Интеллектуальная безопасность опасных производственных объектов ТЭК

Д.А. Блохин, В.А. Потехин (Группа компаний «Системы промышленной безопасности»)

Выявлены факторы, снижающие безопасность, в том числе кибернетическую, опасных производственных объектов, являющиеся причиной развития внеплановых остановов. Предложена концепция проектирования и реализации систем ПАЗ. Отмечен основной базовый принцип кибербезопасности АСУТП, заключающийся в сегментации РСУ и ПАЗ и интеграции сегментов со средствами киберзащиты.

Ключевые слова: противоаварийная защита, сегментация, киберзащита, опасные производства, логические схемы блокировок, человеческий фактор, контроллер.

Сегодняшние производственные объекты топливно-энергетического комплекса находятся в середине четвертой промышленной революции. Разрабатываются новые стандарты, меняются требования безопасности. Заказчики, полагающиеся на концепции безопасности предыдущего поколения, подвергаются значительному риску.

Экономические показатели и эффективность производства напрямую зависят от обеспечения непрерывной эксплуатации, что во многих случаях требует поиска решений и компромиссов между безопасностью и непрерывностью управления [1–3].

На основании исследований проектов систем противоаварийной автоматической защиты (ПАЗ) крупнотонажных нефтеперерабатывающих, нефтехимических и газоперерабатывающих производств, совсем новых и после модернизации АСУТП, для многих объектов можно отметить факторы, снижающие безопасность, в том числе кибернетическую, и являющиеся прямой причиной развития внеплановых остановов:

— построение каскадных структур систем ПАЗ на базе маломощных контроллеров безопасности, объединенных общей с РСУ информационно-управляющей шиной для межконтроллерного обмена данными (рис. 1);

— минимизация функциональности систем ПАЗ по причине ограничения каскадной структуры контроллеров ПАЗ;

— возможность единовременной кибернетической атаки на слои защиты РСУ и системы ПАЗ с вероятностью максимальной тяжести последствий — уничтожение производства.

Вопрос о соответствии типовой структуры АСУТП (рис. 1) требованиям ФНиП, приказу Ростехнадзора № 96 и приказу ФСТЭК № 31 требует компетентного и углубленного анализа взаимодействия всех компонентов структуры с учетом алгоритмов безопасности, реализованных в проекте.

Лучшая мировая инженерная практика исключает применение таких структур, и построение систем ПАЗ для крупнотонажных производств осуществляется на базе высокопроизводительных контроллеров безопасности, таких как HIMAX, практически не имеющих ограничения для реализации сложных взаимосвязанных алгоритмов безопасности.

В рамках Российского Консорциума Комплексной Автоматизации (РККА) в составе ООО «СПБ-XXI», ООО «ПРОСОФТ СИСТЕМЫ», ООО «СИСТЕМ АП» и ООО «ИНФОТЕКС» разработана концепция интеллектуальной безопасности (Smart Safety), в основу которой положены следующие принципы:

— обеспечение уровня полноты безопасности УПБ/SIL=3;

— обеспечение максимального уровня автоматических функций;

— минимизация человеческого фактора как фактора аварийности;

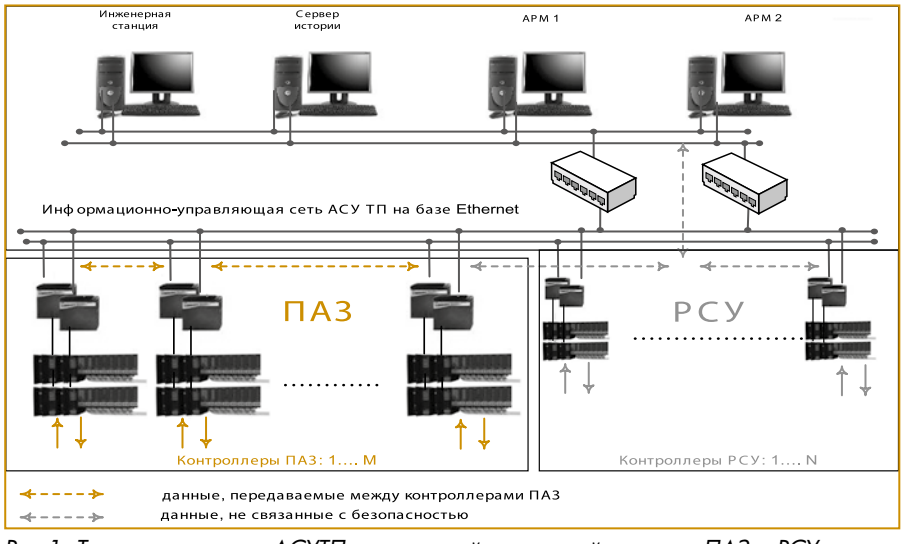

Рис.1. Типовая структура АСУТП с каскадной структурой: система ПАЗ и РСУ используют единую информационно-управляющую шину

— расширенная диагностика и экспертная оценка отклонений управляемого процесса;

— автоматические функции ПАЗ для изменений режимов процесса;

— сегментация РСУ и ПАЗ и интеграция каждого сегмента с аппаратными и программными средствами киберзащиты, согласно приказов ФСТЭК№ 31 и ФЗ-187 (рис. 2).

Важной составляющей частью ПТК (рис. 2) является его функциональность, реализованная в алгоритмах управления и защиты для различных режимов работы опасных производственных объектов (ОПО):

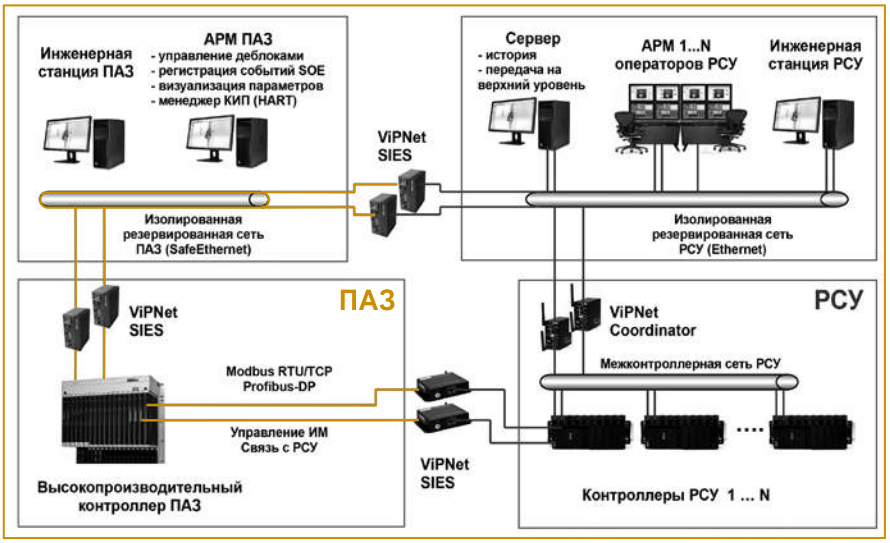

Рис.2. Типовая сегментированная структура АСУТП с высокопроизводительной интеллектуальной системой ПАЗ, включающей интегрированные средства кибернетической защиты

1) пусковые операции, выход на нормальный технологический режим;
2) нормальный технологический режим;
3) режим сниженной нагрузки, циркуляция;
4) плановый последовательный останов;
5) аварийный последовательный останов;
6) проведение ремонта на ОПО;
7) вывод из эксплуатации.

На многих эксплуатируемых ОПО система ПАЗ обеспечивает безопасность только в нормальном технологическом режиме. Часто обнаруживается факт постоянного отключения части контуров безопасности в нормальном режиме для обеспечения бесперебойной работы процесса. Как правило, это следствие проектных ошибок и недоработок.

Как это не парадоксально звучит, часто функциональность систем ПАЗ ограничена и в режиме аварийного останова, так как:

— отсутствуют алгоритмы реакции системы на неполное выполнение функций (например, не закрыт один из отсекателей);

— после срабатывания системы ПАЗ требуется выполнение ручных операций, невыполнение которых приведет к аварии;

— ложное срабатывание системы ПАЗ, например, в результате технической неисправности или алгоритмической ошибки процессора, и как следствие, может происходить останов по непредусмотренному сценарию.

Анализ инцидентов и аварий на технологических производствах показывает, что наиболее часто они происходят в ходе пусковых операций. Причины:

— нестабильные технологические режимы;

— широкое использование ручного дистанционного управления;

— большая частота срабатывания предупредительных сигнализаций;

— местный пуск/останов оборудования и местный контроль параметров процесса оперативным персоналом.

Ошибки операторов и эксплуатирующего персонала, отклонения технологического процесса, происходящие во время выполнения пусковых операций, имеют наиболее тяжелые последствия, так как:

— функции системы ПАЗ частично или полностью отключены;

— активно используются байпасные линии с ручной арматурой;

— в результате неэффективности систем безопасности происходит эскалация аварии (эффект домино);

— численность персонала в опасной зоне максимальна.

Таким образом, риски во время проведения пусковых операций максимальны. Проблема в том, что в пусковых режимах основная система управления (РСУ) и оперативный персонал выполняют достаточно сложные операции, распознать которые функционально ограниченная система ПАЗ не в состоянии. Часто для избегания ложных срабатываний функции безопасности отключаются персоналом. Поэтому системы безопасности должны быть столь же интеллектуальны, как и основная система управления.

В настоящее время на этапах проектирования технологических производств требуется проведение процедуры анализа опасности и работоспособности (АОР/HAZOP). Выполнение этой процедуры обусловлено современным риск-ориентированным подходом, согласно ФЗ-116 «О промышленной безопасности».

Благодаря такому подходу идентифицируются и детально исследуются факторы опасности, но, зачастую, эксперты не акцентируют внимание на выявлении проблем работоспособности, то есть

Рис. 3. Рекомендуемая последовательность разработки логических схем блокировки систем ПАЗ

на обеспечение непрерывного функционирования технологического процесса и систем автоматизации во всех режимах. Например, не выявляются проблемы выполнения последовательности пусковых операций, снижения нагрузки технологической установки, последовательного останова технологических блоков, вывода технологического оборудования и систем автоматизации в обслуживание и ремонт, компенсационные меры и реакция систем автоматизации в случае различных типов отказов их компонентов.

Для исключения этих проблем и разработки компенсационных мероприятий предлагается (рис. 3):

— разработать алгоритмы РСУ и системы ПАЗ для всех режимов работы ОПО;

— выполнить назначение УПБ/SIL и уровня устойчивости к ложным срабатываниям (УЛС) для контуров безопасности, например, с помощью анализа опасности и работоспособности контуров системы ПАЗ (HAZOP SIS — анализ опасности и работоспособности инструментальных контуров безопасности);

— выполнить анализ опасности и работоспособности алгоритмов РСУ и систем ПАЗ;

— использовать для построения систем ПАЗ безопасные и производительные концепции.

Разработка алгоритмов РСУ и систем ПАЗ современных интеллектуальных систем — одна из наиболее сложных и ответственных задач.

На стадии проектирования «П» технологического объекта алгоритмы разрабатываются специалистами-технологами с помощью описания последовательности операций и таблиц причинно-следственных связей (C&E) для всех режимов работы ОПО. Эта же документация используется для процедур AOP/HAZOP технологической части.

Согласно ФНиП, “выбор методов и средств системы защиты, разработка последовательности срабатывания элементов защиты, локализация и предотвращение развития аварий должны определяться в проектной документации по результатам анализа опасностей технологического процесса и оценки риска взрыва на основе анализа схем (сценариев) возможного развития этих аварий.”

Специалисты, разрабатывающие алгоритмы системы управления и СПАЗ, на основании своего опыта и/или используя результаты AOP/HAZOP технологической части проекта (если они были получены ранее) рассматривают как позитивные сценарии эксплуатации ОПО (безопасные режимы и последовательности), так и идентифицируют негативные сценарии (последовательности событий, приводящие к авариям).

Пример позитивного сценария:

«Продувка должна выполняться при следующих условиях:

— заслонки горелочного воздуха должны быть полностью открыты оператором,

— все отсекатели пилотного, магистрального, вторичного газа и мазута закрыты,

— расход дутьевого воздуха не низок,

— никакое пламя не обнаружено,

— системы безопасности в полностью исправном состоянии.

После нажатия кнопки «Начало продувки» система безопасности следит, что в течение 15 минут расход дутьевого воздуха не становится низким.»

Примеры негативных сценариев:

«1. Попытка розжига любой горелки без проверки газоплотности отсекателей и до завершения продувки топки является опасным событием и может привести к взрыву внутри топки или газохода.

2. Отсекатель мазута во время аварийного останова закрыт с запозданием, образование пролива мазута в топке или под горелками, пожар пролива при повторном розжиге.»

Все дальнейшие этапы проектирования интеллектуальной системы ПАЗ должны обеспечивать ее функционирование по позитивным сценариям и исключать работу по негативным сценариям.

На стадии разработки рабочей документации РСУ и СПАЗ на основании описания последовательности операций и таблиц причинно-следственных связей разрабатываются логические схемы блокировок (ЛСБ) в виде функциональных блоков. Для современных интеллектуальных систем логические схемы выполняются в виде многоуровневой, инкапсулированной логики, типовых (библиотечных) логических блоков. В таком виде алгоритмы становятся легкочитаемыми и верифицируемыми специалистами разных направлений (технологами, инженерами КИП, программистами). Кроме того, такой подход соответствует V-модели разработки программного обеспечения согласно ГОСТ Р МЭК 61508-3-2012.

Логические схемы блокировок интеллектуальной системы ПАЗ должны обеспечивать:

— автоматический последовательный пуск, согласно заданной циклограмме пуска (автоматический пуск)/автоматический вывод на режимы эксплуатации по этапам с подтверждением оператором перехода на следующий этап (полуавтоматический пуск)/контроль за действиями оператора при пусковых операциях, введение блокировок на неправильные действия (контроль безопасного пуска);

— контроль и анализ изменения технологических параметров при пусковых режимах, формирование предупредительных сообщений и инициализация компенсационных управляющих воздействий;

— автоматическое взведение и снятие деблокирующих ключей для обеспечения пусковых операций согласно технологического регламента, регистрация изменения состояния ключей;

— автоматический перевод процесса на предыдущую стадию пуска при обнаружении отклонений в пусковой операции, удержание процесса пуска;

— аварийный автоматический останов при достижении параметров, определяющих взрывоопасность аварийных уставок;

Таблица 1. Оценка уровня автоматизации системы ПАЗ и влияния человеческого фактора

Функция автоматизации	Уровень автоматизации	Возможность отключения «технологическими ключами»
Аварийный останов технологического процесса: – срабатывание отсекателей по критическому значению технологических параметров; – отключение динамического оборудования по критическому значению технологических параметров; – световая и звуковая сигнализация	35 %	Запрещено, если не предусмотрено технологическим регламентом
Последовательный пуск в полуавтоматическом режиме (контроль безопасного пуска, автоматическое включение функций безопасности)	15 % *	Разрешено перед началом пусковых операций
Последовательный пуск/останов в автоматическом режиме	30/20 %*	Запрещено
Диагностика предотказных состояний, PST	10 %	Запрещено, кроме PST, если предусмотрено
Функции автодеблокирования датчиков по результатам их диагностики	5 %	Запрещено
*Примечание: учитывается одна из этих двух функций		

— контроль за действием оператора, выдача предупреждающих сообщений, регистрация действий;

— автоматический последовательный или постадийный перевод процесса в безопасное состояние при опасных отклонениях технологических параметров или отказах технологического и инструментального оборудования, при разгерметизации, пожаре;

— контроль местных кнопок управления и местных переключателей исполнительных механизмов и технологического оборудования управляемого из системы ПАЗ, введение блокировки/разблокировки дистанционного или местного управления;

— обнаружение разгерметизации косвенными методами — по скорости изменения параметра при полном раскрытии аппарата или трубопровода, по соотношению динамики взаимосвязанных технологических параметров,

— диагностика контрольно-измерительных приборов методом определения рассогласования или мажорирования (предотаказное или деградированное состояние),

— контроль обрыва цепи или короткого замыкания в электрических внешних цепях контура безопасности, инициализация компенсирующих мер,

— диагностика исполнительных механизмов — отсекателей, электрозадвижек, насосов, вентиляторов по контролю времени после команды на включение/выключение, конечным положениям, идентификации скорости вращения/движения, по превышению или потере тока в электрических цепях двигателей, контролю диагностического частичного стрегивания отсекателей (partial stroke test — PST);

Таблица 2. Оценка полноты автоматических функций СПАЗ

Суммарный уровень автоматизации	Полнота автоматических функций системы ПАЗ
не более 40 %	опасно низкая
не более 60 %	низкая
не более 80 %	средняя
более 80 %	высокая

— автоматическое переключение на резервное оборудование в случае идентификации неисправности (насосы, компрессора, вентиляторы и пр.)

— частичный автоматический останов отдельных блоков (узлов), инициализация компенсирующих мер и обеспечение повторного пуска.

— автоматический перевод объекта на более низкую нагрузку.

В ходе работы в 2017 г. по разработке прототипа Стандарта Технического Отраслевого (СТО) на проектирование систем ПАЗ для объектов ПАО «Газпром-Нефть» авторами разработана методология оценки полноты автоматических функций системы ПАЗ для определения уровня автоматизации и влияния человеческого фактора (табл. 1, 2).

Выводы

При выборе контроллера ПАЗ должна учитываться возможность реализовать сложную логику для обеспечения максимального уровня автоматизации ОПО.

Разработанные ЛСБ, кроме оценки полноты автоматических функций, должны также подвергаться проверке на соответствие требования ФНиП для класса опасности ОПО. В ходе анализа должна оцениваться устойчивость алгоритмов к различным типам отказов и влиянию человеческого фактора.

Использование при построении систем ПАЗ безопасных, устойчивых и производительных концепций не только защищает от ошибок при проектировании, но и исключает тяжелые последствия от кибернетических атак. Киберзащита АСУТП полноценно достигается только при сегментации РСУ и ПАЗ, выполненных на программно-аппаратной базе различных производителей, при интеграции каждого сегмента со специальными аппаратными и программными средствами киберзащиты российского производства, сертифицированных ФСТЭК.

Список литературы

1. *Borcsok Josef.* Electronic Safety Systems. Hardware Concept. Models and Calculation. 2004.
2. *Гражданкин А.И.* О некоторых важных терминах и понятиях из Федеральных норм и правил в области промышленной безопасности "Общие требования к обоснованию безопасности опасного производственного объекта. 2018. https://www.safety.ru
3. *Печеркин А.С.* Взаимоувязанные научные проблемы оценки, нормирования и экспертизы рисков промышленной безопасности. 2017. сентябрь. https://www.safety.ru

Блохин Дмитрий Александрович *– технический директор ООО «СПБ-XXI",*
Потехин Валерий Анатольевич *– генеральный директор ООО «СПБ-Экспертиза»*
Группа компаний «Системы промышленной безопасности».
Контактный телефон (495) 787-28-94.
E-mail: v.potekhin@spb-xxi.ru