстоятельствах.

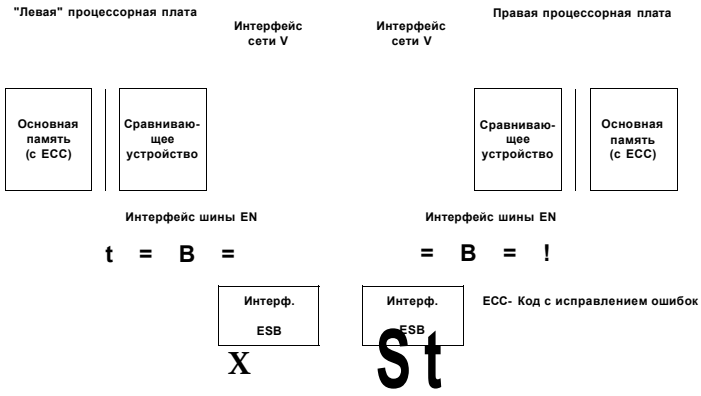


Рис. 9Л

В рамках заявленных ограничений производительность систем реального времени Centum НЕ ЗАВИСИТ от конкретной конфигурации оборудования и конкретной конфигурации прикладного программного обеспечения:

Система делает только то, что нужно, и только тогда, когда это нужно. Этим и определяется смысл, который мы вкладываем в понятие жесткого реального времени.

Проще говоря, в отличие от PLC + SCADA и гибридных систем с серверной организацией, коммутаторами и маршрутизаторами, то есть систем, у которых производительность впрямую зависит от конкретной реализации и катастрофически падает с увеличением информационной и операционной нагрузки на систему, классические распределенные системы Centum ВСЕГДА обеспечивают объявленную производительность в рамках объявленных ограничений. Эти границы настолько широки, что поражают воображение:

- 256 узлов в системе (64 домена по 16 узлов);
- 1,000,000 *(один миллион)* каналов ввода-вывода с частотой сканирования 1 раз в секунду;
- 2500 мнемосхем с частотой обновления 1 раз в секунду, и т.д. и т.п.

Приоритет и превосходство систем Centum в своем основном качестве распределенных систем управления общепризнанны. При этом все системы семейства сохраняют полную совместимость и преемственность.

Но совершенно очевидно и другое:

Возможности систем семейства Centum выходят далеко за рамки РСУ. Нет никаких препятствий к тому, чтобы использовать эти системы для обеспечения всего круга задач АСУТП в пределах единой программно-технической концепции - и РСУ, и ПАЗ. В качестве систем управления и противоаварийной защиты системы Centum представляют собой нечто гораздо большее, чем кем-то разрешенная "*неограниченная работа по любому классу требований*Самое поразительное состоит в том, что система со сто*ль* уникальным оборудованием и программным обеспечением не аттестована на соответствие определенному уровню западных требований безопасности RC или SIL. Понятно, что пускать на западный рынок мощнейшего конкурента с

лучшей системой управления и защиты просто так никто не намерен. К счастью, Ростехнадзор в данном случае проявил профессиональное отношение к делу:

Все системы семейства Centum: Centum CS, Centum CS 1000 и Centum CS 3000 имеют Разрешение Ростехнадзора на применение *"Для создания автоматизированных систем управления, противоаварийной защиты и сигнализации на химических, нефтехимических, нефтеперерабатывающих и других производствах и объектах, связанных с обращением или хранением взрывопожароопасных и токсичных веществ и смесей".*

Авторская позиция в данном случае полностью совпадает с позицией Госгортехнадзора: отсутствие суперсертификата TUV ни в коей мере не должно препятствовать применению систем семейства Centum в качестве однородных систем управления и противоаварийной защиты **в резервированном исполнении.**

Кстати говоря, аналогичная оценка дана системам Centum CS 1000 и Centum CS 3000 несколькими известными американскими и европейскими проектными и технологическими фирмами, работающими в нефтехимии и нефтепереработке.

Преимущества очевидны:

- Единая среда проектирования, разработки, конфигурирования;
- Единые промышленные протоколы связи РСУ и ПАЗ;
- Простота эксплуатации и расширения АСУТП;
- Единый парк запасных частей;
- Единый круг подготовленных специалистов.

Единственное условие, которое должно быть соблюдено - это разделение функций РСУ и функций ПАЗ по раздельным станциям управления, на что косвенно указывает пункт 3.11 ПБ 09-540-03: *"Системы противоаварийной защиты, как правило, включаются в общую систему управления технологическим процессом".*

Опыт внедрения однородной системы управления и защиты Centum на нескольких нефтехимических предприятиях России показал, что система противоаварийной защиты вполне может быть построена на выделенных станциях управле-

ния. Как сказано, уникальность ситуации заключается в том, что станции управления систем семейства Centum уже более двадцати лет построены по схеме 2*2, то есть номинально имеют архитектуру "2oo4^{м}, которая так превозносится ее нынешними поклонниками. Представляется, что данное решение может найти применение для значительного числа взрывоопасных объектов, для которых не выставляется специальных требований по аппаратной и программной альтернативности оборудования системы ПАЗ. (Пример подобного особого случая - защита компрессорных машин от помпажа).

Объекты I и II категории взрывоопасности. Для объектов I и II категории взрывоопасности (SIL3 и RC5-6) необходимо точное разделение функций РСУ и ПАЗ, чтобы обеспечить требуемый уровень безопасности и исключить противоречия при выполнении функций управления и защиты.

Функции защиты должны быть реализованы на специализированном оборудовании, имеющем Разрешение на применение от центральных органов технадзора.

Замечание

Существуют особые случаи, когда трудно обеспечить разделение функций на функции РСУ\ и функции ПАЗ. Например, система защиты газовой турбины от помпажа включает как управляющие, так и функции безопасности.

В этом случае функции управления встраиваются в соответствующую специализированную систему защиты, способную обеспечить безопасное выполнение функций управления и защиты.

Дополнительные условия, которые учитываются для определения требований единых систем управления и безопасности в одном и том же устройстве:

- *Оценка отказа общих компонентов и программного обеспечения, и их влияние на обеспечение функций защиты;*
- *Поддержка жизненного цикла системы именно как системы безопасности по отношению к внесению изменений, эксплуатации, тестированию и документированию;*
- *Дополнительное ограничение доступа к программным средствам и функциям конфигурации системы.*

9.12. Связь между РСУ и ПАЗ

Связь между РСУ и ПАЗ повышает информированность технологического персонала и общую безопасность АСУТП.

Тем не менее, внешняя связь, особенно запись данных в ПАЗ, может вступить в конфликт с целостностью системы защиты.

Должны быть сделаны специальные процедуры проверки, чтобы гарантировать, что все записываемые в систему защиты данные являются достоверными и не оказывают негативного влияния на системную целостность, или на выполнение требуемых операций защиты. Существует несколько путей для внешней связи между РСУ и ПАЗ:

1) **Физическая связь по каналам ввода-вывода РСУ и ПАЗ** (Например, когда аналоговый или дискретный выход от системы ПАЗ подается на физический вход РСУ).

   Это решение приемлемо для объектов всех категорий взрывоопасности, поскольку функции защиты непосредственно не затрагиваются, но использование этого метода носит скорее исключительный, чем регулярный характер.

2) **Система защиты работает по принципу "только чтение" данных из системы ПАЗ.** Это может быть приемлемым для всех категорий взрывоопасности, если проведен соответствующий анализ, чтобы гарантировать, что функции защиты не нарушаются, и нет риска модификации или разрушения данных системы ПАЗ.

   Меры, обеспечивающие защиту от несанкционированной записи в систему ПАЗ, могут включать, например, установку физического или программного ключа, чтобы запретить доступ для записи в ПАЗ.

3) **Внешняя связь типа "чтение-запись" с защитой от воздействия на функции защиты.**

   Использование этого метода для взрывоопасных объектов требует дополнительного исследования и анализа безопасности и защиты данных. Меры, обеспечивающие безопасность для функций защиты, включают, но не ограничиваются следующими действиями:

- Ограниченное окно времени для доступа к записи;
- Программный ключ (например, пароль), чтобы ограничивать доступ для записи;
- Обеспечение независимости логических контуров защиты от воздействия данных из РСУ.

9.13. Программное обеспечение

Встроенное программное обеспечение. Встроенное специальное программное обеспечение предусматривается изготовителями оборудования, и используется при подготовке прикладного программного обеспечения.

Утилиты (Служебные программы). Использование утилит должно придерживаться тех же критериев, что и встроенное программное обеспечение. Утилиты третьих сторон могут быть использованы только после соответствующего анализа и одобрения изготовителя оборудования.

Прикладное программное обеспечение. Рекомендуется модульная организация прикладных программ, поскольку модульность повышает проектную простоту и целостность.

Стандартное программное обеспечение должно включать средства диагностики и само документирования.

Используемые средства и языки программирования должны соответствовать средствам, утвержденным для промышленного применения.

Иначе говоря, программное обеспечение должно иметь в своем составе полный набор программных средств, обеспечивающих полноценное выполнение всего набора функций в соответствии со стандартом Международной Электротехнической Комиссии IEC 61131-3, регламентирующим полноту и синтаксис языков технологического программирования (отечественные нормативные документы отсутствуют).

В соответствии с этим стандартом, система должна иметь следующие средства технологического программирования:

(1) *Function Block Diagrams* -
Графический язык функциональных блоков.

(2) *Sequential Function Chart* -
Функциональные схемы описания последовательности операций.

Для разработки систем противоаварийной защиты, как правило, предусматриваются

(3) Ladder Logic Diagrams -
Графические средства описания логических схем (лестничные диаграммы).

Кроме того, могут использоваться дополнительные программные средства:

(4) *Cause & Effect Matrix Programming Language Editor* -
Средство для реализации такого эффективного приема, как таблицы решений.

Проблемно-ориентированные языки высокого уровня, позволяющие:

- Создавать программы произвольной структуры,
- Оперативно их корректировать,
- Сохранять результаты решения задач в базе данных,
- Организовывать запуск задач по запросу и по времени с соответствующими приоритетами, -

для разработки прикладных программ защиты, как правило, не используются. И это правильно. Как неоднократно подчеркивается на всем протяжении настоящей работы, при создании систем противоаварийной защиты необходимо в максимально возможной степени ограничивать число степеней свободы. Соответственно, тем самым автоматически уменьшается и вероятность привнесения в систему систематических ошибок программирования.

Для подтверждения того, что прикладное программное обеспечение удовлетворяет Спецификации требований безопасности, предусматривается следующее:

- Анализ проекта, демонстрирующий, что все требования, установленные в Спецификации требований безопасности, нашли свое воплощение в проекте;
- Анализ алгоритмов, реализующих функции защиты;
- Разработка специальных тестов для проверки реакции программного обеспечения на обработку данных, выходящих за нормальные границы; на команды, на вводы данных с клавиатуры, и другие действия;
- Программное обеспечение должно быть протестировано для определения его реакции на присутствие аппаратных дефектов.

9.14. Интерфейс пользователя

Интерфейсы пользователя для связанной с безопасностью системы - это:

- Интерфейсы оператора и
- Интерфейсы технического обслуживания, проектирования и разработки.

Интерфейсы оператора. Интерфейс оператора, посредством которого осуществляется взаимообмен информацией между оператором и ПАЗ, может включать:

- Видеоизображения;
- Физические панели, содержащие лампы, кнопки, указатели, ключи;
- Сигнализаторы (оповещатели);
- Принтеры;
- Любая комбинация из предыдущего.

Как правило, операторский видеоинтерфейс системы защиты встраивается в рабочие станции РСУ.

Видеоизображения. Видеоизображения на РСУ могут совмещать обработку функций обеспечения безопасности и в то же время осуществлять собственно управляющие функции РСУ. Данные из системы безопасности, отображаемые для оператора, должны обновляться с частотой, необходимой для своевременной реакции в случае возникновения непредвиденных условий. Видеоизображения, имеющие отношение к ПАЗ, должны ясно идентифицироваться как таковые, исключая возможность неоднозначной интерпретации, или потенциальной неразберихи в непредвиденной ситуации.

Операторы должны иметь легкий доступ к связанным с безопасностью видеоизображениям, предпочтительно посредством единственного нажатия на ключевую клавишу, или сенсорно - экранным способом, дающим прямой вход в иерархию изображений.

Видеоизображения системы защиты должны предоставлять оператору достаточно подробную и наглядную информацию на одном видеокадре, чтобы быстро сообщить критическую информацию. Желательно обеспечить те же методы доступа, способы отображения тревожных сообщений и компонентов изображения, что и в несвязанных с безопасностью видеоизображениях. Слишком много информации на одном

видеокадре может провести оператора к неправильному истолкованию данных, и вызвать неправильные действия. Сообщения должны быть ясными, краткими и однозначными.

Интерфейсы оператора и собственно РСУ должны обеспечивать автоматическую регистрацию событий и сигнализаций, связанных с безопасностью. События, которые нужно регистрировать, также должны включать и те события, которые происходят в то время, когда система ПАЗ доступна для программных изменений, диагностики и технического обслуживания.

Оперативные панели системы ПАЗ. Панели должны быть расположены таким образом, чтобы обеспечивать легкий доступ операторов. Размещение кнопок, сигнальных табло, ключей на панели должно быть таким, чтобы гарантировать, что положение кнопок, ламп, переключателей, надписей и другая информация не запутывает оператора, и не предоставляет возможности совершить ошибку в стрессовой ситуации. Должна быть предусмотрена кнопка тестирования всех ламп.

Принтеры. Принтеры, предназначенные для печати событий ПАЗ, не должны вступать в конфликт с функциями обеспечения безопасности даже в том случае, если принтер отказал, выключен, разъединен, испытывает недостаток бумаги, или ведет себя ненормально.

Система ПАЗ, связанная с РСУ, может использовать средства РСУ, чтобы выполнять функции регистрации событий и печати отчетов, связанных с обеспечением безопасности. Принтер необходим для распечатки отчета о последовательности событий при поиске первопричины останова, для диагностики, и других связанных с безопасностью событий и тревог, с отметкой времени, датой, и идентификацией позиций.

Интерфейсы технического обслуживания, проектирования и разработки системы ПАЗ. Интерфейсы технического обслуживания, проектирования и разработки состоят из средств программирования, тестирования и технического обслуживания системы ПАЗ.

Данные интерфейсы являются теми средствами, которые используются для:

- Конфигурации аппаратных средств;
- Программной разработки, документирования, загрузки системы ПАЗ;

- Доступа к прикладному программному обеспечению для изменения, тестирования и просмотра;
- Контроля эффективности использования системных ресурсов ПАЗ и диагностики;
- Изменения уровня секретности системы ПАЗ и доступа к переменным прикладного программного обеспечения.

Интерфейсы технического обслуживания, проектирования и разработки должны иметь возможность отображения рабочего состояния и диагностического статуса всех компонентов ПАЗ (модулей ввода-вывода, процессоров, и т.п.), включая состояние каналов связи между ними. Интерфейсы технического обслуживания, проектирования и разработки должны иметь средства для копирования прикладных программ на внешний магнитный носитель. Интерфейсы технического обслуживания, проектирования и разработки должны быть доступны только:

- Со специально предназначенной для этих целей станции,
- По специальному разрешению,
- И только для специально допущенного персонала.

9.15. Диагностика

Общие положения. Диагностика - это тестирование, выполняемое периодически для обнаружения скрытых дефектов, которые могут помешать системе защиты в осуществлении предписанных действий.

Скрытый дефект в системе может помешать ПАЗ отреагировать на требование защиты.

Этот отказ может быть единственным отказом в одноканальной системе, или комбинация дефектов в многоканальной системе. Следовательно, очень важно отслеживать не только критические отказы, но также и потенциально критические дефекты прежде, чем они накопятся.

Дефекты могут закончиться двумя типами отказов:

- **Случайные отказы** - спонтанный отказ компонента;
- **Систематические отказы** (или ошибки) - скрытый дефект в конструкции или в реализации проекта.

Случайные отказы возникают спонтанно. Оборудование, вообще говоря, склонно к случайным отказам, но может также иметь и систематические отказы (неправильная синхронизация, компоненты эксплуатируются за пределами предопределенных условий, и т.п.).

В зависимости от частоты проявления дефекта возможны два варианта развития событий:

- Постоянные случайные дефекты упорствуют до тех пор, пока их источник не будет выявлен и исправлен;
- Динамические случайные дефекты (перекрестные, термические эффекты, и т.п.), происходят при определенных обстоятельствах, и на некоторое время исчезают.

Программное обеспечение, как правило, не имеет случайных отказов, но имеет высокую вероятность систематических ошибок. Как только систематическая ошибка обнаружена, она может быть исправлена - и перестанет существовать.

Диагностические тесты. Диагностика может быть выполнена с помощью разнообразной комбинации методов, включая:

- Автоматические встроенные тесты, предусмотренные в пределах приобретенного оборудования ПАЗ (например, внутренние тесты модулей ввода-вывода);
- Автоматический тест, встроенный как часть специфического проекта (например, контрольное чтение выходных сигналов через входные точки);
- Сторожевые таймеры, сравнение сигналов, обнаружение обрывов и т.п.;
- Сравнение резервированных сигналов.

Диагностический охват. Конкретная диагностическая техника на практике не может достичь 100% эффективности в обнаружении всех возможных отказов. Поэтому оценка эффективности использованной диагностики может рассматриваться только для определенного набора конкретных отказов, на выявление которых эта диагностика нацелена.

Критические и потенциально критические сбои (подобно сбоям CPU / RAM / ROM...) приведут к полному сбою всей обработки данных и, следовательно, вызовут более далеко идущий отказ, чем отказ единственной выходной точки. Поэтому требования к обнаружению данного типа отказов должны быть максимально строгими.

Режимы подобных отказов, которые несут высокую вероятность аварийной ситуации на процессе, должны обнаруживаться с наибольшей вероятностью. Для каждой диагностической процедуры необходимо четко определить:

- Периодичность испытаний;
- Порядок действий при обнаружении дефектов;
- Согласованность предпринимаемых действий со Спецификацией требований безопасности.

В тех случаях, когда специфическая диагностика не встроена в оборудование поставщика на аппаратном уровне, необходимые диагностические процедуры должны быть встроены в системное программное обеспечение.

Диагностика не всегда способна обнаружить систематические ошибки (подобные программным дефектам). Тем не менее, соответствующие меры предосторожности для обнаружения возможных систематических дефектов должны быть предприняты.

Общие рекомендации. Цель системы безопасности заключается в защите от аварийных ситуаций на процессе, и в предохранении от ложных остановов. Система безопасности в течение длительного времени находится в ждущем режиме, и подвержена функциональным отказам, которые, вообще говоря, носят неявный характер.

Степень внутреннего диагностического охвата в принципе не может достигнуть ста процентов. Поэтому система защиты нуждается в периодической проверке.

При этом должны быть обеспечены следующие условия:

- Процедура тестирования должна быть максимально простой и быстрой;
- Замена дефектных компонентов должна производиться в реальном времени;
- Процедура замены должна быть простой и понятной, чтобы провести ее быстро и безошибочно;
- Кроме того, должна быть продумана процедура деблокировки полевых устройств с целью поверки, калибровки и обслуживания.

Интервал времени между поверочным тестированием имеет очень важное значение, поскольку, с одной стороны, увеличение частоты тестирования снижает вероятность опасных отказов, а с другой, - потенциал для совершения челове-

ческих ошибок во время тестирования очень высок. При выборе интервала следует учитывать следующие соображения:

1. Степень резервирования системы и уровень внутренней диагностики;
2. Потенциал человеческих ошибок, обусловленный процедурой тестирования и замены;
3. Время, необходимое для выполнения тестирования и замены.

Во время автономного тестирования система не в состоянии выполнять функции защиты. Поэтому поверочное тестирование увеличивает и неготовность системы защиты, и вероятность человеческих ошибок. С другой стороны, редкое тестирование увеличивает риск развития невыявленных ошибок, в особенности для систем с низким уровнем диагностики.

Отечественный общепринятый межповерочный интервал составляет 1 год.

Текущая проверка сомнительных элементов оборудования осуществляется при необходимости.

9.16. Обслуживание и поверка полевого оборудования системы безопасности
(по рекомендациям TUV)

В этом разделе описывается процедура обхода блокировки и технического обслуживания отдельных компонентов систем безопасности: сенсоров, контроллеров, исполнительных элементов, рекомендованная TUV.

Особое внимание необходимо уделять следующим аспектам технического обслуживания:

1. Проведение технического обслуживания посредством обычного ПК или инженерной станции РСУ;
2. Соблюдение общих требований к протоколам связи, используемым в системах защиты;
3. Проведение технического обслуживания посредством публичных сетей типа Internet;
4. Обеспечение требуемой готовности;
5. Процедуры изменения системных данных;
6. Процедуры замены сенсоров и исполнительных устройств, и связанные с этим изменения прикладного программного обеспечения.

Методы проверки периферийного оборудования системы безопасности. В настоящее время существуют несколько методов проверки периферийного оборудования, подключенного к контроллеру системы ПАЗ:

1. Специальные ключи, подключенные как входы в контроллер системы ПАЗ. Эти входы используются в качестве признака деблокировки сенсоров и исполнительных устройств во время технического обслуживания. Условия и способы обслуживания встраиваются как часть прикладного программного обеспечения ПАЗ.
2. На время технического обслуживания сами сенсоры и приводы электрически изолируются (отключаются) от контроллера системы ПАЗ, и поверяются вручную в соответствии с методикой.

В ряде случаев удобно осуществлять функции обслуживания дистанционно, например, **через инженерную станцию РСУ.**

3. Таким образом, появляется третья возможность для проведения технического обслуживания:
   - Команды деблокировки инициируются отдельными от системы безопасности средствами, и направляются в контроллер системы ПАЗ по последовательному протоколу;
   - Связь с контроллерами системы ПАЗ должна обеспечиваться с использованием только разрешенных протоколов. Можно использовать протоколы, которые признаны соответствующими принятому уровню безопасности (такие, как Modbus), или рекомендуемые протоколы изготовителя оборудования системы;
   - В общем случае разрешается использовать только те средства, которые разрешены для конкретного применения;
   - Если коммуникация осуществляется посредством открытых сетей, то в дополнение к требованиям функциональной безопасности должны быть определены дополнительные требования, гарантирующие безопасность доступа.

4. Наиболее эффективное средство обслуживания полевого оборудования - выделенная система обслуживания полевого оборудования - *Plant Asset Management System* - система управления оборудованием производства.

Допустимые режимы обслуживания и протоколы связи должны быть частью сертифицированной системы безопасности, чтобы они применялись безопасным образом.

Процедуры проведения операций деблокировки и внесения изменений в процессе работы должны быть описаны в руководствах по обслуживанию АСУТП. При этом строго рекомендуется, чтобы средства программирования и отладки были отделены от средств технического обслуживания.

Если потребовалось внести изменения в ППО, то тестирование не должно фокусироваться исключительно на тех частях программного обеспечения, которые подверглись изменению, поскольку это не дает гарантии, что внесенные изменения не оказывают воздействия на неизмененные части.

Полнота тестирования системы, подвергнутой изменению, должна соответствовать полноте первоначальных приемосдаточных испытаний.

И поскольку данная процедура по своим последствиям является дорогостоящей, использование средств, не имеющих специального разрешения фирмы-изготовителя, строго не рекомендуется.

Разрешенные средства технического обслуживания в общем случае должны отвечать следующим требованиям:

- Включать измерения, позволяющие проконтролировать случайные сбои вновь созданной или модифицированной программы;
- Включать в себя измерения, позволяющие проконтролировать случайные ошибки данных по каналу связи с контроллером;
- Они должны быть разработаны под конкретную версию программного обеспечения;
- Они должны быть разработаны с использованием средств проверки прикладного программного обеспечения, и средств контроля изменений.

Общая стратегия технического обслуживания:

1. Общая стратегия и процедуры технического обслуживания должны быть разработаны до, или во время разработки прикладного программного обеспечения.
2. Процедуры технического обслуживания в составе прикладного программного обеспечения системы защиты должны предусматривать возможность деблокировки строго ограниченного набора конкретных сигналов.
3. Команды деблокировки должны контролироваться и осуществляться во взаимодействии с прикладным программным обеспечением РСУ и системы ПАЗ.
4. Схемы и алгоритмы автоматического срабатывания системы противоаварийной защиты должны быть настроены таким образом, чтобы была обеспечена их независимость от логических цепей, по которым осуществляется выполнение команд инженера по техническому обслуживанию.
5. Команда "Разрешение на деблокировку" с целью технического обслуживания возможна для целой подсистемы (технологического блока), или контроллера системы ПАЗ в целом, и может быть подана с РСУ, или другим разрешенным способом, например, физическим ключом.
6. Однако "Разрешение на деблокировку" не означает, что собственно команда какой-либо конкретной деблокировки действительно будет выдана.
7. Деблокировка группы параметров разрешается только в том случае, если только одна деблокировка используется в данной группе параметров. Оператор технологического процесса должен подтвердить наступление состояния деблокировки. Непосредственная (т.е. с помощью физических зажимов) деблокировка входов и выходов не разрешается.

Взаимодействие с технологом-оператором:

1. Технолог-оператор не должен иметь возможности отменить сигнализацию деблокировки. При любых обстоятельствах должно быть ясно, что данные входы-выходы находятся в состоянии деблокировки.
2. Контроллер системы ПАЗ извещает оператора РСУ о присутствии условий деблокировки.

Данное предупреждение действует до момента восстановления сигнала (снятия деблокировки).

3. Во время деблокировки проводятся необходимые рабочие операции и проверки, чтобы удостовериться, что сигнал может быть возвращен в исходное состояние.
4. Программное обеспечение в РСУ должно постоянно проверять соответствие между выданными из РСУ командами на деблокировку, и откликом, полученным от контроллера системы ПАЗ в РСУ.
5. Использование функций деблокировки должно быть документировано в архиве РСУ или другом, специально выделенном оборудовании.
6. Распечатка протокола операций по деблокированию и техническому обслуживанию должна включать:
   - Шифр позиции КИП деблокированного сигнала;
   - Отметки времени начала действия команды деблокировки;
   - Отметки времени окончания действия команды деблокировки;
   - Идентификацию конкретного исполнителя процедуры деблокировки.

9.17. Секретность

Должны быть предусмотрены специальные средства контроля над доступом к системе безопасности, включая все главные компоненты системы:

- Логические решающие устройства;
- Интерфейсы технического обслуживания;
- Функции тестирования системы ПАЗ;
- Функции деблокировки;
- Отключение тревожной сигнализации ПАЗ;
- Сенсоры;
- Конечные исполнительные элементы.

Защита доступа может предусматривать:

- Стойки системы - под замок и на физический ключ;
- Доступ "только чтение";
- Коды доступа, Пароли;
- Административные ограничения и т.п.

9.18. Документация

Состав документации. Состав документации системы безопасности должен включать, как правило, следующее:

- Спецификация требований безопасности;
- Описание функций ПАЗ;
- Схемы измерительных контуров и контуров защиты системы ПАЗ ***(Loop Diagrams);***
- Распечатка программ логического управления и защиты системы ПАЗ;
- База данных сигналов ввода-вывода системы ПАЗ;
- База данных параметров обмена с РСУ;
- База данных для программы определения первопричины срабатывания системы защиты;
- Чертежи компоновки системы в шкафах;
- Установочные чертежи;
- Схемы и конфигурация модулей ПАЗ;
- Схемы распределения питания внутри шкафов;
- Схемы заземления;
- Кабельный журнал внутрисистемных соединений;
- Схемы подключения каналов и внешних источников питания;
- Таблицы подключения каналов ввода-вывода к терминальным панелям и клеммным сборкам шкафов системы ПАЗ;
- Заключение о проведении заводских испытаний оборудования ПАЗ на площадке изготовителя;
- Инструкции по монтажу и наладке;
- Процедура приемосдаточных испытаний;
- Инструкции по эксплуатации и техническому обслуживанию;
- Процедура функционального тестирования;
- Порядок внесения изменений в документацию.

Примечание

Строго определенный состав проектной документации приведен в главе "Состав и содержание документации проекта АСУТП" настоящей работы.

Резервная копия программного обеспечения. Техника резервного копирования позволяет провести операцию восстановления системы в кратчайшие сроки. Эти методы защиты могут включать следующее:

- Копирование на сменные носители: магнитная лента или оптический диск, с которого можно произвести восстановление;
- Копирование на сменные носители, которые могут использоваться как замена для поврежденной системы;
- Копия на дублирующий (зеркальный) диск;
- Копирование по каналу связи с другой цифровой системой.

9.19. Временной интервал функционального тестирования

Частота проведения функциональных тестов должна, как минимум, соответствовать рекомендациям изготовителя, или более часто, если это согласуется с предшествующим опытом работы.

Настоятельная рекомендация - создание самостоятельной системы обслуживания полевого оборудования, а именно: внедрение так называемой *Plant Asset Management System* - системы управления оборудованием производства, позволяющей производить оперативное тестирование и диагностику оборудования КИПиА.

9.20. Управление и контроль выполнения проекта

Примечание

Представленные рекомендации относятся к проекту создания собственно системы защиты, однако не отменяют, а дополняют общие рекомендации по порядку выполнения проектных работ для АСУТП в целом - в соответствии с главой "Состав и содержание работ по созданию АСУТП".

Организация выполнения проекта. Для каждой из организаций, участвующих в процессе выполнения проекта, определяются лица, ответственные за сроки и качество выполнения Проекта в соответствии с Техническим заданием на соз-

дание Системы и действующими нормативными документами. В общем случае формируются следующие группы:

От Заказчика:

Главный инженер завода / производства
Главный метролог завода / производства
Руководитель (координатор) проекта

От Проектной организации:

Технический директор
Главный инженер проекта
Начальник отдела КИПиА

От Разработчика:

Технический директор
Руководитель проекта

От Подрядных организаций:

Руководитель Организации
Ответственный исполнитель.

9.21. Распределение ответственности

Руководитель проекта со стороны проектной организации - Главный инженер проекта.

Главной обязанностью Руководителя проекта со стороны проектной организации должно быть планирование, выполнение и контроль выполнения работ в соответствии с Планом-графиком.

Ответственность Руководителя проекта со стороны проектной организации:

- Координация работ с Заказчиком и Разработчиком;
- Соблюдение сроков выполнения работ по проекту;
- Своевременная подготовка всех необходимых исходных данных для разработки и системы защиты, и в целом АСУТП;
- Обеспечение функциональной совместимости всех частей проекта.

Руководитель проекта со стороны Разработчика.

Главной обязанностью Руководителя проекта со стороны Разработчика должно быть планирование, выполнение и контроль выполнения работ в соответствии с Планом-графиком.

Ответственность Руководителя проекта со стороны Разработчика - это организация выполнения своей части проекта, как то:

- Планирование работ;
- Координация работ с Заказчиком и Проектной организацией;
- Обеспечение функциональной совместимости всех частей проекта;
- Обеспечение выполнения требований договора на разработку;
- Контроль поставки оборудования и разработанной документации в соответствии с графиком;
- Ежемесячный отчет о ходе работ по разработке.

Координатор проекта со стороны Заказчика.

Основной ответственностью Координатора проекта является ежедневное отслеживание и контроль хода проекта.

Специфическими задачами являются:

- Согласование хода работ между всеми участниками проекта;
- Контроль и составление отчетов о ходе выполнения проекта;
- Обеспечения необходимых ресурсов для выполнения проектных работ со стороны Заказчика;
- Соблюдение графика работ.

Проектная группа Заказчика.

Проектная группа Заказчика назначается ответственным представителем Заказчика, и должна включать специалистов всех служб, которые задействованы в реализации проекта.

Главной задачей данной группы является обеспечение функциональных требований к проекту.

Данная группа должна участвовать в рассмотрении, экспертизе и приемке проекта, предварительных, опытных и приемочных испытаниях и т.д.

Обычно в эту группу привлекаются:

- Технологи;
- Специалисты КИПиА;
- Энергетики;
- Консультанты;
- Инженеры АСУТП.

Контроль выполнения проекта.

Процесс выполнения проекта должен координироваться Руководителями проекта со стороны Проектной организации, Разработчика и Заказчика.

Все подлежащие сдаче этапы должны утверждаться подписанием соответствующих документов. Свидетельствующие или утверждающие документы должны содержать краткое описание этапа, подлежащего к сдаче, дату приемки, комментарии, подписи сторонних руководителей проекта и Заказчика. Типовой период для рассмотрения и утверждения результатов этапа - одна рабочая неделя.

Проверка и утверждение выполненных работ.

После того, как выполненные работы рассмотрены и утверждены, подписывается соответствующий Акт о выполнении этапа. Это должно служить подтверждением, что выполненные работы проверены и согласованы с Заказчиком, как законченные.

Это также должно служить подтверждением, что все работы по данному этапу приняты Заказчиком.

Документирование хода выполнения проекта.

Вся информация, относящаяся к проекту, должна обобщаться каждым руководителем проекта, и храниться в определенном им месте в виде твердой копии, и в электронном виде. Согласованные и утвержденные копии документации в согласованном количестве экземпляров в виде твердой копии и в электронном виде передаются Заказчику.

Отчетность о ходе выполнения проекта.

Разработчик должен **ежемесячно** информировать Заказчика о ходе выполнения проекта, с использованием согласованной формы отчета. Оперативные вопросы Заказчик и Руководитель проекта должны обсуждать по мере необходимости. Предусматривается следующий порядок взаимодействия Заказчика и Разработчика:

- Ежемесячный письменный Отчет о ходе выполнения проекта;
- Обсуждение хода выполнения проекта по телефону между Заказчиком и Разработчиком в рабочем порядке;
- Электронная почта;
- При необходимости - рабочие встречи.

Протоколирование. Все достигнутые договоренности должны документироваться (протоколироваться) и распределяться между всеми участниками проекта. Все согласованные результаты и отражение существующих проблем должно быть обозначено в ежемесячном отчете о ходе выполнения проекта.

План обеспечения качества.

При разработке Плана обеспечения качества должны быть определены такие критические этапы, как:

- Проектирование;
- Изготовление;
- Конфигурирование;
- Доставка на площадку;
- Пуско-наладка, и
- Ввод системы в действие.

Данный план определяет каждый критический этап по следующим параметрам:

- Определение критериев обеспечения качества на данном этапе;
- Ответственный за выполнение данного этапа исполнитель;
- Документация, которая используется для проверки соответствия на данном этапе;
- Части контракта, отвечающие за данный этап;
- Подписание и утверждение Заказчиком факта выполнения данного этапа;
- Фиксирование даты утверждения этапа.

Данный документ разрабатывается как документ, отображающий реальное выполнение работ, фиксирующий все этапы, все ревизии документации. Все решения, принятые в данном документе, должны быть предоставлены Заказчику для утверждения.

Внесение корректировок.

Согласованные изменения определяются как изменения, влекущие изменение уже рассмотренной и утвержденной Заказчиком документации. Все согласованные изменения должны документироваться в Журнале учета изменений, который должен вестись координатором проекта со стороны Заказчика, и соответствующим руководителем проекта со стороны разработчика и проектной организации.

В результате согласования изменение проекта может быть принято, отклонено, изменено или прояснено для будущего применения.

Утвержденный Журнал учета изменений должен использоваться для планирования работ, изменения графиков и бюджета проекта.

Запросы на изменения проекта. Запрос на изменение проекта определяется как любой запрос, влияющий на:

- Конечную цель проекта,
  и вызывающий
- Изменение графика выполнения, или
- Стоимости.

Все запрашиваемые изменения, независимо от причины и цели, должны быть оформлены письменно с приложением формы Запроса на изменение проекта и представлены Заказчику для рассмотрения и оценки.

Оценочная стоимость и перечень изменений должны быть представлены координатору проекта со стороны Заказчика посредством записи в Журнале учета изменений.

Проектные изменения должны быть рассмотрены и приняты Заказчиком с подписью и возвращены Разработчику.
Примерами таких изменений являются:

1. Изменение объема проекта, то есть запрос на работы, которые выходят за рамки первоначального проекта;
2. Изменение графика работы с обоснованием причин;
3. Работы, которые необходимо выполнить для внесения изменений, после чего изменения должны считаться завершенными;
4. Проектные изменения, которые не подпадают под вышеперечисленные определения или для которых необходимо предоставление дополнительной информации.

Все согласованные изменения оформляются совместным протоколом, а в случае существенных отклонений от исходных требований к системе - дополнением к ТЗ.

Если изменения таковы, что требуют изменения цены исходного договора, составляется дополнительное соглашение.

9.22. Примерная форма Журнала учета изменений

Код Проекта	
Запрос вносит:	
Дата	
Наименование запроса:	

№	Описание изменения	Дата внесения	Срок выполнения	Одобрено	
				Да	Нет
1					
2					
3					
4					
5					
6					

От Заказчика: Дата
От Разработчика: Дата

9.23. Примерная форма для Запроса на изменение проекта

Код Проекта	
Запрос вносит:	
Дата	
Наименование запроса:	

№	**Код части проекта**	**Описание запроса**	**Дата запроса**
1			
2			
3			
4			
5			
6			
7			

Подтверждение получения запроса: подпись дата
Запрос принят: подпись дата

9.24. Примерная форма для контроля выполнения принятых изменений

Формы для контроля выполнения принятых изменений используются для фиксирования выполнения изменений по мере выполнения.

Номер изменения:		Дата

Описание:

Инициировано Разработчиком:	ФИО	Дата

Инициировано Заказчиком:	ФИО	Дата

№ изменения	Код чертежа, документа	Наименование

Проверил От Заказчика	**ФИО**	**Дата**	**Подпись**
Проверил От Разработчика	**ФИО**	**Дата**	**Подпись**
Утвердил От Заказчика	**ФИО**	**Дата**	**Подпись**
Утвердил От Разработчика	**ФИО**	**Дата**	**Подпись**

9.25. Ежемесячный отчет о проделанной работе со стороны разработчика

Со стороны Заказчика необходимо не только контролировать конечное выполнение стадий и этапов выполнения проекта в соответствии с общим Планом-графиком работ, но и четко отслеживать работу всех участников проекта через определенные временные отметки. Это позволяет своевременно отреагировать на потенциально возможное отклонение от графика, и принять соответствующие упреждающие действия.

Ежемесячный отчет со стороны непосредственного исполнителя - конкретного разработчика, проектировщика, поставщика, и генподрядчика проекта в целом - является чрезвычайно важным и эффективным средством контроля общего хода выполнения проекта, и на западе является общепринятым. Ежемесячный отчет о ходе выполнения проекта, как минимум, должен содержать следующие разделы:

1. Работы, выполненные за отчетный период;
2. Ход выполнения графика работ, и процент выполнения каждого из пунктов;
3. Причины задержки, если таковые возникли;
4. Внесенные согласованные изменения;
5. Перечень предстоящих работ;
6. График предстоящих работ;
7. Проблемные вопросы, способные привести к нарушению графика работ;
8. Организация или реорганизация работ с целью разрешения возникших узких мест;
9. Согласованный и скорректированный (при необходимости) дальнейший график выполнения работ.

Глава 10

СИСТЕМА ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ АСУТП

10.1. Исходные данные

В настоящей главе представлена система идентификации всего спектра оборудования, параметров и контуров АСУТП, начиная от полевого оборудования, и заканчивая системами ПАЗ и РСУ.

Базовым документом является американский стандарт ANSI/ISA-S5.1-1984 '*Instrumentation Symbols and Identification",* который признан международной практикой в качестве основного руководящего документа по идентификации параметров автоматизированных систем управления. ISA, существующее с 1945 года как "*Instrument Society of America",* решением Совета общества от 21 августа 2000 года, принятом на выставке EXPO/2000, переименовано в "*Instrumentation, Systems and Automation Society*", как более точно представляющее роль и направление деятельности общества.

Однако и стандарт ISA в основных положениях следует первоначальной версии 1973 года, ориентированной на локальную автоматику (см. таблицы 10.1 и 10.2).

Поэтому подробно изучены системы кодов и графических символов ведущих западных проектно - технологических фирм, работающих в нефтегазодобыче, химии, нефтехимии и нефтепереработке:

- *ABB Lummus Global*, США
- *ABB Simeon*, США
- *Howe-Baker,* США
- *Parsons,* США

- *FINA Technology,* США
- *Davy*, Великобритания
- *Pressindustria /Techint,* Италия
- *Tecnimont,* Италия
- *Toyo Engineering,* Япония, и т.д.

Рассмотрены рекомендации консорциума *Process Industry Practices* - независимой организации собственников и разработчиков технологических процессов, США.

Аналогичные системы идентификации применяются и в атомной промышленности. Таблицы кодировок и графических символов авторитетной правительственной организации *Los Alamos National Laboratory*, США, в точности копируют стандарт ANSI/ISA S5.1-1984.

Общий вывод таков, что ситуация с кодировками параметров далеко не однозначна. Большинство проектировщиков идут по самому простому и практичному пути, и формируют конкретный состав кодов и графических символов, который используется в конкретном проекте, что, конечно же, не освобождает от необходимости иметь целостную концепцию.

Чтобы проще было включиться в непростую тему настоящей главы, в таблицах 10.3-10.8 приведены примеры применяемых графических символов.

Примеры с переводом - в таблицах 10.9-10.10.

В таблице 10.11 представлен набор кодов и описание их смысла, сформированный с максимально возможным соответствием стандарту ANSI/ISA-S5.1-1984.

Горькое замечание

Трудно представить себе более нелепый документ, чем принятый в 1985 году Госстроем ГОСТ 21.404-85 "Обозначения условные приборов и средств автоматизации в схемах Кроме изуродованной копии Table 1 (см. исходную версию в таблице 10.1), взятой со страницы 17 стандарта ANSI/ISA-S5.1-1984 (в ГОСТе она называется Таблица 2), наш ГОСТ вообще не содержит какой бы то ни было внятной графической и символьной идентификации параметров в приложении к системам управления и защиты технологических процессов.

Таблица 10.1

Символы идентификации

	First letter		Succeeding letters		
	Measured or initiating variable	**Modifier**	**Readout or passive function**	**Output function**	**Modifier**
A	Analysis		Alarm		
B	Burner, combustion		User's choice	User's choice	User's choice
C	User's choice			Control	
B	User's choice	Differential			
E	Voltage		Sensor (primary element)		
F	Flow rate	Ration (fraction)			
G	User's choice		Giass, viewing device		
H	Hand				High
1	Current (electrical)		Indication		
J	Power	Scan			
K	Time, time schedule	Time rate of change		Control station	
L	Level		**ught**		Low
M	User's choice	Momentary			Middle, intermediate
N	User's choice		User's choice	User's choice	User's choice
0	User's choice		Orifice, restriction		
P	Pressure, vacuum		Point (test connection)		
Q	Quantity	Integrate, totalizer			
R	Radiation		Record		
S	Speed, frequency	Safety		Switch	
T	Temperature			Transmit	
U	Multivariable		Multifunction	Multifunction	Multifunction
V	Vibration, mechanical analysis			Valve, damper, louver	
W	Weight, force		Well		
X	Unclassified	X axis	Unclassified	Unclassified	Unclassified
Y	Event, state; or presence	Y axis		Relay, compute, convert	
Z	Position; dimension	Z axis		Driver, actuator	

Таблица 10.2

Типичны* комбинации символов

			Recording	Indicating	Blind
Combustion Unci Choice Unci Choice					
		ESH FSH	ESL FSL		
	IRC JRC KRC LRC			JSHL KSHL LSHL	
Level U*er*e Choice User's Choice Ueer"» Choice					
	PCV		PSL		PRT
	POIC POCV		PDSL		PORT
	QRC QIC RRC SRC	QSH RSH SSH	QSL RSt SSL	QSHL RSHL SSHL	QRT RRT SRT
				TSHL	
			VSL	VSHL	
		WOSH	WSL WDSL	WSHL	
		YSH	YSL		
	2RC ZCV	ZSH	ZSL	ZSHL	ZRT
	ZDRC ZOCV				ZDRT

PFR (Ratio)
KOI (Running Time Indicator)
QOt (Indicating Counter)
WKIC (Rate-ot-Weight-LOM Controller)
HMS (Hand Momentary Switch)

The letter* H end L rary ь m the undefined &

Таблица 10.3

Process Flow Diagrams (PFD) and P&ID symbols: Lines

Line types		
Symbol	**Line tvoes**	**Description**
	Continuous .80 mm	Primary process flow line
	Continuous .35 mm	Secondary process flow line
	Continuous .25 mm	Instrument supply or connection to process
	Continuous	Undefined digital
	Continuous	Pneumatic signal
	Dashed	Electric signal
L L	Continuous	Hydraulic signal
—K *Vr-*	Continuous	Capillary tube
<\j	Continuous	Electromagnetic or sonic signal ** (guided)
	Continuous	Electromagnetic or sonic signal ** (no guided)
—o—o—	Continuous	Internal system link (software or data link)
– · – · –	Continuous	Mechanical link

Таблица 10.4

Process Flow Diagrams (PFD) and P&ID symbols: Additional line symbols

Optional and binary (on-off) symbols		
ж ж	Continuous	Pneumatic binary signal
—ч V -	Hidden	Electric binary signal
- E E—	Continuous	Electrical heat tracing
—S S—	Continuous/ dashed2	Steam heat tracing
	Dashed2	Buried lines
	Phantom	Existing
XX	Center	FP - floor penetration RP - roof penetration WP - wall penetration SB - system break

Notes:

"Or" means user choice. Consistency is recommended.

* *The pneumatic signal symbol apples to a signal using any gas as the signal medium. If gas other than air is used\ the gas may be identified by a note on the signal symbol or otherwise.*

** *Electromagnetic phenomena include heat, radio waves, nuclear radiation and light.*

Таблица 10.5

Instrument / Function symbols

	Primary location normally accessible to operator	Field mounted	Auxiliary location normally accessible to operator	Auxiliary location normally inaccessible to operator
Discrete instruments	/XXX\ \xxx/	/xxxЧ \xxxj	/xxxN	/xxx\ \xxiy
Shared display, Shared control	yXXXy	^xxx^4 ^xxx^	Г Н	^XXXN
Computer function	/xxx\ \xxx/	/xxx\ \xxx/		/xxx\ \xxx/
Programmable logic control		s&b.		/

Таблица 10.6

Additional Instrument / Function symbols

Symbol	Description
• >	Flow indicator to be used In conjunction with /xxx\ \xxxj
/xxxVxxx\ \xxxдxxx/	Instruments sharing common housing
	Panel mounted patch board like /xxx\ \xxx/

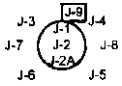
Таблица 10.7

Additional Instrument / Function symbols

Symbol	Description
	P = Purge or flushing device P = Reset for latch-type actuator I = Undefined interlock logic
	Signal directional arrow
	S = Solenoid D = Digital P = Pilot T = Trap M = Magnetic flow meter
	SP = Set point
[7]	Root extraction
[±]	Bias
0	Multiply
[>1	High selecting
[<1	Low selecting
[>1	High limiting
[<1	Low limiting
[к]	Proportional
Q	Reverse proportional
R	Summing
[÷]	Dividing
ISA-11	Equipment tag
4 3	Piping class break or ML classification change
<	

	Pipe or wire continued drawing X (including sheet number) Grid coordinate (Y-#)- Flow is to that drawing reference point
<IZZ	Pipe or wire continued drawing X (including sheet number). Grid coordinate (Y-#)- Flow is from that drawing, or reference point
< ~ 7 T >	Pipe or wire continued drawing X (including sheet number). Grid coordinate (Y-#)- flow is in both directions

Instrumentation identification table



J-1 Component function number
J-2 Component sequence number
J-2A Component sequence # cont'd
J-3 Vendor designation
J-4 Panel number
J-5 Applicable notes
J-7 Acme test symbol for test only or test plus normal use
J-8 Set-point(s)
J-9 Function (see instrument / function symbols)

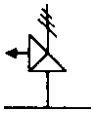
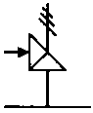
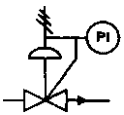
Note:
Instmmentation function identifiers (J-1) and function symbols per ANSI/ISA S5 1-1984.

Таблица 10.8

Process Flow Diagrams (PFD) and P&ID symbols

- e x -	Valve		Two-way valve, fail open
Л	Angle valve	-fcti-	3-way valve with diaphragm actuator
4 \ h	Butterfly valve	V	4-way valve w/diaphragm actuator
▪ 0	Rotary valve	; —	Spring-opposed single-acting actuator
-M-	3-way valve	–	Spring-opposed double-acting actuator
_ * _	4-way valve		Electro hydraulic actuator
	OS & Y valve		Hand actuator or hand wheel
	Diaphragm valve	— i n —	Restriction orifice in process line
\	Pressure relief	н Н ь	Restriction orifice drilled in valve
	Diaphragm actuator	!	Flow straightening vane

Продолжение таблицы 10.8

	Two-way valve, fail closed	G l	Diaphragm pressure-balanced
	Pressure-reducing regulator, self-contained, with hand wheel adjustable set point		Flow direction
	Pressure reducing regulator with external pressure		Pressure relief or safety valve
- М Ж Ь -	Differential-pressure-reducing regulator with external and external taps		Vacuum relief valve
	Back pressure regulator, self-contained	Ч ^ С Н -	Pressure relief or safety valve, straight-through pattern, spring- or weight-loaded, or with integral pilot
	Back pressure regulator with external pressure tap		Rupture disk or safety head for vacuum relief
	Pressure-reducing regulator with integral outlet pressure relief valve, and optional pressure indicator	£	Rupture disk or safety head for pressure relief

Продолжение таблицы 10.8

	Pressure indicator		Pilot light: X=color R-red G=green
	Flex connection (rubber)	Ч	Strainer with valve
НшЬ	Flex connection		Y-strainer
h h	Single pitot tube or pitot venturi tube	4	Compressed air
<x>	Flow meter		Ducted air flow from space
	Flow nozzle or venturi	4	Capped air duct
- o -	Reducer	-Dxb	Gate valve (open)
3	Screwed cap	- м -	Gate valve (closed)
D	Pipe cap	ЧЖ1-	Globe valve (open)
[	Hose connection	НМ-	Globe valve (closed)
—II—	Flanged connection (piping or equip)	-C^O-	Needle valve (open)

Продолжение таблицы 10.8

— l ' b —	Flow orifice fixed	h A H	Needle valve (closed)
ч ж ь -	Plug valve (open)		Four-way valve (arrows indicate flow direction)
- м -	Plug valve (closed)		Ball-check valve
- ш с ъ	Ball valve (open)		Dual purge valve
	Bali valve (closed)	●	Alarm valve
	Check valve		Air intake filter
- H ^ h	Spring check valve		Alarm
г	Angle valve (open)	1	Bubble gauge
ℓ	Angle valve (closed)		In-line filter
	Safety or relief valve (inlet port shown closed)	1	Atmospheric filter
_	Three-way valve (closed port dark-ened)	8	Double basket strainer

Окончание таблицы 10.8

V/	Hose reel		XX		Trap XX annotates function
Y	Open drain (shown)		●		Lubricator
XX	XX - drain system annotation				55 gallon drum
П	Drain (plan view)				Thermostatic vent
®	Cleanout (plan view)		D		Sprinkler alarm (water motor gong)
O	Sanitary vent		A		Flow alarm valve
O	Silencer/muffler				Flow control valve
Го)	Space penetrations		[5		Suction diffuser
г	Fixed louvers		*		Automatic air vent

Замечание

Здесь уместно вспомнить как всегда гениальную фразу Льва Давидовича Ландау: "Английский язык знают даже довольно тупые англичане!". Но и собственная терминология также должна быть четко определенной.

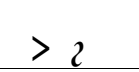
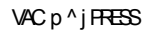
Таблица 10.9

Компоненты трубопровода

>	Направление верх	&	Угловой
Г	Направление вниз		Дроссельный
Т Г	Направление вбок		Переключение
Т	С амортизатором или глушителем	i	Клапан шиберного типа
I	С ловушкой для пламени	ЮН	Двухходовой (кран)
1 X 1	Запорный		Трехходовой
r-v|	Обратный	1 V7 [Ж]	Четырехходовой
1Ж1	Шаровой	О	Двухходовой
Л	Игольчатый	О	Трехходовой
	Y-образный шаровой	А	Трехходовая шаровая задвижка под 120°
СМ	Поршневой	О	Четырехходовой
- S - .	Заглушка-восьмерка	|С3|	Орбитный клапан
- Л -	Временный спускиик	К »	Смотровое стекло

Таблица 10 АО

Символика оборудования КИПиА

	Вихревой расходомер		V - образный шаровой клапан
	Труба ВЕНТУРИ или сужающее устройство		Двухпозиционный проходной клапан с поршневым приводом
	Трубка ПИТО		Перепускной клапан с поршневым приводом
	Элемент измерения расхода (диафрагма)		Трехходовой клапан с поршневым приводом
	Откалиброванная диафрагма с патрубками		Трехходовой шаровой клапан с поршневым приводом
	Датчик расхода (трансмиттер) со встроенной диафрагмой		Пневматическое реле
	Массовый расходомер		Соединение из плавкого нейлона на случай пожара
	Ротаметр с регулятором		Предохранительный клапан
	Ротаметр		Клапан сброса давления или вакуума (дыхательный клапан)

Продолжение таблицы 10.10

Шаровой регулирующий клапан с пневмоприводом		Электрический сигнал
Этот штурвал у того, у кого надо штурвал	o o—	Программная связь или передача данных
Редукционный клапан с внешним отбором	–	Пневматическая линия
Редукционный клапан с внутренним отбором	-X—X X	Капиллярная линия
, Дроссельный регулирующий клапан		Электромагнитный или акустический сигнал
Шаровой клапан с пневмоприводом	0	Полевой прибор
Двухходовой соленоидный клапан	©	Щитовой прибор
Угловой поршневой клапан	G	Прибор за щитом
Шиберный клапан с поршневым приводом	©	Прибор на местной панели
Трехходовой Соленоидный клапан	©	Прибор позади местной панели
Пара трехходовых соленоидных клапанов по схеме 1oo2	0	Лампочка состояния на местной панели

Окончание таблицы 10.

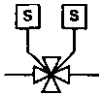
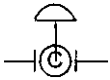
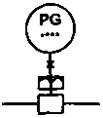
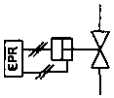
- Л -	Четырехходовой Соленоидный клапан	Г > Л
	Четырехпроходной с двумя соленоидами	7 h s 4 RESET А
	Клапан CAM FLEX	OPEN к Л CLOSE
О - о -	Шаровой клапан с поршневым приводом	pHS^D 14 А
i	Блокировочное устройство на агрегате	Ч У
	Двойной шаровой клапан	и
	Пневматический переключатель	е
	Электропневмопреобразователь (1/P)	о.
	Датчик давления в линии	е !
	Клапан затопления системы затопления	PKXXX
	Клапан с дублированным пневмораспределителем по схеме 2оо2	е

Таблица ЮЛ

Аббревиатуры КИПиА

AAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО АНАЛИЗУ
AE	ПЕРВИЧНЫЙ ИЗМЕРИТЕЛЬНЫЙ ЭЛЕМЕНТ АНАЛИЗАТОРА
AI	ИНДИКАТОР АНАЛИЗАТОРА
AIC	РЕГУЛЯТОР АНАЛИЗАТОРА С ИНДИКАЦИЕЙ
ASH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ АНАЛИЗАТОРА
AT	ТРАНСМИТТЕР (ДАТЧИК) АНАЛИЗАТОРА
AY	ПРЕОБРАЗОВАТЕЛЬ АНАЛИЗАТОРА
AR	АНАЛИЗАТОР С САМОПИСЦЕМ
AL	АЛГОРИТМ (ФУНКЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ)
AAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО АНАЛИЗУ
ASX	РЕЛЕ НЕИСПРАВНОСТИ
AAX	АВАРИЙНАЯ СИГНАЛИЗАЦИЯ НЕИСПРАВНОСТИ НА АНАЛИЗАТОРЕ
ASHH	РЕЛЕ ВЕРХНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ АНАЛИЗАТОРА
AAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО АНАЛИЗУ
AFY	ВЫЧИСЛИТЕЛЬНЫЙ БЛОК (ФУНКЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ)
BE	ДЕТЕКТОР ПЛАМЕНИ
BSH	РЕЛЕ НАЛИЧИЯ ПЛАМЕНИ
BAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ДЕТЕКТОРА ПЛАМЕНИ
DX	ИСТОЧНИК РАДИАЦИИ ДЛЯ ЗАМЕРА ПЛОТНОСТИ
DT	ТРАНСМИТТЕР ПЛОТНОСТИ

Продолжение таблицы 10.11

DY	УСИЛИТЕЛЬ (СИГНАЛА) ПО ПЛОТНОСТИ
DIC	РЕГУЛЯТОР ПЛОТНОСТИ С ИНДИКАТОРОМ
DE	ПЕРВИЧНЫЙ ИЗМЕРИТЕЛЬНЫЙ ЭЛЕМЕНТ ДЛЯ ЗАМЕРА ПЛОТНОСТИ
DR	САМОПИСЕЦ РЕГИСТРАЦИИ ПЛОТНОСТИ
FE	ПЕРВИЧНЫЙ ИЗМЕРИТЕЛЬНЫЙ ЭЛЕМЕНТ ДЛЯ ЗАМЕРА РАСХОДА
F0	ОГРАНИЧИТЕЛЬНАЯ ДИАФРАГМА
FICV	РОТАМЕТР С РЕГУЛЯТОРОМ РАСХОДА
FT	ТРАНСМИТТЕР (ДАТЧИК) РАСХОДА
FQI	ИНДИКАТОР СУММИРОВАНИЯ РАСХОДА
FQ	СУММАТОР РАСХОДА
FQT	ТРАНСМИТТЕР СУММИРОВАНИЯ РАСХОДА
FQHS	СУММАТОР РАСХОДА С РУЧНЫМ ПЕРЕКЛЮЧАТЕЛЕМ
FQIS	СУММАТОР РАСХОДА С ИНДИКАТОРОМ И РЕЛЕ
F1	ИНДИКАТОР РАСХОДА
FR	САМОПИСЕЦ РЕГИСТРАЦИИ РАСХОДА
FSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ РАСХОДА
FSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ РАСХОДА
FAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ РАСХОДА
FAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ РАСХОДА
FY	СОЛЕНОИДНЫЙ КЛАПАН ИЛИ ПРЕОБРАЗОВАТЕЛЬ
FV	(РЕГУЛИРУЮЩИЙ) КЛАПАН РАСХОДА

Продолжение таблицы 10.11

FSLL	РЕЛЕ НИЖНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ РАСХОДА
FALL	' НИЖНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ РАСХОДА
FDA	АВАРИЙНЫЙ СИГНАЛ ОТКЛОНЕНИЯ ПО РАСХОДУ (ОТ ЗНАЧЕНИЯ УСТАВКИ)
FF	РАСЧЕТ (ФУНКЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ)
FSY1	ЭЛЕКТРОПНЕВМОПОЗИЦИОНЕР ЗРК
FSY	СОЛЕНОИДНЫЙ КЛАПАН ЗРК
FIC	РЕГУЛЯТОР РАСХОДА С ИНДИКАТОРОМ
FZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
FZSL	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ
FZLL	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ЗАКРЫТ
FZLH	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ОТКРЫТ
HS	КЛЮЧ РУЧНОГО УПРАВЛЕНИЯ
HIC	РУЧНОЙ РЕГУЛЯТОР С ИНДИКАЦИЕЙ
HY	СОЛЕНОИДНЫЙ КЛАПАН ИЛИ ПРЕОБРАЗОВАТЕЛЬ
HV	КЛАПАН РУЧНОГО УПРАВЛЕНИЯ
HX	ПНЕВМАТИЧЕСКИЙ РАСПРЕДЕЛИТЕЛЬ
HZSL	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ
HZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
HZLL	ИНДИКАЦИЯ - КЛАПАН ЗАКРЫТ
HZLH	ИНДИКАЦИЯ - КЛАПАН ОТКРЫТ
II	. ИНДИКАТОР ТОКА (АМПЕРМЕТР)

Продолжение таблицы ЮЛ

IT	ДАТЧИК ТОКА
ISH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ТОКУ
ISL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ТОКУ
IAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ТОКУ
IAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ТОКУ
IA	СИГНАЛИЗАЦИЯ БЛОКИРОВКИ (АКТИВИРОВАНО / СБОЙ)
JT	ТРАНСМИТТЕР (ДАТЧИК) МОЩНОСТИ
JI	ИНДИКАТОР МОЩНОСТИ
JSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ " ПО МОЩНОСТИ
JSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ 1 ПО МОЩНОСТИ
JAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО МОЩНОСТИ
JAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО МОЩНОСТИ
KC	ТАЙМЕР ИЛИ ПРОГРАММИРУЮЩЕЕ УСТРОЙСТВО
KV	СОЛЕНОИДНЫЙ КЛАПАН - В ЛИНИИ
LI	ИНДИКАТОР УРОВНЯ
LX	ИСТОЧНИК РАДИАЦИИ ДЛЯ ЗАМЕРА УРОВНЯ
LC	КОНТРОЛЛЕР УРОВНЯ
LT	ТРАНСМИТТЕР (ДАТЧИК) УРОВНЯ
LSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО УРОВНЮ
LSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО УРОВНЮ
LSLL	РЕЛЕ НИЖНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО УРОВНЮ

Продолжение таблицы 10.11

LSHH	РЕЛЕ ВЕРХНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО УРОВНЮ
LIC	РЕГУЛЯТОР УРОВНЯ С ИНДИКАЦИЕЙ
LR	i САМОПИСЕЦ РЕГИСТРАЦИИ УРОВНЯ
LAH	. ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО « УРОВНЮ
LAL	"НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО УРОВНЮ
LALL	, НИЖНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО УРОВНЮ
LAHH	; ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО УРОВНЮ
LY	; СОЛЕНОИДНЫЙ КЛАПАН ИЛИ КОНВЕРТЕР
LV	, (РЕГУЛИРУЮЩИЙ) КЛАПАН ПО УРОВНЮ
LP	МЕСТНАЯ ПАНЕЛЬ
LZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
LZSL	| КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ
LZLL	. ИНДИКАЦИЯ на рабочей станции - КЛАПАН ЗАКРЫТ
L2LH	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ОТКРЫТ
LSY1	I ЭЛЕКТРОПНЕВМОПОЗИЦИОНЕР ЗРК
LSY	СОЛЕНОИДНЫЙ КЛАПАН ЗРК
LDA	! СИГНАЛ ОТКЛОНЕНИЯ ПО УРОВНЮ
PI	ИНДИКАТОР ДАВЛЕНИЯ / ИНДИКАТОР ЗАПИТКИ КОНТУРА
PT	ТРАНСМИТТЕР ДАВЛЕНИЯ
PSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ; ПОДАВЛЕНИЮ
PSL	: РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ' ПОДАВЛЕНИЮ

Продолжение таблицы 10.11

PSHL	РЕЛЕ ПЕРЕКЛЮЧЕНИЯ НИЗКОЙ/ВЫСОКОЙ УСТАВКИ ПО ДАВЛЕНИЮ	
PDSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ДИФФЕРЕНЦИАЛЬНОМУ ДАВЛЕНИЮ	
PDSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ДИФФЕРЕНЦИАЛЬНОМУ ДАВЛЕНИЮ	I
PSLL	РЕЛЕ НИЖНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО ДАВЛЕНИЮ	
PSE	ПРЕДОХРАНИТЕЛЬНАЯ (РАЗРЫВНАЯ) МЕМБРАНА ПО ДАВЛЕНИЮ	
PDT	ТРАНСМИТТЕР ДИФФЕРЕНЦИАЛЬНОГО ДАВЛЕНИЯ	
PIC	РЕГУЛЯТОР ДАВЛЕНИЯ С ИНДИКАТОРОМ	
PDI	ИНДИКАТОР ДИФФЕРЕНЦИАЛЬНОГО ДАВЛЕНИЯ	
PDIC	РЕГУЛЯТОР ДИФФЕРЕНЦИАЛЬНОГО ДАВЛЕНИЯ С ИНДИКАЦИЕЙ	
PAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ДАВЛЕНИЮ	
PAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ДАВЛЕНИЮ	1
PAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ДАВЛЕНИЮ	1
PALL	НИЖНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ДАВЛЕНИЮ	
PDAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ДИФДАВЛЕНИЮ	
PDAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ДИФДАВЛЕНИЮ	
PR	САМОПИСЕЦ РЕГИСТРАЦИИ ДАВЛЕНИЯ	
PY	СОЛЕНОИДНЫЙ КЛАПАН ИЛИ КОНВЕРТЕР	
PV	(РЕГУЛИРУЮЩИЙ) КЛАПАН ДАВЛЕНИЯ	
PCV	САМОРЕГУЛИРУЮЩИЙСЯ КЛАПАН ДАВЛЕНИЯ	
PSV	ПРЕДОХРАНИТЕЛЬНЫЙ / ПЕРЕПУСКНОЙ КЛАПАН	

Продолжение таблицы 10.11

PZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
PZSL	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ
PZLL	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ЗАКРЫТ
PZLH	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ОТКРЫТ
PSY1	ЭЛЕКТРОПНЕВМОПОЗИЦИОНЕР ЗРК
PSY	СОЛЕНОИДНЫЙ КЛАПАН ЗРК
PDAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ДИФДАВЛЕНИЮ
PDALL	НИЖНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ДИФДАВЛЕНИЮ
QL	ЛАМПОЧКА ИНДИКАЦИИ КУМУЛЯТИВНОГО СБОЯ СИСТЕМЫ
QA	АВАРИЙНЫЙ СИГНАЛ КУМУЛЯТИВНОГО ТИПА
SV	ПРЕДОХРАНИТЕЛЬНЫЙ КЛАПАН
SE	ЭЛЕМЕНТ ИЗМЕРЕНИЯ СКОРОСТИ (СЕНСОР)
SS	РЕЛЕ СКОРОСТИ
SSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО СКОРОСТИ
SSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО СКОРОСТИ
SAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО СКОРОСТИ
SAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО СКОРОСТИ
SI	ИНДИКАТОР СКОРОСТИ
TW	ТЕРМОКАРМАН (ИЗМЕРИТЕЛЬНЫЙ КАРМАН)
TE	ПЕРВИЧНЫЙ ТЕМПЕРАТУРНЫЙ ЭЛЕМЕНТ
TT	ТРАНСМИТТЕР (ДАТЧИК) ТЕМПЕРАТУРЫ

Продолжение таблицы 10.11

TSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ТЕМПЕРАТУРЕ
TSL	РЕЛЕ НИЖНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ТЕМПЕРАТУРЕ
TSHH	РЕЛЕ ВЕРХНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ~ ПО ТЕМПЕРАТУРЕ
TSLL	РЕЛЕ НИЖНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО ТЕМПЕРАТУРЕ
TIC	РЕГУЛЯТОР ТЕМПЕРАТУРЫ С ИНДИКАТОРОМ
TI	ИНДИКАТОР ТЕМПЕРАТУРЫ
TAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ТЕМПЕРАТУРЕ
TAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ТЕМПЕРАТУРЕ
TAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ТЕМПЕРАТУРЕ
TALL	НИЖНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ТЕМПЕРАТУРЕ
TY	СОЛЕНОИДНЫЙ КЛАПАН ИЛИ КОНВЕРТЕР
TV	КЛАПАН РЕГУЛЯТОРА ТЕМПЕРАТУРЫ
TCV	САМОРЕГУЛИРУЮЩИЙСЯ КЛАПАН ПО ТЕМПЕРАТУРЕ
TDR	ТРАНСМИТТЕР РАЗНОСТИ ТЕМПЕРАТУР
TDA	АВАРИЙНЫЙ СИГНАЛ ОТКЛОНЕНИЯ ПО ТЕМПЕРАТУРЕ
TZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
TZSL	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ
TZLL	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ЗАКРЫТ
TZLH	ИНДИКАЦИЯ на рабочей станции - КЛАПАН ОТКРЫТ
TSY1	ЭЛЕКТРОПНЕВМОПОЗИЦИОНЕР ЗРК
TSY	СОЛЕНОИДНЫЙ КЛАПАН ЗРК

Продолжение таблицы ЮЛ

UA	КУМУЛЯТИВНЫЙ АВАРИЙНЫЙ СИГНАЛ
VT	ТРАНСМИТТЕР (ДАТЧИК) ВИБРАЦИИ
VI	ИНДИКАТОР ВИБРАЦИИ
VSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ВИБРАЦИИ
VSHH	РЕЛЕ ВЕРХНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО ВИБРАЦИИ
VAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ВИБРАЦИИ
VAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПО ВИБРАЦИИ
WT	ДАТЧИК ВЕСА
WIC	РЕГУЛЯТОР ВЕСА С ИНДИКАТОРОМ
WSH	РЕЛЕ ВЕРХНЕЙ ПРЕДУПРЕДИТЕЛЬНОЙ УСТАВКИ ПО ВЕСУ
WSHH	РЕЛЕ ВЕРХНЕЙ ПРЕДАВАРИЙНОЙ УСТАВКИ ПО ВЕСУ
WAH	ВЕРХНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПОВЕСУ
WAHH	ВЕРХНЯЯ ПРЕДАВАРИЙНАЯ СИГНАЛИЗАЦИЯ ПОВЕСУ
WSLH	ПЕРЕКЛЮЧАТЕЛЬ ВЕСА "НИЗКИЙ / ВЫСОКИЙ"
WALH	СИГНАЛИЗАЦИЯ ПЕРЕКЛЮЧЕНИЯ ВЕСА
XV	ДВУХПОЗИЦИОННЫЙ КЛАПАН
XA	ОТКЛЮЧЕНИЕ НАДДУВА С МЕСТНОЙ ПАНЕЛИ
XY	СОЛЕНОИДНЫЙ КЛАПАН
XS	РЕЛЕ
XZSH	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ОТКРЫТ
XZSL	КОНЦЕВОЙ ВЫКЛЮЧАТЕЛЬ - КЛАПАН ЗАКРЫТ

Окончание таблицы 10.11

XZLH	ИНДИКАЦИЯ - КЛАПАН ОТКРЫТ
XZLL	ИНДИКАЦИЯ - КЛАПАН ЗАКРЫТ
XX	ПНЕВМАТИЧЕСКИЙ РАСПРЕДЕЛИТЕЛЬ
YAL	НИЖНЯЯ ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ ПО ДВИГАТЕЛЮ
YLH	ЛАМПОЧКА СВЕТОВОЙ ИНДИКАЦИИ О РАБОТЕ ДВИГАТЕЛЯ
YSLH	РЕЛЕ СОСТОЯНИЯ ДВИГАТЕЛЯ
YS	РЕЛЕ УПРАВЛЕНИЯ ДВИГАТЕЛЕМ (МЕСТНОЕ / ДИСТАНЦ.)
YL	ИНДИКАТОР УПРАВЛЕНИЯ ДВИГАТЕЛЕМ (ДЛЯ МЕСТН / ДИСТАНЦ)
YLL	ЛАМПОЧКА СВЕТОВОЙ ИНДИКАЦИИ ОСТАНОВКИ ДВИГАТЕЛЯ
ZL	СВЕТОВАЯ ИНДИКАЦИЯ ПОЛОЖЕНИЯ
ZS	ОКОНЕЧНЫЙ ВЫКЛЮЧАТЕЛЬ (КОНЦЕВИКИ)
ZI	ИНДИКАТОР ПОЛОЖЕНИЯ
ZT	ТРАНСМИТТЕР (ДАТЧИК) ПОЛОЖЕНИЯ
ZAL	ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ "ЗАКРЫТО"
ZAH	ПРЕДУПРЕДИТЕЛЬНАЯ СИГНАЛИЗАЦИЯ "ОТКРЫТО"
ZLH	ИНДИКАТОР "ОТКРЫТО" (ЛАМПОЧКА)
ZLL	ИНДИКАТОР "ЗАКРЫТО" (ЛАМПОЧКА)
ZSH	РЕЛЕ ПОЛОЖЕНИЯ - ОТКРЫТО
ZSL	РЕЛЕ ПОЛОЖЕНИЯ - ЗАКРЫТО
ZX	ПНЕВМАТИЧЕСКИЙ РАСПРЕДЕЛИТЕЛЬ

10.2. Ключевые идеи

Общепринятый способ построения системы кодирования состоит в следующем. Вам объясняют, что:

- В первой позиции кода может стоять любая из 20-26 букв латинского алфавита;
- Во второй - любая из 5 букв;
- В третьей - любая из 7 и т.д.

В итоге возникает 20*5*7*... возможных комбинаций кода, плюс несколько десятков уникальных обозначений для особых случаев. Навряд ли кто-либо способен угадать точную функцию популярных кодов HS, HC, HPB кроме невразумительного "ручного воздействия", поскольку эти коды используются и для обозначения изменений состояния (статуса) объекта управления, и собственно для управления, причем самыми разнообразными объектами.

Ключевая идея предлагаемого подхода состоит в целенаправленном управлении сложностью информационной модели объекта автоматизации и, прежде всего, в ограничении общего количества различных вариантов кодировок.
Добиться этого возможно за счет:

1. Жесткого отбора только тех функциональных признаков, без которых действительно нельзя обойтись;
2. Четкого определения "своего законного места" для каждого параметра системы - как по типу, так и по выполняемой функции;
3. Строгого задания шаблона кодировки для каждого **информационного** элемента системы.

Требуется решить эту задачу: система должна обеспечивать только необходимое разнообразие.

10.3. Построение перечней входов и выходов РСУ и ПАЗ

В качестве исходной модели использован некий условный проект (таблица 10.12, для иллюстрации приведена первая страница). Входы-выходы системы сгруппированы по контурам. Это удобно при составлении первоначального перечня параметров. Форма электронной таблицы позволяет в дальнейшем легко сделать выборку и сортировку по любой комбинации полей:

- Цех / узел / аппарат;
- РСУ/ПАЗ;
- Вход / выход и т.д.

Набор полей может видоизменяться в зависимости от принятых подходов. Например, кроме колонок со значениями шкалы "прибора" в этой же таблице могут быть указаны и значения предупредительной, предаварийной сигнализации, и т.д. Смысл колонок Перечня входов-выходов понятен из заголовков, однако есть особенности.

Колонка Позиция. Для реконструируемого производства содержит существующую, действующую позицию КИПиА. Отечественная традиция кодировки предполагает цифровой код, который может сопровождаться цифровым или буквенным суффиксом, уточняющим позицию.

Особенность суффикса и кода как такового состоит в том, что он может содержать символы русского алфавита, некоторые из которых совпадают по начертанию (но не по кодировке!) с латинскими.

Поэтому при набивке параметров требуется некоторое внимание к раскладке и регистру клавиатуры, чтобы в дальнейшем не создавать проблем с сортировкой и выборкой.

Автоматизированная работа с перечнем на уровне электронной таблицы предоставляет возможность сортировки и выборки требуемой группы параметров, и, соответственно, ускоряет отладку системы.

Смешение русских и латинских символов с арабскими цифрами не" возбраняется, однако должно быть единообразным.

Символьный код входа-выхода. Перед колонкой Позиция введен дополнительный символьный код (колонка "Датчик"), соответствующий международной транскрипции входных и выходных для РСУ и ПАЗ ***физических полевых устройств*** КИПиА.

Первый символ кода соответствует измеряемой величине, второй - типу устройства входа-выхода.

Дополнительно могут в конце кода могут присутствовать еще один или два символа, которые уточняют конкретную характеристику параметра.

Замечание

Надо подчеркнуть, что Перечень входов-выходов АСУТП - это перечень ***именно*** *ВХОДОВ - ВЫХОДОВ, поэтому при формировании стандартного контура управления используются две строки:*
Первая - для идентификации входа,
вторая - для идентификации выхода.

Пример контура управления по температуре:

- TIC - TE - 0825A,
- TIC - TY-0825A,

где код TE-0825A рассматривается как обозначение первичного измерительного элемента,

- TY - 0825A - как код электропневмопреобразователя, а
- TIC - 0825A - как кодировка контура управления в целом.

Кодировка электропневмопреобразователя TY часто совмещается с кодом клапана TV, и в Перечне указывается обобщенное обозначение выхода TV.

Для обозначения первичного температурного элемента (термопара, термосопротивление) сохранено традиционное обозначение TE.

Измерительные преобразователи со стандартным выходом 4-20мА *(Transmitters)* принято помечать суффиксом T:

FT, LT, PT, TT.

Коды контуров РСУ и ПАЗ. Для взрывоопасных объектов требуется соблюдение требований по резервированию систем контроля параметров, а также по обеспечению резервирования необходимого типа для систем безопасности с информационной, временной и функциональной избыточностью, и наличием систем диагностики и самодиагностики.

Однако в некоторых случаях интересы РСУ и ПАЗ могут пересекаться не только на логическом, но и на физическом уровне.

Для того чтобы выделить контуры "совместного ведения" (например, при использовании одного общего входа) на фоне ординарных контуров управления РСУ, в системе ПАЗ в их кодировку добавлена буква S.

Таблица 10 J 2

Титул	Зона	Ёдобор	Контур					Позиция	Наименование параметра	ПАЗ	РСУ		Ex	,,,,	Макс.шк	Е Л . »	Сигнал	Действие регулятора	1—1	Диаметр клапана мм	Сигнализация		Блокировка		
																					L		LL	HH	
Т 12/4	0	12 фев	р	I			РТ	220	Давление азота на вводе в т 12/2		DCS	AI	1	0	25	кгс/см^	4 20mA								
Т 12/4	О	12 фев	F	I			FT	305	Расход азота на вводе в Т-12/2		DCS	AI	1	0	1250	НМН	4-2 0mA								
Т 12/4	О	№2205	F	I			FT	0522	Расход теплофикационном воды		DCS	AI	1	0	125	т/ч	4 20mA								
Т 12/4	О	№2205	F	I			FT	0555	Расход водорода на хроматографы		DCS	AI	1	0 24	24	кг/ч	4-20mA								
Т 12/4	0	№2205/6	F	I			FT	220	Расход обессоленной воды		DCS	AI	1	0	100	т/ч	4-20mA								
Т 12/4	А	Е-022-1А	L	I			LT	0512А	Уровень в Е-022-1А		DCS	AI	1	0	800	мм	4-2 0mA				200	640			
Т 12/4	А	Е-022-1А	Т	I	С		ТЕ	0225А	Регулир т-ры в Е 022 1А		DCS	AI	1	50	50	°С	ХА								
Т 12/4	А	£-022-1А	Т	I	С		TV	0225А	Регулир т-ры в Е-022-1А		DCS	AO	1			%	4 20mA	обр	н з	25					
Т 12/4	Б	Е-022-1Б	L	I			LT	05128	Уровень в Е-022-1Б		DCS	AI	1	0	800	мм	4 20mA				200	640			
Т 12/4	Б	Е-022-1Б	Т	I	С		ТЕ	0225В	Регулир т-ры в Е-022-1Б		DCS	AI	1	50	50	"С	ХА								
Т 12/4	Б	Е-022 1Б	Т	I	С		TV	0225В	Регулир т ры в Е-022 1Б		DCS	AO	1			%	4 20mA	обр	НЗ	25					
Т 12/4	О	Е-022-2	L	I			LT	513	Уровень в Е-022-2		DCS	AI	1	0	1000	мм	4-2 0mA					800			
Т 12/4	О	Е-303А	Т	I			ТЕ	107А-5	Темп-ра в Е-303А		DCS	AI	1	0	150	℃	ХА					140			
Т 12/4	О	Е-ЭО3А	Р	I			РТ	233А	Давление в Е ЭО3А		DCS	AI	1	0	10	кгс/см²	4-20mA								
Т 12/4	О	Е-ЭО3А	L	I			LT	216	Уровень в Е ЭО3А		DCS	AI	1	0	3000	мм	4-20mA								
Т 12/4	А	К001А	Т	I			ТЕ	107 А 1	Т ра в ха на входе в К 001А		DCS	AI	1	0	300	℃	ХА								
Т 12/4	А	К-001А	Т	I			ТЕ	107А-2	Темп-ра в-ха после К-001А		DCS	AI	1	0	150	℃	ХА								
Т 12/4	А	К001А	F	I			FT	310А	Расход воды в цех водоподготовки		DCS	AI	1	0	12,5	т/ч	4-20mA								
Т 12/4	А	К-001А	L	I	С	S	LT	200А	Регулир уровня в верхней секции К-001А	ESD	DCS	AI	1	0	800	мм	4 20mA				160	640	80		
Т 12/4	А	К001А	L	I	С	S	LV	200А	Регулир уровня в верхней секции К-001А		DCS	AO	1			%	4-20mA	прям	НЗ	40					
Т 12/4	А	К-001А	L	I	С	S	LV	200А	Регулир уровня в верхней секции К-001А		DCS	AO	1			%	4-20mA	прям	НЗ	40					
Т 12/4	А	К001А	L	I	С	S	LT	201А	Регулир уровня в нижней секции К-001А	ESD	DCS	AI	1	0	800	мм	4-2 0mA				160	640	80		
Т 12/4	А	К-001А	L	I	С	S	LV	201А	Регулир уровня в нижней секции К-001А		DCS	AO	1			%	4-20mA	обр	НЗ	25					
Т 12/4	Б	К-001Б	Т	I			ТЕ	107В-1	Т ра в-ха на входе в К 001Б		DCS	AI	1	0	300	℃	ХА								
Т 12/4	Б	К-001Б	Т	I			ТЕ	107В-2	Темп-ра в-ха после К-001Б		DCS	AI	1	0	150	℃	ХА								
Т 12/4	Б	К-001Б	L	I	С	S	LT	200В	Регулир уровня в верхней секции К 001Б	ESD	DCS	At	1	0	800	мм	4-20mA				160	640	80		
Т 12/4	Б	К-001Б	L	I	С	S	LV	200В	Регулир уровня в верхней секции К-001Б		DCS	AO	1			%	4-20mA	прям	НЗ	40					
Т 12/4	Б	К-001Б	L	I	С	S	LV	200В	Регулир уровня в верхней секции К-001Б		DCS	AO	1			%	4-2 0m А	прям	НЗ	40					
Т 12/4	Б	К-001Б	L	I	С	S	LT	201В	Регулир уровня в нижней секции К-001Б	ESD	DCS	AI	1	0	800	мм	4-2 0mA				160	640	80		
Т 12/4	Б	К-001Б	L	I	С	S	LV	201В	Регулир уровня в нижней секции К 001Б		DCS	AO	1			%	4-2 0mA	обр	НЗ	25					
Т 12/4	А	К-101 3А	F	1			FT	325А	Расход насыщенного сорбента из К-101 3А		DCS	AI	1	0	800	т/ч	4-20mA								
Т 12/4	Б	К-101.3Б	F	1			FT	325В	Расход насыщенного сорбента из К-101, 3Б		DCS	AI	1	0	800	т/ч	4-20mA								
Т 12/4	А	К-101 А	Т	1			ТЕ	110А-1	Темп-ра контактного газа на входе в К 101А		DCS	AI	1	0	150	℃	ХА								
1124	А	К-101 А	Т	1			ТЕ	110А2	Темп-ра сорбента на входе в К 101А		DCS	AI	1	0	50	°С	ХА								
Т 12/4	А	К-101А	Т	1			ТЕ	110А5	Темп-ра сорбента в К-101А (32-я тарелка)		DCS	AI	1	0	100	"С	ХА								
Т 12/4	А	К-101А	т	1			ТЕ	110А-6	Темп-ра газа на выходе из К-101 А		DCS	AI	1	0	100	℃	ХА								
Т 12/4	А	К-101А	р	1			PdT	222А	Перепад давл в К-101А		DCS	AI	1	0	0 63	кгс/см*¹	4-2 0mA					0 39			
Т 12/4	А	К-101А	р	1			РТ	225А	Давление в К-101 А		DCS	AI	1	0	40	кгс/см"	4-2 0mA								
Т 12/4	А	К-101А	F	1	С		FT	322А	Регулир расхода сорбента в К-101А		DCS	AI	1	0	630	т/ч	4-20mA								
Т 12/4	А	К-101А	F	1	С		FV	322А	Регулир расхода сорбента в К-101 А		DCS	AO	1			%	4-20mA	обр	НЗ	200					

Примеры:

Параметры системы ПАЗ:

FICS, LICS, PICS, TICS.

При этом в РСУ соответствующий символ S заменяется символом A:

FICA, LICA, PICA, TICA.

Однако нет никаких препятствий к тому, чтобы использовать совпадающие коды и в системе ПАЗ, и в РСУ на основе единого символа S:

FCS, LCS, PCS, TCS.

Примером подобного раздвоения одного общего входа и для РСУ, и для ПАЗ является следующая схема контура управления и защиты:

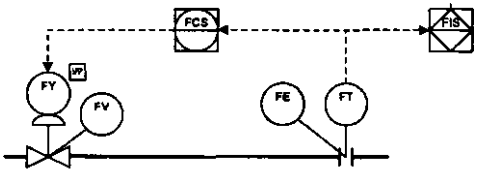


Рис.10.1

Стандартный способ обвязки в подобной ситуации предписывает пропускать сигнал сначала через ПАЗ, а только потом из ПАЗ в РСУ:

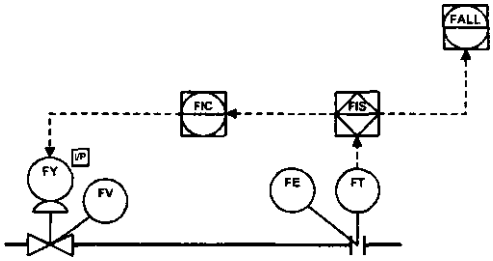


Рис .10.2

Единообразие кодировки в РСУ и ПАЗ вполне согласуется с рекомендациями стандарта ANSI/ISA S5.1-1984.

Замечание внизу таблицы 10.2 к группе параметров *"Switches and Alarm Devices",* помеченное одной звездочкой, гласит:

* A - *сигнализация, устройство оповещения* - может использоваться тем же образом, что и S - *ключ, инициирующее устройство.*

Замечание

Традиционное отечественное обозначение контуров данного типа выглядит следующим устрашающим образом:

LRCSA, LICSA, или даже LIRCSA.

Это обозначение есть результат буквального применения ломового положения стандарта ГОСТ 21.404-85 "Обозначения условные приборов и средств автоматизации в схемах", пункт 2.8:

Порядок расположения буквенных обозначений функциональных признаков прибора принимают с соблюдением последовательности обозначений: I, R, C, S, A".

Уму непостижимо: как можно было умудриться на ровном месте удвоить число необходимых символов с трех до шести?! Человечеству известен всего один способ удвоения, да и то ненадолго: "*Однако! Я чувствую, что после водки вы пили еще и портвейн! Помилуйте, да разве это можно делать!"*

Применительно к цифровым системам управления эти обозначения являются избыточными, поскольку применение вычислительной техники подразумевает и индикацию (I) , и регистрацию (R), и сигнализацию (A). Символ R может применяться лишь для обозначения действительно самопишущих щитовых приборов.

Поэтому в нашей системе координат символы R и A при идентификации ординарных контуров управления не используются:

FIC, LIC, PIC, TIC

Более того, символ индикации I сохранен только как дань традиции. Для обычных регуляторов вполне можно обойтись двухсимвольной кодировкой:

FC, LC, PC, TC

Эти коды замечательным образом укладываются в цепочку кодов контура регулирования:

FE - FT - FC - FY - FV

10.4. Постановка задачи

Стандарт ISA дает достаточно строгую систему идентификации аналоговых сигналов. Однако в кодировке дискретных параметров современных систем управления и защиты обнаруживается существенный пробел.

Это касается элементов технологического оборудования, которые имеют четко выраженные дискретные характеристики состояния и управления:

- Включен / Выключен
- Включить / Выключить
- Открыт / Закрыт
- Открыть / Закрыть и т.д.

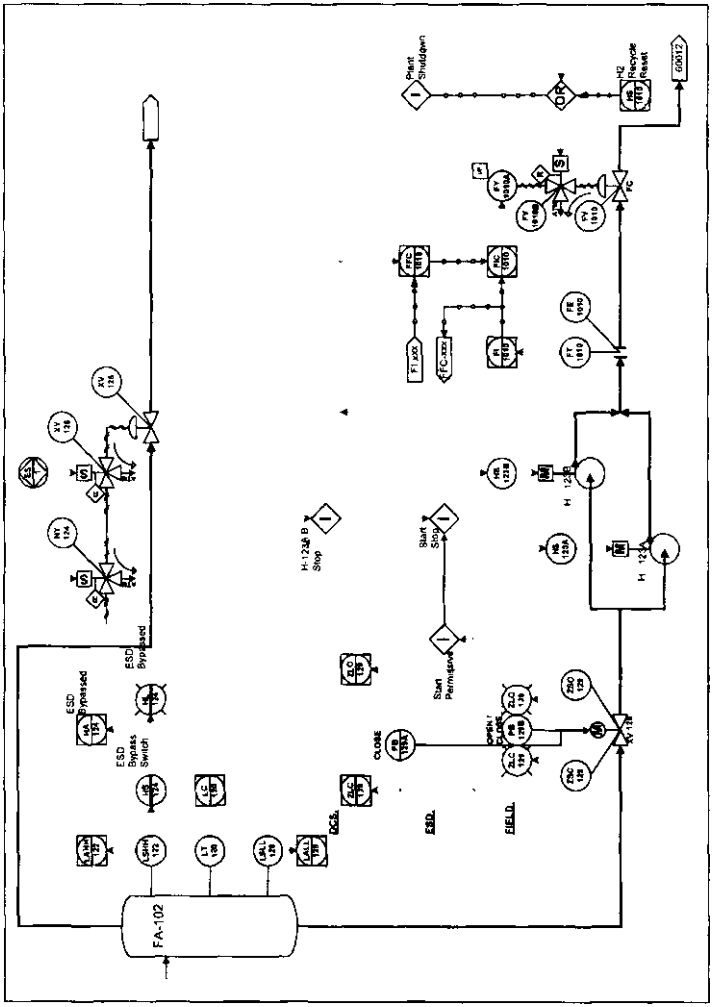
Поэтому проектировщики и разработчики систем вынуждены изобретать собственные коды для идентификации дискретных параметров состояния и управления.

Чтобы наглядно показать степень различия используемых способов кодировки и вариантов графики, на рис.10.3 и 10.4 представлены фрагменты функциональных схем автоматизации в конкретных применениях.

В качестве иллюстрации и инструмента для дальнейшего анализа в таблицах 10.13-10.15 приведены примеры кодов, которые используют различные организации для обозначения ключевых единиц оборудования, имеющих непосредственное отношение к обеспечению безопасности и защиты процесса:

- Электрозадвижек,
- Отсекателей,
- Насосов.

Даже поверхностный взгляд на представленные исходные материалы приводит к очевидному выводу: единообразие подхода отсутствует.


Plant Shutdown
OR
H2 Recycle Reset
FA-102
ESD Bypassed
ESD Bypass Switch
H-124B B Stop
Start Stop
Start Permissive
OPEN
CLOSE
ESD
FIELD
H-124B

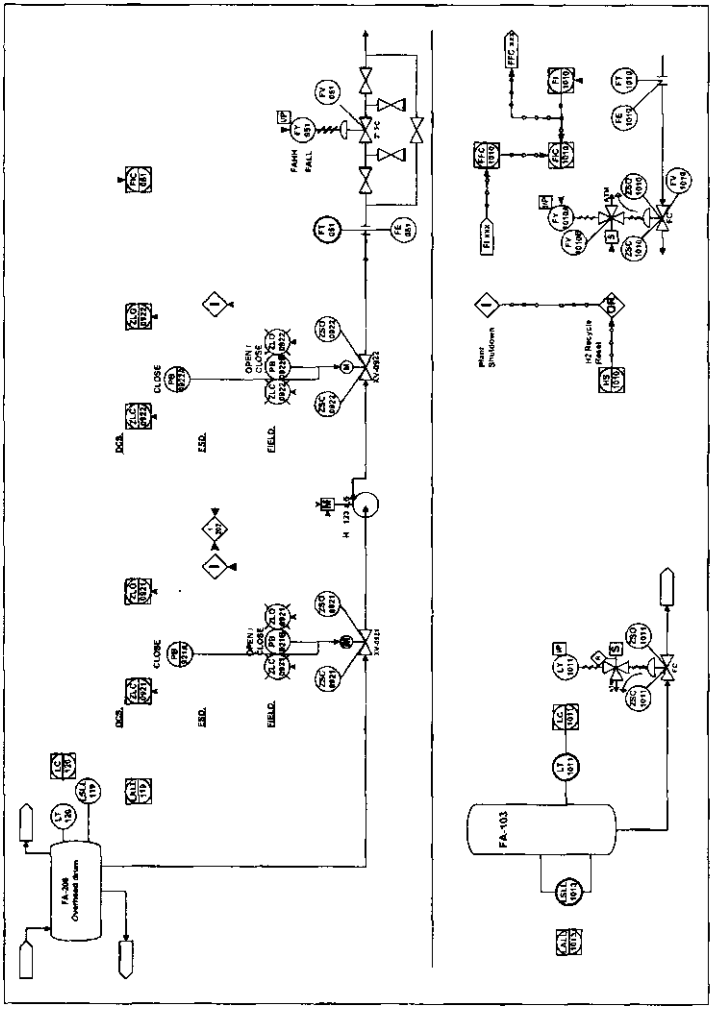

FA-103
Plant Shutdown
H2 Recycle Failed
FAHH
FALL
OPEN / CLOSE
CLOSE
DCS
ESD
FIELD

Рис. 10.4

Таблица 10.13

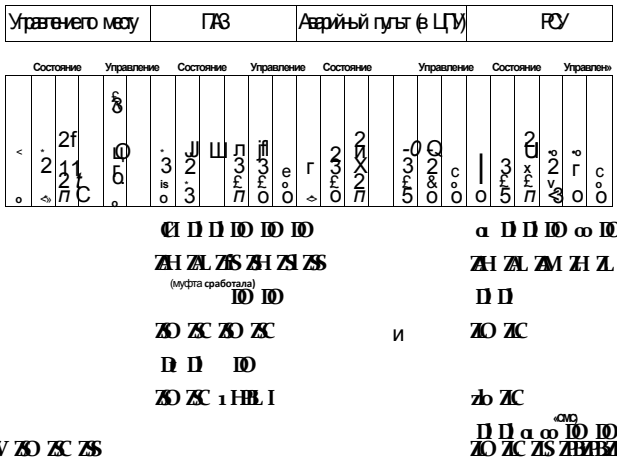


Таблица 10.14

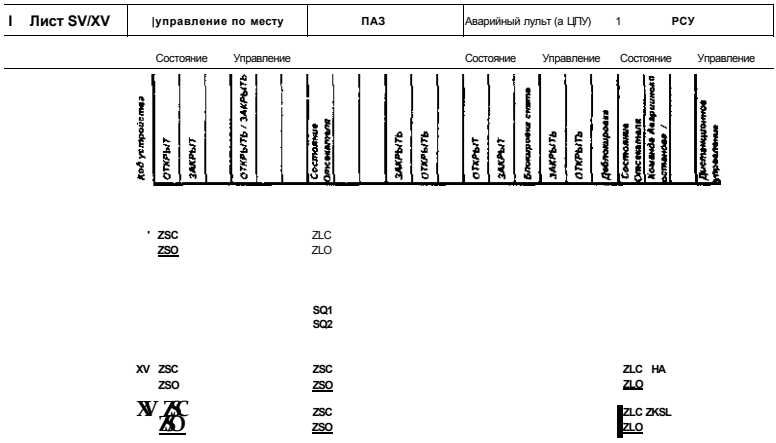
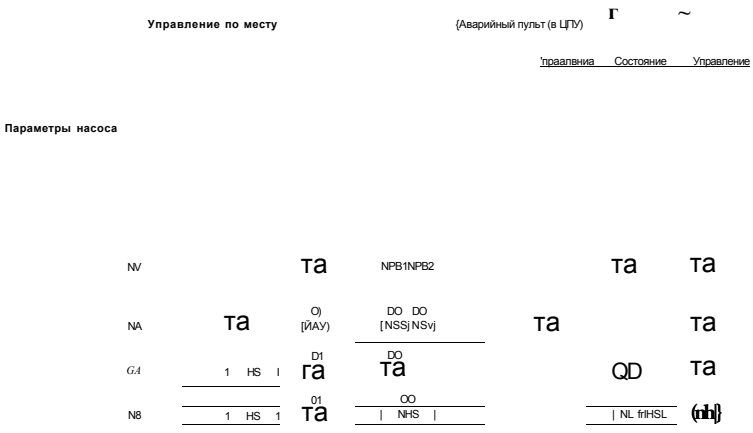


Таблица 10 А 5



Промежуточные результаты анализа. Западные фирмы используют более или менее устойчивые способы идентификации параметров дискретных устройств ***только для отсекателя и задвижки***, да и то лишь для параметров состояния. Причем коды состояний и отсекателя, и задвижки совпадают:

- ZSC / ZSO - обозначение собственно концевиков - и отсекателя, и задвижки;
- ZSC / ZSO - обозначение состояний и отсекателя, и задвижки в системе ПАЗ;
- ZLC / ZLO - обозначение сигнализации состояний и отсекателя, и задвижки в РСУ.

Более того, часто совпадают и коды собственно отсекателя и задвижки, но уже с другим первым символом - XV.

Причем необходимо обратить внимание, что все перечисленные коды отличаются от рекомендованных стандартом ISA S5.1-1984:

ISA рекомендует коды ZSL / ZSH.

Самостоятельная идентификация запорно-регулирующих клапанов никем вообще не рассматривается.

Чтобы продемонстрировать, насколько вычурными могут быть способы кодирования состояний запорно-отсечной арматуры даже у самых известных западных фирм, ниже приводится пример обвязки отсекателя:

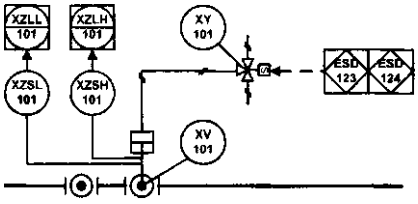


Рис. 10.5

И пример обвязки насоса, который заслуживает внимания как вариант использования символа Y *(Event, State, Presence)* конкретно для обвязки насоса:

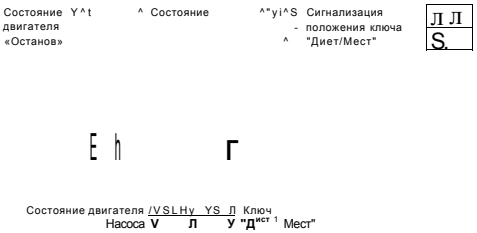


Рис. 10.6

10.5. Коды состояний ISA

Стандарт ISA S5.1-1984 для идентификации состояния запорно-регулирующей арматуры рекомендует обозначения ZSL и ZSH, где смысл использованных символов состоит в следующем:

Z - *Position; Dimension* - Положение; Размер
S - *Safety / Switch* - Безопасность / Ключ
L / H - *Low /High* - Низкий / Высокий

Казалось бы, структура этого кода безупречна, и целиком находится в структуре стандарта. Соответственно, и сам код принадлежит множеству допустимых кодов ISA.

Почему же практически все американские фирмы используют коды ZSC и ZSO, которые отсутствуют в американском же стандарте ANSI/ISA S5.1-1984?

Причина заключается в абсолютной индифферентности кодов ZSL и ZSH по отношению к объекту идентификации. Замена L на C и H на O позволяет дать точное определение именно концевых выключателей отсекающего устройства.

Однако до конца проблема идентификации не решается:

Мы не можем определить тип устройства.

Код ZS_ характеризует **СОСТОЯНИЕ СОСТОЯНИЯ,** то есть абсолютно лишен какой бы то ни было привязки к параметру или устройству, состояние которого он характеризует. Именно это обстоятельство заставляет разработчиков использовать и коды ZSL - ZSH, и коды ZSC — ZSO для обозначения состояния концевиков ВСЕХ устройств, которые их могут иметь: и отсекатели, и задвижки, и запорно-регулирующие клапаны, - они просто не имеют другой возможности.

Ошибка создателей стандарта ANSI/ISA S5.1-1984 возникла из-за того, что в качестве первой буквы кода использована **ХАРАКТЕРИСТИКА** технологической переменной, а не сама **ПЕРЕМЕННАЯ,** как это предначертано всем строем таблиц 10.1 и 10.2.

Аналогичная история произошла с символом

Y - Событие, *Состояние; Присутствие /Наличие.*

Оба символа - и Y, и Z, - использованные в качестве первого символа, не имеют и не могут иметь принадлежности ни к какой **конкретной** технологической переменной, ни к какому элементу **конкретного** оборудования.

Эти символы могут быть характеристиками только того оборудования, к которому они приписаны на монтажно-технологической схеме. Другого способа самоидентификации они не имеют.

Сходная проблема, но уже при идентификации управляющих воздействий, инициированных оператором процесса, возникает для кода H (Hand - Рука). Коды ручного управления также не имеют "национальной" принадлежности: HIC, HC, HS, HV. Поэтому без физической привязки к технологическому процессу определить принадлежность этого кода невозможно.

Достаточно привести пример:

FT-001	-	FIC-001	-	FV-001
LT-001	-	LIC-001	-	LV-001
PT-001	-	PIC-001	-	PV-001
TT-001	-	TIC-001	-	TV-001

Можно ли угадать к какому из перечисленных контуров относятся коды ZSL-001 или HS-001?

Тот аргумент, что кроме основного кода существует еще алфавитно-цифровое расширение, служит не решению проблемы, а скорее запутывает ее решение. Попытка дать уникальные коды расширения разрушает единство контура, и резко увеличивает многообразие кодов. В данной главе предлагаются способы решения этих проблем. И наши решения позволяют адекватно описать и эту, и многие другие коллизии.

10.6. Неоднородность кодов ISA

Фактически все организованное содержание таблиц 10.1 и 10.2 сводится к одной простой формуле:

FV (FY) = FIC (FT),

где на месте символа F может стоять любой из символов первой колонки. Под FY подразумевается электропневмопреобразователь регулирующего клапана, под FV - собственно регулирующий клапан. Формула идеально работает при отсутствии событий, - до тех пор, пока не возникает необходимость дискретных операций:

- Штатный пуск - останов;
- Периодические процессы;
- Переключение оборудования на выпуск новой продукции;
- Техническое обслуживание;
- Противоаварийная защита.

Что же предлагает стандарт ISA для обработки событий? Практически ничего. Из 19 колонок таблицы 10.2 **ЛИШЬ ДВЕ** колонки представляют реальные выходные устройства:

1. Колонка *Solenoids, Relays, Computing Devices* с символом Y во второй позиции.
2. Колонка *Final Element* с символом V во второй позиции.

Причем для ординарных контуров управления оба символа относятся к одному и тому же выходному каналу Y—V, поэтому для идентификации выхода достаточно одного из них. Как правило, на практике так и происходит, и выходной канал обычно привязывается либо к электропневмопреобразователю FY, либо непосредственно к клапану - FV.

Если из таблицы 10.2 стандарта ISA сделать выборку по I см переменным, которыми определяются физические входы и выходы АСУТП, то возникает совершенно разрозненная картина:

Таблица 10J6

	AI	AO	DI	DO
C:	(FT)-FC-(FY)		-	-
S:	-	-	FSL FSH	HS
X:	-	-	-	-
Y:	-	FY	-	FY
Z:	-	-	ZSL ZSH	ZY

Символ С - ***Control,*** если не обращать внимание на избыточный символ I, находится во второй позиции кода.

Символ S - ***Safety***, также стоит во второй позиции, причем может использоваться и для идентификации входа, и 1ля идентификации выхода.

Символ X - один из самых значимых символов любого .шфавита, можно сказать, a-vita, - вообще не участвует в кодировке ISA.

Символ Y - ***Event, State; Presence***. Основное применение символа Y - вторая позиция кода для обозначения соленоида, реле, преобразователя, вычислительного блока.

Символ Z - ***Position; Dimension, -*** согласно ISA, может использоваться во второй позиции кода для обозначения нес тандартных исполнительных (выходных) элементов:

BZ, EZ, IZ, QZ, RZ, VZ, WZ, YZ.

Однако на практике Z используется только в качестве первого символа, и только для определения состояния оконечных **входных устройств.**

Представленная в таблице 10.16 выборка ясно доказывает, что стандартом ISA строго определена только функция ординарного регулирования:

FT - FC - FY.

Уже для событий функциональная связь с реакцией на их появление определяется только по дискретному выходу FY, который уже занят аналоговым выходом регулятора. Обработка дискретных кодов в рамках стандарта ISA может быть выражена формулой

FY = FA(L/H) = FS(L/H).

Внешняя согласованность этой формулы обманчива.

В отличие от формулы регулятора FC, мы не можем определить значение функции FY, - что это? - останов насоса, закрытие отсечного клапана, или нечто другое.

Еще более серьезная проблема возникает при выполнении операций пуска - останова и программно-логического управления. В этом случае необходима обратная связь с технологического объекта, подтверждающая выполнение команды. И только после подтверждения последовательность операций может быть продолжена. **Но стандарт ISA не имеет адекватных средств управления событиями.**

10.7. Семантика состояний

После гениального открытия Декартом системы координат, мы не имеем иной возможности для определения положения и состояния, кроме классического определения координат X, Y, Z.

Историческая справка

Рене Декарт (1596 - 1650г.) - величайший французский философ и математик.

Среди гениальных достижений Декарта находится определение понятия переменной величины, без которого было бы немыслимо открытие дифференциального и интегрального исчислений. Декарт ввел многие алгебраические обозначения: ныне общепринятые знаки для переменных величин x, y, z, коэффициентов a, Ь, c, ... , а также обозначения степеней x^2,

a^3, ... , которые ничем не отличаются от современных. Величайшим достижением Декарта является открытие метода координат (Декартовы координаты).

Семантика понятий, стоящих за символами, которые нас в данном случае интересуют (см. левую колонку таблицы 10.16), в чистом виде с очевидностью распределена следующим образом:

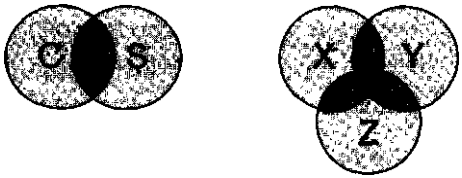


Рис. 4.7

В контексте нашей темы за символами C и S стоят следующие понятия:

C - Control - Контроль, Управление,
S - Safety - Безопасность.

Можно сказать, что символ C олицетворяет весь спектр функций управления. Символ S также подразумевает расширенные функции программно-логического управления, охватывающих весь спектр действий - от реакции на предупреждение до изменения состояния технологического оборудования (часть этих функций вполне может быть реализована в РСУ). За символами X, Y, Z не стоит, если так можно выразиться, "ничего", кроме декартовой системы координат, что, кстати говоря, отмечено стандартом ISA в колонке Modifier 1аблицы ЮЛ. Расположим области действия интересующих нас понятий контроля - защиты в единой цепи:

Рис. 10.8

Мы наблюдаем два взаимосвязанных процесса:

- При нарастании угрозы (перемещение вправо) возрастает значение дискретных операций вплоть до полного останова в состоянии **Z.**
- При возврате к норме (перемещение влево) усиливается роль непрерывного контроля и управления процессом С.

Качественный переход между Непрерывностью и Дискретностью обуславливается понятием Безопасность - *Safety* - и проходит по символу **S.**

10.8. Идентификация запорно-регулирующей арматуры

Исходя из предыдущего обсуждения принадлежность первого символа **С** и последнего символа **Z** в последовательности Непрерывность - Останов (рис. 10.8) определяется легко.

Регулирующий клапан. Не нужно особых аргументов в пользу того, что регулирующие клапаны должны определяться символом **С.**

Электрозадвижка. Последний символ алфавита **Z** естественным образом связывается с понятием полного останова.

Соответственно, обсуждению подлежат идентификаторы отсекателя и запорно-регулирующего клапана. Пойдем методом исключения - вначале определим наиболее приемлемый символ отсекателя. Тогда символ ЗРК определиться сам собой.

Отсекатель.

Рассмотрим возможные доводы в пользу использования оставшихся символов S, X, Y для идентификации Отсекателя.

Символ S:

- Символ непосредственно участвует в составе русских и английских понятий, имеющих отношение к защите: оСтанов, Старт, Стоп, Shutdown, cloSe, bypasS, Switch, и даже Shut up.
- "Эс" звучит в корне нашего слова отСекатель, и не нашего Соленоид.
- Символ S присутствует на графическом изображении соленоидного отсечного клапана:

- Наконец, символ S является зеркальным отражением символа Z, использованного для идентификации Задвижки.

Символ X.

Символ X довольно широко используется многими технологическими и инженерными фирмами для обозначения арматуры - и собственно отсечного клапана **(XV),** и электрозадвижки **(XV).**

Совпадения такого рода наглядность и естественность системы кодирования, мягко говоря, не увеличивают. Причем для обозначения концевиков

- И отсекателя,
- И задвижки,
- И в ПАЗ,
- И в РСУ

используются также одинаковые обозначения, но уже с совершенно другим ведущим символом:

- ZSO/ZSC,
- ZLO / ZLC, что уж совсем ни куда не годится.

Символ Y.

Редкие случаи использования символа Y в первой позиции обнаруживаются у самых авторитетных фирм для не очень понятных кодов типа YI и YL , которые для их авторов символизируют "Состояние насоса". В исходных таблицах 10.1 и 10.2 стандарта ISA символу Y приписаны следующие значения:

- *Event; State; Presence, что можно перевести как*
- *Событие; Состояние; Присутствие /Наличие.*

И сам облик символа Y, и его значение, и пребывание в одной декартовой триаде с символами X и Z может быть аргументом в его пользу. В очередной раз обращаясь к авторитетам, заметим, что стандарт ISA для кодировки

- Соленоида отсечного клапана рекомендует обозначение YY,
- Собственно отсечного клапана - YV,
- А для кода управления отсекателем - YC или YIC.

Концевики же и их состояния обозначены как ZSH и ZSL, что в совокупности с предыдущими кодами как-то не очень логично.

Эти коды полностью соответствуют логике стандарта ISA для обозначения пограничных состояний _SL, _SH, однако использование нового первого символа Z для обозначения единой логической цепочки выпадает из общего строя стандарта.

Приведем для сравнения:

(TE - TT) - TIC - (TУ - TV)

Может быть, по этой причине этаким набором обозначений никто и не пользуется. Но, не пользуясь **именно таким** набором обозначений, фирмы используют:

- Или другие, не менее разнородные коды,
- Или же коды, совпадающие с кодами задвижки, (см. еще раз таблицы 10.13 и 10.14).

Это именно тот случай, из-за которого мы настаиваем на применении уникального символа устройства:

- Как для обозначения самого устройства и его компонентов,
- Так и для кодировки параметров состояния,
- Так и для кодировки параметров управления устройством.

Вариантность использования символов X или Y для идентификации параметров отсекателя можно сохранить, однако приоритет символа Y для обозначения электропневмопреобразователей, электропневмопозиционеров, соленоидов, реле, вычислительных блоков заставляет отдать предпочтение символу X. Кроме того, заслуживает внимания вариант использования Y для идентификации параметров двигателя, с частности, насоса, представленный в таблице 10.11.

Поэтому если не отвлекаться на совсем экзотические варианты, то X-вариант отсекателя - вне конкуренции. Мы приходим к совершенно прозрачной композиции, в которой сочетание

X - для отсекателя

Z - для задвижки

представляется оптимальным.

При этом автоматически устанавливается, что лучшее применение символа S - ЗАПОРНО-РЕГУЛИРУЮЩИЕ КЛАПАНЫ. Таким образом, наша шкала перехода от непрерывности к останову теперь выглядит следующим образом:

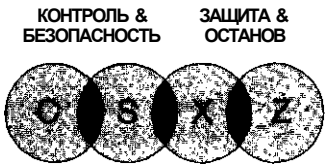


Рис. 10.9

Где символы являются носителями следующих понятий:

C - Контроль, управление
S - Безопасность
X - Защита
Z - Останов.

Тогда конкретные устройства, олицетворяющие эти понятия, определятся следующим образом:

C - Регулирующий клапан
S - Запорно-регулирующий клапан
X - Отсекатель
Z - Электрозадвижка.

Таково наше решение для главного пробела стандарта ISA отсутствие однозначной идентификации запорно-регулирующих устройств. Далее это решение станет основой для формирования кодов состояния и управления исполнительных устройств.

Возможности расширения предлагаемого подхода. Как сказано, для органичного включения кодов состояния и управления оборудования в общую систему идентификации технологических переменных предлагается следующая идея:

Обобщение группы параметров устройства или комплектного оборудования под единым символом устройства, достаточно близким к нему по смыслу и, по возможности, общепринятым.

Единообразная и естественная кодировка параметров состояния и управления устройствами может существенно облегчить процесс разработки и отладки систем управления и защиты, а также будет способствовать повышению наглядности и "понятности" кодов, если это понятие вообще имеет какой-либо смысл.

Естественным образом напрашивается дальнейшее расширение этого подхода. Общая идея заключается в том, что к \аковым устройствам могут быть отнесены **все ключевые**

элементы оборудования установки, имеющие непосредственное отношение к безопасности:

- ОТСЕКАТЕЛИ,
- ЭЛЕКТРОЗАДВИЖКИ,
- ЗАПОРНО-РЕГУЛИРУЮЩИЕ КЛАПАНЫ,
- НАСОСЫ,
- ДВИГАТЕЛИ, ЭЛЕКТРОПРИВОДЫ,
- и даже КОМПРЕССОРЫ.

Как можно заметить, в единую группу выделено оборудование, которое имеет четко выраженное свойство:

- Быть включенным или выключенным;
- Открытым или закрытым;
- Работать или не работать.

Сложно представить это свойство для объектов с распределенными параметрами, таких как колонны, теплообменники, или реакторы. Вместе с тем, и для этих, сугубо "аналоговых" объектов, представить дискретное поведение все-таки можно - хотя бы на уровне команд и операций пуска и останова.

10.9. Объединение группы параметров устройства

Переходим к практическим действиям, понимая при этом, что выбор конкретного кода устройства - шаг, который имеет долговременные последствия.

Ведущий символ устройства. Вводится ведущий символ - символ устройства:

Таблица 10.17

A	**ХРОМАТОГРАФ**
B	**ПЕЧЬ**
C	**РЕГУЛИРУЮЩИЙ КЛАПАН**
D	**ЭЛЕКТРОДВИГАТЕЛЬ, ЭЛЕКТРОПРИВОД**
G	**КОМПРЕССОР**
N	**НАСОС**
V	**ВЕНТСИСТЕМА, ВОЗДУХОДУВКА**

S	ЗАПОРНО-РЕГУЛИРУЮЩИЙ КЛАПАН
X	ОТСЕКАТЕЛЬ
Z	ЭЛЕКТРОЗАДВИЖКА

Дополнительный символ устройства - символ расширения. Ведущий символ оборудования должен быть дополнен уточняющим символом, чтобы устройство однозначно идентифицировалось как таковое при любых обстоятельствах. Это позволит избежать двусмысленности и пересечений с кодами технологических переменных. Полные коды устройств:

Таблица 10.18

AX	ХРОМАТОГРАФ
BA	ПЕЧЬ
CV	РЕГУЛИРУЮЩИЙ КЛАПАН
DV/MV	ЭЛЕКТРОДВИГАТЕЛЬ, ЭЛЕКТРОПРИВОД
HV	ИСПОЛНИТЕЛЬНЫЙ МЕХАНИЗМ С РУЧНЫМ УПРАВЛЕНИЕМ
GB/GT	КОМПРЕССОР, ТУРБОДЕТАНДЕР; ТУРБИНА
NV/GA	НАСОС
W i . . .	ВЕНТСИСТЕМА, ВОЗДУХОДУВКА
SV	ЗАПОРНО-РЕГУЛИРУЮЩИЙ КЛАПАН
XV	ОТСЕКАТЕЛЬ
zv l	ЭЛЕКТРОЗАДВИЖКА

Привлечение уточняющего символа открывает дополнительные степени свободы в кодировке устройств: MV, GA и т.д.

Таким образом, решена первая часть проблемы идентификации оборудования: устройствам присвоены уникальные имена.

10Л0. Постановка общей задачи идентификации

Стандартная информационная функция технологической переменной

PT=P(Переменная)+T(Трансмиттер)

строится в последовательности

Измеряемая характеристика - Устройство.

Для регулирующих, запорно-регулирующих клапанов, и для абсолютного большинства отсекателей первостепенной также является **ФУНКЦИЯ,** определяемая контролируемой технологической переменной. И понятием, объединяющим эти характеристики воедино, является понятие **КОНТУРА.**

Для части насосов и подавляющего большинства электрозадвижек, не связанных в реальном времени с защитой процесса, первостепенным является собственно само **УСТРОЙСТВО.** И для подобных элементов оборудования ведущим кодом является код устройства. Таким образом, информационная функция состояния насоса строится в обратной последовательности:

Устройство - Характеристика состояния.

Для параметров управления подобными самостоятельными устройствами код также выстраивается по принципу

Устройство - Характеристика управления.

Таким образом, существуют две устойчивые группы понятий, по которым происходит объединение состояний и действий систем управления и защиты, и которые, вообще говоря, должны иметь самостоятельные способы идентификации:

1. Взаимосвязанные группы параметров состояния и управления для конкретной функции системы, а именно КОНТУРА:
   - **Измерительного** ("информационного") контура;
   - Контура **управления;**
   - Контура **защиты.**
2. Взаимосвязанные группы параметров состояния и управления для устройства.

Как уже можно было убедиться, стандарт ISA S5.1-1984 дает вполне определенный метод идентификации параметров контура: все компоненты контура привязываются к входной технологической переменной. Этот метод идеально соответствует ординарной функции непрерывного регулирования - от датчика до клапана. Соответственно, и в целом метод хорош для непрерывного технологического процесса без событий.

Тонкое расщепление. Проблема возникает при описании дискретных функций - функций защиты, и вообще любой программно-логической последовательности действий. Суть проблемы заключается в том, что место контура регулирования теперь с необходимостью занимает контур дискретной операции или контур защиты. Здесь тут же выясняется, что на установке существует масса самого разнообразного оборудования, которое в информационном смысле никак не ассоциируется с контуром безопасности. Единственное средство, которые предоставляет стандарт ISA, это две абстрактных переменных:

Y - *State, Event; Presence* - Состояние, Событие; Присутствие.
Z - *Position, Dimension* - Положение, Размер.

Эти две переменных можно привязать к чему угодно, но нас гораздо больше устроило бы, если бы эти абстрактные "состояния" и "положения" описывали конкретные состояния и положения кого-то или чего-то. Тем более что для определения состояний и положений у нас уже есть вполне конкретный способ - буква **S,** во второй балетной позиции. И определять самостоятельные понятия состояния и положения через первый символ кода нет никакой необходимости.

В то же время не то что бы однозначные, но и вообще какие бы то ни было определения для параметров состояния и управления **конкретных устройств,** определяющих безопасность процесса, в стандарте отсутствуют. Их и не может там оыть, поскольку в отличие от понятий трансмиттера, реле, соленоида все исполнительные устройства определены одним общим термином - *Final Element.*

Очевидно, что этот *Final* элемент нуждается в более тонком расщеплении:

1. Нужно дать точные коды для каждого типа исполнительных устройств, участвующих в обеспечении безопасности процесса.

2. Следующее, что легко сказать, но непросто сделать - найти такие правила кодировки параметров устройств, чтобы коды этих параметров однозначно ассоциировались именно с этим устройством. Сложность заключается в том, что в отличие от ординарного датчика, запорно-регулирующие устройства имеют не один, а несколько параметров.

   В свою очередь, параметры устройства подразделяются на параметры управления и параметры состояния устройства. Более того, оперативная работа с устройством обусловлена целым набором дополнительных функций, которые должны быть соответствующим образом обеспечены:

   - Переключение с местного на дистанционное управление *(Local / Remote);*
   - Возврат в исходное состояние *(Reset);*
   - Деблокирующие ключи и т.д.

   Суть состоит в том, что исполнительные устройства, предназначенные непосредственно для управления и защиты процесса, сами нуждаются в управлении и защите, и в известном смысле представляют собой мини-ячейку АСУТП.

3. И главный вопрос. В контексте данной работы речь идет о тех исполнительных устройствах, которые входят в состав контура безопасности. Определенно, что в том случае, если устройство находится в единой логической цепи - в составе контура, принадлежность к конкретному контуру однозначно идентифицируется по контролируемой технологической переменной. Можно ли предложить более-менее рациональный способ включения кодов устройства в систему кодов контура, не превращая при этом код в бессмысленный набор символов?

Сложно согласовать эти противоречивые требования в одном комплексном показателе. По всей видимости, ключ к решению проблемы идентификации контуров защиты находится в разумном сочетании способов формирования кодов. Возможное решение этой задачи для устройств, находящихся в единой логической цепи - цепи контура - измерительного, управляющего, контура безопасности - представлено далее.

Что касается устройств в чистом виде, то возможны следующие варианты кодировки.

Вторая позиция кода. Предположим, для каждого типа устройства определен уникальный символ устройства. Относительно последующих символов, позволяющих однозначно идентифицировать вначале тип переменной - вход или выход, а затем

- Для каждого входа - конкретную характеристику состояния устройства,
- А для каждого выхода - тип команды управления,

можно высказать следующие предварительные соображения.

Стандарт ANSI / ISA S5.1-1984 определяет в качестве признака дискретного входа символ **S** во второй позиции. Для команд дискретного выхода - соленоидов и выходных реле - используется признак **Y.** При этом стандарт рекомендует использовать символ **Y во второй позиции** для обозначения устройств, которые:

- Соединяют *(connects),*
- Разъединяют *(disconnects),*
- Передают / переключают *(transfers)* одну, или несколько цепей управления,

и могут представлять из себя:

- ПЕРЕКЛЮЧАТЕЛЬ *(SWITCH);*
- РЕЛЕ *(RELAY);*
- ДВУХПОЗИЦИОННЫЙ РЕГУЛЯТОР *(ON-OFF CONTROLLER);*
- ЭЛЕКТРОПНЕВМОПРЕОБРАЗОВАТЕЛЬ *(UP CONVERTER);*
- СОБСТВЕННО РЕГУЛИРУЮЩИЙ КЛАПАН *(CONTROL VALVE).*

Дополнительная особенность символа **Y** во второй позиции состоит в том, что кроме перечисленных **физических** устройств, он используется и для идентификации **вычислительных** ("программных") блоков. Традиционно этот символ используется и для обозначения преобразователей общего вида. Таким образом, первая пара вторых символов кода устройс гва - пара **X -Y.** Если же вспомнить классическое определение функциональной зависимости **y = *f(x),*** то вариант **X - Y** становится еще более привлекательным.

Историческая справка

Функция (лат. functio - исполнение, осуществление) - одно из основополагающих понятий математики, выражающее зависимость одних переменных величин от других. Слово "Величина" в данном определении понимается в самом широком смысле - как элемент любого множества. Хотя современное определение функции, свободное от упоминания об аналитическом задании, приписывается Петеру Дирихле (1837), к осознанию этого понятия причастны лучшие умы человечества. В геометрическом и механическом виде отчетливое понимание функции присутствует в работах Исаака Ньютона (1687). Впервые термин "Функция" появился в 1692 году у Готфрида Лейбница. Первые определения Функции принадлежат сотруднику Лейбница Иоганну Бернулли (1718), великому Леонарду Эйлеру (1748), и Жану Батисту Фурье (1822). Одно из определений функции дал Николай Иванович Лобачевский, которое приоткрывает способ мышления этого необыкновенного человека (1826):

"Обширный взгляд теории допускает существование функциональной зависимости только в том смысле, что числа одни с другими в связи следует понимать как бы данными вместе".

Вместе с тем, часто выходные преобразователи запорно-регулирующей арматуры для упрощения помечают по типу устройства - символом V. Поэтому один из рабочих вариантов - пара признаков входа-выхода S - V.

Таким образом, существуют следующие сочетания вторых символов для кодировки рассматриваемых устройств:

dX dY
dX dV
dS dY
dS dV

Несмотря на возможную непривычность некоторых сочетаний, все четыре варианта заслуживают внимания.

Вариант dS-dV используется довольно часто, однако строго соответствует стандарту ISA и общемировой практике только вариант dS-dY. Его и возьмем за основу при формировании кодов состояния и управления запорно-регулирующей арматуры. Но вариант dX-dY также нельзя оставлять без внимания. И этот вариант должен быть сохранен в памяти.

За символом V во второй позиции сохраняется смысл собственно самого физического устройства - клапана. Вместе с тем в оправданных случаях, не вызывающих недоразумений, необходимо оставить за собой право использовать символ V во второй позиции. Примерами могут быть обозначения некоторых служебных кодов типа Деблокирующих ключей, или переключателей Дистанционного / Местного управления устройствами.

10.11. Идентификация параметров состояния и управления устройства

Подобно тому, как ведущий символ технологической переменной модифицируется дополнительным символом (в общем случае - до трех символов, например PSHH = P • S • HH) типа измеряемой величины или типа выходного сигнала, точно так же ведущий символ оборудования должен быть дополнен уточняющим символом (в общем случае - несколькими символами), чтобы **тип входного и выходного сигнала** устройства однозначно идентифицировался при любых обстоятельствах. Исходя из этих предпосылок, вводятся следующие определения.

Определение 1: Код устройства.

Код устройства будет состоять из двух символов:

Код устройства = Ведущий символ устройства * Дополнительный символ.

На примере задвижки:

ZV = Z V

Определение 2: Код состояния устройства.

Код состояния устройства будет формироваться следующей суперпозицией

Код состояния устройства = Ведущий символ устройства * Идентификатор состояния устройства.

Пример

Состояние задвижки - ОТКРЫТА. Стандартный код дискретного входа формирует конъюнкция символа переменной и модификатора - признака дискретного сигнала:

ZS - Z S

Замечание

Согласно ГОСТ 21.404-85, пункт 2.11, "Букву S применяют для обозначения контактного устройства прибора, используемого только для включения, отключения, переключения, блокировки.

При применении контактного устройства прибора, для включения, отключения и одновременно для сигнализации в обозначении прибора используют обе буквы: Su A".

Мало того, что ГОСТ определяет символ S *как символ выходного устройства, так еще и устанавливает одновременное употребление его с символом А.. Единственное, что говорит по этому поводу исходный стандарт ISA, так это уже упоминавшееся замечание к таблице 10.2 о том, что символы S и А могут использоваться* ***равным*** *образом, но никак не одновременно.*

Для устройств с числом возможных состояний не более двух, одного признака состояния вполне достаточно. Однако состояния запорно-регулирующей арматуры представляют особый случай: состояние данного типа оборудования определяется по концевым выключателям. Поэтому нужен еще один символ, определяющий, к какому именно концевику относится данный вход. Тогда на примере концевого выключателя на открытие задвижки код состояния "Задвижка открыта" может быть выражен как

ZSO = Z S O

Строгое следование стандарту ISA привело бы к другому, насколько универсальному, настолько же и индифферентному коду:

ZSH = Z S н

Использование в качестве уникального признака состояния символа О вместо Н позволяет однозначно идентифицировать входную переменную именно как состояние концевика на открытие клапана.

Дополнительно ассоциация подкрепляется уникальным первым символом устройства - в данном случае задвижки Z.

Таким образом, в общем случае идентификатор состояния устройства определяется как

Идентификатор состояния устройства = Признак входа * Признак состояния устройства.

При этом общее стремление состоит в том, чтобы идентификатор состояния устройства состоял не более чем из двух символов.

Определение 3: Код управления устройством.

В свою очередь, код управления устройством формируется суперпозицией ведущего символа устройства и идентификатора управляющего воздействия:

Код управления устройством = Ведущий символ устройства * Идентификатор управляющего воздействия.

Идентификатор управляющего воздействия устройства определяется по аналогии с идентификатором состояния устройства:

Идентификатор управляющего воздействия = Признак выхода * Признак команды управления устройством.

При этом общее стремление состоит в том, чтобы идентификатор управляющего воздействия устройства состоял не более чем из двух символов.

На примере Задвижки:

ZYO = Z Y • O

Естественно, что реформаторский ГОСТ 21.404 и здесь не мог остаться в стороне. В Приложении 1, таблица 1, в качестве дополнительного буквенного обозначения указано:

Y - для построения обозначений преобразователей сигналов и вычислительных устройств.

В не имеющей номера таблице справочного Приложения 2 приводятся следующие примеры использования символа **Y:**

47. *TY - Преобразователь сигнала, установленный на щите. Входной сигнал электрический, выходной сигнал тоже электрический. Например: преобразователь измерительный, служащий для преобразования т.э.д.с. термометра термоэлектрического в сигнал постоянного тока.*
48. *PY - Преобразователь сигнала, установленный по месту. Входной сигнал пневматический, выходной - электрический.*
49. *FY - Вычислительное устройство, выполняющее функцию умножения. Например: множитель на постоянный коэффициент К.*

О преимущественном использовании Y в качестве признака **выходного** преобразователя и реле в соответствии с исходным стандартом ISA S.5.1-1984 даже не упоминается.

По представленным в наших определениях схемам формируются коды состояний и управлений для всех типов запорно-регулирующей арматуры. Для идентификации параметров состояния запорно-регулирующих устройств вводятся следующие коды:

1. Вводится код для идентификации состояний Запорно-регулирующего клапана: SS_: SSC SSO
2. Вводится код для идентификации состояний Отсекателя: XS_: XSC XSO
3. Вводится код для идентификации состояний Задвижки: ZS_: ZSC ZSO

Полученные результаты сведены в табличную форму вместе с соответствующими кодами управляющих воздействий (таблица 10.19).

Таблица 10.19

ЗРК		Отсекатель		Задвижка	
Открыт	SSO	Открыт	XSO	Открыта	ZSO
Закрыт	SSC	Закрыт	XSC	Закрыта	ZSC
Открыть	SYO	Открыть	XYO	Открыть	ZYO
Закрыть	SYC	Закрыть	XYC	Закрыть	ZYC

По аналогии с созданными кодами арматуры вводится код для идентификации параметров состояния и управления Насосом. В соответствии с только что установленными правилами код насоса принимает следующую форму:

NS = N • S

Замечание

Код NS присутствует и в нашем ГОСТе 21.404-85, таблица Приложения 2, *пункт 50. Однако он использован не для*

обозначения ***состояния****, а для обозначения некой "Пусковой аппаратуры для управления электродвигателем (включение / выключение насоса; открытие / закрытие задвижки и т.д.), к тому же установленной по месту. Например: магнитный пускатель, контактор и т.п.*

Подобное применение данного кода - чистой воды самодеятельность создателей ГОСТа. В **стандарте ISA ненормативной лексики нет, и быть не может.**

Сводя полученные результаты воедино, коды состояний и управлений для рассматриваемого оборудования можно представить в виде нижеследующей таблицы 10.20.

Таблица 10.20

Код	Входы	Выходы	Устройство
DV	DSR DSS	DYR DYS	ЭЛЕКТРОДВИГАТЕЛЬ, ЭЛЕКТРОПРИВОД
NV	NSR NSS	NYR NYS	НАСОС
W	VSR VSS	VYR VYS	ВЕНТСИСТЕМА, ВОЗДУХОДУВКА
SV	SSO SSC	SYO SYC	ЗАПОРНО-РЕГУЛИРУЮЩИЙ КЛАПАН
XV	XSO XSC	XYO XYC	ОТСЕКАТЕЛЬ
ZV	ZSO ZSC	ZYO ZYC	ЭЛЕКТРОЗАДВИЖКА

Значение последних символов кода понятно без особых объяснений:

R - Run
S - Stop
O - Open
C - Close.

Интересно посмотреть на ту же самую таблицу, если и для устройств применить принцип формирования граничных кодов по стандарту ISA:

Таблица 10.21

Код	Входы	Выходы	Устройство
DV	DSH DSL	DYH DYL	ЭЛЕКТРОДВИГАТЕЛЬ, ЭЛЕКТРОПРИВОД
NV	NSH NSL	NYH NYL	НАСОС
W	VSH VSL	VYH VYL	ВЕНТСИСТЕМА, ВОЗДУХОДУВКА
SV	SSH SSL	SYH SYL	ЗАПОРНО-РЕГУЛИРУЮЩИЙ КЛАПАН
XV	XSH XSL	XYH XYL	ОТСЕКАТЕЛЬ
ZV	ZSH ZSL	ZYH ZYL	ЭЛЕКТРОЗАДВИЖКА

Если учесть, что все устройства будут однозначно идентифицироваться по первому символу, то в принципе это тоже мог бы быть вполне рабочий вариант.

Но нельзя забывать, что даже если какая-нибудь неприятность ни под каким видом не может случиться, она обязательно случается, и наверняка возникнет ситуация, когда придется разбираться с реле превышения скорости вращения SSH, высоким уровнем вибрации VSH, и т.д.

Продолжим. Если учесть, что для ряда устройств при определении входных и выходных параметров достаточно одного дискретного сигнала, таблицу 10.20 можно упростить (см. таблицу 10.22).

Таблица 10.22

Код	Входы	Выходы	Устройство
DV	DSS	DYS	ЭЛЕКТРОДВИГАТЕЛЬ, ЭЛЕКТРОПРИВОД
NV	NSS	NYS	НАСОС
W	VSS	VYS	ВЕНТСИСТЕМА, ВОЗДУХОДУВКА
SV	SSO SSC	SYS	ЗАПОРНО-РЕГУЛИРУЮЩИЙ КЛАПАН
XV	XSO XSC	XYS	ОТСЕКАТЕЛЬ
ZV	ZSO ZSC ZSF	ZYO ZYC ZYS	ЭЛЕКТРОЗАДВИЖКА

Примечание

Добавлены коды, которые необходимы для некоторых задвижек:

ZSF — *диагностика превышения крутящего момента (задвижка заклинена);*

ZYS - *команда СТОП.*

Если требуется ввести параметры состояния и управления компрессором, это так же может быть сделано в той же структуре кодов:

Таблица 10.23

GB	GSS	GYS	КОМПРЕССОР

Естественно, предполагается, что компрессор имеет собственную автономную систему контроля и защиты.

И последнее. Стандарт ISA S5.1-1984 предлагает всего лишь один способ ручного воздействия на состояние оборудования - ключ HS. Ничто не мешает сделать расщепление команд управления, и ввести специальные коды и для команд управ-

ления оборудованием, и для оповещения о состояниях периферийного оборудования:

Таблица 10.24

DB	КЛЮЧ ОБХОДА БЛОКИРОВКИ (ДЕБЛОКИРУЮЩИЙ КЛЮЧ)
PB	КНОПКА "АВАРИЙНЫЙ ОСТАНОВ", "РАЗРЕШЕНИЕ НА ПУСК" и т.д.
RS	КНОПКА "СБРОС / ВОЗВРАТ В ИСХОДНОЕ СОСТОЯНИЕ"
SW	ПЕРЕКЛЮЧАТЕЛЬ "ДИСТАНЦИОННОЕ / МЕСТНОЕ УПРАВЛЕНИЕ"
AN	ВЫДАЧА СИГНАЛИЗАЦИИ НА СВЕТОВОЕ ТАБЛО

Привязка кнопок и ключей к конкретному оборудованию осуществляется добавлением ведущего символа устройства.

Дополнительные коды могут быть введены и для отслеживания состояния, например, источников электропитания (UPS):

Таблица 10.25

UPS	ИСТОЧНИК БЕСПЕРЕБОЙНОГО ПИТАНИЯ (UPS)

Алгоритмы формирования кодов состояния и управления запорно-регулирующей арматуры для РСУ и ПАЗ на базе признаков входа-выхода S-Y приведены далее на рис. 10.10. Соответствующие алгоритмы для насосов, электроприводов и вентсистем представлены на рис. 10.11.

В таблице 10.26 представлена табличная форма кодов для параметров состояния, управления и служебных ключей запорно-регулирующей арматуры и насосов, которая воспроизводит логику рис. 10.10- 10.11.

Если учесть, что для ряда устройств достаточно одного дискретного сигнала состояния и одного сигнала управления, структуру кодов можно упростить (см. рис. 10.12 и 10.13).

И тогда обе схемы можно просто объединить в одну (рис. 10.14). Единственная аномалия - это коды управления задвижкой, для которой по-прежнему требуется два выходных сигнала - Открыть / Закрыть.

Таблица 10.26

Таблица кодов для параметров состояния, управления и служебных ключей запорно-регулирукощей арматуры и насосов

Запорно-регулирующая арматура	швопустройства											Ид устройства
	0	1	2	3	4	5	6	7	8	9	10	11
РСУ:												
Насос	N	NLS		NLF	NVL	NVB	NHR	NKS	NVX	NVA	NY	NV
Запорно - регулирующий клапан	S	SLO	SLC	SLF	SVL	SVB	SH0	SHC	SVX	SVA	SY1	SV
Отсечной клапан	X	XLO	XLC	XLF	XVL	XVB	XHO	XHC	XVX	XVA	XY	XV
Электрозодоима	Z	ZLO	ZLC	ZLF	ZVL	ZVB	ZH0	ZHC	ZVX	ZVA	ZYO ZYC	ZV
ПАЗ'												
Насос	N	NSS		NSF	NVM	NVD	NYR	NYS	NVX	MVS	NY	NV
Запорно - регулирующий клапан	S	SSO	SSC	SSF	SVM	SVD	SYO	SYC	SVX	SVS	SY	SV
Отсечной клапан	X	XSO	XSC	XSF	XV»	XVD	XY0	XYC	XVX	XVS	XY	XV
Электрозодвижка	Z	ZSO	ZSC	ZSF	ZVM	ZVD	ZY0	ZYC	ZVX	ZVS	ZYO ZYC	ZV

Способы формирования кодов для дополнительных служебных ключей желательно также подчинить общей архитектуре кодов. Один из возможных вариантов приведен на рис. 10.15.

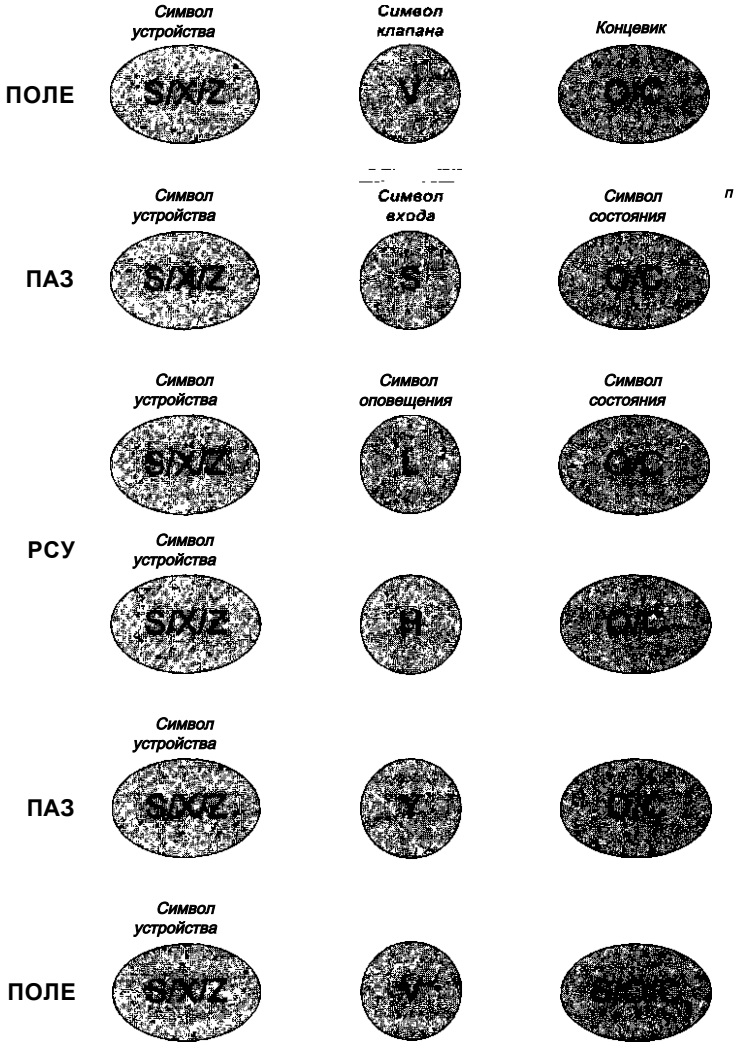

Символ устройства
Символ клапана
Концевик
ПОЛЕ
S/X/Z
V
OAC
Символ устройства
Символ входа
Символ состояния
ПАЗ
S/X/Z
S
OAC
Символ устройства
Символ оповещения
Символ состояния
S/X/Z
L
OAC
РСУ
Символ устройства
S/X/Z
H
OAC
Символ устройства
ПАЗ
S/X/Z
Y
OAC
Символ устройства
ПОЛЕ
S/X/Z
V
OAC

Рис. 10.10

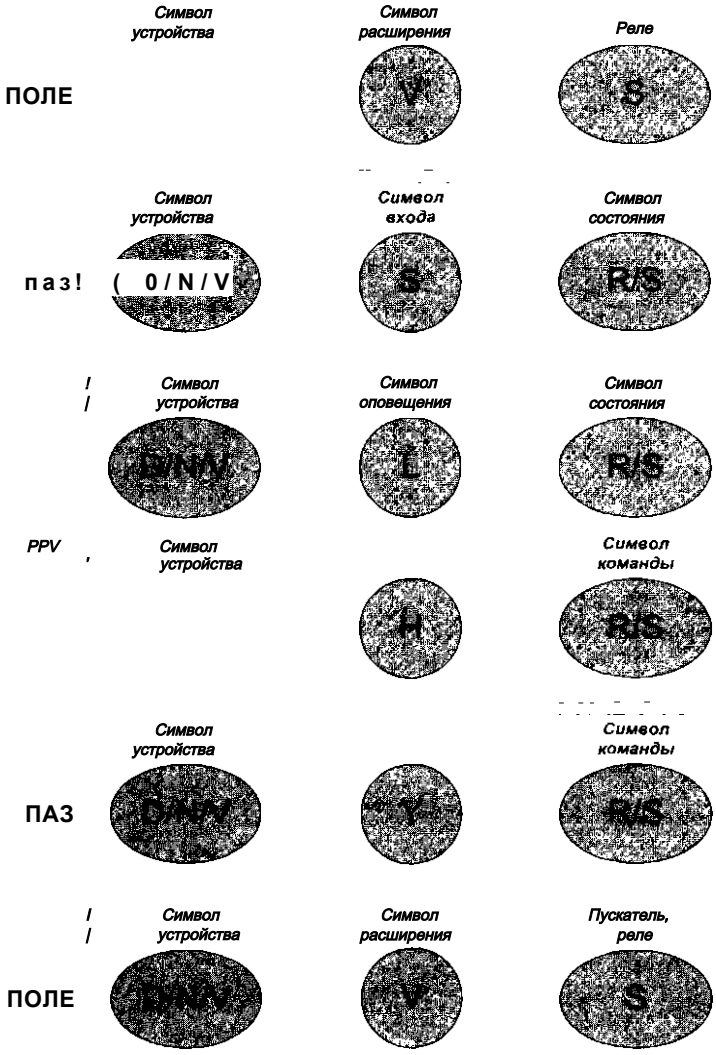

Символ устройства
Символ расширения
Реле
ПОЛЕ
V
S
Символ устройства
Символ входа
Символ состояния
паз!
(0 / N / V
S
R/S
Символ устройства
Символ оповещения
Символ состояния
D/N/V
L
R/S
PPV
Символ устройства
Символ команды
H
R/S
Символ устройства
Символ команды
ПАЗ
D/N/V
V
R/S
Символ устройства
Символ расширения
Пускатель, реле
ПОЛЕ
D/N/V
V
S

Рис. 10.13

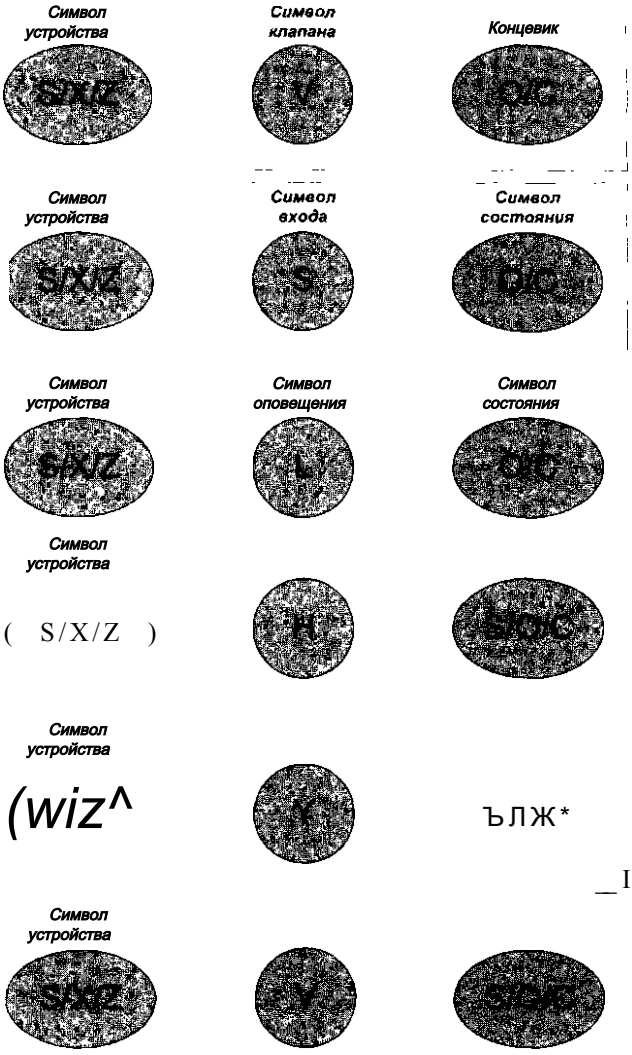

Символ устройства
Символ клапана
Концевик
Символ устройства
Символ входа
Символ состояния
Символ устройства
Символ оповещения
Символ состояния
Символ устройства
(S/X/Z)
Символ устройства
Символ устройства

Рис. 10.10

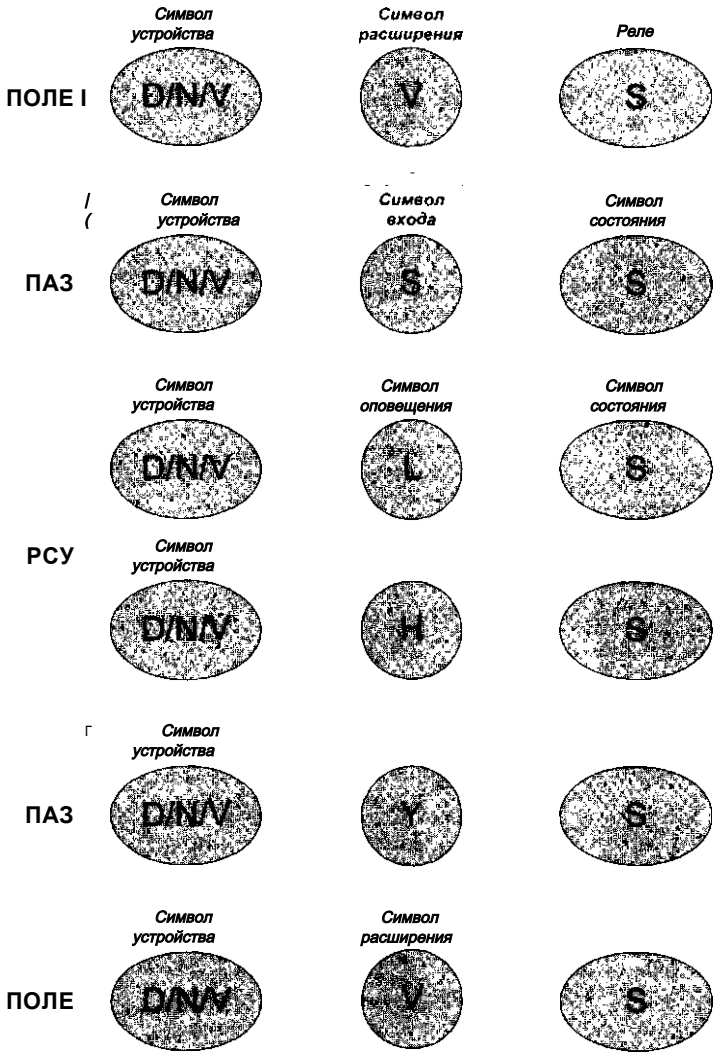

Символ устройства
Символ расширения
Реле
ПОЛЕ I
D/N/V
V
S
Символ устройства
Символ входа
Символ состояния
ПАЗ
D/N/V
S
S
Символ устройства
Символ оповещения
Символ состояния
D/N/V
L
S
РСУ
Символ устройства
D/N/V
H
S
Символ устройства
ПАЗ
D/N/V
Y
S
Символ устройства
Символ расширения
ПОЛЕ
D/N/V
V
S

Рис. 10.13

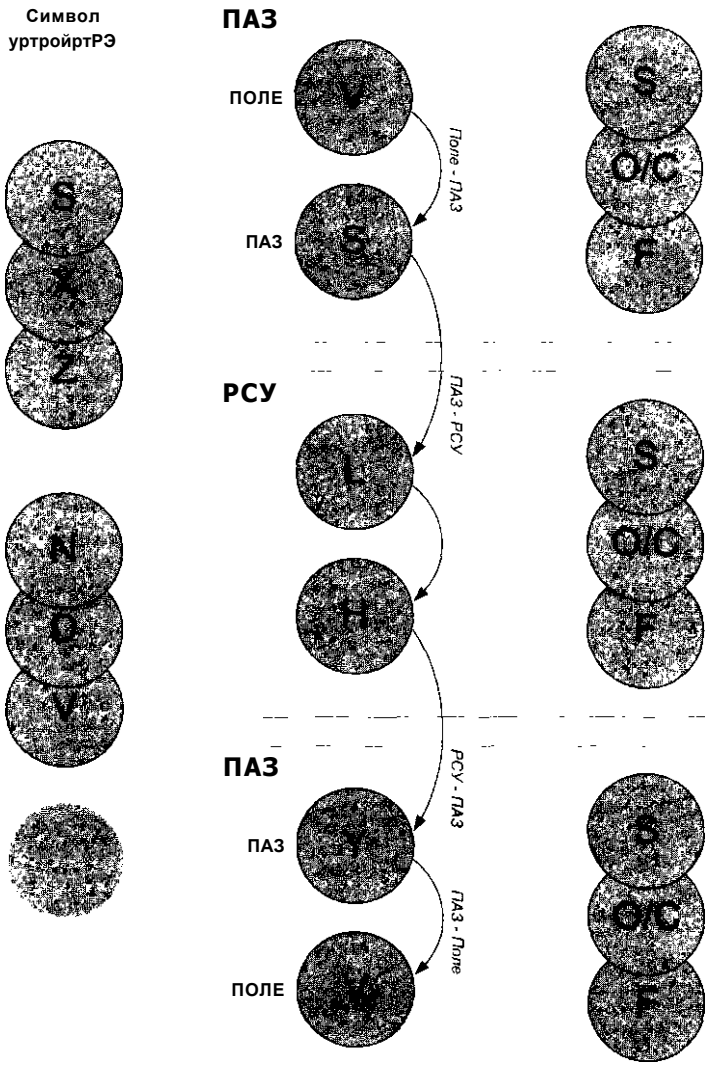

Символ
уртройртРЭ
ПАЗ
ПОЛЕ
V
Поле - ПАЗ
ПАЗ
S
S
O/C
F
ПАЗ - РСУ
РСУ
L
H
S
O/C
F
PCУ - ПАЗ
ПАЗ
ПАЗ
V
ПАЗ - Поле
ПОЛЕ
V
S
O/C
F
S
X
Z
N
O
V

Рис. 10.10

Служебные ключи и сигнализации

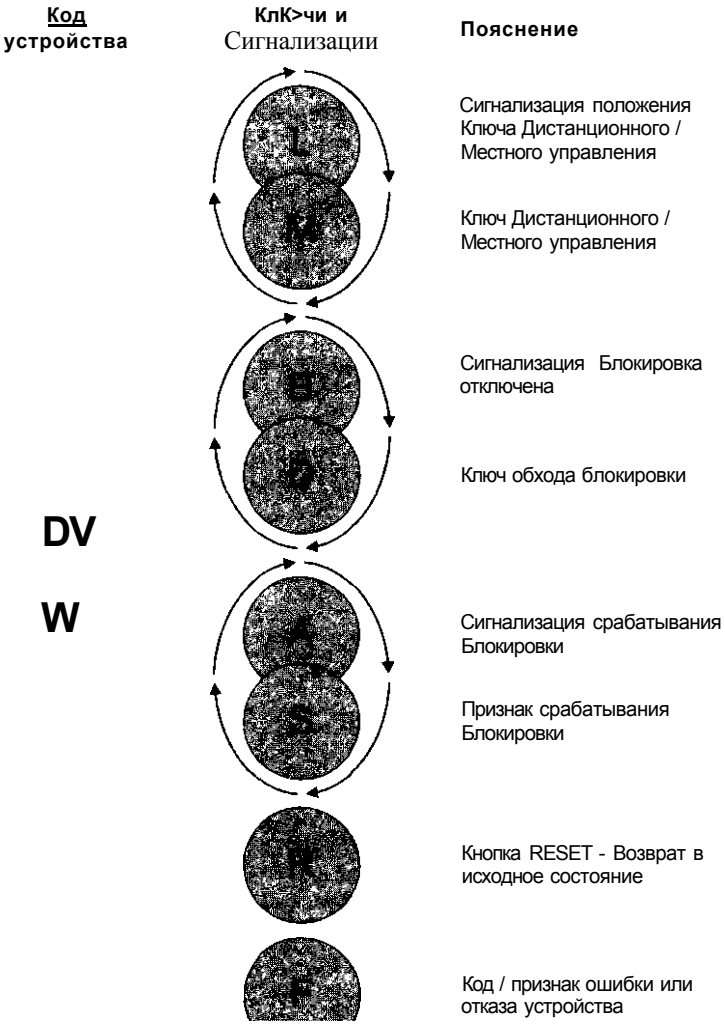


Рис. 10.15

10.12. Промежуточный результат идентификации оборудования без привязки к контурам

Итоговая система кодов для параметров состояния, управления и служебных ключей запорно-регулирующей арматуры и насосов принимает форму таблицы 10.27.

Можно сказать, что из стандарта ISA выжато все, на что он способен. И даже более того.

Для тех устройств, которые не имеют явной привязки к контуру, проблема самоидентификации на этом благополучно заканчивается.

Однако подавляющее большинство из представленного оборудования входит непосредственно в состав контуров управления и защиты. Решением этой проблемы и займемся в следующих разделах.

Примечание

При создании системы кодов очень важно чувствовать ту самую неясную границу между строгостью и свободой выбора. Для примера небольшое отклонение от строгой структуры алгоритмов формирования вспомогательных кодов рисунка 10.15 сделано в кодировке кода "Возврат в исходное состояние" (Reset) - символ возврата к исходному состоянию R заменен на X.

Кроме того, коды неисправности устройства сформированы по шаблонам

_SF и _LF,

хотя шаблон

dvF

рисунка 10.15 также обладает достаточной универсачьностью, ибо позволяет задавать самостоятельные коды ошибок, в том числе и для полевых устройств, например:

FTF = FT F,

PSF **= PS•F,**

что может быть актуальным с применением HART и Fieldbus.

Таблица 10.27

Модифицированная таблица кодов для параметров состояния, управления и служебных ключей запорно-регулирующей арматуры и насосов

Запорно-регулирующая арматура	швопустройства										
	0	1	2	3	4	5	6	7	8	9	10	11
РСУ												
Насос	N	NLS		NLF	NVL	NVB	NHS		NVR	NVA	NY	NV
Запорно - регулирующий клапан	S	SL0	SLC	SLF	SVL	SVB	SHS		SVR	SVA	SY1	SV
Отсечной клапан	X	XLO	XLC	XLF	XVL	XVB	XHS		XVR	XVA	XY	XV
Эпоктро задвижка	*г*	ZLO	ZLC	ZLF	ZVL	ZVB	ZHO	ZHC	ZV R	ZV A	ZYO ZYC	ZV
ПАЗ												
Насос	*Н*	NSS		NSF	NVM	NVD	NYS		NVR	NVS	NY	NV
Запорно регулирующий клапан	S	SSO	SSC	SSF	SVM	SVO	SYS		SVR	**SVS**	SY	SV
Отсечной клапан	X	XSO	XSC	XSF	XVM	XVD	XYS		XVR	**XVS**	XY	XV
Электроодвижка	Z	ZSO	ZSC	ZSF	ZVM	ZVO	ZYO	ZYC	ZVR	**ZVS**	ZYO ZYC	ZV

Примечание

Запорно-регулирующий клапан имеет два средства управления:

1) Электропневмопозиционер;

2) Соленоидный клапан.

Для этих устройств в таблице использованы коды

1) SY1 - электропневмопозиционер ЗРК

2) SY - соленоид ЗРК.

Перебивка сплошного потока символов цифрой заставляет с одного раза запомнить предназначение этого кода. Но если по душе строгий пуризм, можно применить, например, ***SYC*** *и* ***SYS****. Актуальность шаблона* ***dvF*** *согласно рис.* ***10.15*** *для кода неисправности устройства также сохраняется.*

10,13. Идентификация контуров АСУТП

Вторая, еще более важная проблема в рассматриваемом контексте, которая даже не обозначена стандартом ISA - **идентификация контуров программно-логического управления и защиты,** - будет решаться следующим образом:
Для определения принадлежности устройства к конкретной программно - логической цепочке:

- Информационному контуру,
- Контуру защиты,
- Контуру регулирования,

символ устройства будет предваряться символом контролируемой технологической переменной.

Таким образом коды устройств, которые явно входят в состав контура, будут встраиваться в общую структуру кодов на основе тех же шаблонов, которые приняты для кодировки входных и выходных технологических переменных.

Можно утверждать, что это решение целиком находится в архитектуре стандарта ISA, и принадлежит множеству допустимых кодов ISA. Именно так построены коды

- Трансмиттеров **F-T,**
- Электропневмопозиционеров F-Y,
- Регулирующих клапанов F-V.

Мы возвращаемся к началу исследования:

FT = F • T

FY = F Y,

где на месте кода трансмиттера (T) или выходного преобразователя (Y) может находиться не просто любое другое устройство, но код состояния, управления, или служебный код устройства.

Сводя наши рассуждения воедино, алгоритм формирования кода в данном случае состоит из следующих действий:

1. Точное определение типа запорно-регулирующего устройства.
2. Точное определение принадлежности параметра состояния / управления к конкретному устройству.
3. Точная привязка всех параметров устройства и всех компонентов контура к конкретной технологической переменной.

На примере контура регулирования расхода последовательность наших рассуждений выглядит следующим образом.

Исходная модель ISA в чистом виде выражает функциональную зависимость **выходной переменной Y** (выход на >лектропневмопреобразователь или электропневмопозиционер) от **входной переменной** Т (показания Трансмиттера):

1) Y = C (T), где С символизирует функцию регулирования.
   Если произвести развертку контура на составляющие в одну линейку, получим:
2) T - C - Y
   Эта последовательность преобразований должна быть дополнена реальными физическими устройствами, обеспечивающими получение значений входной переменной и собственно выход на клапан:
3) E - (T - C - Y) - V
   Теперь наступает важный момент. Определяется конкретный тип запорно-регулирующего устройства:
4) E - T - C - CY - CV
   В данном случае - это регулирующий клапан - **C.** И, восстанавливая код технологической переменной, получаем:
5) F E - F T - F C - F C Y - F C V ,
   Где FCY - код ЭПП регулирующего клапана FCV.

Таким образом, если существует необходимость точной привязки запорно-регулирующей арматуры к технологической переменной, коды состояний запорно-регулирующего клапана, отсекателя и задвижки должны предваряться символом технологической переменной:

Таблица 10.28

_SS_	_XS_	_ZS_
FSS_	FXS_	FZS_
LSS_	LXS_	LZS_
PSS_	PXS_	PZS_
TSS_	TXS_	TZS_

А сейчас самое интересное: Если принять во внимание, что коды состояний запорно-регулирующего клапана, отсекателя и электрозадвижки по умолчанию являются дискретными, нет никакой необходимости в использовании символа S как признака дискретного сигнала. Получаем уникальную по сочетанию длины и информативности систему кодов (на примере блокировки по температуре):

Таблица 10.29

TSV	**TXV**	**TZV**
TSO	**TXO**	**TZO**
TSC	**TXC**	**TZC**

Как заметил Петр Леонидович Капица, чем фундаментальнее закон, тем меньше символов требуется для его выражения. Ура.

Для сигналов управления привязка к технологической переменной (контуру) с определением типа запорно - регулирующей арматуры приводит к следующей системе кодов:

Таблица 10.30

_CV	**_SV**	**_XV**	**_ZV**
FCY	FSY	FXY	FZY
LCY	LSY	LXY	LZY
PCY	LSY	PXY	PZY
TCY	TSY	TXY	TZY

Можно смело утверждать, что данное решение обладает абсолютной новизной. Причем если нельзя, но очень хочется, то можно пожертвовать строгостью ради наглядности, и использовать вместо признака выхода Y собственно признак устройства V: FCV, FSV, FXV, FZV.

На рис. 10.16-10.27 приводятся диаграммы контуров управления и защиты, и соответствующие этим диаграммам функциональные схемы автоматизации, на которых представлены результаты данного и предыдущих разделов.

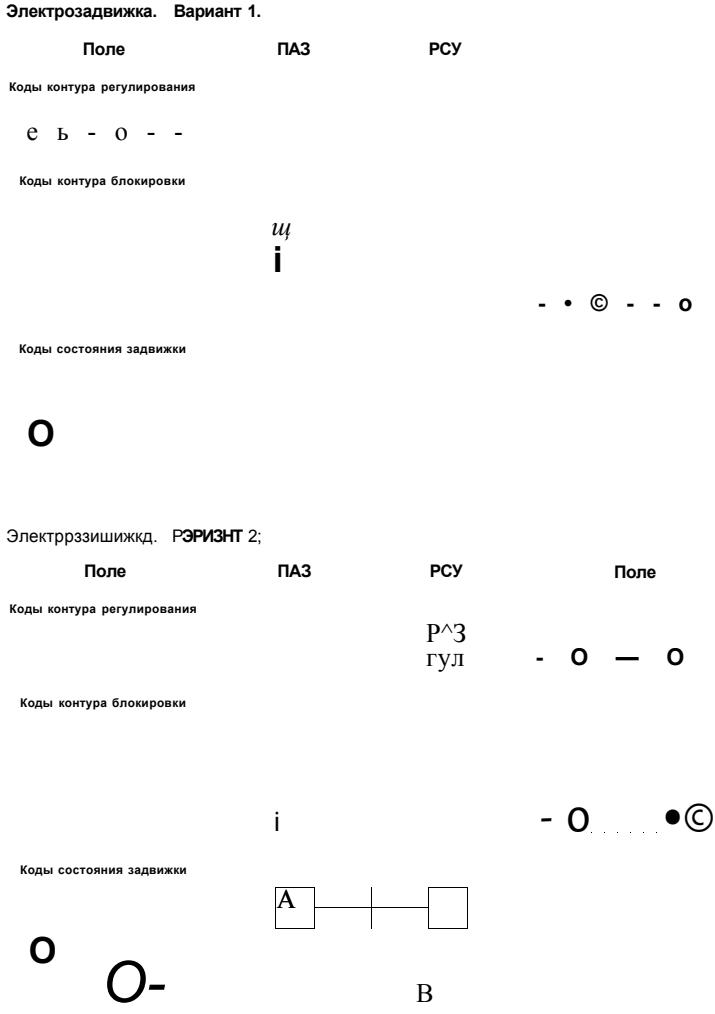
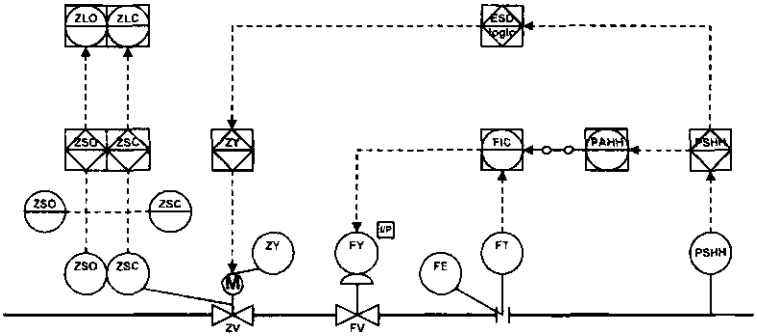

Электрозадвижка. Вариант 1.
Поле
ПАЗ
РСУ
Коды контура регулирования
Коды контура блокировки
Коды состояния задвижки
Электррззишижкд. РЭРИЗНТ 2;
Поле
ПАЗ
РСУ
Поле
Коды контура регулирования
Коды контура блокировки
Коды состояния задвижки
A
B

Рис. 10.16

Электрозадвижка. Вариант 1:



Электоозадвижка. Вариант 2:

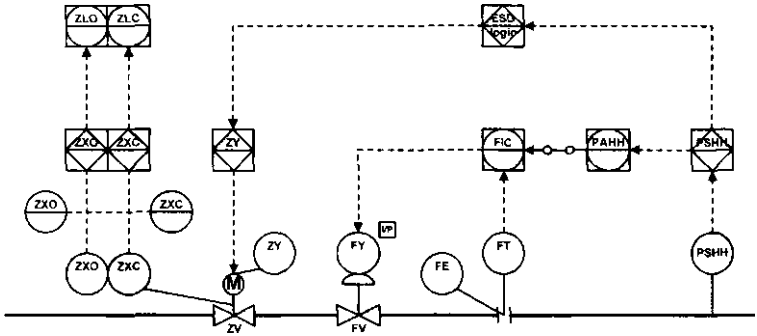
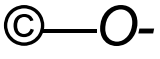


Рис. 10.17

ЭлектР9?9ДРИЖКа, Вариант 3:

Поле **ПАЗ** **РСУ** **Поле**

Коды контура регулирования

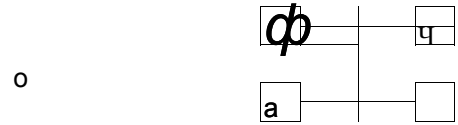


"ЧЭ · "О

Коды контура блокировки

ш

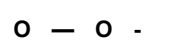
Коды состояния задвижки



Электрозадвижка. Вариант 4:

Лоле **ПАЗ** **РСУ** **Поле**

Коды контура регулирования



к,и

Коды контура блокировки

- О -. . . . .< 5

Коды состояния задвижки-

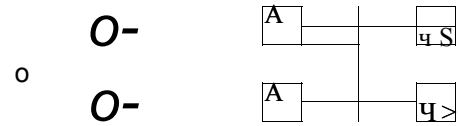
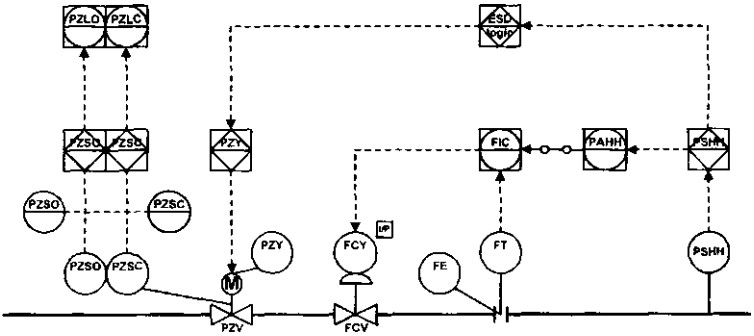


Рис. 10.18

Электрозадвижка. Вариант 3:



Электрозадвижка. Вариант 4:

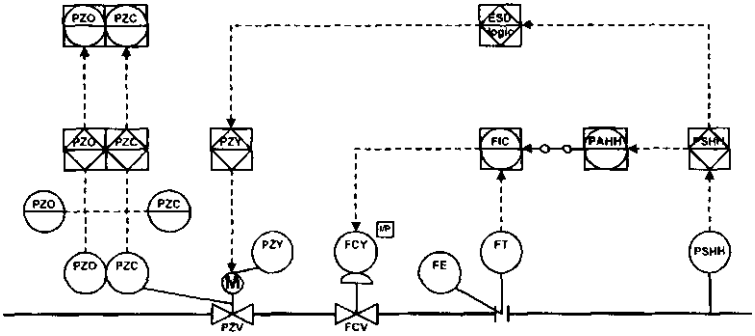


Рис. 10.19

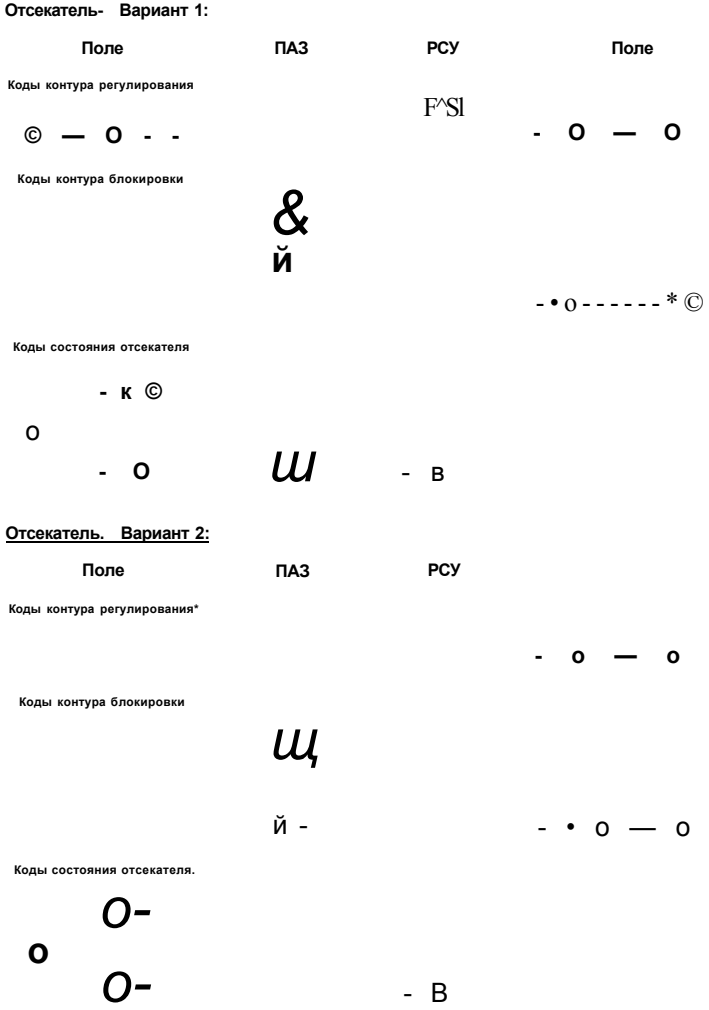
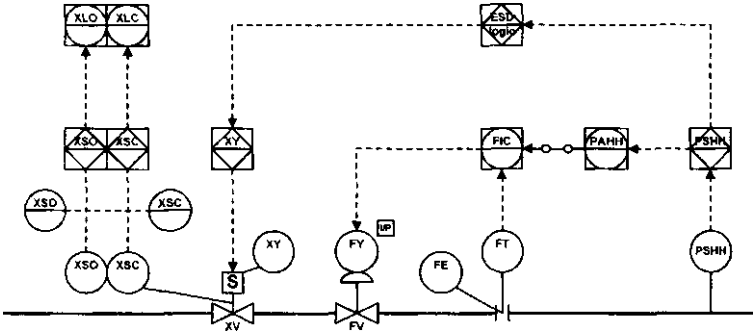

Отсекатель- Вариант 1:
Поле
ПАЗ
РСУ
Поле
Коды контура регулирования
F^Sl
- О — О
Коды контура блокировки
&
й
Коды состояния отсекателя
- к ©
О
- О
ш
- В
Отсекатель. Вариант 2:
Поле
ПАЗ
РСУ
Коды контура регулирования*
- о — о
Коды контура блокировки
щ
й -
- • о — о
Коды состояния отсекателя.
О-
о
О-
- В

Рис. 10.20

Отсзкугель. Вариант 1:



Отсекатель. Вариант 2:

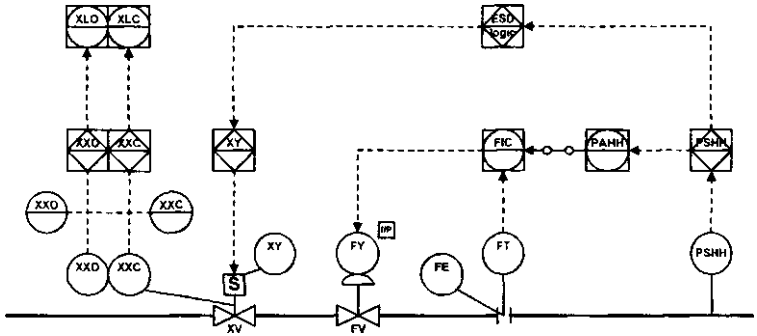
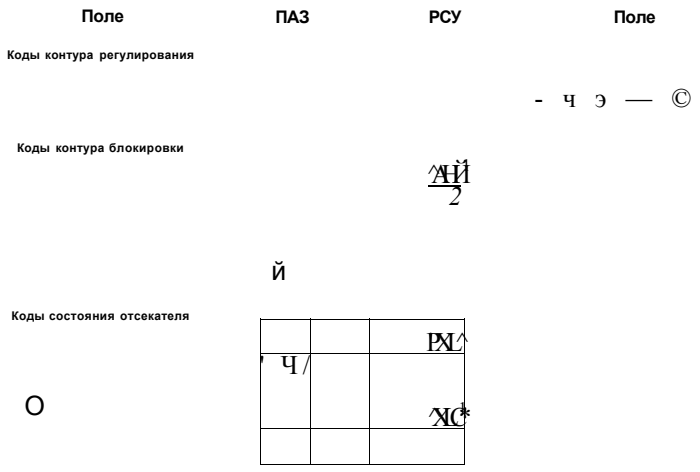
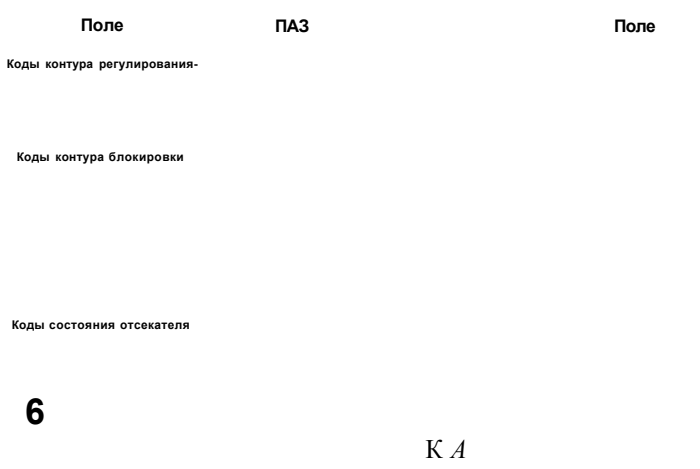


Рис. 10.21

Отсекатель. Вариант 3:



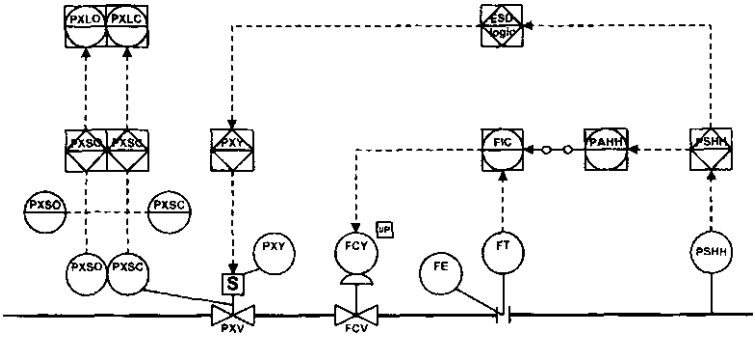
Отсекатель. Вариант 4:



6

Рис,. /0.22

Отсекал*»- Вариант 3:



Отсекатель. Вариант 4:

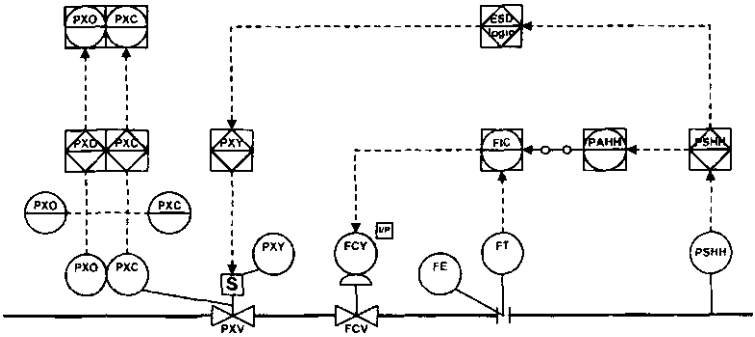
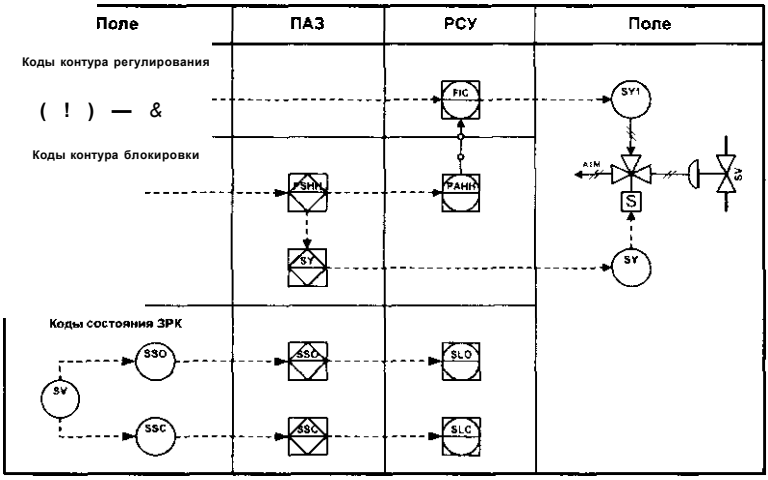


Рис. 10.23

ЗРК. РШМИТ1:



ЗРК, вариант?;

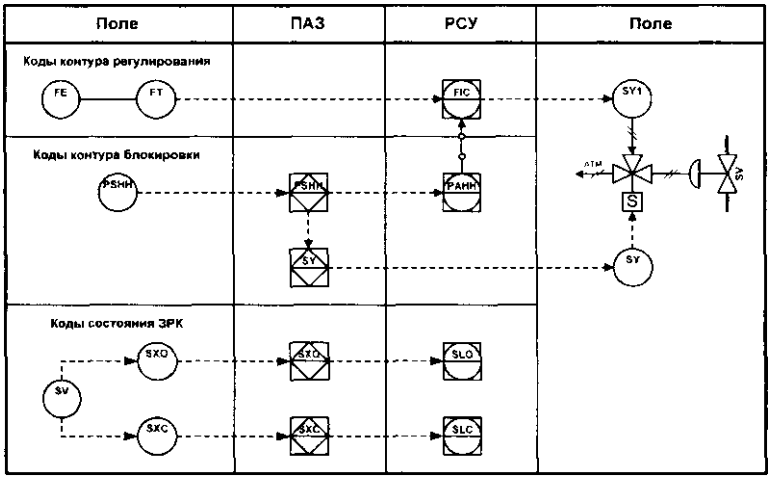
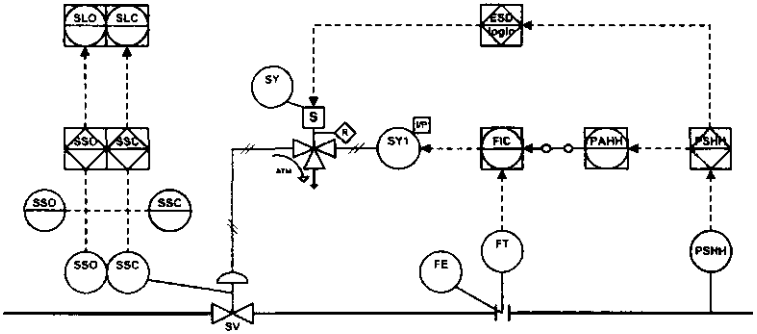


Рис. 10.24

ЗРК. Вариант 1;



?РК, Вариант 2:

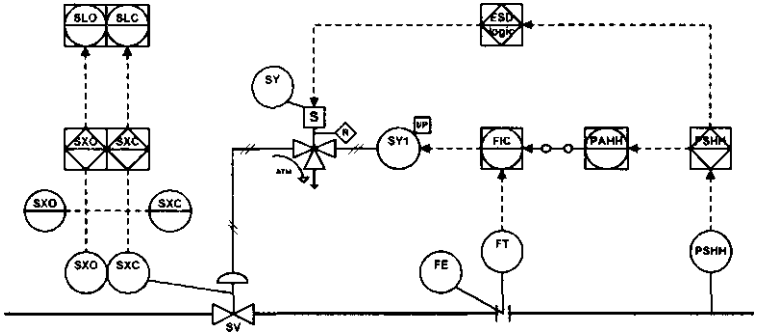
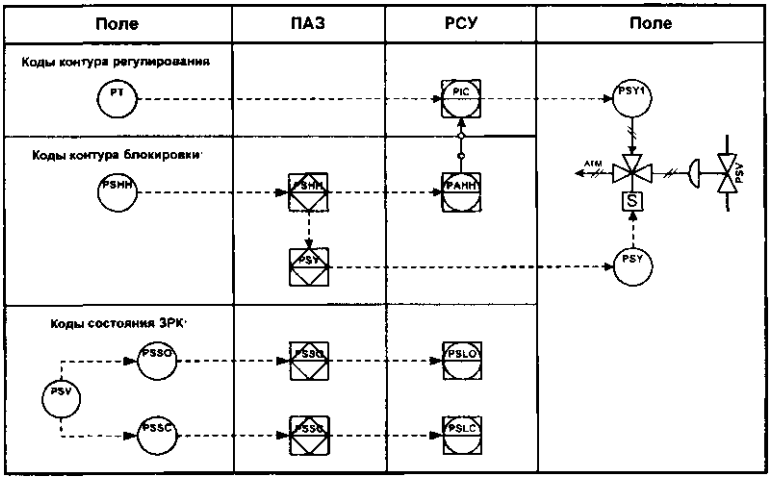


Рис. 10.25

ЗРК, Вариант 3;



ЗРК. Вариант 4:

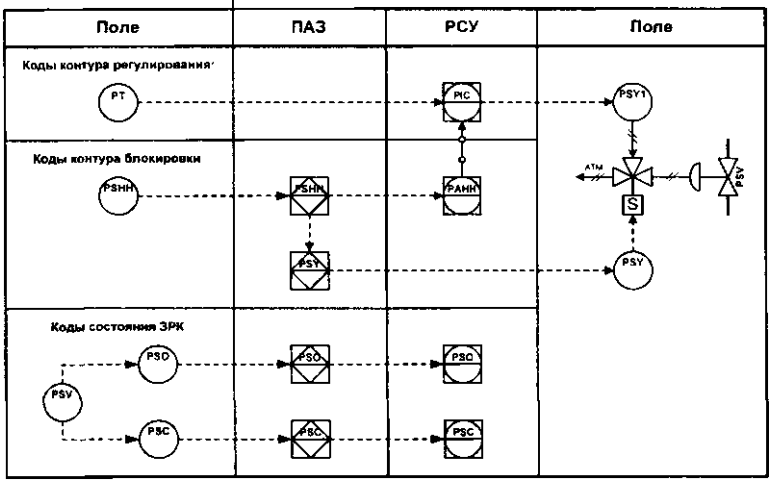
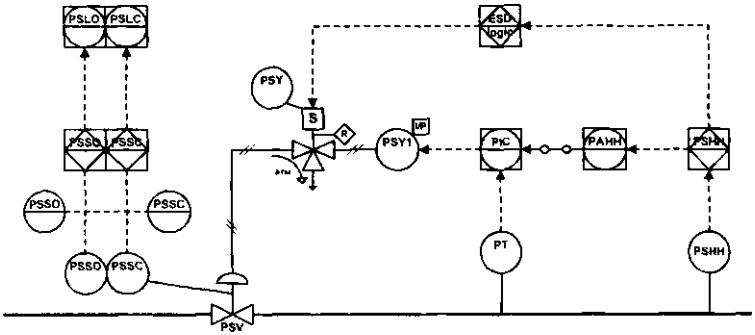


Рис. 10.26

ЗРК. Вдриэнт?:



ЗРК. Вариант 4:

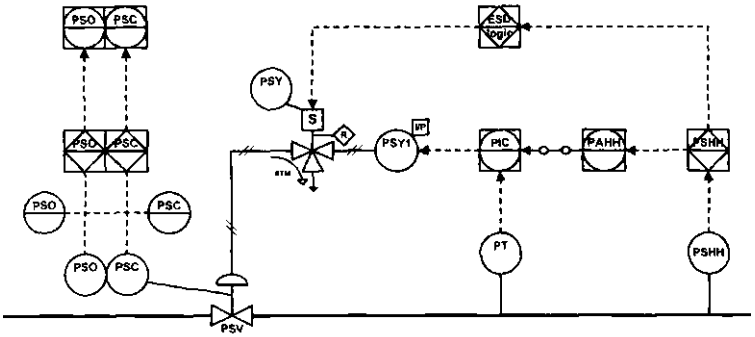


Рис. 10.27

10.14. Таблицы идентификации параметров АСУТП (таблицы 10.31 и 10.32)

Представленные в данном разделе таблицы 10.31 и 10.32 можно рассматривать в качестве информационной модели некоторого вполне реального проекта АСУТП.

Порядок расположения и группировка параметров РСУ и ПАЗ. Порядок расположения и группировка параметров АСУТП призваны отобразить элементарный жизненный цикл системы:

Исходное СОСТОЯНИЕ ЦЕЛЬ ДЕЙСТВИЕ, направленное на изменение состояния для достижения цели. По сути дела - это горизонтальная развертка контура управления или защиты с обратной связью:

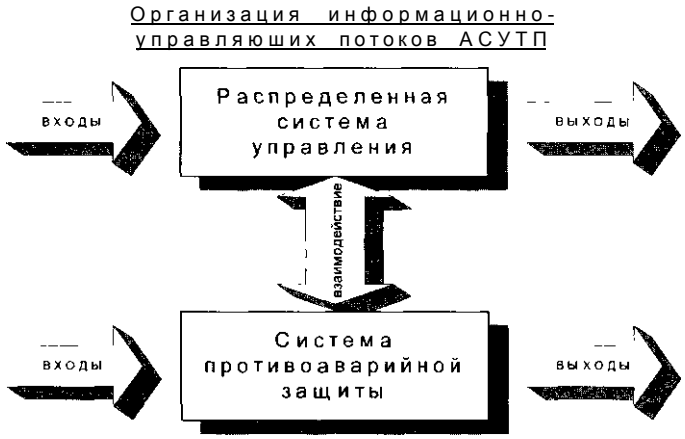


Рис. 10.28

** Необходимо обратить внимание на двунаправленность стрелки с надписью "взаимодействие".*

Таким образом, мы приходим и к архитектуре АСУТП, и к моделирующей ее структуре кодов.

Ключевая идея:

ПАРАМЕТРЫ РСУ И ПАЗ ВЫСТРАИВАЮТСЯ ПО ПРИНЦИПУ ВЗАИМНООДНОЗНАЧНОГО СООТВЕТСТВИЯ.

При этом должно быть обеспечено выполнение следующих требований:

- Все дискретные и аналоговые входы в систему ПАЗ должны быть зеркально отражены в РСУ;
- Для каждого аналогового входа все предаварийные сигналы, порожденные этим входом в системе ПАЗ, должны быть зеркально отражены в РСУ;
- При срабатывании блокировки (активизация логических цепей) соответствующие флаги сигнализаций о срабатывании блокировок должны быть отображены на рабочих станциях РСУ;
- Сбои и отказы системы ПАЗ должны сопровождаться соответствующими диагностическими сообщениями на рабочих станциях РСУ.

Примечание

Само собой разумеется, что все события в системе должны автоматически регистрироваться в соответствующих журналах и архивах.

Как всегда, из любого правила есть исключения. Таким исключением являются агрегаты комплектной поставки, например, компрессорные установки. В этом случае изготовитель оборудования берет на себя всю ответственность за управление и защиту агрегата. Как правило, подобное оборудование оснащается собственными контроллерами, которые самостоятельно обеспечивают функции управления и защиты агрегата.

Тем не менее, даже в этом случае устанавливается взаимодействие с системой противоаварийной защиты всей установки и, соответственно, с РСУ для обеспечения функций контроля, пуска, останова и диагностики состояния оборудования на том же фундаментальном принципе: взаимноодно-значное соответствие параметров ПАЗ и РСУ.

В соответствии с представленной на рисунке 10.28 схемой организации информационно-управляющих потоков, параметры АСУТП разнесены в две таблицы:

Таблица 10.31 - Параметры РСУ

Таблица 10.32 - Параметры ПАЗ

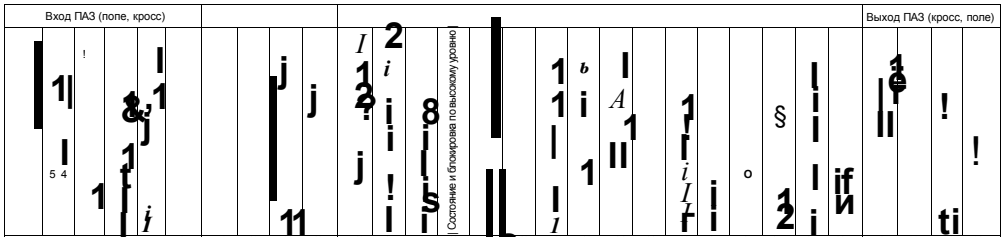
Таблица 10.32

Идентификация параметров РСУ для условного проекта

	вкод РСУ (пот, кросс)							П*р*м»тры РСУ				Пярымтры РСУ и ваимод«йстаия с ПАЗ																Выход РСУ 1«фОСС, поп»)			
	3	4	5	в	7	в		8	10	11	12	13	14	15	16	17	19	1»	го	21	22	23	24	2S	26	27	28	20	30	31	32
	1 E 1	T 1 X	II s	1 f I	1			1 -I 1	_ICn_AL)_AHI			1 -IA |	_CA IL A L L L a H H		1 aa |		} j~.L_ 1		1 dLF 1		1] dvL] dvB		П Н^I Н 11 dvR j dvS |				)_AYI		_V)	_V \
АНАЛИЗАТОР		AT						Al				AIA			AAHH	AAA															
Плмыя горелки														BALL																	
печь																															
ДВИГАТЕЛЬ																															
Расход		FT						FT	FIC				FCS	FALL															FY	FCV
Положение, перемещение												GIA		GALI	SAIH															
КОМПРЕССОР																															
То* (электрический)		IT						II							IAHH																
Уроеень, перепей		(d)LT		tSL				LI	LIC	LAL		U «	LCS	LALL															LY	LCV
НАСОС																		N	LS	NLF		HVL	NVB	N TS		NVR	NVA			*НЧ*	
Давление, перепад		fdIPT		PSL				PI	PIC	PAL		PI A		PALL															PV	PCV
Количество число																															
		ST						SI	SIC			SIA																	SY	scv
ЗАЛОРНО-РЕГ КЛАПАН																		SLO	SLC	SLF		SVL	SVB	SHS		SVR	SVA		SVX	SV
	TE	TT						TI	TIC			TIA																	TV	TCV
												VIA			VAHH															
ОТСЕКАТЕЛЬ																		XLO	XLC	XLF		XVL	XVB	XHS		XVR	XVA				
ЭЛЕКТРОЗАДВИЖКА				zs														ZLO	ZLC	ZLF		ZVL	2V B	ZHO	ZNC	ZVR	ZVA		ZY	ZV	

Таблица 10.32

Идентификация параметров ПАЗ для условного проекта

	Вход ПАЗ (поле, кросс)																														Выход ПАЗ (кросс, поле)			
																																		
	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32				
	1	E 1	_T	_X_	11 S	_I M	1	I -I	I -1C	|| ..AL	j AHI	I	IS I	csII	SLLL	SHH	AY	II	S I	S	|[dSF[	11	dvM I	dvD 11	Y I	Y 11	dvR [	dvS]	2»	AAY	JL - ˅ I	- ˅ I		
АНАЛИЗАТОР					ASHH									ASHH	AAY													AAY					
Пламя горелки					BSLL								BSLL																	BY			
ПЕЧЬ																																		
Расход		FT		FSLL							FIS	FCS	FSLL																	FY			
Положение, пшрая		**от**		GSLL							GIS		GSLL	GSHH																GY			
КОМПРЕССОР																																		
Тон (электрический)				ISHH										ISHH																IY			
		(d)LT		LSLL							LIS	ICS	LSLL																	LY			
НАСОС				NSS	*NSF*												*HSS*		NSF		NVM	NVD		NTS		NVR	MVS			NY			
Давление, **перепад**		**«OPT**		PSLL							PIS		PSLL																	PY			
Количество, число																																		
Радиоактивное ть																																		
Скорость, частота																																		
ЗАПОРНО-РЕГ КЛАПАН				SS	SSF												SSO	SSC	SSF		SVM	SVD		SYS		SVR	SVS			SV	SV		
Вязкость, Вибрация		VT									VIS			VSHH															VY			
Воздуходуака, вантил«																																		
О ГСЕКА *ТЕЛЬ*				XS	XSF												XSO	XSC	XSF		XVM	XVD		X**rs**		XVR	**xvs**			XY	XV		
ЗЛЕКТРОЗАДВИЖКА					ZSF												ZSO	ZSC	ZSF		ZVM	ZVD	ZYO	ZYC		ZVR	**zvs**			ZY	**zv**		

Элементы таблиц разбиты на четыре группы:

1. **Измерительные (входные) устройства (колонки 3-8);**
2. **Собственные параметры и контуры РСУ (колонки 9-12);**
3. **Контуры ПАЗ и параметры взаимодействия РСУ и ПАЗ (колонки 13 -28);**
4. **Выходные устройства (колонки 29-32).**

Замечание

Входные измерительные устройства и преобразователи выходных сигналов не обязательно находятся непосредственно на установке (в "поле"), однако сущность выделения их в самостоятельные группы не меняется: это реальные физические устройства, со своей собственной кодировкой.

Очевидно, не будет большого преувеличения сказать, что таблицы 10.31 и 10.32 вообще не содержат параметров, не имеющих отношения к безопасности (кроме, может быть, колонки 9 - *Индикатор*, да и то лишь по формальным признакам).

Далее следует детальный разбор содержания таблиц идентификации непосредственно по колонкам.

10.15. Структура Таблиц идентификации

Колонка 1 - Первая буква.

Для законного включения в таблицу идентификации **параметров дискретного состояния и управления** устройствами вводятся строки, соответствующие собственно этим устройствам, как то:

- Компрессоры
- Электроприводы, двигатели
- Насосы
- Запорно-регулирующие клапаны
- Отсекатели
- Воздуходувки,вентиляторы
- Электрозадвижки.

Соответственно, в исходную Таблицу стандарта ISA S5.1-1984 вводятся следующие новые определения:

Символ A.
Для идентификации параметров состояния и управления анализатора общего вида, включая:

- Поточные анализаторы,
- Хроматографы,
- Сигнализаторы.

Символ B.
Для идентификации параметров состояния и управления Печи *{Burner* - Печь, Горелка).

Символ D.
Для идентификации параметров состояния и управления Электродвигателя, Электропривода общего назначения.

Символ G.
Для идентификации параметров состояния и управления Компрессора.

Символ N.
Для идентификации параметров состояния и управления Насоса. Любопытно, что в кириллице славянских рукописей 10-го века современная буква Н имела именно такое начертание: N.

Символ S.
Для идентификации параметров состояния и управления Запорно-регулирующего клапана. Символ S - зЪло - также имел место в древнеславянской азбуке, предшествуя и тогдашней, и нынешней букве 3.

Символ V.
Для идентификации параметров состояния и управления Воздуходувки / Вентсистемы.

Символ X.
Для идентификации параметров состояния и управления Отсекателя.

Символ Y.
Возможный вариант для идентификации параметров состояния и управления Насоса, или любого другого устройства. В таблицах 10.31 и 10.32 не используется. Но для взрывоопасных процессов "умственный" резерв так же необходим, как и физический резерв оборудования.

Символ Z.
Для идентификации параметров состояния и управления Задвижки.

Отличающиеся только поворотной симметрией второго порядка символы **N** и **Z** и в отечественной, и в западной версии стандарта свободны и являются резервными, тем более что для обозначения оконечных устройств (концевиков) задвижки буква Z уже используется.

Колонка 2 - Стандартная измеряемая переменная.

Содержит словесное описание переменной. В наших терминах в состав информационных компонент включаются не только наименования технологических переменных, но и наименования конкретных типов технологического оборудования.

Перед описанием кодов таблиц идентификации во избежание недоразумений в определении взаимнооднозначного соответствия отечественных и зарубежных понятий для периферийного оборудования, вводится небольшой, но зато американский глоссарий.

10.16. Небольшой американский глоссарий

ISA дает следующие определения:

Transducer - Преобразователь; Датчик (передатчик) как общий термин для устройства, которое:

- Получает информацию в виде одной или нескольких физических величин;
- Модифицирует полученную информацию или ее форму
  (если требуется);
- Производит результирующий выходной сигнал.

В зависимости от приложения, *Transducer* может быть:

- *Primary element (detector / sensor),*
- *Transmitter,*
- *Relay,*
- *Converter, или другое устройство.*

Поскольку термин *Transducer* не имеет вполне определенного и точного значения, его использование для конкретных приложений стандартом ISA не рекомендовано.

Converter - Преобразователь. Устройство, которое получает информацию в одной форме, а передает *(transmits)* выходной сигнал в другой форме. *Converter* (Преобразователь) часто переводится как синоним термина *Transducer.*

Однако, как уже сказано, *Transducer* - это самый общий термин, и его использование для обозначения именно преобразования сигнала **не рекомендуется.**

Transmitter - Стандартный измерительный преобразователь. Прибор *(Instrument),* который осуществляет преобразование выходного сигнала чувствительного элемента - сенсора - в стандартный сигнал 4-20мА называется Трансмиттером, но не Преобразователем (*Converter*). Так, например,

- Первичный измерительный элемент - *Primary Element — (TE)* может быть интегрирован в
- Стандартный измерительный преобразователь - *Transmitter - (TT),* но не в обобщенный преобразователь - *Converter - (ТУ).*

На наш взгляд, эта рекомендация ISA подкрепляет наше решение отказаться в дальнейшем от использования символа **Y** для определения **входного** преобразователя. Символ **Y** будет использоваться только для определения **выходного** преобразователя.

Таким образом, одним из ключевых определений, которое часто переводится как обобщенное понятие "Датчик", является определение

Transmitter - стандартный измерительный преобразователь. Устройство, которое воспринимает технологическую переменную посредством первичного измерительного элемента - сенсора *(sensor),* чье значение изменяется только как предопределенная функция технологической переменной, и преобразует эту величину в стандартный выходной сигнал.

Sensor / Primary Element - Сенсор / Первичный измерительный элемент. Может быть, а может и не быть встроен или интегрирован в *Измерительный преобразователь - Transmitter ("Датчик").*

А теперь несколько собственных определений, без знания и понимания которых невозможно произвести логическое и физическое разделение функций системы ПАЗ и собственно распределенной системы управления - РСУ.

10.17. Уровни сигнализации. Определения

Точная и ясная терминология имеет решающее значение при решении любых научно-технических и прикладных задач.

В данной работе в отличие от ПБ 09-540-03 предлагается продуманная система определений для граничных значений и сигнализаций, которую вслед за главой "Общие требования при создании АСУТП" не грех повторить.

Предупредительная сигнализация - это сигнализация, которая возникает при выходе за предупредительное значение параметра технологического процесса.

Предаварийная сигнализация - это сигнализация, которая возникает при выходе за предаварийное значение параметра технологического процесса.

Этим определениям и будем следовать, понимая под обозначениями

- SL и SH - **входные для РСУ**
  дискретные сигналы от реле предупредительного нижнего и верхнего уровней.

Соответственно, под

- AL и AH - предупредительную сигнализацию нижнего и верхнего уровней.

Под обозначениями

- SLL и SHH - **входные для системы ПАЗ**
  дискретные сигналы от реле предаварийного нижнего и верхнего уровней.

Соответственно, под

- _ALL и AHH - предаварийную сигнализацию нижнего и верхнего уровней, передаваемую из ПАЗ в РСУ, а также выдаваемую на специальные оперативные панели системы ПАЗ, или на внешние извещатели на площадке.

Представленные определения настолько важны, что для их однозначного понимания подготовлена специальная схема (рис. 10.29).

Примечание

Подробное обсуждение и обоснование этих определений проведено в главе Общие требования при создании АСУТП".

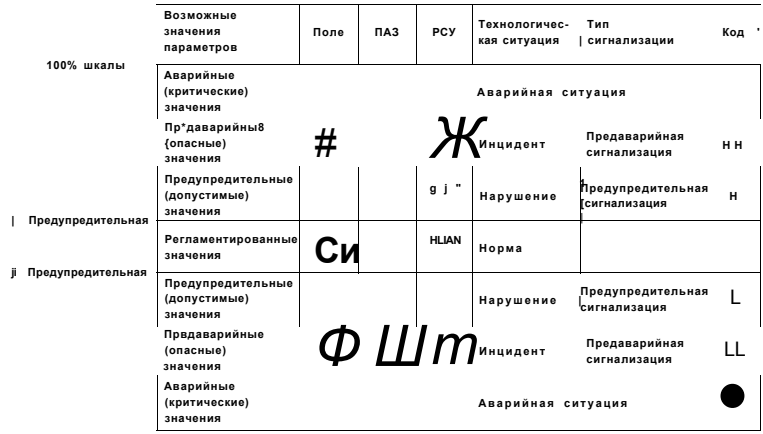


Рис. 10.29

10.18. Входные устройства

Колонка 3 - Первичный измерительный элемент.
(Primary Element. Синоним - Sensorj
Стандартная форма
и для РСУ, и для ПАЗ: _ E *(Element)*

Форма _E сохранена для полноты, и в качестве напоминания, что существующие температурные первичные измерительные элементы TE могут и не иметь преобразователей со стандартным выходом 4-20мА. Если температурный элемент (TE) интегрирован с *преобразователем сигнала стандартного уровня*, то, согласно рекомендации ISA, он будет именоваться **стандартным измерительным преобразователем - трансмиттером** *(transmitter* **- 77),** но не обобщенным преобразователем *(converter - TY).*

Замечание

В отличие от монтажно-технологических схем, на функциональных схемах автоматизации первичные измерительные элементы типа FE - диафрагма, как правило, специально не обозначаются, а чаще вообще не изображаются, чтобы не загромождать схему.

Колонка 4 - Стандартный измерительный преобразователь 4-20 mA. Стандартная форма
и для РСУ, и для ПАЗ: _ T *(Transmitter)*
Если бы речь шла только о привычном локальном регулировании, перечисленных входных параметров было бы вполне достаточно. Сложности возникают:

- В системах с периодическим регламентным переключением технологического оборудования и соответствующей перестройкой технологического процесса,
- При проведении операций пуска - останова и, тем более,
- В системах противоаварийной защиты.

Так возникает необходимость в нижеследующих кодах.

Колонка 5 - Входной измерительный преобразователь общего вида. Стандартная форма
и для РСУ, и для ПАЗ: X _ *(X-transducer)*
Для дискретных входов общего вида форма состоит из двух символов:

- Первый символ - символ параметра или устройства,
- Второй - X - признак дискретного входа.

Третий символ используется для точного определения символьной переменной состояния устройства - 0/C/S/F.

Колонка 6 - Входное контактное устройство, реле общего вида. Стандартная форма
и для РСУ, и для ПАЗ: _ S _ *(Safety)*
Для дискретных входов общего вида состоит из двух символов:

- Первый символ - символ параметра или устройства,
- Второй - S - признак дискретного входа.

Третий символ используется для точного определения символьной переменной состояния устройства - 0/C/S/F.

Пояснение

*Символ **S во второй позиции** стандартом ISA определяется как сокращение термина SAFETY - БЕЗОПАСНОСТЬ. Применяется для обозначения ИСКЛЮЧИТЕЛЬНО и ТОЛЬКО:*

- *Критических первичных измерительных элементов (EMERGENCY PROTECTIVE PRIMARY ELEMENTS),*
- *Оконечных элементов критических исполнительных устройств*

(EMERGENCY PROTECTIVE FINAL CONTROL ELEMENTS).

Примечание

Приведены оба из рассмотренных вариантов кодировки входных дискретных сигналов - и на основе второго символа X, и на основе символа S. Любой из вариантов имеет право на существование. Кодировка на основе символа S находится в структуре кодов ISA. Кодировка на основе символа X отличается уникальностью, и позволяет однозначно соотнести коды входов и выходов: X-Y.

В данной работе излишне общая кодировка для входных и выходных преобразователей всех типов посредством символа ***У*** *сохранена только для* ***выходного*** *преобразователя, чтобы не создавать пересечений, без которых вполне можно обойтись. В любом случае это решение ничуть не хуже, чем форма _Z для обозначения выходов, которую предлагает стандарт ISA.*

Важное утверждение:

Для идентификации состояния оборудования можно обойтись кодами в той же стандартной форме, что и для кодов технологических переменных - _S_ *(Safety),* где ведущий символ - символ устройства. Последний символ - символ конкретного элемента, характеризующего состояние устройства. Главное условие, которое должно быть соблюдено - коды состояния данных устройств должны однозначно идентифицироваться как таковые.

Колонка 7 - Неисправность оборудования.

Стандартная форма системы ПАЗ: _ S F *(Safety- Fault)*
Соответствующая форма РСУ: _ L F *(Light - Fault)*
Ведущий символ - символ устройства.
Неисправность может определяться:

- Непосредственно - как дискретный входной сигнал;
- Косвенно - по группе параметров состояния объекта;
- При использовании "интеллектуальных" датчиков с протоколами HART или Fieldbus - как сопутствующая диагностика.

Как было отмечено ранее, еще один привлекательный вариант данного кода может быть представлен в соответствии с шаблоном **dvF.**

Колонка 8 - Резерв.

10.19. РСУ. Параметры состояния и управления

Колонка 9 - Индикатор.
Стандартная форма: _ I *(Indicator)*
Колонка 10 - Регулятор общего вида.
Стандартная форма: _ T C *(Indicator-Control)*
Альтернативный вариант: _ C
Колонка 11 - Предупредительная сигнализация низкого уровня.
Стандартная форма: _ A L *(Alarm - Low)*
Колонка 12 - Предупредительная сигнализация высокого уровня.
Стандартная форма: A H *(Alarm - High)*

10.20. ПАЗ - РСУ. Параметры взаимодействия

Колонка 13 - Аналоговый ввод с сигнализацией общего вида.
Стандартная форма системы ПАЗ: _ I S *(Indicator - Safety)*
Соответствующая форма РСУ: _ I A *(Indicator - Alarm)*
Колонка 14 - Совместный контур РСУ и ПАЗ.
Стандартная форма системы ПАЗ: _ C S *(Control - Safety)*
Данная форма с дополнительным символом **S** используется для выделения тех контуров управления, которые имеют общий вход и в РСУ, и в ПАЗ, либо выход на общий запорно-регулирующий клапан.
Строго соответствующая форма РСУ: _ C A *(Control - Alarm)*
Если ставится задача единообразия, либо и РСУ, и ПАЗ существуют в единой программно-технической среде, то вполне применима и единая форма **CS** и в РСУ, и в ПАЗ.

Примечание

Для обычных контуров управления РСУ по-прежнему используется либо привычная форма
JC: FIC, LIC, P/C, *TIC,*
либо более компактная
_C: FC, LC, PC, TC.

Колонка 15 - Состояние и блокировка по низкому уровню.
Стандартная форма системы ПАЗ: _ SLL *(Safety - Low Low)*
Соответствующая форма РСУ: _ ALL *(Alarm - Low Low)*

Колонка 16 - Состояние и блокировка по высокому уровню.

Стандартная форма системы ПАЗ: __ SHH *(Safety-High High)*
Соответствующая форма РСУ: _ AHH *(Alarm-High High)*

Примечание

Нет никаких препятствий для использования полностью идентичных кодов для совместных контуров, состояний и блокировок на базе единого символа Sue ПАЗ, и в РСУ.

Колонка 17 - Выдача световой / звуковой предаварийной сигнализации на площадку.

Стандартная форма системы ПАЗ: _ A Y *(Annunciation)*
Соответствующая форма РСУ: _ A A *(Annunciation)*
Ведущий символ - символ параметра или устройства.

Колонка 18 - Резерв.

Колонки 19 и 20 - Состояние оборудования.

Хотя в данном пункте приводятся коды состояния только запорно-регулирующего клапана, отсекателя и задвижки, легко просматривается распространение данного кода и на другие единицы и элементы оборудования, причем не обязательно как чисто физический вход.

Это может быть комплексный показатель, определяемый на основе состояния группы параметров устройства или единицы оборудования.

Стандартная форма системы ПАЗ: _ S _ *(State)*
Соответствующая форма РСУ: _ L _ *(Light)*
Ведущий символ - символ устройства.

Символ в конце формы введен для идентификации конкретных состояний оборудования.

Это дополнительное поле может быть использовано для уточнения состояний элементов и параметров оборудования на основе символов L и H, рекомендованных стандартом ISA S5.1-1984:

ZSL, ZSH и ZLL, ZLH

В данной работе рассмотрены два варианта:

- Стандартный - L/H *(Low / High)*
- Особый - O/C *(Open /Close),* R/S *(Run /Stop)*.

Второй вариант представляется более предпочтительным.
Например, для ЗРК, отсекателя и задвижки в системе ПАЗ и в РСУ вместо кодов, которые должны были появиться по стандарту ISA (таблица 10.33),

Таблица 10.33

ПАЗ			РСУ		
SS_:	SSH	SSL	SA_:	SAH	SAL
XS_:	XSH	XSL	XA_:	XAH	XAL
ZS_:	ZSH	ZSL	ZA_:	ZAH	ZAL

получаем:

Таблица 10.34

ПАЗ			РСУ		
SS_:	SSO	SSC	SL_:	SLO	SLC
XS_:	XSO	**XSC**	XL_:	XLO	XLC
ZS_:	ZSO	**ZSC**	ZL_:	ZLO	ZLC

Как сказано, коды таблицы 10.33, выстроенные в соответствии с правилами стандарта ISA, допускают неоднозначное толкование.

Повторим важнейший результат, который был получен при рассмотрении физических входных устройств:

1. Если существует необходимость точной привязки запорно-регулирующей арматуры к технологической переменной, коды состояний запорно-регулирующего клапана, отсекателя и задвижки предваряются символом технологической переменной:

Таблица 10. 35

ПАЗ			РСУ		
FSS_	FXS_	FZS_	FSL_	FXL	FZL_
LSS_	LXS_	LZS_	LSL_	LXL_	LZL_

PSS_	PXS_	PZS_	PSL_	PXL_	PZL_
TSS_	TXS_	TZS_	TSL_	TXL_	TZL_

2. Если обратить внимание, что параметры состояния ЗРК, Отсекателя и Задвижки по определению являются дискретными, то непосредственной необходимости в использовании символа S в третьей позиции кода ПАЗ - нет. И если сделать следующий шаг, и принять единообразную кодировку данной группы параметров и в поле, и в ПАЗ, и в РСУ, то коды приобретут совершенно лаконичную и законченную форму:

Таблица 10.36

ПОЛЕ	ПАЗ	РСУ
FSO	FSO	FSO
FSC	FSC	FSC
LXO	LXO	LXO
LXC	LXC	LXC
PZO	PZO	PZO
PZC	PZC	PZC
TZO	TZO	TZO
TZC	TZC	TZC

<u>Колонка 21</u> - Неисправность оборудования.
Стандартная форма системы ПАЗ: _ S F *(Fault)*
Соответствующая форма РСУ: _ L F *(Fault)*
Ведущий символ - символ устройства.

Существует еще один вариант данного кода на основе уже не символа устройства, а целиком двухсимвольного кода устройства. Причем код устройства в данном случае можно рассматривать в самом широком смысле - в том числе и как код

некоторого полевого устройства КИП. Шаблон этой формы выразится как **dvF.** Эта форма также обладает достаточной универсальностью, ибо позволяет задавать индивидуальные коды ошибок для всех типов полевых устройств, например:

FTF = FT-F, PSF = PS • F.

Колонка 22 - Резерв.

Колонка 23 - Положение ключа Дистанционное / Местное управление.

Конкретный вид некоторых кодов не имеет решающего значения - главное, чтобы они вообще были. Служебные коды типа ключа "Дист/Мест", ключ "Обхода блокировки", команда "Возврат в исходное состояние" допускают определенную свободу выбора.

Возможна свежая кодировка ключа на основе не затертого термина *Switch* - SW. Код модифицируется предваряющим команду символом устройства.

Стандартная форма системы ПАЗ: __ S W *(Switch)*
Соответствующая форма РСУ: _L W *(Switch-Light)*

Пояснение

Термин SWITCH - ПЕРЕКЛЮЧАТЕЛЬ, КЛЮЧ - стандартом ISA определяется как устройство, которое:

- *Соединяет (conncct),*
- *Разъединяет (disconnects),*
- *Выбирает (selects),*
- *Передает / Переключает (transfers),*

одну, или несколько цепей, но при этом не обозначено как

- *РЕГУЛЯТОР (CONTROLLER),*
- *РЕЛЕ (RELAY), или*
- *РЕГУЛИРУЮЩИЙ КЛАПАН (CONTROL VAL VE).*

Термин SWITCH обычно применяется в тех случаях, если устройство используется для

- *Сигначизации (ALARM)*
- *Оповещения (PILOT LIGHT)*
- *Выбора (SELECTION)*
- *Переключения (INTERLOCK)*
- *Безопасности / Защиты (SAFETY).*

В качестве глагола (действия) данный термин также используется для обозначения ФУНКЦИЙ, выполняемых ПЕРЕКЛЮЧА ТЕЛЯМИ

Колонка 24 - Ключ Обхода блокировки (Деблокирующий ключ).

Стандартная форма РСУ: B *(De Block)*
Стандартная форма системы ПАЗ: D *(De Block)*
Ведущий код - код входной переменной PS, FT, или код устройства SV, NV, ...

Примечание

Если АСУТП строится е единой программно-технической среде, то коды ключей в РСУ и ПАЗ будут совпадать.

Колонки 25-26 - Команды Дистанционного Управления.

Вместо многочисленных вариантов кодов
(см. таблицы 10.13-10.15):

- HS,HC
- HPBL, SB
- ZH, ZL, ZS
- NS

вводится единая форма, основанная на коде переключателя HS *(Hand Switch),* предваряемого символом устройства (N, S, X, Z):

Стандартная форма РСУ: _ H _ *(Hand- witch)*
Стандартная форма системы ПАЗ: Y _
Последнее поле кода служит для уточнения типа команды:

Таблица 10.37

Насос		ЗРК		Отсекатель		Задвижка	
Пуск	**NHR**	**Открыть**	**SH O**	**Открыть**	**XHO**	**Открыть**	**ZHO**
Останов	**NHS**	**Закрыть**	**SHC**	**Закрыть**	**XHC**	**Закрыть**	**ZHC**

Таблица 10.38

Насос		ЗРК		Отсекатель	
Пуск, Останов	NHS	Открыть Закрыть	SHS	Открыть Закрыть	XHS

Важным исключением являются некоторые электрозадвижки - с ТРЕМЯ раздельными физическими кнопками управления:

- ЗАКРЫТЬ
- ОТКРЫТЬ
- СТОП.

Для них можно установить свои собственные уникальные коды, например:

- ЗАКРЫТЬ: ZPBC
- ОТКРЫТЬ: ZPBO
- СТОП: ZPBS,

либо сохранить единообразную с другими устройствами систему формирования кодов. Примеры применения описанной системы кодов представлены на нижеследующих схемах обвязки оборудования.

Пример функциональной обвязки электрозадвижки

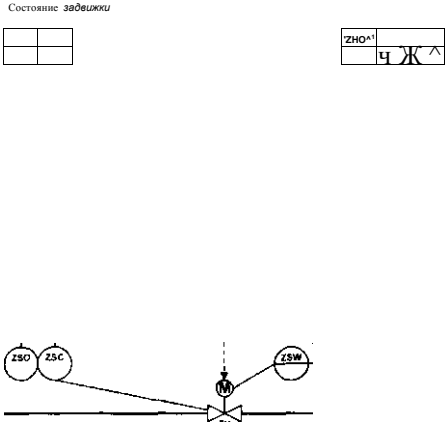


Рис. 10.30

Замечание

Сопровождение функциональных блоков на схеме словесными пояснениями - это хорошая практика.

Примеры функциональной обвязки отсекателя

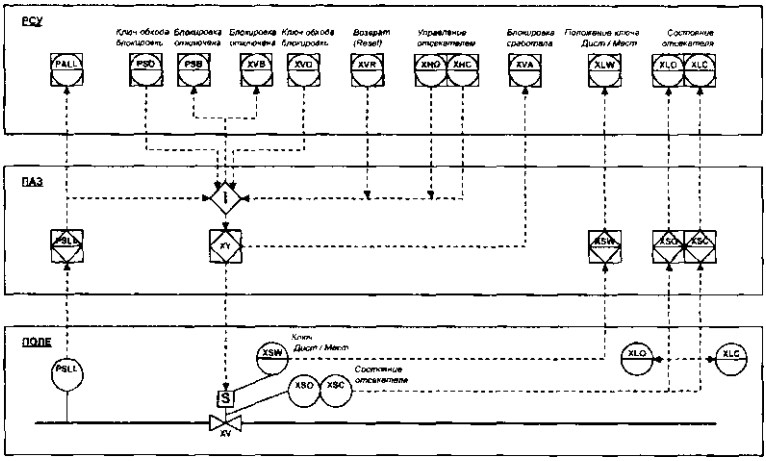


Рис. 10.31

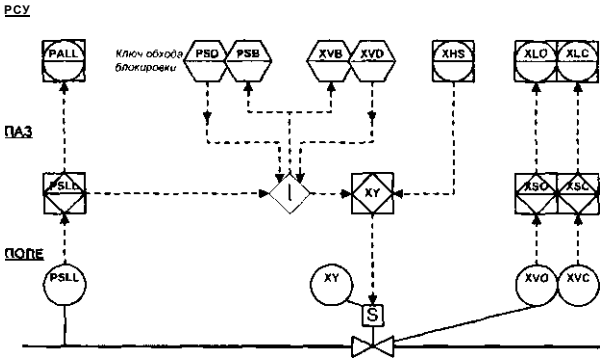


Рис. 10.32

Шестиугольники на последней схеме изображают программные (логические) переменные, доступные инженеру КИПиА с выделенной станции по обслуживанию полевого оборудования, или с инженерной станции РСУ.

Колонка 27 - Готовность, или подготовка оборудования к работе - Возврат к исходному состоянию *{Reset).*

Формируется автоматически, вручную, или на основе состояния группы ключевых параметров устройства (температуры подшипников, заполнение насоса и т.д.) для дополнительной проверки и контроля состояния и возврата устройства в исходное состояние для подготовки оборудования к пуску.

Стандартная форма системы ПАЗ:_____R *(Reset)*

Соответствующая форма РСУ:_____R *(Reset)*

Двухсимвольный ведущий код - код устройства: NV, SV, XV, Z V.

Колонка 28 - Сигнализация срабатывания блокировки.

Признак срабатывания блокировки в ПАЗ:_____S

Получение сигнализации от системы ПАЗ о выдаче команды блокировки:_____A

Двухсимвольный ведущий код - код устройства:
NV, SV, XV, ZV.

Пример функциональной схемы обвязки насоса

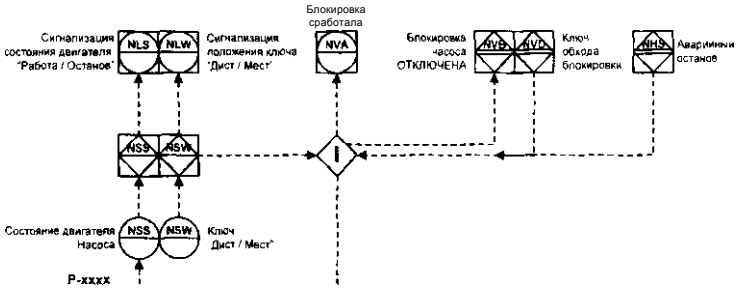


Рис. 10.33

Кнопки с двойной горизонтальной чертой - **NVD, NHS** и световое табло **NVB** расположены на дополнительной оперативной панели системы ПАЗ. Панель располагается в помещении управления в непосредственной близости от рабочих станций РСУ, и предназначена для оперативного технологического персонала.

Если символ G в качестве символа насоса представляется более привычным, чем N, нет никаких помех, чтобы построить схему обвязки насоса на его основе:

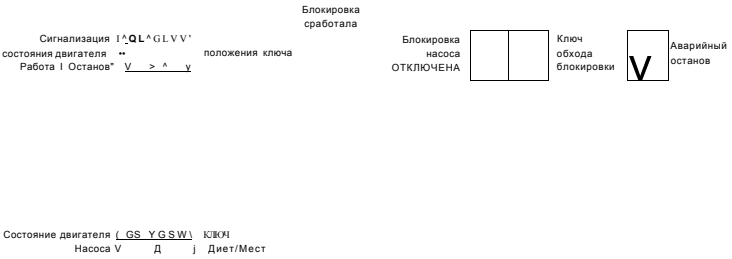


Рис. 10.34

Для сравнения приводится пример обвязки насоса из отечественной практики, выполненный рукой автора, но с точным сохранением графики первоисточника:

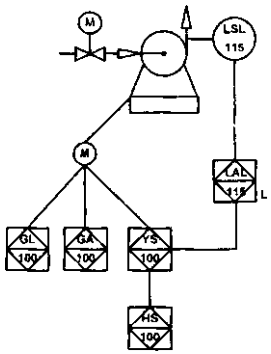


Рис. 10.35

И еще один пример, уже из инородной практики:

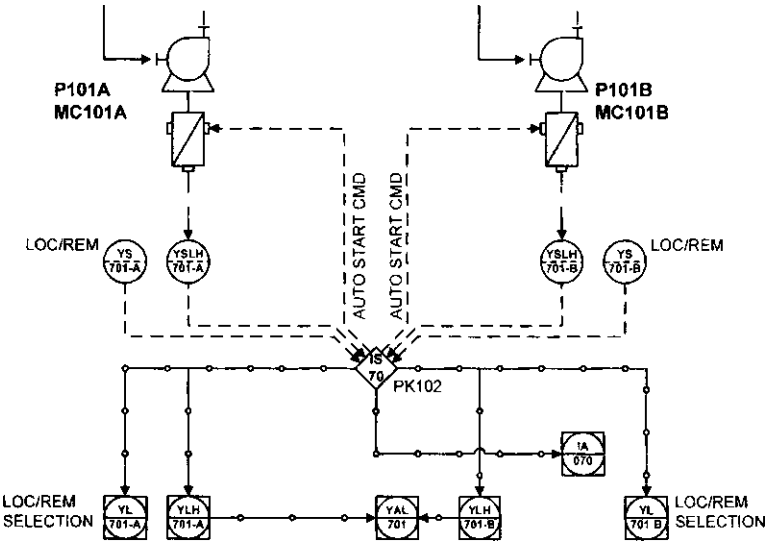


Рис. 10.36

Здесь все идентификаторы выстроены в полном соответствии со стандартом ANSI/ISA-S5.1-1984. Но если не иметь перед глазами эту схему с поясняющими надписями, понять смысл кодов совершенно невозможно.

10.21. Выходные устройства

Главный способ группировки параметров контура - привязка к технологической переменной - символу контура - информационного, управления, защиты.
Поэтому все переменные контура объединяются первым символом - символом технологической переменной. Для линейных контуров управления и защиты этот способ группировки является наиболее естественным.

Колонка 29 - Устройство световой / звуковой предаварнйной сигнализации на площадке.
Стандартная форма: A Y *(Annunciation)*
Первый символ кода - символ технологической переменной или устройства, по которому сработала сигнализация.
Колонка 30 - Резерв.
Колонка 31 - Выходной преобразователь (ЭПП, соленоид, реле). Наши нововведения:
Вводится единая кодировка выходного канала, основанная на коде выходного преобразователя Y.
Стандартная форма:_____Y
Первый символ кода- символ технологической переменной.
Второй символ - символ устройства.
Замечание
В представленной системе один раз использовано дополнительное поле позади кода - для обозначения ЭПП ЗРК.
Колонка 32 - Исполнительный механизм с регулирующим органом.
Стандартная форма:_____V *(Valve)*
Первый символ кода - символ технологической переменной.
Второй символ - символ устройства.
Примеры:

FC V	-	Регулирующий клапан расхода
FSV	-	Запорно-регулирующий клапан
FXV	-	Отсекатель
FZV	-	Электрозадвижка.

10.22. Нумерация контуров РСУ и ПАЗ

До сих пор за рамками обсуждения был оставлен мощнейший резерв уменьшения беспорядка - это алфавитно-цифровой шифр, сопровождающий код контура - существующий на действующем объекте "номер позиции". Далее рассматриваются несколько возможных вариантов нумерации.

Сквозная нумерация. При сквозной нумерации независимо от типа контура или переменной используется единая последовательность номеров либо для всего производства, либо для его отдельных частей. Принцип понятен из примера:

FIC-101 LI-102 TIA-103 PSLL-104 …

Параллельная нумерация. При параллельной нумерации исходная последовательность номеров *повторяется* для каждой новой первой буквы кода:

F1C-100 LI-100 ПА-100 PSLL-100

FIC-101 LIC-101 TI - 101 PIA - 101

FT A-102 LAH-102 TIC-102 PIC - 102

Параллельно-сквозная нумерация. При параллельно-сквозной нумерации *новая серия* номеров начинается для каждой новой первой буквы кода:

Переменная	Группа	Номер серии
F	Расход	100
L	Уровень	200
P	Давление	300
T	Температура	400
A	Анализ	500
	и т.д.	и прочее.

Для более крупных объектов шаг может быть увеличен.

Структурно-технологическая нумерация. Принцип понятен из рисунка:

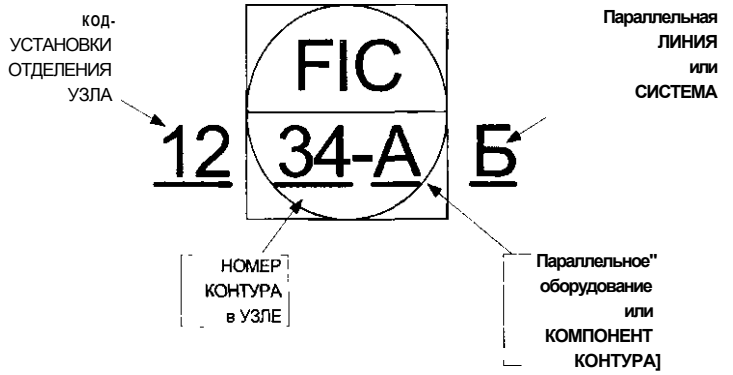


Рис. 10.37

Код установки, отделения или узла должен выноситься на общий уровень монтажно-технологической, функциональной, или экранной мнемосхемы, и указываться в атрибутах наименования или шифра схемы.

Аналогичным образом можно поступить и с кодом технологической линии, или системы.

Количество символов каждого элемента кода определяется масштабом объекта автоматизации. Сочетание представленных способов нумерации также не исключается.

Примечание

Служебные символы типа | - | / | , | . | без большой нужды лучше не использовать.

10.23. Графические символы

Структура таблиц идентификации 10.31 и 10.32 хороша уже тем, что мы ясно видим классы устройств и функций, которые требуют отображения:

- Полевые устройства
- Функции / Устройства РСУ
- Функции / Устройства ПАЗ.

10.24. Графическое изображение оборудования АСУТП

Структура таблиц идентификации является ключом к построению необходимого набора символов. Мы просто переписываем эту структуру, только другим - графическим языком.

Если не мудрить с по-над-за-щитовыми приборами, то для графического изображения оборудования РСУ, ПАЗ и полевого оборудования КИПиА и вполне достаточно нижеследующего небольшого набора графических элементов (рис. 10.38). Из всего многообразия графических изображений, представленных в начале главы, выбрано только самое необходимое. Но наш ГОСТ и здесь пошел по самому примитивному пути.

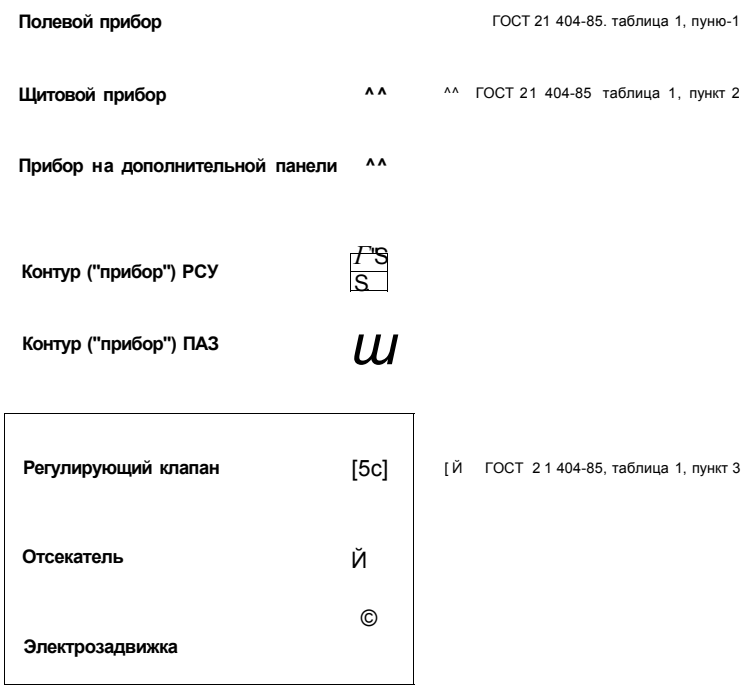


Рис. 10.38

10.25. Дополнительные возможности упрощения

Современные бесщитовые системы предоставляют хорошую возможность избавиться от "квадратуры круга" и использовать для графического изображения параметров и функций РСУ и ПАЗ непосредственно и только круг:

Рис. 10.39

Путаницы не возникнет, так как на монтажно-технологических схемах изображение автоматически и естественно ограничивается *сверху* уровнем локальной автоматики.

На функциональных же схемах АСУТП мы ограничиваемся *снизу* чисто условным обозначением точек подключения к процессу, уделяя главное внимание представлению стратегии управления.

Так что если мы имеем дело с бесщитовой, или "почти" бесщитовой системой (а с точки зрения РСУ и ПАЗ так оно и есть), то можно смело использовать эти легкие в восприятии значки. Именно эту тенденцию мы сейчас и наблюдаем.

Сравнение различных графических систем, а также предлагаемые в данной работе способы изображения оборудования КИПиА представлены на рис. 10.40. В последней колонке представлены графические возможности, или, лучше сказать, невозможности ГОСТа 21.404-85.

Дополнительные символы функциональных схем автоматизации приведены на рис. 10.41 и 10.42. Хрестоматийный набор графических символов стандарта ISA приведен для сравнения на рис. 10.43-10.48.

Сравнение УСЛОВНЫХ **обозначений на функциональных схемах АСУТП**

Обозначения, имеющие отношение к зашита и логике	1SA-S5.1 1984			
Комплектный ПЛК *(ABB Lummus - vendor package PLC ,* *PARSONS • packaged PLC)*	L^NJ I X x I			Не определено
Цифровое логическое управление, встроенное в DCS. *(ABB Lummus • batch or sequential programmable logic, PARSONS - integral to DCS)*	Специально не выделяется			
ПЛК системы противоаварийной защиты (ПАЗ)			<5>e	
Не доступно оператору				
Неопределенная логическая функция или блокировка:	О	Ф	О	Не определено
		ANSI ISA S5 1-1984		
- Параметры системы противоаварийной защиты				Не определено
- Контуры совместного ведения РСУ и ПАЗ.				Не определено
- Все прочие информационно-управляющие параметры, имеющие отношение к РСУ	rFlcN ИИ f PfC			Не определено
- Общее изображение регулирующего клапана (В том числе с электрспневмопозиционером)				
- Соленоидный отсечной клапан				Не определено
- Электрозадвижка				Не определено

Рис. 10.40

Os
oo

ИндтрументТЗЛЬНыд ЛИНИИ

Связь с технологическим процессом		
Пневматический сигнал		
Электрический сигнал		
Внутрисистемная связь (программная, или передачи данных)		
Вычислительное функции		
Функция компьютера, доступная оператору		е
Функция компьютера, недоступная оператору		о
"Регулирующие рганы"		
Проходной вентиль, задвижка		- с х н
Заслонка		4 X 1 -
Шаровой клапан		—DOC!—
Угловой клапан		
Трехходовой клапан		
Четырехходовой клапан		

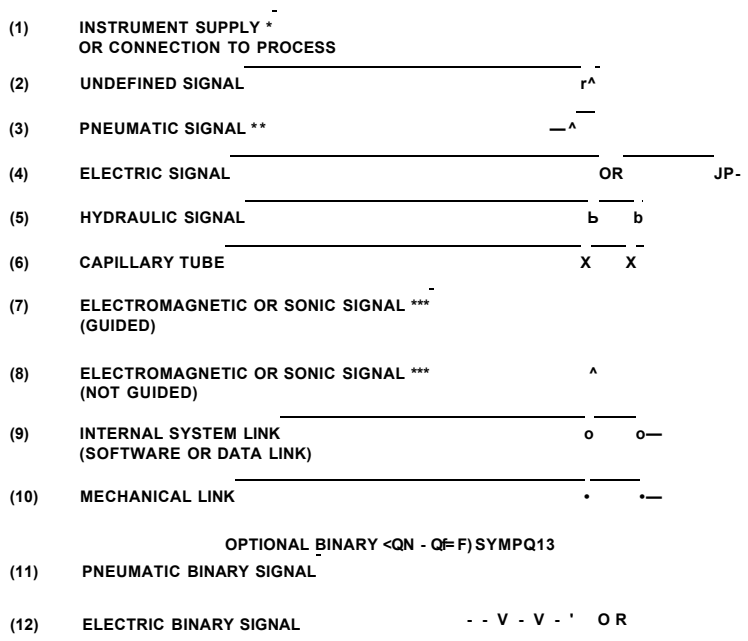
Рис. 10.41

Исполнительные механизмы

Поршневой, одноходовой	
Поршневой, двухходовой	
Рекомендуемое **изображение для всех поршневых приводов на функциональных схемах**	
Соленоид с ручным возвратом в рабочее состояние	
Соленоид с **дистанционным возвратом в рабочее состояние**	
Клапан с электропневмопозиционером	а
Рекомендуемое изображение клапана с электропневмопозиционером на функциональных схемах автоматизации	
Клапан с электропневмопреобразователем	
Рекомендуемое изображение клапана с электропневмопреобразователем на функциональных схемах автоматизации	
Исполнительный механизм, открывающий регулирующий орган при прекращении подачи энергии ("нормально" открыт)	
Исполнительный механизм, закрывающий регулирующий орган при прекращении подачи энергии ("нормально" закрыт)	
Исполнительный механизм, оставляющий регулирующий орган в неизменном состоянии	- f -
Запорно-регулирующий клапан, используемый одновременно и в РСУ, и в системе ПАЗ При отсутствии сигнала аварийной отсечки выполняет обычное регулирование	%

Рис. 10.42

Линии КИПиА



NOTE' 'Or' means user's choice. Consistency is recommended.

* The following abbreviations are suggested to denote the types of power supply. These designations may also be applied to purge fluid supplies.

AS - Air Supply
IA - Instrument Air
PA - Plant Air
ES - Electric Supply
GS - Gas Supply
HS - Hydraulic Supply
NS - Nitrogen Supply
SS - Steam Supply
WS - Water Supply

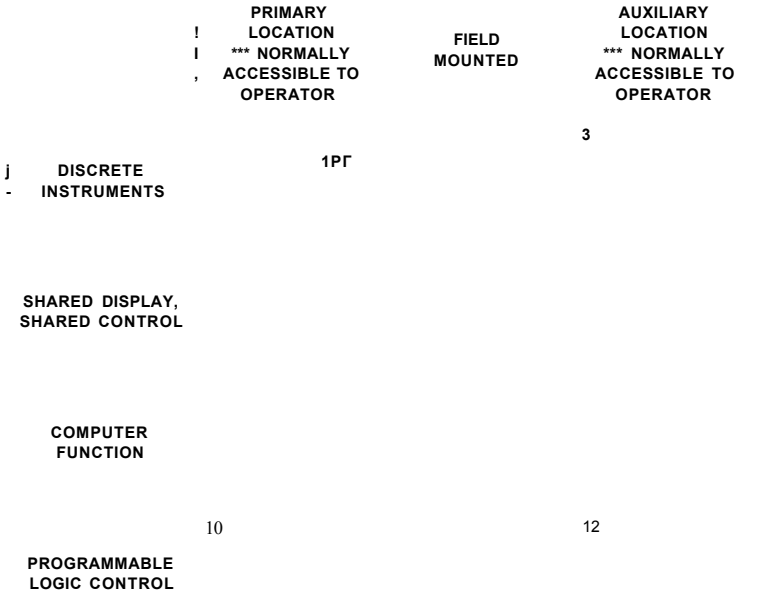
The supply level may be added to the insrument supply line, e.g., AS-10Q, a 100-psig air supply; ES-24DC, a 24-volt direct current power supply.

** The pneumatic signal symbol applies to a signal any gas as the signal medium. If a gas other than air is used, the gas may be identified by a note on the signal symbol or otherwise.

*** Electromagnetic phenomena include heat, radio waves, nuclear radiation, or light

Рис. 10.43

Общие символы приборов и функций АСУТП



Symbol size may vary according to the user's needs and the type of document A suggested square and circle size for large diagrams is shown above Consistency is recommended

Abbreviations of the user's choice such as IP1 (Instrument Panel #1), IC2 (Instrument Console #2), CC3 (Computer Console #3), etc , may be used when it is necessary to specify instrument or function location

Normally inaccessible or behind-the-panel devices or functions may be depicted by using the same symbols but with dashed horizontal bars, i e

Рис. 10.44

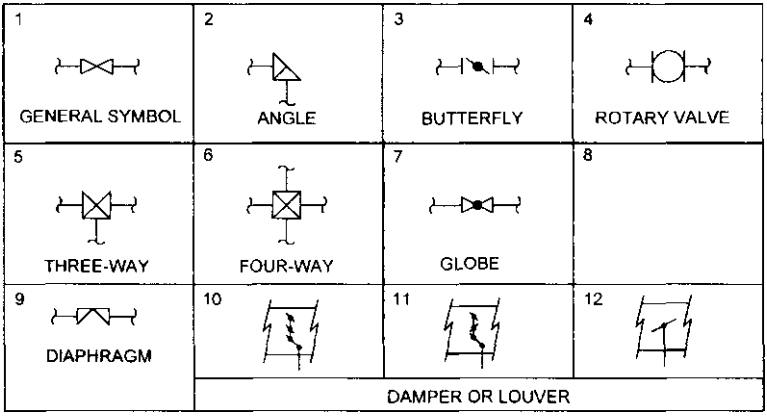
Общие символы приборов и функций АСУТП (дополнение)

13	14 2§84-23 INSTRUMENT WITH LONG TAG NUMBER	15 CO INSTRUMENT SHARING COMMON HOUSING *
PILOT LIGHT	Ф PANEL MOUNTED PATCHBOARD POINT 12	18 Ф " PURGE OR FLUSHING DEVICE
19 RESET FOR LATCH-TYPE ACTUATOR	20 И DIAPHRAGM SEAL	21 О - UNDEFINED INTERLOCK LOGIC

* It is not mandatory to show a common housing
** These diamonds are approximately half the size of the larger ones
*** For specific logic symbols, see ANSI/ISA Standard S5 2

Рис. 10.45

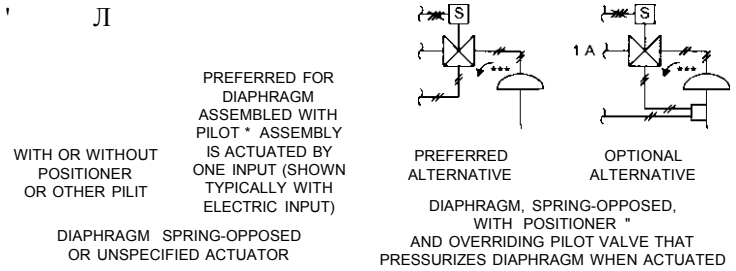
Символы клапанов



Further information may be added adjacent to the body symbol either by note or code number

Рис. 10.46

Символы приводов



* **Pilot may be positioner, solenoid va've, signal converter, etc**

** **The positioner need not be shown unless an intermediate device is on its output The positioner tagging, ZC need not be used even if the positioner is shown The positioner symbol, a box drawn on the actuator shaft, is the same for all types of actuators When the symbol is used, the type of instrument signal, i e , pneumatic, electric, etc , is drawn as appropriate If the positioner symbol is used and there is no intermediate device on its output, then the positioner output signal need not be shown**

*** **The arrow represents the path from a common to a fail open port It does not correspond necessarily to the direction of fluid flow**

Рис. 10.44

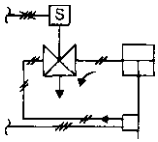
Символы приводов (дополнение)

И

12

PREFERRED ALTERNATIVE A BUBBLE WITH INSTRUMENT TAGGING, E G , TY-1, MAY BE USED INSTEAD OF THE INTERLOCK SYMBOL <£>

13

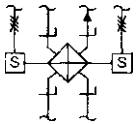


SINGLE-ACTING CYLINDER (IMPLIED L/P)

SOLENOID

CYLINDER WITH POSITIONER AND OVERRIDING PILOT VALVE

14

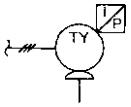


DUAL SOLENOIDS SWITCHING 4-WAY HYDRAULIC VALVE

15

ELECTROHYDRAULLC

16



VALVE ACTUATOR WITH ATTACHED ELECTRO-PNEUMATIC CONVERTER

17

{MANUAL RESET) (REMOTE RESET)
LATCH-TYPE ACTUATOR WITH RESET (SHOWN TYPICALLY FOR SOLENOID ACTUATOR AND TYPICALLY WITH ELECTRIC SIGNAL FOR REMOTE RESET WITH MANUAL RESET ALTERNATIVE)

18

FOR PRESSURE RELIEF OR SAFETY VALVES ONLY DENOTES A SPRING WEIGHT, OR INTEGRAL PILOT

19

T

HAND ACTUATOR OR HANDWHEEL

Рис. 10.48

10.26. Результаты настоящего исследования

По вертикали: ПЕРЕМЕННЫЕ.

При выборе символа переменной удалось встроить новые функциональные коды устройств без нарушения структуры исходной таблицы 10.1 стандарта ISA.

Буква А - *Analyzer.* Вполне согласуется с определением стандарта ISA для характеристик анализа.

Буква В ~ *Burner / Combustion.* Вновь введенные коды предназначены для описания операций пуска и останова печи.

Буква D - *Стандартом ISA не регламентируется (User's Choice).* Может быть использована по усмотрению пользователя для конкретного приложения.

Буква G - *Стандартом ISA не регламентируется (User's Choice).* Может быть использована по усмотрению пользователя для конкретного приложения.

Буква N — *Стандартом ISA не регламентируется (User's Choice).* Может быть использована по усмотрению пользователя для конкретного приложения.

Буква S - *Запорно-регулирующий клапан.* Этот выбор представляется оптимальным.

Буква V - *Вентсистема.* Вновь введенные коды систем вентиляции являются уникальными.

Буква X - *Стандартом ISA не классифицируется (Unclassified).* Может быть использована по усмотрению пользователя. Несмотря на то, что зарубежные разработчики для кодировки отсекателя часто используют букву S, представляется более точным использовать для отсекателя именно данный символ - X, определив S для ЗРК.

Буква Y - *События, Состояние, Присутствие.* Чистый резерв.

Буква Z - *Положение, Размер. JAhtjxq,* кроме как для обозначения арматуры и концевиков, не используется. Что мы и сделали, ограничив область действия задвижками.

По горизонтали: КОДЫ.

Из 19 базовых кодов исходной таблицы 10.2 стандарта ISA в работе остались лишь 9:

- 5 кодов - для кодировки оборудования КИПиА,
- 2 кода - для кодировки параметров ПАЗ,
- 2 кода - для кодировки параметров РСУ.

Л именно, остались нижеследующие (на примере расхода).

Коды оборудования КИПиА.

Входы:	
FE	(10.1)
FT	(10.2)
FS (LL/HH)	(10.3)
Выходы:	
FY	(Ю.4)
FY	(10.5)

Фактически же можно использовать **всего** 3, поскольку, как было замечено, коды FE и FV могут быть упакованы в FT и FY:

FT = FE + FT,

FY = FY + FV.

Но даже эти комплексные коды фигурируют только в перечне входов-выходов, и при маркировке кроссового оборудования, и никак не проявляются на функциональных схемах автоматизации.

Коды ПАЗ.

В структуре исходных таблиц 10.1 и 10.2 стандарта ISA вообще не выделяются. Сохранен код:

FS (LL/HH) (10.6)

Дополнительно введен очень полезный код входной аналоговой блокировки:

FIS (10.7)

Коды РСУ.

(В структуре исходных таблиц 10.1 и 10.2 стандарта ANSI/ISA-S5.1-1984 никак не выделяются).

Естественно, уцелели бессмертные:

FI (10.8)

FIC (10.9)

Введение симметричных кодов ПАЗ - РСУ:

FS (LL/HH) (10.6-1) - **FA** (LL/HH) (10.6-2)

FIS (10.7-1) - **FIA** (10.7-2)

обусловлено необходимостью обеспечить технологический персонал адекватной информацией, объясняющей действия системы противоаварийной защиты, и дающей возможность даже в экстремальной ситуации вести процесс с открытыми глазами.

Еще раз: **ISA не делает подразделения кодов на коды РСУ, и коды ПАЗ.**

Одновременно с сокращением кодов исходной таблицы 10.2 стандарта ISA введено значительное количество новых кодов, позволяющих описать многообразие штатных операций пуска-останова, переключения оборудования, обработки предаварийных ситуаций.

10.27. Общие итоги

1. Рассмотрены существующие системы кодирования параметров автоматизированных систем управления, проведен их сравнительный анализ, и сделана попытка обобщения.
2. Выявлена неполнота и неоднородность системы идентификации по стандарту ISA S5.1-1984. Она заключается в том, что в исходных таблицах (см. таб. 10.1 и 10.2) кодов ISA отсутствует однозначная кодировка параметров для функций (контуров) системы управления и защиты.
3. Отсутствует однозначное определение параметров состояния и управления запорно-регулирующей арматуры и насосов.
4. Соответственно, нет привязки ни к конкретному типу оборудования, ни к технологической переменной, которая должна объединять параметры программно-логической цепочки контура.

В настоящей работе предложена система идентификации, отличающаяся следующими основными особенностями:

1. Определен набор функциональных признаков, дающих возможность однозначно идентифицировать подавляющее большинство параметров информационно - управляющих систем.
2. Введено понятие ШАБЛОНА кодировки (стандартная форма), предохраняющее от использования "незаконных" понятий.
3. В исходные таблицы 10.1 и 10.2 стандарта ISA встроена система кодов для специфических элементов оборудования: насосов, ЗРК, отсекателей, электрозадвижек.
4. Предложенная система кодов оборудования может быть привязана и к конкретному типу оборудования, и к конкретным технологическим переменным. Тем самым, во-первых, появляется возможность выбора, а во-вторых - возможность сохранить единство контура.

   Резко ограничено разнообразие допустимых кодов за счет использования взаимнооднозначного соответствия кодов РСУ и ПАЗ. Отсутствие симметрии может служить признаком возможной ошибки.

Например, при внимательном рассмотрении таблиц **10.31** и **10.32** можно заметить, что в поле **F-13** таблицы **10.31** отсутствует идентификатор **FIA,** в то время как соответствующий ему идентификатор **FIS** в том же поле таблицы **10.32** - есть. Появление несимметричности такого рода должно быть исследовано уже при подготовке первоначального Перечня входов-выходов.

Существенное замечание

Обнаруженная симметрия параметров управления и защиты заставляет задуматься над тем, что, возможно, мы имеем дело с различными сторонами ***одного*** *явления, и очень может быть, что оптимальной по эффективности будет та система, в которой функции управления и защиты реализуются в единой программно-технической среде. Во всяком случае, сегодняшний уровень технических средств позволяет обеспечить любую степень резервирования там, где это действительно необходимо. Примеры подобного рода систем уже имеются.*

Полная система кодов. На основе полученных в данной работе результатов приводится **Полная система кодов АСУТП** - таблица 10.39. В таблице оставлены пустые поля для собственного творчества читателя.

Знание - сила. И слабость тоже. И сила, и слабость стандарта ISA - в его универсальности.

Конкретная форма и состав кодов могут быть теми или иными - современные стандарты предоставляют такую возможность. Но существуют достаточно устойчивые характеристики и связи элементов химико-технологических систем, которые можно и нужно использовать.

Информационно - управляющая модель объекта автоматизации должна обладать совокупностью качеств, отвечающих сущности изучаемых явлений. Система идентификации будет иметь толк, если она основана на знании предмета, и адекватно отражает свойства явлений и понятий, ей подчиненных.

Таблица 10.39

Базовая Таблица идентификации полевого оборудования, параметров РСУ и ПАЗ

№	Первичный элемент	Стандартный элемент - тра		Входное конт общего вида							
	1	2	3	4	5	6	7	8	9	10	11
КОД											
Анализ	AE	AT		AS	AX		ASL	ASH		ASLL	ASHH
Пламя	BE	BT		BS	BX		BSL	BSH		BSLL	BSHH
Проводимость	CE	CT		CS	CX		CSL	CSH		CSLL	CSHH
Плотность	DE	DT		DS	DX		DSL	DSH		DSLL	DSHH
Напряжение	EE	ET		ES	EX		ESL	ESH		ESLL	ESHH
Расход	FE	FT		FS	FX		FSL	FSH		FSLL	FSHH
Положение Перемещение	GE	GT		GS	GX		GSL	GSH		GSLL	GSHH
Ручное управление	HE	HT		HS	HX		HSL	KSH		HSLL	HSHH
Ток	IE	IT		IS	IX		ISL	ISH		ISLL	ISHH
Время	KE	KT		KS	KX		KSL	KSH		KSLL	KSHH
Уровень	LE	LT		LS	LX		LSL	LSH		LSLL	LSHH
Влажность	ME	MT		MS	MX		MSL	MSH		MSLL	MSHH
Энергия, Мощность	NE	NT		NS	NX		NSL	NSH		NSLL	NSHH
Давление	PE	PT		PS	PX		PSL	PSH		PSLL	PSHH
Перепад давления	dPE	dPT		dPS	dPX		dPSL	dPSH		dPSLL	dPSHH
Количество	QE	QT		QS	QX		QSL	QSH		QSLL	QSHH
Радио-активность	RE	RT		RS	RX		RSL	RSH		RSLL	RSHH
Скорость	SE	ST		SS	SX		SSL	SSH		SSLL	SSHH
Температура	TE	TT		TS	TX		TSL	TSH		TSLL	TSHH
Перепад температуры	dTE	dTT		dTS	dTX		dTSL	dTSH		dTSLL	dTSHH
Вязкость	VE	VT		VS	VX		VSL	VSH		VSLL	VSHH
Вес	WE	WT		WS	WX		WSL	WSH		WSLL	WSHH
Вибрация	YE	YT		YS	YX		YSL	YSH		YSLL	YSHH
Позиция, размер	ZE	ZT		ZS	ZX		ZSL	ZSH		ZSLL	ZSHH

Продолжение таблицы 10.39

Базовая Таблица идентификации полевого оборудования, параметров РСУ и ПАЗ	№	13	Запорно-регулирующий клапан ОТКРЫТ	Запорно-регулирующий клапан ЗАКРЫТ						
			14						21	22
Анализ			ASO	ASC	AXO	AXC		AZO	AZC	
Пламя			BSO	BSC	BXO	BXC		BZO	BZC	
Проводимость			CSO	CSC	CXO	CXC		CZO	CZC	
Плотность			DSO	DSC	DXO	DXC		DZO	DZC	
Напряжение			ESO	ESC	EXO	EXC		EZO	EZC	
Расход			FSO	FSC	FXO	FXC		FZO	FZC	
Положение Перемещение			GSO	GSC	GXO	GXC		GZO	GZC	
Ручное управление			HSO	HSC	HXO	HXC		HZO	HZC	
Ток			ISO	ISC	IXO	IXC		IZO	IZC	
Время			KSO	KSC	KXO	KXC		KZO	KZC	
Уровень			LSO	LSC	LXO	LXC		LZO	LZC	
Влажность			MSO	MSC	MXO	MXC		MZO	MZC	
Энергия, Мощность			NSO	NSC	NXO	NXC		N20	NZC	
Давление			PSO	PSC	PXO	PXC		PZO	PZC	
Перепад давления			dPSO	dPSC	dPXO	dPXC		dPZO	dPZC	
Количество			QSO	QSC	QXO			QZO	QZC	
Радио-активность			RSO	RSC	RXO	RXC		RZO	RZC	
Скорость			SSO	SSC	SXO	SXC		SZO	SZC	
Температура			TSO	TSC	TXO	TXC		TZO	TZC	
Перепад температуры			dTSO	dTSC	dTXO	dTXC		dTZO	dTZC	
Вязкость			VSO	VSC	VXO	VXC		VZO	VZC	
Вес			WSO	WSC	WXO	WXC		WZO	WZC	
Вибрация			YSO	YSC	YXO	YXC		YZO	YZC	
Позиция, размер			ZSO	ZSC	ZXO	ZXC		zzo	ZZC	

Продолжение таблицы 10.39

Базовая Таблица идентификации полевого оборудования, параметров РСУ и ПАЗ	№	25	25	27	28	29	30	31	32	33	34	35	36
		Индикатор	Аналоговый вход в систему ПАЗ	Аналоговый сигнал в РСУ из системы ПАЗ	Сумматор	Индицируемый сумматор	Вычислительный блок		Предупредительная сигнализация низкого уровня	Предупредительная сигнализация высокого уровня	Предаварийная сигнализация низкого уровня	Предаварийная сигнализация высокого уровня	
	КОД	I	IS	IA	Q	IQ	FYn		AL	AH	ALL	AHH	
Анализ	A	AI	AIS	AIA	AQ	AIQ	AFYn		AAL	AAH	AALL	AAHH	
Пламя	B	BI	BIS	BIA	BQ	BIQ	BFYn		BAL	BAH	BALL	BAHH	
Проводимость	C	CI	CIS	CIA	CQ	CIQ	CFYn		CAL	CAH	CALL	CAHH	
Плотность	D	DI	DIS	DIA	DQ	DIQ	DFYn		DAL	DAH	DALL	DAHH	
Напряжение	E	EI	EIS	EIA	EQ	EIQ	EFYn		EAL	EAH	EALL	EAHH	
Расход	F	FI	FIS	FIA	FQ	FIQ	FFYn		FAL	FAH	FALL	FAHH	
Положение Перемещение	G	GI	GIS	GIA	GQ	GIQ	GFYn		GAL	GAH	GALL	GAHH	
Ручное управление	H	HI	HIS	HIA	HQ	HIQ	HFYn		HAL	HAH	HALL	HAHH	
Ток	I	II	IIS	IIA	IQ	IIQ	IFYn		IAL	IAH	IALL	IAHH	
Время	K	KI	KIS	KIA	KQ	KIQ	KFYn		KAL	KAH	KALL	KAHH	
Уровень	L	LI	LIS	LIA	LQ	LIQ	LFYn		LAL	LAH	LALL	LAHH	
Влажность	M	MI	MIS	MIA	MQ	MIQ	MFYn		MAL	MAH	MALL	MAHH	
Энергия, Мощность	N	NI	NIS	NIA	NQ	NIQ	NFYn		NAL	NAH	NALL	NAHH	
Давление	P	PI	PIS	PIA	PQ	PIQ	PFYn		PAL	PAH	PALL	PAHH	
Перепад давления	dP	dPI	dPIS	dPIA	dPQ	dPIQ	dPFYn		dPAL	dPAH	dPALL	dPAHH	
Количество	Q	QI	QIS	QIA	QQ	QIQ	QFYn		QAL	QAH	QALL	QAHH	
Радио-активность	R	RI	RIS	RIA	RQ	RIQ	RFYn		RAL	RAH	RALL	RAHH	
Скорость	S	SI	SIS	SIA	SQ	SIQ	SFYn		SAL	SAH	SALL	SAHH	
Температура	T	TI	TIS	TIA	TQ	TIQ	TFYn		TAL	TAH	TALL	TAHH	
Перепад температуры	dT	dTI	dTIS	dTIA	dTQ	dTIQ	dTFYn		dTAL	dTAH	dTALL	dTAHH	
Вязкость	V	VI	VIS	VIA	VQ	VIQ	VFYn		VAL	VAH	VALL	VAHH	
Вес	W	WI	WIS	WIA	WQ	WIQ	WFYn		WAL	WAH	WALL	WAHH	
Вибрация	Y	YI	YIS	YIA	YQ	YIQ	YFYn		YAL	YAH	YALL	YAHH	
Позиция, размер	Z	ZI	ZIS	ZIA	ZQ	ZIQ	ZFYn		ZAL	ZAH	ZALL	ZAHH	

Продолжение таблицы 10.39

Базовая Таблица идентификации полевого оборудования, параметров РСУ и ПАЗ

	№	37	38	39	40	41	42	43	44	45	46	47
	код	Па		>	jt	,'	ГМ»					
Анализ			AC	AIC	AHC		ACS		AY	AAY		
Пламя	%		BC	BIC	BHC		BCS		BY	BAY		
Проводимость	&		CC	CIC	CHC		CCS		CY	CAY		
Плотность	- *, i a		DC	DIC	DHC		DCS		DY	DAY		
Напряжение	$		EC	EIC	EHC		ECS		EY	EAY		
Расход			FC	FIC	FHC		FCS		FY	FAY		
Положение Перемещение	Vто		GC	GIC	GHC		GCS		GY	GAY		
Ручное управление			HC	HIC	HHC		HCS		HY	AAY		
Ток	№		1C	IIC	IHC		ICS		IY	IAY		
Время			KC	KIC	KHC		KCS		KY	KAY		
Уровень			LC	LIC	LHC		LCS		LY	LAY		
Влажность	Щ		MC	MIC	MHC		MCS		MY	MAY		
Энергия, Мощность	№		NC	NIC	NHC		NCS		NY	NAY		
Давление			PC	PIC	PHC		PCS		PY	PAY		
Перепад давления	Щ		dPC	dPIC	dPHC		dPCS		dPY	dPAY		
Количество	й й		QC	QIC	QHC		QCS		QY	QAY		
Радио-активность			RC	RIC	RHC		RCS		RY	RAY		
Скорость	щ		SC	SIC	SHC		SCS		SY	SAY		
Температура			TC	TIC	THC		TCS		TY	TAY		
Перепад температуры	f i		dTC	dTIC	dTHC		dTCS		dTY	dTAY		
Вязкость	T		VC	VIC	VHC		VCS		VY	VAY		
Вес			WC	WIC	WHC		WCS		WY	WAY		
Вибрация	Ш		YC	YIC	YHC		YCS		YY	YAY		
Позиция, размер			ZC	ZIC	ZHC		ZCS		ZY	ZAY		

Окончание таблицы 10.39

Базовая Таблица идентификации полевого оборудования, параметров РСУ и ПАЗ														
	№9	49	50	51	52	53	54	55	56	57	58	59	60
	код												
Анализ		AHY	ACY	ASY1	ASY	AXY	AZY		AHV	ACV	ASV	AXV	AZV
Пламя		BHY	BCY	BSY1	BSY	BXY	BZY		BHV	BCV	BSV	BXV	BZV
Проводимость		CHY	CCY	CSY1	CSY	CXY	CZY		CHV	CCV	CSV	CXV	CZV
Плотность		DHY	DCY	DSY1	DSY	DXY	DZY		DHV	DCV	DSV	DXV	OZV
Напряжение		EHY	ECY	ESY1	ESY	EXY	EZY		EHV	ECV	ESV	EXV	EZV
Расход		FHY	FCY	FSY1	FSY	FXY	FZY		FHV	FCV	FSV	FXV	FZV
Положение Перемещение		GHY	GCY	GSY1	GSY	GXY	GZY		GHV	GCV	GSV	GXV	GZV
Ручное управление		HHY	HCY	HSY1	HSY	HXY	HZY		HHV	HCV	HSV	HXV	HZV
Ток		IHY	ICY	ISY1	ISY	IXY	IZY		IHV	ICV	ISV	IXV	IZV
Время		KHY	KCY	KSY1	KSY	KXY	KZY		KHV	KCV	KSV	KXV	KZV
Уровень		LHY	LCY	LSY1	LSY	LXY	LZY		LHV	LCV	LSV	LXV	LZV
Влажность		MHY	MCY	MSY1	MSY	MXY	MZY		MHV	MCV	MSV	MXV	MZV
Энергия, Мощность		NHY	NCY	NSY1	NSY	NXY	NZY		NHV	NCV	NSV	NXV	NZV
Давление		PHY	PCY	PSY1	PSY	PXY	PZY		PHV	PCV	PSV	PXV	PZV
Перепад давления		dPHY	dPCY	dPSY1	dPSY	dPXY	dPZY		dPHV	dPCV	dPSV	dPXV	dPZV
Количество		QHY	QCY	QSY1	QSY	QXY	QZY		QHV	acv	QSV	QXV	OZV
Радио-активность		RHY	RCY	RSY1	RSY	RXY	RZY		RHV	RCV	RSV	RXV	RZV
Скорость		SHY	SCY	SSY1	SSY	SXY	SZY		SHV	SCV	SSV	SXV	SZV
Температура		THY	TCY	TSY1	TSY	TXY	TZY		THV	TCV	TSV	TXV	TZV
Перепад температуры		dTHY	dTCY	dTSY1	dTSY	dTXY	dTZY		dTHV	dTCV	dTSV	dTXV	dTZV
Вязкость		VHY	VCY	VSY1	VSY	VXY	VZY		VHV	vcv	VSV	VXV	VZV
Вес		WHY	WCY	WSY1	WSY	WXY	WZY		WHV	WCV	WSV	WXV	WZV
Вибрация		YHY	YCY	Y1SY1	YSY	YXY	YZY		YHV	YCV	YSV	YXV	YZV
Позиция, размер		ZHY	ZCY	ZSY1	ZSY	ZXY	ZZY		ZHV	zcv	ZSV	ZXV	ZZV

Глава 11

ПРОЕКТНАЯ ОЦЕНКА НАДЕЖНОСТИ СИСТЕМЫ

11.1. Введение

В отечественной практике основные положения по надежности автоматизированных систем (АС), основным показателям надежности, составу и порядку обеспечения надежности АС определяет ГОСТ 24.701-86 "*Надежность автоматизированных систем управления*В соответствии с ГОСТ 24.701, оценка надежности производится по следующим показателям:

- Надежность реализации функций системы;
- Опасность возникновения в системе аварийных ситуаций.

Описание надежности системы по функциям осуществляют:

- По отдельным составляющим надежности - единичными показателями;
- По нескольким составляющим надежности совместно - по комплексным показателям надежности.

Для описания надежности системы по непрерывно и дискретно выполняемым функциям ГОСТ рекомендует исключительную по полноте группу показателей. Например, для описания безотказности и ремонтопригодности по непрерывным функциям:

- Средняя наработка системы на отказ в выполнении /-той функции (соответствующие показатели стандарта IEC 61508 - *MTTF или MTBF);*
- Вероятность безотказного выполнения системой /-той функции в течение заданного времени *(1 - PFD).*

Допускается использовать следующие показатели:

- Средняя наработка системы до отказа в выполнении /-той функции *(MTTF);*
- Интенсивность отказов системы в выполнении /'-той функции *(PFH).*

В очередной раз необходимо констатировать высший профессионализм создателей советских ГОСТов: ВСЕ показатели ГОСТа 24.701 от 1986 года полностью соответствуют требованиям стандарта Международной электротехнической комиссии IEC 61508 от 2000 года.

Причем за пятнадцать лет до появления стандартов МЭК поставлена задача оценки надежности не просто компонентов оборудования, но ФУНКЦИЙ системы.

Более того, ГОСТ 24.701-86 определяет показатели, которые либо вообще отсутствуют в стандартах МЭК, либо допускают неоднозначное толкование.

Например, используются следующие показатели ремонтопригодности для отдельных функций:

- Среднее время восстановления способности системы к выполнению /-той функции после отказа *(MTTR);*
- Вероятность восстановления в течение заданного времени способности системы к выполнению /-той функции после отказа.

А также комплексные показатели безотказности и ремонтопригодности:

- Коэффициент готовности системы к выполнению /-той функции;
- Коэффициент технического использования системы;
- Коэффициент сохранения эффективности системы.

ГОСТ 24.701-86 определяет показатели надежности системы по аварийным ситуациям как при нормальных условиях функционирования АС, так и при воздействии экстремальных факторов.

Определяются показатели долговечности отдельных подсистем и системы в целом, и т.д. и т. п. В целом по набору показателей надежности наш ГОСТ на порядок превосходит стандарты МЭК. Чего недостает, так это конкретных методик расчета этих показателей, и практических примеров их применения.

Несколько важных определений. В соответствии с ГОСТ 27.002-89 "*Надежность в технике. Основные понятия. Термины и определения",*

Под *Отказом* понимается событие, заключающееся в нарушении работоспособного состояния изделия.

ГОСТ 27.310-95 *"Анализ видов, последствий и критичности отказов"* в дополнение к терминам ГОСТ 27.002-89 вводит следующие термины, относящиеся к *Аначизу видов, последствий и критичности отказов (АВПКО):*

Элемент - составная часть технического объекта, рассматриваемая при проведении анализа как единое целое, не подлежащее дальнейшему разукрупнению.

Система - совокупность элементов, объединенных конструкционно и/или функционально для выполнения некоторых требуемых функций.

Вид отказа - совокупность возможных или наблюдаемых отказов элемента и/или системы, объединенных в некоторую классификационную группу по общности одного или нескольких признаков (причины, механизмы возникновения, внешние проявления и другие признаки).

Тяжесть последствий отказа ~ качественная или количественная оценка вероятного (наблюдаемого) ущерба от отказа элемента и/или системы.

Категория тяжести последствий отказов - классификационная группа отказов по тяжести их последствий. Характеризуется определенным, установленным до проведения анализа сочетанием качественных и/или количественных учитываемых составляющих вероятного отказа или нанесенного отказом ущерба.

Критический отказ - отказ системы или ее элемента, тяжесть последствий которого в пределах данного анализа признана недопустимой и требует принятия специальных мер по снижению вероятности данного отказа и/или возможного ущерба, связанного с его возникновением.

Критичный элемент - элемент системы, отказ которого может быть критическим.

Примечание

В процессе АВПКО конкретного изделия могут быть установлены иные признаки для отнесения элементов к категории критичных, например критичным может быть элемент,

отказ которого, безусловно, ведет к полному отказу системы, независимо от тяжести его последствий.

Критичный технологический процесс - технологический процесс, применяемый при изготовлении и/или монтаже системы или ее элементов, нарушение параметров которого, или вносимые в ходе которого дефекты могут быть причиной критического отказа.

При АВПКО конкретного изделия могут быть установлены иные признаки критичности технологического процесса, например критичным может быть признан техпроцесс, влияние которого на надежность системы или ее элементов неизвестно, или недостаточно изучено.

Показатель критичности отказа - количественная характеристика, учитывающая вероятность отказа за время эксплуатации и тяжесть возможных последствий отказа.

Анализ видов и последствий отказов (АВПО) - формализованная, контролируемая процедура качественного анализа проекта, технологии изготовления, правил эксплуатации и хранения, системы технического обслуживания и ремонта.

Эта процедура заключается в выделении возможных отказов, в прослеживании причинно-следственных связей и возможных последствий этих отказов, а также - в качественной оценке и ранжировании отказов по тяжести их последствий.

Анализ видов, последствий и критичности отказов (АВПКО) - процедура АВПО, дополненная оценками показателей критичности анализируемых отказов.

Технический объект (объект) - любое изделие (элемент, устройство, подсистема, функциональная единица или система), которое можно рассматривать в отдельности.

Из представленных определений следует, что при анализе и расчете характеристик надежности систем управления и защиты главное внимание должно уделяться, прежде всего, критическим элементам системы, отказ которых способен привести к критическому отказу - отказу критических функций защиты.

Важное замечание

Существует отечественный нормативный документ РД 03-418-01 "Методические указания по проведению анализа риска опасных производственных объектовоснованный на анализе деревьев отказов и событий.

11.2. Методики анализа надежности и рисков для автоматизированных систем безопасности

Практически все производители оборудования систем безопасности для нахождения базовых значений интенсивности отказов отдельных компонентов, узлов, модулей используют рекомендации справочника Министерства обороны США Military Handbook, "*Reliability Prediction of Electronic Equipment " M1L-HDBK-217F, 2 December 1991.*

За прошедшие годы это справочное руководство превратилось *de-facto* в стандарт для производителей электронного оборудования всех отраслей промышленности на западе.

MIL-HDBK-217F дает два базовых метода для предсказания надежности:

Первый метод заключается в предсказании характеристик надежности на основе испытаний оборудования в стрессовой ситуации, с корректировкой по сложности устройства, качеству изготовления, конструкции, температуре, перепадам напряжения, и по множеству других эксплуатационных факторов.

Второй метод предсказания надежности применяется на ранних стадиях создания оборудования, когда изучается поведение нового компонента, модуля, устройства. Метод заключается в изучении параметров надежности по каждому компоненту и по каждой категории компонентов (резисторы, конденсаторы, микросхемы и т.д.) с учетом качества, условий внешней среды, технологии изготовления. Комплексный подход к устройству требует детального изучения и анализа, который проводится после разработки и создания электронной схемы устройства (модуля). Таким образом определяются опорные значения характеристик надежности оборудования для систем безопасности. На основе этих данных рассчитываются конкретные параметры надежности конкретных конфигураций оборудования.

Особую ценность этим методикам придает то обстоятельство, что разные производители используют единообразный подход к оценке характеристик надежности оборудования, и пользуются едиными базами данных по интенсивности отказов отдельных компонентов устройств, модулей, разъемов и т.д.

Для оценки интегрального уровня безопасности абсолютное большинство поставщиков и разработчиков систем управления и защиты опирается на Технический отчет безопасного I ехнического допуска dTR84.02 - ISA TR84.0.02 *"Safety Instrumented Systems (SIS) - Safety Integrity Level (SIL) Evaluation Techniques" (Оборудованные под безопасность системы - Техника оценки интегрального уровня безопасности),* разработанный подкомиссией ISA SP84.02.

Технический отчет рекомендует следующие методики анализа рисков для систем безопасности, позволяющие получить ответ на основной вопрос, будет ли система в состоянии выполнить предопределенные функции, когда в этом возникнет необходимость:

- Метод логических блок-диаграмм;
- Анализ дерева отказов;
- Марковский анализ.

Для каждой из перечисленных методик первым шагом является получение исходной информации для расчета - интенеивностей отказа, определенных и заданных изготовителем оборудования, - для каждого элемента, модуля, блока, или комплектной подсистемы.

Для метода логических блок-диаграмм следующим шагом будет объединение (логическое сложение и умножение) вероятностей отказов отдельных компонентов по каждой функции безопасности (управления / защиты).

Однако и этот метод может оказаться не совсем простым, если в составе анализируемой цепочки компонентов оказываемся конкретная конфигурация из нескольких логических устройств, множество разнородных сенсоров и исполнительных устройств, завязанных в единую физическую и логическую I юследовательность.

В случае метода анализа дерева отказов следующим шагом после обретения базовых интенсивностей отказа будет создание диаграммы дерева отказов.

На диаграмме отражается взаимосвязь различных компонентов процесса, вовлеченных в опасное событие. Взаимосвязь компонентов между собой отражается на диаграмме с помощью логических выражений. Далее вычисляется общая вероятность отказа для данного процесса. Анализ дерева отказов идеально подходит для анализа видов, последствий и кри-

тичности отказов (ГОСТ 27.310-95). Поэтому по преимуществу этот метод используется при проектировании новых устройств, а также при проектировании и исследовании алгоритмов управления и защиты. И так же, как и в первом случае, по результатам расчетов производится сравнение полученной сводной вероятности отказа с требуемыми значениями.

Марковский анализ на данном уровне используется редко из-за фантастической сложности систем дифференциальных уравнений, которые возникают для реальных систем управления и защиты, хотя в некоторых случаях может существовать численное решение.

Для справки воспроизводится таблица стандарта IEC 60300-3-1 "*Analysis techniques for dependability: Guide on methodology*в которой приведены ограничения на применение различных методов анализа надежности (см. таблицу 11.1). Надо сказать, что приведенные значения по количеству компонент (колонка *Number of components)* слишком оптимистичны, и вряд ли применимы для реальных систем. В таблице сделаны ссылки на сопутствующие стандарты МЭК:

- IEC 60812 "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)";
- IEC 61025 "Fault tree analysis (FTA)";
- IEC 61078 "Analysis techniques for dependability - Reliability block diagram method";
- IEC 61165 "Application on Markov techniques".

Принятые в таблице 11.1 сокращения и обозначения:

FMEA - Failure Mode and Effects Analysis;
FMECA - Failure Mode, Effects and Critically Analysis;
() - Метод применим с ограничениями или Исключениями;
пс - Метод не способен или не применим;
с - Метод и способен, и применим.

В настоящей главе рассматриваются два варианта реального расчета надежности оборудования АСУТП на примере двух ведущих фирм-производителей средств автоматизации технологических процессов:

1. Yokogawa
2. HIMA.

Обе методики расчета основываются на традиционном анализе логических блок-схем надежности.

Характеристики методов анализа надежности (из Table 2 , IEC 60300-1) *Таблица 11.1*

Analysis method	Characteristics														
	Ability of method to handle model characteristics as								Attributes						
									Approach		Analysis		Analysis effort		
	Number of components	Redundant structure	Irreparable structure	Failure/event combinations and dependencies	Time varying failure/event rates	Complex maintenance strategies	Simulation of functional process	Symbolic representation	deductive	inductive	quantitative	qualitative	qualitative	quantitative	IEC Standard
FMEA	Up to several thousands	(no)	no	(no)	yes	no	no	List	(nc)	c	c	nc	high		60812
FMECA	Up to several thousands	(no)	no	(no)	yes	no	no	List	nc	c	c	(c)	high	low	60812
Fault tree analysis	Up to several thousands	yes	(yes)	(yes)	yes	no	no	Fault tree	c	nc	c	c	high	medium	61025
Reliability block diagram	Up to several thousands	yes	(yes)	(yes)	(yes)	no	no	Reliability block diagram	c	nc	(c)	c	medium	medium	61078
Markov	2 to 100	yes	yes	yes	(no)	yes	(yes)	System state diagram	(nc)	c	c	c	high	medium	61165
Parts count	1 to thousands	(no)	(yes)	no	(no)			List	nc	c	(nc)	c	low	low	
Cause / consequence	Up to several hundreds	yes	yes	(yes)	(yes)	yes	no	Cause / consequence	(c)	c	c	c	high	low / high	
Event simulator	Up to several hundreds	yes	yes	yes	yes	yes	yes	Any	c	c	c	c	high	high	
System reduction	Up to several thousands	yes	no	(yes)	(yes)	(yes)	no	Reliability block diagram	nc	c	(nc)	c	medium	medium	
Event tree	2 to 50	yes	yes	(yes)	yes	no	yes	Event tree	c	c	(nc)	c	low	low	
Truth table	2 to 50	yes	yes	yes				Table	nc	c	c	nc	high		

Вкратце суть обеих методик основывается на следующих предпосылках. Структурная схема для расчета надежности любой из подсистем АСУТП рассматривается как сочетание последовательно и параллельно связанных элементов:

- Последовательное соединение определяет подсистемы или элементы системы, работающие без резерва.
- Параллельное соединение определяет резервированные элементы.

Исходные соотношения для расчета могут быть получены исходя из элементарных результатов теории вероятностей.

Надежность системы, состоящей из п последовательных элементов:

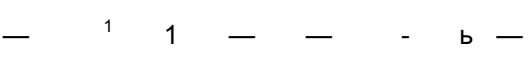


Рис. 11.1

каждый из которых необходим для функционирования системы, и где отказы элементов не зависят друг от друга, равна:

$$Rsenes\ (O = R,(t)\ \ R_2(t) \bullet .. \ \ R_n(t) = \Pi R,(t)$$
$$1=1$$

Допущение *Л - Const* позволяет рассчитать интенсивность отказов линейной системы в целом путем суммирования интенсивностей отказов индивидуальных компонент:

$$^{\wedge}serles \sim \bullet \quad \overset{Я}{\wedge} \sim \bullet \qquad \sim^{\wedge} \qquad Kanes = \underset{I}{Z}\ K$$

Для резервированных (параллельных) систем определение вероятности отказа системы в целом начинается с вычисления вероятности отказа отдельного /-канала *P,(t):*

$$P_l(t) = 1\text{-}R,(t)$$

Рис. 11.2

Очевидно, что для независимых компонентов вероятность отказа системы:

$$P_{pdr_a,e_i(t)} = f\backslash P_i(t) = fl[l-R_i(t)\} \quad .$$
$$i=1 \qquad i=1$$

Тогда вероятность безотказной работы (надежность) параллельной системы:

$$R \wedge (t) = i\text{-}Tl[i\text{-}R,(tj\backslash$$

Для п идентичных элементов

$$P_{pa}r_{a_s}e^{<(t)} = P(t)^n = [l\sim R(t)\}\backslash$$

$$RpsrsHel\,(t) = 1\sim P_{parallel}\,(t) = 1\text{-}[l\sim R(t)f$$

На временном отрезке без отказов и восстановления значения надежности и готовности совпадают: $A(t) = R(t)$.

Представленные соотношения носят самый общий характер. Однако применять их можно по-разному. Поэтому при их конкретной реализации могут возникать серьезные расхождения в оценках. Именно этот аспект и рассматривается в настоящей главе.

Выбор фирм совсем не случаен, поскольку внешняя простота метода логических блок-схем такова, что может проявляться в совершенно разных, можно сказать, диаметрально противоположных ипостасях. Как будет показано, некорректное применение метода приводит к удручающим результатам даже для самого надежного оборудования, каковым, безусловно, является оборудование систем семейства Centum фирмы Yokogawa. **В первом варианте** расчета оценка надежности производится при следующих предпосылках:

- Расчеты на примере оборудования фирмы Yokogawa сделаны в предположении стопроцентного уровня самодиагностики.
- Соответственно, самостоятельная вероятность необнаруженных опасных отказов - отказов несрабатывания - не рассматривается.

Для демонстрации подводных рифов, которые подстерегают разработчика, в расчет сознательно внесены методические ошибки, которые часто допускаются при непродуманном применении данного метода оценки параметров надежности:

- Берется абстрактная сумма всех интенсивностей отказа по всем устройствам. Таким образом, понятие критического отказа не рассматривается - все единичные отказы становятся критическими.

- Кроме того, расчет ограничивается только основным оборудованием системы управления и защиты - надежность полевого оборудования в расчетах не учитывается.

Во втором варианте представлена уже не искусственная, как в первом случае, а фактическая методика расчета параметров надежности, используемая фирмой HIMA:

- Расчеты фирмы HIMA сделаны в полном соответствии с требованиями стандарта IEC 61508.
- Соответственно, учитывается декомпозиция отказов на обнаруженные и необнаруженные, опасные и безопасные отказы.
- Расчету подлежит целостная функция безопасности ~ от сенсора до исполнительного устройства. Более того,
- Учтены доли общих отказов для всех функциональных групп оборудования.

Особенностью расчета являются конфигурации полевого оборудования:

- 2оо3 для датчиков, и
- 1 оо2 для клапанов,

что удается соблюсти далеко не всегда.

И открытой остается проблема общего отказа группы функций (контуров) безопасности.

11.3. Первая методика расчета

Первая из процедур оценки надежности оборудования АСУТП будет проведена^ на примере оборудования системы Centum CS 3000 фирмы Йокогава. Методика расчета соответствует представленным ниже соотношениям. Как всегда, работа начинается с определения терминов и понятий.

Интенсивность отказов *Л* в общем виде определяется как изменение количества отказов в единицу времени на единицу работающего оборудования:

$$№) \qquad N_{op}Jt) \qquad \hat{dt} \; L \qquad \text{где}$$

$N_{oper}(t),N_{fajl}(t)$ - количество работающих, и отказавших единиц оборудования, соответственно.

Среднее время наработки на отказ. Часто интерпретируется и воспринимается как время, определяющее для системы, устройства или компонента системы средний промежуток времени между отказами. К сожалению это не так. Фактически среднее время наработки на отказ определяет характеристический интервал времени, по истечению которого вероятность отказа составляет

$$P(t) = 1\text{-}R(t) = 1\text{-}e\text{-}*^{i} = 1\text{-}e\sim^{1} = 0.63 = 63\%$$

Немного далее этот аспект будет рассмотрен подробнее.

Понятие среднего времени работы до отказа *MTTF* часто смешивается с понятием среднего времени работы между отказами *MTBF,* и каждый из этих показателей в равной степени используется в качестве среднего времени наработки на отказ. Йокогава применяет следующее выражение для определения *MTBF:*

$$MTBF = \frac{}{Я}$$

Среднее время на восстановление. Среднее время на восстановление *MTTR* - среднее время в часах, требуемое на восстановление исходной конфигурации системы после возникновения отказа. В расчетах чаще всего применяют значение *MTTR = 8 часам* (если величина *MTTR* специально не оговаривается производителем оборудования).

Готовность. Динамическая готовность - вероятностная оценка для обслуживаемой системы, устройства или компонента быть работоспособной ("готовой") в определенный момент времени. На практике применяют выражение стационарной готовности.

Замечание

Йокогава в своем руководстве 77 *33Q01K10-01E Reliability Manual, Aug. 2002, определяет готовность через MTBF, определяя к тому же этот показатель не как "Mean time* ***between*** *failures", а как "Mean* ***time to*** *system failure", то есть под кодом MTBF подразумевается MTTF:*

$$\sim \frac{MTBF}{(MTBF + MTTR)}$$

Хотя, строго говоря, стационарная готовность должна определяться не через MTBF, а через MTTF (см. Главы 2 и 4 настоящей работы):

$$A - \frac{MTTF}{\{MTTF + MTTR)}$$

Далее в руководстве *TI 33Q01K10-01E* даются еще несколько нижеследующих определений.

Интенсивность отказов последовательного соединения элементов:

Рис. 11.3

Соответствующая стационарная готовность:

Л, =A_1-A_2 ... = ПА

Интенсивность отказов параллельного соединения двух разнородных элементов:

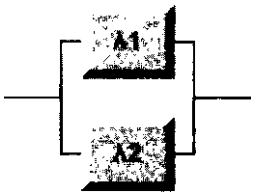


Рис. 11.4

$$Л_{1oo2} = 2 - Л_1 - Л_2 - MTTR$$

Соответствующая стационарная готовность:

$$A_{1OO7}=1-(1-A,)(1-A_2)$$

Для одинаковых параллельных элементов формулы упрощаются:

$$Л_{1OO2} = 2\ Л^2 \bullet MTTR$$

$$A = 1-(1-A)^2 - 2 \bullet A - A^2$$

Замечание

Из представленных соотношений следует, что данная методика исходит из предположения стопроцентного уровня диагностического охвата. Декомпозиция отказов на опасные

и безопасные, обнаруженные и необнаруженные отказы не производится. Соответственно, в отличие от методики МЭК, ог{енка вероятности опасных необнаруженных отказов в данном случае не предусматривается.

Поскольку $MTTF = 1/Л$, то знание одного из этих показателей позволяет легко определить готовность:

$$\sim \frac{MTTF}{MTTF + MTTR} \sim \frac{Л}{Л + p}$$

Для дублированных элементов общий показатель *MTTF* можно найти из выражения

$$Л_{1oo2} = 2 \quad Л^2 \quad MTTR = \frac{}{M}$$

Тогда

$$T002 \sim Л_{1OO2} \sim \frac{MTTF^2}{2 \; Л^2 \; " \; 2 \; MTTR}$$

Очевидно, что *MTTF* резервированных модулей существенно увеличивает среднее время наработки на отказ по сравнению с одиночным модулем.

Как нам уже известно, для подсистем с архитектурой 2oo3 общая интенсивность отказов ровно в три раза больше, чем для архитектуры 1oo2:

$$Л_2OO3 = B \; Л^2 \; MTTR = \frac{}{м}$$

Соответственно, *MTTF* будет ровно в три раза меньше:

$$MTTF \wedge \frac{1}{Л_{2OO3}} = \frac{V}{6 \; Л^2} \quad \frac{MTTp2}{6 \; MTTR}$$

Еще раз необходимо обратить внимание, что как следует из представленных соотношений, здесь предполагается стопроцентный уровень диагностического охвата. Поэтому ключевые характеристики надежности стандарта IEC 61508 - вероятность и интенсивность опасного необнаруженного отказа - в данной методике расчета отсутствуют. Можно напомнить, что для архитектур 1oo2 и 2oo3 эти характеристики определяются, как

$$PFD_{1OO2} = £_{DU} \; Ц- \quad \text{и} \quad PFD_{2003} = \wedge_{DU} \; T^2$$

too2 = 4и Т и $Л_{2003} = з \; A^2_{d1}$ т соответственно.

Замечание

Знание среднего времени наработки на отказ MTTF само по себе не очень плодотворно, поскольку этот показатель не содержит предсказания, когда отказ на самом деле произойдет, и какова вероятность отказа на межтестовом интервале. К тому же важно понимать, что MTTF — это совсем не среднее время жизни устройства, а общий индикатор надежности. Надежность на момент времени t = MTTF составляет

$R(t) = 1 \sim P(t) = e\sim^{м} = e\sim^{t/MTTF} = 0.368.$

А соответствующая вероятность отказа имеет просто угрожающее значение:

P(t) = 1 - R(t) = 63%, а вовсе не ноль, и девять в периоде.

Для межтестового интервала T_1 год более-менее приемлемое значение надежности можно получить лишь для MTTF > 100лет :

$R(MTTF = 100\text{- } TJ = e\text{-}^{001} = 0,99$

Показатель стационарной готовности еще менее информативен. Уже при самых скромных значениях MTTR = 8 часов и MTTF = 1 год (-8000 часов)

$$MTTF + MTTR \qquad MTTF$$

А если MTTF = 100 лет, то есть ~ 8 10^5 часов, то готовность принимает и вовсе фантастическое значение:

A = 1 -0.00001 - 0.99999

причем, как говорится, на ровном месте.

Еще одна возможность для манипуляций - это искусственное сокращение MTTR. Если принять MTTR = 1 час, что вполне реально для современных модульных электронных систем с исключительно высоким уровнем диагностики, то готовность становится просто запредельной:

A- 1 - *0.000001* = 0.999999 /

Единственное, что может дать показатель готовности в практическом смысле - это количественная оценка стоимости простоя и оборудования АСУТП, и технологического процесса. Нужно только использовать не абстрактные и слишком оптимистичные оценки MTTF и MTTR, а скорректировать данный показатель по действительным потерям времени и денег. В расчетах фактической готовности нужно

использовать не абстрактное время восстановления, а фактические потери из-за отказов - и собственно средств автоматизации$_y$ и потери недополученной продукции. См. ГОСТ 24.701, п.2.3.3, "Комплексные показатели безотказности и ремонтопригодности: Коэффициент технического использования системы ".

Поскольку существуют группы параллельно работающих компонентов оборудования, например, модулей ввода-вывода, значительно превосходящих по количеству ординарное дублирование, то соотношений для дублированных и троированных подсистем может оказаться недостаточно. В монографии автора "Основы построения АСУТП взрывоопасных производств" в главе 5 *"IEC 61508 - Вероятность отказа. Альтернативные решения*" было получено общее соотношение для интенсивности отказа резервированных элементов:

$$Л_{Лтооп} = П - (n-1) \cdot \ldots \cdot m - A_{dd} \cdot \frac{T\text{-}T+1 \quad MTTR^{П\ T}}{(n\text{-}m)!} =$$

$$= (П - T + 1) - C^{П}_{П}{\sim}^{T+1} \cdot A^{N}_{D}{\sim}^{M+1}_{D} - MTTR^{П+T}$$

а в главе 4 *"Теоретические основы надежности и безопасности"* - общее соотношение для стационарной готовности:

$$= \sum_{i=0} A^{n}\text{-}'\text{-}(1\text{-}Ay$$

Расчет надежности АСУТП. Переходим к непосредственным расчетам. Согласно исходным предпосылкам, первая методика будет предполагать не более и не менее, чем расчет надежности АСУТП в целом. В самом общем виде интенсивность отказов АСУТП может быть представлена следующим образом:

$$^{ACS} = ^{DCS} + ^{ESD} + ^{PSS}$$

Индексы имеют следующие значения:

ACS	-	АСУТП в целом,
DCS	-	РСУ,
ESD	-	ПАЗ,
PSS	-	Система бесперебойного электропитания *(Power Supply System).*

Соответствующее выражение для готовности (надежности) АСУТП:

$$A_{MCS} \sim A_{DCS} \cdot A_{ESD} \cdot A_{PSS}$$

Дальнейшая последовательность действий сводится к декомпозиции каждой из подсистем, и вычислению характеристик надежности в зависимости от конкретной конфигурации. Детализация заканчивается теми блоками, модулями, компонентами подсистем, для которых известны интенсивности отказов. На представленной ниже схеме показаны типичные устройства базовой конфигурации системы Centum CS 3000.

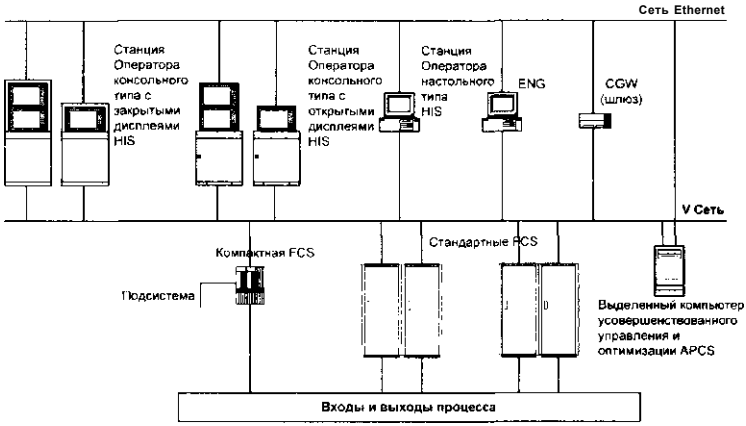


Рис. 11.5

В системе CENTUM базовые подсистемы называются станциями:

- Операторские станции - станции технолога-оператора.
- Полевые станции управления - контроллеры.
- Инженерная станция.

В соответствии с этим подразделением предположим, что РСУ имеет:

- Две операторские станции - HIS,
- Две станции управления - FCS,
- Инженерную станцию - ENG.

Допустим, что каждая из станций управления FCS имеет аппаратное резервирование вплоть до модулей ввода-вывода. Модули аналогового ввода-вывода, связанные с регулированием, также резервированы. Дополнительное оборудование, установленное в промежуточных и кроссовых шкафах не резервировано, за исключением блоков питания =24В.

Далее предположим, что система противоаварийной защиты ESD построена на альтернативном специализированном оборудовании, и имеет архитектуру 2оо3.

Для всего оборудования АСУТП (РСУ, ПАЗ, полевое оборудование) предусмотрим единую систему бесперебойного электропитания - *Power Supply System* - PSS, состоящую из собственно источника бесперебойного питания UPS *(Uninterruptible Power Supply)* и сопутствующего оборудования.

Расчет начнем с наиболее громоздкой системы АСУТП - РСУ. Интенсивность отказов нашей простой, но вполне реальной РСУ для выбранной конфигурации оборудования будет складываться из следующих компонент:

$$Лdcs = 2 \cdot Л^2_{H1\$} \cdot MTTR + Л_{PC51} + A,_{FCS2} + J\text{-}ENG$$

В данном выражении учтен тот факт, что станции оператора полностью дублируют функции контроля и управления, и отказ одной из операторских станций не приводит к отказу в выполнении функций контроля, управления и защиты, поскольку на время восстановления контроль процесса может осуществляться со второй станции. Отказ же любой из станций управления означает потерю функциональности.

Поэтому интенсивность отказов операторских станций входит с выражением для дублированных подсистем, а интенсивности отказов станций управления - линейно. Соответствующая готовность выражается следующим образом:

$$A_{DCS} = A_{FCS1} A_{FCS2} A_{ENG}$$

$$Mh,s^{12} + 2 \cdot >A_{HS} \cdot (1 - A_{HIS})] \cdot >A_{FCS1} \cdot Л_{FCS2} \; A_{ENG} —$$

$$= (2 \cdot A_{HI\$} — A_{HIS}) \cdot A_{FCS1} \cdot A_{FCS2} \; ' A_{ENG}$$

Для стандартной Станции Управления Участком FCS с блоком управления участком FCU, подключенным к узлам через шину RIO, используется:

- Резервирование центрального процессора (CPU),
- Резервирование блока управления участком FCU,
- Резервирование шины RIO, а также
- Опции монтажа в шкаф или в стойку.

Шина дистанционного ввода-вывода RIO связывает FCU с узлами ввода-вывода и также имеет двойное резервирование (см. рис. 11.6).

Архитектура дублированной станции управления FCS с шиной дистанционного ввода-вывода RIO

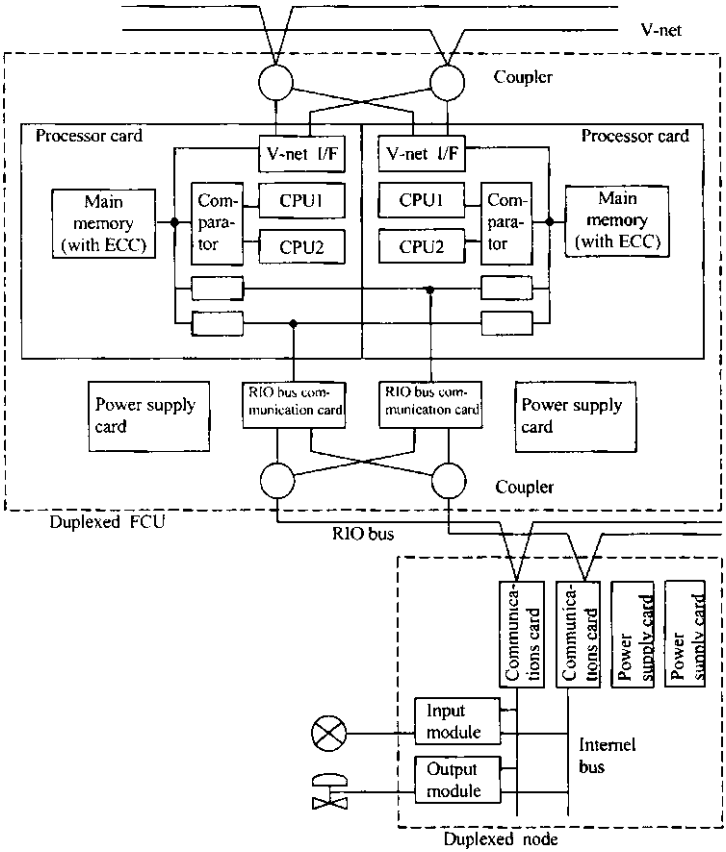


Рис. 11.6

Блок управления участком (узел FCU) для МО. Блок управления участком FCU для **RIO** включает в себя плату центрального процессора, интерфейсные платы и блок питания. Для дуплексного FCU двойное резервирование имеют (см. рис. 11.7):

- Процессорная плата,
- Блок питания,

- Аккумуляторный блок,
- Интерфейсная плата шины RIO.

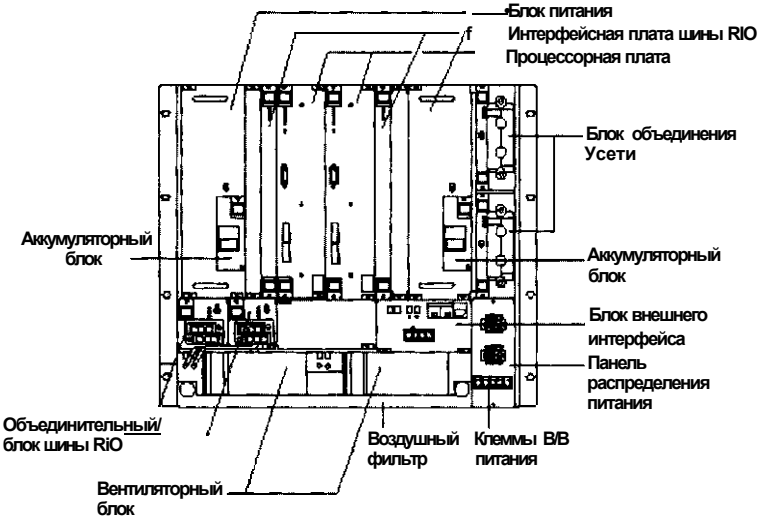


Рис. 11.7

Шина МО (рис. 11.8). Шина дистанционного ввода-вывода (шина RIO) подключает FCU к узлам ввода-вывода, и может иметь двойное резервирование. Узлы ввода-вывода не обязательно должны находиться в шкафу FCU, они могут находиться на удаленном расстоянии. Для расстояний до 750 м используется кабель экранированной витой пары, а на более длинные расстояния до 20 км можно использовать повторители шины или волоконно-оптические линии связи.

Узлы (Nodes). Узлы состоят из блоков ввода-вывода, которые осуществляют интерфейсную связь с аналоговыми и дискретными сигналами от полевых устройств, и интерфейсных блоков узла NIU, которые через шину RIO осуществляют связь с блоками управления участком FCU.

Блоки дублированной корзины для установки модулей ввода-вывода - интерфейсные блоки - **NIU.** Интерфейсные блоки NIU включают в себя коммуникационные платы шины RIO и платы питания, и все они могут иметь двойное резервирование.

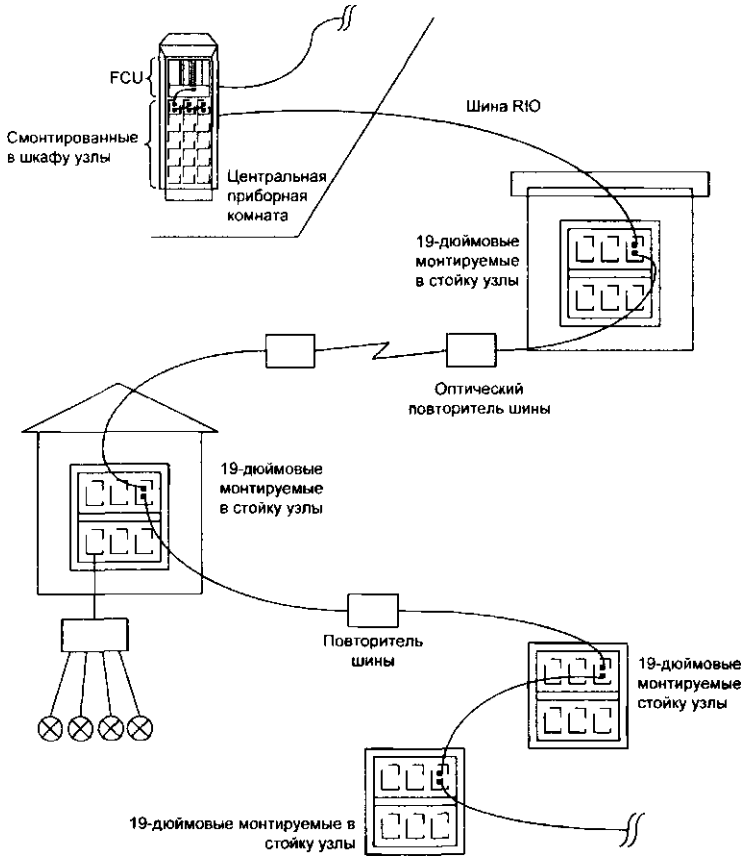


Рис. 11.8

Блоки ввода-вывода (IOU). В состав блоков ввода-вывода входят гнезда для модулей ввода-вывода, включающие модули ввода-вывода, которые через кроссовые соединения подсоединяются к полевому оборудованию технологического процесса.

Архитектура узла FCU с модулями ввода-вывода. Принимается следующая последовательность расчета надежности станции управления:

FCS = FCU + Nodes

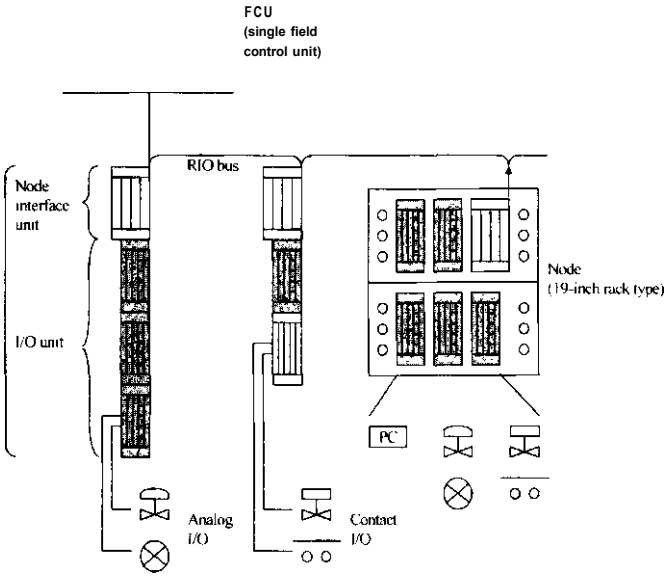


Рис. 11.9

Расчет будет приводиться в соответствии с логической блок-схемой для расчета надежности дублированного контроллера FCU с отображением тех устройств, которые будут резервироваться (см. рис. 11.6). Узлы рассчитываются по следующей схеме:

Node = NIU + I0U(I/0 Modules),

где *NIU* - дублированный интерфейсный узел сопряжения модулей ввода-вывода с контроллером *FCU.*

Пожалуй, самое сложное в проведении подобных расчетов состоит не в громоздких вычислениях, а в нахождении достоверных данных об интенсивностях отказов базовых компонент системы. Далее в таблицах 11.2-11.4 приводятся некоторые из проверенных на практике характеристик, дающих представление об уровне надежности современных средств автоматизации:

- Барьеры искробезопасности
- Реле
- Автоматы питания

- Модули ввода-вывода
- Оборудование UPS.

Во всех расчетах принимается, что среднее время восстановления элемента системы, подсистемы, системы *MTTR = 8 часов.*

Таблица 11.2

Данные о надежности модулей ввода-вывода РСУ

Оборудование		Интенсивность отказов ($10^9$1/час)	MTBF (час)	Готовность
AAI141	Аналоговый входной модуль (4 .20mA, 16-канальный, неизолированный)	3 000	333 333	0.999976
AAI841	Аналоговый модуль ввода-вывода (вход 4. 20mA, выход 4. 20mA, 8 входных каналов / 8 выходных каналов, неизолированные)	3 200	312 500	0.999974
AAP135	Частотный входной модуль (8-анальный, счетчик импульсов, 0 - 10kHz, каналы изолированные)	6 500	153 846	0.999948
ADV161	Дискретный входной модуль (64 канала, 24Vdc, 2 5mA, изолированный)	1 600	625 000	0 999987
ADV169	Дискретный входной модуль (64 канала, изолированный, общий минус на ка>кдые 16 каналов)	2 900	344 828	0 999977
ADV569	Дискретный выходной модуль (64 канала, изолированный, общий минус на каждые 16 каналов)	4 400	227 273	0 999965
ALR121	RS-422/RS-485 Коммуникационный модуль (2 порта, 1200bps-115 2k bps)	2 400	416 667	0 999981

** В интенсивности отказов модулей учтены отказы, связанные с отказами разъемов.*

Таблица 11.3

Данные о надежности дополнительного оборудования

Оборудование		Интенсивность отказов (10^{-9}1/час)	MTBF (час)	Готовность
HID2030	Искробезопасный барьер для AI 4-20 mA, двухканальный	119	8 370 000	0 999999
HID2062	Искробезопасный барьер для T/C{XA), двухканальный	588	1 700 000	0.999997
HID2038Y	Искробезопасный барьер для AO 4-20 mA, двухканальный	147	6 800 000	0 999999
2116 HAT/SAT	Панель объединительная для 16 активных искробезопасных барьеров	500	2 000 000	0 999996
ARS15M-210	Релейная панель дискретных входов (32 канала / внешнее питание 220V AC)	600	1 666 666	0.999997
MRI-214*A	Релейная панель дискретных входов (32 канала / внешнее питание 24V DC)	600	1 666 666	0 999997
UM-16RM	Релейная панель дискретных выходов (32 канала / напряжение 220VAC/5A)	500	2 000 000	0 999996
SF	Автоматы питания	300	3 333 333	0 999997
S8PS-30024C	Источник питания 24V/12A	7 407	135 000	0 999941
G2R	Реле	400	2 500 000	0.999997

Таблица 11. 4

Данные о надежности оборудования бесперебойного питания

Оборудование		Интенсивность отказов ($10^9$1/час)	MTBF (час)	Готовность
ABP	Устройство автоматического выбора резерва	1 ООО	1 ООО ООО	0 999950
UPS	Источник бесперебойного питания	237	4211 412	0 999988
TR	Трансформатор	11 415	87 600	0 999430

Логическая блок-схема дублированного контроллера FCU

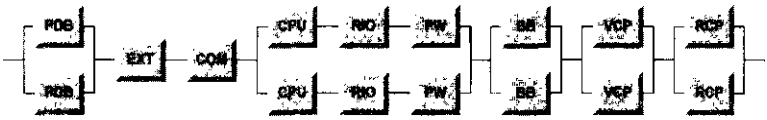


Рис. 11.10

Наименование устройств на рис. 11.10:

PDB - Панель распределения питания
EXT - Внешняя клеммная панель
COM - Общие цепи для дублированных CPU
CPU ~ Карты процессоров
RIO ~ Коммуникационная карта RIO
PW ~ Карты блоков питания
BB - Цепи объединительной панели
VCP ~ Коннектор Vnet
RCP ~ Коннектор RIO-bus.

Интенсивность отказов дублированного контроллера FCU полевой станции управления в целом может быть найдена по выражению:

$$J\text{-}FCU = APOB + Л_{EXT} + Л_{COM} + 2 - (Л_{СРИ} + Л_{НЮ} + Л_{Р1Л,})^2 \cdot MTTR +$$

$$+ 2\text{-}Л^2_{ВВ} \cdot MTTR + 2 \cdot Л^2_{СР} \cdot MTTR + 2 \cdot Л^2_{„СР} \quad MTTR$$

$$A_{FCU} \sim A_{pdb} \cdot A_{EXT} \; ' Acom \; ' (2A_{CPU} - A_{rio} - A_{PW} —$$

$$\sim\sim ACPU \quad ARIO \quad A_{PW})X (2A_{BB} — A_{BB}) \cdot (2A_{VCP} — A_{VCP})$$

где

^FCU	-	Интенсивность отказов FCU
^PDB	-	Интенсивность отказов панели распределения
**EXT		Интенсивность отказов внешней клеммной панели
A-COM	-	Интенсивность отказов общих цепей
^CPU	-	Интенсивность отказов карты процессоров
ARIO	_	Интенсивность отказов коммуникационной
A_{PW}	-	Интенсивность отказов карты блока питания
$Л_{ВВ}$		Интенсивность отказов цепей объединительной панели
KCP	—	Интенсивность отказов коннектора V-net
ARCP	-	Интенсивность отказов коннектора RIO-bus

Интенсивность отказов панели распределения питания PDB считается следующим образом:

$$Яров = 2 \; A^r \; MTTR + 2 \; Я^2_{Рои} \cdot MTTR + 2 \; A^2_{Main} \cdot MTTR ,$$

где

^wesf	~~	Интенсивность отказов панели распределения питания FCU
Лрои	~	Интенсивность отказов блока распределения питания
^Main		Интенсивность отказов панели распределения питания в шкафу

В таблице 11.5 показаны интенсивности отказов каждого компонента FCU, и данные о надежности FCU в целом.

Таблица 11.5

Результаты расчета надежности дублированного FCU

Компонент (Модуль)		Интенсивность отказов (10 ° 1/час)
Панель распределения питания FCU	^Nest	460
Блок распределения литания	ЛPDU	300
Панель распределения питания шкафа	^Main	150
Панель распределения питания	^PDB	150
Внешние панели клемм	ЛEXT	130
Общие цепи для дублированных CPU	ЛCOM	30
Карта процессоров	ACPU	8300
Коммуникационная карта RIO	ARIO	2300
Карта блока питания	APW	2700
Цепи объединительной панели	⊠	1200
Коннектор V-net	Avcp	1400
Коннектор RIO-bus	ARCP	700
Общая интенсивность отказов дублированных FCU	AFCU	300
MTBF дублированных FCU (часы)	MTBF	3.3 Ю^6
Готовность дублированного FCU	A	0 999998

Расчет надежности дублированной корзины для установки модулей ввода-вывода (Node)

На рисунке 11.11 приводится логическая блок-схема для расчета надежности дублированной корзины для установки модулей входов-выходов узла:

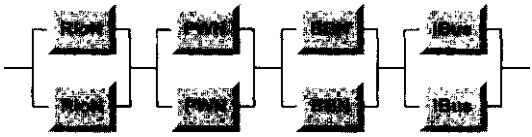


Рис. 11.11

Наименование устройств на рис. 11.11:

RioN	-	Коммуникационная карта шины RIO узла
PWN	-	Блок питания узла
BBN	-	Цепи объединительной монтажной панели узла
IBus	-	Коммуникационная карта внутренней шины

В резервированном варианте все компоненты корзины для установки модулей ввода-вывода дублированы:

$$я^{**}. = 2\text{-}4, o» \; MTTR + 2 - {}^{*2}_{PWN} \; MTTR +$$

$$+ 2 \cdot Я^{2}_{ввы} \cdot MTTR + 2 \cdot A?_{BUS} \; MTTR$$

где

^Node		Интенсивность отказов узла
^RioN		Интенсивность отказов коммуникационной карты узла
		Интенсивность отказов карты блока питания
A-bbn		Интенсивность отказов цепей объединительной панели узла
r/Bus	~	Интенсивность отказов внутренней шины узла

Таблица 11.6

Результаты расчета надежности дублированной корзины для модулей ввода-вывода

Компонент (Модуль)		Интенсивность отказов (10^9 1/час)
Коммуникационная карта RIO	^RioN	1300
Карта блока питания узла	ApWN	1300
Цепи объединительной панели узла	ABBN	300

Внутренняя шина узла	*Л-lBus*	**500**
Интенсивность отказов дублированной корзины	*ANode*	**0 060**
MTBF дублированной корзины (часы)	**MTBF**	**16,700,000,000**
Готовность дублированной корзины	**А**	**0 999999999**

Логическая блок-схема расчета надежности контроллера FCS

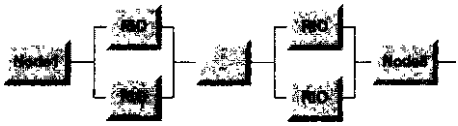


Рис. 11.12

Наименование устройств на рис. 11.12:

SF	-	Автомат питания
FCU	-	Дублированный блок процессоров кон-
RIO	-	Коммуникационная карта шины RIO
Nodel...8	-	Корзины для модулей ввода-вывода.

Интенсивность отказов и готовность полевой станции управления FCS, и подключенных к ней устройств в целом могут быть найдены из соотношений

$$A_{FCS} = A_{sf} + A_{fcu} + n(2-A^2_{ri0} \cdot MTTR) + \pounds A_{Nod\&r}$$

где

Д0,	Интенсивность отказов автомата питания
^lFCU	Интенсивность отказов блока процессоров
	Интенсивность отказов шины RIO
Node,	Интенсивность отказов узла, $1 < i < 8$

$$^FCS — A.SF\ 'Afcu \cdot [n\ (2 - A]^2RIO\ MTTR)] \cdot \prod_{l=1} A_{Node,}$$

$A_я$	Готовность автомата питания
A_{FCU}	Готовность блока процессоров контроллера
	Готовность шины RIO
A_{Node_i}	Готовность узла, $1 < i < 8$

Считается, что вероятность отказа кабеля шины RIO в стойке станции управления практически равна нулю, и в расчетах A_{fcs} не учитывается. Понимая под узлом только оборудование взаимодействия с FCU:

- Коммуникационная карта шины RIO узла,
- Блок питания узла,
- Цепи объединительной монтажной панели узла,
- Коммуникационная карта внутренней шины узла,

то есть без учета модулей ввода-вывода, можно рассчитать характеристики надежности связки FCU + Nodes для возможных конфигураций FCS (таблица 11.7).

Таблица 11.7

No of Nodes	Duplex FCU		Single FCU	
	MTBF	Availability	MTBF	Availability
1	4,937,870	0.999998	60,241	0 999867
2	4,936,096	0 999998	49,751	0.999839
3	4,934,323	0.999998	42,373	0 999811
4	4,932,552	0.999998	36,900	0 999783
5	4,930,781	0.999998	32,680	0 999755
6	4,929,012	0.999998	29,326	0 999727
7	4,927,245	0.999998	26,596	0 999699
8	4,925,478	0.999998	24,331	0 999671

Расчет надежности узла с модулями ввода-вывода

Рис. 11.13

Наименование устройств на рис. 11.13:

Node	-	Корзина для модулей ввода-вывода
AI	-	16-канальные резервированные аналоговые входные модули, *К* штук
DI	-	64-канальные дискретные резервированные входные модули, *L* штук
AO	-	16-канальные резервированные аналоговые выходные модули, Мштук
DO	-	64-канальные дискретные резервированные выходные модули, *N* штук
SF	-	Автомат питания
PS	-	Резервированный блок питания барьеров
RP	-	Релейные панели дискретных выходов
HiP	-	Панели для установки барьеров, I штук
HiD	-	Барьеры аналоговых входов и выходов, *J* штук.

Интенсивность отказов корзины (узла), установленных в ней модулей, и подключенных к ней устройств, в целом может быть найдена из следующего громоздкого соотношения:

$$A\,NODE\,I = KODE + K \cdot (2 \cdot Я, \quad MTTR) + L \quad f2 \cdot A^2_{DI} - MTTR) +$$

$$+ M \,.\, (2 \cdot A^2_0 \quad MTTR) + N - (2 \cdot A^2_{D0} \cdot MTTR) + 2 \cdot A^2_{SF} \cdot MTTR + г$$

$$+ 2 \quad A^2_{PS} \cdot MTTR + A_{RP} + / \cdot A_{HIP} + J \cdot A_{HID}$$

A_M	-	Интенсивность отказов резервированных аналоговых входных 16-канальных модулей, *К* штук
A_{di}	-	Интенсивность отказов 64-канальных резервированных дискретных входных модулей, *L* штук
A_{AO}	-	Интенсивность отказов резервированных аналоговых выходных 16-канальных модулей, Мштук
A_{00}	-	Интенсивность отказов 64-канальных резервированных дискретных выходных модулей, *N* штук
A_{SF}	-	Интенсивность отказов резервированного автомата питания
$Я_{P8}$	-	Интенсивность отказов резервированного блока питания барьеров
A_{RP}	-	Интенсивность отказов релейных панелей дискретных выходов

A_{HiP} - Интенсивность отказов панелей для установки барьеров, / штук

$A_{ню}$ - Интенсивность отказов барьеров аналоговых входов и выходов, *J* штук

Готовность корзины (узла) для установки модулей и подключенных к ней устройств в целом может быть найдена по следующему выражению:

$$A_{ы.,} = >W \quad AA,)^2)* \quad Ao,)^2)^1 \; x$$
$$x(1\sim(1\sim A_{ao})^2)^м \quad .(1-(1-A_{D0})^2)^n X$$
$$A_{SF})^2)- \; (1-(1- \; A_{PS})^2) \; \bullet \; A_{RP} \; \bullet \; A^{\wedge} \; . \; A^J_{HID}$$

где

$A_{A!}$ - Готовность резервированных аналоговых входных 16-канальных модулей, К штук

$A_{0\}}$ - Готовность 64-канальных резервированных дискретных входных модулей, L штук

A_{AO} — Готовность резервированных аналоговых выходных 16-канальных модулей, Мштук

$A_{D}O$ ~ Готовность 64-канальных резервированных дискретных выходных модулей, *N* штук

^SF ~~ Готовность резервированного автомата питания

A_{PS} - Готовность резервированного блока питания барьеров

A_{RP} - Готовность релейных панелей дискретных выходов

A_{HIP} - Готовность панелей для установки барьеров, / штук

$A_{HЮ}$ - Готовность барьеров аналоговых входов и выходов,
./штук

В таблице 11.8 приведены ориентировочные данные надежности комплектного узла (корзины с модулями ввода-вывода), позволяющие оценить порядок значений.

Таблица 11.8

Компонент (Узел)	Значение
Интенсивность отказов узла (1/час) j A_{NODE1}	$4\ 10\sim^{6}$

MTBF для узла (в часах)	*MTBF*	**250000**
Готовность оборудования узла	$Л_{Nodel}$	**0 999968**

Эти расчеты должны быть проведены для всех узлов станции управления FCS. Затем вычисляется надежность станции управления в целом. Этот расчет должен быть произведен для всех станций управления (контроллеров). Приведем ориентировочные значения надежности станций управления:

Таблица 11.9

Оборудование		**Интенсивность отказов** *(1/час)*	**MTBF** *(час)*	**Готовность**
FCS1	**Полевая станция управления FCS1**	$143 \cdot 10^{-6}$	**7000**	**0.998858**
FCS2	**Полевая станция управления FCS2**	$139 \cdot 10^{-6}$	**7200**	**0.998890**

Операторская и инженерная станции

Блок-схема надежности должна включать в себя все ключевые компоненты (модули) станции:

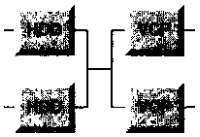


Рис. 11.14

Наименование устройств на рис. 11.14:

COM - Общие цепи станции
PW - Источник питания
CPU - Модуль процессора
MM - Видеокарта
CRT - Монитор
KEY - Клавиатура

HDD - Зеркальный диск

VCP - Коммуникатор шины V-Net.

Общие цепи станции (COM) включают в себя плату распределения питания, шасси, внутреннюю кабельную обвязку, и т.д. Интенсивность отказов операторской или инженерной станции и подключенных к ней устройств в целом может быть найдена по следующему выражению:

$$\text{^HIS ~ ^COM + ^PW + ^CPU + ^MM + ^CRT + ^KEY +}$$
$$+ 2 \cdot A^2_{hdd} \cdot MTTR + 2 \cdot 4_{CP} \cdot MTTR$$

где

AHIS - Интенсивность отказов станции

A-COM - Интенсивность отказов общих цепей

A_{pw} - Интенсивность отказов источника питания

ЛCPU - Интенсивность отказов модуля процессора

J-MM - Интенсивность отказов видеокарты

ЛCRT - Интенсивность отказов монитора

A-KEY - Интенсивность отказов клавиатуры

AHDD - Интенсивность отказов зеркального диска

AVCP - Интенсивность отказов коммуникатора шины V-Net

Соответствующее выражение для готовности:

$$A\mathbf{HIS} — ACOM \ ' APW \ ' A_C\mathbf{PU} \ ' A_{MM} \ ' A_{CRT} \cdot A_{KEY}{}^X$$
$$X \ (2A_{HDD} — A_{HDD}) \cdot (2A_{VCP} — A_{VCP})$$

где

AMIS - Готовность станции

ACOM - Готовность общих цепей

APW - Готовность источника питания

ACPU - Готовность модуля процессора

AMM - Готовность видеокарты

ACRT - Готовность монитора

AKEY - Готовность клавиатуры

AHDD - Готовность зеркального диска

A_VCP - Готовность коммуникатора шины V-net

Расчет надежности РСУ

Интенсивность отказов РСУ в целом может быть найдена из соотношения

$$Adcs \sim 2 \bullet Л^2_{H13} \bullet MTTR + A_{ENG} + A_{FCS1} + A_{FCS\,2}$$

где

ADCS ~ Интенсивность отказов РСУ

A_{HIS} - Интенсивность отказов станции оператора

A_{eng} - Интенсивность отказов станции инженера

AFCSI ~ Интенсивность отказов полевой станции управления FCS1

AFCS2 ~ Интенсивность отказов полевой станции управления FCS2

Готовность РСУ и обеспечивающих её бесперебойную работу устройств в целом может быть найдена из соотношения:

$$Aocs = [1 \sim (1 — Amis)\ 1\ 'A_{ENG}\ \ A_{FCS1} \bullet A_{FC\$2}$$

где

AQCS ~ Готовность РСУ

A HIS — Готовность станции оператора

^ENG _ Готовность станции инженера

^FCS1 — Готовность полевой станции управления FCS1

AFCS2 ~ Готовность полевой станции управления FCS2

Результаты расчета надежности РСУ сведены в таблицу 11Л 0.

Таблица 11.10

Результаты расчета надежности РСУ

Компонент		Значение
Интенсивность отказов РСУ	*1*	*2,86 10⁴*
MTBF для РСУ (в часах)	$MTBF_{DCS}$	**3500**
Готовность оборудования РСУ	A_{DCS}	**0 997720**

Расчет надежности системы ПАЗ

В таблице 11.11 приведены данные о надежности вполне реального контроллера ПАЗ с архитектурой 2oo3, предоставленные фирмой-изготовителем.

Таблица 11.11

Результаты расчета надежности контроллера ПАЗ

Компонент		Значение
Интенсивность отказов контроллера ПАЗ с модулями ввода-вывода	A_{LS}	$7\text{-}10^{-6}$
MTBF контроллера ПАЗ (в часах)	*MTBF*	140000
Готовность контроллера ПАЗ	*ALS*	0 999943

Но посмотрим, каковы будут параметры надежности системы ПАЗ с учетом барьеров, реле, блоков и автоматов питания.

Логическая блок-схема расчета надежности системы ПАЗ с архитектурой 2oo3

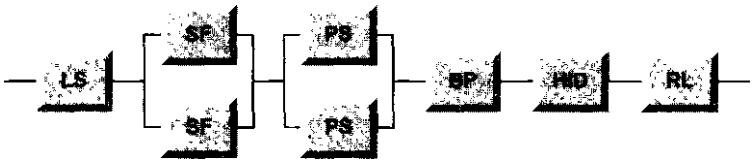


Рис. 11.15

Наименование устройств на рис. 11.15:

LS	-	Контроллер 2oo3 + модули ввода-вывода
SF	-	Автомат питания, 5 пар
PS	-	Блок питания барьеров, 3 пары
BP	-	Панель для установки барьеров, 3 шт.
HiD	-	Барьер аналоговых входов, 16 шт.
RL	-	Реле, 250 шт.

Интенсивность отказов системы ПАЗ и подключенных к ней устройств в целом может быть найдена по выражению:

$$*ESD \quad +5\ (2\text{-}A^2_{SF}\ MTTR) + 3\ (2 \bullet A^2_{PS} \cdot MTTR) + 3\ Я_{вр} +$$
$$+ 16\ \ Л_{ню} + 250\ \ A_{rl}$$

где

$A_E SD$ - Интенсивность отказов системы ПАЗ

Л-s - Интенсивность отказов контроллера

A_{sf} - Интенсивность отказов автомата питания

$Л_{P8}$ - Интенсивность отказов блока питания барьеров

$Л_{BP}$ - Интенсивность отказов панели для установки барьеров

$Я_{ню}$ - Интенсивность отказов барьеров аналоговых

A_{rl} - Интенсивность отказов реле

Готовность системы ПАЗ и подключенных к ней устройств в целом может быть найдена из следующего соотношения:

$$(1\text{-}(1\text{-}A_{SF})^2)^5 \quad (1\text{-}(1\text{-}A_{PS})^2)^3 \quad (A_{вр})^3 \quad (A_{HiD})^{16} \quad (A_{rl})^{25}$$

где

$AESD$ - Готовность системы ПАЗ

A_{LS} - Готовность контроллера

A_{SF} - Готовность автомата питания

A_{PS} - Готовность блока питания барьеров

A_{BP} - Готовность панели для установки барьеров

$A_H IO$ ~ Готовность барьеров аналоговых входов

A_{RL} - Готовность реле

В таблицу 11.12 сведены данные расчета надежности системы ПАЗ целом.

Таблица 11.12

Результаты расчета надежности системы ПАЗ

Компонент (Узел)		Значение
Интенсивность отказов системы ПАЗ	*AESD*	*1,66 10⁴ J*
MTBF для системы ПАЗ (в часах)	*MTBF*	**6000**
Готовность оборудования ПАЗ	*AESD*	0 998666

Расчет надежности системы бесперебойного питания

На рисунке 11.16 приведена логическая блок-схема расчета надежности для цепей бесперебойного питания АСУТП.

Рис. 11.16

Наименование устройств на рис. 11.16:

PSS	-	Система бесперебойного питания (UPS + вспомогательное оборудование)
AVR	-	Блок АВР
UPS	~	Источник бесперебойного питания
TR	-	Трансформатор
SF	-	Автоматический выключатель, 20 шт.

Интенсивность отказов системы бесперебойного питания и обеспечивающих её бесперебойную работу устройств в целом может быть найдена из следующего соотношения:

$$^{PSS} - A\,AVR + A\,UPS + {}^{TR} + 20 \cdot A_{sf}$$

где

^PSS	—	Интенсивность отказов системы бесперебойного питания
^ AVR	-	Интенсивность отказов АВР
AUPS	-	Интенсивность отказов UPS
^TR	-	Интенсивность отказов трансформатора
ASF	—	Интенсивность отказов автоматического выключателя

Готовность цепей бесперебойного питания АСУТП в целом может быть найдена из соотношения:

$$Apss = {}^{avr} \cdot {}^{UPS} \cdot A_{tr} \cdot (A_{SF}) >$$

i де

Apss	~	Готовность системы бесперебойного питания
A_{AVR}	-	Готовность АВР
AUPS	~	Готовность UPS

A_{TR} - Готовность трансформатора

A_{SF} - Готовность автоматического выключателя

Данные расчета надежности цепей бесперебойного питания АСУТП сведены в таблицу 11.13.

Таблица 1L13

Результаты расчета надежности системы бесперебойного питания

Компонент		Значение	
Интенсивность отказов PSS	*Apss*	*22 10~6*	
MTBF для PSS (в часах)	$MTBF_{PSS}$	45000	
Готовность оборудования PSS	A_{PSS}	0.999822	

11.4. Сводные результаты расчета надежности АСУТП

В таблицу 11.14 сведены результаты расчета проектной надежности АСУТП.

Таблица 11A4

Результаты расчетов проектной оценки надежности АСУТП

Оборудование		Интенсивность отказов *(10~6 1/час)*	MTBF (час)	Готовность %
DCS	Система управления РСУ Centum CS3000	*2,86 10~4*	3500	99 77%
ESD	Система ПАЗ	*1,66 10~4*	6000	99 87%
PSS	Система бесперебойного питания	*0,22 Ю-4*	45000	99.98%
АСУ ТП	АСУ ТП в целом	*474-Ю-4*	2099	99 62%

11.5. Авторское заключение по первой методике

Вспомним таблицу оценки интегрального уровня безопасности:

Таблица 11.15

Интегральный уровень безопасности (SIL)

Интегральный уровень безопасности SIL	Допустимая вероятность опасного отказа PFD_{avg}	Требуемая надежность (Стационарная готовность) $(1-PFD_{avg})*100\%$	Интенсивность опасных отказов (1/час) PFH_{avg} (Плуд)	Фактор снижения риска (годы) $RRF = 1 / PFH_{avg}$ $(RRF = 1 / Хвуд)$
1	от 1<Г^{2} ДО 1(Г^{1}	90% - 99%	От Ю$^{-6}$ до Ю$^{-5}$	От 10 до 100 лет
2	от Ю$^{-3}$ До 1СГ^{2}	99% - 99.9%	От Ю$^{-7}$ до 10^	От 100 до 1000 лет
3	от 10^{й} ДОЮ"^{3}	99 9% - 99 99%	От Ю$^{-8}$ до ю-^{7}	От 1000 до 10000 лет
4	Менее КГ^{4}	Более 99 99%	Менее 10"^{8}	Более 10000 лет

Из сопоставления результатов расчета (таблица 11.14) с опорными значениями таблицы 11.15 следует, что максимальный уровень интегральной безопасности, на который может претендовать исследованный комплекс технических средств - это SIL2. Даже надежность вполне реальной системы ПАЗ типа 2оо3 не дотягивает до уровня SIL3. *MTBF* системы ПАЗ, равное 6000 часов (таблица 11.14) означает, что надежность системы в течение *T1 = 1 год* составит

$$R(TJ = e^{-TI/MTBF} = e^{\sim 8760/6000} = 0.23,$$

то есть в течение 1 года отказ системы ПАЗ произойдет с вероятностью 77%. Данный результат не является следствием ненадежности системы ПАЗ. Данный результат является следствием совершенно бездумного применения упрощенной методики расчета.

Достаточно вспомнить дикую формулу расчета готовности для системы ПАЗ:

$$Aeso=A_{ls} \quad (1-(1-A_{sf})^2)^5 \quad (1-(1-A_{PS})^2)^3 \quad X$$

НЮ) (A R L)

Необходимо подчеркнуть, что расчеты проведены на основе вполне реальных данных вполне реальной системы 2оо3 - данных, предоставленных самой фирмой-изготовителем. И это при том, что для контроллера 2оо3 **с модулями ввода-вывода** принято явно излишне оптимистическое значение $Л = 7 \bullet 10^{6} 1/час.$

По РСУ получены еще более удручающие значения, а в целом по АСУТП - и вовсе 2099 часов, или

$R(T_l) = {}_E\sim^{TL/MTBF} - 0.015$, то есть

полуторапроцентная надежность в течение года.

Полученный результат ясно демонстрирует, что даже для самых надежных систем, какой, вне всякого сомнения, является система Centum, прежде чем приниматься за расчеты надежности, надо хорошо понимать смысл и цель расчета.

Самое главное, понимать смысл определения **Функции безопасности, и Вероятности опасного отказа выполнения требуемой функции** как величины, характеризующей вероятность того, что система **не выполнит предопределенную функцию защиты** в момент возникновения необходимости ее выполнения.

По сути *PFD* - это усредненная по времени мера НЕГОТОВНОСТИ системы защиты выполнить критическую функцию безопасности в самый нужный момент.

Для системы безопасности **по каждой функции безопасности** эта вероятность определяется как сумма

$$PFD_{AVG} = z\,p\,f\,d_{s\,e} + I\,P\,P\,D_{1s} + 1\,PFD_{FE}$$

где

PFD_{MG} - Средняя вероятность отказа выполнения требуемой функции защиты;

$I\,P\,F\,D_{s\,e}$ - Средняя вероятность отказа выполнения требуемой функции связной группы сенсоров ("датчиков") и входного интерфейса (входных модулей);

$£\,P\,F\,D_{1s}$ - Средняя вероятность отказа выполнения требуемой функции со стороны логического устройства или нескольких устройств;

$Z\,P\,F\,D_{F£}$ - Средняя вероятность отказа выполнения требуемой

функции выходного интерфейса (выходных каналов) и группы конечных (исполнительных) элементов.

Далее по каждой функции может быть определена и так называемая готовность. **Вероятностное определение стационарной готовности** *(Safety Availability)* выражается как $(1\text{-}PFD_{AVG})100\%$.

Считать общую интенсивность, или общую вероятность отказа АСУТП в совокупности по всем элементам системы без разбору - совершенный абсурд.

Подобный подход приводит к тому, что отказ любого из датчиков становится равносильным отказу АСУТП в целом.

Показатели надежности АСУТП зависят от множества обстоятельств:

- Состояния самого технологического процесса,
- Состояния полевого оборудования,
- Состояния системы защиты и ее компонентов,
- Интервала межповерочного тестирования,
- Состояния, квалификации и ответственности персонала,
- И от того, насколько часто возникает потребность в выполнении функций защиты.

Все сказанное еще раз подтверждает тезис, который неоднократно звучал, и еще будет звучать на всем протяжении настоящей работы:

Сведения из рекламных проспектов производителей и поставщиков оборудования систем управления и защиты без учета конкретной конфигурации оборудования и конкретных условий применения практического значения не имеют.

Именно так стандарты IEC 61508 и IEC 61511 предписывают относиться к априорным оценкам вероятности отказа и интегрального уровня безопасности.

11.6. Методика фирмы HIMA

Уже Стандарт ANSI / ISA S84.01-96 определял Систему безопасности SIS как "*Систему, состоящую из сенсоров, логических решающих устройств, и конечных (исполнительных) цементов, предназначенную для перевода процесса в безопасное состояние при возникновении нарушений предопределенных условий* ".

С появлением стандарта IEC 61508 производители оборудования переходят на расчеты в терминах интегральной безопасности. Основное внимание в этих расчетах уделяется самым опасным видам отказов - оценкам вероятности опасных необнаруженных отказов.

Главным объектом расчета выступает функция безопасности - законченная самостоятельная группа элементов, осуществляющая самостоятельную, "относительно" независимую группу операций управления и защиты. Относительность независимости определяется влиянием общих отказов на подсистему, или на всю систему безопасности в целом.

Стандарт IEC 61511 определяет Систему безопасности SIS как "*Систему, оснащенную соответствующим полевым оборудованием, используемую для выполнения одной или нескольких функций защиты. Система безопасности состоит из сенсоров, логических решающих устройств, и конечных (исполнительных) элементов".*

Будем считать по определению, что Система безопасности состоит из:

- Сенсоров,
- Логических устройств,
- Исполнительных элементов,
- И, вообще говоря, *контингента* (в стандартах МЭК не фигурирует),

и предназначена для:

- Автоматического перевода технологического процесса в безопасное состояние при возникновении нарушений предопределенных условий;
- Разрешения на продолжение нормальной работы технологического процесса при отсутствии нарушения предопределенных условий;
- Осуществления действий, направленных на предотвращение технологических нарушений.

Практическое применение методик стандарта IEC 61508 будет представлено фирмой HIMA - одной из ведущих мировых фирм-производителей высококлассного оборудования для систем противоаварийной защиты. Надо отдать должное профессиональной смелости специалистов фирмы HIMA, которые первыми представили в открытой печати результаты расчетов для своих систем защиты по новой методике IEC.

твии со стандартом IEC 61508 расчеты
ля основного оборудования защиты -
его контура безопасности - от датчика
еханизма. Расчеты HIMA проводятся
ных начальных условий:
) интеовап между процедурами авто-
вания. Надо ли объяснять, что увели-
это интервала с одного года до десяти
ятикратному увеличению базовой ин-
а по всем компонентам системы,
их отказов.
10, специалисты HIMA в своих рас-
ке при полном резервировании всех
2НОСТИ от трубы до трубы сводный
езопасности вовсе не обязательно
энному SIL3. В расчетах исполь-
щины и понятия (табл. 11.16).

Таблица 11.16

jiiure rate (per hour)
s failure rate (per hour)
-ate (per hour)
e common-cause failure
ommon-cause failure
ck
actor. Is the proportion of the dangerous ed to all dangerous failures
^{3}rogrammab!e Electronic Systems
rol
зrance

PFD	Probability of Failure on Demand (A function is requested up to a maximum of twice per year)
PFH	Probability of Failure per Hour (A function is requested more than two times per year)
SFF	Safe Failure Fraction Part of safe failures and dangerous detectable failures related to ail failures
SIL	Safety Integrity Level. Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

Современный подход к оценке надежности систем безопасности радикальным образом отличается от методики ISA. Принципиальная разница состоит не в том, что вместо логических блок-схем используется некий иной инструмент - логические блок-схемы также используются. Принципиальная разница состоит в тонком анализе интенсивности и вероятности отказа с декомпозицией отказов на:

- На опасные и безопасные,
- На обнаруженные, и необнаруженные:

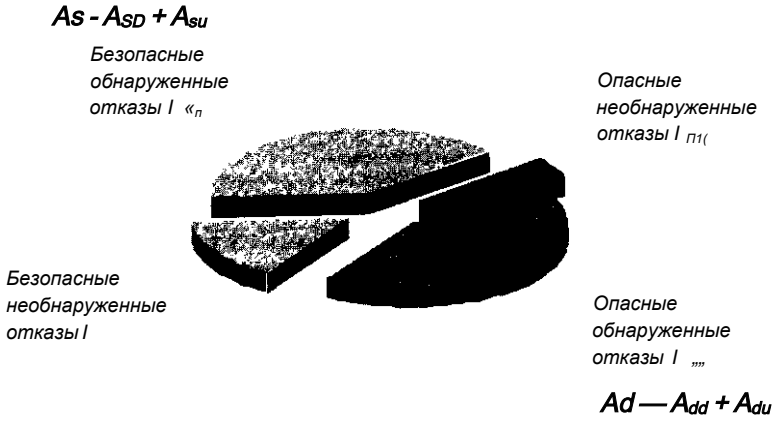


Рис. 11.17

Причем основное внимание уделяется оценке вероятности **опасных необнаруженных отказов.**

Следующее принципиальное отличие - это расчет не только средней интенсивности отказов, но и вероятности от-

каза в течение межтестового интервала - интервала ме&ду процедурами автономного тестирования. При этом вводится еще один важный настроечный фактор - уровень диагностического охвата.

И, наконец - сделана серьезная попытка учесть влияние общих отказов. И для них также вводится подразделение на долю обнаруженных и необнаруженных общих отказов.

Претензии, высказанные ранее к стандарту IEC 61508, сводятся к следующим обстоятельствам:

- Недовведенное до конца исследование поведения различных архитектур в зависимости от уровня диагностики. Таковое исследование возможно только при исключении влияния общих отказов. При этом можно показать, что соотношения IEC вносят ошибку при высоких уровнях самодиагностики.
- Второе, еще более важное обстоятельство — это отсутствие оценок для вероятности ложного срабатывания.

Эти претензии ни в коей мере не умаляют попытки создателей стандарта найти универсальные методы для оценки надежности современных систем безопасности технологических процессов.

Программный пакет *SILence.* Образцом воплощения рекомендаций МЭК является пакет *SILence* фирмы HIMA. В 2003 году этот программный продукт получил сертификат TUV на право проведения расчетов надежности систем безопасности в полном соответствии с требованиями стандарта IEC 61508.

Детальное описание пакета приводится в фирменном Руководстве HI 800 131 BEA "*SILence Manual2004.* Есть и открытые публикации с результатами практических расчетов. Например, Отчет *"Safety considerations*" одного из создателей пакета доктора *J. Borcsok, HIMA Paul Hildebrandt GmbH + Co KG, 2002*, а также описание системы защиты морских трубопроводов "*Critical Aspects of Safety, Availability and Communication in the control of a sub sea pipeline, Requirements and Solutions". 2000.*

Программное обеспечение *SILence* позволяет определить интегральный уровень безопасности SIL для каждого проектируемого контура - от сенсора до исполнительного устройства.

Ф *SILence* является первым инструментальным продуктом, который получил благословение TUV на вычисление SIL в соответствии со стандартом IEC 61508. *SILence* позволяет сделать проектную оценку SIL по каждому новому контуру безопасности, документировать и сохранять результаты в архиве, и использовать эти данные для расчета сводного уровня безопасности системы в целом. В основе расчета находятся базовые соотношения вероятности и интенсивности отказов по методике IEC 61508-6 (Приложение В1 стандарта).

Архитектура 1oo1. Средняя вероятность опасного отказа - 01каза выполнить требуемую функцию защиты:

$PFD_G = Я_0 \cdot t_{c£} = (Л_{ou} + A_{dd}) \cdot t_{CE}$, где

$t_{CE} = ^ - ^ + MTTRy^-MTTR$

Средняя интенсивность отказов в час:

$PFH_a = A_{DU}$

Архитектура 1oo2, loo2D (!).

$PFD_C = 2\text{-}[(1 - p_D)\ A_{dd} + (1 - P)\text{-}A_{du}]^2 \cdot t_{CE} \cdot t_{GE} +$

$+ p_D \cdot kn \cdot MTTR + p \cdot Я_{o\ u} + MTTR\mathbf{j}$

$*_{CE} = \frac{'f}{Л_{,,}} + MTTR\backslash + \frac{}{Л_0} \cdot MTTR$

$tos \sim (y + MTTRj + ^ \cdot MTTR$

$PFHe = 2\ [(1-/1_d)\ A_{dd} + (1-P)\ A_{du}]^2\ t_{CE} +$

$+ PD \cdot A_{od} + p \cdot A_{du}$

Архитектура 2oo3.

$PFD_g = 6\text{-}[(i\text{-}fi_D y z_m + (i\text{-}fi)\text{-}Z_{ou} y\text{-}t_{CE}\ t_{SE} +$

$+ P_D \cdot Л_т \cdot MTTR + P\text{-}A_{du}\ MTTR\mathbf{j}$

$t_{CE} = \frac{f}{A_d} + MTTR) + \frac{}{Л_0} \cdot MTTR$

$t_{GE} = \frac{^l.(L_-+MTTR)}{Л_0} + \frac{^--MTTR}{A_d}$

$PFH_C = 6[(1\text{-}P_D)\ A_{dd} + (1\text{-}P)A_{du}]^2 \cdot t_{CE} + Po\text{-}A_{dd+}P\text{-}\ A_{du}$

Замечательно, что HIMA оставляет без внимания вычурные соотношения IEC 61508 для расчета вероятностных характеристик архитектуры loo2D: все расчеты проводятся по единым соотношениям для архитектуры 1oo2. Более того, нигде даже вскользь не упоминается мифическая архитектура QMR "2oo4". Получить подтверждение своей позиции из первых рук дорогого стоит: "Я же говорил, скрипач не нужен". Надо ли говорить, что данная глава написана последней из всех глав настоящей работы - примерно через год после фактического завершения книги. Но знакомство с последними разработками фирмы HIMA заставило дополнить работу современным образцом не умозрительных, а реальных, и очень убедительных расчетов.

Первая из представленных в данной главе методик предусматривает оценку вероятности только **обнаруженных опасных отказов,** и восстановление в течение *MTTR.* Оценка вероятности **опасного необнаруженного отказа** на межповерочном интервале T_1 не производится. Кроме того, в отличие от первой методики расчета по упрощенным соотношениям (без учета отказов общего порядка и доли диагностического охвата), в пакете *SILence* использованы непосредственно соотношения стандарта IEC 61508. Оценка фирмы HIMA выгодно отличается еще и тем, что расчеты проведены не для наиболее выигрышного годового или даже полугодового межповерочного интервала, как это делают многие фирмы, а для наиболее жесткого 10-летнего интервала.

И самое главное, расчеты проведены для всего контура безопасности - от датчика до исполнительного устройства. Большинство производителей, если и предоставляет данные по вероятностям отказа, то только для основного оборудования РСУ и ПАЗ - без учета поля.

Для расчета средних вероятностей отказа по каждой подсистеме необходимо определить следующие данные:

- Базовую архитектуру,
- Базовую интенсивность отказов для каждого канала,
- Фактор диагностического охвата DC для каждого канала,
- Доли опасных и безопасных отказов общего порядка (общей причины) /? и $/3_D$.

Для всех подсистем должны быть приняты идентичные условия расчета. HIMA проводит свои расчеты при следующих параметрах:

Таблица 11.17

Parameter	Description	Values
P	Dangerous undetectable common-cause failure	2%
Po	Dangerous detectable common-cause failure	1 %
T1	Proof-test interval	10 years
MTTR	Mean Time To Repair	8 hours

В качестве ключевых компонент контура безопасности рассматриваются:

- Дискретные и аналоговые датчики
- Входные дискретные и аналоговые модули
- Коммуникационные модули
- Модули центрального процессора
- Выходные дискретные и аналоговые модули
- Исполнительные устройства (приводы).

11.7. Краткое описание возможностей пакета *SILence*

Пользователь имеет возможность создавать, сохранять и загружать проекты. Проект состоит, по крайней мере, из одной системы (контура), который состоит из единичных систем:

- Сенсор;
- Логическое устройство;
- Исполнительное устройство (Привод).

Программное обеспечение пакета позволяет определить категорию *SIL*, а также *MTTF, PFD, PFH* и SSF для отдельных компонентов системы (модулей) и системы в целом. Каждый проект может содержать до 20 систем. Если требуется большее количество, то системы разбиваются на несколько проектов. Далее представлена процедура создания проекта *SILence* - от собственно самого проекта и до функционального компонента.

11.8. Структура проекта в *SILence*

Проект. В *SILence* проект состоит из конфигурируемых систем:

System 01

l i S I M System 20

Рис. 11.18

Системы. Системы состоят из единичных систем:

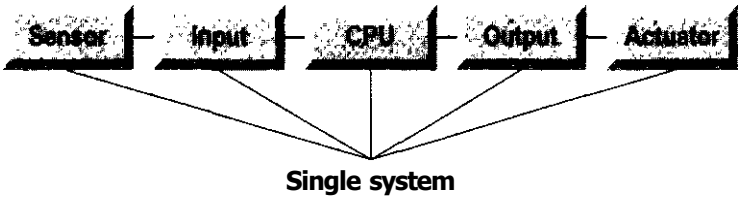


Рис. 11.19

Единичные системы. Для каждой из единичных систем определяется архитектура, состоящая из одного или нескольких модулей:

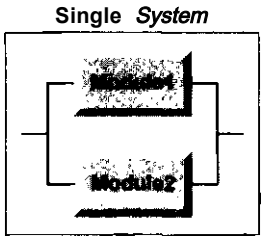


Рис. 11.20

Модули. Пользователь может выбрать предопределенные модули из библиотеки, или сконфигурировать собственные модули:

Рис. 11.21

Компоненты. Модуль состоит из компонентов, таких, как CPU, сторожевой таймер, блок питания и т.д. На рис. 11.22 представлен модуль, состоящий из трех компонент.

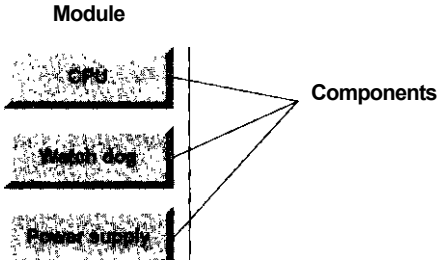


Рис. 11.22

Устройства. Компонент имеет собственную архитектуру (1oo1, 1oo2, 2oo2, 2oo3), состоящую из индивидуальных элементов - устройств. Эти устройства описываются в параметрах интенсивностей отказа: $Л_{00}$,$Л_{Ш}$,$Л_{З}$. На рис. 11.23 представлен компонент, состоящий из двух элементов.

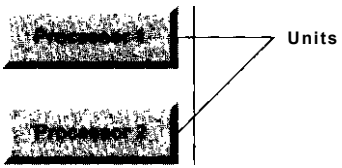


Рис. 11.23

Таблица 11.18

Конфигурационные параметры модуля

Module Parameter	Description
Name	Name of the selected module (max 15 characters)
Description	Description of the module
Type	Type A / B
Module SIL (1 to 4)	Certified SIL (according to the module manufacturer's specifications)
Property	Module type (e g Sensor, Input, CPU, Output, Actuator)
Subtype (0 to 9999)	Only modules of the same subtype may be interconnected Redundantly
MTTR (Default 8 h)	Mean Time To Repair
MTTF	Mean Time To Failure
P	Weighting factor for dangerous undetectable common-cause failures of the module
Po	Weighting factor for dangerous detectable common-cause failures of the module

Согласно IEC 61508, для модулей сторонних производителей, аттестованных на применение в системах безопасности, перечисленные параметры должны присутствовать в технической документации, и предоставляться производителями оборудования.

Следует обратить внимание, что в качестве среднего времени наработки на отказ выбрана правильная характеристика - MTTF, а не MTBF.

В отечественной практике часто происходит смешение при переводе этих терминов. Недоразумения возникают еще и по той причине, что интенсивность отказов в равной степени определяется и через MTBF, и через MTTF.

Параметры конфигурации компонентов модуля. Модуль состоит из компонентов модуля, для которых определены соответствующие значения *Л & /З.* Все компоненты модуля (CPU, шина ввода-вывода, стабилизатор питания и т.д.) воспроизводятся на экране и могут быть отредактированы.

Таблица 11.19

Component Parameters	Description
Name	Name of the selected component
Architecture	Select the component architecture in the drop-down list (1oo1, 1oo2, 2oo2, 2oo3)
p	Weighting factor for dangerous undetectable common-cause failures of the module
Po	Weighting factor for dangerous detectable common-cause failures of the module

Примечание

Для модулей сторонних производителей, аттестованных на применение в системах безопасности, перечисленные параметры должны присутствовать в технической документации, и предоставляться производителями оборудования. Не надо упускать из виду, что /3 - факторы компонента могут отличаться от /3 - факторов модуля.

Конфигурирование параметров устройства. В зависимости от архитектуры (1oo1, 1oo2, 2oo2, 2oo3), компонент может состоять из четырех устройств. Для каждого компонента задаются следующие параметры:

Таблица 11.20

Unit Parameters	Description
Description	Name of the unit
K	Safe failure rate (per hour)
Ku	Undetected dangerous failure rate (per hour)
Add	Detected dangerous failure rate (per hour)

Все параметры устройства воспроизводятся на экране, и могут быть отредактированы.

Замечание

Модули третьих производителей могут быть сконфигурированы по своему усмотрению. Естественно, ответственность за результат возлагается в таком случае на разработчика, производившего расчет.

Модули HIMA и аттестованные модули с известными характеристиками стороннего производителя предопределены, и их характеристики изменить нельзя.

Таблица 11.21

Примеры единичных систем

Single System	Description
Input	Input module
Output	Output Module
Input and Output	Input / Output Module
Input —>CPU -^Output	H! Matrix Compact System
CPU	CPU Module
Connector	Coupling Module
Transmitter	Current, Voltage Transmitter
Sensor	Pressure, Temperature, Gas Sensor
Actuator	Valve, Pump, Motor
Power supply unit	Power Supply Unit
Booster	Booster

11,9. Конфигурирование систем в *SILence*

Функции безопасности (контуры) конфигурируются как системы. Система должна быть сконфигурирована для каждого контура в контроллере. Один проект может состоять не более чем из 20 систем.

Если требуется более чем 20 систем, они распределяются по другим проектам. Оборудование систем HIMA H41q/H51q предустановлено в библиотеках пакета. Модули единичных систем могут выбираться из контекстного меню.

Таким образом, единичные системы, добавленные к предопределенным системам HIMA, могут быть переконфигурированы.

Конфигурация контура *SILence* представлена на рис. 11.24. Слева от системы H51q-HRS - единичная система "Сенсор" с архитектурой 1oo2.

Справа от системы H51q-HRS - единичная система "Привод", также с архитектурой 1oo2.

Пример предопределенной системы H51q-HRS

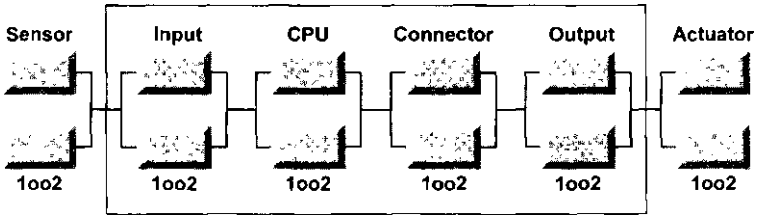


Рис. 11.24

Таблица 11.22

Единичные системы и модули для создания контура

Single System	Architecture	Module	Module Description
Sensor	1oo2	Pressure Sensor	Standard Pressure Sensor
Input	1oo2	F 3238	8-channel Input Module, safety related
CPU	1oo2	c occnc F 8650E	Central Module, safety related
Connector	1oo2	F 7553	Connector module
Output	1oo2	f ooon ****	8-channel Output Module, safety related
Actuator	1 oo2	Valve	Standard Valve

Результаты расчета контура системы H51q-HRS для низкого и высокого уровня требований приведены в Таблицах 11.23 и 11.24.

Таблица 11.23

Результаты расчета для низкого уровня требований

Lo*Demand~Result [Proof «Test Interval - 1 0 Years]						
System / System Parts	Archi-tecture	PFH	SIL	SFF %	MTTF years	PFD in % for overall result
Pressure Sensor	1oo2	9,24 E-5	4	94,58	76,61	71,60
F 3238	1oo2	4,63 E-7	4	99,92	52,30	0,36
F 8650E	1oo2	3,078 E-6	4	99,77	27,40	2,38
F 7553	1oo2	2,17 E-7	4	99,95	102,00	0,17
F 3330	1oo2	5,81 E-7	4	99,77	69,89	0,45
Valve	1oo2	3,23 E-5	4	94,76	206,06	25,04
System without Sensors and Actuators		4,34 E-6	4	99,83	12,54	100,00
System with Sensor and Actuator		1,29 E-4	3	98,46	10,24	100,00
TUV claimed SIL for Systems without Sensor and Actuator			3			

Таблица 11.24

Результаты расчета для высокого уровня требований

Lo-Demand-Resuft [Proof -Test Interval« 10 Years]						
System / System Parts	Archi-tecture	PFH	SIL	SFF %	MTTF years	PFD in % for overall result
Pressure Sensor	1oo2	1,98 E-8	3	94,58	76,61	50,57
F 3238	1oo2	1,55 E-9	4	99,92	52,30	3,95
F 8650E	1oo2	7,26 E-9	4	99,77	27,40	18,47
F 7553	1oo2	2,28 E-9	4	99,95	102,00	5,81
F 3330	1oo2	1,23 E-9	4	99,77	69,89	3,13
Valve	1oo2	7,08 E-9	4	94,76	206,05	18,07
System without Sensors and Actuators		1,23 E-8	3	99,83	12,54	100,00
System with Sensor and Actuator		3,92 E-8	3	98,46	10,24	100,00
TUV claimed SIL for Systems without Sensor and Actuator			3			

После нахождения PFD системе присваивается категория SIL3. После нахождения PFH системе также присваивается категория SIL3.

Определение *SIL* **по отказоустойчивости** *HFT (Hardware Failure Tolerance)* **и по доле безопасных отказов** *SFF (Safe Failure Fraction).* **Отказоустойчивость** оборудования характеризуется количеством отказов, которое может пережить система без потери функциональности. Например, для одноканальной системы 1oo1 значение *HFT* составляет

N=1-1=0.

Для резервированных систем 1oo2 и 2oo3

N=2-1=1

N = 3 — 2 = 1 соответственно.

Таблица 11.25

Результаты расчета SIL для контура системы H51q-HRS на базе *HFT* и *SFF*

SIL based on HFT (N) and SFF (TGv Approved)					
System / System Parts	**Architecture**	**Type A/B**	**SIL**	**SFF %**	**MTTF years**
Pressure Sensor	**1oo2**	**B**	**2**	**94,58**	**76,61**
F 3238	**1oo2**	**B**	**3**	**99,92**	**52,30**
F 8650E	**1oo2**	**B**	**3**	**99,77**	**27,40**
F 7553	**1oo2**	**B**	**3**	**99,95**	**102,00**
F 3330	**1oo2**	**B**	**3**	**99,77**	**69,89**
Valve	**1oo2**	**B**	**2**	**94,76**	**206,06**
System without Sensors and Actuators			**3**	**99,83**	**12,54**
System with Sensor and Actuator			**2**	**98,46**	**10,24**
TUV claimed SIL for Systems without Sensor and Actuator			**2**		

Таким образом, окончательно контур классифицируется по категории SIL2.

В следующем разделе представлены результаты расчетов для различных конфигураций функций (контуров) безопасности. Базовые расчетные характеристики надежности для основных элементов контура представлены в таблице 11.26.

Таблица 1L26

Module	Pressur* sensor	Temp sensor	DI F 3236	DI F 3238	AI- F 8214	Ai F6217	V-BG F7S53	CPU F 8650E	DO F 3330	DO. F 3334	AO F 8705	Actuator valve
iambdab m(1/h]			7 43E 07	1 09E 06	1 11E 06	1 11E 06	5 60E 07	2 08E 06	817E-07	6 21E-Q7	9 45E 07	
MTTF m {years]			153,66	104 60	102 80	103 17	203 99	54 79	139 78	183 91	120 79	
Proof-check interval T, wi [years]	10	10	10	10	10	10	10	10	10	10	10	10
MTTR	8	8	8	8	8	8	8	8	8	8	8	8
Po	0 01	0 01	0 01	0 01	0 01	0 01	0 01	0 01	0 01	0 01	0 01	0 01
P	002	0,02	0 02	0 02	0 02	0 02	0 02	0 02	0 02	0 02	0 02	0.02
PFO,».,m[1]			9 796 06	2 38E 05	5 12E-05	2 87E-05	978E-06	2 94E-05	8 18E-06	1 40E-05	1 see 05	
PFH,.* m[1/h]			2 05E-10	5 14E 10	1 11E-09	9 64E 10	5 76E-10	4 08E 09	6 58E-10	6 87E 10	617E 10	
PFDwj.»* men*'	1 00E-04	1 56E04										3 33E-05
PFHipэjnoo3 m ft/hi	2 22E-08	3 47E-08										7 40£ 09
TUV clamed SIL			3	3	3	3	3	3	3	3	3	

11.10. Расчет вероятностей опасного отказа контуров защиты

Для расчета средних вероятностей отказа по каждой части системы необходимо определить следующие данные:

- Базовую архитектуру каждой из подсистем и системы в целом;
- Базовую интенсивность отказов для каждого элемента системы;
- Базовую интенсивность отказов для каждого канала системы;
- Фактор диагностического охвата DC для каждого канала / контура безопасности;
- Доли опасных и безопасных отказов общего порядка, общей причины /3 и /}$_0$.

Предыдущая методика предусматривает оценку только вероятности опасных **обнаруженных отказов,** и восстановление в течение *MTTR.* Оценка вероятности **опасного необнаруженного отказа** на межтестовом интервале Т, отсутствует.

Оценка фирмы HIMA выгодно отличается еще и тем, что расчеты проведены не для выигрышного годового или даже полугодового межтестового интервала, как это делают многие

фирмы, а для наиболее жесткого 10-летнего интервала. Расчеты проведены для всего контура безопасности - от датчика до исполнительного устройства.

Характерной особенностью расчетов H1MA являются конфигурации датчиков и исполнительных устройств:

- Все датчики имеют архитектуру 2oo3;
- Все исполнительные устройства имеют архитектуру 1oo2.

Здесь необходимо заметить, что если для исполнительных устройств дублирование хотя бы на уровне соленоидов является обычной практикой, то архитектура 2oo3 для датчиков даже на западе применяется только в самых ответственных случаях. Примером могут служить протяженные газопроводы, проложенные по морскому дну.

Необходимо обратить внимание, что в руководстве HI 800 131 BE A "*SILence Manual2004,* и в отчете "*Safety considerations", HIMA Paul Hildebrandt GmbH + Co KG,2003,* представлены расчеты вероятности опасных отказов **только для единичных контуров.** Если в единой логической цепи находится более-менее приличная группа сенсоров и исполнительных устройств, то результат будет вовсе не таким радужным.

И, наконец, общий пробел всех методик, основанных на методике IEC - отсутствие расчетов для вероятности ложного срабатывания.

В качестве ключевых компонент контура безопасности рассматриваются:

- Дискретные и аналоговые датчики
- Входные дискретные и аналоговые модули
- Коммуникационные модули
- Модули центрального процессора
- Выходные дискретные и аналоговые модули
- Исполнительные устройства (приводы).

Далее приводятся результаты расчета вероятностей опасного отказа контуров в различных конфигурациях. В расчетах использованы следующие опорные значения:

Po = 1%

P =2%

T_1 *= 10 лет*

MTTR = 8 часов.

Подсистема 1: Дискретный вход, Дискретный выход.

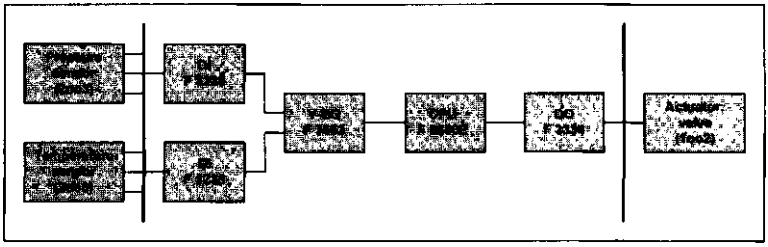


Рис. 11.25

Таблица 11.27

	*шштя^*		^pj Ё^.		tBsfc 4 *ш* . 1
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47 E-08**	**3**	**3**
Dl: F 3238	**1oo2**	**4.63E-07**	**1.55E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo1**	**2.94E-05**	**4.08E-09**	**3**	**3**
DO: F 3334	**1oo1**	**1.40E-05**	**6.87E-10**	**4**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**5.36E-05**	**6.90E-09**	**4**	**4**
System with sensor and actuator		**3.43E-04**	**7.12E-08**	**3**	3
TOVcfatmetf m forsya* ^ tem$ without ЛиявЬ^""""			%		**lfe**

Подсистема 2: Дискретный вход, Дискретный выход.

А#с. 11.26

Таблица 11.28

4					
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
DI: F 3238	**1oo2**	**4.63E-07**	**1.55E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo2**	**3.08E-06**	**7.24E-09**	**4**	**3**
DO: F 3334	**1oo1**	**1.40E-05**	**6.87E-10**	**4**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**2.73E-05**	**1.01E-08**	**4**	**3**
System with sensor and actuator		**3.17E-04**	**7.43E-08**	**3**	**3**

Подсистема 3: Дискретный вход, Дискретный выход.

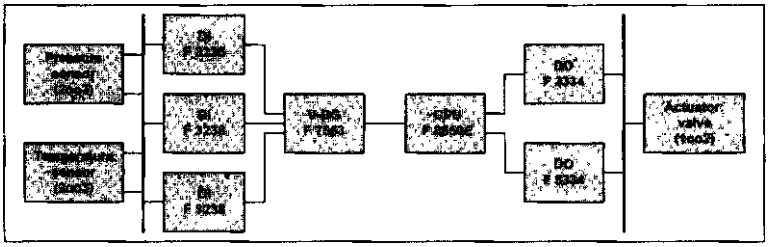


Рис. 11.27

Таблица 11.29

Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
DI: F 3238	**2oo3**	**4.65E-07**	**1.57E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo1**	**2.94E-05**	**4.08E-09**	**3**	**3**
DO: F 3334	**1oo2**	**6.09E-07**	**1.29E-09**	**4**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**4.03E-05**	**7.52E-09**	**4**	**4**
System with sensor and actuator		**3.30E-04**	**7.18E-08**	**3**	**3**

Подсистема 4: Дискретный вход, Дискретный выход.

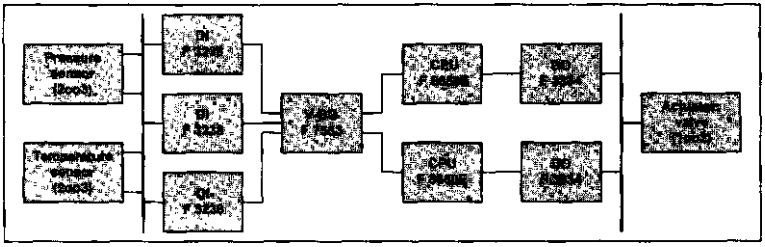


Рис. 11.28

Таблица 11.30

Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
DI: F 3238	**2oo3**	**4.65E-07**	**1.57E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo2**	**3.08E-06**	**7.24E-09**	**4**	**3**
DO: F 3334	**1oo2**	**6.09E-07**	**1.29E-09**	**4**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**1.39E-05**	**1.07E-08**	**4**	**3**
System with sensor and actuator		**3.03E-04**	**7.50E-08**	**3**	**3**
actuator					

Подсистема 5: Аналоговый вход, Дискретный выход.

'Щт:':

"Ш&г **i p** 2

Рис. 11.29

Таблица 11.31

3 f: та: Щ> W 1 3 to^S^ У			щШШЩЩЩшр 1 уу;щящ	Щ :	
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
AI: F 6214	**1oo2**	**1.00E-06**	**3.44E-09**	**4**	**3**
Connector: F 7553	**1 oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo1**	**2.94E-05**	**4.08E-09**	**3**	**3**
DO: F 3334	**1 oo1**	**1.40E-05**	**6.87E-10**	**4**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**5.42E-05**	**8.78E-09**	**4**	**4**
System with sensor and actuator		**3.43E-04**	**7.31 E-08**	**3**	**3**
IK	Й Щ р 'ШЩш ш а	^ t 9 y hЧ'М3**У*: к %	И Ч ^ Ш Щ &ШРЛ		

Подсистема 6: Аналоговый вход, Дискретный выход.

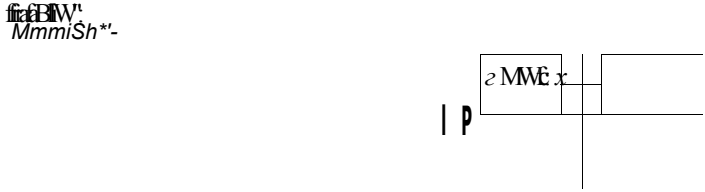


Рис. 11.30

Таблица 11.3

4					%
Pressure switch	2oo3	1.00E-04	2.22E-08	3	3
Temperature switch	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	1oo2	1.00E-06	3.44E-09	4	3
Connector: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo1	1.40E-05	6.87E-10	4	4
Actuator: Valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor and actuator		2.79E-05	1.19E-08	4	3
System with sensor and actuator		3.17E-04	7.62E-08	3	3

Подсистема 7: Аналоговый вход, Дискретный выход.

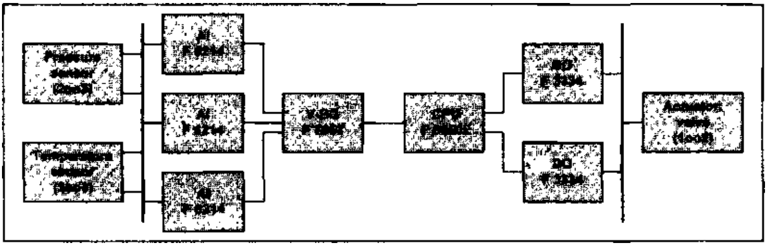


Рис. 1131

Таблица 11.33

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Pressure switch	2oo3	1.00E-04	2.22E-08	3	3
Temperature switch	2oo3	1.56E-04	3.47E-08	3	3
AI: F6214	2oo3	1.01E-06	3.50E-09	4	3
Connector: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: Valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor and actuator		4.08E-05	9.45E-09	4	4
System with sensor and actuator		3.30E-04	7.37E-08	3	3
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Подсистема 8: Аналоговый вход, Дискретный выход.

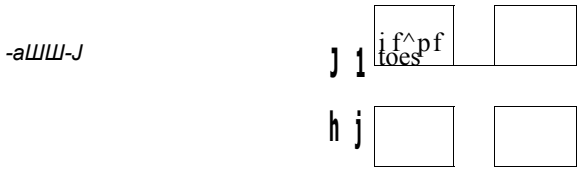


Рис. 11.32

Таблица 11.34

	toc-		<JMt		m B L 1
Pressure switch	2oo3	1.00E-04	2.22 E-08	3	3
Temperature switch	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	2oo3	1.01E-06	3.50E-09	4	3
Connector: F 7553	1 oo1	9.78E-06	5.76E-10	4	
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: Valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor and actuator		1.45E-05	1.26E-08	4	3
System with sensor and actuator		3.04E-04	7.69E-08	3	3
					да

Подсистема 9: Аналоговый вход, Аналоговый выход.

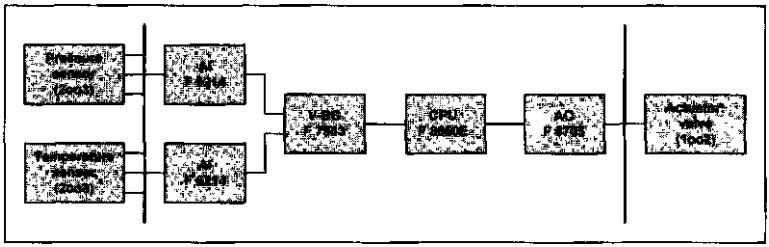


Рис. 11.33

Таблица 11.35

тМШаШжл					
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
AI: F6214	**1oo2**	**1.00E-06**	**3.44E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo1**	**2.94E-05**	**4.08E-09**	**3**	**3**
AO: F 6705	**1oo1**	**1.86E-05**	**6.17E-10**	**3**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**5.88E-05**	**8.71 E-09**	**4**	**4**
System with sensor and actuator		**3.48E-04**	**7.30E-08**	**3**	**3**

Подсистема 10: Аналоговый вход, Аналоговый выход.

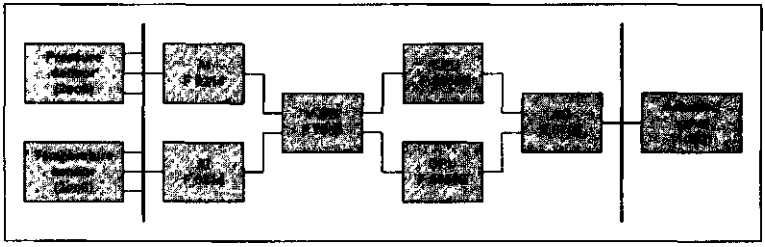


Рис. 11.34

Таблица 11.36

ш ш т ^ящшММшшщ &			*tm*		
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
AI: F 6214	**1oo2**	**1.00E-06**	**3.44E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78 E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo2**	**3.08E-06**	**7.24E-09**	**4**	**3**
AO: F 6705	**1oo1**	**1.86E-05**	**6.17E-10**	**3**	**4**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
	i	**s**	**i**	**i**	**i i**
System without sensor and actuator		**3.25E-05**	**1.19E-08**	**4**	**3**
System with sensor and actuator		**3.22E-04**	**7.62E-08**	**3**	**3**
tern* w£thrai* *щттттШ*			£ ^		

Подсистема 11: Аналоговый вход, Аналоговый выход.

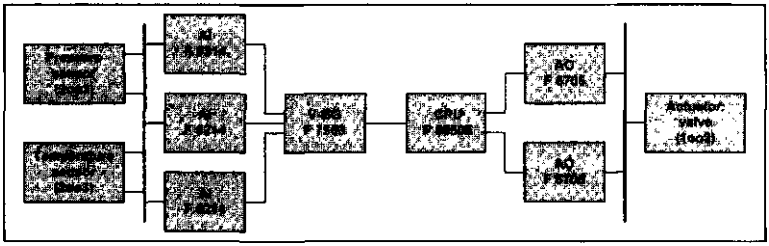


Рис. 11.35

Таблица 11.37

^ в		*n o m*	I	% ^	Л Ш ; iic ;
Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
Ai: F 6214	**2oo3**	**1.01 E-06**	**3.50E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F 8650E	**1oo1**	**2.94E-05**	**4.08E-09**	**3**	**3**
AO: F 6705	**1oo2**	**3.78E-07**	**2.26E-09**	**4**	**3**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**4.06E-05**	**1.04E-08**	**4**	**3**
System with sensor and actuator		**3.30E-04**	**7.47E-08**	**3**	**3**

Подсистема 12: Аналоговый вход, Аналоговый выход.

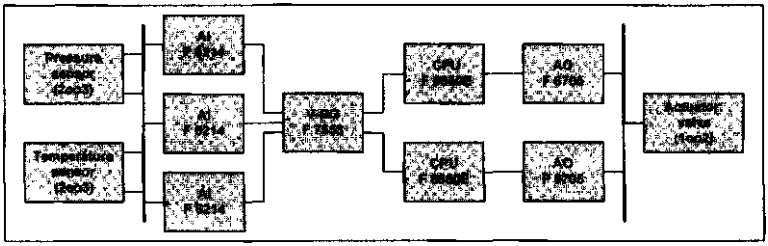


Рис. 11.36

Таблица 11.38

Pressure switch	**2oo3**	**1.00E-04**	**2.22E-08**	**3**	**3**
Temperature switch	**2oo3**	**1.56E-04**	**3.47E-08**	**3**	**3**
AI: F 6214	**2oo3**	**1.01E-06**	**3.50E-09**	**4**	**3**
Connector: F 7553	**1oo1**	**9.78E-06**	**5.76E-10**	**4**	**4**
CPU: F8650E	**1oo2**	**3.08E-06**	**7.24E-09**	**4**	**3**
AO: F 6705	**1oo2**	**3.78E-07**	**2.26E-09**	**4**	**3**
Actuator: Valve	**1oo2**	**3.33E-05**	**7.40E-09**	**4**	**3**
System without sensor and actuator		**1.43E-05**	**1.36E-08**	**4**	**3**
System with sensor and actuator		**3.04E-04**	**7.79E-08**	**3**	**3**

11.11. Оценка SIL по доле безопасных отказов (SFF) и по отказоустойчивости

В контексте интегральной безопасности уровень SIL, который может быть объявлен и для отдельной функции безопасности, и для системы безопасности в целом, ограничивается отказоустойчивостью и долей безопасных отказов подсистемы, осуществляющей данную функцию безопасности.

Таблицы 2 и 3 IEC 61508-2, стр. 47, определяют предельный SIL, который может быть приписан для функции безопасности подсистемы исходя из доли безопасных отказов и отказоустойчивости подсистемы. Соответствие этим требованиям должно проверяться для каждой подсистемы.

Определение 1

Отказоустойчивость оборудования - N - означает, что N+1 сбой приводит к потере функции безопасности. При определении отказоустойчивости оборудования не должно предприниматься никаких дополнительных действий, которые могут оказать воздействие на результаты отказов, например, таких, как диагностика.

Таким образом, отказоустойчивость подсистемы определяется максимальным числом случайных отказов оборудования (random hardware failures), которое не приводит к опасному отказу системы безопасности в целом. При этом считается, что даже если одиночный сбой (fault) является причиной одного или нескольких последующих сбоев, сбой считается одиночным.

Определение 2

Подсистема - это сенсор, логическое устройство, или исполнительное устройство. Комплектная система безопасности состоит из набора идентифицируемых и самостоятельных подсистем, которые в совокупности воплощают функцию безопасности системы.

Требования к отказоустойчивости могут быть ослаблены для систем с резервированием, допускающих оперативную замену *on-line.* Однако и в этом случае вероятности отказа должны быть просчитаны с учетом необходимого времени на восстановление *MTTR.*

Определение типов подсистем по IEC 61508-2:

Согласно IEC 61508-2, пункт 7.4.3.1.2,

Подсистема относится к типу А, если для всех компонентов, участвующих в осуществлении функции безопасности:

- Режимы отказов всех компонентов подсистемы хорошо определены;
- Поведение подсистемы при возникновении отказа полностью детерминировано;
- Имеются достаточные экспериментальные данные о поведении подсистемы, дающие уверенность, что обеспечивается необходимая мера обнаруженных и необнаруженных отказов.

Согласно IEC 61508-2, пункт 7.4.3.1.3,

Подсистема относится к типу В, если для всех компонентов, участвующих в осуществлении функции безопасности:

- Режимы отказов хотя бы для одного из компонентов подсистемы не определены полностью;
- Поведение подсистемы при возникновении отказа не полностью детерминировано;
- Нет достаточных экспериментальных данных о поведении подсистемы, дающих уверенность, что обеспечивается необходимая мера обнаруженных и необнаруженных отказов.

Из этих определений следует, что если хотя бы один из компонентов подсистемы относится к типу В, то и вся подсистема будет типа В.

Таблица 11.39

Ограничения по SIL для подсистем типа А

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
>99%	SIL3	SIL4	SIL4

Таблица 11.40

Ограничения по SIL для подсистем типа B

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed 1	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	S1L3	SIL4
> 99 %	SIL3	SIL4	SIL4

11Л2. SIL единичного канала

(Пример 1 из стандарта IEC 61508-2, Пункт 7.4.3.1.5)

Общее правило: Если функция безопасности исполняется посредством единичного канала, то максимальное значение интегрального уровня безопасности SIL для оборудования всей системы по отношению к данной функции определяется подсистемой с самым низким уровнем SIL, определенным по таблицам 11.39 и 11.40. Предположим, что одноканальная функция защиты состоит из подсистем 1, 2 и 3. Архитектура этой системы приведена на рис. 11.37.

Пример определения интегрального уровня безопасности для одноканальной функции

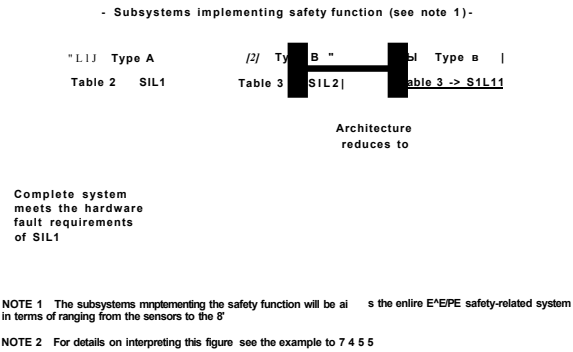


Рис. *11.20*

Пусть каждая из подсистем обеспечивает следующие требования безопасности, определенные по таблицам 11.39 и 11.40:

- Подсистема 1 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL1, тип А.
- Подсистема 2 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL2, тип В.
- Подсистема 3 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL1, тип В.

Несмотря на то, что SIL подсистемы 2 равен двум, общий уровень безопасности для этой архитектуры будет лимитирован SIL подсистем 1 и 3, и в целом для всей системы (контура) равен единице. Более того, контур относится к самому низкому типу - типу В, то есть к типу с неопределенным и недетерминированным поведением, и вполне соответствует контуру с характеристиками человеческих существ.

11.13. SIL многоканальной функции безопасности

(Пример 2 из стандарта IEC 61508-2, Пункт 7.4.3.1.6)

Для систем, реализующих функции безопасности посредством многоканальных подсистем, общий уровень безопасности определяется с помощью следующих шагов:

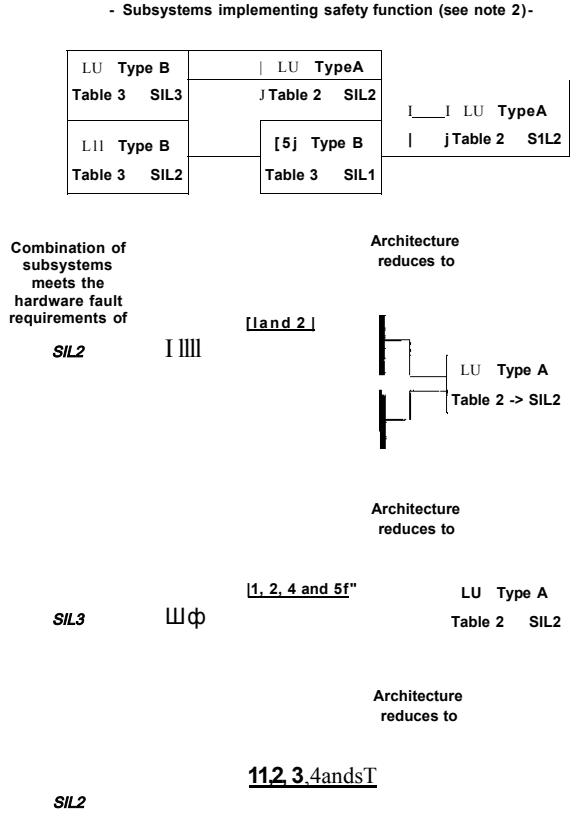
- Выбор по таблицам 11.39 и 11.40 для каждой из подсистем уровня SIL, соответствующего уровню диагностики и отказоустойчивости подсистемы;
- Группировка подсистем и назначение соответствующего уровня SIL для группы;
- Анализ и определение общего SIL для оборудования системы.

Предположим, что функция безопасности обеспечивается пятью подсистемами по двум путям (см. рис. 11.38):

- Последовательность подсистем 1, 2 и 3, или
- Последовательность подсистем 4, 5 и 3.

В этом случае комбинации подсистем (1+2), и (4+5) имеют одинаковую функциональность, и обеспечивают самостоятельный выход на подсистему 3.

Пример определения интегрального уровня безопасности для многоканальной функции



NOTE 1 Subsystems 1 and 2 and subsystems 4 and 5 have the same functionality as regards implementing the safety function, and provide separate inputs into subsystem 3

NOTE 2 The subsystems implementing the safety function will be across the entire E/E/PE safety-related system in terms of ranging from the sensors to the actuators

NOTE 3 For details on interpreting this figure, see the example to 7 4 5 6

Рис. 11.38

Функция безопасности будет исполняться следующим образом:

- В случае отказа подсистемы 1 или 2 - подсистемами 4 и 5.
- В случае отказа подсистемы 4 или 5 - подсистемами 1 и 2.

Предположим, что каждая из подсистем обеспечивает следующие требования безопасности, определенные по таблицам 11.39 и 11.40:

- Подсистема 1 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL3, тип В.
- Подсистема 2 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL2, тип А.
- Подсистема 3 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности SIL2, тип А.
- Подсистема 4 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности S1L2, тип В.
- Подсистема 5 при конкретном уровне диагностики и отказоустойчивости способна обеспечить интегральный уровень безопасности S1L1, тип В.

Этот пример совсем не так прост, как может показаться:

- Как следует из Примера 1, комбинация подсистем 1 и 2 имеет максимально разрешенный SIL=2.
- Комбинация подсистем 4 и 5 имеет максимально разрешенный SIL-1.

Однако в случае отказа комбинации (1+2) функция безопасности будет обеспечена комбинацией (4+5). Поэтому отказоустойчивость комбинации (1+2) автоматически повышается на 1. Следовательно,

- Общий SIL для комбинации подсистем 1, 2, 4, 5 имеет максимальный уровень интегральной безопасности SIL3.

Найдем общий SIL для системы в целом:

- Общий SIL определяется комбинацией SIL3 (общий SIL для подсистем 1, 2, 4, 5) и SIL2 подсистемы 3.

Таким образом,

- Общий SIL для системы определяется одноканальной последовательностью SIL3(rpynna 1+2, 4+5) + SIL2 (подсистема 3), и соответствует по уровню отказоустойчивости SIL2.

В стандарте не уточняется, что, в соответствии с определением, тип всей системы соответствует типу В.

Данный пример наглядно показывает, что определение общего уровня безопасности для системы, состоящей из множества разнородных подсистем, может оказаться совершенно нетривиальным.

11.14. Пример вычисления фактора диагностического охвата по методике IEC

Исходные данные для расчета представлены в таблице 11.41 (см. IEC 61508-6, Annex C). Для наглядности предполагается, что некоторые из компонентов системы (например, резистор R6) не имеют никакой диагностики, поскольку невозможно выявить все режимы отказов для всех компонентов системы.

В таблице 11.42 представлены ограничения по степени диагностического охвата, которые могут быть приписаны к определенным компонентам или подсистемам. Конкретные значения диапазонов в таблице 11.42 являются эмпирическими, и основаны на инженерной практике.

Таблица 11.41 появилась в результате следующих действий:

1. Для каждого компонента системы был проведен анализ режимов и последствий отказов компонента *(FMEA - failure mode and effect analysis)* при отсутствии диагностического тестирования. Доли общей интенсивности отказов по каждому типу отказа для каждого компонента разделены на долю безопасных (S) и опасных (D) отказов. Это разделение может быть как полностью детерминированным для простых компонентов, так и основанным на опыте для компонентов сложных. Обычно для комплексных компонентов, для которых невозможно провести детальный анализ всех режимов отказов, принимается разделение 50/50 между опасными и безопасными отказами.

Таблица 11.41

Пример вычисления фактора диагностического охвата

Item	No	Type	Division of safe and dangerous failures for each failure mode								Division of safe and dangerous failures for diagnostic coverage and calculated failure rates													
					SC		Drift		Function		DC													
			S	D	S	D	S	D	S	D	S	D												
Print	1	Print	0 5	0,5	0 5	0 5	0	0	0	0	0 99	0 99	1 t 0		11 0				0,1	10 9	10 9			
CN1	1	Con96pin	0 5	0 5									14 5		11 5				0 1	11 4	11 4			
C4	1	1QOnF		0		0	0	0	0	0		0	3 2		0 0				0 0	3 2	0,0			
C2	1	10 M F	0	0	0	0	0	0	0	0		0	0 8		0 0				0 0	0 8	0 0			
R4	1	1M	0 5	0 5	0 5	0 5					1	1	17		17				0 0	t 7	17			
R6	1	100k									0	0	0 0		0 0				0 0	O 0	0,0			
osc?	1	OSC24 MHz	0 5	0 5	0 5	0 5	0 5	0 5	0 5	0 5	1	1	16 0		16 0				0 0	16 0	'6 0			
U8	1	MC6SOOO-12	0 5	0 5	O 5	0 5	0,5	0 5	0 5	0 5	0 99	0 99	22 8		22 8				0 2	22 6	22,6			
U16	1	MC6SOOO-12	0	0	0 5	1	0 6	0 5	0 5	0 5	0 90	0 90	260 4		483 6				695 6	48 4	234 4			
U26	1	74HC774	0 s	0 5	0 5	0,5	0 5	0 5	0 5	0 5	0 99	0 98	22,8		22 8				45 4	0 2	22 6			
U27	1	74	0 s	0,5	0 5	0 5	0 6	0 5	0 5	0 5	0 98	0 98	14 4		14 4				28 7	0 1	14 3			
U28	1	PAL16L8A	0	1	0	1	0	1	0	/	0 98	0 98	0 0		88 0				86.2	1.8	o.o			
T1	1	BC817	0	0	0	0 67	0	0 5	0	0	1	1	0 0		0 2				0 4	O 0	o 0			
Total													365		672				986	SO 9	338			

NOTE None of the failure modes of item R6 an but a failure does nc>t affect either safety or availability

Key

s Safe failure

Dangerous failure

Open circuit

s c Short circuit

Drift Change of value

Function Functional failures

DC,,,, „ Specific diagnostic coverage for the component

See also table B 1 although in this table failure nxtes are for the individual components iri question rather than every component in a channel

Таблица 11.42

Диагностический охват и эффективность для различных подсистем

Component	Low diagnostic coverage	Medium diagnostic coverage	High diagnostic coverage
CPU (see note 3)	total less than 70 %	total less than 90 %	
register internal RAM	50 % - 70 %	85 % - 90 %	99 % 99,99%
coding and execution including flag register	50 % - 60 %	75 % - 95 %	
{see note 3)	50 % 70 %	85% 98%	
address calculation (see note 3)	50 % 60 %	60% 90%	85 % - 98 %
program counter stack pointer	50 % 70 %		
	40 % - 60 %		
Bus			
memory management unit	50%	70 %	90 % - 99 %
bus-arbitration	50%	70%	90 % - 99 %
Interrupt handling	40 % - 60 %	60 % - 90 %	85 % - 98 %
Clock (quartz) (see note 4)	50 %		95 % - 99 %
Program flow monitoring			
temporal (see note 3)	40 % - 60 %	60 % - 80 %	
logical (see note 3)	40 % 60 %	60 % - 90 %	
temporal and logical (see note 5)		65 % - 90 %	90 % - 98 %
Invariable memory	50 % 70 %	99%	99 99 %
Variable memory	50 % - 70 %	85 % - 90 %	99 % - 99 99 %
Discrete hardware			
digital I/O	70 %	90%	99%
analogue I/O	50 % - 60 %	70 % 85 %	99%
power supply	50 % - 60 %	70 % 85 %	99%
Communication and mass storage	90 %	99,9 %	99,99 %
Electromechanical devices	90%	99%	99,9 %
Sensors	50 % - 70 %	70 % - 85 %	99%
Final elements	50 % 70 %	70% 85%	99%

NOTE 1 This table should be read in conjunction with table A 1 of IEC 61508-2 which provides the failure modes to be considered

NOTE 2 When a range is given for diagnostic coverage, the upper interval boundaries may be set only for narrowly tolerated monitoring means or for test measures that stress the function to be tested in a highly dynamic manner

NOTE 3 For techniques where there fs no high diagnostic coverage figure at present no measures and techniques *of* high effectiveness are known

NOTE 4 At present no measures and techniques of medium effectiveness are known for quartz clocks

NOTE 5 The minimum diagnostic coverage for a combination of temporal and logical program flow monitoring is medium

2. Фактор диагностического охвата для каждого компонента представлен колонкой DC_{COMP}.
3. В колонках (1) и (2) для каждого компонента представлена интенсивность безопасного и опасного отказа при отсутствии диагностического тестирования - $Л_8$ и $Л_0$ соответственно.
4. Обнаруженные опасные отказы можно рассматривать как объективно безопасные.
   Таким образом, можно выделить группу объективно безопасных отказов (обнаруженные и необнаруженные безопасные отказы, плюс обнаруженные опасные отказы), и группу необнаруженных опасных отказов.
   Тогда эффективная интенсивность безопасных отказов (колонка 3) определится как

   $$+Л_{00} = Л_8 + DC_{COMP} - Л_0 .$$

   Аналогичным образом, интенсивность необнаруженных опасных отказов (колонка 4) может быть получена как

   $$Л_0и - (1 \sim DC_{COMP}) \cdot Л_0$$

5. В колонке (5) представлена интенсивность безопасных обнаруженных отказов. В колонке (6) представлена интенсивность опасных обнаруженных отказов. Значения получены перемножением соответствующего значения уровня самодиагностики на интенсивность безопасных и опасных отказов соответственно:

   $$Л\$o \sim DC_{COMP} \cdot Л_8 , \quad Л_{00} = DC_{COMP}\ Л_0$$

Окончательно из таблицы 11.41 выделяются следующие результаты:

1. Общая интенсивность необнаруженных опасных отказов:

   $$IЛ_ш = 5{,}0910\sim^{8}$$

2. Общая интенсивность отказов системы

   $$л = IЛ_8 + £Л_{00} + £.Л_ш = 9{,}86 \cdot 1СГ^{7} + 5{,}09\ 10\sim^{8} = 1{,}04 \cdot 10\sim^{6}$$

3. Общая интенсивность необнаруженных безопасных отказов:

   $$I\,Л_{8и} = ХЛ_8 - £Л_{50} = (365 - 338) \cdot 10^{9} = 2{,}7 \cdot 10\sim^{8}$$

4. Фактор диагностического охвата для безопасных отказов:

$$SC = \frac{\text{Z A s d}}{\text{I Я}_5} = \frac{3\text{ M}}{365} = 93\ \text{O}_{/\text{o}}$$

5. Фактор диагностического охвата для опасных отказов:

$$DC = \frac{\text{£}}{l\ Я_0} = \frac{}{672} = 92\ \%$$

Эту характеристику и ассоциируют обычно с диагностическим охватом.

6. Доля безопасных отказов SFF *(Safe Failure Fraction)* для системы в целом

$$SFF = \bullet \frac{\text{Z 4}^{+}\text{Z 4o}}{\text{I я}_5 + 1\ 4\text{d} + 14<,} - \frac{\text{Z 4 + £ 4o}}{\text{Z я}_5 + \text{Z я}_D}$$

$$\frac{\text{L 4 + I 4}_D}{\text{s Я}} - \frac{9S6}{365 + 672} = 95\ \%$$

Для сравнения:

В отсутствие диагностического тестирования общая интенсивность отказов делится между безопасными и опасными отказами в следующем соотношении:

$$\frac{\text{L 4}}{\text{I я}} = \frac{\text{Z 4}}{\text{X я}_5 + \text{X Я}_0} = \frac{365}{365 + 672} = 35\ \%$$

$$\text{ЕЯ} - \frac{}{\text{I я}_5 + \text{X Я}_0} - \frac{672}{365 + 672} = 65\%$$

11.15. Выводы

Существуют различные подходы к оценке надежности оборудования систем безопасности. Однако их бездумное применение может оказаться совершенно бесплодным. Более того, может привести к абсолютно противоположному результату: великолепное оборудование, которое во множестве реально существующих приложений на самых сложных технологических процессах проявляет себя наилучшим образом, может оказаться никуда не годным с точки зрения абстрактного расчета. И наоборот.

Глава 12

УСОВЕРШЕНСТВОВАННОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ

В задачу настоящей работы не входит изложение теории оптимального управления и методов математического моделирования, хотя и этот предмет известен автору не понаслышке. Но обозначить роль современных методов управления в контексте создания полноценных АСУТП необходимо. Ведь грамотное управление технологическим процессом в не меньшей степени служит безопасности, одновременно открывая значительные резервы повышения эффективности производства. В настоящей главе рассматриваются ключевые аспекты современных методов управления технологическими процессами:

- Средства автоматической настройки контуров регулирования
- Упреждающее управление
- Многопараметрическое управление
- Упреждающее управление по модели.

Приводятся конкретные примеры решения реальных задач управления. На примере управления тепловым режимом реактора показывается, что в подавляющем большинстве случаев не требуется особых изощренных моделирующих программных комплексов.

Для упреждающих действий по управлению часто остаточно простейших соотношений материального и теплового баланса, чтобы радикальным образом улучшить качество управления. Бессмысленно рассчитывать на необыкновенный эффект от суперсовременного пакета оптимизации, если устаревшее полевое оборудование не способно ни предоставить

реальные данные с процесса, ни обеспечить элементарное регулирование. На рисунке 12.1 показано место усовершенствованного управления процессом *(Advanced Process Control* - APC) в общей структуре управления нефтегазодобывающим, химическим, нефтехимическим или нефтеперерабатывающим производством.

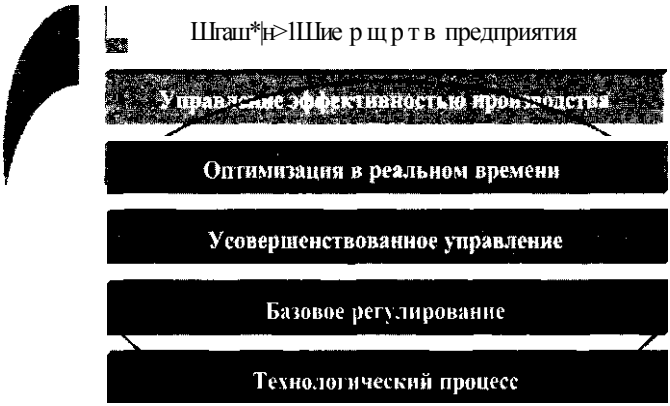


Рис. 12.1

Усовершенствованное управление представлено многосвязными предсказывающими по модели контроллерами, которые являются надстройкой над ординарным и связным регулированием.

В свою очередь, многопараметрический контроллер получает задание от технолога-оператора. В очень дорогом и далеком идеале он может получать задание от пакета оптимизации в реальном времени.

Принципиальные преимущества усовершенствованного управления заключаются в следующем:

- Управление переменными процесса с учетом взаимосвязей между переменными;
- Эффективная работа с ограничениями переменных;
- Быстрый отклик на изменение технологической ситуации за счет управления по упреждению;
- Уменьшение амплитуды и длительности переходного процесса, и соответствующая стабилизация процесса.

12.1. Пакеты автонастройки контуров управления

Ни одна из самых лучших систем управления не может существовать без качественной настройки контуров управления. Существенное сокращение времени запуска системы управления и уменьшение затрат по обслуживанию могут оказать специализированные пакеты автоматизированной настройки контуров регулирования.

Важное замечание.

Основное условие качественной настройки контуров регулирования - добротное полевое оборудование. В первую очередь это касается регулирующих клапанов. Обследование показывает, что с регулирующими клапанами связано от 30 до 35% проблем при настройке контуров. Это значит, что для каждого третьего контура необходима регулировка или замена клапана для обеспечения удовлетворительного качества регулирования.

Если вычисленные с помощью пакета автонастройки значения приводят к неадекватному поведению контура, это, скорее всего, означает, что имеются проблемы с клапаном. Если вычисленный коэффициент усиления слишком велик, или время интегрирования слишком мало, в первую очередь необходимо проверить клапаны. Многие регулирующие клапаны имеют заедание штока или зону нечувствительности (гистерезис), что вызывает неправильную идентификацию модели процесса и, соответственно, неправильную настройку.

Настройка контура.

После того, как контур сконфигурирован для управления конкретным процессом, он должен быть настроен. Определение значений параметров, обеспечивающих стабильную и эффективную работу контура, называется **настройкой контура.**

Если контур настроен так, что имеет слишком медленный отклик, то процесс регулирования, возможно, и будет стабильным, но не достаточно динамичным. Если контур настроен на слишком быстрый отклик, то он может быть очень динамичным, но может иметь большое перерегулирование и колебания около заданного значения, и вносить большие возмущения в процесс.

Целью настройки является получение контура регулирования с приемлемой реакцией и устойчивостью.

Наиболее часто используемыми методами настройки контуров являются **метод непосредственных проб и ошибок и методы автоматизированного вычисления настроек:**

- Метод проб и ошибок предполагает ручное изменение параметров настройки до тех пор, пока не будет достигнута стабилизация контура.
- Метод вычисления настроек использует вычисление параметров регулятора на основе проверенных практикой методов и алгоритмов.

Метод автоматизированного вычисления настроек является предпочтительным по сравнению с простым методом проб и ошибок, поскольку он требует меньшего числа циклов для достижения желаемого результата. Если процесс является не слишком динамичным, то использование метода вычисления настроек может быть существенно более эффективным, чем метод проб и ошибок.

Один из основных методов автоматизированной настройки - метод ступенчатых возмущений процесса. Данный алгоритм использует простейшее описание канала регулирования технологического процесса моделью первого порядка с запаздыванием. Однако и приближение первого порядка во многих случаях дает значительный эффект.

Во время настройки выход выбранного ПИД-регулятора задается с помощью ступенчатой функции, действующей как реле с временной задержкой. Это реле формирует прямоугольный управляющий сигнал определенной длительности, и вызывает колебания переменной процесса с небольшой контролируемой амплитудой. На основе амплитуды и частоты колебаний регулируемой переменной программа настройки вычисляет результирующий коэффициент усиления и период переходного процесса. Затем на основании найденных параметров переходного процесса вычисляются настройки ПИД-регулятора.

Преимущества пакетов автонастройки определяются проверенной на практике методологией:

- Настройка основывается на хорошо зарекомендовавшей себя теории автоматического регулирования;
- Пакеты применимы к широкому классу процессов благодаря тому, что используются простейшие универсальные модельки поведения процесса;

- Пакеты позволяют производить автонастройку контура и в ручном режиме, и в автоматическом;
- Методы настройки применимы к широкому спектру и инерционных, и динамичных процессов;
- Имеют простой интерфейс оператора;
- Пакеты легко интегрируются в среду практически всех известных систем управления;
- Реализуют широкий набор известных методов настройки.

По результатам настройки выдается отчет.

В отчете указывается, кто и когда выполнял настройку, содержатся исходные и итоговые параметры настройки, динамические характеристики процесса и используемые при настройке правила.

Отчетная информация автоматически сохраняется в архиве, и при следующем запуске пакета может использоваться в качестве исходных значений параметров настройки для данного контура.

Опытный инженер может воспользоваться экспертным режимом, и задействовать альтернативные методы настройки, такие как

- Модифицированный метод Зиглера-Николса;
- Настройка по заданному коэффициенту усиления и запасу по фазе;
- Метод лямбда и лямбда - среднего;
- Предиктор Смита, или
- Метод настройки по внутренней модели.

Модифицированный метод Зиглера-Николса для пропорционально-интегрального регулирования базируется на методе Зиглера-Николса с поправками, минимизирующими перерегулирование.

Метод задания коэффициента усиления и запаса по фазе для ПИД-регулирования задает первоначальный запас по фазе, который в большинстве случаев обеспечивает минимальное перерегулирование, то есть переменная процесса не будет значительно отклоняться от заданного значения. Более медленный отклик с меньшим перерегулированием в большинстве случаев может быть достигнут при увеличенном запасе по усилению и запасе по фазе.

Метод лямбда для ПИ-регулятора позволяет оценить отношение постоянной времени замкнутого контура к постоянной времени разомкнутого контура как характеристический коэффициент лямбда.

Метод лямбда-среднего предназначен для контуров ПИ - регулирования объектов без самовыравнивания, например, уровня в емкости.

Предиктор Смита эффективен в случаях, когда запаздывание процесса больше постоянной времени этого процесса.

Метод управления по внутренней модели обеспечивает настройки пропорциональной, интегральной и дифференциальной составляющим на основе модели первого порядка с запаздыванием. Модель процесса настраивается в процессе испытаний. Метод IMC *(Internal Model Control)* особенно полезен, когда запаздывание процесса больше половины постоянной времени этого процесса. Величина запаздывания процесса и постоянная времени процесса отображаются на экране настройщика в окне результатов теста. Если используется экспертный режим, то не нужно повторно вводить исходные параметры для следующих тестовых испытаний. Как только настройщик определит динамические характеристики контура, он вычислит новые параметры для другого метода настройки.

Базовыми блоками в пакетах настройки являются блоки ПИД-регулятора. Автонастройщик может использоваться для автоматического вычисления пропорциональной, интегральной и дифференциальной составляющей для конкретного процесса на основе выбранного типа процесса и метода настройки. Автонастройщик может также автоматически вычислять параметры нечеткой логики, обеспечивающие наилучший отклик.

Применение функций автонастройки должно находиться под жестким контролем. Как правило, доступ к этим функциям организуется с инженерной станции РСУ. Физический доступ к самой инженерной станции должен быть возможен только для ограниченного круга лиц, имеющих специальный допуск. Функции перенастройки также дополнительно защищаются от несанкционированного доступа. Запуск автонастройки возможен только в том случае, если разработчик обладает необходимыми привилегиями на инженерной станции, используемой для работы с пакетом.

Критичные ко времени операции, связанные с идентификацией процесса, реализуются в функциональных блоках. Такой подход позволяет определять динамические свойства процесса более точно за счет исключения ошибок, возникающих из-за задержек обмена данными. Часть пакета, находящаяся в инженерной станции, поддерживает отображение параметров контроллера и вычисление настроек на основе динамических свойств процесса, определяемых функциональным ПИД-блоком. Перед началом процесса настройки необходимо убедиться в том, что контур является относительно стабильным, а переменная процесса PV находится вблизи значения SP. Если выход контроллера постоянно изменяется из-за шумов и нестабильности процесса, то лучше начать настройку контура с ручного режима. Иногда это может обеспечить лучшие результаты.

Если переменная процесса PV стабильна, но выход контроллера постоянно изменяется, то может понадобиться защита контура от шумов. Если настраиваемый контур имеет очень высокий уровень шумов, то параметры настройки, вычисляемые автонастройщиком, могут оказаться неприемлемыми. Поэтому если значения SP и PV слишком далеки друг от друга, то в начале тестирования должно выдаваться предупредительное сообщение.

С другой стороны, изменение выхода регулятора должно вызвать соответствующее изменение переменной процесса. Если изменение PV недостаточно велико, процесс настройки может не начаться вовсе из-за отсутствия автоколебаний.

Колебания могут отсутствовать в следующих случаях:

- Незначительные возмущения нагрузки не влияют на PV;
- Слишком большой шум в контуре;
- Регулирующий клапан неисправен.

В то же время, в процессе настройки необходимо соблюдать большую осторожность, чтобы ступенчатое возмущение на процесс не привело к срабатыванию блокировки. Поэтому необходимо тщательно следить за соблюдением следующих условий:

- Во время настройки параметры SP, PV, и выход контура OUT никогда не должны достигать окрестности своих предаварийных значений.

- Во время настройки параметры SP, PV не должны достигать 10% до верхней и нижней границы шкалы в инженерных единицах, а выход OUT не должен достигать 10% до сконфигурированной шкалы выхода.

Период настройки.

На рисунке 12.2 приведена типичная временная диаграмма ступенчатого релейного возмущения и отклика переменной процесса PV при настройке. Реле возмущений переключается в моменты времени, когда PV переходит через значение задания SP.

Амплитуда ступенчатых возмущений *d* обычно составляет от 5 до 10% от диапазона выхода регулятора. Для управляющих блоков это соответствует изменению выходного значения OUT в процентах. Изменение переменной процесса PV максимально на этапе инициализации, то есть во время первого периода колебаний. Обычно, выходная переменная процесса PV может изменяться от 1 до 5% от шкалы PV.

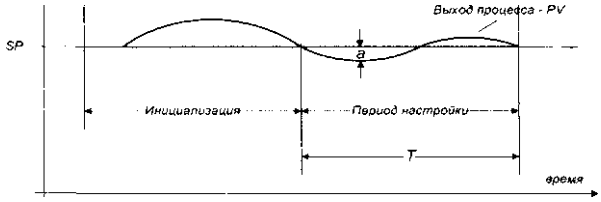


Рис. 12.2

Колебания должны продолжаться как минимум в течение одного периода после инициализации. Если для настройки используется большее число периодов колебаний, то для определения результирующего коэффициента усиления применяется средняя амплитуда колебаний. Автонастройщик использует по умолчанию два периода колебаний настройки, и определяет амплитуду как среднюю амплитуду колебаний.

Во время периодов колебаний, следующих за инициализацией (периоды настройки), переключения ступенчатых возмущений блокируются в начале каждого полупериода для увеличения устойчивости настройщика к шуму. Длительность этих блокировок переключения зависит от зоны нечувствительности настраиваемого контура, которая определяется в течение цикла инициализации.

В некоторых случаях переменная процесса характеризуется высоким уровнем шума или большими возмущениями нагрузки. В таких условиях лучшие результаты могут быть получены при использовании гистерезиса ступенчатых возмущений, или при увеличенной длительности тестирования процесса.

Гистерезис колебаний.

Для процессов с высоким уровнем шума, необходимо настроить величину гистерезиса ступенчатых возмущений для дополнительной защиты от шумовых составляющих процесса. При конфигурировании гистерезиса, реле переключается только в том случае, если PV отличается от SP на указанное значение. При стабильных условиях процесса соотношение между входом и выходом может быть выражено передаточной функцией. В общем виде передаточная функция процесса может быть представлена размахом (или амплитудой) и углом (или фазовым сдвигом).

Конфигурация регулятора.

Пакеты автонастройки имеют широкий набор методов настройки и различных установок, которые могут быть использованы для достижения наилучшей настройки контура. Ниже даны некоторые общие рекомендации.

- После изменения значений настройки необходимо понаблюдать за контуром некоторое время, чтобы проверить его реакцию на шум, возмущения нагрузки, и небольшие ступенчатые изменения заданного значения SP;
- Если качество регулирования контура неудовлетворительное, можно сначала изменить установки для отклика контура (медленный, нормальный, быстрый);
- Если качество регулирования контура по-прежнему не устраивает, существует возможность использовать другой тип переходного процесса.

- Значение отклика по умолчанию Normal соответствует средней чувствительности. При выборе Fast, изменение выхода контроллера будет иметь большее значение, и отклик контура будет быстрее. При выборе Slow достигается обратный эффект.

Чувствительность контура определяет скорость, с которой контур реагирует на изменение задания и изменения переменной процесса. Рекомендуемое значение коэффициента пропорциональности для конкретного процесса зависит от отклика контура:

- Как правило, по умолчанию в начале настройки используется модифицированный метод настройки Зиглера-Николса. Если обнаруживается, что результаты настройки являются неудовлетворительными, то можно выбрать из меню другой метод настройки;
- Если есть ощущение неточности некоторых из коэффициентов после стандартной настройки, то можно вручную изменить нужные коэффициенты;
- После завершения настройки можно повторно изменить настройки и вычислить новые значения, снова выполнить настройку контура, или изменить вычисленные значения. Для наблюдения за откликом контура во время настройки используется окно трендов.

12.2. Общие рекомендации для выбора метода настройки

Для большинства ординарных контуров регулирования расхода, уровня жидкости и давления газа используется простое ПИ-регулирование. ПИД-регулирование, каскадное, или с упреждающей коррекцией управление используется для регулирования температуры, pH и связного регулирования. Однако связное регулирование может потребовать некоторых ограничений на дифференциальную составляющую.

Если первоначально контур настроен методом проб и ошибок, и он работает удовлетворительно, то имеет смысл попробовать настроить его с помощью автонастройщика более точно. Если значения, вычисленные автонастройщиком, существенно отличаются от значений, найденных по методу "проб и ошибок", то следует очень внимательно их изучить, прежде чем изменять параметры настройки контура.

Существуют ограничения на конфигурацию ПИД-регулятора для некоторых приложений. Например, если отношение времени запаздывания по каналу регулирования к постоянной времени процесса превышает единицу, то качество ПИД-регулирования не может быть гарантировано.

Поэтому результаты автонастройки должны быть тщательно проверены. Если отклик контура неприемлем, то возможно, понадобиться изменить результаты настройки. Для таких приложений лучшие результаты может обеспечить использование для управления предиктора Смита.

Далее приведены типичные примеры приложений при работе с пакетами автонастройки:

- Классический контур с обратной связью;
- Каскадный контур регулирования;
- Контур регулирования по упреждению.

12.3. Автонастройка контура с обратной связью

Пример настройки контура с обратной связью относится к контуру регулирования температуры на приведенной ниже схеме (рис. 12.3). В этом простом примере вода нагревается за счет конденсации насыщенного пара, подаваемого в теплообменник.

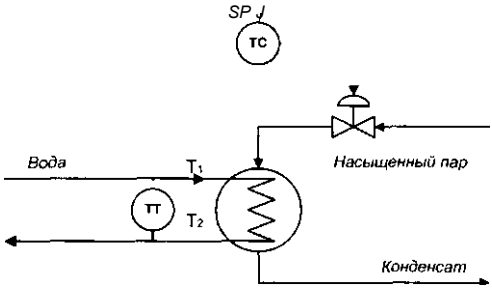


Рис. 12.3

После настройки контура и перевода его в рабочий режим, необходимо проверить отклик на изменения задания SP, и на возмущения по нагрузке. Если контур имеет слишком большое перерегулирование, то необходимо выбрать настройки с меньшим коэффициентом пропорциональности.

12.4. Автонастройка каскадных контуров управления

Каскадные контуры являются составными, поэтому они настраиваются особым образом:

- Сначала нужно настроить вторичный (подчиненный) контур;
- И только затем - первичный ("мастер") контур регулирования.

В качестве примера рассмотрим каскадный контур регулирования уровня (см. рис. 12.4):

- Первичный контур регулирует уровень;
- Вторичный контур регулирует расход на входе.

функциональная схема к?дуяднгц-о контура управления

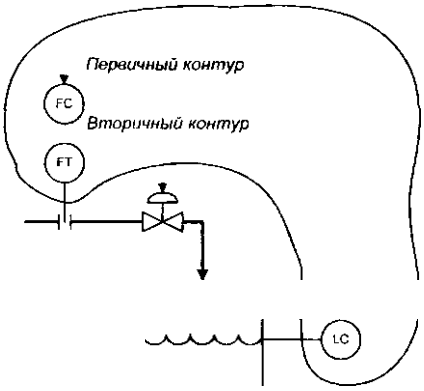


Рис. 12.4

Для настройки каскадного регулятора уровня, приведенного на данной схеме, необходимо выполнить следующие шаги:

- Перевести вторичный контроллер в режим Авто или Ручной для того, чтобы контур стабилизировался;
- Настроить вторичный контур с помощью автонастройщика или вручную так, как если бы это был одиночный контур;

- Перевести вторичный контроллер в Каскадный режим;
- Установить SP первичного контроллера в значение PV;
- Настроить первичный контур с помощью автонастройщика.

12.5. Автонастройка контуров регулирования по упреждению

Чтобы настроить упреждающую коррекцию в контуре регулирования по упреждению, необходимо зафиксировать значение самой упреждающей коррекции (она должна быть константой) во время процесса настройки.

Функциональная схема контура управления по упреждению

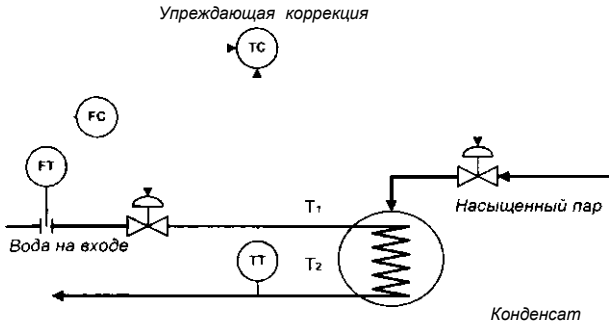


Рис. 12.5

Контур регулирования температуры по упреждению на приведенной схеме (рис. 12.5) похож на обычный контур регулирования температуры воды на выходе теплообменника, описанный выше, за исключением того, что расход воды, проходящей через теплообменник, заводится в регулятор температуры как упреждающая коррекция.

Для настройки регулятора уровня по упреждению необходимо выполнить следующие шаги (рис. 12.6):

- Выключить упреждающую коррекцию контура;
- С помощью автонастройки настроить контур управления так, как если бы это был обычный контур;
- Включить упреждающую коррекцию контура.

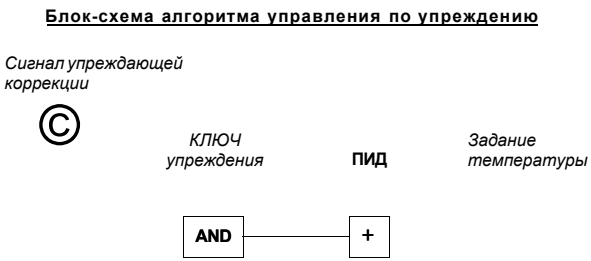


Рис. 12.6

12.6. Усовершенствованное управление технологическим процессом

Грамотное применение схем связного управления с упреждением способно дать необыкновенный эффект стабилизации процесса и соответствующего стабильного качества продукции, и, что не менее актуально, - в энергосбережении.

В этом разделе приводится вполне реальный пример применения алгоритмов усовершенствованного управления, дающий общее представление о современных методах управления. Исходная схема автоматизации приведена на рисунке 12.7. Модифицированная и усовершенствованная схема автоматизации приведена на рисунке 12.8.

Повышение качества конечного продукта.

Качество конечного продукта может быть в существенной степени улучшено за счет использования в алгоритмах регулирования комбинированных схем управления, когда традиционные контуры управления по обратной связи сочетаются с контурами управления по возмущению (упреждению).

Причем наиболее значительный эффект от применения алгоритмов управления по возмущению проявляется именно в наиболее типичных для нас условиях эксплуатации, при которых возникает частая необходимость в изменении нагрузки на установку. С этой целью в исходную схему управления введены следующие вычислительные блоки и блоки управления.

Управление дозировкой катализатора.

Блок FFIC-01 - блок расчета требуемого расхода катализатора по заданному соотношению расходов катализатора и Реагента 1. Блок работает следующим образом:

Исходя из заданного значения соотношения потоков катализатора *F2* и Реагента 1 *F1*, равного $(F2/F1)^{sp}$, вычисляется требуемое опорное значение расхода катализатора $FF2^{SP}$:

$$FF2^{SP} = \quad j \quad ^{F1} \qquad (^{12Л})$$

где F1 - текущее значение расхода Реагента 1.

Замечание

Использование упреждающего регулятора по действительному, а не заданному значению нагрузки на установку позволяет не только синхронизировать подачу катализатора, Реагента 2 и стабилизатора при изменении нагрузки на установку, но и вплотную подойти к автоматизации пуска и останова данного узла.

Блок FFY- 01. По изменению вычисленного блоком AIC-01 корректирующего изменения расхода катализатора:

$$AF2^{SP} = K - (pH1^{SP} - pH1)$$

и по выходу блока соотношения FFIC-01 определяется новое заданное значение расхода катализатора F2:

$$F2^{SP} = FF2^{SP} + AF2^{SP} \qquad (12.2)$$

Найденное значение позволяет вычислить величину, на которую необходимо скорректировать задание уровня для регулятора LIC-01:

$$A\ L1 \frac{F?^{sp} \cdot At}{P'9'S} \sim K1 \cdot At \cdot F2^{SP}, \qquad (12.3)$$

где

р	-	Плотность катализатора;
g	-	Ускорение свободного падения;
S	-	Площадь поперечного сечения емкости с катализатором Е-1;
At	-	интервал работы алгоритма компенсации возмущений.

Дополнительно, с целью защиты процесса при критическом уменьшении-запаса катализатора в емкости Е-1, в систему вводятся следующие функции:

1) Предупредительная сигнализация по нижнему предаварийному пределу уровня в емкости Е-1 на регуляторе LIC-01, и
2) Блокировка подачи Реагента 1 по аварийному исчерпанию запаса катализатора LSLL-01 в емкости Е-1 с помощью отсекателя XV-01, оснащенного концевиками с сигнализацией положения.

Управление дозировкой реагента 2.

Блок FFIC-02 - блок расчета требуемого расхода Реагента 2 по заданному соотношению потоков Реагента 2 и Реагента 1. Блок работает следующим образом:

Исходя из заданного значения соотношения потоков Реагента 2 *F4* и Реагента 1 *F1,* равного $(F4/F1)^{SP}$, вычисляется заданное значение расхода Реагента 2 $FF4^{sp}$:

$$FF4^{SP} = \left(\frac{F4}{F1}\right)^{SP} \cdot F1 \qquad (12.4)$$

где *F1* - текущее значение расхода Реагента 1 (см. предыдущее Замечание). Это значение выдается в качестве задания регулятору расхода Реагента 2 FIC-04.

Управление дозировкой стабилизатора. Полностью аналогично алгоритму управления дозировкой катализатора (См. рис. 12.8). Соответствующая цепочка блоков —

FIC-01 - FFIC-03 - FFY-03(AIC-02) - LIC-02(LSLL-02)

Экономия пара.

Почти вся энергия, используемая для нагрева реакционной смеси, поступает за счет скрытой теплоты парообразования, которая отдается при конденсации пара.

Скорость, с которой происходит конденсация пара и отдача тепла, зависит от давления пара в рубашке реактора и от температуры реакционной смеси. Открытие клапана на линии подачи пара позволяет подавать пар с большим расходом, что приводит к повышению давления пара в рубашке и, следовательно, к увеличению передачи тепла реакционной смеси.

Проблема, которая возникает в одноконтурной схеме регулирования температуры реакционной смеси (см. контур TIC-02 на исходной схеме рис. 12.7) состоит в том, что давление пара может неожиданно меняться. В таком случае изменится и расход пара и, следовательно, температура реагентов будет отличаться от заданного значения.

Конечно, регулятор направит корректирующее воздействие на клапан и вернет температуру к заданному значению, однако на это потребуется время, в результате чего значительное количество реакционной смеси выйдет из реактора R-1 при нерасчетной температуре.

Первое улучшение.

Первое усовершенствование системы регулирования теплового режима реактора состоит в том, чтобы расход пара регулировался собственным регулятором расхода (См. рис. 12.8, блок FIC-05).

В случае изменения давления пара регулятор расхода, действующий значительно быстрее регулятора температуры, обеспечит возврат к заданному значению расхода пара. Задание регулятора расхода каскадно связано с регулятором температуры на выходе реактора.

При отклонении температуры продукта на выходе реактора от заданного значения, регулятор температуры окажет корректирующее воздействие на задание регулятора расхода в сторону его (расхода) увеличения или уменьшения. Последний, в свою очередь, изменит положение клапана для увеличения или уменьшения количества пара, поступающего в рубашку реактора.

Второе улучшение: включение в схему управления упреждающего регулятора.

Управление тепловым режимом реактора можно существенно улучшить путем использования регулирования по возмущению независимо от того, являются ли проблемы регулирования результатом запаздывания, или же они вызваны другими причинами.

Регулирование по возмущению представляет собой метод, при котором учет влияния параметров, способных отрицательно сказаться на температуре продукта, производится до того, как им фактически представится возможность повлиять на конечный продукт.

В нашем случае ключевыми параметрами при отработке возмущений являются следующие параметры:

1) Расход продукта F5;
2) Температура продукта на входе в реактор T1;
3) Требуемая температура продукта на выходе из реактора $T2^{SP}$.

Эти переменные и принимаются во внимание в предлагаемой схеме упреждающего регулирования температуры продукта - цепочка блоков

TIC-01 - FFIC-05 - FFY-05 - TIC-02,

в результате чего управляющее воздействие обеспечивает:

- Более точное выдерживание заданной температуры продукта при изменениях нагрузки на реактор;
- Существенную экономию пара за счет сбалансированной подачи пара в рубашку реактора, вычисленной по достаточно простой, но, тем не менее, **модели теплового баланса реактора.**

Ниже приводится уравнение для элемента управления по возмущению FFIC-05:

$FF5 = K2\ F5 - (T2 - T1)$, где (12.5)

FF5 - Вычисленное значение расхода пара;
T1 ~ Температура на входе в реактор;
T2 - Температура на выходе из реактора;
F5 - Расход реакционной смеси.

Оценку коэффициента пропорциональности *K2* можно получить из уравнения теплового баланса реактора:

$K2 \sim C_P/Л$, где (12.6)

Ср - Теплоемкость реакционной смеси;
Я - Удельная теплота парообразования / конденсации водяного пара.

Дополнительное усовершенствование.

Дополнительный эффект повышения устойчивости системы управления температурой продукта на выходе реактора можно достичь за счет использования в алгоритме упреждающего регулятора (формула 12.5) **не текущей** температуры на выходе реактора, **а заданной.**

Это будет давать существенное преимущество, поскольку именно эту, заданную температуру должен иметь продукт, а не ту, что имеется на данный момент времени. Кроме того, в отличие от переменной температуры на выходе реактора, **задание температуры меняется гораздо реже** (если вообще меняется). Таким образом, модель (12.5) преобразуется к следующему виду:

$FF5 = K2\ F5\ (T2^{SP} - T1)$, (12.7)

где $T2^{SP}$ - **Заданная** температура на выходе реактора.

Полученная в результате расчета величина пропорциональна количеству тепла, которое должно быть передано продукту, и равна требуемому расходу пара.

Общий эффект.

Общий эффект повышения точности регулирования достигается за счет того, что к сигналу упреждающего регулятора добавляется сигнал регулирования по обратной связи, который присутствует на выходе регулятора температуры TIC-02. Суперпозиция сигналов управления по обратной связи T1C-02 и по возмущению (блок FFY-05) используется в качестве задания для регулятора расхода пара FIC-05.

Рассмотренные предложения не могут противоречить действующему регламенту работы установки, а ключевые моменты внесенных в схему управления улучшений:

- Упреждающее управление дозировками и
- Управление по модели теплового баланса реактора -

сохраняют свое значение при любых условиях эксплуатации, и дают возможность реально обеспечить заданное качество продукта и экономию энергозатрат.

Представленный алгоритм носит общий характер. На любом из производств можно обнаружить множество технологических узлов, для которых алгоритм управления по упреждению в сочетании с простейшими моделями материального и теплового баланса дадут не эфемерный, а вполне реальный экономический эффект. Данный алгоритм без особого труда может быть адаптирован под конкретное применение.

Существуют возможности дальнейшего усовершенствования представленной схемы управления. Это прежде всего - управление тепловым режимом теплообменника T1, и регулирование уровней в емкостях E1 и E2 не по стоку, а по притоку. Подготовленный читатель может поэкспериментировать над схемой рис. 12.8 уже самостоятельно.

Вот почему так важно готовить специалистов, способных осознавать и отстаивать принципиальную разницу между бездумной модернизацией оборудования, и методами усовершенствованного управления, дающими реальный эффект в повышении стабильности процесса, улучшении качества продукции, снижении энергозатрат, и обеспечении безаварийности производства.

Исходная схема автоматизации

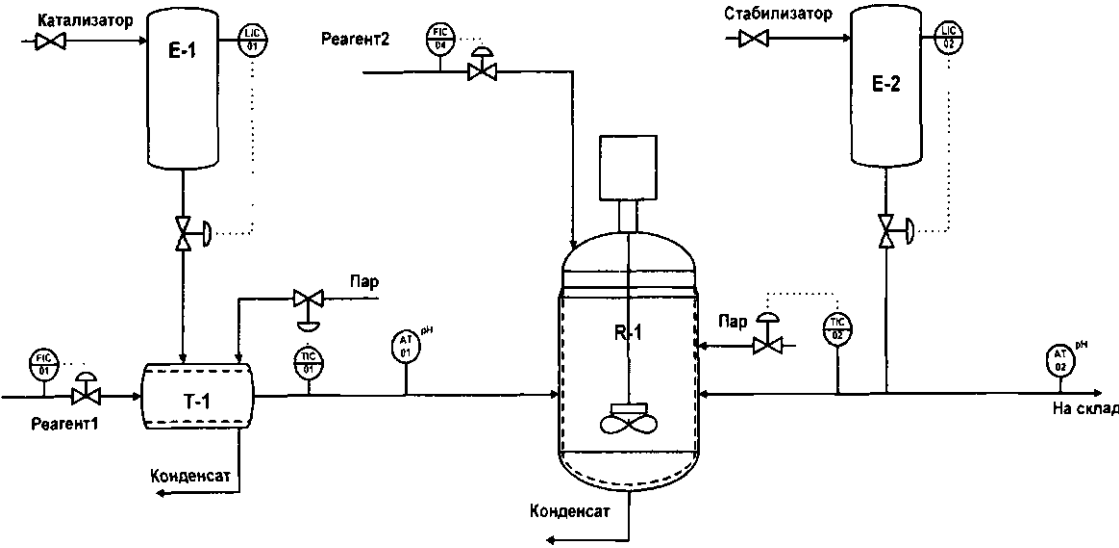


Рис. 12.7

Усовершенствованная схема автоматизации

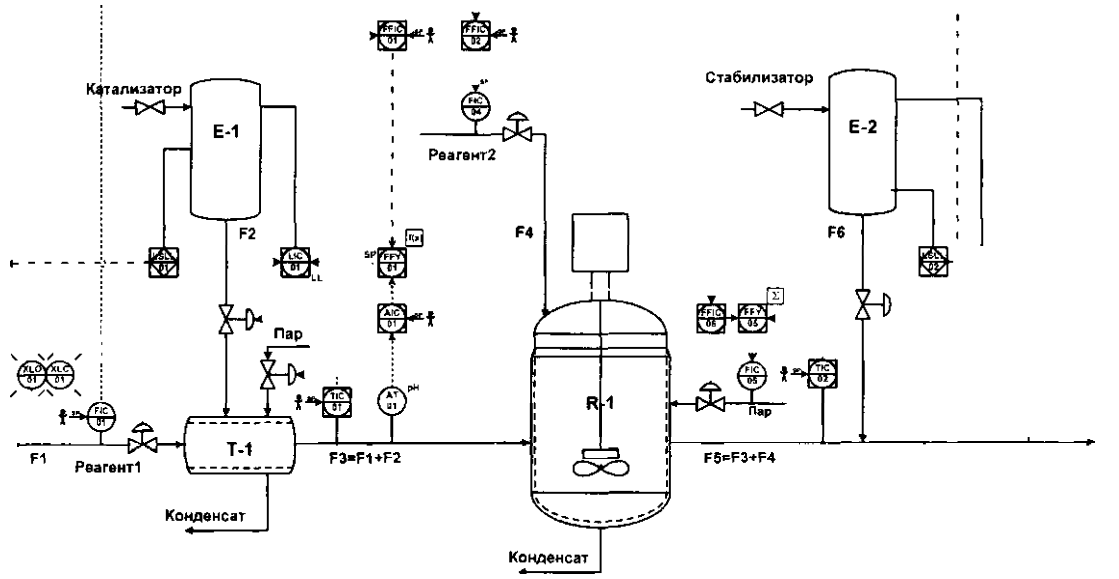


Рис. 12.8

12.7. Многопараметрический контроллер

Традиционные промышленные контроллеры используют PID-алгоритм регулирования: на основе показаний единичного датчика формируется единичное управляющее воздействие на исполнительный механизм (рис. **12.9).**

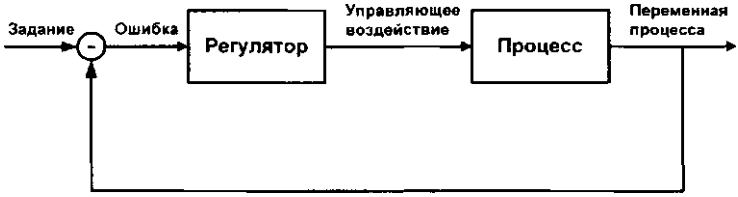


Рис. 12.9

Этот одномерный алгоритм работает вполне эффективно во множестве случаев, когда технологические переменные могут в первом приближении рассматриваться как независимые.

Однако в реальности подобное взаимнооднозначное соответствие регулируемых и регулирующих переменных является скорее исключением, чем правилом. Даже для относительно простых технологических объектов, как например, дистилляционная колонна, существуют тесные взаимосвязи между нагрузкой на колонну, распределением температур и давления по колонне (см. рис. 12.10).

Одним из решений проблем многосвязного управления являются многопараметрические контроллеры.

В идеале многопараметрический контроллер должен рассматривать группу традиционных условно независимых контуров регулирования как единое целое, и на основе текущего состояния определять наилучшие в смысле некоторого критерия управляющие воздействия.

Строго говоря, многосвязность переменных технологического процесса - это правило, а не исключение. Как правило, при традиционном подходе к управлению проблемы взаимного влияния параметров процесса решаются эмпирическим путем, или просто остаются на ответственности технолога-оператора. Не надо объяснять, к чему это приводит.

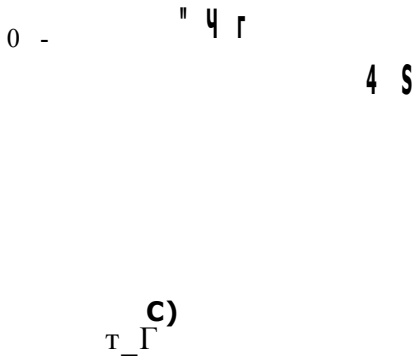


Рис. /2.70

Схема управления депропанизатором (рис. 12.10) предназначена для достижения двух главных целей:

- Предотвратить уход бутана по верху колонны.
- Уменьшить содержание пропана в бутане в кубе колонны.

Однако обе концентрации тесно взаимосвязаны между собой. Более того, они зависят от орошения, нагрузки по пару в кубовый ребойлер, и колебаний расхода и состава сырья. На блок-схеме (рис. 12.11) представлены взаимосвязи переменных процесса.

Эта статическая схема уже не представляется элементарной. Однако ситуация станет на самом деле серьезной, если рассматривать поведение объекта управления во времени.

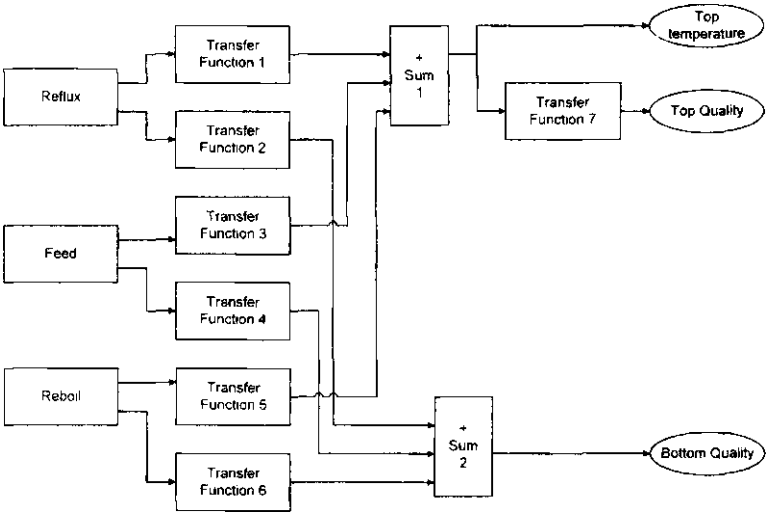


Рис. 12.11

Колебания состава сырья приведут к изменению состава куба быстрее, чем они проявятся по верху колонны. Как только регулятор обнаружит изменение качества кубового продукта, он сразу скорректирует расход орошения и расход пара в ребойлер. Кроме того, контроллер должен учесть влияние этих изменений на концентрацию пропана по верху колонны. Если для управления колонной используются независимые регуляторы для управления концентрациями по верху и в кубе, то колонна будет испытывать долговременный переходный процесс из-за взаимных эффектов влияния расхода пара и орошения на концентрации по верху и по низу колонны.

Этот простой пример наглядно показывает, что проблемы управления, безопасности и эффективности производства совершенно неразделимы. Ценой некорректного управления могут быть не просто потери продукции, но угроза безопасности и здоровью. Только после рационального решения проблем управления и защиты можно переходить к решению проблем повышения эффективности. Но, к сожалению, в отечественной традиции экономические потери важнее человеческих.

Задачи многосвязного управления:

- Предупреждение нарушения ограничений по входным и выходным переменным;
- Поддержка управляемых переменных в стабильном заданном состоянии;
- Поддержка управляющих воздействий в стабильном заданном состоянии;
- Предупреждение недопустимых изменений управляющих воздействий;
- Перевод технологического режима в наиболее выгодное состояние.

12.8. Упреждающее управление по модели

Чтобы перевести технологический процесс в заданное состояние, необходимо знать, как поведет себя объект в ответ на управление.

Таким образом, необходимо иметь средство для предсказания состояния объекта в ответ на каждое изменение по входам. В идеале этим средством должна служить математическая модель процесса.

Имея модель, можно в реальном времени найти оптимальные управляющие воздействия для перевода процесса из текущего состояния в требуемое состояние. Существенным элементом управления по предсказывающей модели является возможность упреждающих воздействий *(feedforward control)*. При этом должны учитываться все ограничения по переменным, и неизбежный шум.

Упреждающее управление по модели *(Model Predictive Control - MPC)* позволяет заранее определить влияние той или иной стратегии управления на поведение объекта управления. Более того, в зависимости от отклика объекта модель может быть скорректирована.

Естественно, что допустимые управляющие воздействия могут быть определены только с учетом существующих ограничений на допустимые диапазоны и скорости изменения технологических переменных, допустимые отклонения от заданных значений и т.д.

На рисунке 12.12 показано, как упреждающий контроллер может на основе модели построить последовательность управляющих воздействий.

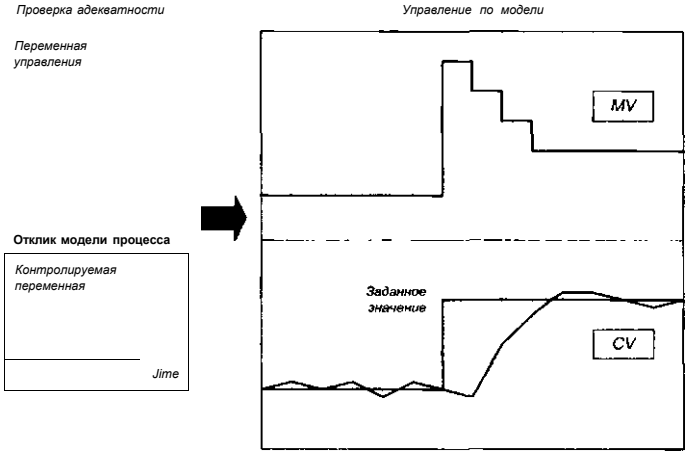


Рис. 12.12

MPC также способен управлять процессами с большими временами запаздывания и кумулятивным откликом. Механизм обратной связи с объектом позволяет контроллеру производить обновление модели (см. рис. 12.13).

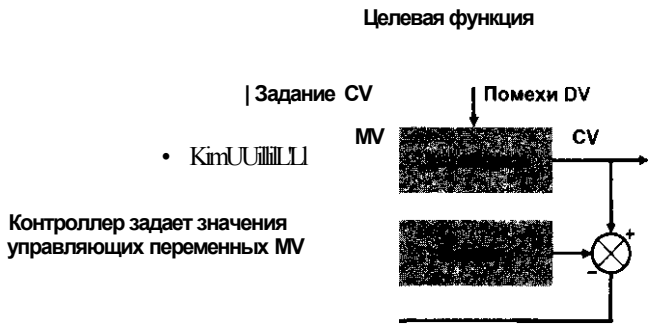


Рис. 12.13

Для многомерных и многосвязных объектов этот механизм является определяющим.

На рисунке 12.14 показано, как алгоритм предсказывающего управления воздействует на управляющую переменную таким образом, чтобы выдержать соответствие базовой траектории, и минимизировать расхождение между заданным и фактическим значением на каждом шаге решения.

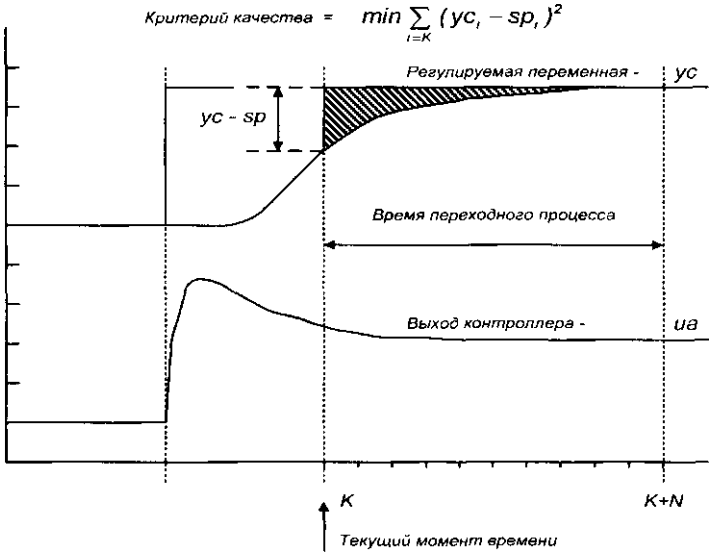


Рис. 12.14

Но каковы преимущества усовершенствованного управления с экономической точки зрения?

12.9. Экономические преимущества внедрения APC

Очевидный и немедленный эффект внедрения усовершенствованного управления - гладкие, постепенные, не разрушающие изменения в лучшую сторону. Но само по себе уменьшение разброса значений не может принести серьезного экономического эффекта.

Главное, что дает уменьшение дисперсии - это возможность безопасно приблизиться к граничным значениям технологического процесса. Как следствие - более полное использование ресурсов установки (рис. 12.15).

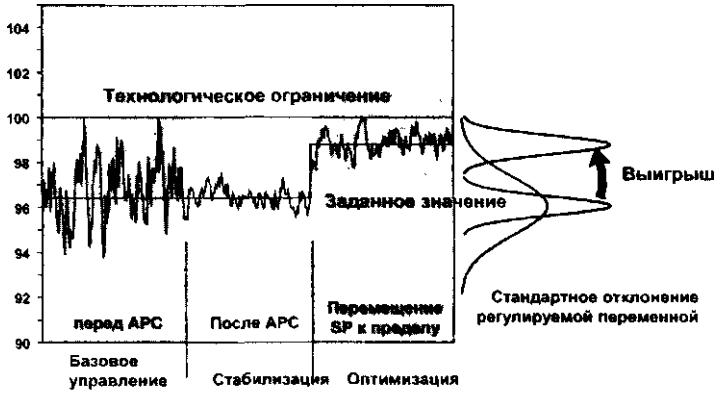


Рис. 12.15

Главной целью усовершенствованного управления является расширение возможностей управления процессом, позволяющее работать с большей производительностью, лучшей степенью извлечения конечных продуктов, и с учетом ограничений оборудования и технологического процесса.

Необходимо понимать, что в данном случае речь идет не только о тривиальных регламентных ограничениях. Преимущества усовершенствованного управления в существенной степени определяются способностью вычислять значения и ограничения расчетного характера, которые иным способом просто не найти:

- Тепловая нагрузка на печь;
- Конверсия;
- Степень конденсации и т.д.

Существуют и не столь очевидные, но вполне реальные преимущества усовершенствованного управления.

Уменьшение неоправданных потерь.

Сразу следом за производительностью установки по значимости следует качество продукции. Часто это приводит к тому, что продукт обладает гораздо лучшим качеством, чем это требует регламент производства. В результате материальные и энергетические затраты на выпуск продукции превышают потенциально необходимые. APC способно снизить планку до необходимого уровня, и тем самым сократить расходы.

Сохранение выхода ценных продуктов.

В процессах нефтепереработки и нефтехимии товарная продукция часто состоит из смеси дорогостоящих и дешевых продуктов. В этой ситуации важно не перерасходовать ценные продукты более того, что требуется по техническим условиям. APC способствует работе вблизи допустимого порога без ущерба качеству продукции.

Работа на меньших давлениях.

Как правило, работа колонн дистилляции на меньших давлениях означает лучшее разделение и меньшее потребление энергии.

Рабочее давление колонны определяется температурой по верху колонны. APC может контролировать давление сверху и температуру флегмы, и одновременно поддерживать давление на минимально допустимом уровне.

Уменьшение потребления пара.

При работе колонны под пониженным давлением снижаются требования к расходу греющего пара в ребойлер.

Уменьшение концентрации кислорода в отходящих газах. Заданная температура на выходе печи поддерживается за счет соотношения расхода избыточного воздуха или кислорода, и расхода топливного газа.

Избыточное количество кислорода или воздуха приводит к снижению температуры на выходе из змеевиков печи, или к повышенному потреблению топлива. Даже незначительный избыток кислорода приводит к существенному снижению эффективности горения или потерям топлива.

Это - классическая область для применения многопараметрического регулирования.

Уменьшение брака.

APC способно не только способствовать улучшению качества продукта, но и избежать выпуска некачественной продукции.

Стабилизация качества продукции уменьшает общие энергетические затраты за счет снижения расхода топлива, пара, хладагентов, электроэнергии.

Уменьшение жесткости работы риформинга за счет снижения требований к октановому числу, что достигается за счет точного контроля смешения.

Увеличение пропускной способности смесителя, поскольку уменьшается или вовсе исключается необходимость повторного смешения.

Плавное и гладкое управление означает меньшее вмешательство оперативного персонала. Это приводит к уменьшению производственной нагрузки на персонал, поскольку усовершенствованное управление способно не только устойчиво поддерживать процесс, но и плавно перевести на новый режим или новую рецептуру.

Увеличение безопасности процесса.
Стабилизация процесса означает снижение вмешательства операторов в процесс. Вероятность человеческой ошибки также резко снижается. Возникает естественный вопрос:
Если преимущества усовершенствованного управления столь очевидны, то почему в отечественной практике усовершенствованное управление практически не используется?

12.10. Основания для выбора усовершенствованного управления

Чудес, по крайней мере, в системах управления технологическими процессами не бывает. Один из ключевых аспектов, которых часто игнорируется, но является самым важным, заключается в том, что пакеты APC нуждаются в постоянной поддержке и обслуживании.

В мозгах должно прочно засесть понимание того, что усовершенствованные многопараметрические контроллеры нуждаются в постоянном обслуживании точно так же, как клапан, насос или компрессор. Вопрос, насколько просто работать, обслуживать, модифицировать программный комплекс зависит от множества условий. Причем эти условия могут быть и в противоречии друг с другом:

- С одной стороны - это жесткость, устойчивость пакета и алгоритмов настройки;
- Ас другой - способность пакета адаптироваться к изменению технологических условий.

Разработчик системы управления должен обладать достаточно высоким уровнем компетентности, чтобы дать ясный ответ на следующие вопросы:

- Какое из вновь поставленного оборудования действительно нуждается в математическом моделировании;
- Как подтвердить, или хотя бы проверить адекватность новой модели;
- Насколько быстро он может перенастроить модель;
- Насколько сложно для него перестроить модель в случае существенных изменений технологического процесса;
- Насколько просто он сам, а не чудодейственные алгоритмы, может интегрировать новые модели с существующими.

12.11. Требования к программному обеспечению усовершенствованного управления

Любое программное обеспечение должно быть рассчитано конечного потребителя. Еще лучше, если программное обеспечение создано при непосредственном участии потребителя.

И совсем фантастический вариант - если потребитель сам обладает необходимым уровнем знаний, чтобы создать нужное ему программное обеспечение.

Вместе с тем, настроенное усовершенствованное управление должно создаваться в расчете на минимальные требования к теоретической подготовке технологического персонала. Однако тому, кто претендует на разработку алгоритмов усовершенствованного управления необходимо ясно осознавать, что без основательных знаний:

- Теории автоматического регулирования;
- Методов математического моделирования;
- Численных методов;
- Теории идентификации;
- Теории вероятностей;
- Математической статистики;
- Теории стохастической аппроксимации;
- Линейного и квадратичного программирования;
- Теории оптимального управления,

наивно рассчитывать на хотя бы минимальный успех от своих экзерсисов с пакетом APC.

Моделирование с помощью современных пакетов АРС основано на концепции "серого" ящика (в отличие от традиционного "черного"). Внутри серого ящика формирование модели конкретного процесса производится с помощью языка блочной структуры. Это упрощает понимание и дальнейшее развитие модели. Для создания модели используется наглядное графическое представление. Пакет должен иметь встроенные средства статистической проверки адекватности модели и определения доверительных интервалов. Должна быть возможность в качестве критерия качества управления использовать экономические показатели. Пакет усовершенствованного управления должен естественным образом встраиваться в общую иерархию функций контроля и управления АСУТП (рис.12.16).

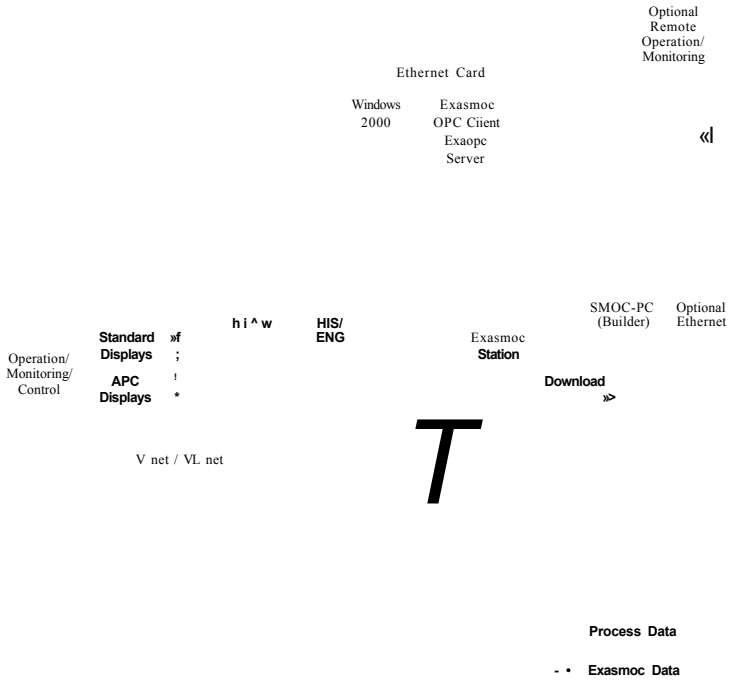


Рис. 12.16

При настройке пакета кроме технологических данных должно использоваться все многообразие настроечных параметров:

- Настройки регуляторов;
- Весовые коэффициенты;
- Допустимые границы;
- Штрафные функции;
- Экономические показатели;
- Приоритеты и т.д.

Интеграция с DCS сторонних производителей. Программное обеспечение APC должно позволять интеграцию с системами управления сторонних производителей с помощью шлюза и OPC-сервера (рис. 12.17).

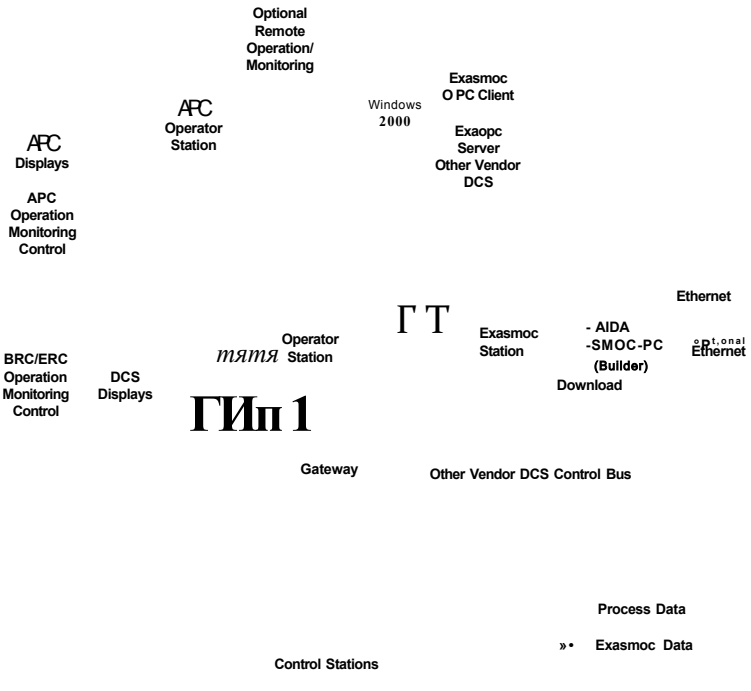


Рис. 12,17

12.12. Структура модели

Создание модели начинается с изучения отклика технологического процесса на ступенчатое или импульсное возмущение по входам. Сущность этого метода точнее всего определяет выражение Козьмы Пруткова: "*Щелкни кобылу в нос - она махнет хвостом* ".

Однако данные с установки никогда не бывают свободны от шума. Источники шума неистребимы - это результат неконтролируемых возмущений самого технологического процесса и ошибок измерения. Следовательно, модель неизбежно будет подвержена влиянию зашумленных исходных данных.

Во-вторых, для многосвязных объектов невозможно смоделировать влияние всех возмущений. Следовательно, модель должна строиться таким образом, чтобы адекватно представлять истинный отклик процесса и одновременно отфильтровывать посторонние составляющие, искажающие результат.

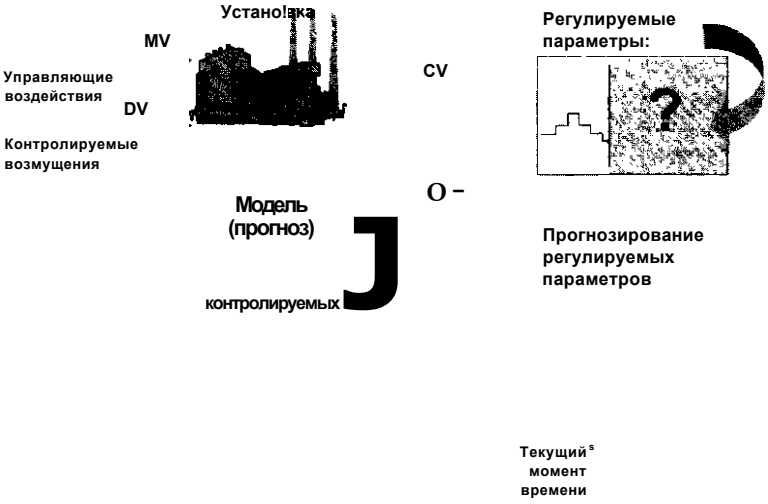


Рис. 12.18

Модель ошибок.

На первом этапе построения модель подразделяется на две части:

- Детерминированную, и
- Стохастическую, вызванную ошибками измерения и посторонними возмущениями.

Детерминированная часть и будет использована в многопараметрическом упреждающем контроллере.

Модель шума на рис. 12.19 состоит из неконтролируемых возмущений и ошибок измерения. Модель шума вычитается из исходных данных, чтобы освободить передаточную функцию от помех.

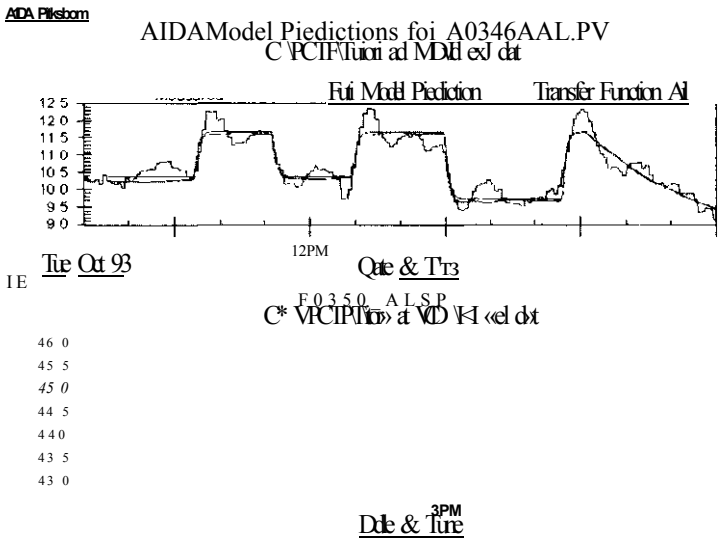


Рис. 12Л9

Статистические средства проверки достоверности модели. Для проверки статистической значимости коэффициентов модели могут использоваться различные статистики, например критерий Фишера. На основе F-статистики можно удостовериться, что влияние некоторой переменной значительно превосходит влияние другой переменной.

Доверительные интервалы.

Вычисляется 99% доверительный интервал для параметров модели. Это дает возможность оценить, насколько могут изменяться параметры модели. Показателем степени досто-

верности параметров служит отношение полезного сигнала к шуму. Это соотношение может быть улучшено за счет увеличения амплитуды ступенчатых или импульсных изменений входных параметров. Другой способ уточнения параметров модели - набрать больше данных, и сделать повторную оценку на большой выборке. Можно сочетать использование обоих методов. Выбор определяется тем, что более приемлемо: внести существенные возмущения в процесс, или потратить большее время на повторное проведение однотипных тестов.

Алгоритм отклика на конечный импульс генерирует 95% доверительный интервал для коэффициентов с одновременной оценкой самих коэффициентов. Это позволяет удостовериться, что для модели найдено устойчивое решение, и на последних шагах коэффициенты модели практически не меняются (см. рис. 12.20).

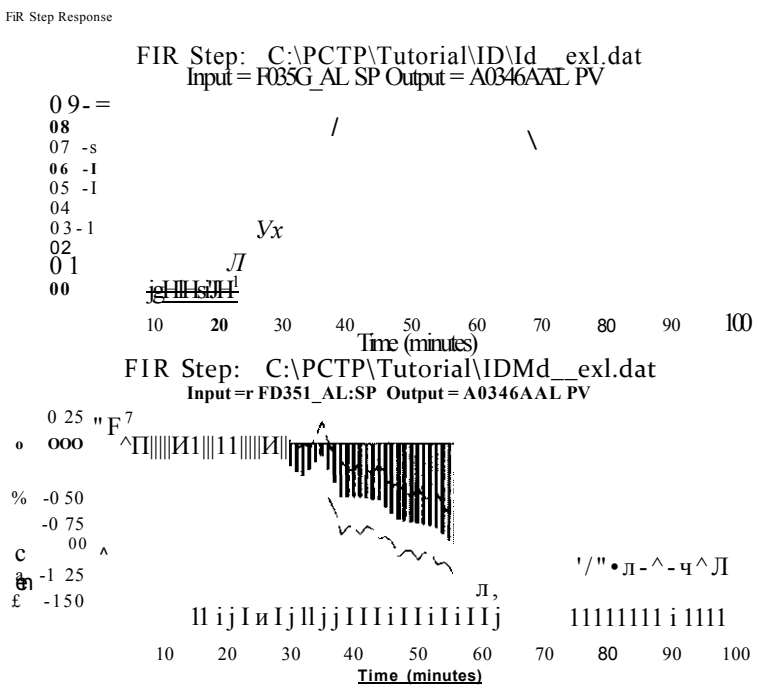


Рис. 12.20

Возможность заморозить некоторые, или все параметры модели. Это дает возможность произвести поверочный расчет: проверить надежность параметров, полученных на одной выборке, на другом наборе данных.

Кросс-корреляция.

Должна существовать возможность рассчитать и вычертить взаимную корреляционную функцию для любых сочетаний входных, выходных и сгенерированных переменных. Те из переменных, которые имеют более двух значимых коэффициентов корреляции, могут претендовать на включение в модель. Естественно, эти расчеты должны сопровождаться определением степени доверительности полученных значений. Однако личный опыт автора говорит о том, что надежда на определение структуры и взаимосвязей модели процесса с помощью исключительно статистических методов совершенно не оправданы. Слишком близки и тесны связи между всеми параметрами процесса, и проявляются они со своими временными характеристиками. Поэтому создание адекватных моделей невозможно без математического описания детерминированных материальных, энергетических и физико-химических превращений реального технологического процесса.

Исследование технологических данных, проектирование и синтез модели - это трудоемкий и долговременный процесс. К тому же доступны эти процедуры далеко не каждому. Поэтому нет никакой необходимости (да и реальной возможности) проводить поиск и идентификацию моделей на реальной системе управления. Программное обеспечение для поиска и создания модели должно быть автономным. В реальном времени на реальной системе управления должен работать собственно многопараметрический предсказывающий контроллер.

Таким образом, процедура формирования алгоритма усовершенствованного управления будет выглядеть следующим образом:

1. Автономная разработка математической модели технологического процесса;
2. Конфигурирование целей управления;
3. Определение настроечных факторов;
4. Генерация контроллера;
5. Тестирование контроллера;
6. Загрузка контроллера.

Возмущения. Это те переменные, которые не доступны для изменения, но влияние которых может быть некоторым образом учтено.

Модель контролируемых возмущений учитывает влияние возмущений, которые могут быть идентифицированы по выходным переменным процесса. Модель неконтролируемых возмущений учитывает влияние тех возмущений, которые не могут быть идентифицированы по выходным переменным процесса. К таковым моделям относятся стохастические модели шума.

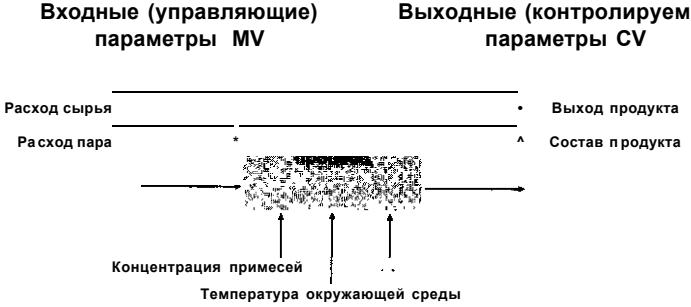


Рис. 12.21

В отличие от сколь широко известного, столь и бесплодного черного ящика, внутренняя структура серого ящика (рис. 12.21) хорошо известна, и фактически повторяет структуру схемы материальных потоков и блоков реального процесса.

Эта концепция позволяет производить разработку модели процесса последовательно, блок за блоком. Любой из блоков может быть модифицирован, либо разработчик вправе использовать собственный блок. Настройка модели производится с учетом всех ограничений.

Корректировка параметров модели может производиться в режиме on-line с использованием фильтра Калмана. При этом корректируется так называемая наблюдаемая модель ошибок, что позволяет повысить устойчивость управления. Фильтр Калмана встраивается непосредственно в схему управления (рис. 12.22). Большим преимуществом такого подхода является прозрачность.

Достаточно настроить параметры передаточных функций, и одновременно наблюдать результат фактически по схеме технологического узла.

Важным средством повышения устойчивости модели является возможность создания промежуточных переменных. Промежуточные переменные описывают внутренние взаимосвязи между переменными состояния и управления. Кроме стандартных переменных блока - управляющая переменная, управляемая переменная, отклонение от задания и т.д. - разработчик имеет возможность определить новые промежуточные переменные. Анализ изменения промежуточных (внутренних) переменных способствует раннему обнаружению отклонений процесса по сравнению с теми выходными переменными, которые доступны для измерения.

Для идентификации контролируемых и неконтролируемых возмущений строятся самостоятельные модели.

Модель контролируемых возмущений представляет собой регулятор по упреждению, который строится на учете параметров, которые доступны для измерения, но находятся за пределом зоны влияния данного контроллера. В отличие от контролируемых возмущений, которые хотя и находятся вне зоны действия контроллера, но, тем не менее, могут быть измерены, неконтролируемые возмущения непредсказуемы и случайны. Наличие неконтролируемых возмущений приводит к ошибке предсказания модели. Наиболее известным средством моделирования случайных неконтролируемых помех является фильтр Калмана.

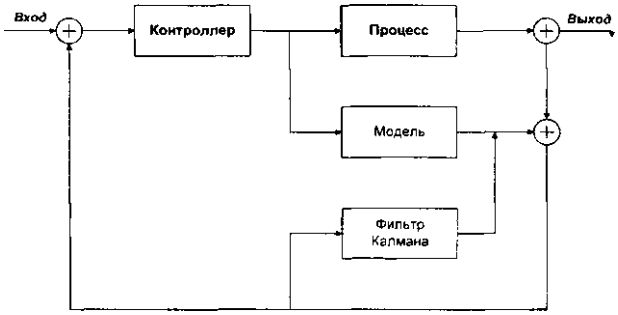


Рис. 12.22

12.13. Усовершенствованное управление колонной

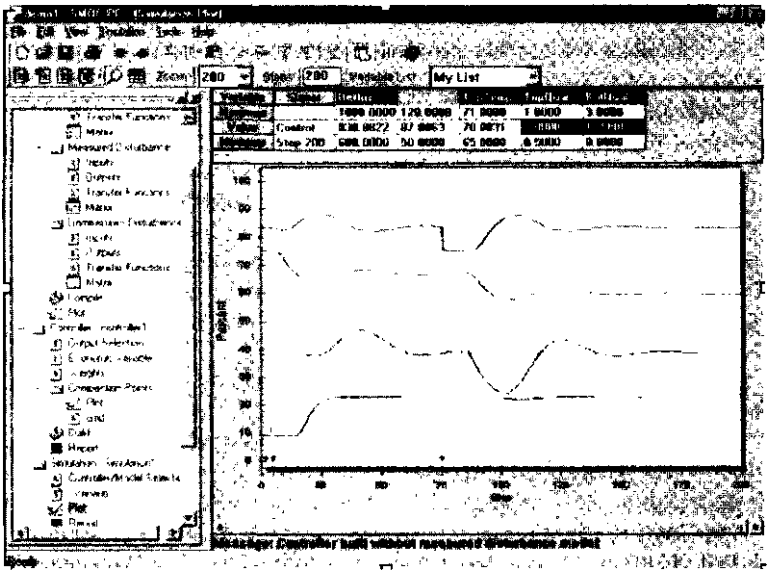


Рис. 12.23

Первая кривая на рисунке 12.23 представляет температуру наверху колонны. Вторая кривая - расход флегмы на колонну, и четвертая - качество (концентрация пропана) сверху колонны. Концентрация пропана - это целевой показатель, который должен поддерживаться. Соответственно, расход орошения будет определяться данной концентрацией. Температура сверху колонны является хорошим индикатором качества ключевого компонента.

Однако изначально управляющее воздействие может быть сделано только после того, как произойдет изменение концентрации. На обнаружение отклонения концентрации и возврат к заданному значению будет потрачено существенное время, в течение которого пострадает качество целевого продукта. Два пика на четвертой кривой (концентрация по верху) как раз и свидетельствуют данный переходный процесс.

Рассмотрим поведение того же объекта управления, в тех же исходных обстоятельствах, но с использованием упреждающего контроллера (рис. 12.24).

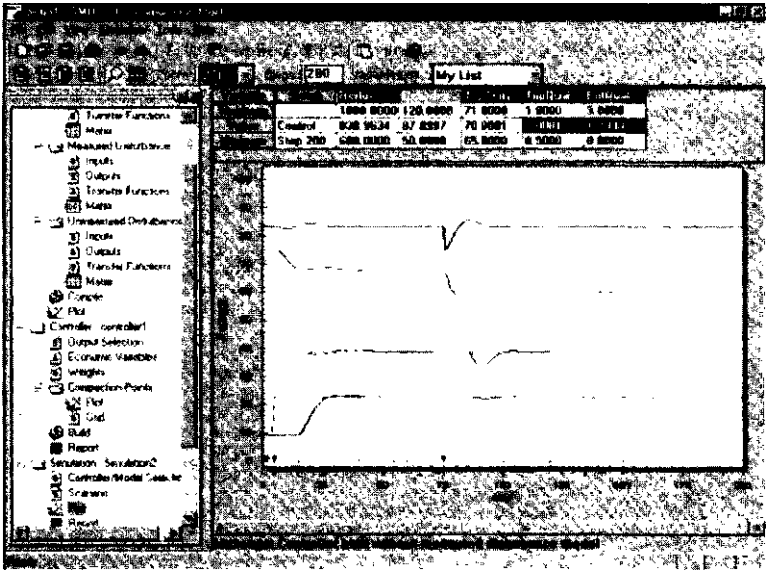


Рис. 12.24

Если температура по верху объявлена как внутренняя переменная, контроллер немедленно произведет управляющие воздействия по расходу флегмы, как только обнаружит отклонение температуры.

Контролируемой переменной, естественно, остается концентрация ключевого компонента по верху. В результате предваряющая корректировка орошения предпринимается до того, как концентрация изменится.

Более того, упреждающий контроллер "помнит", что действия по корректировке орошения уже предприняты, и не реагирует на проявившиеся изменения концентрации. В итоге отклонение концентрации от задания становится минимальным.

Единственное, что остается упущенным, - это неоправданный проскок по расходу флегмы (вторая кривая на рис. 12.24) из-за того, что отсутствует фильтрация помех на основе модели возмущений.

Очень важным элементом системы управления является жесткость, устойчивость (*robustness)* алгоритма управления к воздействию случайных неконтролируемых возмущений. Контроллер должен иметь способность к самообучению на основе анализа действительного уровня помех с процесса. Данная проблема решается с применением эталонной модели. Если контроллер построен без учета модели возмущений, и работает без эталонной модели, то любые изменения в процессе приводят к потере контроля над процессом (рис. 12.25).

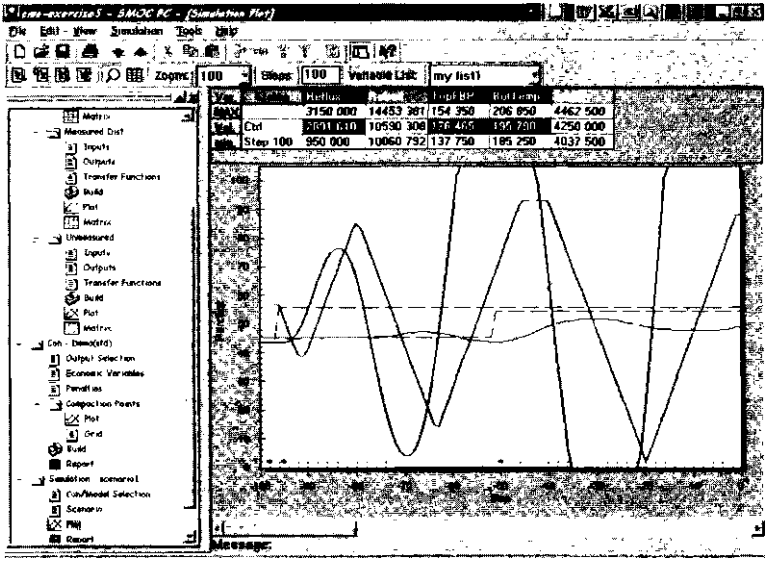


Рис. 12.25

Контроллер полностью вывел процесс из равновесия. Причиной такого поведения явились незначительные ошибки измерения и неконтролируемые возмущения процесса.

С использованием эталонной модели выход идеального контроллера сглаживается, и процесс сохраняет устойчивость (см. рис. 12.26).

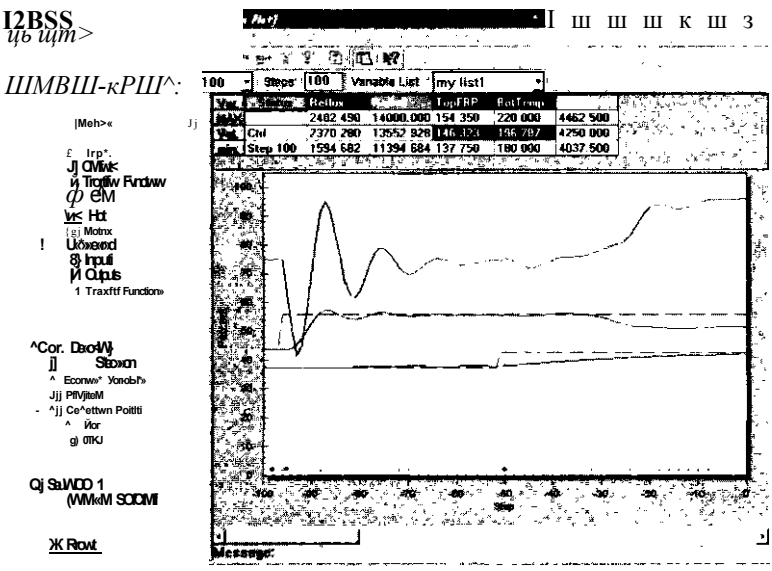


Рис. 12.26

В данном примере контроллер анализирует разницу между фактическим поведением объекта и предсказанным на основе модели. При этом контроллер плавно делает управляющие воздействия, невзирая на возмущения и ошибки измерения.

Представленные примеры наглядно демонстрируют и громадные возможности, заложенные в современные методы управления, но одновременно и опасности, которые подстерегают при их некорректном применении. **Чтобы эффективно заниматься усовершенствованным управлением, требуются специалисты, хорошо знающие и понимающие и процесс, и математику.** С **сожалением остается добавить, что если сами специалисты этого не осознают, то появиться им в нынешней жизни будет неоткуда.**

Пока сконструированный контроллер испытывается в автономном режиме, он работает в идеальных условиях:

- На идеальном технологическом оборудовании,
- Без влияния реальных возмущений и флуктуаций,
- Без учета неопределенностей технологического процесса.

Никакие самые значительные усилия разработчика модели не могут быть чрезмерными для того, чтобы учесть все внешние обстоятельства при работе контроллера в реальных условиях.

Реальные данные с процесса подвержены влиянию множества возмущений:

- Дрейф и флуктуации измерительных устройств;
- Влияние неконтролируемых возмущений, которые невозможно моделировать (например, действие микропримесей, отравляющих катализатор);
- Пусть частичная, но неизбежная неадекватность модели.

Что же можно "противопоставить" реальным обстоятельствам?

Решение этой проблемы находится в использовании реального отклика с технологического процесса в качестве обратной связи контроллера.

На практике существует множество случаев, когда изменение одной из переменных процесса является косвенным показателем изменения другой переменной.

В нашем случае таким примером является связь между температурой наверху колонны и концентрацией верхнего погона. И, вообще говоря, целевым параметром управления будет именно концентрация сверху, а управляющим - расход орошения. Тогда рабочая модель должна быть разработана с учетом связи между орошением и концентрацией. Вдобавок должна быть предусмотрена связь между концентрацией и верхней температурой.

Связь между температурой и орошением должна быть встроена в модель неконтролируемых возмущений. Эффект будет таков, что контроллер будет изменять расход флегмы при изменении температуры, не дожидаясь изменения концентрации. При этом температура по верху колонны не будет ни контролируемой переменной, ни управляющей.

Эта температура будет промежуточной переменной, которая является своего рода индикатором для стабилизации качества верхнего продукта.

Одна из реальных причин неудач при попытке внедрить упреждающее управление по модели заключается в том, что разработчик стратегии управления не знает, не понимает, и не чувствует сущности технологического процесса. Как результат - несоразмерность и несогласованность различных уровней управления между собой.

Типичным примером служит отсутствие динамической синхронизации между алгоритмом АРС и локальным регулированием:

АРС дает новое задание локальному регулятору, и остается в убеждении, что к следующему такту это задание будет выполнено. На следующем такте выясняется, что контролируемая переменная так и не приняла заданное значение. Контроллеру АРС невдомек, что причина состоит в инерционности локального регулятора - он просто не успел отработать предыдущее задание. Контроллер АРС принимает более жесткое решение, и увеличивает задание регулятору. В итоге процесс выходит из-под контроля.

Одно из возможных решений данной проблемы - ввести локальный регулятор в состав и под контроль модели АРС.

Эффективным средством повышения устойчивости упреждающей модели служит моделирование неконтролируемых возмущений с помощью матрицы наблюдений. После того, как матрица наблюдений пропускается через фильтр Калмана, случайные флуктуации отвергаются, а действительные отклонения учитываются упреждающим контроллером. Дополнительным средством повышения устойчивости служит эталонная модель (фильтр первого порядка), которая может быть быстро настроена *on-line*. Это весьма эффективный альтернативный способ отслеживания заданного значения и отсева возмущений.

Существенным элементом хорошего пакета АРС является способность сохранять работоспособность при отказе или недостоверности измерительных устройств. Это свойство не просто адекватности, а структурной устойчивости модели и является тем качеством, которое определяет ее практическую ценность.

12.14. АРС на установке каталитического крекинга

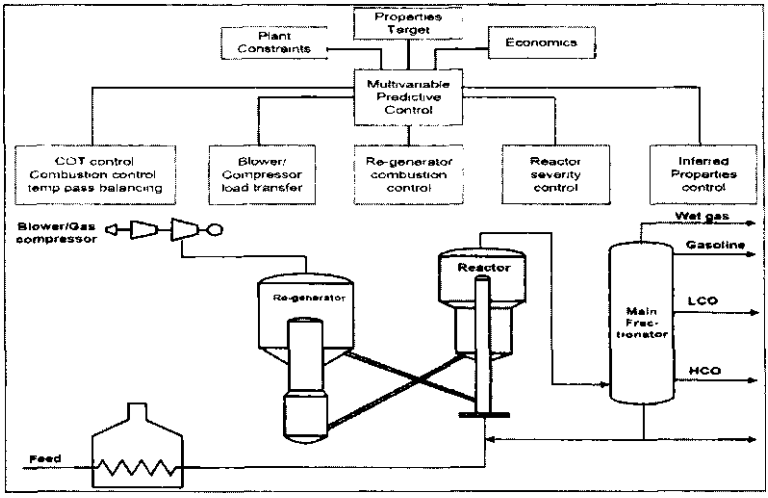


Рис. 12.27

Установка каталитического крекинга представляет собой прекрасную возможность для демонстрации эффекта стабилизации процесса и экономической выгоды при умелом применении усовершенствованного управления.

Знание особенностей процесса позволяет обойти многие из существующих проблем управления:

1. Сырьем для установки является смесь тяжелых нефтей, поэтому поточный анализ состава сырья невозможен.
2. Каталитический крекинг проходит с множеством побочных реакций высокомолекулярных и ароматических углеводородов, затрудняющих выбор технологического режима для повышения выхода целевых продуктов.
3. Хотя активность катализатора является одним из важнейших показателей, его очень сложно определить.
4. Скорость коксования змеевиков оказывает решающее воздействие на состав выходов реактора, но предсказать ее крайне сложно.

5. Критическим параметром установки является давление. Влиянием давления определяются выходы реактора, эффективность укрепляющей колонны, выгорание кокса, энергопотребление компрессора и т.д.
6. На неопределенность технологических переменных накладываются специфические особенности процесса:
   - Наличие тяжелого вращающегося оборудования;
   - Выход реактора представляет собой сложную смесь углеводородов, которая требует сложного анализа;
   - Питание главной колонны фракционирования находится в перегретом состоянии, и его истинный расход и состав также непросто измерить;
   - Унос катализатора в виде твердых частиц, и их присутствие в жидких и газовых потоках создает проблемы с отложениями в теплообменниках;
   - Температурные ограничения, накладываемые конструкционными материалами;
   - Реакционные процессы представляют собой множество экзотермических и эндотермических реакций. Следовательно, система управления должна строиться с учетом массового, теплового баланса, и баланса давлений.

Технология управления установкой каталитического крекинга должна создаваться не только для преодоления всех трудностей, описанных выше, но и для расширения рабочего диапазона и лучшей управляемости с целью:

1. Увеличения производительности установки;
2. Увеличение жесткости крекинга;
3. Уменьшение потребления энергоресурсов;
4. Увеличение степени извлечения целевых продуктов.

12.15. Управление реактором и регенератором

Управление расходом сырья. Подача сырья в реактор лимитируется несколькими ограничениями:

- Производственное задание;
- Давление на всасе компрессора;
- Ограничения воздушного компрессора;
- Ограничения колонны фракционирования и т.д.

Управление режимом регенератора.

Стратегия регенерации катализатора заключается в управлении выжигом кокса с максимизацией активности катализатора и без нарушения физических ограничений регенератора.

Управление нагрузкой газового компрессора.

Эта стратегия заключается в максимизации производительности газового компрессора для снижения давления реактора и колонны фракционирования. Это позволяет регулятору перепада давления реактор/регенератор перенести нагрузку на воздушный компрессор.

Управление подачей воздуха.

Эта стратегия должна минимизировать давление регенератора, давая возможность увеличить подачу воздуха на сжигание. Это позволит увеличить пропускную способность или поднять конверсию.

12.16. Управление главной колонной фракционирования

Цель управления главной колонной фракционирования заключается в разделении продуктов реакции на промежуточные компоненты, которые при дальнейшей переработке превратятся в конечную продукцию.

Поскольку сырьем для колонны фракционирования является перегретый газовый поток, колонна является главным источником рекуперации энергии.

Основные принципы работы колонны фракционирования являются общими для всех процессов разделения, но есть существенные отличия:

1. Питание колонны и продукты разделения - это сложные многокомпонентные смеси, которые гораздо труднее поддаются фракционированию, чем легкие компоненты.
2. Кроме ключевых компонентов разделения, производится множество побочных продуктов и по верху и по кубу колонны.
3. Питание подается снизу колонны в перегретом газообразном состоянии, и само по себе является носителем тепловой энергии.

4. Поэтому колонна фракционирования, в отличие от большинства ректификационных колонн, не нуждается во внешних источниках тепловой энергии.
5. Профили скоростей жидких и газовых потоков внутри колонны сильно меняются в силу сложного механизма массообмена и удаления тепла с помощью боковых ребойлеров.
6. Внутренняя конструкция колонны является нетрадиционной, в особенности нижняя часть колонны, в которой присутствует катализатор.

12.17. Эффективность АРС на каталитическом крекинге

Поскольку производительность установок каталитического крекинга очень высока, даже незначительное улучшение приводит к существенному экономическому выигрышу.

Эффект, полученный на конкретном узле, зависит от эффективности работы самого узла и всей установки в целом.

Общий результат применения алгоритмов усовершенствованного управления и не только на установках каталитического крекинга, но и на многих других химических, нефтехимических и нефтегазоперерабатывающих производствах складывается из следующих преимуществ:

- **Увеличение производительности установки на 1-10%;**
- **Увеличение выхода целевых продуктов на 5-15%;**
- **Плавный и быстрый перевод установки на новую нагрузку.**
  Время перехода на новую нагрузку сокращается на 20-60%;
- **Уменьшение потребления энергии и производственных затрат на 1-5%;**
- **Увеличение пробега установки за счет точного выдерживания технологического режима и соблюдения всех ограничений до 10%;**
- **Повышение стабильности технологического режима в 1.5 раза;**
- **Увеличение безопасности установки.**

12.18. Решения в области добычи нефти и газа
(по материалам фирмы Honeywell)

В данном разделе описаны требования и современные решения по созданию автоматизированного интеллектуального месторождения, а также возможности Honeywell по обеспечению заказчиков аппаратными средствами и технологиями, отвечающими этим требованиям и реализующими соответствующие решения.

Современные системы реального времени способны собирать множество технологических данных и показателей хода производственных процессов, таких как расходы, температура, давление и т.д. DCS или SCADA системы обеспечивают основу для этих функций. Необходимость в этих системах и уменьшение их стоимости за последние годы определили то, что внедрение и модернизация этих систем стали обязательной частью разработки новых, и развития действующих автоматизированных месторождений.

Автоматика и надзор - местный и дистанционный. Центр управления включает DCS или SCADA систему управления, которая наблюдает за всем оборудованием от скважин и кустов до промыслового пункта подготовки нефти.

Honeywell's Digital Video Manager (DVM) позволяет операторам постоянно следить визуально за всеми операциями. DVM интегрирован с Experion PKS и системой безопасности - EB1. Инструменты операторов, такие как беспроводные Tablet PC's также как портативные PC's могут быть использованы операторами для сбора информации в процессе их обходов. Эти приборы могут быть беспроводными, дают полный доступ к дисплеям системы управления и обеспечивают связь между производством и командами ремонтников.

Honeywell's IntelliTrac и Mobile PKS обеспечивают наиболее широкие возможности. Неизмеряемые величины, такие как ручные установки заслонок, коррозионная инспекция, отчеты по вращающимся механизмам, инструкции операторов могут быть введены и использованы в этих устройствах.

Мониторинг потоков. Динамическая модель потоков на сети трубопроводов от скважин, кустов к промысловым пунктам сбора, дожимным и кустовым насосным станциям (ДНС и КНС) может также использоваться, чтобы дать раннее преду-

преждение об изменениях в процессе из-за утечек, прорывов воды, остановках скважин и т.п.

Технологическая безопасность. Возможность выключения оборудования безопасным образом при нештатных ситуациях - обязательная часть хорошей работы оборудования. Система безопасности, называемая Emergency Shutdown System (ESD) или Safety Instrumented System (SIS), должна иметь высокую вероятность срабатывания в случае необходимости.

Измерения. Измерение добычи требует точности и компенсационных вычислений при обмене потоками между компаниями, партнерами. Это еще более важно в местах раздела продукции, областях с несколькими владельцами скважин или кустов. Очень вероятно, что государственные органы хотят иметь записи о продукции для фискальных целей.

Во многих случаях фискальные измерения реализуются в автономных системах, с их собственными базами данных, графикой, системами ввода-вывода. Такие системы изолированы исторически, чтобы сохранять любые изменения отдельно и быть уверенным в высокой точности компенсационных вычислений.

Контроль утечек. Контроль утечек в системе промысловых трубопроводов и трубопроводов по перекачке нефти от промыслов пунктов сбора до магистральных трубопроводов представляет собой очень важную задачу.

Honeywell предоставляет заказчикам современную акустическую систему определения утечек ALDS. ALDS является проверенной на практике технологией обнаружения и определения положения утечек. ALDS на сегодняшнее время является единственной системой низкого уровня с подтвержденным временем послужным списком по успешной обработке ложных срабатываний, что требуется для полностью автоматического отключения задвижек трубопроводов. Акустическая система определения утечек (ALDS) разработана для обнаружения и определения координат утечек в жидкости, газе и для двух фазных течений.

Контроль коррозии. Возможности Honeywell включают уникальные измерения уровня коррозии в выбранной точке процесса или трубы. При этом информации становится доступной немедленно. В добыче нефти и газа это значит, что изменения в уровне коррозии на основном оборудовании мо-

гут стать известными немедленно. Это переводит управление коррозией от спорадических проверок оборудования к непрерывному отслеживанию процесса коррозии.

Охрана - устройства, системы, компьютерные решения. Физическая защита стала областью пристального внимания за последние несколько лет. Мотивы этого заключаются в необходимости защиты от вмешательства третьей стороны, нежелательного проникновения на объект, предотвращения порчи оборудования, воровства оборудования или подделки. В нефтяной и газовой промышленности удаленное размещение является частью бизнеса, поэтому требуется особое внимание к охране. Удаленность объектов требует использования IT и коммуникационных сетей.

Универсальный Центр Управления. Для мониторинга технологических процессов и поддержки принятия решений при управлении нефтегазодобывающими производствами и трубопроводами концерном Honeywell разработан специализированный программный пакет **Production Control Center** (PCC). Будучи по сути интегрирующей средой, PCC позволяет объединить различные функциональные приложения в единую информационное пространство, обеспечивающее визуализацию производственных параметров и управление процессами одновременно. PCC является оболочкой, предназначенной для интеграции не только ряда специализированных приложений, но и для совместной работы с другими приложениями фирмы Honeywell семейств Business.FLEX (приложения для производственного управления, MES), ProfitPLUS (усовершенствованное управление технологическим процессом - APC) и т.д. Это часто требуется для эффективной работы операторов технологического процесса.

Программные средства других поставщиков решений также могут быть интегрированы в PCC. Основные данные и результаты работы этих приложений включаются как в общие отчеты (например, журнал смен операторов), так и в экранные формы (например, экран общего обзора). Средства контроля доступа PCC распространяются и на эти приложения.

Приложения PCC. Ниже указаны лишь основные приложения Production Control Center, типичные для систем производственного управления нефтегазодобывающими производствами и трубопроводами.

Production Event Analyzer — анализ и отчеты по событиям, сгенерированным системами DCS и системами обеспечения безопасности. Данный инструмент позволяет создавать специальные фильтры, позволяющие в значительной мере ускорить поиск требуемой информации, хранящейся в базе данных, что обеспечивает повышение эффективности работы операторов, технологов и инженеров.

Safety Module - модуль контроля производственной безопасности. Safety Module представляет собой программное средство, позволяющее анализировать в заданные пользователем промежутки времени и отображать значения тэгов, критичных для контроля безопасности производственных процессов. Возможна фильтрация по именам и описаниям тэгов, поиск по различным зонам их ответственности (например, процедура останова насосного оборудования) и т.д.

Shutdown Analyzer - анализ отключений. Данное программное средство позволяет осуществлять мониторинг и создавать отчеты по процедурам полного или частичного отключения оборудования. В его функции входит:

- Отслеживание всех активных отключений
- Группировка возможных отключений по иерархическим уровням
- Поиск и анализ событий, ставших причинами отключений
- Диагностика всех сконфигурированных при настройке "ожидаемых эффектов" для каждого уровня отключений
- Отслеживание корректности исполнения операций отключения и контроль состояний исполнительного оборудования

Safety Valve Scout - диагностика клапанов безопасности. Позволяет постоянно в оперативном режиме контролировать исправность клапанов, задействованных в процедурах экстренных и плановых отключений.

Исправность клапанов определяется как соответствие их паспортных и реальных параметров (время отклика, скорость открытия/закрытия и т.п.). Результаты анализа фиксируются в отчетах: текущие параметры клапанов, список неисправных клапанов, частота отказов с разделением по уровням отключений, детальный отчет по каждому клапану и др.

Production Summary Screen - экранная форма контроля производственных показателей.

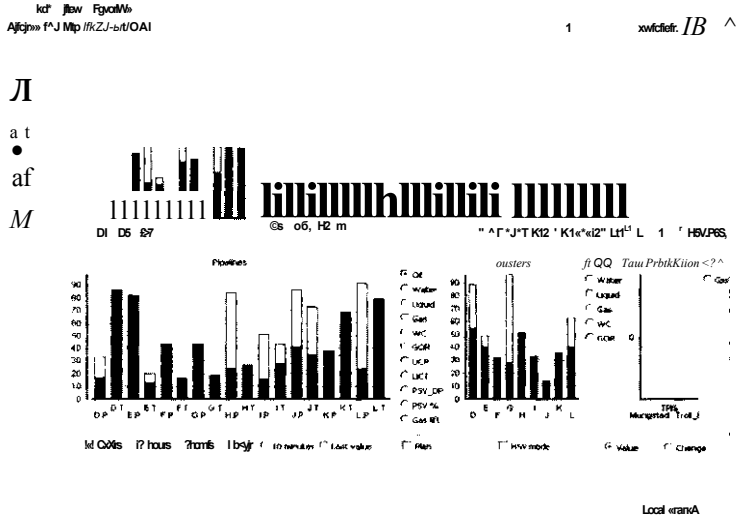


Рис. 12.28

Отражает состояние производственных показателей, сконфигурированных в ходе настроек системы. Позволяет контролировать состояние всех производственных процессов и оборудования на одном экране.

Trending - средство работы с трендами. Позволяет отображать тренды технологических параметров с использованием цветовой маркировки, изменять масштабы и временные диапазоны и т.п. (рис. 12.29).

Operations Monitoring - средство отслеживания исполнения производственных процедур. Предназначено в первую очередь для начальников смен операторов и позволяет авторизованному персоналу создавать отчеты по отклонениям показателей производственных параметров в зоне их ответственности, а также вводить причины этих отклонений.

Применение Operations Monitoring позволяет в конце каждой смены осуществлять анализ соответствия выполненных производственных процедур предварительному плану и, при

необходимости, отмечать выделять процедуры, требующие отдельного анализа со стороны технологов и инженеров.

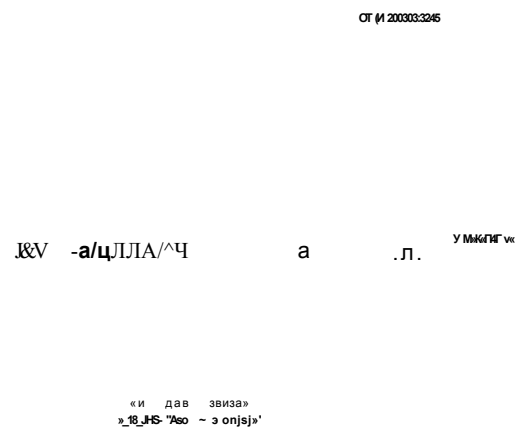


Рис. /2.29

Комплексное решение по автоматизации терминалов (Terminal Automation Solution)

Данное решение представляет собой проект по автоматизации работы нефтебазы. Опыт компании Honeywell позволяет предлагать клиентам апробированные, технически совершенные, комплексные решения в этой области.

Контрольные и технологические системы:

- Контроль состояния резервуаров (включая автоматическую работу с уровнемерами и пр.);
- Контроль потоков (включая автоматическую работу с расходомерами, автоматическими клапанами и т.д.);
- Системы взвешивания.

Системы безопасности и наблюдения:

- Системы контроля доступа (включая контроль доступа на территорию);
- Система безопасности нефтебазы (в т.ч. противопожарная система);
- Система противоаварийной защиты слива/налива;

- Управление системой передвижения по нефтебазе;
- Система наблюдения (включая автоматическое видеонаблюдения и видеозапись, в т.ч. событийную).

Информационная система:

- Инфраструктура (серверы, рабочие станции, периферийное оборудование, контроллеры, программное обеспечение и т.д.);
- Работа с корпоративными информационными системами (ERP).

Комплексное решение для автоматизации работы сети АЗС. Комплексное решение для автоматизации работы сети АЗС включает в себя следующее:

- Автоматизацию работы розничных продаж на АЗС (мониторинг, офис АЗС, поддержка различных средств продажи, управление стоимостью и т.д.);
- Автоматизация работы центрального офиса по эксплуатации сети АЗС (централизованное управление сети АЗС, управление ценообразованием, контроль, управление маркетинговыми программами, финансовая отчетность, интеграция с ERP и т.д.);
- Расширение спектра услуг и автоматизация по обслуживанию корпоративных клиентов (fleet management system) АЗС (дополнительные услуги для транспорта корпоративных клиентов, включая расширенный контроль и дополнительные услуги).

Внедрение. Одним из преимуществ описанного выше модульного подхода к автоматизации управления предприятием является возможность поэтапного внедрения функциональных систем. Безусловно, первым этапом является внедрение системы информационной поддержки и построение адекватной референтной модели предприятия.

Этот процесс достаточно трудоемок и требует существенных временных затрат. В то же время он не является очень сложным, на этом этапе активное участие в работах принимают специалисты предприятия, обученные Honeywell и разрабатывающие модель под руководством специалистов Honeywell. Такой подход позволяет значительно сократить стоимость этапа (в зависимости от количества интерфейсов к оборудованию АСУТП, степени детализации модели и т.д.).

Дальнейшая последовательность этапов внедрения определяется важностью решаемых задач для конкретного предприятия и компании, а также с учетом уже имеющихся и активно используемых элементов. Как уже отмечалось выше, модульность является несомненным преимуществом решений Honeywell, позволяющим проводить постепенное внедрение и наращивание системы производственного управления. Ряд систем может внедряться параллельно, независимо друг от друга. Honeywell проводит весь комплекс работ по разработке дизайна решения, его внедрению, обучению пользователей, а также обеспечивает его сопровождение и поддержку в течение всего жизненного цикла.

12.19. Оптимизация

Термин, который для многих разработчиков и практиков давно стал синонимом дискредитации. Однако если не замахиваться на высоты динамической оптимизации, то реальный эффект статической оптимизации все же достигается.

На рисунке 12.30 представлено процентное соотношение затрат и эффектов для основных уровней управления по данным Yokogawa Electric Corporation, Tl 36J06D10-01E, "Advanced process control solutions", October 2001.

Возврат инвестиций (по данным фирмы Yokogawa)

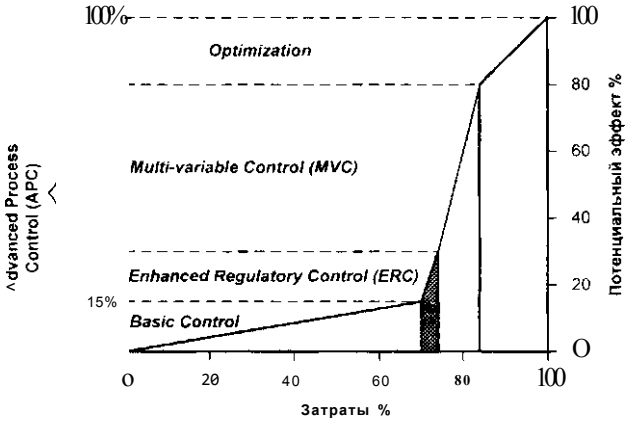


Рис. 12.22

1. Первичное внедрение РСУ (начальные инвестиции) - Базовая система управления:

- Повышение безопасности эксплуатации;
- Снижение эксплуатационных издержек;
- Более стабильное качество продукции;
- Повышение эффективности работы операторов.

Результат - 30% потенциальной прибыли от 70% затрат.

2. Перспективные возможности РСУ (реальные преимущества пользователя) - Усовершенствованное управление:

- Полное использование функционштьных возможностей;
- Максимальная стабильность и рентабельность установки (АРС, оптимизация);
- Оптимальная интеграция с уровнем управления производством;
- Уменьшение воздействия на окружающую среду.

Результат ~ 70% потенциальной прибыли от 30% затрат.

Возврат инвестиций (по данным фирмы Honeywell)

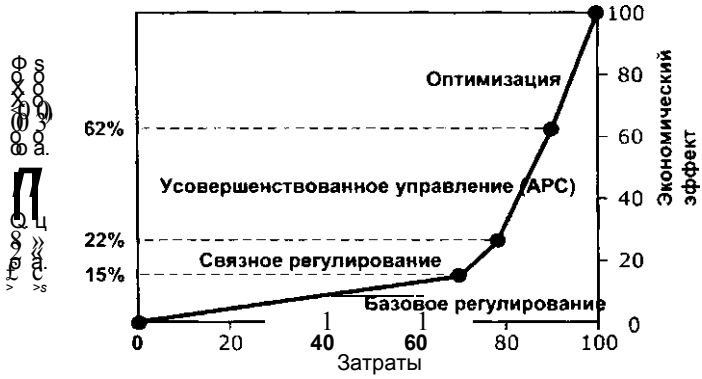


Рис. 12.31

1. Первичное внедрение РСУ (начальное капиталовложение) - Базовое и связное управление:

- Повышение безопасности эксплуатации;
- Снижение эксплуатационных расходов;
- Более стабильное качество продукции.

Результат - 22% потенциальной прибыли от 80% затрат.

2. Дальнейшее развитие РСУ (реальная прибыль заказчика) - Усовершенствованное управление:

- Повышение эффективности управления процессом;
- Максимизация стабильности и рентабельности установок (APC);
- Оптимальная интеграция с уровнем управления производством;
- Улучшение экологических показателей.

Результат - 78% потенциальной прибыли от 20% затрат.

12.20. Необходимые условия получения прибыли

Предпосылками успешного внедрения систем усовершенствованного управления являются:

- Современные СИ и СА;
- Современная распределенная система управления;
- Устойчивое базовое регулирование: непосредственная реализация проектов APC должна начинаться "снизу": с проверки и настройки системы локального и связного регулирования. Часто только эти мероприятия уже приносят ощутимый экономический эффект
- Экономические данные о работе технологического процесса;
- Хорошо организованный проект. Проект внедрения APC, конечно, требует материальных затрат, однако, не настолько больших, как, например, приобретение дорогостоящих многопоточных анализаторов.

Преимущества внедрения усовершенствованного управления производством

- Коммерческие преимущества
- Повышение безопасности процесса
- Повышение межагрегатной устойчивости
- Повышение эффективности работы операторов
- Повышение качества оперативной информации
- Снижение воздействия на окружающую среду.

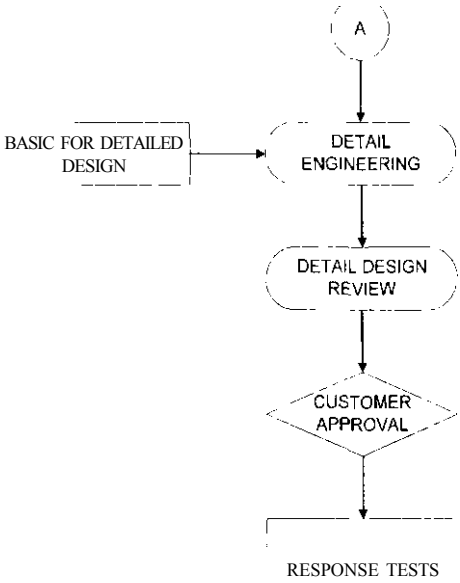
В завершение главы в таблице 12.1 приводится рекомендованная фирмой Yokogawa Electric процедура создания системы усовершенствованного управления по этапам.

Таблица 12.1

Этапы проекта создания системы усовершенствованного управления

	START	После заключения договора на поставку пакета усовершенствованного управления создается команда разработчиков в составе - Руководитель проекта - Инженер-технолог - Инженер АСУТП - Инженер КИПиА
	KEEK OFF MEETING j	На стартовой встрече между Разработчиком и Заказчиком согласовываются вопросы. - Организация проекта. - График выполнения Проекта. - Каналы взаимодействия.
	Benefits Estimation	Определяются экономические критерии качества проекта и оценивается потенциальный экономический эффект на основе: - Текущих экономических показателей - Архивных данных процесса - Лабораторных данных.
CUSTOMER SPEC ON I QUALITY STRATEGIES !"1		
	BASIC SYSTEM DESIGN	На основе исходных данных выполняется предварительный (базовый) проект.
Г P&ID EQPT DRGS П		
	BASIC DESIGN REVIEW \ J	Базовый проект подвергается экспертизе Заказчика и после уточнений утверждается для детального проектирования.

Продолжение таблицы 12А



6 В процессе разработки рабочег о проекта выполняется*
- Конфигурирование исходных данных
- Проектирование ЧМИ
- Проектрование технического обеспечения

7. В детальном проекте учитываются всс замечания базового проекта.

8 Перед испытаниями модели на площадке предпринимаются следующие действия
- Утверждаются процедуры проведения испытаний
- Проверяется готовность и работоспособность полевого и технологического оборудования.

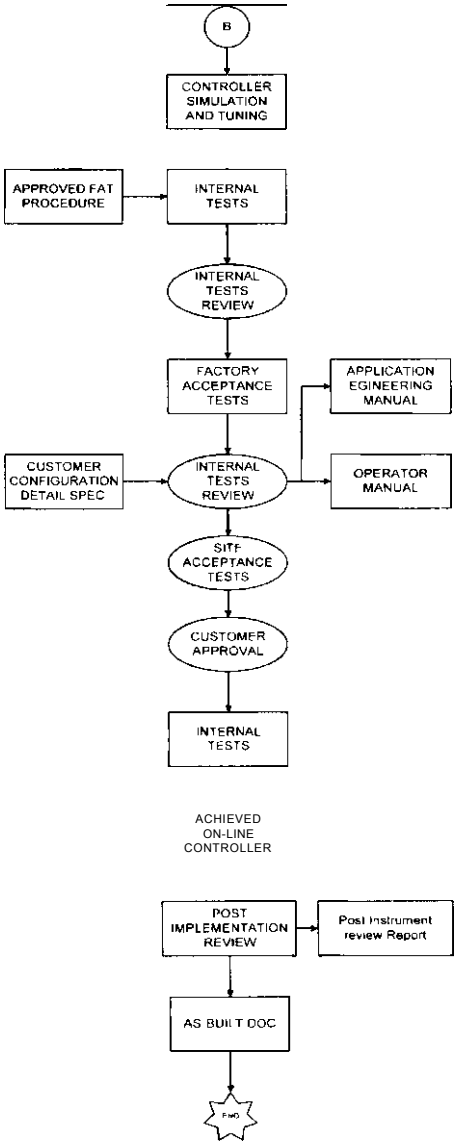
На следующем этапе в течение как минимум 24 часов проводятся полевые испытания Системы.

9. В результате испытаний генерируется идентифицированная модель установки. Формируются динамические связи переменных состояния и управления.

10 Модель проходит испытания на адекватность в составе контроллера в режиме off-line Работоспособность контроллера проверяется на и вмене-ние заданных значений, измеряемых и не измеряемых возмущений, и подстраивается.

11 ГЧ'зультатом является настроенный контроллер, который можно опробовать в режиме реального времени.

Окончание таблицы 12.1



12. На следующем этапе строится, отлаживается и окончательно настраивается контроллер реального времени с разработанной моделью.

Проводится автономное тестирование

Проводятся приемосдаточные испытания на площадке Разработчика системы Присутствие Заказчика на этих испытаниях крайне желательно. Выпускается проектная документация

После приемки системы на площадке Разработчика проводятся испытания системы на площадке Заказчика.
- Загружаются параметры контроллера, и запускается пробег в режиме предсказания.
- Проверяется точность предсказания модели.
- Если динамическая модель настроена корректно, запускается контроллер реального времени.

16. В результате опытных испытаний в течение 2 месяцев оценивается полученный экономический эффект

Глава 13

ВЫБОР И ПОСТРОЕНИЕ НАДЕЖНЫХ И ЭФФЕКТИВНЫХ АСУТП

13.1. Принципиальные источники отказов

На протяжении всей работы неоднократно звучал тезис, что принципиальные источники отказов были, и остаются в поле. Различные источники дают разные оценки соотношения отказов логических устройств и полевого оборудования. Но все сходятся в том, что главные причины отказов систем безопасности - полевое оборудование. Опубликованные оценки соотношения интенсивности отказов логических устройств и полевого оборудования колеблются от 15:85 до 5:95. Тем самым утверждается, что вероятности отказов полевого оборудования и логического устройства соотносятся практически на порядок. Причем доля ложных отказов смещена в сторону сенсоров, а доля опасных отказов - в сторону исполнительных элементов.

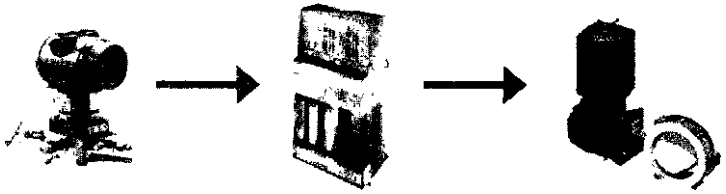
E.R. Bruyn, Exxon Mobil Refinery, в докладе "*Asset Management & Safety Instrumented Systems"* на семинаре *"The Role of Instrumentation in Plant Asset Management*International Instrument User's Association, 2003, приводит просто удручающие значения (рис. 13.1).

Чтобы сразу обозначить авторскую позицию и задать тональность дальнейшего обсуждения, выскажем следующее замечание.

Существенное замечание

Данные типа тех, что представлены на рис. 13.1, кочуют из работы в работу, и уже стали общим местом. Остается только выяснить, насколько достоверными являются значения рис. 13.1, и что они собственно означают.

Если судить по упомянутому отчету, то на рис. 13.1 представлено процентное соотношение интенсивностей отказа по всей совокупности оборудования.



Датчики 40% **Контроллеры 5%** **Клапаны 55%**

Рис. 13.1

В таком случае возможен и иной взгляд на искусство:

- *Отказ одного из множества датчиков ~ это в худшем случае отказ ОДНОЙ функции защиты из множества имеюгцихся функций защиты.*
- *Отказ одного логического устройства - это отказ одного логического устройства из ОДНОГО имеющегося, а значит, в лучшем случае отказ множества функций.*

Кроме эффектных картинок типа рис. 13.1 существуют вполне серьезные и достоверные источники данных об интенсивности и вероятности отказов оборудования систем управления и защиты. Авторитетнейшая норвежская ассоциация нефтяной промышленности OLF (The Norwegian Oil Industry Association) в своих "Руководящих материалах по применению IEC 60508 и IEC 61511 в нефтедобыче на норвежском континентальном шельфе" приводит собственные значения интенсивности и вероятности отказа различных компонентов автоматизированных систем (см. таблицы 13.1 и 13.2). Обращает на себя внимание искчючительный уровень источников данных:

- *Reliability Data for Control and Safety Systems (PDS);*
- *SINTEF data / includes the failure modes;*
- *Reliability data of components in Nordic nuclear power plants;*
- *OREDA - Offshore Reliability Data Handbook.*

Таблица 13.1

Базовые интенсивности отказов

Component	Failure rate W * 1 0 ^{6})	TIF-lest independent Failure Probability	Data sourcc/comments
Pressure transmitter	0 1	3M0-^{4} " 5*10 ^{4}	Reliability Data for Control and Safety Systems, 1998 Fdition (PDS) [11] For smart transmitter "'For standard transmitter
Level transmitter	0 1		
Temperature transmitter	0 i		
Smoke detector	0 8	-*)	Reliability Data for Control and Satety Systems, 1998 Edition (PDS) Coverage of self-test has increased during the last years, and in particulai the rate ot the flame detector now seems high *) No TIF values are given tor the detectors since the definitions of F&G functions in table 7 1 assume exposed detector, whereas the TIFs given in PDS include the likelihood of the detector not being exposed
Heat detector	0 5		
Flame detectors, conventional	2 1		
Gas detector, catalytic	0 6		
IR Gas detector, Conventional pomt detector	0 7		
IR Gas detector, Line	0 7		
PLC including I/O card (single PLC)	**1.6**	5*10 * " 5*10^{4} ^{2}>	Reliability Data for Control and Safety Systems, 1998 Edition (PDS). Experience indicate that this failure rate is high, e.g. compared to the FTO rate of valves " For TUV certified PLC [2] For standard PLC
XV/ESV inci actuator	1 3	1*10*	Reliability Data for Control and Safety Systems, 1998 Fdition (PDS) Same failure rate for blowdown valves as tor ESVs has been assumed " hor complete functional testing [1] For incomplete functional testing
Blowdown valve inci actuator	1 3		
X-mas tree valves Wing valve (WV) Master Valve (MV)	0 8		
Down Hole Safety Valve - DHSV	2 0		Internal SINTTF data/includes the failure modes Fail To Close (FTC) and leakage in closed position
Solenotd/pilot valve	1 4		Reliability Data for Control and Safety Systems, 1998 Edition (PDS)
Circuit Breaker < 600V	0 34		T-Boken "Reliability data of components in Nordic nuclear power plants", rev 3
Circuit Breaker 6 KV - 10 KV	0 18		
Fire water pump	1 critical failure, 400 demands, Probfail to start = 2 5* 10		OR EDA 97, 13 13
Deluge valve including actuator, solenoid and pilot valve	Prob fail to open=5*10 ^{1}		This value is better than the observed, but increased testing should make this value realistic

Источник информации - OLF Recommended Guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf 01.02.2001.

Таблица 13.2

Сводная таблица надежности компонентов

Component	Test interval т, (months)	Failure rate, / DU per 10^6hrs	PFD	TIF-Test Independent Failure Probability	p-factor [5]
Pressure transmitter	12	0 1	**0 44*10 '**	**3*!0^4** [2]	**2% (5% for TIF)**
I cvel transmitter	12	0 1			
1 emperature transmitter	12	0 1			
Smoke detector	12	08	3 50*10'	**5*10^4** [2]	**5% (20% for TIF)**
Heat detector	12	0 5	2 19*10'		
blame detectors, conventional	12	2 **1**	920*10^3		
Gas detector, catalytic	12	06	2 63*10^3		
IR Gas detector. Com point detector	12	07	**3 07*10^1**		
IR Gas detector. Line	12	07			
PLC including I/O card (single PLC)	**6**	**1.6**	**3.50*10^3**	**1*10"***	**1% (50%)**
XV/hSV incl actuator	6	1 1	2 85*10 *	**5* 10^6**	**2% (5% for TIF)**
Blowdown valve inci actuator	6	I 3 "	2 85*10 '		
X-mas tree valves (WV, MV)	6	08	1 75*10^3		
Down Hole Saiety Valve - DHSV	6	20	4 W 0 ^{1}	5*10"* [3]	-
Solenoid/pilot valve	6	1 4	3 07*10^1	.[4]	2%-10% [6]
Circuit Breaker < 600V	24	0 34	2 98*10^3		
Circuit Breaker 6 KV - !0 KV	24	0 18	1 58*10^1		
Fire water pump, (fail to start)			2 5*10^1	-	5%
Deluge valve incl actuator, solenoid and pilot valve, (fail to open)			5 0*10^3		*

[1] Use the same KTO rate as for XV/ESV even if this another failure mode (here Fail-To-Open)

Suggested TIF-probability, given exposed detector

[2] It is suggested to use same TIF-probability as for XV/ESV

[4] T1Г-probability ior pilot is included m figure for main vahe/actuator

Value applies to dangerous undetectable random hardware failures (duplicated system) Values in parenthesis apply for systematic failures (TIF)

[6] for pilot valves on the same valve, otherwise fi=2%

Таблицы дают ясное представление о том, что надежность одноканального PLC вполне сопоставима с надежностью периферийного оборудования. Если же межтестовый интервал будет увеличен с шести месяцев до одного года, то вероятность опасного отказа контроллера вырастет ещё в два раза. Стоит еще раз поразмыслить над кем-то кому-то "разрешенным" одноканальным вариантом PLC (см. главу 1, раздел 1.11 *"Применимость одноканальных систем"*).

Но как бы то ни было, проблема оперативного обнаружения отказов полевого оборудования всегда будет сохранять свою актуальность. Поскольку для непрерывных (да и реальных периодических) процессов невозможно провести полно-

ценное функциональное тестирование полевого оборудования без останова производства, в последние годы бурное развитие получает направление, которое в конечном итоге связывают с возможностью оперативной диагностики полевого оборудования в режиме *on-line.*

13.2. Тестирование полевого оборудования в реальном времени

Если вернуться к вероятности опасного отказа (несрабатывания) единичного элемента оборудования, например, отсечного клапана

$$PFD = V_y .$$

то становится ясно, что при постоянной интенсивности отказов единственной возможностью снижения вероятности отказа является уменьшение межтестового интервала 77 (часто обозначается как T_y).

Примечание

Применение пары отсечных клапанов на одной линии способно существенно снизить вероятность опасного отказа:

$$pfd,OO2=4 \qquad TL,$$

однако зависимость от интервала тестирования становится еще более сильной. И уменьшить его без останова процесса можно только одним способом - обеспечив возможность тестирования с частотой большей, чем 1/TI.

Проверка в режиме *on-line* работоспособности отсечного клапана, участвующего в обеспечении безопасности процесса - непростая задача. Традиционное решение предполагает установку дополнительной арматуры, что влечет существенное увеличение капитальных затрат. Наиболее приемлемым способом тестирования отсечных клапанов в режиме *on-line* на сегодняшний день считается частичное открытие или закрытие клапана в сочетании с инспекцией и обслуживанием по месту. По экспертным оценкам разных компаний эта методика позволяет обнаружить от 60 до 95% отказов.

Можно выделить три основных метода тестирования отсечных клапанов путем частичного изменения их положения в оперативном режиме.

13.3. Механическое ограничение хода клапана

Используется механический ограничитель хода или устройство, ограничивающее перемещение клапана на определенную величину хода. Обычно - это 10-20%.

Это механическое устройство может быть встроено в клапан, или вручную устанавливается на клапан только на время испытаний.

Хотя эти устройства недороги, но они не дают развернутой диагностики, требуют больших трудозатрат и контроля над тем, что они не оставлены в ограничивающем положении по окончании испытаний. Самое неприятное - это то, что во время тестирования клапан недоступен для выполнения функций защиты.

13.4. Тестирование с использованием ПЛК системы ПАЗ

Для осуществления этого метода требуется специальное программное обеспечение в ПЛК, а также датчик положения или ограничивающие ключи на клапане. Дополнительно может использоваться датчик давления.

Этот метод кроме самой проверки работоспособности соленоида и перемещения клапана позволяет проверить временные характеристики и кривую изменения давления на клапане. Результаты тестирования могут быть архивированы для сравнения с предысторией.

Принципиальный недостаток этого метода - система противоаварийной защиты используется для выполнения несвойственных ей функций. Таким образом, существенно повышается риск ложного срабатывания системы противоаварийной защиты во время технического обслуживания.

Кроме того, данный подход неявным образом подразумевает использование рабочей или инженерной станции РСУ, поскольку система ПАЗ по определению не должна иметь рабочих станций реального времени.

Наиболее рациональный вариант, который позволителен для систем противоаварийной защиты, - это специализированная выделенная инженерная станция для обслуживания и сопровождения системы ПАЗ.

13.5. Специальные цифровые контроллеры клапанов

Контроллер способен проверять работоспособность соленоида, и изменять положение клапана в соответствии с предопределенным тестовым профилем, контролируя положение клапана, давление на клапане, и время выполнения задания.

В случае отклонения фактических характеристик от эталонных, контроллер выдает соответствующую диагностику, которая воспроизводится и фиксируется системой обслуживания полевых устройств (о ней речь впереди).

Система обслуживания полевых устройств позволяет хранить и документировать предысторию всех тестовых операций и их результатов, поэтому всегда будет существовать возможность сравнения с исходным состоянием и исходными характеристиками полевых устройств. Этот метод диагностики требует дополнительных затрат на оборудование, которые, однако, окупаются в процессе эксплуатации как за счет снижения расходов на обслуживание, так и снижения числа ложных остановов и опасных отказов, приводящих к непосредственной угрозе аварии.

Примечание

Если во время проведения операции тестирования с установки приходит сигнал о реальной необходимости срабатывания данного клапана, то эта команда будет иметь приоритетное значение.

13.6. Расчет эффекта оперативной диагностики

Покажем, как тестирование путем частичного изменения положения клапана способно реально повысить уровень безопасности системы за счет уменьшения вероятности опасного отказа, и без установки дополнительной арматуры.

Пусть интервал функционального тестирования (межтестовый интервал) равен 1 году. Тогда вероятность отказа клапана в течение года определится как

$$\text{PPO} = Л_0 \sim = Я_0 . | = 0.5 \quad Л_0$$

Если допустить возможность более частого, но частичного тестирования клапана в течение межтестового npo6eia 77, то вероятность отказа будет складываться из двух компонент:

= ^ у + где

$Л_{ор}$ - Интенсивность отказов в течение интервала частичного тестирования T_p;

A_{DF} - Интенсивность отказов в течение интервала полного функционального тестирования T_F =77 .

Обозначим долю диагностического охвата во время частичного тестирования клапана как а . Тогда интенсивности отказов на интервалах частичного и полного тестирования выразятся следующим образом:

$Л_{ор} = a \cdot A_0$

$A_{DF} = (1 - a) A_0$, и окончательно

$PFD \sim a \cdot Я_0 - + (1 - a) A_D -$

Оценки *а* могут быть разными, но обычно считается, что степень уверенности в работоспособности или неработоспособности клапана после частичного тестирования достаточно высока, ведь одно уверенное определение работоспособности клапана составляет половину успеха.

Исходя из предположения, что главная задача отсечного клапана - не застрять и не заклинить и точно выполнить команду, ведь именно эти неисправности определяются при частичном тестировании в первую очередь, P. Gruhn в статье *"It s time to bring sanity back to SIS design "* предлагает оценку доли диагностического охвата а = 0.8.

Допустим, что частичное тестирование клапана проводится ежеквартально, то есть 4 раза в год. Тогда вероятность отказа определится как

$PFD \sim 0.8 \quad Л_0 \sim + 0.2Л_о \sim = 0.1\text{-}Л_о + 0.1 \quad Л_0 = 0.2 \quad Л_0$

Выше мы получили значение вероятности отказа в течение 1 года без промежуточного ежеквартального тестирования:

$PFD = 0.5 \ A_d$

Таким образом, промежуточное тестирование оборудования действительно позволяет существенно снизить вероятность отказа, и, главное, существенно повысить уверенность технологического персонала в дееспособности системы безопасности.

Завершая пример, найдем эквивалентное время полного функционального тестирования, которое потребовалось бы для достижения полученных характеристик нашей системы с комбинированным тестированием:

$0.2 \cdot Л_0 = Я_0 \cdot у \qquad ТІ = 0.4$ года.

Мы видим, что возможность оперативного тестирования полевого оборудования дает возможность реального повышения уровня интегральной безопасности SIL **без установки дополнительного оборудования.**

Возникает вопрос:
Какими средствами в составе АСУТП может быть обеспечено выполнение операций тестирования в режиме *on-line?*
Стандартно мы имеем только то, что имеем, однако:

- ПАЗ - Совершенно исключено.
- РСУ - Практически исключено.

Реальные возможности создания подобного рода систем возникли только с появлением так называемых "интеллектуальных" полевых устройств с микропроцессорным управлением, и средств взаимодействия с этими устройствами - полевых шин:

- Гибридных аналогово-цифровых протоколов типа HART;
- Полностью цифровых шин (Profibus, Fieldbus).

13.7. Системы обслуживания полевого оборудования

Системы *Plant Asset Management* — исключительно эффек-I ивный инструмент повышения безопасности производства.

Системы обслуживания поля органически включаются в общую иерархию средств управления ресурсами и эффективностью предприятия (см. рис. **13.2).**

Важное замечание

В настоящее время в состав интеллектуального полевого оборудования кроме датчиков, анализаторов и клапанов, включаются электродвигатели и насосы, работоспособность которых наряду с КИП имеет определяющее значение для технологического процесса. Это ли не подтверждение наше-•о подхода к созданию универсальной системы идентификации параметров АСУТП, представленной в главе 10.

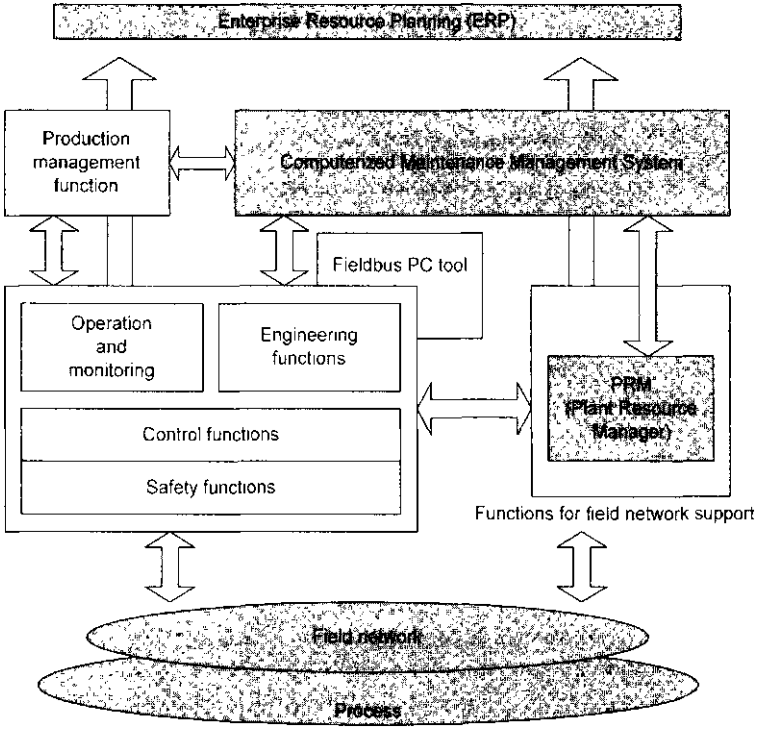


Рис. 13.2

Идея этих систем, которые выступают под общим термином *Plant Asset Management Systems* - управление оборудованием производства, или под названиями фирм-производителей, например:

- *Asset Management Solutions - A MS* (Система обслуживания поля - СОП) фирмы Emerson,
- *Plant Resource Manager - PRM* (Менеджер ресурсов производства - МРП) фирмы Yokogawa Electric,

заключается в том, что, подобно обычному регулированию параметров технологического процесса, вводятся средства обслуживания полевого оборудования, обеспечивающего безопасность и управление технологическим процессом.

13.8. Архитектура систем обслуживания

В силу специфических особенностей РСУ, ПАЗ и систем обслуживания, все они включаются в состав АСУТП как самостоятельные системы / подсистемы, способные к взаимодействию между собой.

В зависимости от типа полевого протокола (чисто цифровой или цифро-аналоговый) конкретные подробности архитектуры АСУТП, имеющей в своем составе систему обслуживания КИП, будут меняться, но общий подход сохраняется:

Используется выделенная рабочая станция КИП, которая работает с цифровой частью протокола, или полностью цифровыми средствами взаимодействия с полевым оборудованием.

Безусловно, системы обслуживания полевого оборудования предназначены для осуществления всего спектра задач по работе с оборудованием:

- Объявление новой единицы оборудования в составе АСУТП;
- Определение характеристик;
- Автоматизированная калибровка;
- Диагностика *on-line;*
- Архивирование;
- Отчетность и т.д.

Но ключевым моментом являются новые возможности по выявлению неполадок и отказов оборудования.

Обслуживание полевого оборудования можно проводить по-разному:

1. После того, как устройство "неожиданно" отказало;
2. Планово-профилактическое обслуживание:
   Приборы поверяются по определенному графику независимо от того, есть ли в этом реальная необходимость;
3. Превентивное, предупредительное обслуживание:
   График обслуживания подстраивается под реальные данные об отказах;
4. Обслуживание по запросу с поля:
   Встроенной диагностика прибора дает запрос на техническое обслуживание.

Текущая ситуация на подавляющем большинстве отечественных предприятий элементарна - обслуживание проводится по первым двум вариантам:

- При отказе, и
- По графику.

Современная тенденция - разработка полевого оборудования, способного самостоятельно выявлять главные нарушения и сбои в своей собственной работе, и сообщать о них персоналу. Пример: Автоматическое определение забивки импульсной линии датчика давления (рис. 13.3).

Для определения забивки импульсной линии интеллектуальный датчик анализирует вариацию шума с высокой частотой, которую не может обеспечить АСУТП:

Параметры шума изменились, но при этом сами данные о переменной остаются вполне приемлемыми! Самодиагностика позволит выявить это нарушение и провести превентивное обслуживание.

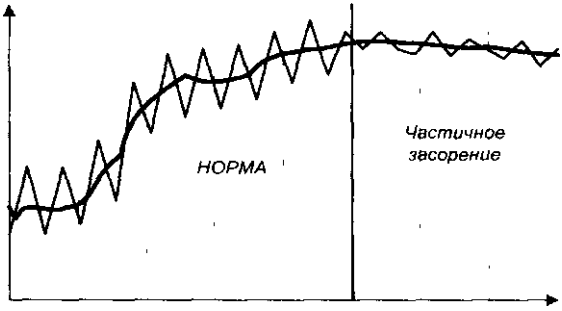


Рис. 13.3

Системы управления полевым оборудованием в реальном масштабе времени позволяют существенным образом повысить надежность систем управления и защиты, уменьшить затраты на обслуживание, сократить число и время простоев.

Основная цель - приблизиться к оптимальному уровню обслуживания. На рис. 13.4 представлены главные опорные точки графика обслуживания:

1. Недостаточный уровень обслуживания.
   Следствие - дорогостоящие остановы производства.

2. Уровень, близкий к оптимальному.
3. Неоправданно частое обслуживание также увеличивает издержки производства.

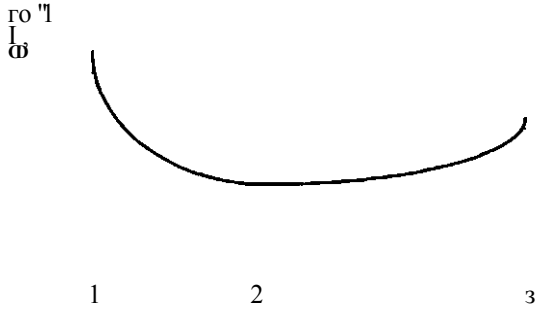


Рис. 13.4

Системы обслуживания поля способны радикальным образом повысить степень доверия к системе и уровень взаимодействия с полевым оборудованием:

- Дистанционные операции с полевым оборудованием;
- Автоматизация обслуживания;
- Связь с функциями управления оборудованием;
- Поддержка приложений *plug-in;*
- Возможность превентивного обслуживания.

Сводный эффект внедрения систем управления оборудованием:

- Увеличение безопасности производства;
- Улучшение качества продукции;
- Автоматизированный контроль эффективности и стоимости обслуживания.

На сегодняшний день существует несколько реально действующих образцов подобных систем. Рассмотрим особенности этих систем на примере достаточно известных:

- *Asset Management Solutions - A MS*
  (Система обслуживания полевого оборудования - СОП) фирмы Emerson, и
- *Plant Resource Manager - PRM*
  (Менеджер ресурсов производства - МРП)
  фирмы Yokogawa Electric.

13.9. AMS - Система обслуживания поля фирмы Эмерсон

Пакет программ *Asset Management Solutions* (AMS, Система обслуживания приборов) и прилагаемые к нему приложения - это набор программных решений для учета всей деятельности по обслуживанию приборов, связанной с датчиками и исполнительными устройствами.

AMS является полнофункциональным инструментом для конфигурирования, управления документацией, калибровки и диагностики устройств. AMS предоставляет пользователям доступ к инструментам управления процессом в реальном времени, и автоматически использует всю информацию о текущем состоянии устройств. Одновременно AMS является инструментом для составления прогнозов по обслуживанию и эксплуатации, предоставляя возможность предсказывать мероприятия по обслуживанию приборов вместо простого реагирования на происходящие отказы.

Стандартная конфигурация системы AMS состоит из выделенной рабочей станции, набора программного обеспечения, и встраиваемых приложений (рис. 13.5).

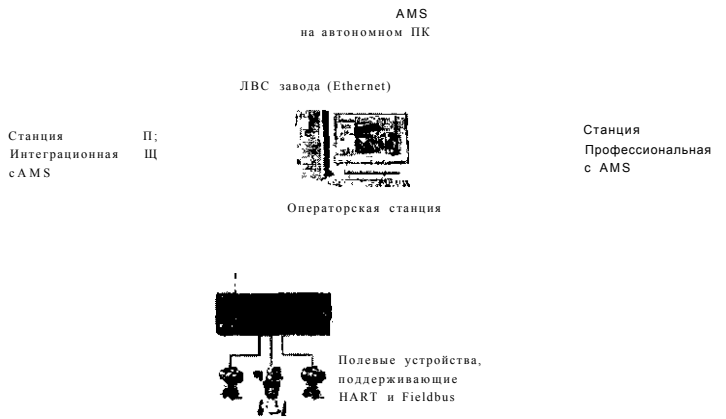


Рис. 13.5

При использовании AMS в режиме *off-line*, обслуживающий персонал получает возможность удаленно проверять устройство, конфигурировать его, и обновлять калибровочные данные путем нажатия нескольких клавиш.

Используя AMS в режиме *on-line*, эксплуатационный и обслуживающий персонал может непрерывно вести наблюдение за полевыми устройствами для мгновенного получения информации в случае возникновения проблемы. Всё это приводит к значительной экономии средств, ибо перед тем, как вызвать серьезные сбои в производстве, проблемы с оборудованием могут быть выявлены заранее.

AMS позволяет получить доступ к внутренним механизмам самодиагностики, которые встроены в устройства HART и Fieldbus. Это позволяет сосредоточиться на решении проблемы, поскольку не требуется тратить время на путь к клеммному шкафу или к полевому устройству для поиска неполадки.

13.10. Функциональные возможности AMS

AMS позволяет:

- Конфигурировать устройства в режиме *on-line* с интегрированными интерфейсами систем DeltaV, RS3, PROVOX с помощью мультиплексоров HART, и пользоваться системным интерфейсом в режиме *off-line,* используя возможности загрузки и выгрузки конфигурации устройств с помощью прибора HART Communicator, или использовать модем HART для временного подключения к устройству.
- Осуществлять планирование и хранение созданных вариантов конфигураций в базе данных оборудования. При следующем подключении к устройству с помощью AMS или прибора HART Communicator, можно загрузить в него новую конфигурацию, обновленную при работе в режиме *off-line.*
- Выполнять проверку контуров, самодиагностику приборов, и просматривать состояние устройства.
- Получать текущую информацию от подключенных устройств для определения их рабочего состояния, и просмотра переменных процесса.
- Диагностика устройств, результаты проверки контуров и самодиагностика могут быть автоматически документированы.

- Имеется возможность просмотра информации о статусе для определения состояния устройства без исключения устройства из процесса.
- Проводить калибровочные процедуры. Определять схему теста, которая может быть использована для нескольких устройств. Любые изменения в схеме теста будут автоматически обновлены для всех ассоциированных устройств.
- Импортировать и экспортировать информацию между несколькими системами AMS. Если есть много отдельных рабочих станций, объединенных в сеть, существует возможность вести общую базу данных.
- Входить в систему с использованием пароля. Системным администратором устанавливаются имена пользователей и пароли, позволяющие различным пользователям иметь различный уровень доступа к системе AMS.

13,11. Монитор сигналов тревоги

Корпоративная сеть предприятия позволяет в полной мере воспользоваться преимуществами системы AMS. Каждая зона сети подключается к отдельному серверу AMS, который передает данные на AMS Server Plus.

Web-интерфейс AMS собирает локальные пакеты данных с каждого сервера AMS, и отображает их в одном окне обозревателя. С помощью безопасного доступа, предоставляемого системой AMS, можно отслеживать сигналы тревоги, поступающие из различных подразделений производства.

Интерфейс позволяет просматривать конфигурацию и данные калибровки устройств, присоединенных к нескольким серверам AMS, опрашивать и отображать информацию о состоянии приборов, датчиков и исполнительных механизмов, отсортированную по типам устройств или по технологическим установкам. Затем можно отфильтровать данные и представить их в виде, удобном для принятия решений.

Web-интерфейс AMS снижает количество повторно выполняемых типичных операций настройки, сохраняя часто посещаемые или специально отобранные страницы.

13.12. PRM - Менеджер ресурсов производства фирмы Йокогава Электрик

Фирма Yokogawa Electric отстаивает канонический иерархический подход к структуре и функциям АСУТП (рис. 13.6).

Каноническая иерархическая структура АСУТП

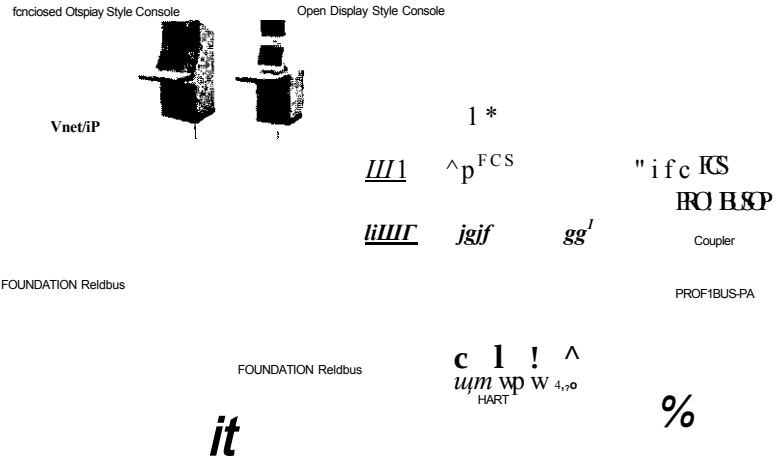


Рис. 13.6

Программный пакет Менеджера ресурсов производства (МРП) встраивается в общую архитектуру системы Centum на уровне самостоятельной системы (подсистемы). МРП поддерживает такие функции, как:

- Конфигурация устройств и управление устройствами;
- Планирование проверок и регистрация результатов;
- Графики работ по техобслуживанию;
- Корректировка параметров устройств и ведение журнала регистрации;
- Диагностика устройств;
- Интерактивная документация.

Существует пять основных функциональных направлений для работы и обслуживания полевого оборудования:

- Навигатор устройств;
- Управление информацией по техобслуживанию;

- Анализ эксплуатации;
- Диагностика и настройка;
- Служебные и сервисные функции.

Неоспоримый приоритет Йокогавы состоит в пионерском расширении панорамы потенциальной области диагностики до масштабов основного оборудования. Иерархия уровней диагностики системы управления **всеми** ресурсами производства представлена на рис. 13.7.

13.13. Навигатор устройств

Навигатор устройств обеспечивает:

- Обзор установки / производства;
- Обзор сети;
- Обзор класса.

Обзор установки / производства дает возможность просмотреть расположение полевого оборудования в привычном для пользователей Windows формате проводника Explorer.

Иерархия повторяет естественную для технологического персонала группировку оборудования по титулам, цехам, отделениям, узлам, параметрам.

Обзор сети дает возможность рассмотреть позицию устройства по отношению к физической конфигурации полевой шины в иерархическом представлении. Цвет иконки устройства отражает текущее состояние устройства.

Обзор класса иерархически представляет устройства, сгруппированные по производителям, моделям, версиям. Состояние устройства (техобслуживание, резерв и т.д.) также помечается соответствующими ключевыми словами и цветом.

13.14. Управление информацией по техобслуживанию

Обеспечивает следующие направления:

- Мастер устройств;
- Архив инспекций (проверок оборудования);
- График инспекций;
- Список составных частей устройств;
- Связанная документация.

Иерархия уровней диагностики оборудования

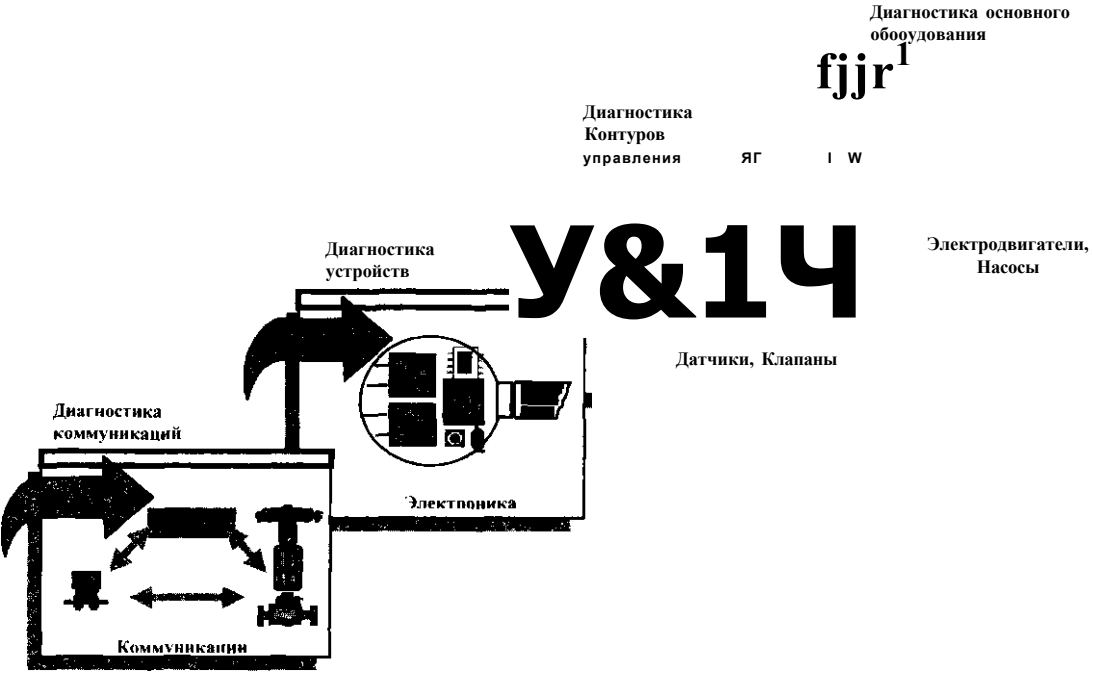


Рис. 13.7

Мастер устройств управляет всей совокупностью оборудования. Может предоставить список всех существующих устройств с детальной информацией завода-изготовителя, и текущей информацией по каждому устройству.

Архив инспекций (проверок оборудования) обеспечивает архивирование всех инспекций устройства, фиксацию и формирование отчетов по всем сбоям и нарушениям в работе полевых устройств.

График инспекций создается и поддерживается для проверки, настройки, калибровки каждого из имеющихся устройств.

Список составных частей устройств содержит список компонентов каждого устройства с указанием их наличия на складе запасных частей.

Связанная документация - воспроизводится электронная документация, связанная с данным устройством:

- Конфигурация;
- Технологические схемы с киповской обвязкой;
- Технологические инструкции, и т.д.

Вызов всей совокупности сопутствующей документации осуществляется по шифру киповской позиции.

13.15. Функция анализа эксплуатации

Данная функция поддерживает базу данных, содержащую предысторию существования оборудования:

- Первоначальные установочные параметры;
- Сохраненные параметры устройства;
- Текущие параметры устройства;
- Проведенные калибровки;
- Предыстория инспекций (контрольных проверок).

Содержимое базы данных может быть воспроизведено:

- В хронологическом порядке;
- По типу события;
- В сводном или детальном виде.

Записи могут быть отфильтрованы по шифру позиции или ее составных элементов, так что информация о поведении конкретного устройства может быть легко прослежена и проанализирована.

13.16. Функции диагностики и настройки

Поддерживают функции диагностики и настройки устройств в режиме *on-line*.

Настройка и сравнение.

Данная функция позволяет воспроизводить и устанавливать параметры устройства. Текущие установки устройства в любой момент времени могут быть сравнены с архивными записями, переустановлены и сохранены.

Инструменты.

При использовании Foundation Fieldbus существенным образом расширяются возможности по автоматическому обнаружению вновь введенных устройств и их самодиагностике.

Калибровка.

С помощью этой функции производится настройка параметров устройства с функциями диагностики.

Информация по всем типам устройств третьей стороны может быть зарегистрирована в приложениях *plug-in*, и также может быть использована для их калибровки.

13.17. Служебные и сервисные функции

Функция просмотра *(browser)* позволяет осуществлять поиск устройства по атрибутам устройства, таким, как:

- Идентификационный номер устройства;
- Позиция КИП;
- Имя блока;
- Значение параметра и т.д.

Функция защиты информации (секретность) позволяет ограничить доступ для определенных пользователей или для определенных операций к функциям обслуживания полевых устройств, предохраняя от возможных несанкционированных вмешательств в систему.

Все действия и попытки проникновения в систему фиксируются в архиве.

Функция самодокументирования автоматически создает документацию по работе устройства. Позволяет по запросу делать распечатку накопленной информации.

Также может быть распечатана информация по текущему обслуживанию непосредственно в виде копии экрана.

Обеспечение функции *plug-in.*

Функции подключения устройств сторонних изготовителей обеспечиваются соответствующими библиотеками базы данных на PRM-сервере.

13.18. Преимущества использования Менеджера ресурсов

Программное обеспечение Менеджера ресурсов производства обеспечивает преимущества многими способами (рис. 13.8), включая:

- Сокращение стоимости обслуживания;
- Дистанционный контроль состояния устройства;
- Настройка параметров устройства;
- Выполнение диагностики устройств в режиме *on-line;*
- Усовершенствование работ по обслуживанию;
- Регистрация отчетов по обслуживанию;
- Ведение единой базы данных оборудования;
- Безболезненная интеграция оборудования сторонних производителей.

Рис. 13.8

13.19. Программное обеспечение для комплексных решений

Фирмы предлагают целый спектр пакетов прикладного программного обеспечения, начиная от многопараметрических оптимизирующих контроллеров и управления с нечеткой логикой, и заканчивая, но "не ограничиваясь", всеобъемлющими системами организации производства *(Management Enterprise System - MES)* (рис. 13.9). Однако необходимо обдавать себе ясный отчет, что для результативного применения средств более высокого уровня необходимо пройти все соподчиненные ступени автоматизации - от модернизации полевого оборудования до усовершенствованного управления.

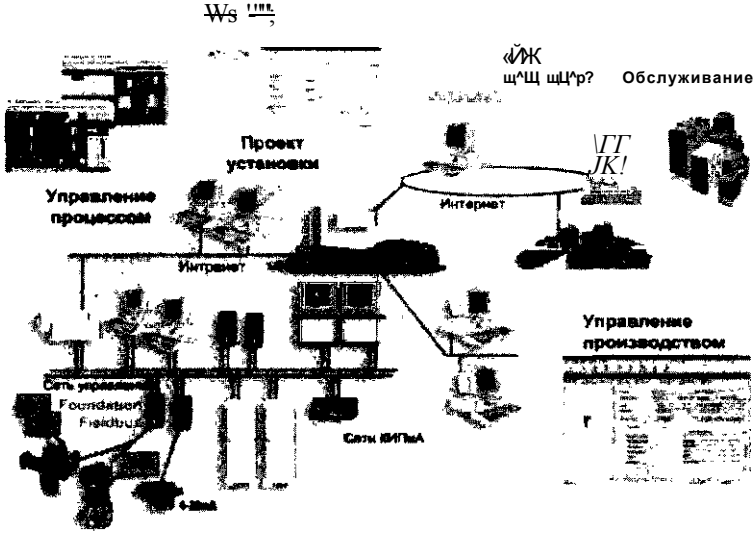


Рис. 13.9

стоят эти средства недешево, однако надежды на чудесное избавление от трудов праведных за счет всемогущего моделирования и оптимизации не всегда оправдываются. Причина неудач заключается в том, что интеллектуальные средства требуют интеллектуального персонала, с которым и в добрые-то времена было негусто.

Вместе с тем, существуют недорогие решения, которые не требуют особой квалификации для настройки и обслуживания, а рассчитаны на обыкновенный здравый смысл. Рассмотрим некоторые возможности, которые находятся непосредственно в контексте данной работы.

13.20. Решения для расширенной поддержки операций

Данная группа решений представлена следующими пакетами фирмы Yokogawa Electric:

- **Exaplog** - Пакет анализа событий. Анализирует технологические операции и действия оперативного персонала, и фиксирует события, сообщения и сигнализации с процесса.
- При анализе, опираясь на журнал сообщений АСУТП, используется фильтр 3W - What? Where? When? (Что? Где? Когда?).
- Производительность персонала и установки может быть существенно повышена за счет устранения избыточных и ненужных сообщений и сигнализаций, и исправления некачественных алгоритмов и прикладных программ.
- **Exapilot** - Пакет повышения эффективности технолога - оператора. Обеспечивает комплексные стандартизированные операции повышения эффективности управления, основанные на знаниях опытных операторов технологического процесса.
- Автоматизация стандартных рабочих процедур позволяет автоматизировать практический опыт испытанных операторов.

Exaplog: Пакет анализа событий.

С развитием средств автоматизации количество контуров, контролируемых одним оператором, непрерывно возрастает и достигает своего предельного значения.

При таких условиях для обеспечения стабильности и безопасности работы требуются качественно новые решения возникающих проблемных ситуаций, таких, например, как лавина сигнализаций и событий, требующих вмешательства оператора, чтобы предпринять соответствующие меры противодействия.

Пакет анализа событий и расширенной поддержки операций Exaplog позволяет провести анализ проблем, связанных с неэффективным использованием возможностей технологического процесса, как в режиме нормальной эксплуатации, так и при проведении операций пуска-останова. Пакет анализа событий Exaplog обеспечивает доступ к файлам регистрации событий на DCS и формирует временные диаграммы, позволяющие сопоставить запросы технологического процесса (сигнализации, сообщения и инструкции для оператора) в зависимости от действий оператора (рис. 13.10).

Пакет Exaplog позволяет проводить анализ работы установки с целью повышения эффективности ее работы путем достижения улучшенной управляемости и дальнейшей автоматизации, а также сокращает нагрузку на операторов.

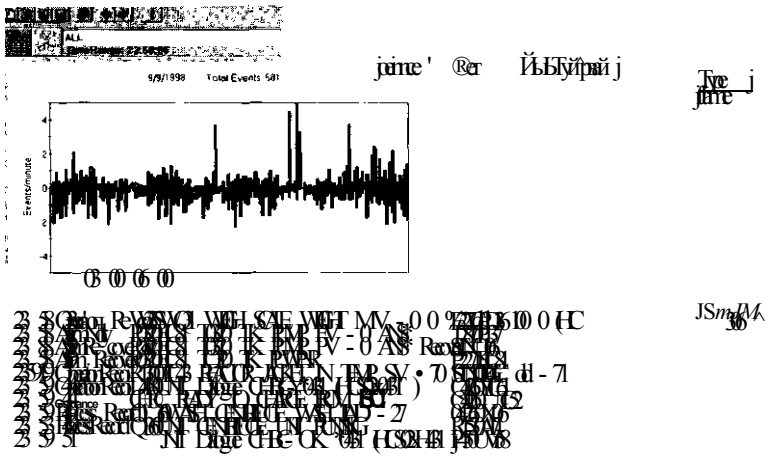


Рис. 13.10

Exapilot: Пакет повышения эффективности работы.

Операции во время пуска и останова в ответ на нештатные состояния процесса или устройств, ручное вмешательство во время нормальной работы, вызванное различным опытом операторов, могут привести к нарушению технологического процесса, что в свою очередь окажет влияние на эффективность производства.

С помощью пакета Exapilot опытный квалифицированный оператор может формализовать свой опыт для автоматизации операций управления, и таким образом способствовать качеству работ менее опытных товарищей на стабильном и высоком уровне. Пользователь может репродуцировать поддержку передовых методов работы и повысить эффективность производства путем повтора отлаженного цикла программы Exapilot для создания новых приложений.

Приложения Exapilot используют стандартные рабочие процедуры для вывода на дисплей формализованного ноу-хау в наглядном формате (рис. 13.11).

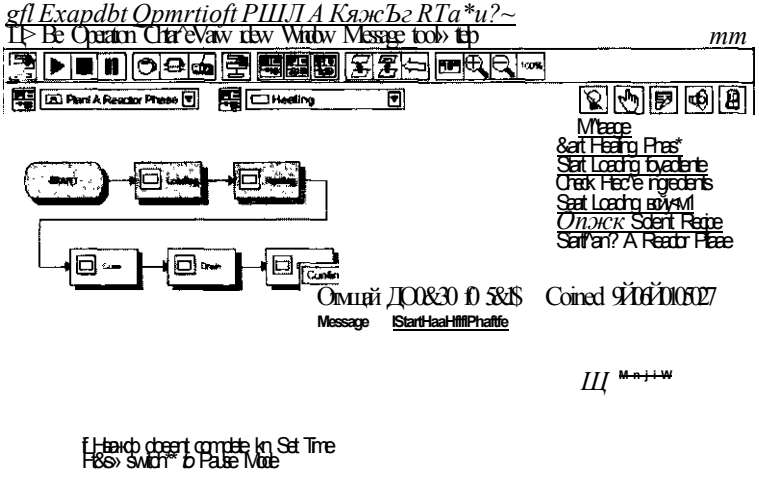


Рис. 13.11

Динамическая настройка порога тревожной сигнализации. Пакет Exapilot обладает совершенно уникальной способностью радикально уменьшить количество избыточных сигнализаций. Эта способность реализуется за счет того, что в соответствии с изменением режима технологического процесса автоматически загружаются новые пороги тревожной сигнализации. Динамическое изменение порога тревожной сигнализации в соответствии с изменением фазы работы (например, с изменением рецептуры или нагрузки) позволяет избежать выдачи излишних сигнализаций (рис. 13.12).

Одна из сущностей, открытых этими средствами, кратко формулируется следующим образом:

Взаимоотношение числа и динамики появления сигнализаций, и соответствующих манипуляций в ответ на эти сообщения является индикатором уровня стабильности и безопасности процесса.

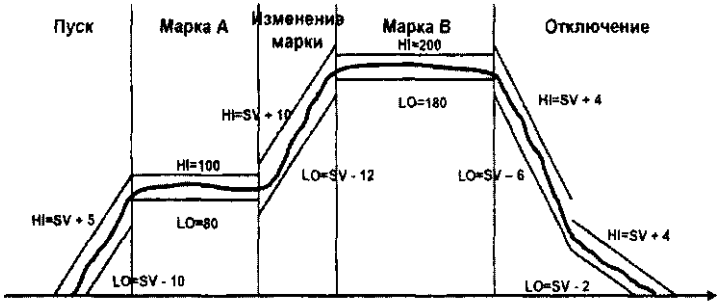


Рис. 13.12

Разработчики данного подхода задаются самыми простыми вопросами:

- Как уменьшить число оповещений?
- Как снизить ручное управление?

В качестве основы для принятия решений о необходимости и достаточности сигнализаций процесса предлагается произвести анализ соотношения событий, сообщений, сигнализаций, и ответных действий оператора процесса (см. рис. 13.13).

Тренд баланса событий и манипуляций.

На дисплей выводится баланс между:

1. Запросами процесса:
   - Сигнализация системы,
   - Сигнализация процесса,
   - Руководство оператора, и т.д.
2. Действиями оператора:
   - Ввод данных тэга,
   - Подтверждение или игнорирование сигнализаций,
   - Изменение режима тэга, и т.д.

Авторы разработки на основе собственного опыта внедрения этой методики предлагают нижеследующие опорные соотношения сигнализаций и ответных действий оператора, которые можно считать приемлемыми.

Стабильность:

- 12 оповещений в сутки на 100 точек;
- 144 манипуляций в сутки на 100 контуров.

Безопасность:

- 12 оповещений в сутки на 100 точек;
- 144 манипуляций в сутки на 100 контуров.

Надо признаться, представленные опорные значения вызывают настоящее восхищение. Автору настоящей работы за более чем тридцать лет работы в нефтехимии и нефтепереработке не доводилось видеть установок с таким мизерным количеством оповещений (кроме еще не построенных, или, в лучшем случае, полностью законсервированных). Характерный пример в подтверждение этих слов приведен на рис. 13.14. На основе анализа трендов событий и манипуляций при пуске, останове и во время долговременной эксплуатации принимаются решения по изменению регламента работы установки и оперативного персонала.

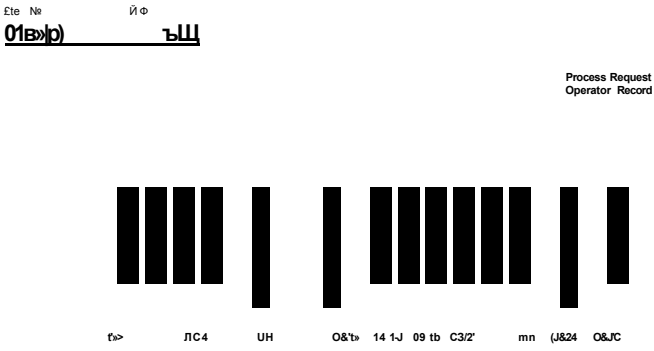
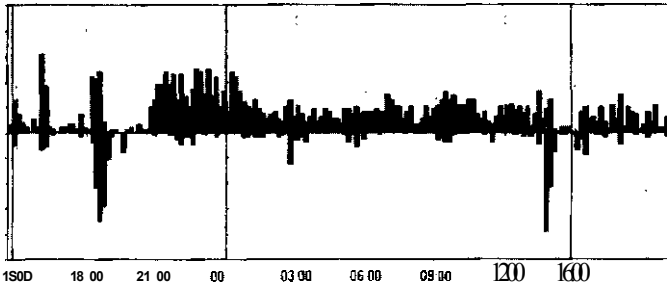


Рис. 13.13

Оригинальные авторские рекомендации фирмы Йокогава по устранению избыточных сигнализаций и действий персонала представлены в таблице 13.3.

Пуск установки



27 февраля, 2002 (9 часов)
545 оповещений
155 манипуляций

28 февраля, 2002 (24 часа)
1195 оповещений
395 манипуляций

1 марта 2002 (12 часов)
447 оповещений
693 манипуляций

Рис. 13.14

Таблица 13.3

Анализ трендов баланса событий и манипуляций

№	Тип шаблона	Шаблон	Вероятная проблема	Меры по устранению
1	Баланс Событий и Действий оператора	- Ш г	Отсутствие серьезных проблем	Долгосрочный анализ изменений производства
2	Избыточные сообщения		Ненужные сигнализации / сообщения Избыточные сигнализации / сообщения	Перенастройка граничных значений сигнализации Объединение избыточных сигнализаций / сообщений
3	Избыточные действия оператора		Низкая степень автоматизации Избыточная работа оператора процесса	Расширение использования РСУ. Упрощение действий оператора
4	Переполнение оператора работой		Низкая квалификация оператора. Сложная последовательность действий оператора	Обучение оператора процесса Упрощение работы оператора
5	Неадекватные действия оператора		Нестабильность процесса. Человеческий фактор	Внедрение усовершенствованного управления процессом. Обучение оператора процесса

13.21. Методы снижения числа оповещений

Современные системы управления и защиты используют многообразную диагностику состояния технологического процесса и контрольно-измерительного оборудования (см. таблицу 13.4). Если не предпринимать специальных мер по сокращению избыточных оповещений и тревожных сигнализаций, можно просто утонуть в их потоке, перестать их воспринимать, и пропустить действительно опасную ситуацию.

Таблица 13.4

Тип	Описание	Возможные причины	
	Тревожный сигнал размыкания вывода	Обнаружено размыкание вывода	Блочный режим адресации данных не работает (0/S)
		Отаг модуля B!B	
BAD	Тревожный сигнал ошибки ввода (активирован сигнал ЮР}	Обнаружено размыкание ввода	блочный режим адресации данных не работает (O/Si
		Отказ модуля B/B	Состояние или происхождение данных действительно (ОШИБКА)
ЮР	Тревожный сигнал размыкания ввода	Порог тревожного сигнала непригоден	Отказ датчика
ЮР	Тревожный сигнал размыкания ввода	Обрыв провода	Превышение диапазона
	никнего предела	Отказ клеммы обнаружения	
HH	Трев сиж ввода еерхн высок предела	Порог тревожного сигнала непригоден	
LL	Трев сигн ввода никн низкого предела	Гистерезис тревожн сигнала непригоден	
HI	Трев сиж ввода высокого предела	Действие непригодно	
10	Трев сиж ввода низкого предела		
DV+	Трев сиж отклонения (полож направл)	Порог тревожного сижала непригоден	Параметр ПИД регулирования непригоден
0V	Трев сиж отклонения (отриц напраел)	Гистерезис тревожн сигнала непригоден	Действие непригодно
		Фильтр проверки отклонения непригоден	
VEL+	Трев сиж ввода скор (полож напрвл)	Порог тревожного сигала непригоден	Параметр ПИД регулирования непригоден
	Трев сиж ввода скор (отриц напрвл)	Гистерезис тревожн сигнала непригоден	Действие непригодно
		Отказ клеммы/датчика обнаружения	
MHI	Трев сигн ввода высокого предела	Порог тревожного сигнала непригоден	Параметр ПИД регулирования непригоден
ML0	Трев сиж ввода низкого предела	Гистерезис тревожн сигнала непригоден	Ручное действие непригодно
CNF	Трев сиж состояния плохого соединения	Подсоединенный блок функций ввода/вывода не работает (0/S)	
		Пропуск разработки	
CERR	Трев сиж ошибки вычислений	Ошибка вычисл (деление на нуль и т л)	
PERR	Трев сиж непредвиденного ответа	Отказ КИПиА участка	
ANS+	Ошибка ответа	Отказ оборудования участка	
ANS	Ошибка ответа		
AUT	Автоматический режим	Действие должно быть автоматизировано	
MAN	Ручной режим		
CAS	Каскадный режим		
SV	Установка переменной		
MV	Управление переменной		

Для снижения общего количества сигнализаций необходимо решить следующие задачи:

- Во-первых, определить причину каждого сообщения тревоги или оповещения.
- Во-вторых, решить проблему, не прибегая к маскированию сообщений и сигналов тревоги.

Необходимые мероприятия:

1. Улучшение работы поля *(ЮР / ООР alarm):*
   - Замена полевого оборудования;
   - Замена отсечных и регулирующих клапанов.
2. Улучшение контроля и управления *(DValarm, VEL alarm, MH/ML alarm):*
   - Настройка параметров PID-регуляторов;
   - Инсталляция APC пакетов;
   - Настройка программ последовательного управления в РСУ.
3. Настройка тревог *(HI /HH /LO /LL alarm):*
   - Настройка тревожных сигнализаций;
   - Оптимизация связи тревог с процессом;
   - Снятие ненужных тревог.
4. Перенастройка уставок предупредительных и предаварийных сигнализаций *(HI/HH / LO / LL alarm):*
   - Исключение участков бездействия системы в ответ на событие;
   - Унификация полевого оборудования и управления.

Представленные действия приводят к тому, что признаки действительно аномальной ситуации обнаруживаются быстрее, чем бездумная лавина предупредительных сигнализаций РСУ. В анализ вовлечены все средства, способные дать дополнительную информацию об истинном состоянии процесса:

- Долговременное отклонение технологической переменной;
- Аномалия материального / теплового баланса;
- Пропуск технологической операции;
- Отказ оборудования КИПиА.

Таким образом, на основе комплексного опыта технолога-оператора, инженера-технолога, инженера КИП создаются предпосылки для:

- Снижения непродуктивной рабочей нагрузки на оператора;
- Предотвращения цепных тревожных сигналов;
- Повышения устойчивости и безопасности процесса;
- Уменьшения потерь сырья, энергоносителей, непроизводительных потерь времени;
- Повышения производительности.

13.22. Ключевые аспекты построения АСУТП

В предыдущих главах данного руководства дано развернутое представление о методах создания надежных и безопасных АСУТП. В завершение настоящей работы некоторые ключевые аспекты необходимо выделить особо.

13.23. Техническое задание на создание АСУТП

Исключительно важно начать "новую жизнь" не с импровизаций, а с тщательной подготовки к созданию АСУТП, и не вообще, а В ПИСЬМЕННОМ ВИДЕ:

- С формирования требований к АСУТП;
- С разработки концепции АСУТП;
- С разработки и утверждения Технического задания на создание АСУТП.

См. главу "Состав и содержание работ по созданию АСУТП", главу "Состав и содержание документации проекта АСУТП", и главу "Техническое задание на создание АСУТП".

Техническое задание создается разработчиком АСУТП при деятельном участии заказчика, и затем согласовывается со всеми участниками проекта:

- Проектная организация
- Поставщик оборудования
- Разработчик АСУТП
- Технадзор
- И собственно Заказчик.

И пройти эти стадии необходимо ПРЕЖДЕ, чем подписывать какие бы то ни было договоры на поставку оборудования, проектирование и разработку. Это позволит в значительной степени избавиться от многих проблем:

- И во время предварительного обследования процесса,
- И при выборе поставщика оборудования,
- И во взаимоотношениях с проектной организацией,
- И во взаимоотношениях с разработчиком АСУТП,
- Ив течение выполнения проекта,
- И во время приемо-сдаточных испытаний,
- И при прохождении экспертизы проекта в органах технадзора.

13.24. Полевое оборудование

За последние годы полевое оборудование претерпело революционные преобразования. В аспекте промышленной безопасности сегодня к полю предъявляются совершенно особые требования.

Для вновь создаваемых производств - применение "интеллектуального" полевого оборудования с поддержкой гибридных HART и цифровых полевых шин Fieldbus.

Для действующих реконструируемых производств - поэтапный переход на "интеллектуальное" полевое оборудование с поддержкой гибридных HART и цифровых полевых шин Fieldbus.

Протокол Fieldbus (рис. 13.15) представляет собой протокол **двунаправленной цифровой связи для полевого оборудования.** Протокол Fieldbus является серьезным нововведением в технологии систем управления процессом. Он предлагается для замены стандартной аналоговой связи 4-20 мА, на которой работает большинство существующих в настоящий время устройств низовой автоматики. К сожалению, даже это миллиамперное большинство не на нашей стороне. Использование полевой шины открывает совершенно новые возможности управления процессом:

- Цифровой протокол обеспечивает точную обработку информации и строгий контроль качества информации;
- Поддерживается мультиплексорная передача, что позволяет передавать параметры функциональных блоков контрольно-измерительных приборов и средств автоматизации;
- Связь между контрольно-измерительными приборами позволяет реализовать автономное распределенное управление;
- Возможность взаимодействия позволяет объединять в единую систему устройства от различных поставщиков;
- Широкий выбор устройств от различных поставщиков позволяет сконфигурировать оптимальную систему;
- Объединять можно самые разнородные системы, такие как контрольно-измерительные приборы, анализаторы

и электрическое оборудование, заводскую вычислительную сеть, сочетать корпоративную бизнес-автоматизацию и офисные приложения;

- Настройку и проверку оборудования можно выполнять дистанционно.

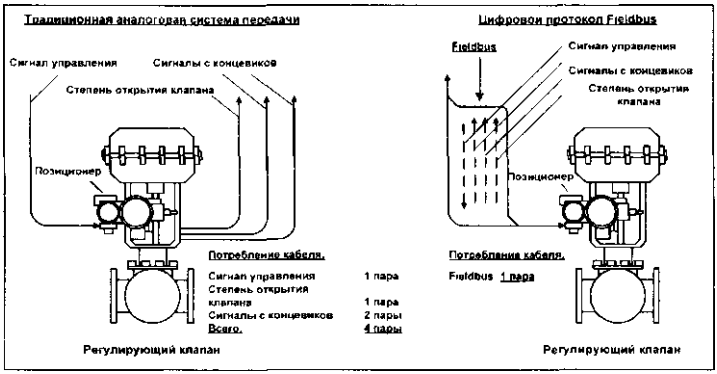


Рис. 13.15

Примечание

Необходимо обратить внимание, что в отличие от сигналов 4-20 mA и HART, шина Fieldbus имеет двунаправленный характер.

Полевые шины позволяют существенно сократить число каналов ввода-вывода в систему (см. рис. 13.15), поскольку могут делать измерения и передачу множественных переменных процесса, одновременно производя сопутствующие вычисления, компенсацию нелинейностей и т.д.:

- Датчики дифференциального давления Fieldbus - обеспечивают массовый расход, объемный расход, давление, температуру потока;
- Магнитные расходомеры - объемный расход, температуру и проводимость среды;
- Вихревые расходомеры - массовый расход, объемный расход, давление, температуру;
- Кориолисовые расходомеры - массовый расход, объемный расход, давление, температуру;
- Уровнемеры дифдавления - уровень плотность жидкости, давление и температуру в аппарате;

- Ультразвуковые уровнемеры - уровень и температуру измеряемой среды;
- Температурные датчики - влажность, температуру окружающей среды, уровень вибрации;
- pH-метры - собственно pH и температуру;
- Датчики проводимости - проводимость и температуру измеряемой среды.

Блоки управления (*PID, Ratio, Feed Forward* и т.д.) являются составной частью Fieldbus - датчики и позиционеры со встроенными блоками PID-регулирования уже существуют.

Поэтому система управления может быть сконфигурирована таким образом, что в случае отказа какого либо контура в DCS управление может быть подхвачено контуром полевого оборудования с поддержанием последнего заданного значения. Возврат к основной конфигурации происходит после восстановления взаимодействия с DCS (рис. 13.16).

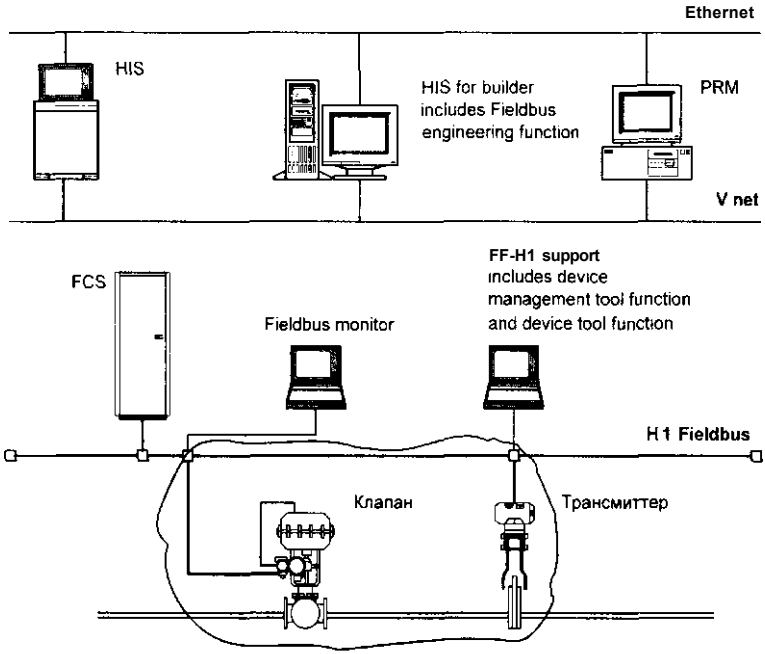


Рис. 13.16

13.25. Системы противоаварийной защиты

Контроллер системы защиты В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ должен иметь программное обеспечение для **определения первопричины останова** технологического процесса вне зависимости от типа отказа.

Все оборудование системы защиты, включая и полевое оборудование, должно быть сертифицировано на применение в системах безопасности *(Safety Instrumented Systems).*

Важное замечание

Современные международные стандарты безопасности рекомендуют производить замену дискретных входов в систему ПАЗ на интеллектуальные аналоговые приборы (Smart transmitters).Там, где по требованиям безопасности необходимо установить 2 датчика на один и тот же технологический параметр, они могут иметь различные принципы измерений (альтернативное резервирование).

13.26. Резервирование

Необходимо предусматривать резервирование ВСЕХ элементов системы, имеющих отношение к безопасности:

- Полевое оборудование;
- Полевые шины;
- Модули ввода-вывода;
- Модули управления;
- Источники питания;
- Грамотный и ответственный персонал.

13.27. Избыточность

АСУТП должна строиться с достаточной степенью избыточности. Как РСУ, так и система ПАЗ, должны иметь 10-20 % резерв по информационным и управляющим каналам.

Вместе с тем, необходимо понимать, что требование избыточности относится не только к оборудованию, но и ко всем программным компонентам системы.

Необходимо предусмотреть достаточные резервы по оперативной и дисковой памяти, а также по быстродействию микропроцессорных вычислителей и промышленных сетей,

которые потребуются для развития функций системы. Запас и информационной, и функциональной избыточности должен быть никак не менее 20, а лучше 40%, включая, прежде всего, быстродействие. Эти требования в обязательном порядке включаются в Техническое задание на систему.

13.28. Иерархия - закон управления сложностью

Цели, которые мы стремимся достичь при построении систем управления и защиты, должны принять ясное выражение в виде вполне понятной архитектуры.

Данный подход хорошо известен в художественном творчестве. Излюбленный тезис художников - *форма освобождает.* Невозможно построить осмысленное сооружение, не имея плана, и не представляя архитектуру объекта.

В контексте нашей темы это означает, что изначально должна быть осмыслена и выстроена информационно-управляющая модель, адекватно отражающая свойства реального объекта автоматизации.

Ф. Брукс, руководитель грандиозного проекта разработки операционной системы IBM ОС 360, перед которой все поделки Microsoft - детский лепет, в своей замечательной книге *"Как проектируются и создаются программные комплексы. Мифический человеко-месяц. Очерки по системному программированию*Наука, 1972 г., пишет:

"Организации, разрабатывающие системы, стремятся к разработке систем, которые являются копией структур и связей, существующих в самих организациях

Успешно работающие сообщества - это успешно организованные сообщества, будь то люди, технические устройства, или насекомые (перечислено в порядке *возрастания* уровня организации).

Только после осознания информационной структуры объекта могут быть оформлены и формализованы функции элементов структуры. Прежде чем функции превратятся в утилитарную последовательность операций, даже если это декларируется под лозунгом новомодных "процессных" подходов, и полностью соответствует и ISO, и чему-то еще, должна быть построена осознанная информационно-управляющая модель объекта автоматизации.

По определению, ***Иерархия*** *(гр. Hierarchia = hieros, священный + arche, власть) ~ расположение частей или элементов целого в порядке от высшего к низшему.* И здесь как нигде применим картезианский принцип: разделять проблему до тех пор, пока решение задачи не станет очевидным. Декомпозиция модели, являясь по определению средством анализа, удивительным образом воздействует на процесс созидания, и возвращает единый синтетический результат.

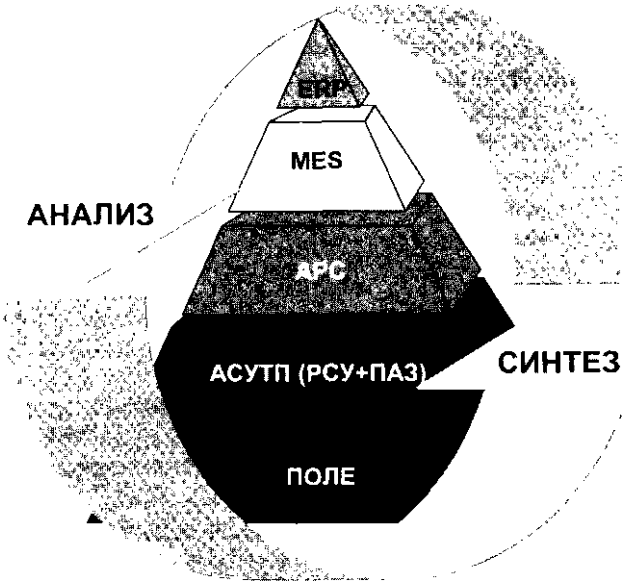


Рис. 13.17

"Делить каждую из рассматриваемых трудностей на столько частей, сколько потребуется, чтобы лучше их разрешить. Располагая свои мысли в определенном порядке, начиная с предметов простейших и легко познаваемых, восходить мало-помалу, как по ступеням, до познания идей наиболее сложных, допуская существование порядка даже среди тех, которые в естественном ходе вещей не предшествуют друг другу", -

Рене Декарт, *Размышление о методе, чтобы верно направлять свой разум и отыскивать истину в науках*, 1637 год.

13.29. Функции контроля и управления

- **Общие функции:**
  - Вход в систему
  - Рабочий режим экрана
  - Окно системных сообщений
  - Иерархия окон
  - Окно навигатора
  - Вызов динамического окна
  - Функция циркуляции изображений
  - Функция обработки сигнализаций
  - Функции печати копии экрана.
- **Стандартные окна управления и контроля:**
  - Объекты обзора
  - Графические окна (мнемосхемы)
  - Графические объекты
  - Объекты управления (контуры)
  - Окно настройки
  - Окно тренда
  - Окно сигнализации процесса
  - Окно руководства действиями оператора
  - Окно контроля сообщений.
- **Функции поддержки управления и контроля:**
  - Функции отчета о процессе
  - Функции отчета исторических сообщений
  - Функции защиты доступа
  - Специализация настольного окружения системы
  - Функция голосовых сообщений
  - Функции нескольких мониторов.
- **Функции техобслуживания системы:**
  - Окно обзора состояния системы
  - Окно системной сигнализации
  - Окно состояния станции управления
  - Окно настройки Станции оператора
  - Окно установки времени
  - Диалог помощи.
- **Окна дисплея состояния управления:**
  - Окно схемы управления

- Окно таблицы последовательности
- Окно логической схемы
- Окно прикладной программы.

• **Функция тренда:**
- Тренды
- Настройка тренда
- Вывод на дисплей трендов с других Станций
- Функция архивирования долговременных данных
- Функции выхода на внешний регистратор.

• **Функции контроля внешних интерфейсов.**

Представленная структура функций может показаться самоочевидной, и недостойной высокого внимания и серьезного осмысления. Но стоит попробовать создать нечто подобное самому, не заглядывая в ответ, от гонора не останется следа.

13.30. Операторский интерфейс

Таким образом, представление информации на станциях оператора должно иметь иерархическую организацию, повторяя организационно-технологическую структуру производства. **Следует всячески избегать излишней гибкости представления информации, и избытка возможных способов проведения операций технологическим персоналом,** с тем, чтобы технологический персонал не плутал в бесконечном количестве динамических окошек, а приобретал устойчивые навыки автоматических действий.

Необходимо в максимально возможной степени ограничить (лучше - отсечь) все возможности Windows, не имеющие прямого отношения к функциям системы и технологического персонала. Очень эффективное средство предотвращения несанкционированных или ошибочных действий - специализированные функциональные панели вместо стандартных алфавитно-цифровых клавиатур. Функциональная клавиатура, как одно из ключевых средств взаимодействия человека с процессом, понуждает оператора действовать по жестко определенным правилам. Функциональная клавиатура заставляет оператора процесса использовать только разрешенные команды, и вырабатывает стереотипы, не провоцируя на бесконечную мышиную возню с аморфными окошками.

13.31. Тренажеры

Согласно ПБ 09-540-03 "*Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств*стр. 7, пункт 2.12,

"Для приобретения практических навыков безопасного выполнения работ, предупреждения аварий и ликвидации их последствий на технологических объектах с блоками **I** и **II** категории взрывоопасности все рабочие и инженерно-технические работники, непосредственно занятые ведением технологического процесса и эксплуатацией оборудования на этих объектах, проходят курс подготовки с использованием современных технических средств обучения и отработки навыков (тренажеров, учебно-тренировочных полигонов и т.д.)". И далее:

"С этой целью указанные организации должны иметь компьютерные тренажеры, ***включающие максимально приближенные к реальным динамические модели процессов и*** *реальные средства управления (функциональные клавиатуры, графические экранные формы и т.д.).*

Обучение и отработка практических навыков на компьютерных тренажерах должны обеспечивать освоение технологического процесса и системы управления, пуска, плановой и аварийной остановки в типовых и специфических нештатных и аварийных ситуациях

Прежде, чем выставлять подобные требования, необходимо ясно понимать, что за ними стоит. Может быть, поэтому тех, кто у нас занимается тренажерами - ноль целых ноль десятых, а моделирующих комплексов, способных дать реальный эффект - и того меньше.

Но и потенциальная возможность дать эффект вовсе не означает, что этот эффект будет получен. Для его обеспечения на установке **постоянно** должна работать группа специалистов высшей квалификации, способных поддерживать адекватность моделей процесса реальному состоянию установки. И позволить себе создание подобных человеко-машинных комплексов даже на западе могут только те немногочисленные фирмы, которые специализируются на проектировании и эксплуатации вполне определенной группы технологических процессов.

Заниматься этим в комплексе - от обследования технологического объекта до разработки специального программного обеспечения - должны специально определенные для этих задач специальные организации, специально уполномоченные Ростехнадзором.

И проверять адекватность *"максимально приближенных к реальным динамических моделей процессов",* и давать разрешение на их использование должен собственно автор идеи - технадзор.

При этом не надо забывать, что основные усилия по управлению процессом должны быть направлены на обеспечение СТАБИЛЬНОСТИ производства, нежели выбрасывать время и деньги на бесконечный поиск и уточнение максимально приближенных к реальным "динамических" моделей нестабильной установки. В предыдущей главе были представлены методы усовершенствованного управления технологическим процессом, способные привнести на установку значительный позитивный эффект.

Поэтому совершенно нереальную для подавляющего большинства наших теперешних предприятий формулировку Правил в части *"реальных динамических моделей"* необходимо ослабить, сделав основной упор на отработку навыков предотвращения и устранения аварийных ситуаций - отработку Плана локализации и ликвидации аварийных ситуаций:

"С этой целью предприятия должны иметь компьютерные тренажеры с моделированием режимов технологического процесса, необходимых для первоначального освоения и последующего подтверждения знаний:

- *Системы управления,*
- *Процедур пуска, планового и аварийного останова, и*
- *Для отработки Плана локализации и ликвидации аварийных ситуаций (ПЛАС)".*

Сценарии ПЛАС по поручению предприятия должны разрабатываться Проектной организацией. Собственно тренажерные комплексы должны разрабатываться специализированными организациями, уполномоченными на то органами технадзора.

13.32. Приемо-сдаточные испытания

Программа и методика приемо-сдаточных испытаний должны быть подготовлены самым подробным и тщательным образом с тем, чтобы проверка на **соответствие проекта и самой системы требованиям Технического задания** дала возможность полностью удостовериться в этом соответствии. Особого внимания требует проверка реакции системы на:

- Технологические нарушения;
- Отказы полевого оборудования;
- Отказы компонентов основного оборудования системы управления и защиты.

Глава *"Программа и методика испытаний АСУТП"* настоящей работы специально посвящена подробнейшему разбору процедуры приемо-сдаточных испытаний.

13.33. Оценка требуемого количества запасных частей

Знание среднего времени наработки на отказ *MTBF* позволяет сделать оценку количества запасных частей N_{SPARE}, необходимого для обеспечения работоспособности системы в течение всего жизненного цикла системы.

Это количество можно оценить исходя из пропорции:

$$N_{TOTAL} = \frac{J_i \text{ тм}}{MTBF} \quad \text{откуда}$$

$$N_{SPARS} = N_{total} \cdot \Gamma \text{, где}$$

Ntotal ~ общее количество каких-либо однотипных компонентов, элементов, или модулей системы;

Тюти - предполагаемое время работы системы до ее списания.

Проделаем несложные расчеты количества и процента запасных частей к исходному количеству оборудования для предполагаемого времени жизни системы

$$T_{TOTAL} = 10 \text{ лет},$$

и примем число используемых элементов (например, входных модулей)

$$N_{total} = 200 \text{ штук.}$$

Таблица 13.5

*" * ; я (1/час) '*	t,OS-OS	1.0E-O6	1,0E-07
MTBF=1/Я:	11,42 года	114 лет	1141 год
:-fy	tO лет	10 ш т	10 лет
R = exp(-AT$_{T07AL}$):	0,416	0,916	0,991
% o m m m :	5в,зе%	8,39%	0,87%
N_{TOTAL}	200	200	200
'Jtqtal	175,2	17,52	1,752
Требуемый % запчастей *(N_{SPARE}/N_{total}) 100%:*	**87,6%**	**8,76%**	**0,876%**

Представленная таблица 13.5 ясно показывает, насколько важно для конечного потребителя знать истинные характеристики надежности оборудования.

Таблица предъявляет довольно жесткие требования к надежности элементов системы:

Для обеспечения обычного процента запаса в 10% среднее время наработки на отказ должно быть в районе ста лет.

С другой стороны, если производитель или поставщик оборудования имеет, и готов предоставить сведения об интенсивности отказов, то стандартное требование 10% запаса могло бы претерпеть значительные изменения.

Появилась бы возможность сделать индивидуальную оценку по каждому из компонентов оборудования. Таким образом, мы могли бы оперировать не только исходной ценой оборудования, но и с достаточной точностью определить и стоимость дальнейшей эксплуатации.

Вопрос в том, а готов ли производитель предоставить эти сведения, и насколько достоверны его данные?

И главное: а продуктивны ли вообще средние оценки интенсивности отказов?

13.34. Методы оценки параметров надежности

Перед производителем оборудования встает непростая задача:

Каждый отдельный компонент системы состоит, в свою очередь, из большого количества собственных компонентов, произведенных к тому же самыми разными изготовителями.

И единственный достоверный, и одновременно нереальный способ проверки или доказательства заявленных характеристик - дождаться полного отказа этих самых двух или скольки-то еще сот модулей, причем в реальных условиях реальной эксплуатации на площадке заказчика.

Существующие методы оценки надежности электронных систем подразделяются на две основных категории:

1. Методы предсказания надежности.
2. Методы демонстрации надежности.

13.35. Методы предсказания надежности

Существуют общепризнанные методы предсказания надежности, выраженные в стандарте Министерства обороны США M1L-HDBK-217, или отчетах типа Bellcore Technical Reference TR-332 *"Reliability Prediction Procedure for Electronic Equipment*" но практически все производители, так или иначе, приспосабливают эти методики под свой опыт и под свою продукцию.

Одним из основных факторов воздействия на интенсивность отказов является температура. Влияние температуры на скорость прохождения химических и физико-химических процессов выражается классическим уравнением Аррениуса, отражающем экспоненциальный рост скорости реакции с ростом температуры:

$$R(T) = R_0 \quad E^{KT}$$

где

R_0 **-** Предэкспоненциальный множитель;

E - Энергия активации (eV);

K - Константа Больцмана, $8.6\text{-}10\sim^{5} eV/K$;

T - Абсолютная температура в градусах Кельвина.

Физические и химические процессы, приводящие к увеличению количества отказов, также в основном непосредственно связаны с температурой.

Для оценки температурного фактора увеличения числа отказов используется следующее соотношение, отражающее экспоненциальный рост тепловой нагрузки на элемент с ростом температуры:

$$\pi^{T} = e^{\frac{E}{K}\left(\frac{1}{T_0}-\frac{1}{T_1}\right)}, \text{ где}$$

T_0 - Базовая температура;

Г, - Рабочая температура;

к^{T} - Температурный фактор.

Это соотношение используется при лабораторных испытаниях, в том числе и для сокращения общего периода испытаний, и определения тепловой устойчивости оборудования.

Если известна оценка интенсивности отказов при базовой температуре T_0, то интенсивность отказов при температуре Г, определяется умножением базовой интенсивности отказов электронных компонентов Л^{в} на температурный фактор к^{1}:

$$A^{c}(T_1) = A^{B}(T_0).x^{T}$$

Для остальных факторов риска:

- Качества компонентов *(Quality);*
- Нагрузки *(Stress);*
- Напряжения *(Electricity),* и т.д.

также разработаны соответствующие методики оценки. В итоге формируется кумулятивное значение интенсивности отказов комплектного изделия (блока, модуля, ...):

$$\text{JIC} — \dot{x}^{C}, 2\text{-}\hat{V}^{hi}\text{-}\text{IB} \bullet 7t, \text{r} \bullet \text{/Г}, \; 7\Gamma, ^{S}7T_i^{\pounds} \bullet ..$$

Компания Tyco Electronic Соф. в своем отчете "*Reliability Concepts for Electronic Power Supplies*2001, приводит результаты сравнения расчетной интенсивности отказов и среднего времени наработки на отказ для своих блоков питания по трем известным методикам:

- *Стандарт Министерства обороны США MIL-HDBK-217, Reliability Prediction of Electronic Equipment, U.S. Department of Defense;*

- *Bellcore TR-332, Issue 6, Reliability Prediction Procedure (RPP) for Electronic Equipment, Telcordia Technologies;*
- *Tyco Reliability Information Notebook, (RIN).*

Результаты просто удручающие - они расходятся в два-четыре раза (см. таблицу 13.6).

Таблица 13.6

Параметр	RIN	RPP	MIL-HDBK
Интенсивность отказов (Fits)	*729*	*1291*	*2714*
MTBF 10^3 часов	*1372*	*775*	*368*
MTBF в годах	*157*	*88*	*42*

Нижеследующий график наглядно демонстрирует, что для методик RIN и MIL прогноз на десятилетний период дает соотношение 76% к 95%, а на двадцатилетний - 62% к 88% вероятности выживания.

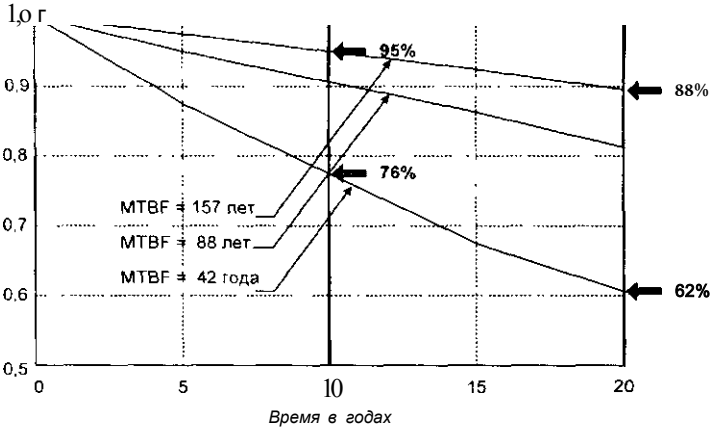


Рис. 13.18

В чем причины такого значительного расхождения?

1. Во-первых, в своих расчетах производители используют разные базы данных по базовой интенсивности отказов электронных компонентов Af .

2. Во-вторых, результат в существенной степени зависит от полноты и подробности включения электронных компонентов в расчет: п и Л/,.
3. В-третьих, конкретные значения факторов корректировки по следующим показателям:
   — качеству деталей к®,
   - рабочей температуре п] ,
   - нагрузке /r,^{s},
   — напряжению xf

   практически всеми производителями устанавливаются исходя из собственного опыта.

Поэтому при выборе конкретных технических устройств, предназначенных для систем безопасности, пользователь должен обратить внимание не только на итоговые значения интенсивности отказов или времени наработки на отказ, но и присмотреться к методикам, по которым эти значения были получены.

Как мы только что имели возможность убедиться, в зависимости от исходных предпосылок и методик результаты расчетов значительно расходятся, и могут ввести в заблуждение кого угодно.

13.36. Методы демонстрации надежности

Наиболее продуктивными методами демонстрации являются процедуры всесторонних испытаний продукции на самых жестких условиях:

- По температуре,
- По перепадам напряжения,
- По вибрации,
- По влажности.

При этом на первоначальных этапах испытаний для определения экстремальных границ существования оборудования, испытания проводят до полного разрушения *(Destruct Limits).*

Окончательные испытания оборудования проводятся в более узких пределах *(Precipitation Screen, Detection Screen),* но, тем не менее, выходящих за конечный рабочий диапазон (см. рис. 13.19).

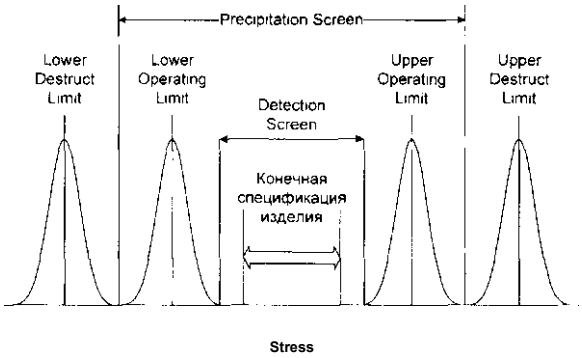


Рис. 13.19

13.37. **Соотношения цены отказа для главных архитектур**

Конечно, можно думать, что вероятности отказа современных электронных систем настолько малы, что трех или четырехкратное увеличение не играет особой роли.
Но если одна архитектура отказывает

- 1 раз в 1 условную единицу времени,
- другая - 3 раза,
- третья - 4,
- а четвертая - 12 раз,

то надо хотя бы знать об этом.

Естественно, речь идет о соотношениях вероятностей отказа для основных архитектур, которые были получены в монографии автора "Основы построения АСУТП взрывоопасных производств", Синтег, 2006:

lm№ 12Ш /" = 1 / 3 / 4 / 1 3

И спорить с этим результатом не приходится:

Добавление второго элемента в канал вдвое увеличивает интенсивность отказа канала. А поскольку вероятность отказа и дублированной, и троированной системы связана с интенсивностью квадратичной зависимостью, то вероятность отказа увеличивается вчетверо.

В данном случае - это цена, которую надо заплатить за повышенный уровень диагностики состояния канала.

Нельзя выдавать средство диагностики, - два работающих канала из трех возможных в архитектуре 2oo3, а средство повышения уровня самодиагностики, - два работающих на одной плате процессора в архитектуре 2*2 ("2oo4") - за резервирование каналов.

Архитектуры 2oo3 и "2oo4" имеют столько каналов, сколько они имеют: первая - 3, вторая - 2. Разница между ними состоит в том, что в архитектуре 2oo3 резервные каналы являются средством диагностики, и после отказа одного канала два оставшихся составляют последний рубеж, на котором архитектура способна сохранять самоконтроль.

Для архитектуры "2oo4" отказ одного из процессоров означает отказ канала, - именно это и выражено формулой 4-2-0. Эта архитектура по определению не может работать по схеме 4-3-2-1-0, ведь у нее только два канала, а не четыре. Единичный отказ процессора на одном модуле выводит из работы сразу два процессора, то есть весь канал целиком. Отказ двух процессоров, находящихся на двух разных модулях означает полный отказ системы. Именно по этой причине архитектуры "2oo4" не рассматриваются в качестве самостоятельных архитектур в стандарте IEC 61508.

Архитектуры loo2D занимают самое достойное место в общей иерархии систем - то есть принадлежат к тому классу систем, которые имеют самые высокие показатели по надежности и безопасности из ныне существующих, и без всяких натяжек. Уникальность систем loo2D вне зависимости от числа процессоров на плате состоит совершенно в другом:

2 набора модулей управления в сочетании с двумя наборами диагностических цепей создают уникальную четырехполюсную архитектуру, которая имеет минимально возможную вероятность ложных срабатываний, и минимально возможную вероятность опасных отказов среди всех известных на сегодня архитектур.

В завершение остается представить важнейшие результатов автора настоящей работы, впервые представленные в монографии "Основы построения АСУТП взрывоопасных производств", в 2-х томах, Синтег, 2006. Это - соотношения для вероятности и интенсивности опасного отказа, а также вероятности и интенсивности ложного срабатывания для систем произвольной архитектуры, отсутствующие в IEC 61508.

13.38. Общие решения для вероятности опасного отказа системы

В стандарте IEC 61508 общие решения **не** просто отсутствуют: для представленных в стандарте **IEC** 61508-6 решений для элементарных архитектур 1oo1, 1oo2, 2oo2, loo2D, 2oo3 не указывается и даже не рассматривается способ их получения. В данном разделе представлены общие соотношения для расчета вероятности отказа систем безопасности **произвольной архитектуры** *MooN* на границах интервала диагностики.

Общее решение для PFD в случае обнаружения опасных отказов только во время автономного тестирования (DC=0). Вероятность опасного необнаруженного отказа одиночного канала на момент времени *t* равна $Л_{DU}t$. Для резервированных систем безопасности типа *MooN (M out of N)* вероятность отказа *(пчт+1)* каналов на момент времени *t* в общем случае будет определяться числом сочетаний *(пчт+1)* отказавших каналов из п возможных, и теоремой умножения вероятностей независимых событий:

$$c^{n}{}_{n} — {}^{l} \cdot (Я\, o\, u \quad \cdot t\, y \cdot {}^{m}$$

Тогда среднее значение вероятности отказа в течение межповерочного интервала определится усреднением по времени:

$$PFD_{AVG}\,[DC = 0] = \text{C;-}^{m+1} \cdot \frac{1}{0}\,(A_{DU} \cdot T)^{\wedge\prime} \cdot DT/T,, \text{ или}$$

$$PFD_{avg}[DC = 0] = СГ \cdot (Лou \cdot T;r^{m+'} /(n\text{-}m + 2),$$

$C^{n\text{-}m+1}_{n}$ - число сочетании *(n-m+1)* отказавших каналов из п возможных:

$$Qn\text{-}m+1 = \frac{n!}{(n\text{-}m + 1)!\{n\text{-}(n\text{-}m + 1))l} = \frac{n!}{(n - m + Щm - 1))!}$$

Общее решение для PFH в случае обнаружения опасных отказов только во время автономного тестирования (DC=0). Аналогично предыдущему, для резервированных систем безопасности типа *MooN (M out of N)* вероятность опасного отказа одного канала, и вероятность отказа *(пчт+1)* каналов в интервале времени *[OFTJ* равны $Л_{ou}T_1$ и $C^{n\text{-}m+1}_{n}\,{}^{(л}{}_{\{aDu}{}^{m}{}_{Ч)}{}^{n\text{-}m+1}$ соответственно.

Тогда можно получить среднюю интенсивность отказов системы в интервале времени *[O, TJ :*

$$PFH_{AVe}[DC = o; = A_{sys} = c;-'. \quad (i \quad m \text{ У}^{7}\text{тм}\wedge \quad \frac{}{\cdot 1} =$$

$$\{n-m + l)!\{m-1))l \quad \overset{T!-}{} \quad {}^{\prime a}\overset{gn-m+7}{du} \quad 1 1^{-rn-m}$$

ИМЕННО ЭТО СООТНОШЕНИЕ ЛЕЖИТ В ОСНОВЕ ВСЕХ СООТНОШЕНИЙ СТАНДАРТА IEC 61508, ЧАСТЬ 6.

Но спектр возможных состояний исследуемых архитектур далеко не исчерпывается, и не должен исчерпываться только этим соотношением.

Общее решение для PFD в случае полного диагностического охвата (DO=l). Поскольку отказ немедленно обнаруживается, то усреднения вероятности по времени существования отказа в данном случае не требуется.

Неготовность, или вероятность обнаруженного опасного отказа резервированной системы *MooN* в общем случае будет определяться непосредственно теоремой умножения вероятностей:

$$PFD_{evg}[DC=1] = C^{n}_{n}{\sim}^{m+1} \bullet (X_{DD} - MTTR)^{n}{\sim}^{m+1} =$$

$$= \frac{}{(n-m + 1)!(m-1)!} \quad 1 \quad (A_{DD} MTTR)^{n}{\sim}^{m+1}$$

где $c\wedge{\sim}^{m+1}$ - число возможных сочетаний *(n-m)+1* устройств, которые должны отказать, чтобы система из п элементов считалась отказавшей.

Общее решение для PFH в случае полного диагностического охвата (DC=1).

Способ решения 1. Первое решение для *PFH[DC = 1]* проведем с помощью математической индукции.

Средняя интенсивность отказа одного из п исходных каналов составляет *n-A.* Поскольку *DC=1*, отказ немедленно обнаруживается, и отказавший канал восстанавливается в течение интервала времени *MTTR.*

Вероятность отказа следующего канала из *(n~1)* оставшихся каналов определится, как *(n-1)- A- MTTR.*

Следовательно, интенсивность отказа систем типа *(N-1)ooN* (например, 1оо2 или 2оо3) выразится, как

$$PFH_{avg}[DC = 1] = n\text{-}(n - I)\text{-}\ A^2_{DD} \bullet MTTR$$

Следующим шагом для систем типа *(N-2)ooN* , то есть с тремя отказами, необходимыми для полного отказа системы, с учетом характеристического среднего времени проявления третьего отказа, равного *MTTR* / 2, получаем

$$PFH_{AVG}[DC = 1] = n(n\text{-}1)>(n\text{-}2)A^3_{DD}MTTR^2 /2$$

В общем случае для нормальной работы системы с архитектурой *MooN* необходимо *M* работающих каналов. С помощью математической индукции интенсивность опасных отказов систем *MooN* выразится следующим образом:

$$PFH_{MG}[DC = 1] = n (n\text{-}1)\text{-}... m R_{DD}{}^{\wedge\prime} \frac{MTTR^{n-m}}{(n-m)!} =$$

$$= (n\text{-}m+1) \bullet C^n_{n\sim m+1} - r_{DD}{}^{m+1} \bullet MTTR^{n\sim m}$$

Способ решения 2. Тот же результат можно получить **и** комбинаторным способом.

Средняя интенсивность отказа одного из п исходных каналов составляет *п • А*. Тогда в течение *MTTR* вероятность отказа *(m-1)* каналов из оставшихся *(n-1)* составит

$$с\ г/\ r_{DD}{}^m \quad MTTR$$

Тогда общая интенсивность опасного обнаруженного отказа составит

$$PFH_{avg}[DC \sim 1] = n \bullet A_{dd} \bullet C;// \bullet A''_{DD}{}^m \text{-} MTTR =$$

$$= n\text{-}A_{DD} \frac{(n-1)!}{(n-m)!\sim(m-1)!} A^n_{DD}{}^m MTTR^{n\sim m} =$$

$$= (n\text{-}m + 1)\ C^n_{n\sim m+1} \bullet A^n{}_{DD}{}^{m+1} \bullet MTTR^{n\ m}$$

Примечание

В указанной в предыдущем разделе монографии найдены общие соотношения вероятности и интенсивности отказа Оля произвольных значений уровня диагностического охвата DC E [0,1].

Сведем все полученные в данном разделе соотношения воедино.

13.39. Полная система соотношений для расчета вероятности отказа архитектур общего вида

$$PFD_{a}JDC = 0] = \text{c};\text{-}^{\text{m}}\text{"} \bullet (Л_{ви}\ \ T, Г\text{""} /(n - m + 2) = \frac{n!}{(n\text{-}m\ +\ 1)i(m\text{-}1)!} \frac{(Л_{си}\ \ TJ\text{-}'}{(n\text{-}m\ +\ 2)} \quad (13.I)$$

$$PFH_{avg}[DC\ =\ 0]\ =\ A_{sys}\ =\ cr^{t1}\ \ \frac{(ЯшТ\ )П_{\text{,,,}}}{\text{'1}} \quad (13.2)$$

$$\sim\ (\text{,,-}_{\text{m}\,+}\ i).i.(_{m}\text{-}i)y\ \ ^{\text{A}_{\text{o}}\text{и}}\ \frac{ln\text{-}m\ +\ 1\ \text{-}m\text{-}m}{\text{'<}}$$

$$PFD_{avg}[DC = 1] = C\text{"}_{n}\text{""}^{+1} \bullet (Лоо \bullet MTTRf^{m}*^{1}\ \text{-} \quad (13.3)$$

$$PFH_{avg}\ [DC = 1\ ] = n \bullet (n - 1) \bullet ... \bullet m \bullet \ \ ^{mt,}\ \ \frac{MTTR^{\ n\text{-}m}}{(n\ \ \text{-}m)!} \quad (13.4)$$

$$= (n - m + 1) \bullet C\text{"}\sim^{m}*'\ A\text{"}_{DD}{}^{mt1} \bullet MTTR\ \text{""}$$

Полученные результаты дают возможность найти общие соотношения, связывающие вероятности отказа низкого и высокого уровня требований безопасности *(см. главу "Современная концепция автоматизации", раздел "Термины и определения").*

Из уравнений (13.1) - (13.4) следует, что в общем виде связь вероятностей опасного отказа низкого и высокого (интенсивности отказов) уровня требований определяется следующими выражениями:

$$PFD_{Km0} = PFH_{BC\_\_0}\ \ T, /(n - m + 2) \quad (13.5)$$

$$PFD_{DCs1} = PFH_{nc}\ , \bullet MTTR /(n\text{-}m + 1) \quad (13.6)$$

В таблицах 13.7-13.8 воспроизводятся решения соотношений 13.1-13.4 для опасных обнаруженных и необнаруженных отказов наиболее значимых архитектур, дающие возможность еще раз удостовериться в справедливости наших выводов. Сравнение полученных результатов с некорректными решениями стандарта IEC 61508 для вероятности опасного отказа приводится в таблицах 13.10и 13.11.

13.40» Общие уравнения вероятности и интенсивности ложных срабатываний для систем произвольной архитектуры

(в стандарте IEC 61508 данные соотношения отсутствуют)

Элегантное решение для вероятности и интенсивности ложных срабатываний для архитектур общего вида можно получить, если обратить внимание на **зеркальность поведения архитектур типа *MooN* по отношению к опасным отказам, и архитектур типа *(N-M+1)ooN* по отношению к ложным срабатываниям.**

Ключом к решению является соотношение (13.3):

$$PFD_{s\,n\,p}^{(\sim m+1)oon} = PFD^{\text{™}\circ''} = C^{\wedge 1} \cdot (A \cdot MTTR)^{n\sim m+1}$$

Чтобы придать этому соотношению законченную форму, сделаем подстановку $к = (n\text{-}m+1)$. Тогда при $A = A_{SP}$ **автоматически** получаем соотношение вероятности ложного срабатывания для систем произвольной архитектуры *KooN:*

$$PFD_{p}^{ko\ on} = C_{n}^{k} \text{-}(A_{SP}\ \ MTTR)^{k} \qquad (13.7)$$

Аналогично, интенсивность ложных срабатываний архитектуры *KooN = (N-M+1)ooN* определится через интенсивность опасных отказов архитектуры *MooN:*

$$PFH_{s\,n\,p}^{(m+1)oon} = PFH^{\text{™}''} = (n\text{-}m + 1)\text{-}\ C^{\circ}\text{-}^{m+1} \cdot Я^{\,n} \quad \cdot MTTR^{n\ m}$$

С помощью подстановок $к = (n\text{-}m+1)$ и $A\sim A_{SP}$ получаем соотношение для интенсивности ложного срабатывания *(Spurious Trip Rate - STR):*

$$PFH \quad = STR \sim k\ \ C^{k}\ \ A^{k}_{SP} \cdot MTTR^{\,k\sim 1} \qquad (13.8)$$

Выражения вероятности и интенсивности ложного срабатывания для наиболее известных архитектур представлены в таблице 13.9. Еще раз:

Хотя для создателей стандарта IEC 61508 ложных срабатываний как бы и не существует, именно их якобы отсутствие и есть главное ложное срабатывание создателей стандарта. И абсолютное большинство разработчиков стандарта было вынуждено целиком согласиться и с позицией, и с результатами автора настоящей работы.

Таблица 13 7

Сводная таблица PFD и PFH для случая обнаружения опасного отказа во время автономного тестирования

Архитектура	Число каналов		PFH_{AVC}
1 Ш 1	-		
1оо2	2		$6 \cdot Я^2_{Ш} \cdot \Gamma,$
2оо4 (4-2-0)	2		
1оо3	3		
	3		
4оо6 (6-4-0)	-	$4\text{-}Я^2_{ои}$ Tf	12 $\text{-}ЛЬ$ $T,$
3оо3	3	${}^3я$ T	3 $я_{ои}$
1оо4	4	1 2^4 T^4	
2оо4	4	2^3_{DU} T_I^3	$4 \cdot л^3_{ш} \cdot m^2$
3оо4	4	$2 \cdot л^2_{0и}$ m^2	$б \cdot л^2_{ои} \cdot m,$
4оо4	4	$2 \cdot Я_{ои} \cdot T_1$	$4\text{-}Л_{ои}$

Таблица 13.8

Сводная таблица PFD и PFH для случая немедленного обнаружения опасного отказа

Архитектура	Число каналов	PFD_{AVG}	$^{PF}H_{AVG}$
	^ ^ Й		
.«««• 1	Z ^ . « d		Г " ^ i >. . . .. „J
~ * * <			i x . . . * « - w a *]
1 oo2D %			Ш ^ ^ Щ Ш Г r
"2oo4 (4-3-0)	2	$6 \cdot A^2_{dd}$ $MTTR^2$	$12\ A^2_{dd}\ MTTR$
"2oo4" (4-2-0)	2	$4 - A^2_{dd} \bullet MTTR^2$ i	$8\text{-}A^2_{DD}\ MTTR$
1oo3	3	$A^3_{dd}\ MTTR^3$	$3\ A^3_{dd}\ MTTR^2$
			ШШШШШ
"4oo6" (6-4-0)	3	$12 - A^2_{dd}\ MTTR^2$	$24 \cdot A^2_{dd} \cdot MTTR$
3oo3	3	$3\text{-}A_{DD}$ ' $MTTR$	$3 \bullet A_{dd}$
1oo4	4	$A^4_{dd} \bullet MTTR^4$	$4 \bullet A^4_{dd} \bullet MTTR^3$
2oo4	4	$4 \cdot A^3_{dd} \bullet MTTR^3$	$12 \bullet A^3_{dd}\ MTTR^2$
3oo4	4	$6\ \text{-}A^2_{DD}\text{-}\ MTTR^2$	$12 - A^2_{dd} MTTR$
4oo4	? j 4	$4\ A_{dd}\ MTTR$	

Таблица 13.9

Сводная таблица PFD и STR для ложного срабатывания

Архитектура	Число каналов	PFD_{AVG}	STR
^ШЩ		ЩШ	
"2oo4" (4-3-0)	2	$6 \cdot A^2_{)D} \cdot MTTR^2$	$72 \cdot A^2_{dd} \cdot MTTR$
"2oo4" (4-2-0)	2	$4 \cdot A^2_{dd} \cdot MTTR^2$	$8 \cdot A^2_{dd} MTTR$
3oo3	3	$A^3_{dd} \cdot MTTR^3$	$3\text{-}A^3_{DD} \cdot MTTR^2$
		r.^^sef^	Г^ффЩлф/
"4oo6" (6-4-0)	3	$12\ A^2_{dd}\ MTTR^2$	$24\ A^2_{dd}\ MTTR$
1oo3	3	$3\text{-}A_{DD}\text{-}\ MTTR$	$3>A_{dd}$
4oo4	4	$A^4_{dd} \cdot MTTR^4$	$4 \cdot A^4_{dd} \cdot MTTR^3$
3oo4	4	$4 \cdot A^3_{dd} \cdot MTTR^3$	$12 \cdot A^3_{dd}\ MTTR^2$
2oo4	4	$6\ A^2_{DD} \cdot MTTR^2$	$12 \cdot A^2 \cdot MTTR$
1oo4	4	$4\text{-}A_{dd}\ MTTR$	4

Таблица 13.10

Соотнесение решений IEC 61508 с точными решениями для случая обнаружения опасного отказа во время автономного тестирования (DC=0)

Архитектура системы	*PFDAVG* Согласно IEC 61508	*PFHAVG* Согласно IEC 61508	PFD_{AVG} Точные значения	*PFHAVG* Точные значения
	ШШш		p g f i	щ а
	S i l t)			
ЩШШШЩ	^ Jи.ви^	(G M M	1 Я Ш	
	i . ! _ _ . ! . l _ _ J			
яйкИЯжзй			Ш Ш 1	
	i i		L s l	
	ШЖк			
	l l !		!	!
			'JT »	

Таблица 13.11

Соотнесение решений IEC 61508 с точными решениями для случая немедленного обнаружения опасного отказа (DO1)

Архитектура системы	PFD_{AVG} Согласно IEC 61508	PFH_{AVG} Согласно IEC 61508	PFD_{AVG} Точные значения	PFH_{AVG} Точные значения
1oo1	$\lambda_{DD} \cdot MTTR$		$\lambda_{DD} \cdot MTTR$	λ_{DD}
2oo2	$2 \cdot \lambda_{DD} \cdot MTTR$		$2 \cdot \lambda_{DD} \cdot MTTR$	$2 \cdot \lambda_{DD}$
1oo2		$2 \cdot \lambda_{DD}^2 \cdot MTTR$	$\lambda_{DD}^2 \cdot MTTR^2$	$2 \cdot \lambda_{DD}^2 \cdot MTTR$
1oo2D			$\lambda_{DD}^2 \cdot MTTR^2$	$2 \cdot \lambda_{DD}^2 \cdot MTTR$
2oo3		$6 \cdot \lambda_{DD}^2 \cdot MTTR$	$3 \cdot \lambda_{DD}^2 \cdot MTTR^2$	$6 \cdot \lambda_{DD}^2 \cdot MTTR$

Таблицы 13.10 и 13.11 позволяют наглядно убедиться, что:

1. Решения стандарта МЭК соответствуют правильным решениям **только для нулевого уровня диагностики.**
2. **ШЕСТЬ соотношений стандарта ИЗ ДЕСЯТИ для 100% уровня диагностики дают неправильное решение.**

С выводами автора согласны и эксперты рабочей группы MT13 комитета SC65 по переработке стандарта [EC 61508, и члены комитета S84 по переработке приложения (отчета) TR 84.00.02-2009 к стандарту ANSI/ISA 84.01-96.

13.41. Право выбора

Как было во всех деталях исследовано в главе 1 *"Постановка задач автоматизации"* (см. разделы 1.17-1.20), системы 2oo3 не имеют никаких технических преимуществ перед системами loo2D. Поэтому, какая из конкретных систем более предпочтительна, в конце концов, решает потребитель.

Классические системы loo2D самодостаточны: они имеют архитектуру минимальной сложности для резервированных систем. Два набора модулей управления в сочетании с двумя наборами диагностических цепей создают уникальную четырехполюсную архитектуру, которая имеет минимально возможную вероятность и опасных, и безопасных отказов среди всех известных на сегодня архитектур.

Тем не менее, обе системы - и loo2D, и 2oo3 - аттестуются по RC5-6 и SIL3. Водораздел между системами класса RC5-6 и SIL3, и системами низших уровней допуска проходит вовсе не по количеству процессоров на модулях управления. Наивысшего ранга удостоены только те системы, которые допускают восстановление исходной конфигурации в режиме *on-line*, сохраняя при этом полный контроль над объектом управления, включая программно-управляемый останов.

Все прочие архитектуры - loo1, loo ID, 1oo2, 2oo2, - такой возможности не имеют, поэтому любой отказ этих систем приводит к жесткому физическому останову процесса. Потому эти системы и аттестуются не выше RC4 и SIL2.

Разница между этими двумя классами систем является принципиальной для подавляющего большинства современных технологических процессов:

Системы loo2D и 2oo3 позволяют произвести программно - управляемый останов, и определить первопричину останова. Кроме того, системы loo2D и 2oo3 идеально подходят для решения задач программно-логического управления как такового, в особенности для периодических процессов.

13.42. С чего начать?

Ключевыми стадиями для успешного создания АСУТП являются самые первые стадии, в которых определяются начальные условия всего процесса создания будущей системы, и в значительной степени предопределяется результат:

1. Формирование требований к АСУТП,
2. Разработка концепции АСУТП,
3. Разработка Технического задания на создание АСУТП.

Неформальное и тщательное выполнение этих стадий позволяет избежать множества проблем в последующей реализации проекта. В частности, при разработке и определении концепции АСУТП необходимо выполнить следующее: выбор конкретного поставщика средств автоматизации должен осуществляться на конкурсной основе с участием нескольких, как правило, **3 ± 1 поставщиков.**

Согласно методике профессора Э.Л. Ицковича (Институт Проблем Управления РАН), при проведении тендеров и при сравнении различных программно-технических комплексов необходимо исходить из учета следующих критериев:

1. Технический уровень оборудования и программного обеспечения;
2. Уровень обеспечения требуемой надежности;
3. Уровень полноты программных средств и простоты конфигурирования;
4. Степень защиты от проникновения в систему;
5. Опыт применения данного оборудования на аналогичных объектах;
6. Уровень доверия к поставщику оборудования и программного обеспечения;
7. Способность выполнить весь спектр работ по созданию АСУТП - от обследования технологического объекта до пуско-наладочных работ;
8. Адекватность цены и предлагаемых средств и услуг.

Процедура выбора конкретного поставщика для конкретного объекта состоит из выполнения следующих шагов:

1. Определение технических требований к составу и качеству оборудования и программного обеспечения;
2. Анализ рынка АСУТП и выбор поставщиков, участвующих в тендере;
3. Рассылка требований;
4. Получение и анализ полученной технической и коммерческой информации;
5. Составление сводных таблиц для сопоставления предложений;
6. Организация группы экспертов из представителей заинтересованных служб предприятия;
7. Определение критериев и их ранжирование;
8. Индивидуальная работа экспертов над полученными данными;
9. Составление сводных таблиц с экспертными оценками;
10. Ранжирование потенциальных поставщиков в соответствии с полученными средневзвешенными показателями;
11. Утверждение результатов и окончательный выбор поставщика.

По окончанию данной стадии разрабатывается отчет. В основной части отчета приводят:

1. Описание результатов обследования объекта автоматизации;
2. Описание и оценку преимуществ и недостатков разработанных альтернативных вариантов концепции создания АСУТП;
3. Сопоставительный анализ требований Заказчика к АСУТП и вариантов построения АСУТП;
4. Обоснование выбора наиболее рационального варианта концепции и описание предлагаемой АСУТП;
5. Ожидаемые результаты и эффективность реализации выбранного варианта концепции АСУТП;
6. Ориентировочный план реализации выбранного варианта построения АСУТП;
7. Оценка затрат на реализацию проекта создания АСУТП.

Здесь необходимо сделать важное уточнение. Вовсе не обязательно зацикливаться на бесконечных тендерах по каждому объекту: выбор каждого НОВОГО поставщика оборудования и услуг должен диктоваться не конъюнктурой, а только действительной необходимостью, и оценкой РЕАЛЬНЫХ долговременных последствий выбора.

В выигрыше оказываются те предприятия, которые сумели не размазать, а сконцентрировать усилия на ключевых направлениях, определив в качестве генеральных поставщиков конкретных единиц оборудования и услуг самых авторитетных представителей на рынке автоматизации, и оформившие с ними долгосрочные соглашения о сотрудничестве.

13.43. Стандарты МЭК - призыв к осмотрительности

Необходимо критически относиться к сведениям из проспектов поставщиков оборудования безопасности, и всегда перепроверять наличие сертификатов третьей стороны на фактический уровень допуска предлагаемого оборудования по последним международным стандартам - IEC 61508, 1EC 61511. Но, к сожалению, и сертификаты не гарантируют соответствие оборудования заявленным характеристикам. К примеру, сокращение расчетного межповерочного интервала в два раза приводит к пропорциональному снижению расчетной вероятности опасного отказа в два раза, и соответственно к искусственному завышению характеристик системы.

В стандартах IEC 61508 и 61511 прямо указывается на **необходимость опыта непосредственного применения конкретных систем безопасности в течение достаточного интервала времени на различных процессах, как одного из решающих условий выбора.** В особенности это касается комплексных компонент системы с многочисленными функциями. Заказчик должен точно знать, какие из этих функций действительно были проверены на практике.

Вполне понимая неоднозначность проблемы выбора конкретной системы безопасности, Международная электротехническая комиссия рекомендует проявлять сдержанность по отношению к любому появлению существенной новизны в отношении программируемых электронных систем в промышленности.

13.44. Использование единой платформы программно-технических средств, и выбор единого подрядчика по созданию АСУТП

Выбор единого подрядчика оборудования и услуг, связанных с созданием АСУТП, продиктован стремлением к унификации и единообразию проектных решений на всех папах создания эффективной системы управления и защиты технологического процесса. При этом необходимо отдавать себе отчет, что ответственность за результаты данного выбора возрастает пропорционально той роли, которая будет возложена и которую возьмет на себя конкретный генподрядчик АСУТ11. Заказчику нужна полная уверенность в успешном выполнении проекта. Не должно быть никаких сомнений в способности подрядчика выполнить весь объем работ в установленные сроки с заранее заданным качеством.

Проверка дееспособности потенциальных преюндетои должна быть произведена с исключительной тщательностью, чтобы выбор был сделан в пользу поставщика, успешно реализующего проекты подобного масштаба в течение последних 5-10 лет и в России, и за рубежом.

Некоторые фирмы предлагают в качестве неоспоримою преимущества своих систем так называемое свойство "открытости". Под этим качеством понимается возможность объединения в рамках общей системы оборудования и программной обеспечения самых разных производителей.

Согласиться с таким подходом можно только в том слу чае, когда у Заказчика уже существует, или в силу объекшв ных обстоятельств он вынужден установить несколько разно родных систем, которые затем будут объединяться в общи! комплекс. Этот подход обычно используется на предприятия: пищевой, фармацевтической, целлюлозно-бумажной, мс і ал лургической промышленности и тому подобных произволе) вах, на которых сосредоточено большое количество разнород ных дискретных или периодически действующих узлов и ;и регатов (конвейеры, смесители, печи, дозаторы, упаковочпы машины и т.д.). Эти агрегаты обычно полностью укомплект ваны средствами автоматизации, и поставляются комплект со своими собственными панелями управления и специализи рованными контроллерами.

Для объединения разнотипного оборудования приходится применять универсальные открытые сети общего назначения типа Ethernet.

Таким образом, в обмен на возможность применения разнородного, но потенциального любого оборудования приобретается множество проблем, связанных с эксплуатацией и обслуживанием программно-технических комплексов разных производителей. Плюс - открытые для несанкционированного доступа недетерминированные сети, и проблема защиты от внешнего вмешательства и проникновения вирусов.

Для современных систем управления и защиты непрерывных нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств современный уровень требований заключается в максимально возможной унификации оборудования и программного обеспечения с учетом потенциально возможного расширения архитектуры и функций системы без привнесения инородных элементов.

Такой подход предопределен спецификой данных производств: современные распределенные системы управления и защиты непрерывных химических, нефтехимических и нефтеперерабатывающих производств **заранее проектируются под конкретные применения** с заведомо известными требованиями и параметрами технологических процессов.

Поэтому в качестве фундаментального требования к оборудованию и программному обеспечению АСУТП выступает не абстрактная "открытость", а напротив, детерминированность (строгая определенность и предсказуемость) поведения, и жесткость, устойчивость программно-технической конструкции для конкретного применения.

Универсальность применения специальных РСУ и ПАЗ достигается за счет воплощения и реализации многолетнего опыта для всего спектра нефтегазодобывающих, химических, нефтехимических и нефтеперерабатывающих производств, наработанного производителем и проектировщиком. Данный класс систем не нуждается в некоем эфемерном предположении о потенциально возможном применении каких-то неизвестных на момент проектирования установки подсистем. Предполагается, что как проектировщик технологического процесса, так и проектировщик АСУТП имеют ясное представление о конечном результате.

При непременном условии, что процедура выбора конкретного исполнителя будет проведена со скрупулезной тщательностью по всем без исключения критериям оценки, данный подход предоставляет множественные и значительные преимущества.

1. **Коммерческие преимущества:**
   - 1.1. Соглашение о договорной цене на основное оборудование РСУ и ПАЗ в течение всего срока выполнения проекта;
   - 1.2. Общий контроль над целевым использованием средств.
2. **Организационные преимущества:**
   - 2.1. Единые стандарты, нормы и правила выполнения работ по созданию АСУТП;
   - 2.2. Единая взаимная ответственность Генподрядчика и Заказчика;
   - 2.3. Отработанные схемы взаимодействия между всеми участниками проекта;
   - 2.4. Единый График выполнения проекта.
3. **Сокращение сроков проектирования и внедрения АСУТП:**
   - 3.1. Унификация проектных решений;
   - 3.2. Упреждающая разработка;
   - 3.3. Единообразная проектная и рабочая документация.
4. **Сокращение затрат на этапе монтажа, пусконаладки и внедрения:**
   - 4.1. Унификация оборудования и программного обеспечения;
   - 4.2. Унификация технических решений;
   - 4.3. Ускоренная подготовка и обучение персонала.
5. **Сокращение затрат на этапе эксплуатации и технического сопровождения:**
   - 5.1. Уменьшение страхового запаса ЗИП;
   - 5.2. Простота внесения модификаций;
   - 5.3. Взаимозаменяемость узлов и модулей;
   - 5.4. Сокращение численности эксплуатационного и обслуживающего персонала;
   - 5.5. Уменьшение частоты проведения планово-предупредительного ремонта;
   - 5.6. Повышение надежности системы.

БИБЛИОГРАФИЯ

1. ГОСТ 1.5-2004 ПРАВИЛА ПРОВЕДЕНИЯ РАБОТ ПО МЕЖГОСУДАРСТВЕННОЙ СТАНДАРТИЗАЦИИ. Общие требования к построению, изложению, оформлению и содержанию стандартов.
2. ГОСТ 7.32-2001 Отчет о научно-технической работе. Структура и правила оформления.
3. ГОСТ 2.106-96 ЕСКД Текстовые документы.
4. ГОСТ 24.104-85 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы управления. Общие требования.
5. ГОСТ 34.003-90 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Термины и определения.
6. ГОСТ 34.201-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды, комплектность и обозначение документов при создании автоматизированных систем.
7. ГОСТ 34.601-90 ЕСС АСУ. Автоматизированные системы. Стадии создания.
8. ГОСТ 34.602-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
9. ГОСТ 34.603-92 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды испытаний автоматизированных систем.
10. ГОСТ 24.701-86 ЕСС АСУ. Надежность автоматизированных систем управления. Основные положения.
11. ГОСТ 27.301-95. Надежность в технике. Расчет надежности. Основные положения. М.: Издательство стандартов, 1997.
12. РД 03-418-01. Методические указания по проведению анализа риска опасных производственных объектов. Госгортехнадзор, 2001.

13. ГОСТ 24.702-85 ЕСС АСУ. Эффективность автоматизированных систем управления. Основные положения.
14. ПБ 09-540-03 "Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств".
15. СНиП 3.05.07-85 Системы автоматизации.
16. РД 50-34.698-90 МЕТОДИЧЕСКИ УКАЗАНИЯ. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Требования к содержанию документов.
17. ГОСТ Р 8.596-2002. ГСИ. Метрологическое Обеспечение измерительных систем. Основные положения.
18. МИ 2439-97. Метрологические характеристики измерительных систем. Номенклатура. Принципы регламентации, определения и контроля.
19. МИ 2441-97. Испытания для целей утверждения типа измерительных систем. Общие требования.
20. ПР 50.2.009-94 ГСИ. Порядок проведения испытаний и утверждения типа средств измерений.
21. Стандарт DIN V 19250 "Fundamental Safety Aspects To Be Considered For Measurement And Control Protective Equipment" (Фундаментальные аспекты безопасности, рассматриваемые для связанного с безопасностью оборудования измерения и управления).
22. Стандарт DIN V VDE 0801 "Principles For Computers In Safety Related Systems" (Принципы для компьютеров в системах, связанных с безопасностью).
23. Стандарт ANSI/ISA 84.01-96 "Application of Safety Instrumented Systems for the Process Industries" (Применение оборудованных под безопасность систем для технологических процессов).
24. Стандарт IEC 61508 "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems" (Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью).
25. Стандарт IEC 61511 " Functional Safety: Safety Instrumented Systems for the Process Industry Sector" (Функциональная безопасность: Оборудованные под безопасность системы для перерабатывающего сектора промышленности).

ОГЛАВЛЕНИЕ

СПРАВОЧНИК
ИНЖЕНЕРА ПО АСУТП:
Проектирование и разработка

Учебно-практическое пособие

Руководитель проекта
К.Н. Уваров

Главный редактор
О.С. Швецова

Корректор
Е.В. Лукина

Подписано в печать 16.04.2008.
Формат 84x108/32. Бумага офсетная.
Гарнитура «Прагматика».
Объем 29 печ. л.
Тираж 2000 экз. Заказ № 3110.

Отпечатано с готового оригинал-макета
в ООО ПФ «Полиграф-Книга».
160001, г. Вологда, ул. Челюскинцев, 3.
Тел.: (8172) 72-55-31, 72-61-75

Издательство «Инфра-Инженерия»
109004, г. Москва, Николоямский пер., д.4-6, стр. 3.
Тел.: 8(911)512-48-48
E-maii: infra-e@yandex.ru

Исследование методов создания систем будет актуальным всегда и для всех - от дилетантов, до профессионалов.

В настоящей работе автор развивает идеи, представленные в монографии «Основы построения АСУТП взрывоопасных производств», Синтег, 2006, вызвавшей значительный интерес отечественных и западных специалистов.

Предлагается продуманная и проверенная практикой методология построения АСУТП, восполняющая отсутствие специальной технической литературы на заданную тему.

«In regards to your work, I enjoyed it immensely. I am impressed by how you provided such a detailed mathematical presentation of the issues induced by IEC 61508 methodologies. Your work caused quite a stir. Best Regards», -

A. E. Summers, Ph.D., P.E., President of SIS-TECH Solutions, USA, член комитета SC65A по переработке стандарта IEC 61508, председатель комитета по переработке технического отчета ISA-TR84.00.02-2009 к стандарту ANSI/ISA 84.01 -96.

«First at all I would like to thank Dr. Fedorov because he shows, in another form, what I (and also Yoshi Kaiyodai) have already tried to tell several times:

There is problems with definitions.
There is problems with probabilistic calculations (IEC 61508-6),
Spurious trips handling is missing», -

Jean-Pierre Signoret, Total, France, руководитель группы MT13 по переработке математической части стандарта IEC 61508.

ISBN 978-5-9729-0019-0