Решение проблемы безопасности с помощью технологии EtherCAT

Компания Beckhoff

Современные коммуникационные системы обеспечивают не только детерминированную передачу данных управления, но и позволяют передавать в той же среде данные, связанные с технической безопасностью. При использовании технологии EtherCAT эта задача решается путем создания протокола Safety over EtherCAT (обеспечение безопасности в среде EtherCAT).

До недавнего времени стандартной считалась ситуация, когда меры по технической безопасности оборудования разрабатывались в отрыве от создания автоматизированного управления и интегрировались в концепцию машины на более поздней стадии. Это часто приводило к громоздким и негибким решениям, которые иногда могли ограничить эксплуатационные характеристики машины, и тогда возникал риск, что пользователь захочет обойти эти меры, тем самым, сделав их неэффективными и потерявшими смысл.

Элементы аппаратуры обеспечения безопасности, такие как защитная световая завеса, устройства контроля защитной двери, двуручные органы управления обычно контролируются посредством ряда анализирующих устройств, которые сами оказывают влияние на выходные сигналы через неадаптивное логическое реле. Вспомогательные провода питания и/или контакторы с электродвигательным приводом устанавливаются внутри вала привода таким образом, чтобы можно было в любой момент предотвратить опасное движение.

В настоящее время развитие идет в новом направлении: решения по обеспечению безопасности с использованием микропроцессорной техники в системах автоматизированного управления и коммуникационных системах обеспечивают интеграцию системы технической безопасности с конструкцией машины. Что касается датчиков системы безопасности, то они становятся предохранительными устройствами со встроенными функциональными возможностями, такими как бесшумная настройка.

Из последних достижений следует отметить создание сенсорных систем пространственного контроля с использованием видеокамер, предоставляющих новые возможности по взаимодействию оператор/машина при обеспечении безопасности в определенных зонах. Для выполнения аналитических функций и построения предохранительных логических схем (в дополнение к "большим" контроллерам системы безопасности) уже предлагаются локальные логические устройства малого размера, способные решать соответствующие задачи. Неадаптивное логическое реле уходит в прошлое. В области технологии обеспечения безопасности приводов также предлагается использование встроенной предохранительной аппаратуры для быстрой остановки привода и для автоматического контроля рабочих параметров (например, безопасной скорости).

Одним из факторов, обеспечивающих возможность такого типа интеграции, является надежная коммуникационная связь между компонентами системы. Современные достижения в области науки и техники стали основной предпосылкой для создания международных стандартов, определяющих уровень надежности для программируемых предохранительных устройств (см. документы IEC 61508, IEC 62061, ISO 13849).

Обеспечение безопасности в среде EtherCAT

С целью обеспечения передачи данных по безопасности по системе промышленной шины EtherCAT подразделением EtherCAT Technology Groupe (ETG) был создан протокол Safety over EtherCAT. При разработке протокола принципиальным являлось обеспечение следующих требований:

- соответствие разделу SIL 3 международного стандарта IEC 61508;
- единая коммуникационная система передача информации любого типа (в том числе по безопасности);
- независимость протокола от системы транспортировки и используемой среды передачи данных;
- отсутствие в протоколе ограничений на длину данных по безопасности;
- возможность работы с информационными кадрами очень короткой длины;
- отсутствие ограничений по скорости передачи и длительности цикла.

Соответствие требованиям стандарта IEC 61508 SIL 3 важно для широкого использования протокола в области промышленной автоматизации. Для промышленных шин это означает, что вероятность появления необнаруженных ошибок должна быть $<10^{-9}$ 1/час. Это соответствует 1% от значения коэффициента необнаруженных ошибок, величина которого в соответствии с требованиями SIL 3 должна быть $\geq 10^{-8}$ и $<10^{-7}$. Остальные 99% приходятся на другие компоненты системы безопасности: датчики, предохранительные логические устройства, приводы. В частности, такая вероятность появления необнаруженных ошибок означает, что не должно произойти ни одной незамеченной ошибки при продолжительной эксплуатации в течение 105 лет.

Система промышленной шины EtherCAT используется как одноканальная коммуникационная система для передачи информации по безопасности и прочей информации. Среда передачи данных считается "черным каналом" и не учитывается при оценке степени безопасности. Кадр с информацией по безопасности, содержащий данные процесса обеспечения безопасности и необходимые возвратные данные, включен в процесс обработки данных EtherCAT. Этот "контейнер" надежно анализируется в устройствах на прикладном уровне. Связь остается одноканальной, что находится в соот-

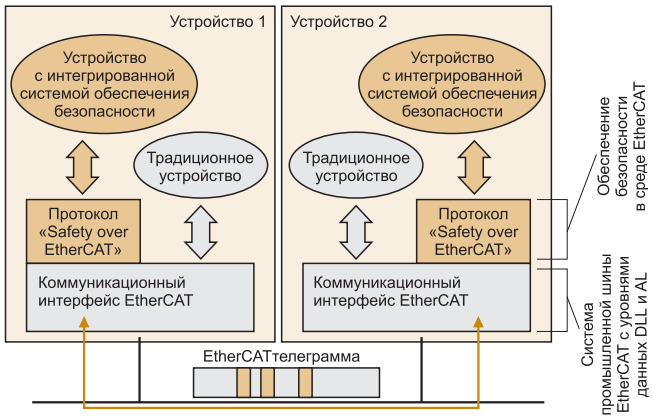

Рис. 1

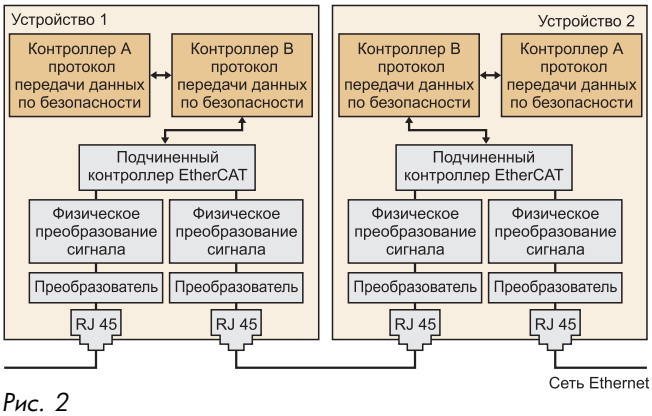

Рис. 2

ветствии с моделью A из приложения к стандарту pre-IEC 61784-3. В этом стандарте, вступившем в настоящее время в силу, определены требования по передаче сообщений в промышленных сетях, связанных с безопасностью работы. Оценка вероятности появления необнаруженных ошибок для протокола Safety over EtherCAT не зависит от механизма определения ошибок коммуникационной системы. Поэтому данный протокол может передаваться также через другие коммуникационные системы. Это свойство используется, например, во внутренних системах с субшиной для модульных компонентов системы ввода/вывода. Шинный соединитель EtherCAT может без ограничений переправлять кадр с информацией по безопасности к терминалам ввода/вывода, участвующим в передаче информации о безопасности, через субшину.

На рис. 1 и 2 представлена программная и аппаратная структуры обеспечения безопасности в среде EtherCAT.

Описание технологии протокола Safety over EtherCAT

Основные принципы тестирования и сертификации шинных систем, использующихся для передачи сообщений, связанных с безопасностью работы, впервые были представлены рабочей группой по электронной инженерии HVBG (HVBG electrical engineering committee) в 2000 г. Базовые принципы тестирования, определенные в последнем варианте (GS-ET-26), легли в основу международного стандарта pre-IEC 61784-3. В нем приведен перечень возможных для такого типа сетей ошибок: искажение данных, повторение, ошибки при обмене данными, выпадение данных, задержка поступления данных, ошибки ввода, нелегальное проникновение и неверная адресация сообщений. Протокол обеспечения безопасности должен справиться со всеми этими ошибками с помощью подходящих приемов, то есть они должны быть детектированы в соответствии с требуемой категорией безопасности. Задержка поступления сообщений – характерная особенность систем, использующих Ethernet-технологию. Использование не прошедших сертификацию на безопасность работы компонентов инфраструктуры, таких как переключатели или маршрутизаторы, приводит к возможности возникновения задержек сообщений. Даже контроль времени (сторожевой таймер) прибытия сообщений не играет существенной роли.

На рис. 3 показан процесс связи между источником и получателем сообщений. Получатель контролирует циклическое поступление сообщений от источника с помощью сторожевого таймера. На каждом цикле сообщения задерживаются в компоненте системы на величину Δ, которая не обнаруживается сторожевым таймером. При накоплении задержки за несколько циклов получатель не может больше определить, что сообщение недопустимо устарело. В худшем случае, это может привести к тому, что аварийный сигнал остановки от датчика (источника) поступит на привод (получателю) только через несколько минут.

Одним из способов избежать подобного рода ошибок является использование единого общего времени и постановка на сообщениях временных меток. Следует отметить, что использование механизма временной синхронизации, уже присутствующего в коммуникационной системе, не всегда возможно. Синхронизация должна дополнительно быть привязана к протоколу обеспечения безопасности.

В связи с этим в протоколе Safety over EtherCAT используется более простой метод (рис. 4). Уникальная связь между двумя устройствами (главное/подчиненное) и наличие протокола Safety over EtherCAT обеспе-

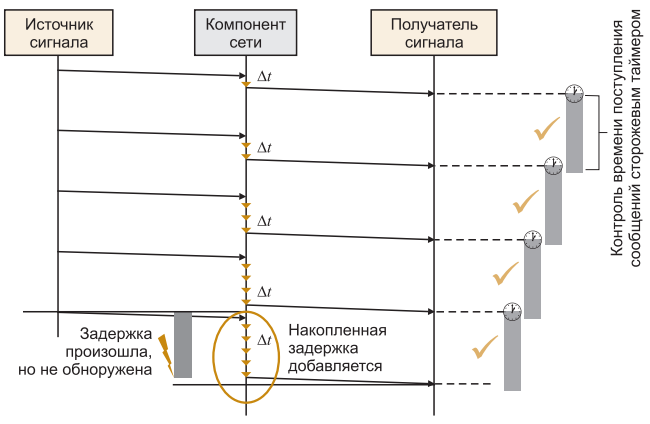

Рис. 3

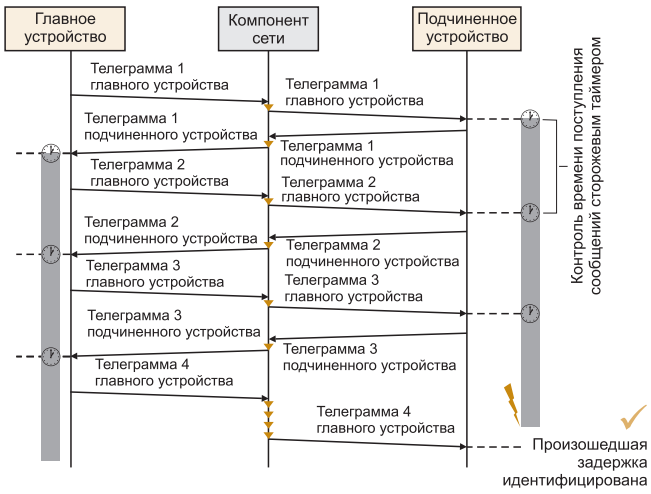

Рис. 4

чивают такой алгоритм работы, при котором каждое из устройств посылает свое новое ответное сообщение, как только само получит новое. Весь путь передачи данных между главным и подчиненным устройствами, таким образом, контролируется на каждом цикле, и накопление задержки либо отсутствует, либо детектируется. Это обеспечивает ра циональную реализацию протокола и умеренность требований по подключению к коммуникационной системе, поскольку отсутствуют жесткие нормы по обеспечению временной синхронизации. Тот факт, что это может привести к увеличению трафика в сети, не является критичным из-за достаточной ширины полосы пропускания и практически не является недостатком.

Для контроля за ошибками других типов в протоколе предусмотрены следующие меры:

• номер сеанса связи (для определения буферизации общей последовательности запуска);

• уникальный идентификационный номер соединения и уникальный адрес подчиненного устройства (для надежного детектирования неверно адресованных сообщений с помощью уникальной адресной системы);

• контрольная сумма CRC (для определения ошибок передачи от источника к получателю). Кроме того, эта мера обеспечивает возможность определения ошибок обмена данными внутри контейнера, например, если контейнер повредился по пути. Оцениваются правильность и соответствие кода и требуемая независимость от подчиненной связи;

• номер последовательности (для определения ошибок обмена данными, повторения, ввода или выпадения данных всего сообщения).

С помощью определенных приемов кадр формируется таким образом, что минимальной длины контейнера в 6 байт становится достаточно для передачи всей информации по детектированию и коррекции ошибок, включая один байт на запись данных по безопасности. В частности, протокол не налагает никаких ограничений на длину данных по безопасности. Это означает, что компоненты, оборудованные встроенными элементами системы безопасности с большим количеством снимаемых данных по безопасности, также поддерживаются. Например, в дополнение к информации о безопасном состоянии предохранительные устройства также могут передавать информацию о безопасном положении, скорости и/или крутящем моменте. Не существует ограничений по минимальному времени цикла для контейнера. При правильном выборе метода детектирования ошибок и корректировки информации скорость передачи данных не влияет на вероятность появления необнаруженных ошибок при использовании протокола Safety over EtherCAT.

При запуске системы с протоколом Safety over EtherCAT как главные, так и подчиненные устройства системы проходят ряд состояний (рис. 5). И здесь, чтобы добиться как можно большей простоты реализации, упор был сделан на простоту структуры. Смена состояний инициируется главным устройством и подтверждается подчиненным. Состояние также определяет возможность изменения и проверки информации для установления взаимосвязи. Настройка сторожевого таймера, например, меняется в состоянии "Параметр". Это время находится в жесткой зависимости от канала связи и от устройств системы безопасности, поэтому должно настраиваться отдельно. Параметры системы безопасности также могут быть переданы от главного устройства к подчиненному на этом этапе. Это приводит в рабочее состояние центральную систему управления данными по безопасности главного устройства. Параметры аппаратуры могут иметь длину до 216 байт на соединение, что достаточно для передачи, например, сконфигурированного защитного поля лазерного сканера.

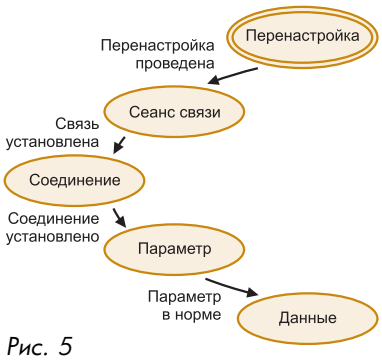

Рис. 5

Выйти из состояния передачи данных по безопасности можно только на этапе "Данные". Это обычное рабочее состояние, в котором происходит обмен данными по безопасности. Если одно из устройств детектирует во время запуска системы наличие коммуникационной ошибки или ошибки обмена данными, оно переходит в состояние "Перенастройка", тем самым возобновляя соединение. На рис. 6 показана упаковка кадра протокола Safety over EtherCAT в систему передачи данных EtherCAT.

Сертификация

Протокол Safety over EtherCAT был проверен Германским агентством по техническому контролю (German Technical Inspection Agency (TÜV)). Он сертифицирован как протокол обмена данными между

Свобода выбора коммуникационных стандартов опасна, но только она обеспечивает нам безопасность.

Журнал "Автоматизация в промышленности"

поддерживающими этот протокол устройствами, соответствующими требованиям SIL 3 стандарта IEC 61508. При реализации протокола Safety over EtherCAT в устройстве должны быть соблюдены условия критерия безопасности. При этом должны учитываться специальные требования к устройству.

Могут использоваться любые каналы связи: системы полевых шин, Ethernet или сходные линии связи, оптоволоконные кабели, медные провода или радиоканалы. Нет никаких ограничений для шинных соединителей и прочих устройств, располагаемых на линии передачи.

В настоящее время разрабатывается процедура проверки возможности реализации протокола в устройствах. Этот тест служит для проверки прохождения протокола Safety over EtherCAT через коммуникационный интерфейс испытательного устройства (тест с использованием "черного ящика").

На первом этапе происходит считывание файла описания испытательного устройства для определения вероятных параметров тестирования. Полученные в результате конфигурирования тестовые сценарии можно затем запустить на стандартном компьютере. На испытательное устройство подаются правильные и дефектные кадры, после чего полученный отклик сравнивается с ожидаемой реакцией. Результаты отдельных этапов тестирования объединяются в тестовом отчете.

Совокупность данных тестирования анализируется, результаты утверждаются испытательным центром и могут быть использованы производителем устройств для подтверждения соответствия требованиям протокола. Предполагается создание независимой лаборатории по испытаниям на соответствие. Сертифицирующий орган производителя устройства, таким образом, может подтвердить возможность использования этого протокола для обеспечения безопасной работы. Однако прохождение теста не гарантирует возможность реализации протокола Safety over EtherCAT (например, при двухканальной обработке). Что касается оборудования со встроенными устройствами обеспечения безопасности, это должно быть сделано производителем в соответствии с требованиями по безопасности сертифицирующего органа.

Пример использования

Надежность и функциональность протокола передачи данных по безопасности может быть подтверждена только при реализации технических характеристик на практике. Устройства для реализации протокола Safety over EtherCAT стали доступны с 2005 г. Поэтому Safety over EtherCAT – один из первых протоколов передачи данных по безопасности, поддерживаемых промышленными коммуникационными Ethernet-системами PB.

Рассмотрим пример использования системы TwinSAFE с протоколом Safety over EtherCAT (рис. 7). Компоненты системы обеспечения безопасности размещаются в любом требуемом месте автоматизированной системы. В системе могут использоваться расширяемые локальные компоненты системы ввода/вывода. Дополнительные элементы системы ввода/вывода могут быть легко введены в систему путем гибкого использования шинных соединителей системы безопасности и соединителей, не относящихся к таковой.

Предохранительная логическая схема также внедрена в конструкцию сети. Таким образом, стандартный контроллер может продолжать выполнение задач по управлению без использования расширения, касающегося обеспечения безопасности. Функции по получению и пересылке данных по обеспечению безопасности сосредоточены в локальной предохранительной логической схеме, представляющей собой

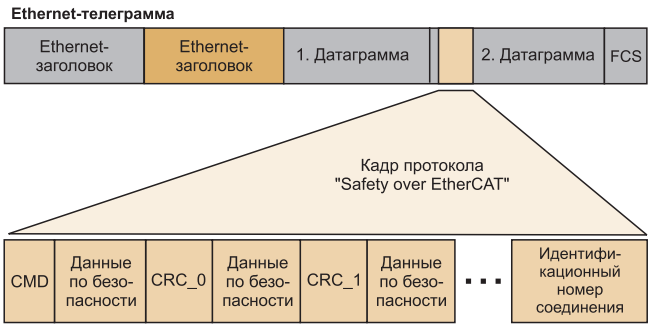

Рис. 6

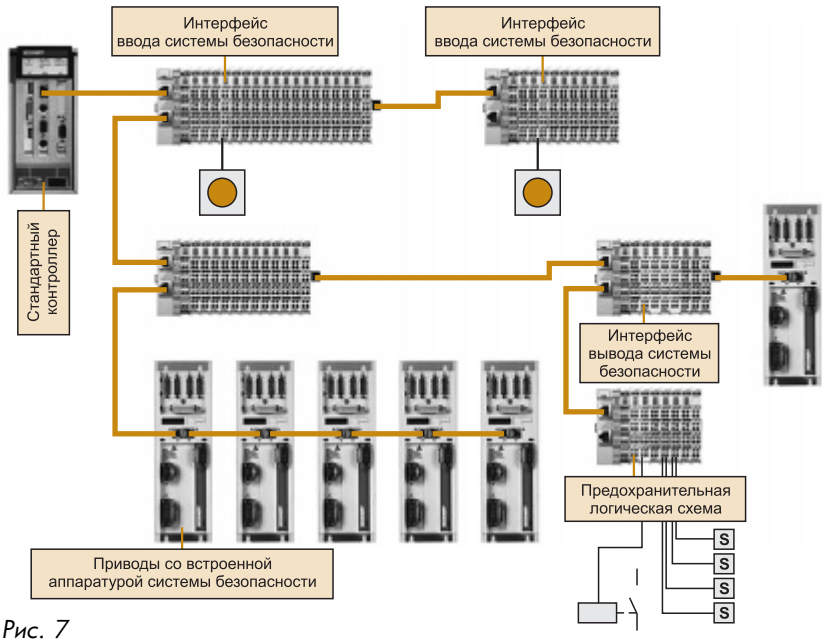

Рис. 7

интеллектуальный шинный терминал системы обеспечения безопасности. Это позволяет уменьшить расходы за счет отказа от использования специального дорогостоящего контроллера системы безопасности и обеспечивает возможность масштабирования логики при необходимости. Через стандартный контроллер проходят только сообщения между главным и подчиненными устройствами, взаимодействующими с помощью протокола Safety over EtherCAT.

В настоящее время Beckhoff предлагает три вида устройств ввода/вывода для системы обеспечения безопасности: терминал ввода с четырьмя вводами системы безопасности, терминал вывода с четырьмя выводами системы безопасности и логический терминал с конфигурируемой предохранительной логической схемой и четырьмя выводами системы безопасности. Задание связанных с обеспечением безопасности параметров устройств может быть осуществлено с помощью встроенного в стандартное ПО (TwinCAT) инструмента для конфигурации системы обеспечения безопасности. В итоге, определенный набор параметров по безопасности загружается (с использованием пароля) в логический терминал системы безопасности. Во время каждого запуска логический терминал распределяет данные по безопасности по сконфигурированным терминалам ввода и вывода. Это обеспечивает простоту обмена данными между терминалами ввода/вывода без дополнительной подстройки или перезагрузки конфигурации.

Заключение

Таким образом, рассмотрен протокол передачи данных по безопасности по системе промышленной шины EtherCAT – Safety over EtherCAT, не имеющий ограничений по длине данных по безопасности, среде и скорости передачи данных. В новом протоколе EtherCAT используется как "черный канал", то есть коммуникационная система не оказывает влияние на оценку степени безопасности. Протокол соответствует техническим условиям и требованиям стандарта IEC 61508 SIL3. Устройства для реализации протокола Safety over EtherCAT стали доступны с 2005 г.

Контактный телефон (495) 411-88-82.
E-mail: info@beckhoff.ru Http:// www.beckhoff.ru

SIMATIC NET Industrial Ethernet

С.Ю. Кухаренко (ООО "Сименс")

Представлено решение SIMATIC NET от компании Siemens для построения стандартных Ethernet сетей, включающее: шинную систему с пассивными и активными сетевыми компонентами; интерфейсы для подключения систем управления к шинной системе; сетевые переходы; ПО для конфигурирования сетей; инструменты для обслуживания и диагностики.

С момента своего создания в 80-х годах Ethernet, каким мы знаем его сегодня, прошел через несколько этапов обновления. Его исключительное положение на мировом рынке, как основного стандарта для офисных сетей, делает в настоящее время невозможным представить без него само существование компьютерной техники. Сегодня Ethernet – сеть номер один в мире, занимающая более 95% рынка и показывающая устойчивые темпы роста.

Практически с момента становления Ethernet фирма Siemens выбрала его как один из стандартов для своих промышленных сетей. Интенсивные предварительные исследования, расширение стандарта унифицированной концепцией экранирования и заземления, разработка специальных протоколов дали возможность использования Ethernet в промышленных условиях. В этой первой промышленной версии с 1985 г. шинная система Ethernet стала известна под названием SINEC H1, развившись в настоящее время в концепцию SIMATIC NET Industrial Ethernet.

Необходимо сразу отметить, что изначально разработчики фирмы Siemens ставили перед собой задачу полноценного использования международного стандарта IEEE 802.3 (Ethernet), а в дальнейшем IEEE 802.3u и IEE 802.11 a/b/g/h (Wireless LAN) при создании промышленного сетевого оборудования, что дает возможность полноценного использования в сетях Industrial Ethernet наряду со специализированным промышленным оборудованием и офисного, создавая единые информационные инфраструктуры промышленных предприятий, обеспечивая совместную работу программных и аппаратных средств АСУТП, АСУП и систем класса MES.

В настоящий момент SIMATIC NET для Industrial Ethernet предлагает все необходимые сетевые компоненты для построения стандартных Ethernet сетей, которые отвечают жестким промышленным требованиям. Полное решение от SIEMENS включает: шинную систему с пассивными (например, кабелями) и активными сетевыми компонентами (например, коммутаторами); интерфейсы для подключения систем управления к шинной системе (интегрированные интерфейсы, коммуникационные процессоры); сетевые переходы; ПО для конфигурирования сетей; инструменты для обслуживания и диагностики.

Пассивные сетевые компоненты

Пассивные компоненты SIMATIC NET включают электрические и оптические кабели, а также соединительные устройства различного назначения. Для большинства электрических пассивных компонентов поддерживается технология FastConnect, позволяющая выполнять быстрый и безошибочный монтаж сети.

Так кабели IE FC (Fast Connect) 2x2 и 4x2 предназначены для применения в промышленных и офисных ус-