

ИНТЕГРАЦИЯ СИСТЕМ ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ С АСУ ТП

Лёвин Сергей Николаевич
главный конструктор ГК «СИГМА»

В статье рассматриваются вопросы построения автоматической системы противопожарной защиты (АСПЗ) для крупных промышленных объектов, а также интеграции АСПЗ с автоматизированной системой управления технологическими процессами (АСУ ТП) нефтеперерабатывающих и нефтехимических производств. Современная АСПЗ организуется по трехуровневому принципу построения:

- *Полевой (объектовый) уровень.*
- *Уровень управления.*
- *Уровень диспетчеризации.*

Собственно говоря, по такому же принципу строится и АСУ ТП. Причем интеграция АСПЗ с АСУ ТП может производиться на любом из указанных уровней.

АВТОМАТИЧЕСКАЯ СИСТЕМА ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ

Рассмотрим состав, назначение и способы взаимодействия уровней АСПЗ.

На полевом уровне размещаются извещатели, исполнительные устройства управления, оповещения и пожаротушения. Для производственных помещений без требований к взрывозащищенности чаще всего применяются адресно-аналоговые точечные дымовые и тепловые извещатели, адресные ручные пожарные извещатели, адресные светозвуковые оповещатели. Применение адресных устройств позволяет повысить надежность работы системы, снизить затраты на кабели шлейфов сигнализации и упростить техническое обслуживание. В условиях большого предприятия возможность удаленной автоматической диагностики состояния оборудования является определяющей для эксплуатационных служб. Например, адресно-аналоговые дымовые пожарные извещатели имеют возможность передачи в ППК (прибор приемно-контрольный пожарный) значения параметров запыленности дымовой камеры. На основании этих данных может быть составлен план предупредительного технического обслуживания.

Для открытых производственных площадок и взрывоопасных зон применяется термокабель – линейный тепловой пожарный извещатель для монтажа во взрывоопасных зонах. Для обнаружения открытых очагов возгорания применяются оптические инфракрасные или ультрафиолетовые извещатели пламени, способные обнаруживать возникновение источников возгорания углеводородного, водородного, гидроксидного топлива, легко воспламеняемых металлов и неорганических материалов в поле зрения извещателя. Извещатели пламени размещают в местах установки технологического оборудования резервуарных пар-

ков, наливных эстакад и т. д. Извещатели во взрывозащищенном исполнении подключаются к адресным расширителям через барьер искрозащиты. Адресный расширитель, в свою очередь, включается в общий адресный шлейф наряду с другими адресными устройствами. Для защиты от короткого замыкания в адресном шлейфе должны быть предусмотрены специальные модули, размыкающие шлейф при обнаружении КЗ. Для сохранения работоспособности после срабатывания модуля КЗ, а также для защиты от обрыва адресный шлейф имеет кольцевую топологию. Двухпроводный адресный шлейф служит для передачи данных между адресными устройствами и ППК, а также одновременно используется для подачи электропитания на устройства в шлейфе.

Уровень управления для АСПЗ строится на базе специализированных приемно-контрольных приборов (ППК), которые обеспечивают обработку данных от извещателей и выдачу команд управления на исполнительные устройства. Как правило, данное оборудование размещается в контроллерных – специальных помещениях для управляющего оборудования АСУ ТП. Для включения в общую систему ППК должны иметь соответствующие интерфейсы (Ethernet, RS-485), а также поддерживать распространенные протоколы (Modbus RTU, Modbus TCP, OPC).

На уровне диспетчеризации организуются автоматизированные рабочие места (АРМ) операторов и администраторов АСПЗ. Связь между ППК и верхним уровнем реализуется чаще всего через сеть Ethernet. Применение Industrial Ethernet решений позволяет получить резервированное подключение между уровнями управления и диспетчеризации. Многие крупные нефтеперерабатывающие и нефтехимические предприятия подпадают под требования 188-ФЗ, что означает обязательное применение российского программного обеспечения для решения задач по организации уровня диспетчеризации.

**КОМПЛЕКСНЫЕ
СИСТЕМЫ**

■ КОМПЛЕКСНЫЕ СИСТЕМЫ

Это касается как прикладного, так и системного программного обеспечения, прежде всего операционных систем. Исходя из личного опыта и сравнительной эксплуатации нескольких отечественных ОС (МСВС, Astra Linux, Эльбрус), могу отметить, что в настоящий момент наиболее развитой и совершенной российской защищенной операционной системой является Astra Linux SE релиз «Смоленск» производства АО «НПО РусБИТех».

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Автоматизированная система управления технологическими процессами промышленного предприятия (АСУ ТП) – это человеко-машинная система управления, обеспечивающая автоматизированный сбор и обработку информации, необходимой для оптимизации управления технологическим объектом в соответствии с принятыми критериями по технологии и безопасности.

АСУ ТП строятся на основе отказоустойчивых промышленных логических контроллеров управления (ПЛК) для долговременной круглосуточной эксплуатации на технологических объектах, для которых последствия отказа представляют серьезную угрозу для оборудования, жизни и здоровья людей.

Современный комплекс АСУ ТП включает в себя две основные составляющие: распределенную систему управления (РСУ) и систему противоаварийной автоматической защиты (ПАЗ). РСУ, в свою очередь, представляет собой программно-аппаратный комплекс, состоящий из контрольно-измерительных приборов и автоматики (КИПиА), программируемых логических контроллеров (ПЛК), интерфейсов связи и человеко-машинного интерфейса (станция оператора, станция инженера, станция инженера КИПиА).

РСУ – система управления, характеризующаяся построением распределенной системы ввода/вывода и децентрализацией обработки данных. РСУ, как правило, применяются для управления непрерывными технологическими процессами. К непрерывным процессам можно отнести те, остановка которых может привести к порче изготавливаемой продукции, поломке технологического оборудования и даже несчастным случаям, а также те, возобновление которых связано с большими издержками.

Если рассматривать иерархическое построение АСУ ТП в сравнении с АСПЗ, то распределение по уровням выглядит следующим образом.

Полевой уровень – это датчики, исполнительные устройства и измерительные приборы КИПиА. Устройства полевого уровня включаются в промышленную сеть или, как чаще говорят, в полевую шину. В основном применяют подключения на базе витой медной пары, существует большое количество стандартов организации физического уровня и протоколов полевых шин. Пожалуй, самыми распространенными являются Modbus и Profibus. Modbus – это открытый промышленный протокол передачи данных, реализуемый поверх интерфейса RS-485 (Modbus RTU) или Ethernet (Modbus TCP). Profibus (Process Field Bus) – открытая промышленная сеть, первая реализация которой была разработана компанией Siemens для своих промышленных контроллеров Simatic. На основе этого прототипа разработаны международные стандарты IEC 61158 и EN 50170. Поддержкой, стандартизацией и развитием сетей стандарта Profibus занимается Profibus Network Organization (PNO).

Уровень управления организуется на базе программируемых логических контроллеров (ПЛК). Если ПЛК в АСПЗ имеют во многом predetermined функциональность, то ПЛК предполагает свободную реализацию алгоритма работы контроллера под конкретную задачу. Для программирования ПЛК используются стандартизированные языки МЭК (IEC) стандарта IEC61131-3. Среди них самыми распространенными являются LD (Ladder Diagram) – язык релейных схем и FBD (Function Block Diagram) – язык функциональных блоков.

Как уже говорилось выше, устройства нижнего уровня связаны с ПЛК через полевые шины. Между собой контроллеры также могут быть объединены в сеть через аналогичные интерфейсы полевых шин или через индустриальный Ethernet. Так как РСУ предполагает

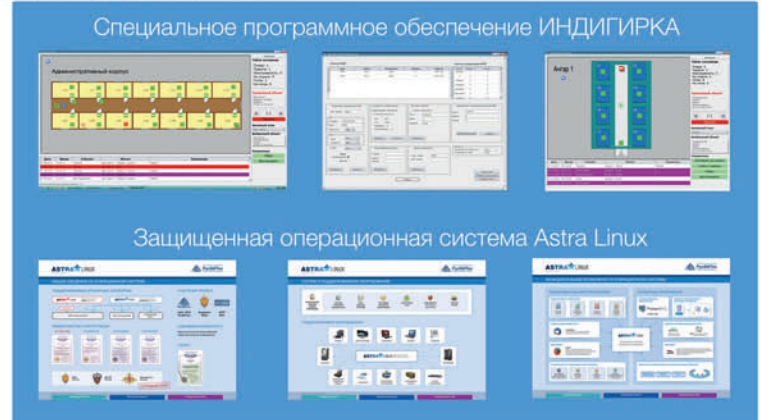
ИНДИГИРКА

ЗАЩИТА ВАЖНЫХ ОБЪЕКТОВ

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ ОБЪЕКТОВ ТЭК

Все три уровня системы построены на российской продукции

Уровень диспетчеризации



Уровень управления



Полевой уровень



децентрализованную архитектуру, то сеть ПЛК должна быть одноранговой – организована без выделенного сервера. В такой сети все узлы, в данном случае ПЛК, равноправны и при выходе из строя любого контроллера работоспособность остальных устройств сохраняется. Вообще, при проектировании отказоустойчивой АСУ предъявляются требования, что единичный выход из строя любого компонента не должен приводить к сбою в работе системы. Конечно, плата за такие требования – резервирование оборудования и каналов передачи данных, вследствие этого избыточность и повышение стоимости системы. Тем не менее, для ответственных применений такой подход, безусловно, оправдан и является единственно верным. Помимо резервирования компонентов РСУ на потенциально опасных объектах обязательной к применению является и система ПАЗ, которая в свою очередь также подстраховывает основную АСУ на случай сбоя или отказа в обслуживании. Нарушение работы системы управления не должно влиять на работу системы противоаварийной защиты.

Уровень диспетчеризации в АСУ ТП традиционно строится на базе специального ПО SCADA (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных). SCADA-системы решают следующие основные задачи: обмен данными с ПЛК, отображение информации на экране монитора в удобной и понятной для человека форме, ведение базы данных реального времени с технологической информацией, аварийная сигнализация и управление тревожными сообщениями, подготовка и генерирование отчетов о ходе технологического процесса.

ИНТЕГРАЦИЯ СИСТЕМ АСПЗ И АСУ ТП

Интеграция систем АСПЗ и АСУ ТП может быть выполнена на каждом из трех уровней. Взаимодействие на полевом уровне характерно, прежде всего, для ПАЗ. Система противоаварийной защиты реализуется максимально независимо от других

систем. Как правило, система ПАЗ получает данные о состоянии объекта от собственных дублированных датчиков. Одной из самых надежных схем считается «2оо3», когда срабатывание любых 2 из 3 датчиков, установленных на одной контрольной точке, считается необходимым условием для срабатывания защитной блокировки. Также ПАЗ управляет своими резервированными исполнительными механизмами. Конечное оборудование не зависит от оборудования РСУ и АСПЗ, к примеру, если сложилась аварийная ситуация и для ее предотвращения нужно закрыть клапан, то при возникшей ситуации сработает исполнительный механизм системы ПАЗ.

Вообще, все оборудование ПАЗ должно выполнять требования ГОСТ Р МЭК 61508 по функциональной безопасности систем. Согласно данному стандарту системы по уровню безопасности делятся на 4 уровня, в зависимости от допустимой частоты отказа системы и величины вероятного ущерба при возникшем отказе.

Уровень SIL1 (Safety integrity level – уровень полноты безопасности)

Возможный ущерб:

оборудование, продукция

Допустимое число отказов:

1 на 0,1 млн часов

Уровень SIL2

Возможный ущерб:

травматизм персонала

Допустимое число отказов:

1 на 1 млн часов

Уровень SIL3

Возможный ущерб:

гибель персонала или населения

Допустимое число отказов:

1 на 10 млн часов

Уровень SIL4

Возможный ущерб:

общая техногенная катастрофа

Допустимое число отказов:

1 на 100 млн часов

При проектировании ПАЗ задается требуемый уровень безопасности, и все оборудование должно быть сертифицировано на выбранный уровень SIL. Если

выбран SIL3, то все контроллеры, датчики и исполнительные механизмы ПАЗ должны быть не ниже SIL3. Возможно повышение уровня безопасности отдельных элементов за счет их дублирования. Если два взаимно резервируемых датчика имеют SIL1, то их общая сборка может дать уже уровень SIL2. Системы ПАЗ для нефтеперерабатывающих и нефтехимических объектов являются в прямом смысле последним рубежом обороны, за которым происходят уже неконтролируемые действия: разрушение технологического объекта, взрыв, выброс опасных веществ и связанные с этим угрозы для жизни людей.

Также на полевом уровне может быть организовано взаимодействие между АСПЗ и РСУ. Извещение о пожаре в этом случае передается в РСУ через «сухие контакты». При большом количестве сигналов для передачи между системами может быть задействован уровень управления. В этом случае оборудование АСПЗ работает с РСУ через информационные каналы передачи данных. Например, ППК может быть подключен к ПЛК распределенной системе управления через Modbus TCP. В объеме автоматизации РСУ сигналы от АСПЗ занимают значительное место, так как при опасности возгорания практически все участки технологического процесса должны реагировать на пожароопасную ситуацию с целью перевода объекта в максимально безопасное состояние. Также как при построении самой АСУ ТП, при решении задачи интеграции с АСПЗ, такую же важную роль играет надежность стыковки этих систем. Поэтому требования к резервированию распространяются и на интерфейсы передачи данных между АСПЗ и РСУ.

На объекте может быть реализован единый уровень диспетчеризации. В этом случае на базе SCADA-системы организуются как технологические АРМ, так и рабочие места операторов АСПЗ. Типовая схема подключения оборудования к SCADA-системе предполагает применение технологии OPC (OLE for Process Control). Со стороны оборудования выступает OPC-сервер, позволяющий любое оборудование представить унифицированным образом, как и данные для OPC-клиента, которым, по сути, является SCADA-система. В настоящее время все еще распространены OPC серверы, разработанные на базе технологии DCOM компании Microsoft. Однако в современных проектах все чаще используется новая технология OPC UA (Unified Architecture), главное достижение которой, это отвязка архитектуры OPC от Windows, что позволяет реализовать OPC UA сервер на хосте под управлением Unix/Linux систем.

Как мы видим, АСПЗ и АСУ ТП тесно связаны на всех уровнях, так как противопожарная защита и своевременное реагирование на пожарную опасность является важнейшей задачей обеспечения безопасного функционирования сложных технологических объектов.

