Необходимые свойства систем противоаварийной защиты производственных объектов

Э.Л. Ицкович (ИПУ РАН)

Рассматриваются существующие недостатки в области разработки и использования систем противоаварийной защиты (ПАЗ) на российских предприятиях технологических отраслей. Приводятся требования и рекомендации по построению систем ПАЗ, зафиксированные в нормативных документах. Выделяются особенности систем ПАЗ, которые должны учитываться заказчиками и разработчиками.

Ключевые слова: АСУТП, противоаварийная защита, нормативные документы, разработка систем ПАЗ, эксплуатация систем ПАЗ.

Введение

Самостоятельным и наиболее ответственным классом систем автоматизации производственных объектов являются системы противоаварийной защиты (ПАЗ), обеспечивающие безопасность работы взрывоопасных производственных объектов, широко распространенных на предприятиях разных технологических отраслей. Задачей таких систем является слежение за ходом автоматизируемого процесса в объекте и в случае возникновения предаварийного состояния проводить немедленный автоматический перевод процесса в безопасное состояние и сигнализировать об этом оператору. Подобную же задачу решают системы пожарной и газовой безопасности; системы управления горелками; системы критических защит опасных процессов; системы безопасности компрессоров; системы защиты резервуаров от перелива, от течи, от повышения давления и температуры; системы защиты от загазованности окружающей среды.

Практически на большинстве предприятий технологических отраслей определенная часть производственных объектов оснащается системой ПАЗ.

Важно отметить, что если системы контроля и управления рабочими режимами могут разрабатываться по требованиям заказчиков без специального согласования с какими-либо нормативами, стандартами и правилами; то системы ПАЗ обязательно должны соответствовать требованиям и рекомендациям определенных (отмеченных ниже) документов. Однако результаты обследования конкретных предприятий разных отраслей промышленности показывают, что полное соответствие систем ПАЗ изложенным в документах правилам их разработки и эксплуатации можно увидеть на предприятиях достаточно редко.

Основные показатели систем ПАЗ

Системы ПАЗ предназначены для обеспечения функциональной безопасности объектов, достигаемой снижением риска аварийных ситуаций в любых производственных объектах, в которых обрабатываются или хранятся токсичные продукты и/или присутствует риск взрывоопасности самих объектов. Под риском понимается произведение вероятности и последствий аварийной ситуации, а под снижением риска аварийных ситуаций понимается снижение средней вероятности возникновения таких ситуаций, которое обеспечивается благодаря работе системы ПАЗ. При этом оставшаяся при работе ПАЗ вероятность аварийных ситуаций определяется вероятностью отказа системы ПАЗ на команду оператора или на технологическую причину по переводу объекта в безопасное состояние.

Работа системы ПАЗ достаточно специфична: она должна автоматически переводить ТП или производственный объект в безопасное состояние при нарушениях заданных условий его работы и полностью исключить свое воздействие на процесс/объект при нормальном режиме его функционирования. Таким образом, в отличие от всех других управляющих АСУ производственных объектов система ПАЗ не влияет (не воздействует) на процесс/объект при его нормальной работе и становится активной только при его аварийном выходе из заданного нормального режима. Поскольку эта ситуация возникает достаточно редко, то добавляется задача диагностирования нормального состояния системы ПАЗ при ее нахождении в неактивной фазе.

Требуемая величина снижения риска аварийной ситуации определяется уровнем необходимой защиты (требуемой безопасностью работы объекта или (что то же) мерой ожидаемой надежности работы объекта) — Safety Integrity Level, который повсеместно обозначается аббревиатурой — SIL, а в российских документах часто имеет обозначение — «Уровень полноты безопасности» (УПБ). Этот уровень полноты безопасности (SIL или УПБ), обеспечиваемый системой ПАЗ для разных функций объекта, должен соответствовать самому высокому требуемому уровню полноты безопасности из всех реализуемых системой ПАЗ функций.

Сам риск аварийных ситуаций принципиально оценивается произведением вероятной частоты ава-

рий в объекте на катастрофичность/стоимость ущерба в результате аварии. Под ущербом понимаются затраты на компенсацию страховых возмещений потерпевшему персоналу, стоимость заменяемого оборудования и ремонта помещений, штрафы за загрязнение окружающей среды, коммерческие потери и даже ущерб репутации предприятия. Поскольку понимаемые так риски аварийной ситуации у разных технологических процессов/объектов сугубо различны, то и уровни SIL (УПБ) у них будут разными.

Принимаются четыре категории рисков, задаваемые особенностями возможной аварийной ситуации. Эти категории фиксируются уровнем полноты безопасности работы объекта — SIL (УПБ):

— категория риска типа катастрофы, тогда необходима защита по уровню SIL 4;

— категория риска типа смерти нескольких человек обслуживающего объект персонала, тогда защита по уровню SIL 3;

— категория риска типа травматизма персонала и повреждений оборудования, защита по уровню SIL 2;

— категория риска типа повреждений оборудования и продукции, защита по уровню SIL 1.

Уровень SIL в свою очередь определяет требуемую надежность работы системы ПАЗ, то есть требуемую среднюю вероятность отказа от перевода процесса/объекта в безопасное состояние. В результате работы необходимой системы ПАЗ риск аварийной ситуации должен снижаться до остаточного приемлемого уровня.

Поясняет влияние заданного уровня SIL на требование к безопасности системы ПАЗ и на снижение риска аварии (последний оценивается фактором снижения риска аварии, который показывает снижение средней вероятности возникновения аварийных ситуаций) приведенная ниже таблица.

Таблица

Уровень защиты	Содержание требуемой защиты	Требуемая средняя вероятность отказа системы ПАЗ на запрос	Фактор снижения риска аварии
SIL 4	Защита от катастрофы	От 10^{-5} до 10^{-4}	От 10 000 до 100 000
SIL 3	Защита персонала от смерти	От 10^{-4} до 10^{-3}	От 1000 до 10 000
SIL 2	Защита оборудования и персонала от травм	От 10^{-3} до 10^{-2}	От 100 до 1000
SIL 1	Защита оборудования от повреждений	От 10^{-2} до 10^{-1}	От 10 до 100

Руководящие документы по созданию и эксплуатации систем ПАЗ

Системы ПАЗ должны соответствовать требованиям, указаниям, правилам и рекомендациям, изложенным в ряде нормативных документов. При их перечислении выделены и кратко рассмотрены те положения, которые имеют наиболее важное значение при создании и эксплуатации конкретных систем ПАЗ производственных объектов предприятий технологических отраслей промышленности.

Основополагающими документами по построению и эксплуатации указанных систем являются утвержденные в РФ международные стандарты: ГОСТ Р МЭК 61508-2012 «Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью» и базирующийся на нем и поясняющий его применение для предприятий перерабатывающих отраслей ГОСТ Р МЭК 61511-2011 «Системы обеспечения функциональной безопасности: для перерабатывающих отраслей промышленности».

ГОСТ Р МЭК 61508-2012: Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью

Данный ГОСТ рассматривает функциональную безопасность того класса систем, к которому принадлежат системы автоматизации производственных объектов. ГОСТ состоит из семи отдельно выпущенных частей.

I. Общие требования.

II. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью.

III. Требования к программному обеспечению.

IV. Термины и определения.

V. Рекомендации по применению методов определения уровней полноты безопасности.

VI. Руководство по применению. Руководящие указания в документе базируются на использовании известных пользователю стандарта средних вероятностей отказов по запросу датчиков, логической подсистемы ПАЗ (контроллеров), исполнительных комплексов при разной их архитектуре: разных вариантах резервирования и диагностики. Считается известной интенсивность обнаруженных и необнаруженных опасных отказов.

VII. Методы и средства. Рассмотрены методы случайного отказа оборудования, методы исключения систематических отказов, методы достижения полноты безопасности программного обеспечения, вероятностный метод определения полноты безопасности предварительно разработанных программных средств.

ГОСТ Р МЭК 61511-2011: Системы обеспечения функциональной безопасности: для перерабатывающих отраслей промышленности

Стандарт призван конкретизировать подход к обеспечению безопасности, изложенный в стандарте ГОСТ Р МЭК 61508, для производственных процессов и объектов перерабатывающих отраслей промышленности, то есть непосредственно относится к произ-

водственным объектам предприятий технологических отраслей промышленности. В значительной степени он предназначен для проектных организаций. Стандарт состоит из трех отдельно выпущенных частей.

I. Требования к системе, аппаратному и программному обеспечению.

Требования оценки опасности и степени риска аварийной ситуации для каждой функции, реализуемой системой ПАЗ, должны определяться комиссией, состоящей из проектанта системы, поставщика средств автоматизации для нее, заказчика системы, эксплуатирующего систему предприятия, подрядчика работ по внедрению системы. Стандарт указывает, что при выработке требований необходим учет всех компонентов системы ПАЗ и также учет человеческого фактора. Стандарт не определяет должности лица, ответственного за выполнение всех требований к достижению функциональной безопасности, он лишь отмечает, что это не должен быть человек, участвующий в проектировании системы. В анализе опасностей и рисков должны принимать участие службы технолога и КИПиА.

При разработке требований к системе ПАЗ должны быть предусмотрены:

— описания каждого опасного события, включая возможные ошибки персонала;

— оценка последствий и правдоподобности опасных событий;

— рассмотрение условий нормальной работы объекта: его пуска, нормальной работы, останова, обслуживания, аварийного останова;

— требуемое снижение риска (требуемая защита: уровень SIL) для каждой функции системы ПАЗ.

В частности, должны быть не забыты требования к следующим свойствам системы ПАЗ:

— описание измерений состояния объекта, которые должны быть предусмотрены в системе;

— описание исполнительных воздействий, которые система должна реализовать на объекте при наступлении предаварийных событий;

— описание алгоритмов защиты, которые должны быть реализованы в системе;

— требуемые реакции на предаварийные события: останов объекта, сигнал оператору, останов и сигнал оператору;

— необходимое быстродействие системы;

— требования к прикладному программному обеспечению системы;

— интервал времени между тестовыми испытаниями системы во время ее эксплуатации;

— требуемое среднее время ремонта системы;

— предельные значения параметров окружающей среды, в интервалах которых должна нормально работать система;

— максимально допустимая частота ложных срабатываний системы.

Отдельно в этой части стандарта зафиксированы требования к проектированию системы ПАЗ:

— из всех функций контроля и управления объектом должны быть выделены функции безопасности, которые составят содержание системы ПАЗ;

— система ПАЗ должна проектироваться по самому высокому уровню SIL, имеющемуся у выделенных функций безопасности; если нельзя показать, что функции безопасности с более низким уровнем SIL не могут влиять негативно на функции с более высоким уровнем SIL;

— проектирование должно учитывать задачи, которые решают операторы по функциям безопасности и имеющиеся у них ограничения;

— должна быть предусмотрена непрерывность электропитания системы ПАЗ;

— должны быть предусмотрены ручные средства останова процесса оператором, кроме заложенных в проект воздействий по автоматическому останову процесса при возникновении предаварийной ситуации;

— все средства системы ПАЗ должны быть отказоустойчивыми (резервируемыми) и доказательствами пригодности средств является их сертификация по требуемому уровню SIL и известный опыт их эксплуатации в аналогичных условиях;

— должны быть подвергнуты оценке на функциональную безопасность инструментальные средства разработки и тестирования системы ПАЗ, частота проведения проверки работоспособности системы ПАЗ аудитом независимого персонала, процедуры управления внесения изменений в систему ПАЗ.

II. Руководство по применению стандарта МЭК 61511-1.

Целью этой части стандарта является показ того, как надо выполнять указания первой части стандарта.

III. Руководство по определению требуемых уровней полноты безопасности (SIL).

В этой части приводятся описания различных методов определения требуемого уровня SIL:

— концепция приемлемого риска, т. е. достижение настолько низкого остаточного риска, который возможно практически реализовать;

— полуколичественный метод;

— метод матрицы слоев безопасности;

— качественный метод: граф риска.

Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств

Системы ПАЗ должны базироваться на утвержденном Федеральной службой по экологическому, технологическому и атомному надзору (приказ от 11 марта 2013 года N 96) нормативном документе о федеральных нормах и правилах в области промышленной безопасности: *«Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств»*. Рассмотрим наиболее важные положения этого документа, касающиеся создания и эксплуатации конкретной системы ПАЗ. Номера этих положений соответствуют номерам статей рассматриваемого документа.

3.10. Для взрывоопасных ТП должны предусматриваться системы ПАЗ, предупреждающие возникновение аварии при отклонении от предусмотренных технологическим регламентом на производство продукции предельно допустимых значений параметров процесса во всех режимах работы и обеспечивающие безопасную остановку или перевод процесса в безопасное состояние по заданной программе.

3.11. Системы ПАЗ включаются в общую АСУТП.

6.3.2. Системы ПАЗ функционируют независимо от системы управления ТП. Нарушение работы системы управления не должно влиять на работу системы ПАЗ.

6.3.3. Система ПАЗ выполняет следующие функции:

— автоматическое обнаружение потенциально опасных изменений состояния технологического объекта или системы его автоматизации;

— автоматическое измерение технологических переменных, важных для безопасного ведения ТП (например, измерение переменных, значения которых характеризуют близость объекта к границам режима безопасного ведения процесса);

— автоматическая (в режиме on-line) диагностика отказов, возникающих в системе ПАЗ и (или) в используемых ею средствах технического и программного обеспечения;

— автоматическая предаварийная сигнализация, информирующая оператора ТП о потенциально опасных изменениях, произошедших в объекте или в системе ПАЗ;

— автоматическая защита от несанкционированного доступа к параметрам настройки и (или) выбора режима работы системы ПАЗ.

6.3.6. ... не допускается использовать в качестве источников информации для систем ПАЗ одни и те же датчики, которые применяются в составе других подсистем АСУТП (например, в системе автоматического регулирования, в системе технологического или коммерческого учета).

6.3.7. Для объектов... не допускается использовать в качестве исполнительных устройств систем ПАЗ одни и те же устройства, которые предусмотрены в составе другой подсистемы АСУТП (например, в системе автоматического регулирования).

6.3.9. В системах ПАЗ не допускается применение многоточечных приборов контроля параметров, определяющих взрывоопасность процесса.

6.3.10. Проектирование системы ПАЗ и выбор ее элементов осуществляются исходя из условий обеспечения работы системы в процессе эксплуатации, обслуживания и ремонта в течение всего жизненного цикла защищаемого объекта.

6.3.11. Показатели надежности, безопасности и быстродействия систем ПАЗ определяются разработчиками систем с учетом требований технологической части проекта.

6.3.12. Время срабатывания системы защиты должно быть таким, чтобы исключалось опасное развитие возможной аварии.

6.3.13. К выполнению управляющих функций систем ПАЗ предъявляются следующие требования:

— команды управления, сформированные алгоритмами защит (блокировок), должны иметь приоритет по отношению к любым другим командам управления технологическим оборудованием, в том числе к командам, формируемым оперативным персоналом АСУТП (если иное не оговорено в техническом задании на ее создание). Срабатывание одной системы ПАЗ не должно приводить к созданию на объекте ситуации, требующей срабатывания другой такой системы. В алгоритмах срабатывания защит следует предусматривать возможность включения блокировки команд управления оборудованием, технологически связанным с аппаратом, агрегатом или иным оборудованием, вызвавшим такое срабатывание.

6.3.14. В системах ПАЗ и управления ТП ... должно быть исключено их срабатывание от кратковременных сигналов нарушения нормального хода ТП, в том числе и в случае переключений на резервный или аварийный источник электропитания.

6.3.15. В проектной документации, технологических регламентах на производство продукции и перечнях систем ПАЗ взрывоопасных объектов наряду с уставками защиты по опасным параметрам должны быть указаны границы критических значений параметров.

6.3.16. Значения уставок систем защиты определяются с учетом погрешностей срабатывания сигнальных устройств средств измерения, быстродействия системы, возможной скорости изменения параметров. При этом время срабатывания систем защиты должно быть меньше времени, необходимого для перехода параметра от предупредительного до предельно допустимого значения. Конкретные значения уставок приводятся в проекте и технологическом регламенте на производство продукции.

6.3.17. ... предусматривается предаварийная сигнализация по предупредительным значениям параметров, определяющих взрывоопасность объектов.

6.3.18. В случае отключения электроэнергии или прекращения подачи сжатого воздуха для питания систем контроля и управления системы ПАЗ должны обеспечивать перевод технологического объекта в безопасное состояние. Необходимо исключить возможность произвольных переключений в этих системах при восстановлении питания. Возврат технологического объекта в рабочее состояние после срабатывания системы ПАЗ выполняется обслуживающим персоналом по инструкции.

6.3.19. Исполнительные механизмы систем ПАЗ, кроме указателей крайних положений непосредственно на этих механизмах, должны иметь устройства, позволяющие выполнять индикацию крайних положений в помещении управления.

6.3.21. Показатели надежности систем ПАЗ устанавливаются и проверяются не менее чем для двух типов отказов данных систем: отказы типа «несрабатывание» и отказы типа «ложное срабатывание».

6.3.23. Все программные средства вычислительной техники, предназначенные для применения в составе любой системы ПАЗ, подлежат обязательной проверке на соответствие требованиям, указанным в ТЗ, которая проводится их изготовителем или поставщиком по программе, согласованной с заказчиком системы ПАЗ.

6.3.24. Перечень контролируемых параметров, определяющих взрывоопасность процесса в каждом конкретном случае, составляется разработчиком процесса и указывается в исходных данных на проектирование.

6.4.1. Для контроля загазованности по предельно допустимой концентрации и нижнему концентрационному пределу распространения пламени в производственных помещениях, рабочей зоне открытых наружных установок должны предусматриваться средства автоматического непрерывного газового контроля и анализа с сигнализацией, срабатывающей при достижении предельно допустимых величин и с выдачей сигналов в систему ПАЗ. При этом все случаи загазованности должны регистрироваться приборами с автоматической записью и документироваться.

ГОСТы по управлению надежностью и менеджменту риска

Важное значение для анализа возможного повышения надежности работы систем ПАЗ имеют ниже указанные стандарты, которые рассматривают различные аспекты снижения рисков и повышения надежности технологических систем.

— ГОСТ Р 51901-2002. Управление надежностью. Анализ риска технологических систем.

— ГОСТ Р 51901.2-2005. Менеджмент риска: системы менеджемента надежности.

— ГОСТ Р 51901.3-2007. Менеджмент риска: руководство по менеджементу надежности.

— ГОСТ Р 51901.4-2005. Менеджмент риска: руководство по применению при проектировании.

— ГОСТ Р 51901.5-2005. Менеджмент риска: руководство по применению методов анализа надежности.

— ГОСТ Р 51901.6-2005. Менеджмент риска: Программа повышения надежности.

— ГОСТ Р 51901.10-2009. Менеджмент риска: Процедуры управления пожарным риском на предприятии.

— ГОСТ Р 51901.11-2005. Менеджмент риска: исследование опасности и работоспособности. Прикладное руководство. (Копия стандарта МЭК 61882: 2001. Исследование опасности и работоспособности (HAZOP). Руководство к применению).

Термин «HAZOP» обозначает исследование опасности и работоспособности, а под риском (как и во всех документах) понимается сочетание вероятности появления опасного события и его последствий.

HAZOP служит для идентификации потенциальных отклонений от целей проекта (от нормального режима работы объекта), экспертизы их возможных причин и оценки последствий. Экспертиза должна производиться под руководством опытного лидера исследований, гарантирующего всесторонний анализ системы на основе логических и аналитических заключений.

Подход HAZOP должен определить возможные отклонения от заданного состояния, причины отклонений, меры устранения их последствий. Важно не пропустить отклонения, связанные с взаимодействием нескольких частей (отдельных контуров контроля и управления) системы, а не просто отклонения одной какой-либо части (одного контура); а также учесть влияние отклонений одной части на работу других частей системы. Следует подчеркнуть, что любые планируемые изменения в системе требуют предварительного анализа HAZOP.

Рекомендации по составу экспертной группы HAZOP:

— лидер группы, не являющийся проектантом, поскольку иногда в результате обсуждения в группе в законченный проект требуется ввести изменения;

— проектант, разъясняющий проект и объясняющий возможные отклонения от него;

— пользователь системы, поясняющий текущее состояние системы, последствия отклонений и степень их опасности;

— эксперт по анализу работы системы;

— представитель ремонтной службы, отвечающий за технической обслуживание системы;

— регистратор, документирующий все предложения и заключение группы.

Предлагаемая процедура работы экспертной группы HAZOP: анализ системы по отдельным элементам и контурам; рассмотрение условий аварийных режимов нежелательных действий, которые приводят к отказу системы; прогноз временной деградации системы; оценки ее надежности, ремонтопригодности, простоты обслуживания.

Этапы работы экспертной группы HAZOP:

— планирование исследований и сбор исходных данных;

— определение заданных состояний и идентификация отклонений от них, выделение их причин, последствий, механизмов защиты, возможных смягчающих мероприятий;

— оформление результатов.

— ГОСТ Р 51901.12-2007. Менеджмент риска: метод анализа видов и последствий отказов.

— ГОСТ Р 51901.13-2005. Менеджмент риска: анализ дерева неисправностей.

— ГОСТ Р 51901.14-2007 Менеджмент риска: структурная схема надежности и булевы методы.

— ГОСТ Р 51901.15-2005. Менеджмент риска: применение марковских методов.

— ГОСТ Р 51901.16-2005. Менеджмент риска: повышение надежности. Статистические критерии и методы оценки.

— ГОСТ Р 52806-2007. Менеджмент риска проектов: общие положения.

— ГОСТ Р МЭК 61160-2006. Менеджмент риска: формальный анализ проекта.

— ГОСТ Р ИСО/МЭК 16085-2007. Менеджмент риска: применение в процессах жизненного цикла систем и программного обеспечения.

Конкретные особенности построения и эксплуатации систем ПАЗ, соответствующих нормативным документам

Рассматривая отмеченные положения указанных нормативных документов и сопоставляя их с существующим практическим состоянием систем ПАЗ на производственных объектах многих предприятий технологических отраслей России, выделим основные нестыковки и недоработки, характерные для построения и эксплуатации реальных систем ПАЗ по отношению к отдельным требованиям нормативов.

Рассмотрим элементы конкретных систем ПАЗ, которые требуют большего внимания и более тщательного выполнения, чем это зачастую происходит на практике.

Особенности разработки технического задания на систему ПАЗ

Разработку требований на систему ПАЗ должна выполнять комиссия, состоящая из отвечающих за нормальную работу объекта специалистов служб технолога, КИПиА, обслуживания оборудования и из проектантов системы ПАЗ. Комиссия должна выделить каждое опасное событие при работе объекта, оценить его последствия, зафиксировать функцию его предотвращения или компенсации, указать требуемое снижение риска (уровень SIL) при возникновении события.

На практике количественная оценка риска, определяемая оценкой частоты аварий в объекте (как формулируется в нормативных документах), достаточно мало вероятна, поскольку аварии (к счастью) происходят весьма редко и для расчета статистически достоверной оценки риска почти всегда нет достаточного числа исходных данных. Процедура задания риска (уровня SIL) конкретного опасного события обычно производится комиссией экспертно, с учетом мнений разработчиков ТП и производителей используемого в объекте оборудования.

В разработанном комиссией ТЗ на систему ПАЗ должны быть отмечены следующие ее свойства:

— описание реализуемых системой ПАЗ функций при всех режимах и этапах работы объекта (пуск, работа, останов и т. п.) и параметров функций: их скорости реализации, точности выполнения;

— уровень безопасности для каждой реализуемой функции, определяющий ответственность реализации функции для обеспечения безопасности объекта;

— интегральный уровень безопасности (SIL), который должен обеспечиваться ПЛК системы ПАЗ (он должен соответствовать самому высокому уровню безопасности реализуемых в системе ПАЗ функций);

— допустимая частота ложных срабатываний системы ПАЗ (последние не приводят к аварийной ситуации, но вызывают определенные материальные потери);

— подтверждение сертификации заданного уровня безопасности SIL для всех компонентов системы ПАЗ каждой конкретной функции защиты.

Важно отметить, что документ результата работы комиссии должен по обоснованности своих решений удовлетворять вышеуказанным нормативам и может быть подвергнут анализу Ростехнадзора.

Свойства, которые должны быть учтены в проекте на систему ПАЗ:

— полная автономность системы ПАЗ от всех других подсистем АСУТП: все ее средства (датчики, контроллер, исполнительный комплекс, объединяющая их сеть) не реализуют никаких посторонних системе ПАЗ функций контроля и управления;

— выделенное от других систем электропитание средств системы ПАЗ и его резервирование;

— значения параметров системы ПАЗ: точность, время реагирования на возникшую предаварийную ситуацию, предельные характеристики окружающей среды и т. п.;

— интерфейс связи системы ПАЗ с оператором для сигнализации о наступлении предаварийного состояния и момента включения системы ПАЗ в работу. При отказе системы ПАЗ сигнализация оператору о необходимости ручного управления;

— преимущественное использование датчиков и исполнительных комплексов с самодиагностикой, контроллеров с двойным и тройным модульным резервированием по схеме с голосованием или контроллеров с двойным резервированием и диагностикой, или использованием контроллеров в режиме “пара и резерв”, когда пара контроллеров работает параллельно, а вторая пара находится в горячем резерве и, если у первой пары в какой-то момент выходные сигналы начинают не совпадать, то работа безударно переключается на вторую пару, а первая тестируется на предмет выявления неисправности в одном из контроллеров;

— заданный интегральный уровень безопасности SIL, который должен обеспечиваться системой ПАЗ, подтверждается обязательной сертификацией всех компонентов системы ПАЗ на возможность их применения в системе ПАЗ заданного уровня SIL. Сертификация любого средства автоматизации на работу в системе ПАЗ заданного уровня SIL, которая подтверждает соответствие средства требованиям стандарта ГОСТ Р МЭК 61508-2012, производится независимым сертифицирующим агентством TUV Rheinland GmbH и его подразделениями в разных странах, в том числе в России. В США подобную сертификацию проводит агентство EXIDA;

— реализуется надежный интерфейс связи ПТК системы ПАЗ с оператором, который необходим для сигнализации о наступлении предаварийного состояния

и о моменте включения системы ПАЗ в работу, а также для выполнения команд оператора по пуску/останове объекта. При отказе системы ПАЗ специальная, надежная сигнализация об этом событии указывает оператору о необходимости ручного управления;

— связи системы ПАЗ с другими системами автоматизации данного объекта допускаются, только если они не нарушают заданных функций защиты и не могут изменить данные и программы системы ПАЗ;

— типовой набор прикладных программ, реализуемых в ПТК системы ПАЗ, состоит из анализа контролируемых в объекте величин, определяющих возможные неисправности в работе объекта, которые могут привести к аварии; выявления возникающих нарушений, имеющих предаварийный характер, и немедленной реакции на них в виде управляющих воздействий на взаимосвязанные исполнительные механизмы объекта, переводящие автоматизируемый объект в безопасное состояние. Управляющие программы системы ПАЗ, являющиеся логическими блокировочными схемами, обычно реализуются на языке Ladder Logic Diagrams (лестничных диаграмм) и тщательно тестируются и сертифицируются;

— операционная система контроллера является системой жесткого реального времени, точно обеспечивающая заданное время выполнения анализа измеряемых величин и реализации управляющих функций;

— кроме заложенных в проект воздействий по автоматическому останову процесса при возникновении предаварийной ситуации, должны быть предусмотрены ручные средства останова процесса оператором;

— проект должен учитывать функции безопасности и предотвращения аварий, которые решают операторы.

Требования, которые должны быть указаны в документации по эксплуатации системы ПАЗ:

— должны быть зафиксированы периоды необходимых проверок работоспособности системы ПАЗ и ее отдельных компонентов, включая контроль сети ПАЗ, тестирование прикладного программного обеспечения системы и рабочих характеристик исполнительного механизма, мониторинг работоспособности клапанов или других регулирующих органов путем задания их частичного хода. Следует отметить, что особенное значение имеет мониторинг клапанов (в большинстве случаев наиболее важных и наименее надежных компонентов системы). Их тестирование на неполный ход в пределах 5...10% от диапазона полного закрытия целесообразно повторять наиболее часто;

— сигналы тревоги при возникновении предаварийных ситуаций следует передавать как операторам, так и обслуживающему оборудование объекта персоналу;

— процедуры и правила внесения изменений в систему ПАЗ при любой модернизации автоматизируемого объекта должны регистрироваться с указанием следующих данных: содержания изменений, даты и времени внесения изменений, причины проведения изменений, имени проводившего изменения лица.

Заключение

Основными причинами широко распространенного отступления построенных систем ПАЗ от нормативных документов являются:

— экономия заказчика на проведении процедур анализа риска и определении конкретных показателей SIL функциям защиты; на приобретении всех компонентов систем ПАЗ, сертифицированных по необходимому уровню SIL; на полную изоляцию системы ПАЗ от системы контроля и управления объектом. В частности, приобрели контроллер, сертифицированный по уровню SIL 3, и считают, что вся система ПАЗ стала иметь уровень SIL3, что ошибочно;

— недостаточная квалификация организации, разрабатывающей и проектирующей систему ПАЗ (например, повторяют проекты прошедших лет без изменений, касающихся требований нормативных документов последних лет);

— отсутствие у заказчика или привлеченного системного интегратора органа, который может сформировать четкие, конкретные, полные и тщательно обоснованные существующими документами технические требования на систему ПАЗ (например, размыта ответственность за формирование недостаточно обоснованного задания на систему ПАЗ, по которому проводится ее создание).

Подробный анализ систем ПАЗ проведен в монографии [1], а также в [2].

Список литературы

1. *Федоров Ю.Н.* Справочник инженера по АСУТП: проектирование и разработка. Изд. «Инфра-Инженерия». 2008. 926 стр.
2. *Федоров Ю.Н.* Тенденции развития безопасных систем автоматизации // Автоматизация в промышленности. 2007. №8.

Ицкович Эммануил Львович *– д-р техн. наук, проф., главный научный сотрудник ИПУ им. В.А. Трапезникова РАН. Контактный телефон (495) 334-90-21.*