# Тенденции развития безопасных систем автоматизации

Ю.Н. Федоров (ООО "Кама-Автоматика")

*Анализируются достоинства и недостатки стандартов Международной электротехнической комиссии (МЭК) IEC 61508, IEC 61511. Рассматривается состояние отечественной нормативной базы в части создания безопасных систем управления и защиты. Впервые предлагается соответствие отечественных категорий взрывоопасности и зарубежных классов и уровней интегральной безопасности. Даются рекомендации по выбору архитектуры систем защиты в зависимости от категории взрывоопасности. Предлагаются меры по укреплению нормативной базы предприятий путем утверждения Стандарта предприятия на проектирование, разработку, внедрение и эксплуатацию АСУТП.*

Особенность автоматизированных систем заключается в том, что системы, предназначенные для управления и защиты ТП, сами по себе представляют значительную опасность. Сложность ТП приводит к усложнению автоматизированных систем и еще большему увеличению потенциала опасности.

С появлением микроэлектроники системы управления и защиты ТП становятся все более мощными, и возникает проблема обоснованности применения электронных систем в отраслях промышленности, связанных с опасностью. Исследования, проведенные Международной электротехнической комиссией (МЭК) в конце 80-х – начале 90-х гг., 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.

Одним из важнейших событий последних лет в области безопасного применения электронных средств в промышленности является появление стандартов МЭК – IEC 61508 [1] и IEC 61511 [2]. Часть 1 стандарта IEC 61508, пункт 1.1 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 (Е/Е/РЕ) связанных с безопасностью систем в тех областях, в которых прикладной сектор международных стандартов отсутствует".*

**Интегральная и функциональная безопасность.** К сожалению, в нашем отечестве в последние годы выбор оборудования АСУТП все чаще становится одновременно и первой, и последней стадией проекта создания АСУТП. Система рассматривается как набор обособленных групп оборудования, а договор на поставку – как эквивалент самого проекта.

Стандарты МЭК отстаивают подход, основанный на понятиях общей (интегральной) и функциональной безопасности. Система становится системой, если достигается соразмерность структуры и функций. Вместо того чтобы проектировать систему *"настолько хорошо, насколько это возможно"*, а затем считать ее достаточно безопасной, стандарты предлагают подход, основанный на анализе рисков. Все действия по обеспечению безопасности должны основываться на понимании и оценке риска, который неизбежно присутствует в любой системе. Стандарты МЭК 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. Меры по снижению риска подразделяются на два компонента:

- общие (интегральные) требования безопасности (Safety integrity requirements);
- функциональные требования (Functional requirements).

Соответственно Спецификация требований безопасности (Safety Requirements Specification – SRS – аналог нашего ТЗ) должна определять:

- Спецификацию требований интегральной безопасности, содержащую общие требования безопасности, которую должна обеспечивать система;
- Спецификацию требований функциональной безопасности, содержащую требования к самим функциям безопасности, которые должна выполнять система.

Главным объектом анализа становится *функция безопасности* – группа элементов, осуществляющая самостоятельную, относительно независимую группу операций управления и защиты. Относительность независимости определяется влиянием общих отказов (как например, отказ единственного источника питания) на подсистему или на всю систему безопасности в целом. В общем случае *функция безопасности* определяется как функция, предназначенная для достижения и поддержки безопасного состояния контролируемого оборудования по отношению к опреде-

*Таблица 1*

| SIL | Вероятность опасного отказа | Степень защиты |
|---|---|---|
| 4 | $10^{-5}$... $10^{-4}$ | Защита от общей катастрофы |
| 3 | $10^{-4}$...$10^{-3}$ | Защита персонала и оборудования |
| 2 | $10^{-3}$...$10^{-2}$ | Защита оборудования и защита от травматизма |
| 1 | $10^{-2}$...$10^{-1}$ | Защита оборудования и продукции |

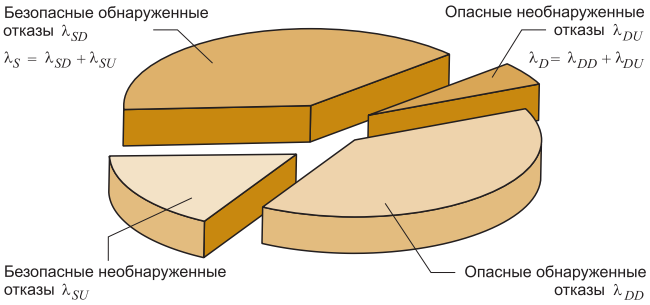



*Рис. 1*

ленному опасному событию. Функции безопасности в интерпретации МЭК фактически являются полным аналогом *контуров безопасности (защиты)*, а *интегральная безопасность* – не более чем *надежность системы*. Надо сказать, оба стандарта МЭК написаны довольно косноязычным англо-французским языком с изрядно запутанной терминологией, и требуется некоторое усилие, чтобы включиться в их систему координат.

Стандарт IEC 61508 использует единую меру снижения риска, которая впервые была предложена американским стандартом ANSI/ISA 84.01-1996 (ранее – S84.01-1996) [3]. Эта мера определяется *интегральным уровнем безопасности – Safety Integrity Level (SIL), который задает требуемую меру снижения риска*. Смысл его состоит в следующем: чем большее снижение риска требуется, тем более объект становится зависимым от самой системы защиты, обеспечивающей это снижение, и тем большее значение SIL необходимо для общей безопасности. Проще говоря, чем более ответственным является объект, тем более надежной должна быть система. SIL и является той мерой, которая определяет степень безопасности самой системы безопасности. Согласно IEC 61508, SIL – это дискретная величина от единицы до четырех, предназначенная для определения уровня требований к интегральной безопасности (табл. 1).

Считается, что высший уровень *SIL4* по вероятности неблагоприятного события соответствует катастрофическому событию. На сегодняшний день существует всего лишь несколько контроллеров, аттестованных по уровню *SIL4*. Радикальным отличием этих контроллеров является отсутствие системного, диагностического и вообще какого бы то ни было ПО. Технология основывается на ферритовой логике, определяющей алгоритмы 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. Применение эти контроллеры находят на самых опасных ТП.

На первый взгляд, представленные значения вероятностей отказа *SIL3* вполне приемлемы и для современных технических средств легко достижимы. Однако для реальных автоматизированных систем среднего класса, состоящих из нескольких тысяч сигналов ввода/вывода, лобовой расчет вероятности отказа системы даже на минимальном временно́м интервале в 1 год дает просто угрожающие значения. Далее будет представлено авторское понимание решения этой проблемы.

Стандарт IEC 61511 определяет *систему (интегральной) безопасности (Safety Integrity System – SIS) 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"*.

Это определение является парафразом определения из стандарта ANSI/ISA 84.01-1996. Стандарт ANSI/ISA 84.01-1996 определяет систему безопасности термином *"Safety Instrumented System – SIS"*, что в буквальном переводе означает: *"Оборудованная под безопасность система"*. Стандарт определяет систему безопасности как *"Систему, состоящую из сенсоров, логических решающих устройств и конечных (исполнительных) элементов, предназначенную для перевода процесса в безопасное состояние при возникновении нарушения предопределенных условий"*. (Автор публикации приглашен к участию в подготовке новой версии стандарта ANSI/ISA 84.01-1996 в составе одного из комитетов ISA – ред.).

В общем случае система безопасности предназначена для:

- осуществления действий, направленных на предотвращение технологических нарушений;
- автоматического перевода ТП в безопасное состояние при возникновении нарушения предопределенных условий;
- разрешения на продолжение работы ТП при исчезновении нарушения предопределенных условий.

**Специфика систем безопасности.** Многие неприятности, связанные с системами безопасности, вызваны неучетом специфики этих систем. Системы безопасности обладают рядом специфических свойств, присущих только этим системам:

- должны находиться в непрерывном контроле параметров процесса, однако по определению никак не могут проявить свою дееспособность до момента наступления опасного события;
- могут формально находиться в работе, но в момент наступления опасного события на процессе не способны отреагировать на него. Подобный тип отказа принято называть опасным отказом;
- могут совершить немотивированный ложный останов процесса, в то время как в действительности ничего опасного на процессе не произошло. Подоб-

*Прогресс имеет один недостаток: время от времени он взрывается.*
Элиас Канетти

ный тип отказа некоторые люди (например, эксперты МЭК) называют "безопасным" отказом.

Стандарт IEC 61508 подразделяет отказы системы безопасности на опасные с интенсивностью отказов $\lambda_D$ и безопасные с интенсивностью отказов $\lambda_s$ – обнаруженные и необнаруженные – и в части 4 дает их определения (рис. 1).

**Вероятность опасного отказа.** Стандарт IEC 61508 в шестой части приводит соотношения для средней вероятности опасного отказа $PFD_{AVG}$ в течение преопределенного межповерочного интервала (в отечественной практике – 1 год), и средней интенсивности опасных отказов $PFH_{AVG}$, однако дает их без каких бы то ни было объяснений, откуда они взялись. Анализ этих соотношений показывает, что они дают неверные оценки вероятности отказа для высоких уровней самодиагностики. В работе [4] подробно исследована природа соотношений стандарта IEC 61508 для определения вероятности и интенсивности опасного отказа. В результате исследования получены:

• корректные соотношения вероятности и интенсивности опасных отказов для базовых архитектур стандарта IEC 61508;

• общие соотношения для вероятности и интенсивности опасного отказа для систем произвольной архитектуры, отсутствующие в стандарте.

**Отсутствие оценок вероятности ложного срабатывания.** Наиболее серьезным пробелом стандарта IEC 61508 является недоведенное до конца исследование структуры отказов систем безопасности. Стандарт не дает никаких рекомендаций по оценке вероятности так называемых "безопасных" отказов, которые на практике означают немотивированный, ложный останов процесса, и как раз-то и могут представлять значительную опасность. 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 неспособных 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.*

Понятие "безопасный отказ" – самое неудачное понятие для тех, кто использует оборудование и системы безопасности. 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?.. И в то же время *это понятие очень удобно для производителей и поставщиков оборудования.* Фактически оно означает безопасность самой системы безопасности от ТП. Система защиты просто снимает с себя какую бы то ни было ответственность за факт и результат ложного срабатывания.

В отличие от стандарта МЭК, американский стандарт ANSI/ISA 84.01-1996 дает вполне корректные определения. Согласно этому стандарту, ложное срабатывание определяется как *"ложное, беспричинное срабатывание блокировки (spurious trip, nuisance trip, false shut down) или немотивированный останов процесса по причинам, не связанным с действительными событиями на процессе".*

Ложное срабатывание может произойти: из-за ошибки обслуживания, неправильной калибровки; неверной предаварийной уставки; отказов полевого оборудования, модуля ввода/вывода, центрального процессора; из-за ошибки ПО; электрического сбоя; электромагнитной наводки; короче – из-за чего угодно.

*Отсутствие расчетов вероятности ложных срабатываний*, которые для взрывоопасных производств, как минимум, создают предпосылки к аварийной ситуации, *является самым серьезным пробелом стандарта IEC 61508.* Эту оценку разделяют и члены рабочей группы MT13 комитета IEC SC65A по переработке стандарта IEC 61508, которым автор направил результаты своих исследований, полученные в работе [4]:

• соотношения для вероятности ложного срабатывания и среднего времени наработки на ложное срабатывание для базовых архитектур систем безопасности, отсутствующие в стандарте IEC 61508;

• общие соотношения для вероятности и интенсивности ложных срабатываний для систем произвольной архитектуры, также отсутствующие в стандарте.

Остается надеяться, что полученные результаты помогут закрыть серьезные бреши в конструкции стандартов IEC 61508 и IEC 61511.

**Степень доверия к заявленному уровню интегральной безопасности**. Во всех странах применение электронных систем (в том числе и программируемых) в качестве систем противоаварийной защиты регламентировано существующими национальными и международными стандартами, и требует специальной сертификации для определения допуска к применению. Однако надо ясно понимать, что наличие сертификатов на уровень допуска по самым международным стандартам не дает никакой гарантии. В основе выбора должен находиться только *опыт практического применения.* И этот опыт применения технических средств для конкретного класса ТП должен быть проверен и документально подтвержден.

Зная это, поставщики, тем не менее, предлагают свои индивидуальные устройства (будь то полевые устройства или контроллеры) как сертифицированные на определенный уровень SIL продукты. Более того, производители предлагают совершенно новые устройства, которые не могли пройти никакой серьезной проверки в полевых условиях.

Те производители и поставщики, которые дорожат своей репутацией, даже после всеобъемлющего тестирования в лабораторных условиях рекомендуют пользователям применять новые устройства только в некритичных приложениях, чтобы и пользователь, и производитель могли выявить все ошибки, необнаруженные при стендовых испытаниях. 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 взрывоопасных объектах. В особенности это касается комплексных компонент системы с многочисленными функциями: пользователь должен точно знать, какие из этих функций действительно были проверены на практике.

**Требования к полевым испытаниям систем безопасности**. При закупке импортного оборудования наличие сертификата на право использования данного оборудования на объектах того или иного класса требований *теоретически* позволяет использовать это оборудование как законченное изделие, удовлетворяющее определенному уровню требований, поскольку предварительные расчеты, испытания и проверки проведены и представлены потребителю. Кроме того, потребитель может быть уверен, что предоставленные данные по надежности системы были проверены независимой третьей стороной.

Вместе с тем, вполне понимая неоднозначность выбора конкретной системы безопасности, МЭК рекомендует проявлять *сдержанность по отношению к любому появлению существенной новизны в отношении программируемых электронных систем в промышленности*. Важнейшим положением стандартов IEC 61508 и 61511 является прямое указание на необходимость *опыта непосредственного применения* систем безопасности в течение достаточного интервала времени на конкретных процессах как одного из решающих условий выбора. В этой связи исключительное по важности значение имеют жесткие требования стандартов МЭК к полевым испытаниям систем безопасности.

Чтобы система считалась прошедшей полевые испытания, стандарты IEC 61508 (часть 7, пункт B.5.4) и IEC 61511 (часть 4) требуют, что должны быть выполнены следующие условия:

- неизменная спецификация;
- 10 систем в различных приложениях;
- $10^5$ рабочих часов (11,42 года, то есть по году на систему);
- как минимум 1 год сервисного обслуживания.

Для исключения расширенной перепроверки или перепроектирования системных программных модулей при каждом новом применении должны быть выполнены требования, которые позволят удостовериться, что программные модули свободны от систематических ошибок проектирования и разработки, или от оперативных отказов:

- неизменная спецификация;
- 10 систем в различных приложениях;
- вероятность неопасных отказов в течение года $10^{-5}$ с доверительной вероятностью 99,9%;
- отсутствие опасных отказов.

Сведения о том, что система прошла данные испытания на практике, должны быть предоставлены изготовителем или поставщиком системы в виде конкретных документов, подтверждающих *опыт применения на аналогичных технологических объектах*. Для проверки того, что компонент оборудования или модуль ПО отвечает всем этим критериям, следующие позиции должны быть документированы:

- точная идентификация системы и ее компонентов, включая контроль версии ПО и соответствующего оборудования;
- послужной список системы с указанием потребителей и даты внедрения, а также время эксплуатации;
- процедуры для выбора системы под конкретные применения, и варианты применения;
- процедуры для выявления отказов, их регистрации и устранения.

Важно помнить, что кроме требований к отдельным компонентам системы безопасности, функциональные требования IEC 61508 установлены для *всего контура безопасности* – от датчика до клапана, и степень соответствия этим требованиям должна быть проверена для каждого конкретного применения.

**Проектная оценка надежности системы.** Здесь, как нигде, нужно суметь соблюсти меру между необходимым и достаточным уровнем обобщения. Имеется в виду следующее:

- с одной стороны, нельзя ограничиваться данными от поставщиков оборудования по надежности отдельных компонентов системы (модулей, блоков, датчиков, клапанов и т.д.). Понятно, что эти данные никак не будут представлять уровень надежности системы;
- с другой стороны, от разработчика системы вряд ли стоит требовать расчета суммарной надежности по всему программно-техническому комплексу системы, имеющей несколько тысяч каналов ввода/вывода. Очевидно, что вне зависимости от того, что считать единичным отказом – отказ единичного элемента, или отказ некоторой группы элементов (контура) – для любой архитектуры всегда существует верхний предел по числу элементов системы, при котором суммарная вероятность отказа системы превысит единицу.

Необходимо соблюсти разумный компромисс между единичным (функциональным) и общим (интегральным) аспектом надежности. Этот компромисс может быть найден в расчете надежности комплексных функций безопасности – самостоятельных, "единичных" контуров защиты. Если под единичной функцией защиты понимать, в том числе и комплексную функцию, состоящую из нескольких взаимоувязанных ветвей с собственной логикой, то этот уровень обобщения следует признать вполне достаточным. Если угодно, можно интерпретировать такую комплексную функцию безопасности как своего рода аналог многопараметрического прогнозирующего контроллера для некоторого технологичес-

кого узла соответствующей системы усовершенствованного управления. Важно только не забывать, что такой комплексный контур должен рассчитываться с учетом всех компонентов – начиная от датчиков, барьеров, источников питания и заканчивая исполнительными элементами. Если рассматривать проблему оценки надежности системы под таким углом, появляется возможность декомпозиции абстрактной массы отказов на самостоятельные и осмысленные функции защиты.

Данное решение не вступает в противоречие с концепцией интегральной безопасности (общей надежности) стандартов МЭК. Ведь стандарты вовсе не требуют считать любой единичный отказ какого-либо из элементов системы за отказ всей системы. Таким образом, предлагается под вероятностью отказа системы понимать не абстрактную совокупность вероятностей отказа отдельных элементов и устройств, а суперпозицию независимых вероятностей отказа элементарных и комплексных функций (контуров) безопасности.

Одно важное замечание. 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 ТЗ на создание АСУТП взрывоопасного производства.*

**Диаграмма 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 диаграмма рисков по немецким стандартам DIN V 19250 [5] и DIN V VDE 0801 [6]. Классификация DIN класса требований к системе защиты по уровню опасности ТП построена с глубоким пониманием существа проблемы и заслуживает серьезного отношения. Стандарт DIN V 19250 устанавливает иерархию систем безопасности, соответствующих требованиям установленных классов АК (*Anfonderungs Klasse*), начиная с АК1 и заканчивая АК8 (соответствующее английское сокращение – *Requirements Class RC*). Стандарт рассматривает следующие факторы риска, свойственные ТП:

- последствия аварии $S_i$, $i = 1,...4$;
- интенсивность (частота и время) нахождения в опасной зоне $A_j$, $j = 1,2$;
- 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. 2). Итоговый класс требований к системе безопасности определяется целочисленной функцией: RC = RC($S_i$, $A_j$, $G_m$, $W_n$).

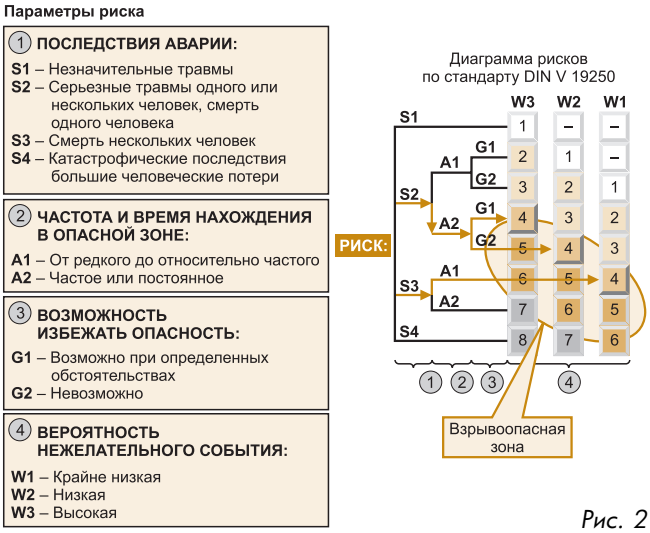



*Рис. 2*

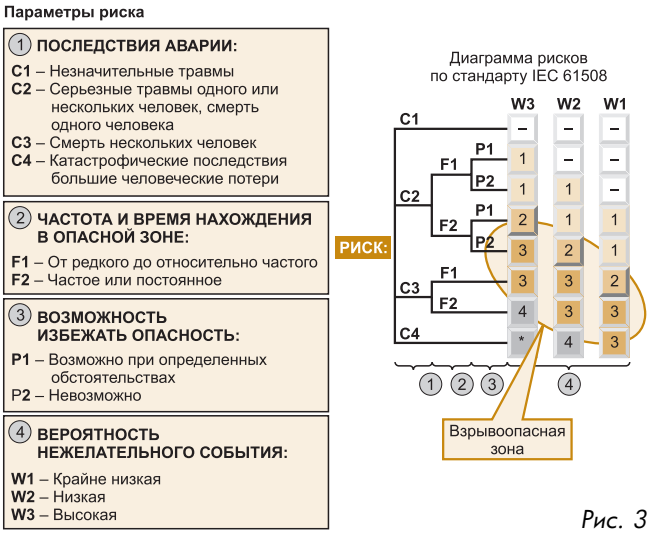



*Рис. 3*

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 (рис. 3).

В первую очередь обращает на себя внимание то обстоятельство, что 3 критических пути к наиболее простым одноканальным системам защиты *1oo1D* класса *RC4* (на рис. 2 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 химических, 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 сис-*

*Таблица 2. Соответствие отечественных категорий взрывоопасности зарубежным классам и уровням безопасности*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| % Надежности / готовности: | | | 90 | 99,0 | 99,9 | 99,99 | 99,999 |
| Вероятность опасного отказа: | | | 0,1 | 0,01 | 0,001 | 0,0001 | 0,00001 |
| ПБ 09-540-03 | Категория | | | III | II I | | |
| DIN V 19250 | AK | 1 | 2 3 | 4 | 5 6 | 7 8 | |
| DIN V VDE 0801 | RC | 1 | 2 3 | 4 | 5 6 | 7 8 | |
| ANSI/ISA 84.01 | SIL | | 1 | 2 | 3 | | |
| IEC 61508 | SIL | | 1 | 2 | 3 | 4 | |

*Таблица 3. Применение различных архитектур систем безопасности в зависимости от категории взрывоопасности*

| Категория | RC | SIL | Архитектура системы | Пояснение |
|---|---|---|---|---|
| III | 4 | 2 | Нерезервированные (1oo1) или резервированные (1oo2) входы | Периодическое тестирование входов. Входы могут быть аналоговыми или дискретными |
| | | | ПЛК 1oo1D<br>Стандартные контроллеры РСУ | ПЛК с двумя центральными процессорами или резервированными модулями управления. Или по согласованию с технадзором – выделенное резервированное оборудование РСУ |
| | | | Нерезервированные (1oo1) выходы | Периодическое тестирование выходов |
| II | 5 | 3 | Резервированные (1oo2) входы | Оперативное тестирование входов. Входы могут быть аналоговыми или дискретными |
| | | | Архитектуры 1oo2D, 2oo3 | Полностью резервированные (дублированные, троированные) системы |
| | | | Нерезервированные (1oo1) выходы | Оперативное тестирование выходов |
| I | 6 | 3 | Резервированные (1oo2 или 2oo3) входы | Оперативное тестирование входов. Голосующие входы – аналоговые |
| | | | Архитектуры 1oo2D, 2oo3 | Полностью резервированные (дублированные, троированные) системы |
| | | | Резервированные (1oo2) выходы | Оперативное тестирование выходов |

*темы не ниже 5-го класса*, а единственной степенью свободы является выбор из архитектур *1oo2D* или *2oo3*. Таким образом, мы приходим к принципиально важному результату, а именно:

**Классы 4 – 5 – 6 соответствуют нашим III – II – I категориям взрывоопасности.**

Дополнительным подтверждением корректности соответствия категорий *II-I* классам *RC 5-6* является принадлежность пары *RC 5-6* к одному общему уровню интегральной безопасности *SIL3*.

Полученные результаты сведены воедино в виде таблицы соответствия стандартов России, Германии, США и стандартов МЭК (табл. 2).

Рекомендации по выбору архитектуры систем защиты для взрывоопасных объектов приводятся в табл. 3.

*Простейшая процедура предварительного выбора* требуемой системы безопасности могла бы заключаться в следующем:

- для обеспечения интегрального уровня безопасности система защиты должна быть построена соразмерно, то есть иметь резервирование необходимого типа не только для основного оборудования АСУТП, но также и для сенсоров, и для исполнительных элементов, определяющих безопасность процесса;
- в соответствии с категорией взрывоопасности объекта и с учетом временных ограничений на работу в неполной конфигурации определить соответствующий класс требований и интегральный уровень безопасности системы.

Вместе с тем необходимо отдавать себе отчет, что выбор, сделанный таким тривиальным путем, серьезно ослабляет уверенность в адекватности выбора. Поэтому нелишне еще раз напомнить, что при определении класса требований должны приниматься в расчет все аспекты безопасности ТП, такие как:

- допустимое время реакции системы;
- структурная, функциональная и информационная избыточность;
- наличие средств для определения первопричины останова;
- уровень оперативной и автономной диагностики;
- состав и содержание документации и т.д.

При выборе конкретной архитектуры системы безопасности разработчик должен определить резервирование, полноту диагностического охвата, промежутки времени между автономными испытаниями 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 оперативной диагностики полевого оборудования и программируемых логических устройств.

От заказчика же требуется выбирать только тех поставщиков, проектировщиков и разработчиков, которые имеют достаточный опыт и репутацию в проектировании АСУ и защиты на технологических объектах аналогичного класса.

**Ограничение на работу в случае частичного отказа.** *Надежность и готовность системы безопасности* означают, что система может находиться в оперативном режиме, будучи устойчивой к одному или нескольким отказам, и при этом сохранять способность произвести действия для безопасного *программно-управляемого останова* процесса, в то время как отказ идентифицирован, и производится оперативная замена дефектного оборудования.

Максимальный интервал времени одноканальной работы для резервированных систем, который устанавливает TUV 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 RC5 (II категория взрывоопасности по предложенной в табл. 2 классификации) в одноканальном режиме работы – останов после 72 ч работы в контролируемом режиме (*supervised operation*);

• для уровня требований RC6 (I категория взрывоопасности по предложенной в табл. 2 классификации) в одноканальном режиме работы – останов после 1 ч работы в контролируемом режиме (*supervised operation*). Таким образом, подчеркивается, что в одноканальном варианте работа системы возможна только под жестким наблюдением.

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* с резервированием сенсоров и исполнительных устройств, определяющих безопасность процесса. Следовательно, общее правило состоит в следующем: *постоянная одноканальная работа систем 1oo2D и 2oo3 для объектов I и II категории взрывоопасности запрещена.*

Время восстановления работоспособности системы безопасности после ее полного отказа стандартами DIN, ISA, IEC никак не регламентируется, хотя стандарт IEC 61508 оперирует интервалом 8...24 ч. TUV также не дает никаких конкретных рекомендаций. Исходя из реальных возможностей по времени:

• определения причин отказа;

• времени замены дефектных компонентов;

• времени на пробный запуск и тестирование системы,

можно в качестве ориентира для объектов всех категорий взрывоопасности определить интервал в 8 часов на восстановление готовности системы к выполнению своих функций.

***Важное замечание.*** *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 технадзора подразумевает право на применение технических устройств на объектах всех категорий взрывоопасности. Поэтому ответственность за технические решения по выбору архитектуры системы безопасности для конкретного технологического объекта перекладывается на разработчика и на заказчика. Но выход есть. Он состоит в том, что эти решения должны быть обоснованы в ТЗ на создание АСУТП и согласованы с технадзором.*

**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.

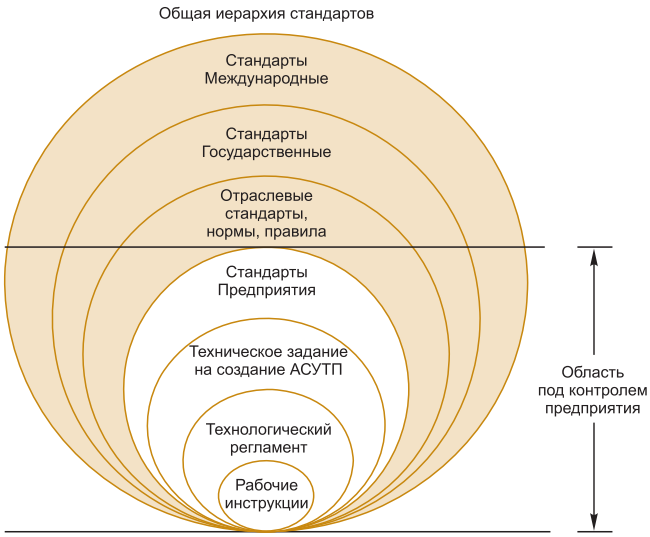



*Рис. 4*

Принципы построения и существования автоматизированных систем в течение всего жизненного цикла (рис. 4) должны регламентироваться: специфическими стандартами предприятия; отраслевыми стандартами; Государственными стандартами; официально признанными международными стандартами.

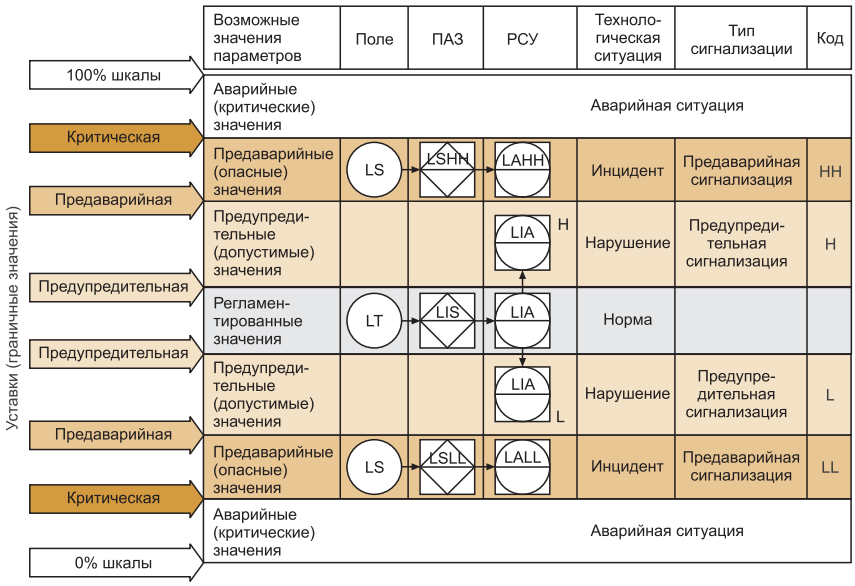
Объявленный еще в 2002 г. Законом "О техническом регулировании" набор неких технических регламентов нам, судя по всему, еще долго дожидаться. А пока наши законодатели "дремучий" русский лес рубят – "цивилизованный" парк будут сажать, – в работе с потенциальными поставщиками и разработчиками промышленные предприятия имеют полное право воспользоваться непосредственной поддержкой отечественных нормативных документов. Надо отдать честь создателям отечественных ГОСТов для автоматизированных систем [7-10]. Эти ГОСТы и по сей день сохраняют свою актуальность.

Вместе с тем, необходимость корректировки отечественных нормативных документов существует. В наибольшей степени в этом нуждается документ ПБ 09-540-03 *"Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств"*. С технологической точки зрения – это в целом вполне приемлемый документ. Однако он совершенно непродуктивен в отношении систем управления и защиты ТП, в особенности тех самых взрывоопасных. Достаточно привести всего лишь один характерный пример. Пункт 3.10 ПБ 09-540-03 утверждает:

"Для взрывоопасных ТП 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

*Таблица 4. Таблица определения значений технологических параметров, сигнализаций и блокировок*




критических только на величину ошибки измерительного канала, а критическое значение – это такое значение, при котором возможен взрыв или разгерметизация (табл. 3 в ПБ 09-170-97 – 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 в табл. 4.

Кроме того, в табл. 4 введена классификация технологических ситуаций с четким разграничением таких важных понятий, как "Инцидент" и простое "Нарушение", 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 ТП, нарушение положений настоящего Федерального закона, других федеральных законов и иных нормативных правовых актов РФ, а также нормативных технических документов, устанавливающих правила ведения работ на опасном производственном объекте".*

В данной формулировке понятие *"отклонение от режима ТП"* 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 РФ"*, которое уже и не нарушение законов, а просто инцидент!

Таким образом, формулировка закона в максимально возможной степени усилена по отношению к непосредственному исполнителю – аппаратчику, начальнику смены, дежурному слесарю КИП и т.д., 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 за 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 еще каких-то *"иных нормативных правовых актов РФ"* из категории техноло-

*Поздравляем Юрия Николаевича Федорова с 55-летием!*
*Только прирожденный инженер способен трудиться так, чтобы им стать.*
Редакция журнала «Автоматизация в промышленности»

гических 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 ТП за пределами предупредительных граничных значений, 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 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 и не предвидится, позиция автора публикации однозначна: предприятия в максимально возможной степени должны использовать существующую отечественную нормативную базу. Никто не мешает закрепить ее лучшие образцы в собственных стандартах промышленных предприятий (СТП). В контексте обсуждаемой темы это можно сделать, приняв Стандарт предприятия на проектирование, разработку, внедрение, эксплуатацию и сопровождение АСУТП. 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.*

Опыт автора показывает, что защита предприятия от недобросовестных поставщиков, 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 *"ТЗ на создание АСУТП"*;

• 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 предпоследние годы, перед самым появлением Закона "О техническом регулировании", 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 химической, нефтехимической и нефтеперерабатывающей промышленности прочно занимают положение, для которого *количественный анализ риска обязателен.*

Если предприятие *до заключения контракта* проявляет компетентность и твердо настаивает на том, что:

• оборудование системы должно иметь все необходимые отечественные разрешительные документы: сертификаты Госстандарта на средства измерения, разрешения Ростехнадзора на применение, и т.д.;

• система должна соответствовать требованиям Общих правил взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств (ПБ 09-540-03);

• система должна соответствовать требованиям Стандарта предприятия по обеспечению промышленной безопасности и Стандарта предприятия на проектирование, разработку, внедрение и эксплуатацию АСУТП;

• система должна соответствовать требованиям ТЗ на создание АСУТП;

• импортное оборудование и ПО системы безопасности по умолчанию должно иметь сертификаты соответствия стандартам IEC 61508 и IEC 61511;

• импортное оборудование и система в целом должны иметь стандартную техническую и проектную документацию не только на английском, но и на русском языке,

то будьте уверены – так оно и будет. Правда – на нашей стороне. Главное, чтобы и мы находились на ней же.

**Системы обслуживания полевого оборудования в оперативном режиме.** Проблема оперативного обнаружения неполадок и отказов полевого оборудования всегда будет сохранять свою актуальность. Об-

служивание 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.

Текущая ситуация элементарна – обслуживание проводится по первым двум вариантам: при отказе и по графику.

В последние годы бурное развитие получило направление, которое в конечном итоге связывают с возможностью оперативной диагностики полевого оборудования, и разработка полевого оборудования, способного самостоятельно выявлять главные нарушения и сбои в своей собственной работе, и сообщать о них оперативному и обслуживающему персоналу.

Пример: автоматическое определение забивки импульсной линии датчика давления. Для определения забивки импульсной линии "интеллектуальный" датчик анализирует вариацию шума с такой высокой частотой, которую не может обеспечить АСУТП. При изменении заданных характеристик встроенная диагностика прибора обнаруживает разладку сигнала задолго до ее проявления в системе. Основная цель – приблизиться к оптимальному уровню обслуживания, поскольку недостаточно частое обслуживание приводит к дорогостоящим остановам производства, а неоправданно частое обслуживание увеличивает издержки. Если рассмотреть вероятность $P$ опасного отказа (несрабатывания) единичного элемента оборудования в течение межтестового (межповерочного) интервала $T$:

$$P = \lambda \cdot \frac{T}{2},$$

то понятно, что при постоянной интенсивности отказов $\lambda$ единственной возможностью снижения вероятности отказа является уменьшение интервала $T$. Поэтому при создании систем защиты и управления основной упор должен делаться на использование специального полевого оборудования с возможностью оперативной диагностики. Реальная возможность создания подобного рода систем возникла 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, Foundation Fieldbus).

Если при этом используется полевое оборудование, имеющее специальный допуск на применение в системах защиты, то оперативная диагностика дает возможность повышения уровня интегральной безопасности SIL *даже без установки дополнительного оборудования*. При этом средства обслуживания поля органически включаются в общую иерархию средств управления на уровне самостоятельной подсистемы. Идея этих систем, которые выступают под общим термином *Plant Asset Management Systems* – управление оборудованием производства, заключается в том, что, подобно обычному контролю и управлению ТП, вводятся средства контроля и управления полевым оборудованием:

- оперативный дистанционный контроль и диагностика состояния устройства;
- настройка параметров устройства;
- поддержка графиков работ по обслуживанию;
- регистрация отчетов по обслуживанию;
- ведение единой базы данных оборудования;
- интерактивная документация на полевое оборудование;
- безболезненная интеграция оборудования сторонних производителей.

*Важное замечание: в настоящее время в состав интеллектуального полевого оборудования кроме датчиков, анализаторов и клапанов включаются* ***электродвигатели и насосы****, работоспособность которых также имеет решающее значение для ТП.*

Системы управления полевым оборудованием в масштабе РВ позволяют радикальным образом повысить доверие к системе управления и защиты, уменьшить затраты на обслуживание, сократить число и время простоев и обеспечить дистанционные операции с полевым оборудованием; автоматизацию обслуживания; возможность превентивного обслуживания; поддержку автоматического распознавания нового оборудования (plug-in).

Сводный эффект внедрения системы управления оборудованием: увеличение безопасности процесса и пробега оборудования; автоматизированный контроль эффективности и стоимости обслуживания; общее сокращение стоимости обслуживания.

Немаловажной с точки зрения повышения безопасности является возможность установки выделенного рабочего места инженера по обслуживанию полевого оборудования, недоступного для оперативного персонала.

**Оперативное тестирование отсечных клапанов.** 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.

На сегодняшний день наиболее перспективным методом тестирования отсечных клапанов в режиме on-line считается *частичное открытие или закрытие клапана* непосредственно на рабочем потоке в сочетании с инспекцией по месту. По экспертным оценкам ведущих компаний эта методика позволяет обнаружить 60...95% отказов. Можно выделить три основных метода тестирования отсечных клапанов путем частичного изменения их положения в оперативном режиме.

1. *Механическое ограничение хода клапана*. Используется механический ограничитель хода или устройство, ограничивающее перемещение клапана на определенную величину хода. Обычно – это 10...20%.

Механическое устройство может быть встроено в клапан или 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 окончанию испытаний. Самое неприятное во время тестирования, когда отсекатель недоступен для выполнения функций защиты.

2. *Тестирование с использованием системы ПАЗ.* Для осуществления этого метода требуется специальное ПО в системе защиты, а также датчик положения или ограничивающие ключи на клапане. Дополнительно может использоваться датчик давления. Этот метод кроме проверки работоспособности соленоида и перемещения клапана позволяет проверить временные характеристики и снять кривую изменения давления на клапане. Результаты тестирования могут быть архивированы для сравнения с предысторией.

Принципиальный недостаток этого метода – система ПАЗ используется для выполнения несвойственных ей функций. Кроме того, данный подход неявным образом подразумевает использование рабочей или инженерной станции РСУ, поскольку система ПАЗ по определению не может иметь рабочих станций РВ. Таким образом, существенно повышается риск ложного срабатывания системы ПАЗ во время технического обслуживания.

3. *Специальный цифровой контроллер на клапане.* Контроллер способен проверять работоспособность соленоида, 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 фиксируется и воспроизводится системой обслуживания полевых устройств. Система обслуживания полевых устройств позволяет хранить и документировать предысторию всех тестовых операций и их результатов, поэтому всегда существует возможность сравнения с исходным состоянием и эталонными характеристиками клапана.

Если во время проведения операций тестирования с технологической установки приходит сигнал о реальной необходимости срабатывания данного клапана, то эта команда будет иметь приоритетное значение. Этот метод диагностики требует дополнительных затрат на оборудование, которые, однако, окупаются в процессе эксплуатации как за счет снижения расходов на обслуживание, так и за счет снижения числа опасных отказов и ложных срабатываний, приводящих к непосредственной угрозе аварии.

И последнее. В отечественной практике полная ревизия полевого оборудования проводится во время капитального ремонта – 1 раз в год. Оперативное тестирование открывает перспективу перейти на двух – четырехлетние межповерочные интервалы.

**Подготовка персонала.** Прямые методы защиты и оперативной диагностики имеют чрезвычайное значение. Но никакие технические ухищрения не спасут от неприятностей без грамотного и ответственного


*Рис. 5*

персонала. При этом квалификация оперативного и обслуживающего персонала должна соответствовать сложности и опасности процесса.

К сожалению, далеко не каждое предприятие может себе позволить реализацию требований ПБ 09-540-03, пункт 2.12: "С этой целью указанные организации (имеются в виду объекты I и II категорий взрывоопасности – Ю.Ф.) должны иметь компьютерные тренажеры, включающие *максимально приближенные к реальным динамические модели процессов* и реальные средства управления (функциональные клавиатуры, графические экранные формы и т.д.)". Но в данном случае речь в первую очередь должна идти о *регулярном, не реже, чем раз в полгода тренинге оперативного персонала с отработкой автоматических навыков по Плану локализации аварийных ситуаций (ПЛАС) и сдачей экзамена на допуск к работе на взрывоопасном производстве*. Подобные тренажерные системы на несколько рабочих мест уже вполне по карману большинству стоящих на ногах химических и нефтехимических предприятий.

### Заключительное замечание

Без современных средств КИПиА, без надежной системы базового управления и защиты невозможно перейти к реализации функций управления более высокого порядка (рис. 5). К сожалению, последние 20 лет безграничной свободы (в очередной раз сбылась народная мечта: *темницы рухнут, и – свобода!..*) привели к тому, что практически невозможно найти человека, способного более-менее внятно объяснить понятие "усовершенствованное управление" (*Advanced Process Control*). А тем более "управление с прогнозирующей моделью" (*MPC – Model Predictive Control*) с учетом ограничений на управляющие и управляемые переменные. Невозможно не потому, как говорил Козьма Прутков, что наши понятия слабы, а потому, что сии вещи не входят в круг наших понятий.

По независимым оценкам фирм Honeywell и Yokogawa, экономический эффект от внедрения пакетов усовершенствованного управления составляет 40...60% в общей доле прибыли от внедрения ком-

плексных АСУ 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.

Необходимо иметь дело с теми компаниями, которые могут предложить весь спектр работ, подтвержденный на аналогичных предприятиях, и ориентироваться на долговременное сотрудничество. И если сделан 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 со все бóльшим усложнением и ТП, и средств автоматизации, и соответствующим увеличением числа и масштабов аварий на производстве. Все, что способно снизить уровень этих требований, должно рассматриваться как проявление легкомыслия и с профессиональной, и с социальной точки зрения, и с позиции коммерческих интересов.

**Список литературы**


1. Стандарт IEC 61508 "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems" (Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью).
2. Стандарт IEC 61511 "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" (Функциональная безопасность: Оборудованные под безопасность системы для перерабатывающего сектора промышленности).
3. Стандарт ANSI/ISA 84.01-1996 "Application of Safety Instrumented Systems for the Process Industries" (Применение оборудованных под безопасность систем для технологических процессов).
4. *Федоров Ю.Н.* "Основы построения АСУТП взрывоопасных производств", в 2-х томах. М.: СИНТЕГ, 2006.
5. 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).
6. Стандарт DIN V VDE 0801 "Principles For Computers In Safety Related Systems" (Принципы для компьютеров в системах, связанных с безопасностью).
7. ГОСТ 34.201-89 Виды, комплектность и обозначение документов при создании автоматизированных систем.
8. ГОСТ 34.601-90 Автоматизированные системы. Стадии создания.
9. ГОСТ 34.602-89 Комплекс стандартов на автоматизированные системы. ТЗ на создание автоматизированной системы.
10. РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов.


***Федоров Юрий Николаевич*** *– главный специалист по АСУТП ООО "Кама-Автоматика".*

*Контактный телефон (8555)-313-919, факс 8-(8555)-319-995.*

*Email: fedorov-yn@mail.ru*

# Принципы построения и практическая реализация высоконадежных АСУТП потенциально опасных производств

**О.Г. Тюрин, В.С. Кальницкий (Фирма "Пластик Энтерпрайз")**

*Сформулированы принципы, применяемые фирмой "Пластик Энтерпрайз" при создании АСУТП потенциально опасных производств. Наряду с общепринятой структурно-технической составляющей обеспечения надежности таких систем, поставлен вопрос о важной роли ее интеллектуальной составляющей. Приведены примеры АСУТП, внедренных на предприятиях специальной технической химии в течение последних трех лет.*

Фирма "Пластик Энтерпрайз" в течение многих лет уверенно занимает сегмент рынка автоматизации наиболее представительного класса потенциально опасных объектов – ТП и производств отрасли специальной технической химии. В большинстве своем это непрерывные и непрерывно-периодические процессы переработки опасных веществ и смесей в изделия, сопровождающиеся интенсивным тепло- и газовыделением.

Наряду с главной особенностью – потенциальной пожаро- и взрывоопасностью для таких ТП характерны также: изготовление дорогостоящих и ответственных изделий; повышенные требования к их качеству; значительная длительность (до нескольких недель) жизненного цикла изготовления; большое число параметров контроля, регулирования, сигнализации и блокировок; существенные транспортные запаздывания, обусловленные территориальной рассредоточенностью оборудования; нестандартность самого технологического оборудования и сложность протекающих в аппаратах физических, химических, термомеханических, физико-химических, химико-физических и других процессов, а также их динамических характеристик при нанесении управляющих воздействий; отсутствие в ряде случаев измерительной аппаратуры для контроля важных информативных параметров, обусловленное специфическими свойствами перерабатываемого сырья и полуфабрикатов;