Введение

На любом производственном предприятии необходимо помнить о вероятности отказа или выхода из строя оборудования, а также об авариях, связанных с так называемым человеческим фактором. При возникновении нештатных ситуаций необходимо предусмотреть возможность обеспечения безопасности оператора и оборудования. Ответственность за ситуации, непредусмотренные ТП, берет на себя система противоаварийной защиты (ПАЗ).

Более подробно об аппаратных и программных компонентах, входящих в системы ПАЗ, рассказывается в статье "Failsafe – значит повышенная безопасность" (Компания Siemens).

Трудно переоценить задачу организации передачи данных между устройствами, входящими в систему ПАЗ. Материал "Желтые" модули противоаварийной защиты работают по промышленной шине" повествует о новом подходе к организации обмена данными в системе ПАЗ через традиционные промышленные шины на основе модулей безопасности ввода/вывода TwinSAFE и технологии PROFI-safe (Компания Beckhoff).

Обсудить все составляющие системы ПАЗ в одном номере журнала не представляется возможным. Поэтому в этом выпуске журнала акцент сделан на средствах и системах обеспечения техники безопасности персонала. Представлена продукция от компаний Banner, Omron и SICK AG.

Термины, наиболее часто встречающиеся при обсуждении темы

Время доступа – время, необходимое для доступа к опасным деталям механизма после поступления команды останова от запорного механизма. Вычисления основаны на оценках скорости, значения которых выбираются для конкретных случаев с учетом параметров из стандарта EN 999.

Категория безопасности – разделение деталей блока управления на категории в отношении их отказоустойчивости и поведения в случае отказа, связанного со структурной организацией компонентов и/или их надежностью.

Оценка риска – определение опасных ситуаций и событий, которые могут вызвать повреждение оборудования, а также вероятность возникновения таких событий.

Разрешение – минимальный размер объекта, который может быть обнаружен защитным устройством, чувствительным к электричеству.

Связанный контакт – нормально замкнутые и разомкнутые контакты, механически связанные в устройстве таким образом, чтобы исключить их одновременное замыкание.

FAILSAFE – ЗНАЧИТ ПОВЫШЕННАЯ БЕЗОПАСНОСТЬ

С.А. Михайлин (ООО "Сименс")

Показана и обоснована значимость системы противоаварийной защиты (ПАЗ) на производстве. Приводятся положения из нормативной базы, регламентирующей построения систем ПАЗ. Кратко рассмотрены все составляющие компоненты, необходимые для построения полноценной системы ПАЗ, начиная с датчиков и заканчивая контроллерами и ПО.

Технику безопасности по работе с бензопилой я знаю, как все свои три пальца...

Введение

Безопасность на производстве... Как много разговоров на эту тему ведется на реальных технологических площадках, и как часто, порой, они не находят свою реализацию на практике. Казалось бы, все просто, согласно первому закону робототехники, робот (он же, система управления любым ТП), не должен своим действием или бездействием нанести вред человеку. То есть АСУ должна любым образом пресечь возникновение опасной для человека ситуации, будь это тривиальный удар 220В или катастрофический взрыв химического реактора. Но когда дело доходит до реализации этого принципа, то возникает множество вопросов и споров о том, как это сделать. Как правило, речь сразу заходит о построении системы противоаварийной защиты (ПАЗ) или Emergency Shutdown System (ESD). Многие видят в этом термине только контроллер, который следит за объектом и не дает развиться опасной ситуации. Но в реальности система ПАЗ должна представлять собой некий специальный программно-технический комплекс, подкрепленный особой нормативной базой. Именно о таких продуктах от фирмы Siemens я и хотел бы рассказать в данной статье. Все они входят в особое семейство, которое называется Safety Integrated.

В 1880 г. основатель нашей фирмы Вернер фон Сименс сказал: "Техника безопасности должна быть расценена не только как закон, а скорее как следование человеческим обязательствам и экономической рациональности". И сегодня это высказывание является философией построения систем безопасности от Siemens.

Стандарты и правила

Начнем с азбучных истин, которыми для систем ПАЗ являются как раз стандарты и законодательные документы. Обратим внимание сначала на теперь уже очень близкую нам Европу и увидим огромное число нормативных документов, регламентирующих различные аспекты безопасности на производстве. Но это не значит, что они входят в противоречие между собой. Просматривается удивительно четкая иерар-

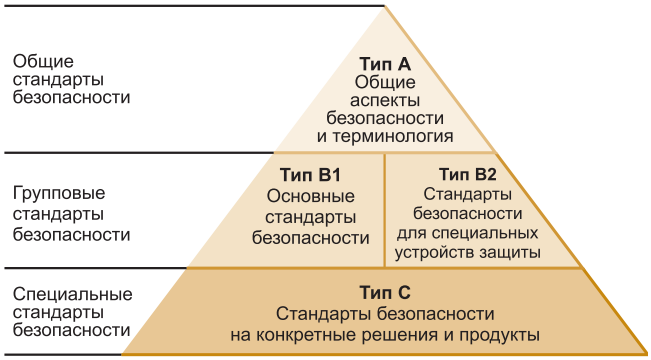

Рис. 1

Таблица 1

Класс безопасности (AK) DIN V 19250	Уровень безопасности (SIL)IEC61508	Категория безопасности EN954-1
1	C	B
2 и 3	1	1 и 2
4	2	3
5 и 6	3	4
7 и 8	4	C

хия этих стандартов, позволяющая четко определить требования, которые должны быть предъявлены к системе безопасности. Европейские стандарты EN для безопасности на производстве, признаваемые по всему миру, имеют структуру в виде пирамиды, приведенной на рис. 1.

Стандарты типа А содержат базовую терминологию и определения для всех производств. Например, стандарт EN 292 "Safety of machinery – Basic Concepts, general principles for design" в основном указывает на конкретные части стандартов типа В и С.

Стандарты типа В включают все стандарты безопасности, относящиеся к определенным группам оборудования. Данный тип разбит на две части: В1 – стандарты высокого уровня такие, как эргономика, безопасное расстояние до источника опасности, минимальное расстояние для предотвращения повреждения частей тела и т. д.; В2 – стандарты на оборудование для безопасности (кнопки аварийного останова, блоки защиты, безопасные исполнительные механизмы и т.д.).

Стандарты типа С регламентируют безопасность для конкретных применений: станки, лифты, горелки, прессы, конвейеры, теплообменники, печи, реакторы и т.д.

Европейские стандарты структурированы так, что основные утверждения, которые уже прописаны в типах А или В не повторяются в С. Для конечного пользователя или разработчика именно стандарты типа С имеют наивысший приоритет. Если же для какого-либо применения не существует стандарта С, то силу имеет стандарт В.

В соответствии с этими стандартами разработана система оценки степени опасности того или иного оборудования. В табл. 1 приведены различные критерии безопасности для промышленного оборудования.

Чем выше критерий, тем опаснее данное оборудование и тем строже должны быть требования для системы ПАЗ. Именно здесь и кроется первый и важнейший аспект построения этой системы. Она должна быть построена *только* на сертифицированных для данного класса или уровня безопасности программных и аппаратных компонентах.

Именно этим занимается, например, всемирно известная организация TUV. Она сертифицирует компоненты для применения их в системах ПАЗ для установок различной степени опасности по всему миру. И, естественно, нельзя применять несертифицированное оборудование.

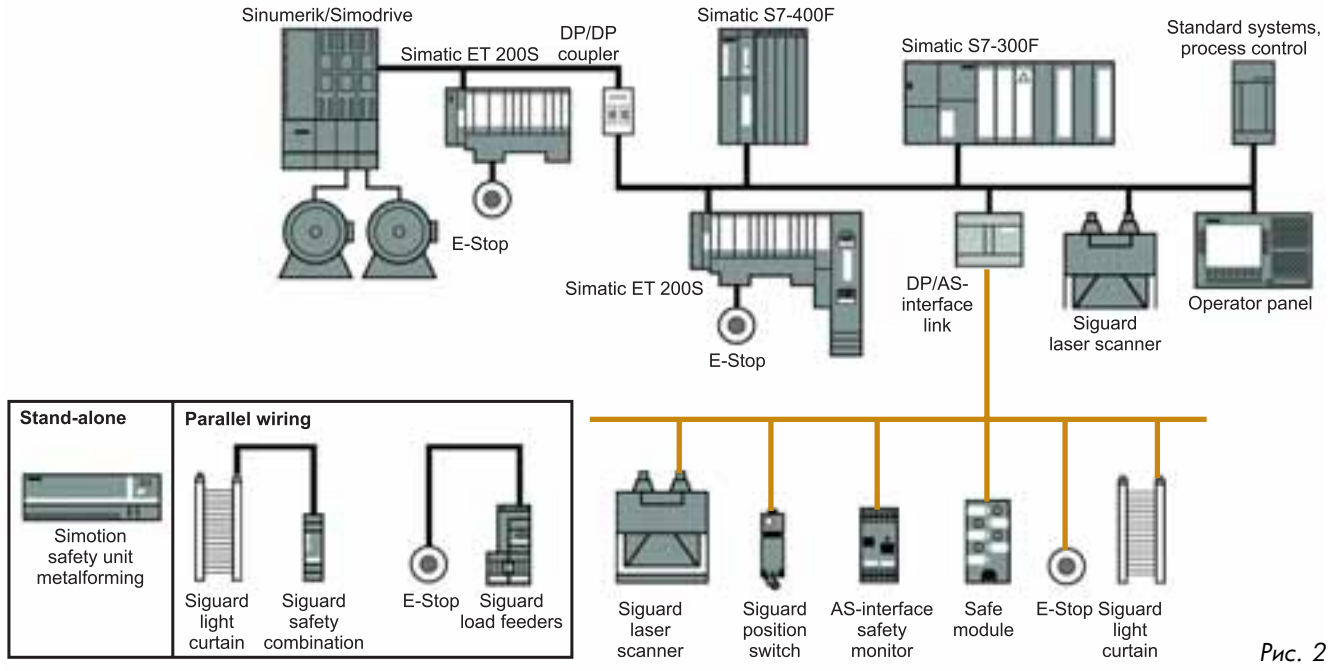

Рис. 2

Безопасная производственная система - это выведенная из действия система...

Журнал "Автоматизация в промышленности"

В связи с этим наряду с обычными компонентами автоматизации в спектре многих фирм-производителей появляются так называемые Failsafe компоненты повышенной безопасности. Ими могут быть центральные процессоры, модули ввода/вывода, ПО, датчики и исполнительные механизмы и даже сетевые протоколы. Эти компоненты работают в составе систем ПАЗ, и с помощью них достигается нужный уровень безопасности.

Разработчику в Европе не нужно думать, на каких компонентах построить систему ПАЗ. Он знает стандарт безопасности на свою установку и соответственно знает ее класс или уровень безопасности. Остается только выбрать соответствующие сертифицированные компоненты определенной фирмы, и юридический вопрос исчерпан.

А что в России? В России существуют ГОСТы и Правила, регламентирующие построение систем ПАЗ, но, как правило, они плохо структурированы. Нет четкой единой концепции безопасности для различных отраслей промышленности, а есть отдельные нормативные документы на каждую отрасль или агрегат. Причем нередко эти документы несут несколько расплывчатую информацию. Также полностью отсутствует единая система классификации безопасности на производстве, с одной стороны, и ни в какой мере нигде в этих документах нет ссылок на международные нормы, описанные выше, – с другой. То есть при построении той или иной системы ПАЗ разработчик может применить *любые* компоненты управления, а правила и ГОСТы определяют исключительно архитектуру ПАЗ системы, а никак не сами компоненты, причем часто и этот выбор тоже предоставляется разработчику.

Возьмем, к примеру, химическую и нефтеперерабатывающую отрасли. Для них существуют классификация объектов по взрывоопасности и правила безопасности Госгортехнадзора за номером ПБ 09-170-97. В этих правилах глава 5.3 полностью посвящена построению систем ПАЗ[1].

Что мы видим? Только пункты 5.3.11 и 5.3.13 имеют строгие требования по архитектуре, остальное ... определяется разработчиком. То есть, один и тот же объект может иметь абсолютно разную реализацию системы ПАЗ, предложенную разными разработчиками и все они будут соответствовать правилам.

А так как не существует российской классификации компонентов управления по безопасности, то их выбор полностью остается за разработчиком. И примерно такая же ситуация наблюдается в остальных отраслях.

Итак, получается, что система ПАЗ в России может иметь самую различную структуру и быть построена на самых разных и любых компонентах. Это нисколько не противоречит правилам.

Какая система ПАЗ более или менее безопасна, определит только опыт работы. И получится как в эпиграфе.

Из всего этого можно сделать неутешительный вывод, что специализированные Failsafe компоненты управления из Европы не имеют в России нормативной базы, и так как они несколько дороже своих стандартных собратьев, редко применяются по своему прямому назначению. "Зачем платить больше, если можно применить стандартные компоненты в системе ПАЗ и это удовлетворяет всем требованиям?" – думает разработчик и конечный пользователь. Этим и объясняется почти полное отсутствие полноценных Failsafe компонентов на реальных производствах.

Казалось бы на этом можно закончить; нет бумажки – нет разговора, но реально Failsafe компоненты могут гораздо больше и обеспечивают безопасность на качественно новом уровне, чем стандартные. И именно рассказом об этих особенностях продолжим статью.

Основное отличие любого Failsafe компонента в том, что он работает как параноик, постоянно проверяя все вокруг себя на предмет возникновения любой ошибки и, если она возникает, то компонент автоматически переходит в безопасное для ТП состояние. Это достигается за счет внутренних функций и специализированного ПО на системном уровне. Это дает гарантию того, что на безопасность не повлияет пресловутый человеческий фактор. Ведь если используются стандартные компоненты, где эти функ-

[1]5.3.1. Надежность и время срабатывания систем противоаварийной автоматической защиты определяются разработчиками систем ПАЗ с учетом требований технологической части проекта. При этом учитываются категория взрывоопасности технологических блоков, входящих в объект, и время развития возможной аварии.

5.3.3. Выбор системы ПАЗ технологических объектов и ее элементов осуществляется, исходя из условий обеспечения ее работы при выполнении требований по эксплуатации, обслуживанию и ремонту в течение всего межремонтного побега защищаемого объекта.

5.3.10. Надежность систем ПАЗ обеспечивается аппаратурным резервированием различных типов (дублирование, троирование), временной и функциональной избыточностью и наличием систем диагностики и самодиагностики. Достаточность резервирования и его тип обосновываются разработчиком проекта.

5.3.11. Надежность контроля параметров, определяющих взрывоопасность процесса, на объектах с технологическими блоками I и II категорий взрывоопасности обеспечивается дублированием систем контроля параметров, наличием систем самодиагностики с индикацией рабочего состояния, контролем значений технологически связанных (косвенно) параметров.

Технические решения по обеспечению надежности контроля параметров, имеющих критические значения, на объектах с технологическими блоками III категории взрывоопасности разрабатываются и обосновываются разработчиком проекта.

5.3.13. Контроль за параметрами, определяющими взрывоопасность ТП с блоками I категории взрывоопасности, осуществляется не менее, чем от двух независимых датчиков с раздельными точками отбора.

ции не заложены, то все операции по обработке *всех возможных* ошибок ложатся на человека, который программирует систему ПАЗ, и, следовательно, на него должна ложиться вся ответственность за ее работу. С применением Failsafe компонентов пользователь имеет сертификат, удостоверяющий необходимый уровень безопасности и дающий определенные гарантии от изготовителя и сертифицирующих органов. И несколько большие финансовые затраты на закупку Failsafe компонентов с лихвой окупаются на этапе проектирования и работы установки в технологическом и, самое важное, аварийном режимах.

Failsafe компоненты от компании Siemens

Перейдем непосредственно к Failsafe компонентам, поставляемым компанией Siemens. В эту линейку входят все необходимые кирпичики для построения полноценной ПАЗ системы, начиная с датчиков и заканчивая контроллерами и ПО. Обобщенная структура представлена на рис. 2.

Первыми хотелось бы упомянуть центральные процессоры Failsafe, которые имеют ряд отличительных особенностей в принципе работы по сравнению со стандартным ЦПУ. Помимо контрольных сигналов из модулей ввода/вывода эти ЦПУ полностью контролирует корректность выполнения как отдельной программной операции, так и всей программы целиком. Такие процессоры помечены литерой F, что означает возможность их применения в Failsafe системах. На сегодняшний день имеются следующие типы F-процессоров из линейки: S7-400 (ЦПУ 414F, 416F и 417F); S7-300 (ЦПУ 315F и 317F); станции распределенной периферии ET 200S (ЦПУ 151F). Все эти процессоры сертифицированы для построения Failsafe систем вплоть до SIL3.

Рассмотрим простейший пример работы оператора "И" в Failsafe ЦПУ (рис. 3).

Стандартный ЦПУ обработает эту команду "в лоб", а Failsafe ЦПУ подвергнет проверке саму логику работы этого блока, преобразуя входные операнды на обратные и проведя над ними обратную операцию. Затем, сравнив результат, можно судить о корректности работы данной операции. В случае несоответствия результатов прямой и обратной операции, будет выдан сигнал об ошибке, и можно принимать решение о безопасном аварийном останове. И такая процедура проводится на всех этапах работы системы. Даже вся программа выполняется дважды в одном Failsafe ЦПУ с последующим сравнением результатов. Можно сказать, что в одном аппаратном процессоре работают по принципу "И" два виртуальных процессора, т. е. и тот, и другой процессоры должны работать и результаты этих работ сравниваются. Но не надо думать, что Failsafe ЦПУ узко специализировано и может только что-то одно. Интеграция – очень важное достоинство F-ЦПУ от Siemens. В нем можно программировать и исполнять одновременно как Failsafe, так и стандартную программу управления. Это позволяет использовать один процессор как для управления установкой, так и для ее защиты. Причем это никак не повлияет на степень ее безопасности. Программы исполняются в разных циклах и областях памяти и не зависят друг от друга, но при желании могут обмениваться данными друг с другом.

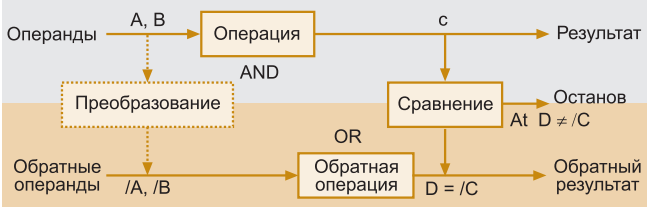

Рис. 3

Здесь мы подходим к другому аспекту Failsafe систем, а именно к ПО для их программирования. С одной стороны, логика описанная выше не присутствует в стандартных блоках, а, с другой – конечный пользователь всегда хочет избавиться от ошибок при программировании, особенно в системе ПАЗ. Поэтому такие системы от Siemens всегда программируются *только* сертифицированными TÜV блоками из специальной библиотеки. Все эти блоки имеют встроенную логику проверки функционирования и сравнения результатов. Это не усложняет разработку, поскольку все эти задачи скрыты от программиста и выполняются ОС самого ЦПУ. Программист не может использовать в Failsafe программе свой собственный или стандартный блок, поскольку они не сертифицированы для этого применения. Это дает гарантию отсутствия внутренних программных ошибок. Кроме того, при каждой компиляции Failsafe программы создается уникальная электронная подпись, позволяющая отследить изменения в ней, и, конечно же, программа защищается паролем.

Далее рассмотрим специальные модули ввода/вывода. Да-да, именно специальные. Периферия Failsafe системы, центральная или распределенная на базе станций ET 200, строится с применением особых сертифицированных модулей ввода/вывода. Они поддерживают уровень вплоть до SIL 3 и имеют в своем составе модули дискретного ввода/вывода и аналогового ввода. Аналоговый вывод в системах ПАЗ отсутствует, потому что в ней нет регулирования, и все, что требуется сделать, это закрыть и отключить, то есть исключительно дискретные команды. Каждый из этих модулей имеет дополнительные контрольные цепи для каждого канала, чтобы проводить проверку достоверности сигнала и выявлять ошибки в нем. То есть сигнал с датчика логически раздваивается в канале и проходит дополнительную обработку с последующим сравнением, что гарантирует правильную работу модуля (рис. 4). Для этого в Failsafe модулях присутствует свой собственный микропроцессор для анализа сигналов по основной и контрольной цепям.

Причем, если при подключении по менее жесткому SIL 2 стандарту разводка производится по закону дат-

чик – канал, то по SIL 3 датчик разводится сразу на два аппаратных канала, то есть сигнал проходит удвоенную проверку в контрольных цепях каждого их каналов. Эти каналы не дублируют друг друга, хотя и это возможно, они проводят дополнительный контроль сигнала на предмет выявления ошибки. Каждый канал вывода имеет два ключа, управляемые по принципу "И" соответственно основной и контрольными цепями.

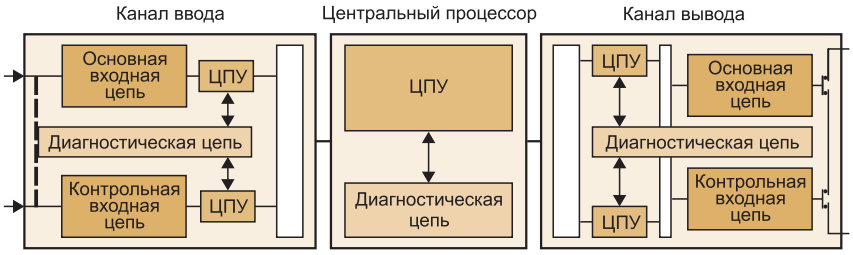

Рис. 4

Стандартные функции связи и функции F-связи между программируемым контроллером и станциями распределенного ввода/вывода ET 200M/ET 200S реализуются через сеть PROFIBUS DP. Для передачи данных F-систем в сети PROFIBUS используется специальный профиль *PROFISafe*. Этот профиль позволяет использовать для передачи данных F-систем стандартные фреймы сообщений PROFIBUS DP со специальными добавками для проверки корректности выполняемых операций. Дополнительные аппаратные компоненты для этой цели не нужны. Необходимое ПО либо интегрировано в ОС аппаратных компонентов, либо загружается в центральный процессор в виде сертифицированных программных блоков.

Конечно же, нельзя не упомянуть специальные Failsafe датчики. Особенно большая серия этих датчиков, под названием SIGUARD (рис. 5), представлена для машиностроения и тяжелой промышленности, где преобладают дискретные сигналы защиты в виде зоны безопасности и безопасных концевых положений. Наиболее продвинутыми датчиками из этой серии являются световые барьеры и сканеры для контроля зоны безопасности. Они незаменимы для приложений, где есть прессы, станки, обрабатывающие центры и другое машиностроительное оборудование.

Эти устройства также сертифицированы вплоть до SIL 3 и имеют возможность настройки на определенные условия эксплуатации такие, как число нарушений зоны до срабатывания, настройка зон нечувствительности, времени прохождения сигнала и т. д (рис. 6).

Лазерные сканеры представляют собой еще более интеллектуальные устройства для контроля доступа в опасную зону (рис. 7). Они имеют функцию обучения и могут быть подключены как к Failsafe входам/выходам, так и полевым сетям PROFIBUS и AS-интерфейсам с профилями безопасности.


Рис. 5

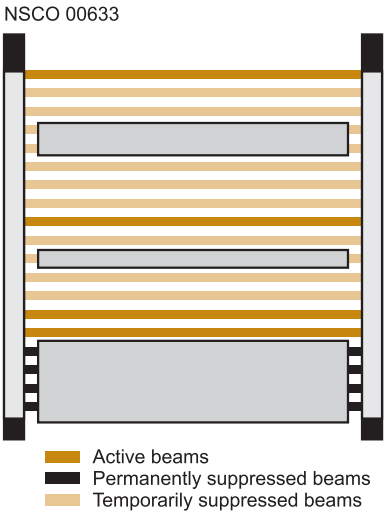

Рис. 6

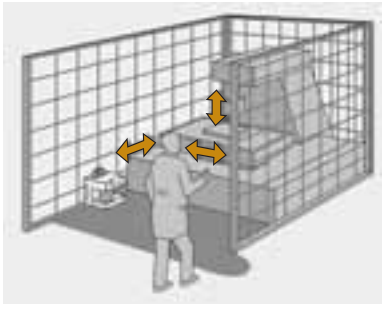
Рис. 7

Надежность или безопасность?

Очень часто при построении систем ПАЗ на вопрос "какой структуры она должна быть?", следует ответ – дублированной, что в принципе, опять же, соответствует правилам. И повсеместно в России на крупные установки ставят в качестве ПАЗ контроллеры с "горячим" резервом. И здесь допускается серьезная ошибка, ведь контроллеры повышенной надежности (дублированные системы) имеют задачу обратную системам повышенной безопасности (ПАЗ системам). Задача дублированного контроллера – не дать остановиться процессу, задача системы ПАЗ наоборот – остановить процесс в случае ошибки. И для отслеживания этих ошибок применяются специальные методы, и на них дается сертификат, тогда как даже в обычных дублированных системах их нет. Подчеркнем, что максимально допустимый уровень безопасности SIL для сертифицированной электронной Failsafe системы равен 3 (SIL 4 не достигается электронными средствами), тогда как даже 100% дублированный контроллер не может подняться выше SIL 1.

Если поставить стандартный дублированный контроллер в качестве системы ПАЗ, возникает вопрос, как гарантировать достоверность входных Failsafe сигналов, переход выходных Failsafe сигналов в безопасное состояние при возникновении аварии, корректность написания программы ПАЗ и ее сопровождение? Все эти вопросы остаются за рамками стандартного и даже дублированного котроллера и часто остаются на совести програм-

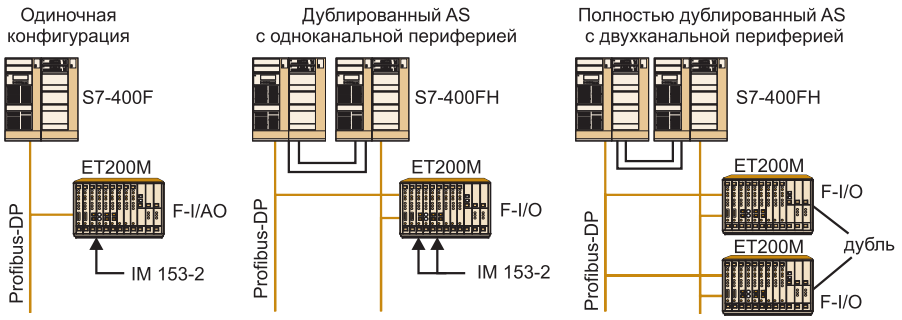

Рис. 8

миста-разработчика. Дублированный контроллер просто переключается на резервный компонент при отказе основного, но не более того. Он надежен, но небезопасен.

Теперь рассмотрим три варианта Failsafe систем автоматизации (AS) на рис. 8.

Все три варианта могут обеспечить уровень безопасности вплоть до SIL 3. Даже вариант 1 с одним процессором и с одинарной периферией удовлетворяет этому требованию за счет механизмов безопасности, описанных выше. Это сертифицированное Failsafe решение и вариант 1 безопасен. Но что произойдет в случае отказа ЦПУ? Функции ПАЗ будут выполнены за счет Failsafe сигнальных модулей: все выходы будут переведены в безопасное положение, то есть возможная аварийная ситуация не получит развития. Именно возможная, потому что технологические параметры в момент поломки могли находиться в норме, и останов процесса технологически не был необходим. Но Failsafe система его все равно выполнила для предотвращения возможной аварии: вариант 1 безопасен, но не надежен. Именно для предотвращения ложных срабатываний применяются варианты 2 и 3, где отказ одного Failsafe компонента парируется переключением на резервный компонент с сохранением уровня безопасности. И только наступление реального случая ПАЗ, нажатия кнопки аварийной остановки, нарушение технологических параметров безопасности (давления, температуры и т. д.) гарантированно приведет к выполнению безопасного останова. Такие системы и надежны, и безопасны.

Надежность и безопасность – абсолютно разные вещи и не стоит путать их на реальном производстве. Поэтому, при построении систем ПАЗ надо четко отдавать себе отчет в том, что вы хотите получить в конце концов, какую функцию и какие задачи должна выполнять ваша система безопасности.

Михайлин Сергей Александрович *– руководитель технической группы отдела A&D AS ООО "Сименс".*

Контактный телефон (095) 737-24-31.

E-mail: sergej.michajlin@siemens.com Http:// www.simatic.ru www.siemens.com/safety

"Желтые" модули противоаварийной защиты работают по промышленной шине

Компания Beckhoff

Представлена система модулей безопасности ввода/вывода TwinSAFE, описан состав системы, технические характеристики и варианты использования. Представлена концепция защиты данных, передаваемых по системе промышленных шин, на основе технологии PROFIsafe. Описываются перспективные разработки компании Beckhoff.

Технология промышленных шин дает пользователям преимущества практически во всех приложениях автоматизации. Объем электропроводки сократился, и устройства и системы стали меньше по размеру и более модульными. Новые методы и компоненты дают дополнительный потенциал усовершенствованию. Неиспользуемые ранее преимущества промышленных шин в технологии обеспечения безопасности привлекают к себе все большее внимание.

Подключение устройств аварийного отключения, световых экранов и других элементов, обеспечивающих безопасность работы устройств и персонала, сейчас занимает значительную часть свободного места в кабельных каналах связи и шкафах управления. Настало время передавать сигналы, относящиеся к обеспечению безопасности, с помощью технологии промышленных шин. Технически это уже стало возможно раньше, но проблема заключалась в отсутствии открытого интерфейса, независимого от изготовителя, с сертификатом, гарантирующим соответствующую безопасность.

Объединение технологии обеспечения безопасности и системы модулей ввода/вывода Beckhoff позволило использовать преимущества промышленных шин в системах ПАЗ. Новая система модулей ввода/вывода TwinSAFE совместима с технологией PROFIsafe и может работать в автономном режиме или вместе с отказобезопасным устройством управления.

Структурный комплект ввода/вывода "безопасно" расширен

Объединение оборудования защиты и ввода/вывода в системе модулей ввода/вывода Beckhoff дает пользователю дополнительные преимущества. Общая стоимость этого решения с точки зрения компонентов, сборочных работ и работ по проектированию минимизирована. Уменьшенное число интерфейсов делает систему более простой для понимания и упрощает доступ ко всей информации, имеющей отношение к защите.

Приложения, автоматизированные с помощью TwinSAFE, предлагают возможности диагностики зна-