

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 предот-

вращения 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.

Теперь рассмотрим три варианта Failsafe систем автоматизации (АС) 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,

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

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.

Объединение технологий 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 отказо-безопасным устройством управления.

Структурный комплект ввода/вывода "безопасно" расширен

Объединение оборудования защиты и 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-

чительно более высокой степени и сокращают время простоя. Пользователю надо знать только одну систему – TwinSAFE, а не многочисленные защитные системы.

Компания Beckhoff предлагает возможность очень простого расширения проверенной системы модулей ввода/вывода с помощью защитных модулей ввода/вывода, полностью заменяя, таким образом, разводку защитных цепей. Сигналы "защиты" могут сочетаться с обычными сигналами без ограничения. При этом экономятся затраты на проектирование, установку и материалы.

Техническое обслуживание значительно упрощается благодаря ускоренной диагностике и простой замене всего нескольких компонентов. Новая система модулей ввода/вывода TwinSAFE включает только три основных функциональных устройства: терминалы дискретного ввода KL19xx и вывода KL29xx, устройство связи (логический терминал) KL6900. Таким образом, обеспечивается связь всех общих защитных датчиков и исполнительных механизмов, например, аварийного выключателя, защитной блокировки, переключателей позиционного, двуручного и с кабельным приводом, световой завесы, светового экрана, лазерного сканера и т.д., а также исполнительных механизмов таких, как контактор, защитный дверной выключатель с тумблером, сигнальная лампа или сервоусилитель.

#### Концепция защиты на базе PROFIsafe

Модули ввода/вывода TwinSAFE основаны на новом стандарте PROFIsafe и вместе с отказоустойчивым устройством управления, совместимым с PROFIsafe, могут использоваться в приложениях различной сложности. Организация пользователей Profibus (Profibus User Organization) создала "профиль" для безопасной передачи данных в PROFIsafe, позволяющий защитным устройствам работать в рамках сети Profibus. Для кабеля или проводки шины RS-485 не требуется никаких изменений. В проекте используется одна система промышленных шин для задач автоматизации, относящихся и не относящихся к защите. PROFIsafe может использоваться для задач, удовлетворяющих стандартам безопасности вплоть до SIL3 (Safety Integrity Level – уровень безопасной сохранности) IEC 61508, кат. 4 EN 954 или DIN V 19251 AK 6. На данный момент разработаны механизмы защиты данных от следующих типов ошибок: повторение, потеря, вставка, неправильная последовательность, искажение данных пользователя, задержка, соединение данных, относящихся и не относящихся к защите, и неправильная адресация.

PROFIsafe предлагает последовательную нумерацию защитных блоков данных. Время связи контролируется ведущим и ведомым устройствами, связь защищена паролем. Для защиты целостности данных PROFIsafe использует 16/32 битный CRC (cyclic redundancy check – циклический избыточностный контроль). В одном блоке данных может быть передано максимум 12/122 байт (16/32 битный CRC) надежных данных. В соответствии с технологией PROFIsafe передает не только данные пользователя, но и байт состояния или управляющий

байт. Состояние партнера связи и канала передачи данных проверяется для каждого блока данных с помощью счетчика надежности (последовательное число).

#### Независимое от промышленных шин решение

Механизмы, используемые в рамках PROFIsafe, защищают данные внутри кадра данных от возможных воздействий со стороны тракта передачи данных. С точки зрения системы шин PROFIsafe представляет собой небольшой блок данных, который необходимо когерентно и безошибочно перенести, что является не очень сложной задачей для промышленной шины. Внедрение безопасной упаковки данных означает, что безопасные данные доступны любой шине. Единственное условие заключается в том, что для системы шин имеется соответствующий контроллер узла шины. Возможность передавать данные PROFIsafe по целому ряду систем шин одновременно очень полезна для пользователей. Таким образом, можно обмениваться "безопасными данными" за пределами различных контроллеров и систем.

#### Функциональные возможности отказоустойчивого ПЛК в модулях ввода/вывода

В настоящее время решение обеспечения безопасности с помощью одного или более реле блокировки (т.н. релейная защита) становится дорогим в связи с очень ограниченными возможностями логического сочетания сигналов. Классический контроллер защит экономит пространство и упрощает сборку, но может дорого стоить из-за необходимости организовывать отдельный интерфейс для управления контроллером защит и отображения его состояния. Интерфейс, способный предоставлять информацию о состоянии контроллера защит, состоит обычно из нескольких дискретных сигнальных контактов, являющихся дополнительной проводкой. Использование интерфейса промышленных шин требует дополнительных усилий при параметризации сети.

Система модулей ввода/вывода TwinSAFE работает вместе с контроллерами защит, совместимыми с PROFIsafe. В небольших и средних приложениях безопасные модули ввода/вывода данных работают на "незащищенном" контроллере, но при наличии устройства связи KL6900 TwinSAFE. ПЛК более высокого уровня (CX1000 Embedded PC, контроллеры узла промышленной шины серии BC или BX) при непосредственном соединении с терминалами защит TwinSAFE могут служить в качестве контроллера. Логический терминал KL6900 – это устройство связи между терминалами цифрового безопасного ввода/вывода, обеспечивающее простое, гибкое и экономически эффективное управление более чем с 64 каналами. С этой целью необходимые функции логической безопасности для связи вводов/выводов данных внедряются в виде функционального блока и параметризуются в зависимости от области применения. Для небольших конфигураций задачи противоаварийного ПЛК могут, таким образом, выполняться в рамках системы промышленных шин. Больше не требуется дополнительных затрат на интерфейс с

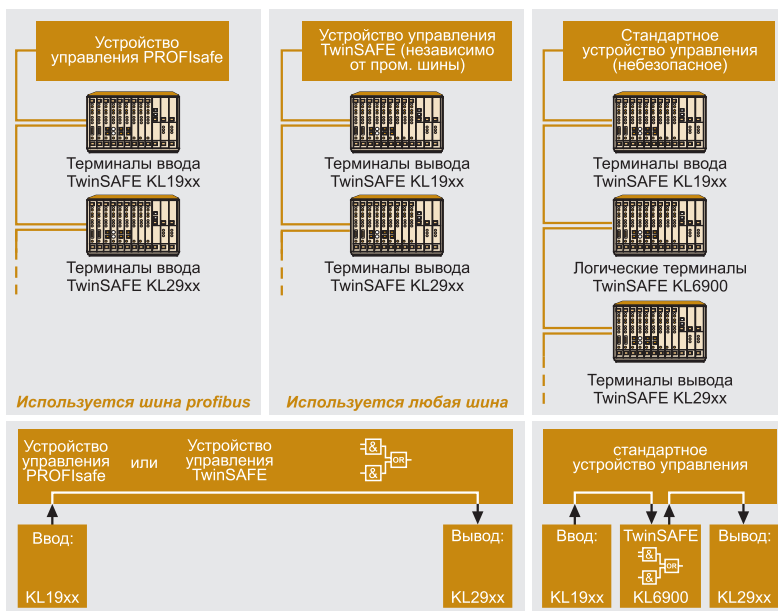


Рис. 1. Три схемы использования модулей TwinSAFE

ПЛК. В общем случае доступны все режимы контроллера защит. KL6900 подходит к приложениям вплоть до SIL3 в соответствии с IEC 61508 или EN 954 кат. 4 и DIN V 19251 AK6.

Логическая схема TwinSAFE легко параметризуется через контроллер узла шины или промышленную шину. Для ПК в качестве инструмента имеется системный администратор TwinCAT. Независимо от TwinCAT, KL6900 может конфигурироваться через контроллер узла шины с помощью ПО конфигурации KS2000. Выбранные параметры запоминаются в терминале и защищаются от перерывов в подаче питания или искажения. Доступ защищен паролем. Эксплуатация возможна только в безопасном состоянии без помех.

С помощью модулей ввода/вывода Beckhoff и на базе PROFIsafe пользователи теперь могут при большей экономической выгоде для себя устанавливать и эксплуатировать сети комплексной автоматизации, включая приложения, относящиеся к безопасности. Система TwinSAFE предлагает аппаратные средства и ПО открытого стандарта для защитных технологий.

#### Перспективные разработки

Модуль защитной логики KL6900 привносит новый уровень качества в область обработки сигнала: это больше, чем реле и меньше, чем "противоаварийный ПЛК". KL6900 имеет не более 64 каналов для того, чтобы удовлетворять стоимости небольших и простых приложений. Число каналов можно увеличить с помощью объединения нескольких KL6900. Различные комбинации использования защитной логики системы модулей TwinSAFE предоставляют возможность оптимальным

образом решать поставленную техническую задачу (рис. 1). В существующих модулях TwinSAFE производится комплексная обработка сигнала и выдерживается время обратной связи меньше 50 мс.

В ближайшее время компания Beckhoff предложит быстрый "противоаварийный ПЛК". Общее время обратной связи системы, составляющее 2 мс, и время связи, равное 100 мс, для команд размером в 1 Кбайт – это рабочие характеристики, к которым мы стремимся. "Безопасный" ПЛК находится в стадии разработки, как и ступенчатый принцип подключения к плате с электронной схемой устройства промышленных шин в семействе CX1000 Embedded PC. Программирование выполняется в IEC 61131-3. Связь с "небезопасной" частью ПЛК осуществляется системой автоматически. С точки

зрения пользователя безопасные сигналы просто являются "безопасными переменными", которые объединяются в программу в любом месте.

#### Дискретные модули ввода/вывода

Модули ввода/вывода KL1904 и KL1908 TwinSAFE представляют собой устройства дискретного ввода с четырьмя и восемь отказоустойчивыми каналами соответственно (рис. 2). При двухканальной связи терминалы отвечают требованиям IEC 61508 SIL3 и EN 954 кат. 4 или DIN V 19251 AK6.

Модуль ввода/вывода KL2904 TwinSAFE – дискретный терминал вывода с четырьмя каналами, удовлетворяющий стандартам безопасности SIL3 в соответствии с IEC 61508 или EN 954 кат. 4 и DIN V 19251 AK6. Он коммутирует исполнительные механизмы, рассчитанные на  $\approx 24$  В при силе тока до 2 А. Если модуль ввода/вывода обнаружит ошибку, он автоматически выключится.

Модуль ввода/вывода KL2901 TwinSAFE – это терминал подачи потенциала с встроенным выключением источника питания, который может быть размещен в любом месте между терминалами модулей ввода/вывода. Потенциал передается последующему модулю ввода/вывода через силовые контакты. Это обеспечивает реализацию отдельных групп потенциала в блоке шин. KL2901 связан с отказоустойчивым устройством управления через протокол PROFIsafe и может быть выключен отказоустойчивым устройством управления более высокого уровня. Выключение также происходит, если терминал обнаруживает внутреннюю ошибку.

Модуль ввода/вывода KL2901 TwinSAFE – это терминал подачи потенциала с встроенным выключением источника питания, который может быть размещен в любом месте между терминалами модулей ввода/вывода. Потенциал передается последующему модулю ввода/вывода через силовые контакты. Это обеспечивает реализацию отдельных групп потенциала в блоке шин. KL2901 связан с отказоустойчивым устройством управления через протокол PROFIsafe и может быть выключен отказоустойчивым устройством управления более высокого уровня. Выключение также происходит, если терминал обнаруживает внутреннюю ошибку.

Контактный телефон компании Beckhoff (095)980-80-15.  
E-mail: info@beckhoff.com.ru Http://www.beckhoff.com.ru

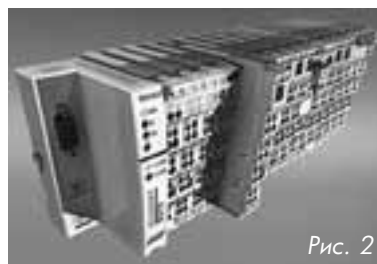


Рис. 2