ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61784-3-8— 2016

Промышленные сети

ПРОФИЛИ

Часть 3-8

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 8

(IEC 61784-3-8:2010, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 58 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 30 ноября 2016 г. № 1885-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61784-3-8:2010 «Промышленные сети. Профили. Часть 3-8. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 8» («IEC 61784-3-8:2010 «Industrial communication networks — Profiles — Part 3-8: Functional safety fieldbuses — Additional specifications for CPF 8», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения, обозначения и сокращения 2
3.1 Термины и определения 2
3.2 Обозначения и сокращения 7
3.3 Условные обозначения 8
4 Обзор FSCP 8/1 (CC-Link Safety™) 8
5 Общие положения 8
5.1 Внешние документы, предоставляющие спецификации для профиля 8
5.2 Функциональные требования безопасности 9
5.3 Меры безопасности 9
5.4 Структура коммуникационного уровня безопасности 10
5.5 Связи с FAL (и DLL, PhL) 11
6 Услуги коммуникационного уровня безопасности 11
6.1 Общие положения 11
6.2 Элементы SASE 11
6.3 SAR связи 12
6.4 Данные процесса для элементов ASE связи SAR 13
7 Протокол коммуникационного уровня безопасности 14
7.1 Формат PDU безопасности 14
7.2 Описание состояния 21
8 Управление коммуникационным уровнем безопасности 25
8.1 Общие положения 25
8.2 Установление соединения и подтверждение обработки 25
8.3 Верификация ведомого устройства безопасности 25
9 Системные требования 26
9.1 Индикаторы и коммутаторы 26
9.2 Руководство по установке 27
9.3 Время реакции функции безопасности 27
9.4 Длительность запросов на обслуживание 29
9.5 Ограничения на вычисление системных характеристик 29
9.6 Техническое обслуживание 30
9.7 Руководство по безопасности 31
10 Оценка 31
Приложение А (справочное) Дополнительная информация для удовлетворяющих функциональной безопасности профилей коммуникаций CPF 8 32
Приложение В (справочное) Информация для оценки удовлетворяющих функциональной безопасности профилей коммуникаций CPF 8 33
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 34
Библиография 35

Введение

0.1 Общие положения

Стандарт МЭК 61158, посвященный полевым шинам, вместе с сопутствующими ему стандартами МЭК 61784-1 и МЭК 61784-2 определяет набор протоколов передачи данных, которые позволяют осуществлять распределенное управление автоматизированными приложениями. В настоящее время технология полевых шин считается общепринятой и хорошо себя зарекомендовала. Именно поэтому появляются многочисленные расширения, направленные на еще не стандартизированные области, такие как приложения реального времени, связанные с безопасностью и защитой.

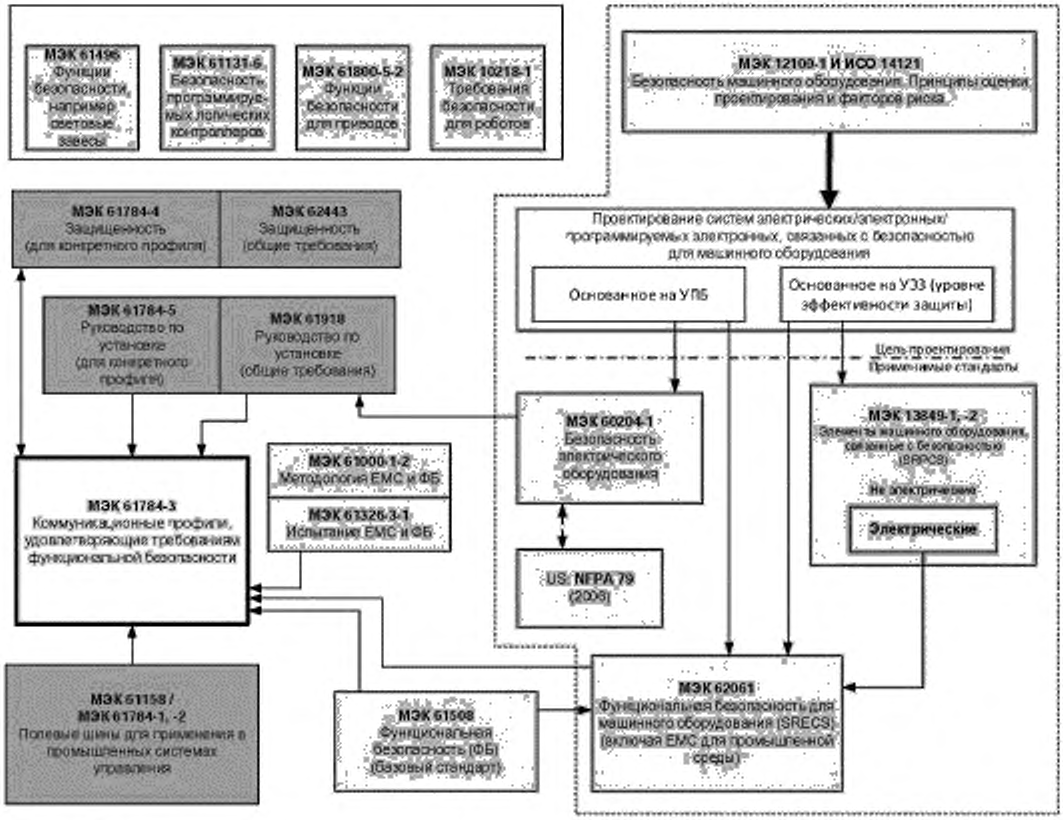
Настоящий стандарт рассматривает важные принципы функциональной безопасности коммуникаций, на основе подхода, представленного в комплексе стандартов МЭК 61508, и определяет несколько коммуникационных уровней безопасности (профилей и соответствующих протоколов) на основе профилей передачи данных и уровней протоколов, описанных в МЭК 61784-1, МЭК 61784-2 и в комплексе стандартов МЭК 61158. Настоящий стандарт не рассматривает вопросы электробезопасности и искробезопасности.

На рисунке 1 представлена связь настоящего стандарта с соответствующими стандартами, посвященными функциональной безопасности и полевым шинам в среде машинного оборудования.

На рисунке 2 представлена связь настоящего стандарта с соответствующими стандартами, посвященным функциональной безопасности и полевым шинам в области промышленных процессов.

Коммуникационные уровни безопасности, реализованные в составе систем, связанных с безопасностью, в соответствии с МЭК 61508, обеспечивают необходимую достоверность при передаче сообщений (информации) между двумя и более участниками, использующими полевые шины в системе, связанной с безопасностью, или же достаточную уверенность в безопасном поведении при возникновении ошибок или отказов в полевой шине.

Коммуникационные уровни безопасности, определенные в настоящем стандарте, обеспечивают уверенность в том, что полевые шины могут использоваться в применениях, требующих обеспечение функциональной безопасности для конкретного уровня полноты функциональной безопасности (УПБ), для которого определен соответствующий ему профиль коммуникации, удовлетворяющий требованиям функциональной безопасности.



Примечание — Подпункты 6.7.6.4 (высокая степень сложности) и 6.7.8.1.6 (низкая степень сложности) МЭК 62061 устанавливает связь между уровнем эффективности защиты (Категорией) и УПБ.

Рисунок 1 — Связь МЭК 61158-3 с другими стандартами (машинное оборудование)

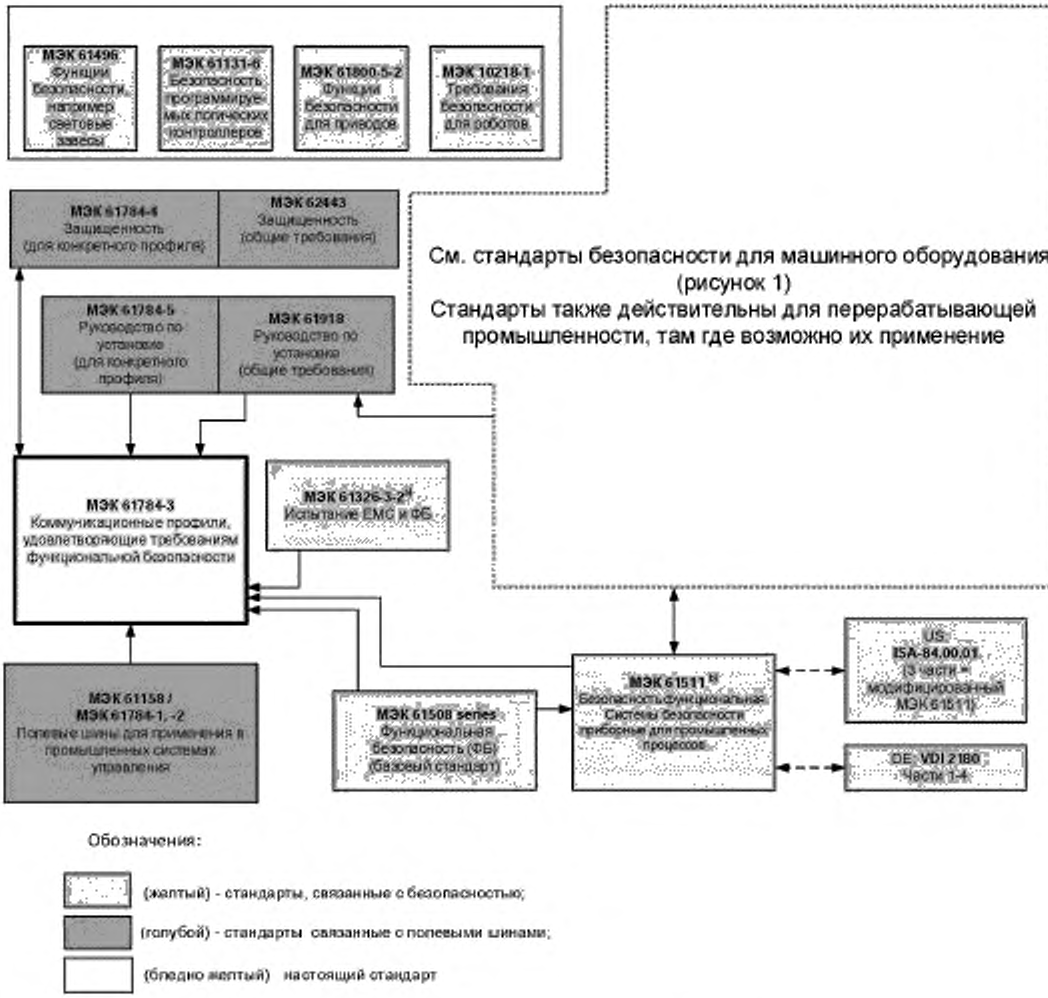


Рисунок 2 — Связь МЭК 61158-3 с другими стандартами (промышленные процессы)

Результирующий УПБ, заявляемый для системы, зависит от реализации выбранного профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, внутри этой системы. Но реализации профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, в стандартном устройстве не достаточно для того, чтобы устройство считалось устройством безопасности.

Настоящий стандарт описывает:

- основные принципы реализации требований комплекса стандартов МЭК 61508 для связанной с безопасностью передачи данных, включая возможные сбои при передаче данных, меры по устранению неисправностей и факторы, влияющие на полноту данных;
- индивидуальные описания профилей, удовлетворяющих требованиям функциональной безопасности, для нескольких семейств профилей передачи данных, представленных в МЭК 61784-1 и МЭК 61784-2;
- расширения уровня безопасности до служб передачи данных и разделов протоколов в стандартах комплекса МЭК 61158.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Промышленные сети

ПРОФИЛИ

Часть 3-8

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 8

Industrial communication networks. Profiles. Part 3-8. Functional safety fieldbuses.
Additional specifications for CPF 8

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт описывает коммуникационный уровень безопасности (услуги и протокол), на основе CPF 8, представленного в МЭК 61784-1и МЭК 61158, Тип 18. Настоящий стандарт идентифицирует принципы для осуществления коммуникаций, удовлетворяющих требованиям функциональной безопасности, определенным в МЭК 61784-3, и имеющих важное значение для данного коммуникационного уровня безопасности.

Примечание — Настоящий стандарт не затрагивает вопросы электробезопасности и искробезопасности. Электробезопасность связана с угрозами, такими как электрический шок. Искробезопасность связана с угрозами, относящимися к возможным взрывам в атмосфере.

Настоящий стандарт определяет механизмы для передачи важных для безопасности сообщений между участниками распределенной сети, использующей технологию полевых шин, в соответствии с требованиями функциональной безопасности, представленными в комплексе МЭК 61508[1)]. Эти механизмы могут широко использоваться в промышленности, например в управление процессом, автоматизации производства и машинном оборудовании.

Настоящий стандарт содержит руководства, как для разработчиков, так и для оценщиков соответствующих приборов и систем.

Примечание — Результирующий УПБ, заявляемый для системы, зависит от реализации выбранного профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, внутри этой системы. Но в соответствии с настоящим стандартом реализации выбранного профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, в стандартном устройстве не достаточно для того, чтобы устройство считалось устройством безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы следующие международные стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных ссылок применяют последнее издание ссылочного стандарта (включая все его изменения).

[1)] Далее в настоящем стандарте используется «МЭК 61508» вместо «комплекс МЭК 61508».

Издание официальное

IEC 60204-1, Safety of machinery — Electrical equipment of machines — Part 1: General requirements (Безопасность машинного оборудования. Электрическое оборудование машин. Часть 1. Общие требования)

IEC 61131-2, Programmable controllers — Part 2: Equipment requirements and tests (Программируемые контроллеры. Часть 2. Требования к оборудованию и тестирование)

МЭК 61158 (все части), Промышленные сети связи. Спецификации полевых шин (Industrial communication networks — Fieldbus specifications)

IEC 61158-2, Industrial communication networks — Fieldbus specifications — Part 2: Physical layer specification and service definition (Промышленные сети связи. Спецификации полевых шин. Часть 2: Спецификация физического уровня и определение сервиса)

IEC 61158-3-18, Industrial communication networks — Fieldbus specifications — Part 3-18: Data-link layer service definition — Type 18 elements (Промышленные сети связи. Спецификации полевых шин. Часть 3-18: Определение сервиса канального уровня. Элементы типа 18)

(IEC 61158-4-18, Industrial communication networks — Fieldbus specifications — Part 4-18: Data-link layer protocol definition — Type 18 elements (Промышленные сети связи. Спецификации полевых шин. Часть 4-18: Определение протокола канального уровня. Элементы типа 18)

IEC 61158-5-18, Industrial communication networks — Fieldbus specifications — Part 5-18: Application layer service definition — Type 18 elements (Промышленные сети связи. Спецификации полевых шин. Часть 5-18: Определение сервиса прикладного уровня. Элементы типа 18)

IEC 61158-6-18, Industrial communication networks — Fieldbus specifications — Part 6-18: Application layer protocol specification — Type 18 elements (Промышленные сети связи. Спецификации полевых шин. Часть 6-18: Спецификация протокола прикладного уровня. Элементы типа 18)

IEC 61326-3-1, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) — General industrial applications (Электрооборудование для измерений, управления и лабораторного применения. Часть 3-1. Требования защищенности для систем, связанных с безопасностью и для оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональной безопасности). Общие промышленные приложения)

IEC 61326-3-2, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) — Industrial applications with specified electromagnetic environment (Электрооборудование для измерений, управления и лабораторного применения. Часть 3-1. Требования защищенности для систем, связанных с безопасностью и для оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональной безопасности). Промышленные приложения сопределенной электромагнитной средой)

IEC 61508 (allparts), Functional safety of electrical/electronic/programmable electronic safety-related systems (Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью)

IEC 61511 (allparts), Functional safety — Safety instrumented systems for the process industry sector (Функциональная безопасность. Инструментальные системы безопасности для сектора перерабатывающей промышленности)

IEC 61784-1, Industrial communication networks — Profiles — Part 1: Fieldbus profiles (Промышленные сети. Профили. Часть 1. Профили полевых шин)

(IEC 61784-3:2010, Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions (Промышленные сети. Профили. Часть 3. Полевые шины функциональной безопасности. Общие правила и определения профиля)

(IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems (Безопасность оборудования. Функциональная безопасность систем управления электрических/электронных/программируемых электронных, связанных с безопасностью)

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 Общепринятые термины и определения

3.1.1.1 **готовность** (availability): Вероятность того, что в течение заданного промежутка времени в автоматизированной системе не наблюдается неисправных состояний в системе, приводящих к потере производительности.

3.1.1.2 **черный канал** (blackchannel): Канал связи, для которого отсутствуют доказательства того, что проектирование и подтверждение соответствия были выполнены в соответствии с МЭК 61508.

3.1.1.3 **канал связи** (communication channel): Логическое соединение между двумя оконечными точками в коммуникационной системе.

3.1.1.4 **коммуникационная система** (communication system): Система (устройство), состоящая из технических средств, программного обеспечения и среды распространения, которая обеспечивает передачу сообщений (прикладной уровень по ИСО/МЭК 7498) от одного приложения другому.

3.1.1.5 **соединение** (connection): Логическое связывание между двумя прикладными объектами в одном или в разных устройствах.

3.1.1.6 **циклический контроль избыточности** [Cyclic Redundancy Check (CRC)]. Получаемые из блока данных (значений) избыточных данных, которые запоминаются и передаются вместе с этим блоком данных, для обнаружения искажения данных. Процедура (метод), использующаяся для вычисления избыточных данных.

Примечания

1 Термины «CRC код» и «CRC подпись» и обозначения, такие как «CRC 1» и «CRC 2» также могут применяться в данном стандарте в отношении избыточных данных.

2 См. Также [32], [33].

3.1.1.7

ошибка (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и истинным, установленным или теоретически верным значением или условием.

[МЭК 61508-4:2010], [МЭК 61158]

Примечания

1 Ошибки могут возникнуть вследствие ошибок проектирования аппаратных средств/ программного обеспечения и/или вследствие искажения данных, вызванного электромагнитными помехами и/или другими воздействиями.

2 Ошибки не обязательно являются причиной отказов или сбоев.

3.1.1.8

отказ (failure): Прекращение способности функционального блока выполнять необходимую функцию либо функционирование этого блока любым способом, отличным от требуемого.

Примечание — В МЭК 61508-4 приведено такое же определение, но дополнено примечаниями.

[МЭК 61508-4:2010, модифицировано], [ИСО/МЭК 2382-14.01.11, модифицировано]

Примечание — Причиной отказа может служить ошибка (например, проблема, связанная с проектированием программного обеспечения/аппаратных средств или с нарушением при передаче сообщений).

3.1.1.9

сбой (fault): Ненормальный режим, который может вызвать снижение или потерю способности функционального блока выполнять требуемую функцию.

Примечание — Международный электротехнический словарь (191-05-01) определяет «сбой» как состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая неспособность, возникающую во время профилактических работ или других плановых мероприятий, либо в результате недостатка внешних ресурсов.

[МЭК 61508-4:2010, модифицировано], [ИСО/МЭК 2382-14.01.10, модифицировано]

3.1.1.10 **полевая шина** (fieldbus): Коммуникационная система, основанная на последовательной передаче данных и применяющаяся в промышленной автоматизации или приложениях управления процессами.

3.1.1.11 **кадр** (frame): Упрощенный синоним для DLPDU (Блок данных протокола канала передачи данных).

3.1.1.12

хеш-функция (hash function): (Математическая) функция, которая преобразует значения из (вероятно очень) большого набора значений в (обычно) меньший диапазон значений.

Примечания

1 Хеш-функции могут применяться для обнаружения искажений данных.

2 Распространенные хеш-функции включают в себя контроль четности, вычисление контрольной суммы или CRC.

[МЭК/ТО 62210, модифицировано]

3.1.1.13 **опасность** (hazard): Состояние или набор условий в системе, которые вместе с другими, связанными с этим, условиями неизбежно приведут к причинению вреда человеку, имуществу или окружающей среде.

3.1.1.14 **ведущее устройство** (master): Активный объект коммуникации, способный инициировать и управлять во времени коммуникационной деятельностью других станций, которые могут быть как ведущими, так и ведомыми.

3.1.1.15

сообщение (message): Упорядоченные последовательности октет, предназначенные для передачи информации.

[ИСО/МЭК 2382-16.02.01, модифицировано]

3.1.1.16

уровень эффективности защиты; УЭЗ [performance level (PL)]: Дискретный уровень, применяющийся для определения способности связанных с безопасностью частей системы управления выполнять функцию безопасности в прогнозируемых условиях.

[ИСО 13849-1]

3.1.1.17

защитное сверхнизкое напряжение (protective extra-low-voltage, PELV): Электрическая цепь, в которой значение напряжения не может превышать среднеквадратичное значение переменного напряжения в 30 В, пиковое напряжение 42,4 В или постоянное напряжение 60 В при нормальных условиях и одиночном сбое, за исключением короткого замыкания на землю в других цепях.

Примечание — Электрическая цепь PELV аналогична цепи SELV с защитным заземлением.

[МЭК 61131-2]

3.1.1.18

избыточность (redundancy): Существование более одного средства выполнения необходимой функции или представления информации.

Примечание — В МЭК 61508-4 такое же определение, но дополнено примером и примечаниями.

[МЭК 61508-4:2010, модифицировано], [ИСО/МЭК 2382-14.01.12, модифицировано]

3.1.1.19

надежность (reliability): Вероятность того, что автоматизированная система может выполнять требующуюся функцию в заданных условиях на протяжении заданного промежутка времени (t1, t2).

Примечания

1 Принято считать, что автоматизированная система в состоянии выполнять данную требующуюся функцию в начале заданного промежутка времени.

2 Понятие «надежности» также используются для обозначения показателя надежности, измеряемого данной вероятностью.

3 На протяжении среднего времени между отказами (MTBF) или среднего времени до отказа (MTTF) вероятность того, что автоматизированная система выполнит требующуюся функцию — уменьшается.

4 Надежность отличается от готовности.

[МЭК 62059-11, модифицирован]

3.1.1.20

риск (risk): Сочетание вероятности события причинения вреда и тяжести этого вреда.

Примечание — Более подробно это понятие обсуждается в МЭК 61508-5:2010, приложение А.

[МЭК 61508-4:2010], [ИСО/МЭК Руководство 51:1999, определение 3.2]

3.1.1.21 **коммуникационный уровень безопасности;** КУБ (safety communication layer, КУБ): Уровень коммуникации, включающий все необходимые меры для обеспечения безопасной передачи информации в соответствии с требованиями МЭК 61508.

3.1.1.22 **безопасное соединение** (safety connection): Соединение, которое применяет протокол безопасности для транзакций коммуникаций.

3.1.1.23 **данные безопасности** (safety data): Данные, передаваемые через безопасную сеть, используя протокол безопасности.

Примечание — Коммуникационный уровень безопасности не гарантирует безопасность самой информации, а только то, что она передается безопасно.

3.1.1.24 **устройство безопасности** (safety device): Устройство, спроектированное в соответствии с МЭК 61508 и реализующее профиль коммуникации, удовлетворяющий требованиям функциональной безопасности.

3.1.1.25

безопасное сверхнизкое напряжение (safety extra-low-voltage, SELV): Электрическая цепь, в которой значение напряжения не может превышать среднеквадратичное значение переменного напряжения в 30 В, пиковое напряжение 42,4 В или постоянное напряжение 60 В при нормальных условиях и одиночном сбое, включая короткое замыкание на землю в других цепях.

Примечание — Цепь SELV не подсоединена к защитному заземлению.

[МЭК 61131-2]

3.1.1.26

функция безопасности (safety function): Функция, реализуемая Э/Э/ПЭ (электрической, электронной, программируемой электронной) системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния управляемого оборудования по отношению к конкретному опасному событию.

Примечание — В МЭК 61508-4 такое же определение, но дополнено примером и примечанием.

[МЭК 61508-4:2010, модифицирован]

3.1.1.27 **время реакции функции безопасности** (safety function response time): Наихудшее время между срабатыванием датчика системы безопасности, подключенного к полевой шине, и достижением соответствующего безопасного состояния с помощью необходимого исполнительного устройства этой системы безопасности при наличии ошибок или отказов в канале функции безопасности.

Примечание — Данное понятие введено в МЭК 61784-3:2010, 5.2.4 и реализуется профилями коммуникаций, удовлетворяющими требованиям функциональной безопасности, определенными в настоящем стандарте.

3.1.1.28

уровень полноты безопасности; УПБ (safety integrity level, SIL): Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

Примечания

1 Целевые значения отказов (см. МЭК 61508-4:2010, пункт 3.5.17) для четырех уровней полноты безопасности указаны в МЭК 61508-1:2010, таблицы 2 и 3.

2 Уровни полноты безопасности используют при определении требований полноты безопасности для функций безопасности, которые должны быть распределены по Э/Э/ПЭ системам, связанным с безопасностью.

3 Уровень полноты безопасности (УПБ) не является свойством системы, подсистемы, элемента или компонента. Правильная интерпретация фразы «УПБ системы, связанной с безопасностью, равен *n*» (где *n* = 1, 2, 3 или 4) означает: система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до значения, равного *n*.

[МЭК 61508-4:2010]

3.1.1.29 **мера безопасности** (safety measure): Средство управления возможными ошибками коммуникаций, спроектированное и реализованное в соответствии с требованиями МЭК 61508.

Примечания

1 На практике, как правило, объединяют несколько мер безопасности для достижения требуемого уровня полноты безопасности

2 Ошибки коммуникаций и связанные с ними меры безопасности подробно рассмотрены в МЭК 61784-3:2010, 5.3 и 5.4.

3.1.1.30 **приложение, связанное с безопасностью** (safety-related application): Программы, разработанные в соответствии с МЭК 61508 и удовлетворяющие требованиям УПБ приложения.

3.1.1.31 **система, связанная с безопасностью** (safety-related system): Система, выполняющая функцию безопасности в соответствии с МЭК 61508.

3.1.1.32 **ведомое устройство** (slave): Пассивный объект коммуникации, способный принимать сообщения и отправлять их в ответ на другой объект коммуникации, который может быть ведомым или ведущим.

3.1.1.33 **временная метка** (time stamp): Информация о времени, включенная в сообщение.

3.1.2 CPF 8. Дополнительные термины и определения

3.1.2.1 **цикл** (cycle): Интервал, за который повторно и непрерывно выполняется деятельность.

3.1.2.2 **взаимосвязь приложений безопасности, ВСПБ** [safety application relation ship (SAR)]: Взаимосвязь приложений двух или более оконечных точек взаимосвязи приложений, связанных с безопасностью.

3.1.2.3 **элемент услуг приложения безопасности** [safety application service element (SASE)]: Элемент услуг, связанный с безопасностью приложения.

3.1.2.4 **таймер устройства контроля данных безопасности** (safety data monitor timer): Таймер, используемый функцией ожидания времени для передачи данных безопасности.

3.1.2.5 **таймер устройства контроля безопасности** (safety monitor timer): Таймер, используемый функцией ожидания времени для управления безопасным соединением.

3.1.2.6 **PDU безопасности** (safety PDU): Синоним для DLPDU, связанного с безопасностью.

3.1.2.7 **слот** (slot): Один квант (степени детализации) зависящего от позиции отображения полей циклических данных.

3.1.2.8 **станция** (station): Устройство и соответствующая ему SAREP, связанные с передачей и принятием данных безопасности.

Примечание — Номер станции используется в зависящем от позиции отображении полей циклических данных (станция занимает один или более слотов).

3.1.2.9 **информация передачи протокола безопасности** (safety protocol transmission information): Информация, характеризующая сообщения, имеющие значение для безопасности.

3.2 Обозначения и сокращения

3.2.1 Общие обозначения и сокращения

Сокращение	Полное наименование	Источник
CP	Профиль коммуникаций	[МЭК 61784-1]
CPF	Семейство профилей коммуникации	[МЭК 61784-1]
CRC	Циклический контроль избыточности	
DLL	Уровень канала данных	[ИСО/МЭК 7498-1]
DLPDU	Блок данных протокола канала передачи данных	
ЭМС	Электромагнитная совместимость	
УО	Управляемое оборудование	[МЭК 61508-4:2010]
Э/Э/ПЭ	Электрические/электронные/программируемые электронные	[МЭК 61508-4:2010]
FAL	Прикладной уровень полевой шины (Fieldbus Application Layer)	[МЭК 61158-5]
ФБ	Функциональная безопасность	
FSCP	Профиль коммуникации, удовлетворяющий требованиям функциональной безопасности	
MTBF	Среднее время между отказами	
MTTF	Среднее время до отказа	
PDU	Блока данных протокола	[ИСО/МЭК 7498-1]
PELV	Защитное сверхнизкое напряжение	
PhL	Физический уровень	[ИСО/МЭК 7498-1]
УЭЗ	Уровень эффективности защиты	[ИСО 13849-1]
PLC	Программируемый логический контроллер	
КУБ	Коммуникационный уровень безопасности	
SELV	Безопасное сверхнизкое напряжение	
УПБ	Уровень полноты безопасности	[МЭК 61508-4:2010]

3.2.2 CPF 8. Дополнительные термины и определения

SIS — Инструментальная система безопасности (safety instrumented systems)

Сокращение	Полное наименование
СП	Связь приложений
ASE	Прикладной элемент услуг
CMD	Командная информация
СИД	Светоизлучающий диод
LID	Идентификатор канала
PSD	Данные поддержки протокола
RNO	Текущий номер
СПБ	Связь приложений безопасности
SAREP	Оконечная точка связи приложений безопасности

Сокращение	Полное наименование
SARPM	Машина состояний протокола связи приложений безопасности
SASE	Элемент услуг приложения безопасности
SRC	Контроллер, важный для безопасности
SRP	Периферийное устройство, важное для безопасности
TPI	Информация пакета передачи данных безопасности
TPI-T	Информация пакета передачи данных безопасности от ведущего устройства
TPI-R	Информация пакета передачи данных безопасности от ведомого устройства

3.3 Условные обозначения

Условные обозначения, используемые в настоящем стандарте, определены в МЭК 61158, Типе 18 и CPF 8 МЭК 61784-1.

4 Обзор FSCP 8/1 (CC-Link Safety™)

Серия 8 профилей коммуникаций (общеизвестная как CC-Link™ [2]) определяет профили коммуникаций, основанные на МЭК 61158-2,Тип 18, МЭК 61158-3-18, МЭК 61158-4-18,МЭК 61158-5-18 и МЭК 61158-6-18.

Базовые профили CP 8/1, CP 8/2, CP 8/3 определены в МЭК 61784-1.Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 8/1 (CC-Link Safety™ [2]) серии CPF 8, основан на базовых профилях CPF 8 из МЭК 61784-1, а также на спецификациях коммуникационного уровня безопасности, определенных в настоящем стандарте.

FSCP 8/1 является протоколом для сообщения данных, связанных с безопасностью, таких как, сигнал срочной остановки между участниками в пределах распределенной сети, используя технологию полевых шин, в соответствии с требованиями МЭК 61508 для функциональной безопасности. Данный протокол имеет множество различных применений, таких как управление процессом, автоматизация производства и машинное оборудование.

Протокол FSCP 8/1 спроектирован для поддержания УПБЗ (МЭК 61508), используя CPF 8 с дополнительно установленными механизмами для реализации порядкового номера, временного ожидания, проверки подлинности соединения, сообщения обратной связи, обеспечения целостности данных, а также различные меры безопасности по обеспечению целостности данных.

Функциональные возможности КУБ протокола FSCP 8/1 предоставляются вместе с введением специальных прикладных элементов услуг (SASE). Эти SASE элементы используются вместо соответствующих им прикладных элементов услуг ASE, как установлено в МЭК 61784-3-8. Но, так как они наследуют напрямую от своих родительских классов, определенных в CPF 8, эти SASE элементы устанавливают дополнения к CPF 8, требующиеся для функциональной безопасности, использующей метод черного канала

5 Общие положения

5.1 Внешние документы, предоставляющие спецификации для профиля

Производителям устройств безопасности FSCP 8/1 рекомендуется ознакомиться с документами [43]—[45], предоставляющими дополнительные спецификации, значимые для реализации КУБ, определенного в настоящем стандарте.

[2] CC-Link™ и CC-Link Safety™являются торговыми марками некоммерческой организации CC-Link Partner Association. Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований CC-Link™ и CC-Link Safety™. Использование торговых марок CC-Link™ и CC-Link Safety™ требует разрешения со стороны CC-Link Partner Association.

5.2 Функциональные требования безопасности

В настоящем стандарте описываются услуги и протоколы для системы коммуникаций функциональной безопасности, основанные на МЭК 61158, Тип 18.

Следующие требования применяются к разработке устройств, реализующих протоколы FSCP 8/1. Те же требования были использованы при разработке FSCP 8/1.

- Протоколы FSCP 8/1 спроектированы для поддержки уровня полноты безопасности УПБ3 (см. МЭК 61508).
- Реализации FSCP 8/1 должны соответствовать МЭК 61508.
- Базовые требования для разработки протокола FSCP 8/1 содержаться в МЭК 61784-3.
- Состояние безопасности для дискретных данных является обесточенным состоянием (0). Для аналоговых значений обесточенное состояние должно быть задано приложением, связанным с безопасностью.
- Условия окружающей среды должны соответствовать МЭК 61131-2 для базовых уровней и МЭК 61326-3-1, МЭК 61326-3-2 для испытаний запаса безопасности, если отсутствуют конкретные стандарты для самого изделия.
- Если в настоящем стандарте не установлено, то требования CPF 8 для безопасности не должны изменятся.

5.3 Меры безопасности

5.3.1 Общие положения

Коммуникационный уровень безопасности, описанный в настоящем стандарте, предоставляет следующие детерминированные корректирующие меры для его реализации:

- порядковый номер;
- временное ожидание,
- аутентификация соединения;
- сообщение обратной связи;
- обеспечение целостности данных (CRC 32);
- другие системы обеспечения целостности данных.

Данная подборка различных мер для исправления возможных ошибок показана в таблице 1.

Таблица 1 — Выбор различных мер для исправления возможных ошибок

Ошибка коммуникации	Детерминированная корректирующая мера							
	Порядковый номер	Временная метка	Временное ожидание	Аутентификация соединения	Сообщение обратной связи	Обеспечение целостности данных	Избыточность с перекрестной проверкой	Другие системы обеспечения целостности данных
Искажение						x		
Непреднамеренное повторение	x							
Неверная последовательность	x							
Потеря	x				x			
Недопустимая задержка			x					
Внесение	x			x	x			
Подмена				x	x			x
Адресация				x				
Примечание — Таблица адаптирована из МЭК 62280-2 [16] и ЕН 954-1 [27].								

5.3.2 Порядковый номер

Сообщения безопасности содержат порядковый номер (RNO) размером в 4 бита и установленную последовательность (см. 7.1 и 7.2). Если последовательность не соблюдается, то все выходные сигналы, связанные с безопасностью, должны быть установлены в их безопасные состояния.

5.3.3 Временное ожидание

Встроенный сторожевой таймер, предоставляющий временное ожидание каждого канала вывода на каждом ведомом устройстве безопасности, обеспечивает время реакции функции безопасности, являющееся временем между обнаружением события на ведомом устройстве ввода безопасности и реакцией на соответствующем выходе канала(ов) на ведомых устройствах вывода безопасности без учета времени на обработку ввода безопасности. Более подробно см. в 9.3.

Время реакции функции безопасности состоит из времени передачи по полевой шине от ведомого устройства ввода безопасности ведущему устройству и от ведущего устройства ведомому устройству вывода безопасности, включая возможные повторения PDU безопасности, вызванные ошибками передачи, время обработки на ведомом устройстве вывода безопасности и время обработки в контроллере, связанном с безопасностью (SRC).

Если время реакции функции безопасности определенного вывода канала ведомого устройства вывода безопасности превышено, то соответствующий канал вывода устанавливается в его безопасное состояние, которым, как правило, является состояние отключенного питания (power OFF state). Это должно соблюдаться прикладным уровнем SRP.

5.3.4 Аутентификация соединения

Аутентификация соединения реализуется набором ID соединения безопасности (канальных ID) и номером станции. Каждое ведомое устройство безопасности использует 3 бита ID канала, описывающих ее систему сети безопасности. Это предоставляет SRC вплоть до 8 систем сети безопасности. В рамках коммуникационной системы функциональной безопасности назначение значений ID канала должно быть уникальным. Сообщения безопасности всегда содержат ID канала.

5.3.5 Сообщение обратной связи

Сообщение обратной связи поступает от каждого ведомого устройства, подтверждающего получение сообщений от ведущего устройства. Сообщение обратной связи содержит информацию о статусе ошибки, поступившую от ведомого устройства, а также подтверждение RNO, ID канала, командный ID и поле данных поддержки протокола.

5.3.6 Другие системы обеспечения целостности данных

Различие между сообщениями, важными и не важными для безопасности в том, что сообщения безопасности содержат контрольную сумму CRC (32 бита). Протокол МЭК 61158,Тип 18 использует другой CRC алгоритм (16-битовый CRC). Кроме того, каждая телеграмма содержит 16-битовое поле данных поддержки протокола, 8-битовый командный ID, 3-битовый ID канала и 4-битовый RNO.

5.4 Структура коммуникационного уровня безопасности

Функциональные возможности КУБ для FSCP 8/1 предоставляются вместе с введением элементов услуг приложения безопасности (SASE). Эти SASE элементы используются вместо соответствующих им прикладных элементов услуг (ASE элементов), как это установлено в настоящем стандарте.Так как они наследуют напрямую от родительских классов, заданных в CPF 8, эти SASE элементы определяют дополнения к CPF 8. Элементы SASE реализуются, основываясь на следующем.

- менеджер устройства — спецификации класса ASE для менеджера устройства типа M1 и S1;
- менеджер соединения — определение класса AR для менеджера соединения типа M1 и S1;
- циклическая передача — спецификация класса ARASE данных процесса для циклической передачи типа M1 и S1.

КУБ дополняет эти определения ASE:

- менеджером устройства безопасности типа M1 и S1;
- менеджером соединения безопасности типа M1 и S1;
- циклической передачей типа M1 и S1.

Все управление, поведения и функции КУБ обрабатываются с помощью этих элементов услугприложения безопасности.

5.5 Связи с FAL (и DLL, PhL)

5.5.1 Обзор

На рисунке 3 показана связь между КУБ и другими уровнями коммуникационного стека Типа 18 стандарта МЭК 61158.

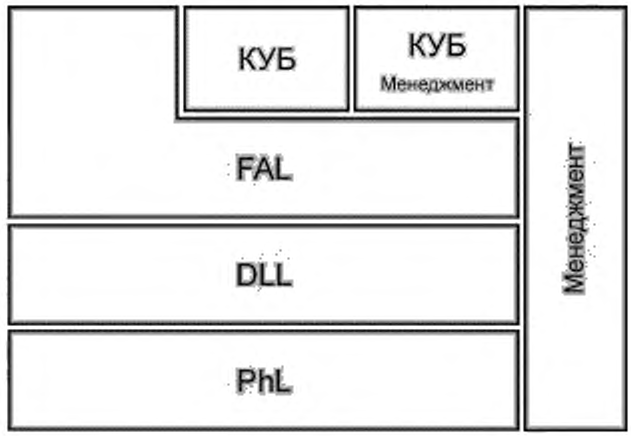


Рисунок 3 — Связь между КУБ и другими уровнями МЭК 61158, Тип 18

5.5.2 Типы данных

Типы данных для данных безопасности описаны в МЭК 61158-5-18.

6 Услуги коммуникационного уровня безопасности

6.1 Общие положения

SARFSCP 8/1 использует буферизованные средства передачи для обработки данных входов и выходов.Услуги типа запуска передачи требуются в зависимости от конфигурации конкретизированных объектов. Управление соединением осуществляется классом менеджера безопасного соединения.

Приложения, связанные с безопасностью, используют сервисные элементы приложения безопасности для взаимодействия через коммуникационный уровень безопасности. Формальная модель этих элементов услуг определена в данном разделе.

6.2 Элементы SASE

6.2.1 Спецификация класса менеджера устройства безопасности M1

Класс менеджера устройства безопасности M1 поддерживает пользователя КУБ типа ведомое устройство в реализации DL опросного типа.

КУБ ASE:			SASE управление.
КЛАСС:			Менеджер устройства безопасности M1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Менеджер устройства M1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Информация по управлению.
1.1	(m)	Атрибут:	Id канала.

1.2	(o)	Атрибут:	Версия программного обеспечения/протокола.
2	(m)	Атрибут:	Информация по управлению соединенными ведомыми устройствами.
2.1	(m)	Атрибут:	Версия 1 программного обеспечения/протокола.
...	...	...	...
2.n	(m)	Атрибут:	Версия n программного обеспечения/протокола.
...	...	...	...
2.64	(m)	Атрибут:	Версия 64 программного обеспечения/протокола.

6.2.2 Спецификация класса менеджера устройства безопасности S1

Класс менеджера устройства безопасности поддерживает пользователя КУБ типа ведомое устройство в реализации DL опросного типа.

КУБ ASE:			SASE управление.
КЛАСС:			Менеджер устройства безопасности S1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Менеджер устройства S1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Информация по управлению.
1.1	(m)	Атрибут:	Id канала.
1.2	(m)	Атрибут:	Версия программного обеспечения/протокола.

6.3 SAR связи

6.3.1 Класс менеджера соединения безопасности M1

Класс менеджера соединения безопасности M1 поддерживает пользователя КУБ типа ведущее устройство в DL реализации опросного типа.

КУБ ASE:			SASE управление.
КЛАСС:			Менеджер соединения безопасности M1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Менеджер устройства M1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Информация о параметре.
1.1	(m)	Атрибут:	Значение таймера устройства контроля безопасности.
1.2	(m)	Атрибут:	Значение таймера устройства контроля данных безопасности.
1.3	(m)	Атрибут:	Спецификация ведомого устройства безопасности.
1.4	(m)	Атрибут:	Источник спецификации ведомого устройства безопасности.
1.5	(m)	Атрибут:	Информация о продукте для ведомого устройства безопасности.
2	(m)	Атрибут:	Данные параметров ведомого устройства безопасности.
3	(m)	Атрибут:	Статус канала ведомого устройства безопасности.

6.3.2 Класс менеджера соединения безопасности S1

Класс менеджера соединения безопасности S1 поддерживает пользователя КУБ типа ведомое устройство в реализации DL опросного типа.

КУБ ASE:			SASE управление.
КЛАСС:			Менеджер соединения безопасности S1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Менеджер соединения S1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Информация о продукте, предназначенном для безопасности.
2	(m)	Атрибут:	Данные параметров ведомого устройства безопасности.

6.4 Данные процесса для элементов ASE связи SAR

6.4.1 Спецификация класса циклической передачи данных безопасности M1

Класс циклической передачи данных безопасности M1 поддерживает пользователя КУБ типа ведущего устройства в связке с менеджером соединения безопасности M1.

КУБ ASE:			Данные Процесса ASE связи SAR.
КЛАСС:			Циклическая передача безопасности M1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Циклическая передача M1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Данные на выходе.
1.1	(m)	Атрибут:	Данные RY безопасности.
1.2	(m)	Атрибут:	Данные RWw.
1.2.1	(m)	Атрибут:	Данные RWw безопасности.
1.2.2	(m)	Атрибут:	TPI-T безопасности.
2.	(m)	Атрибут:	Данные на входе.
2.1	(m)	Атрибут:	Данные безопасности в 1.
2.1.1	(m)	Атрибут:	Данные RX безопасности в 1.
2.1.2.	(m)	Атрибут:	Данные RWr 1.
2.1.2.1	(m)	Атрибут:	Данные RWr безопасности 1.
2.1.2.2	(m)	Атрибут:	TPI-R безопасности.
...	...	...	...
2.n	(m)	Атрибут:	Данные безопасности в n.
...	...	...	...
2.64	(m)	Атрибут:	Данные безопасности в 64.

6.4.2 Спецификация класса циклической передачи данных безопасности S1

Класс циклической передачи данных безопасности S1 поддерживает пользователя КУБ типа ведомое устройство в связке с менеджером соединения безопасности S1.

КУБ ASE:			Данные Процесса ASE связи SAR.
КЛАСС:			Циклическая передача безопасности S1.
ID КЛАССА:			Не используется.
РОДИТЕЛЬСКИЙ КЛАСС:			Циклическая передача S1.
АТРИБУТЫ:			
1	(m)	Атрибут:	Данные на выходе.
1.1	(m)	Атрибут:	Данные RY безопасности.
1.2	(m)	Атрибут:	Данные RWw.
1.2.1	(m)	Атрибут:	Данные RWw безопасности.
1.2.2	(m)	Атрибут:	TPI-T безопасности.
2	(m)	Атрибут:	Данные на входе.
2.1	(m)	Атрибут:	Данные RX безопасности.
2.2	(m)	Атрибут:	Данные RWr.
2.2.1	(m)	Атрибут:	Данные RWr безопасности.
2.2.2	(m)	Атрибут:	TPI-R безопасности.

7 Протокол коммуникационного уровня безопасности

7.1 Формат PDU безопасности

7.1.1 Общие положения

Синтаксис PDU безопасности и его кодирование описаны в МЭК 61158-6-18 в понятиях абстрактного синтаксиса и синтаксиса передачи.

7.1.2 Абстрактный синтаксис

7.1.2.1 Абстрактный синтаксис PDU менеджера устройства безопасности M1

Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 2.

Таблица 2 — Формат атрибутов менеджера устройства безопасности M1

Атрибут	Формат	Размер, бит
Информация по управлению	Структура из двух элементов	11
Id Канала	Unsigned3	3
Версия программного обеспечения/ протокола	1 октет, побитное отображение	8
Информация по управлению подсоединенным ведомым устройством	Массив из 64 членов:	64 октета
Версия программного обеспечения/ протокола	1 октет, побитовое отображение	8

7.1.2.2 Абстрактный синтаксис PDU менеджера устройства безопасности S1
Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 3.

Таблица 3 — Формат атрибутов менеджера устройства безопасности S1

Атрибут	Формат	Размер, бит
Информация по управлению	Структура из трех элементов	11
Id канала	Unsigned 3	3
Версия программного обеспечения/ протокола	1 октет, побитное отображение	8

7.1.2.3 Абстрактный синтаксис PDU менеджера соединения безопасности M1
Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 4.

Таблица 4 — Формат атрибутов менеджера соединения безопасности M1

Атрибут	Формат	Размер, бит
Информация о параметрах	Структура из пяти элементов	2004 октетов
Значения таймера устройства контроля безопасности	Unsigned16	16
Значение таймера устройства контроля данных безопасности	Unsigned16	16
Спецификация ведомого устройства безопасности	8 октетов, побитное отображение	64
Источник спецификации ведомого устройства безопасности	8 октетов, побитное отображение	64
Информация о продукте для ведомого устройства безопасности	Массив из 64 членов:	1984 октетов
Информация об изделии, предназначенном для безопасности 1—64	Структура данных, ориентированная на слова	31 октет
Данные параметров ведомого устройства безопасности	16—52 224 октетов	16—52 224 октетов
Статус канала ведомого устройства безопасности	8 октетов, побитное отображение	64

7.1.2.4 Абстрактный синтаксис PDU менеджера соединения безопасности S1
Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 5.

Таблица 5 — Формат атрибутов менеджера соединения безопасности S1

Атрибут	Формат	Размер, бит
Информация об изделии, предназначенном для безопасности 1-64	Структура данных, ориентированная на слова	31 октет
Данные параметров ведомого устройства безопасности	16—816 октетов	16—816 октетов

7.1.2.5 Абстрактный синтаксис PDU циклической передачи данных безопасности M1
Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 6.

Таблица 6 — Формат атрибутов циклической передачи данных безопасности M1

Атрибут	Формат	Размер, бит
Данные на выходе	Структура из двух элементов	96*n*
Данные RY безопасности	Бит-ориентированная структура данных	32*n*
Данные RWw	Структура данных, ориентированная на слова	64*n*
Данные RWw безопасности	Данные, ориентированные на слова	64(*n*–*m*)
TPI-T безопасности	Информация пакета передачи данных безопасности	64*m*
Данные на входе	Структура из n элементов	96*n*
Данные безопасности в 1	Структура из двух элементов	96p_1
Данные RX безопасности	Бит-ориентированная структура данных	32p_1
Данные RWr	Структура данных, ориентированная на слова	64p_1
Данные RWr безопасности	Данные, ориентированные на слова	64 (p_1 – 1)
TRI-R безопасности	Информация пакета передачи данных безопасности	64
…	…	…
Данные безопасности в *n*	Структура из двух элементов	96p_n
Примечание — Значения *n* и *m* зависят от значений соответствующих настроек конфигурации в статусе ведущего устройства. Значение *p* зависит от номера слотов, занятых ведомой станцией.		

7.1.2.6 Абстрактный синтаксис PDU циклической передачи данных безопасности S1

Абстрактный синтаксис для атрибутов, принадлежащих данному классу, описан в таблице 7.

Таблица 7 — Формат атрибутов циклической передачи данных безопасности S1

Атрибут	Формат	Размер, бит
Данные на выходе	Структура из двух элементов	96*p*
Данные RY безопасности	Бит-ориентированная структура данных	32*p*
Данные RWw	Структура данных, ориентированная на слова	64*p*
Данные RWw безопасности	Данные, ориентированные на слова	64 (*p* – 1)
TPI-T безопасности	Информация пакета передачи данных безопасности	64
Данные на входе	Структура из n элементов	96*p*
Данные RX безопасности	Бит-ориентированная структура данных	32*p*
Данные RWr	Структура данных, ориентированная на слова	64*p*
Данные RWr безопасности	Данные, ориентированные на слова	64 (*p* – 1)
TRI-R безопасности	Информация пакета передачи данных безопасности	64
Примечание — Значение *p* зависит от номера слотов, занятых ведомой станцией.		

7.1.3 Синтаксис передачи

7.1.3.1 Кодирование PDU менеджера устройства безопасности M1

Определенное кодирование PDU для атрибутов, принадлежащих данному классу, описано в таблице 8.

Таблица 8 — Кодирование атрибутов менеджера устройства безопасности M1

Атрибут	Кодирование		
Информация по управлению	Устанавливает конфигурацию ведущего устройства		
Id канала	0—7 — допустимый диапазон		
Версия программного обеспечения/протокола	Бит	Описание	Значение
	5—0	Версия программного обеспечения	1—63 — допустимый диапазон
	7—6	Версия протокола	0 — Версия 1 1 — Версия 2 2 — Версия 3 3 — Версия 4
Информация о подсоединенном ведомом устройстве	Устанавливает конфигурацию подсоединенных устройств		
Информация о ведомом устройстве 1—64	Массив из 64 элементов, каждый закодирован как:		
Версия программного обеспечения/протокола	Бит	Описание	Значение
	5—0	Версия программного обеспечения	1—63 — допустимый диапазон
	7—6	Версия протокола	0 — Версия 1 1 — Версия 2 2 — Версия 3 3 — Версия 4

7.1.3.2 Кодирование PDU менеджера устройства безопасности S1

Определенное кодирование PDU для атрибутов, принадлежащих данному классу, описано в таблице 9.

Таблица 9 — Кодирование атрибутов менеджера устройства безопасности S1

Атрибут	Кодирование		
Информация по управлению	Устанавливает конфигурацию ведущего устройства		
Id канала	0—7 — допустимый диапазон		
Версия программного обеспечения/протокола	Бит	Описание	Значение
	5—0	Версия программного обеспечения	1—63 — допустимый диапазон
	7—6	Версия протокола	0 — Версия 1 1 — Версия 2 2 — Версия 3 3 — Версия 4

7.1.3.3 Кодирование PDU менеджера соединения безопасности M1

Определенное кодирование PDU для атрибутов, принадлежащих классу, описано в таблице 10.

Таблица 10 — Кодирование атрибутов менеджера устройства безопасности М1

Атрибут	Кодирование
Информация о параметрах	Устанавливает конфигурацию ведущего устройства
Значения таймера устройства контроля безопасности	1—65535 мс
Значение таймера устройства контроля данных безопасности	1—65535 мс
Спецификация ведомого устройства безопасности	Бит 0—63 соответствует слоту 1—64, где: 0 — КУБ не поддерживается, 1 — КУБ поддерживается
Источник спецификации ведомого устройства безопасности	Бит 0—63 соответствует слоту 1—64, где: 0 — спецификация КУБ-пользователя не поддерживается, 1 — спецификация КУБ-пользователя поддерживается
Информация о продукте для ведомого устройства безопасности 1—64	Массив из 64 элементов, каждый закодирован как:
Информация о продукте, предназначенном для безопасности	31 октет данных для информации об изделии, предназначенном для безопасности
Данные параметров безопасности	0—52224 октетов данных для доступа к данным ведомого устройства
Статус канала ведомого устройства безопасности	Бит 0—63 соответствует слоту 1—64, где: 0 — ведомая станция безопасности не работает, 1 — ведомая станция безопасности работает

7.1.3.4 Кодирование PDU менеджера соединения безопасности S1

Определенное кодирование PDU для атрибутов, принадлежащих классу, описано в таблице 11.

Таблица 11 — Кодирование атрибутов менеджера соединения безопасности S1

Атрибут	Кодирование
Информация о продукте, предназначенном для безопасности	31 октет данных для информации об изделии безопасности
Данные параметров безопасности	0—816 октетов данных для доступа к данным ведомого устройства

7.1.3.5 Кодирование PDU циклической передачи данных безопасности М1

Определенное кодирование PDU для атрибутов, принадлежащих к данному классу, описано в таблице 12.

Таблица 12 — Кодирование атрибутов циклической передачи данных безопасности М1

Атрибут	Кодирование
Данные на выходе	Регистры процесса данных, установленные ведущим устройством для выхода ведомого устройства
Данные RY безопасности	Поле отображенной позиции бит-ориентированных выходных данных для всех соединенных ведомых устройств, упорядоченных по слоту с 32 битами на каждый слот
Данные RWw	Поле отображенной позиции, на которое отображается: выходные данные, ориентированные на слова, для всех соединенных ведомых устройств безопасности и информация пакета передачи данных безопасности для передачи ведомым устройствам безопасности

Продолжение таблицы 12

<table>
<tr><th>Атрибут</th><th colspan="4">Кодирование</th></tr>
<tr><td>Данные RWw безопасности</td><td colspan="4">Поле отображенной позиции выходных данных, ориентированных на слова, для всех соединенных ведомых устройств. Содержит 4 слова на каждый слот, начиная со второго слота. Так происходит потому, что последующее поле занимает пространство, предназначенное для первого слота в ведомом устройстве, не связанном с безопасностью</td></tr>
<tr><td rowspan="11">TPI-T безопасности</td><td>Октет</td><td>Бит</td><td>Описание</td><td>Значение</td></tr>
<tr><td>0—1</td><td>—</td><td>Данные поддержки протокола (PSD), используемые менеджментом КУБ</td><td>0—65535</td></tr>
<tr><td rowspan="7">2 3</td><td>0—3</td><td>Порядковый номер</td><td>0—15</td></tr>
<tr><td>4—6</td><td>Id канала</td><td>0—7</td></tr>
<tr><td>7</td><td>зарезервировано</td><td>0</td></tr>
<tr><td>8—11</td><td>Тип данных передачи</td><td>0—15</td></tr>
<tr><td>12</td><td>Флажок занятости</td><td>0 — занят, 1 — не занят</td></tr>
<tr><td>13</td><td>зарезервировано</td><td>0</td></tr>
<tr><td>14</td><td>Запрос на чтение</td><td>0 — нет запроса,
1 — запрос</td></tr>
<tr><td>15</td><td>Прикладной режим пользователя КУБ</td><td>0 — тестовый режим,
1 — режим безопасности</td></tr>
<tr><td>4—7</td><td>—</td><td>CRC 32</td><td>CRC32</td></tr>
<tr><td>Данные на входе</td><td colspan="4">Регистры данных процесса, считываемые ведущим устройством, представляющие собой вводы ведомого устройства</td></tr>
<tr><td>Данные безопасности на входе</td><td colspan="4">Регистры данных процесса, считываемые ведущим устройством, представляющие собой вводы ведомого устройства</td></tr>
<tr><td>Данные RX безопасности</td><td colspan="4">Поле, содержащее бит-ориентированные входные данные от ведомого устройства n, упорядоченные по слоту с 32 битами на каждый слот. Число слотов, занятых ведомым устройством, определяет общую длину данного поля</td></tr>
<tr><td>Данные RWr</td><td colspan="4">Поле, содержащее входные данные, ориентированные на слова, от ведомого устройства n, упорядоченные по слоту с 4 словами на каждый слот. Число слотов, занятых ведомым устройством, определяет общую длину данного поля</td></tr>
<tr><td>Данные RWr безопасности</td><td colspan="4">Поле отображенной позиции входных данных, ориентированных на слова, от ведомого устройства n. Содержит 4 слова на каждый слот, начиная со второго слота. Так происходит потому, что последующее поле занимает пространство, предназначенное для первого слота в ведомом устройстве, не связанном с безопасностью</td></tr>
<tr><td rowspan="5">TPI-T безопасности</td><td>Бит</td><td colspan="2">Описание</td><td>Значение</td></tr>
<tr><td>0—15</td><td colspan="2">Данные поддержки протокола (PSD), используемые менеджментом КУБ</td><td>0—65535</td></tr>
<tr><td>16—19</td><td colspan="2">Порядковый номер</td><td>0—15</td></tr>
<tr><td>20—22</td><td colspan="2">Id канала</td><td>0—7</td></tr>
<tr><td>23</td><td colspan="2">зарезервировано</td><td>0</td></tr>
<tr><td>24—27</td><td colspan="2">Тип данных передачи</td><td>0—15</td></tr>
</table>

Окончание таблицы 12

Атрибут	Кодирование		
	28	Флажок занятости	0 — занят, 1 — не занят
	29	Уведомление об ошибке	0 — нет запроса, 1 — запрос
	30	зарезервировано	0
	31	Прикладной режим пользователя КУБ	0 — тестовый режим, 1 — режим безопасности
	32—63	CRC 32	CRC 32

7.1.3.6 Кодирование PDU циклической передачи данных безопасности S1

Определенное кодирование PDU для атрибутов, принадлежащих данному классу, описано в таблице 13.

Таблица 13 — Кодирование атрибутов циклической передачи данных безопасности S1

Атрибут	Кодирование		
Данные на выходе	Данные процесса, полученные от ведущего устройства		
Данные RY безопасности	Поле, содержащее бит-ориентированные входные данные, упорядоченные по слоту с 32 битами на каждый слот. Число слотов, занятых ведомым устройством, определяет общую длину данного поля		
Данные RWw	Поле отображенной позиции, на которое отображается: выходные данные, ориентированные на слова (не обязательно) и информация пакета передачи данных безопасности, в том виде, в каком она получена от ведущего устройства		
Данные RWw безопасности	Поле отображенной позиции выходных данных, ориентированных на слова, для ведомого устройства. Содержит 4 слова на каждый слот, начиная со второго слота. Так происходит потому, что последующее поле занимает пространство, предназначенное для первого слота в ведомом устройстве, не связанном с безопасностью		
TPI-T безопасности	Бит	Описание	Значение
	0—15	Данные поддержки протокола (PSD), используемые менеджментом КУБ	0—65535
	16—19	Порядковый номер	0—15
	20—22	Id канала	0—7
	23	зарезервировано	0
	24—27	Тип данных передачи	0—15
	28	Флажок занятости	0 — занят, 1 — не занят
	29	зарезервировано	0
	30	Запрос на чтение	0 — нет запроса, 1 — запрос
	31	Прикладной режим пользователя КУБ	0 — тестовый режим, 1 — режим безопасности
	32—63	CRC 32	CRC 32
Данные на входе	Данные процесса, передаваемые ведущему устройству		
Данные RX безопасности	Поле, содержащее бит-ориентированные входные данные, упорядоченные по слоту с 32 битами на каждый слот. Число слотов, занятых ведомым устройством, определяет общую длину данного поля		

Окончание таблицы 13

Атрибут	Кодирование		
Данные RWr	Поле, содержащее входные данные, ориентированные на слова, от ведущего устройства. Число слотов, занятых ведомым устройством, определяет общую длину данного поля		
Данные RWr безопасности	Поле отображенной позиции входных данных, ориентированных на слова, для ведомого устройства. Содержит 4 слова на каждый слот, начиная со второго слота. Так происходит потому, что последующее поле занимает пространство, предназначенное для первого слота в ведомом устройстве, не связанном с безопасностью		
TPI-T безопасности	Бит	Описание	Значение
	0—15	Данные поддержки протокола (PSD), используемые менеджментом КУБ	0—65535
	16—19	Порядковый номер	0—15
	20—22	Id канала	0—7
	23	зарезервировано	0
	24—27	Тип данных передачи	0—15
	28	Флажок занятости	0 — занят, 1 — не занят
	29	уведомление об ошибке	0
	30	зарезервировано	0 — нет запроса,1 — запрос
	31	Прикладной режим пользователя КУБ	0 — тестовый режим, 1 — режим безопасности
	32—63	CRC 32	CRC 32

7.2 Описание состояния

7.2.1 Обзор

Модель состояния для КУБ, представленная в МЭК 61158, Тип 18, расширена добавлением безопасного состояния, как это показано на рисунке 4.Переход в безопасное состояние осуществляется в условиях наличия ошибок, а само состояние конфигурируется для обеспечения поддержания всех выводов в безопасном состоянии: низкий уровень цифровых выходных сигналов, ноль или выключено, а аналоговые выходы поддерживаются на безопасном уровне, предварительно сконфигурированном пользователем КУБ. Ведущее устройство безопасности М1 управляет состояниями каждого ведомого устройства индивидуально.



Рисунок 4 — Диаграмма состояний

Общий метод установления соединения, верификации ведущего устройства и обновления данных также расширен по сравнению с методом из стандарта МЭК 61158, Тип 18 и включает передачу параметров безопасности и их обработку (см. управление КУБ в разделе 8), а также передачу данных безопасности и контроль (мониторинг) подтверждения их получения.

7.2.2 Ожидание

7.2.2.1 Обзор

Состояние ожидания имеет место перед какими-либо коммуникациями FAL между устройствами.

7.2.2.2 Передача

В случае надлежащего запроса от пользователя FAL к ведущему устройству безопасности M1 подтверждение получения должного ответа от ведущего устройства безопасности S1 приводит к переходу из состояния ожидания в состояние выполнения FAL.

После принятия опросных сообщений от ведущего устройства безопасности M1 ведомое устройство безопасности S1 переходит в состояние выполнения FAL.

7.2.3 Выполнение FAL

7.2.3.1 Обзор

Ведущие устройства безопасности M1 и ведомые устройства безопасности S1 имеют установленные связи (коммуникации), не имеющие отношения к безопасности.

7.2.3.2 Переход

После получения запроса от ведущего устройства безопасности M1 ведомое устройство безопасности S1 переходит в состояние выполнения КУБ.

Любые условия ошибки или сбоя при нахождении в состоянии выполнения FAL или же неудачная попытка перейти в состояние выполнения КУБ приводит к переходу устройства FSCP 8/1 в отказоустойчивое состояние.

7.2.4 Выполнение КУБ

7.2.4.1 Обзор

Состояние выполнения КУБ подробно рассмотрено и объяснено в разделе 8.

7.2.4.2 Переход

Как объяснено в 7.2.6, устройство FSCP 8/1 переходит в отказоустойчивое состояние при обнаружении любых из следующих типов ошибок:

- порядковый номер;
- временное ожидание;

- аутентификация соединения;
- сообщение обратной связи;
- обеспечение целостности данных (CRC 32),
- другие системы обеспечения целостности данных.

Как объяснено в 7.2.7, устройство FSCP 8/1 переходит в отказоустойчивое состояние после получения запроса на программное прерывание.

7.2.5 Отказоустойчивость

7.2.5.1 Обзор

Отказоустойчивое состояние — это состояние, при котором все выводы содержатся в их безопасном состоянии.В случае цифровых выходов, если не указано иначе, это отключенное (или нулевое, низкоуровневое) состояние, а в случае аналоговых выводов, если не указано иначе, это состояние нулевого выхода (т. е., отсутствие напряжения и/или тока).

Как правило, аналоговые выходы конфигурируются с включением безопасного значения, которое накладывается на выход в случае его нахождения в отказоустойчивом состоянии.

7.2.5.2 Переход

Выход из отказоустойчивого состояния возможен только посредством перезапуска ведомого устройства.

7.2.6 Передача данных безопасности и их обработка

7.2.6.1 Обзор

КУБ уровень FSCP 8/1 предоставляет следующие меры обеспечения безопасности:

- порядковый номер;
- временное ожидание;
- аутентификация соединения;
- сообщение обратной связи;
- обеспечение целостности данных (CRC 32);
- другие системы обеспечения целостности данных.

Ведущее устройство безопасности и каждое ведомое устройство безопасности управляет передачами данных безопасности и анализирует их для целей верификации их целостности.

7.2.6.2 Порядковый номер

Сообщения безопасности содержат порядковый номер (RNO) размером 4 бита с установленной последовательностью. RNO изменяется и передается с помощью ведущего устройства безопасности. Ведомое устройство безопасности отражает полученный RNO. Если принят RNO, не входящий в последовательность, то ведомое устройство безопасности переводится в безопасное состояние.

7.2.6.3 Временное ожидание

КУБ использует таймер контроля безопасности и таймеры контроля данных безопасности для обеспечения надежной и непрерывной связи. Менеджмент КУБ устанавливает значение таймера равным от 1 мс до 65 535 мс.

Таймер контроля безопасности используется для подтверждения того, что циклическая коммуникация безопасности осуществляется нормально, а таймеры контроля данных безопасности применяются для подтверждения того, что последующие циклические коммуникации безопасности осуществляются нормально. Станции безопасности контролируют интервал принятия циклических данных, защищенных этим таймером контроля безопасности с помощью обычной информации о защите данных безопасности. Кроме того, ведомые станции безопасности контролируют интервалы принятия циклических данных, защищенных таймерами контроля данных безопасности с помощью обычной информацией о защите данных безопасности.

В таблицах 14 и 15 описана операция таймера контроля безопасности, как для ведущего, так и для ведомого устройства безопасности.

Таблица 14 — Операция таймера контроля безопасности ведущего устройства

Запуск	Прекращение	Прекращение в случае ошибки
Отправка данных безопасности (RNO ≠ 0)	Принятие данных ответа (обновления) ведомого устройства (с тем же RNO, как и отправленный RNO) к которым надлежащим образом была добавлена информация данных защиты	(1) В случае тайм-аута контроля (2) При обнаружении ошибки RNO

Таблица 15 — Операция таймера контроля безопасности ведомого устройства

Запуск	Перезапуск	Прекращение
Отправка данных безопасности (CMD ID = 01h)	Принятие опроса ведущей станции и обновления данных (предварительно: RNO + 1) к которым надлежащим образом была добавлена информация данных защиты	(1) В случае тайм-аута контроля (2) При обнаружении ошибки RNO (3) При получении запроса программного прекращения

Таблица 16 — Операция таймера контроля данных безопасности

Запуск	Перезапуск	Прекращение
Принятие циклических I/O данных безопасности (CMD ID = 0Fh)	Принятие опроса ведущей станции и обновления данных (предварительно: RNO+2) к которым надлежащим образом была добавлена информация данных защиты	(1) В случае тайм-аута контроля (2) При обнаружении ошибки RNO (3) При получении запроса программного прекращения
Примечание — Ведомые станции безопасности имеют два таймера контроля данных безопасности. Таймер контроля данных безопасности запускается при приеме циклических I/O данных безопасности (CMS ID = 0Fh and RNO = n), а принятие двух последующих данных (RNO = n + 2) перезапускает его. Другой таймер контроля данных безопасности запускается после получения циклических I/O данных безопасности (CMD ID = 0Fh and RNO = n + 1), а принятие двух последующих данных (RNO = n + 3) перезапускает его.		

Поведение ведущего устройства безопасности в случае истечения таймера контроля безопасности описывается следующим образом:

1) отказоустойчивая обработка, например, очистка S-RX (обнуление), доставленных пользователю КУБ;

2) уведомление пользователя КУБ об ошибках;

3) переход в состояние ожидания.

Поведение ведомого устройства безопасности в случае истечения таймера контроля безопасности описывается следующим образом:

1) отказоустойчивая обработка, например, прерывание выходных сигналов, отправляемых внешним устройствам;

2) уведомление пользователя КУБ об ошибках;

3) переход в безопасное состояние.

7.2.6.4 Аутентификация соединения

Аутентификация соединения реализуется набором ID соединения безопасности (канальных ID) и номером станции. Каждое ведомое устройство безопасности использует 3-битный ID канала, описывающий систему сети безопасности данного устройства. Это предоставляет SRC вплоть до 8 систем сети безопасности. В рамках коммуникационной системы функциональной безопасности ID канала должны назначаться уникально. Сообщения безопасности всегда содержат ID канала.

7.2.6.5 Сообщение обратной связи

Сообщение обратной связи поступает от каждого ведомого устройства, подтверждающего получение сообщений от ведущего устройства. Сообщение обратной связи содержит информацию о статусе ошибки, поступившую от ведомого устройства, а также подтверждение RNO, ID канала, командный ID и поле данных поддержки протокола.

7.2.6.6 Целостность данных

CRC 32 для FSCP 8/1 вычисляется согласно приложению А. Интенсивность возникновения остаточной ошибки для FSCP 8/1 рассматривается в 9.5.2.

7.2.6.7 Различные системы обеспечения целостности данных

Различие между сообщениями, значимыми и не значимыми для безопасности обеспечивается подтверждением уникальности сообщений безопасности включением грамотно отформатированной контрольной суммы CRC (32 бита), 16-битового поля данных поддержки протокола, 8-битового командного ID, 3-битового ID канала и 4-битового RNO. Протокол МЭК 61158,Тип 18 использует другой CRC алгоритм (16-битовый CRC) и не включает поле данных поддержки протокола, командный ID, ID канала или RNO.

7.2.7 Программное прерывание (прекращение)

Обработка программного прерывания используется, когда ведущее устройство безопасности запрашивает ведомое устройство безопасности о прерывании коммуникаций. Ведомое устройство безопасности, получающее запрос на программное прерывание, переходит в отказоустойчивое состояние (останавливает внешние выходы) и затем немедленно прерывает коммуникации.

8 Управление коммуникационным уровнем безопасности

8.1 Общие положения

Приложения, связанные с безопасностью, используют следующие услуги для конфигурации коммуникационной системы безопасности:

- установка соединения;
- верификация конфигурации ведомого устройства;
- передача параметров ведомому устройству безопасности.

8.2 Установление соединения и подтверждение обработки

После установления соединения, начальная конфигурация подтверждается проверкой того, что точки SAREP располагаются в устройствах безопасности и что циклическая передача данных безопасности поддерживается. Этот процесс описан в таблице 17.

Таблица 17 — Подробное рассмотрение установления соединения и ожидания подтверждения

Тип SAREP	Подробность обработки
Ведущее устройство безопасности	(1) Подтвердить, что ведомое устройство является ведомым устройством безопасности (подтверждается передачей циклических данных безопасности) (2) Подтвердить, что ведомое устройство безопасности приняло команду установки соединения (подтверждается проверкой идентичности CMD и PSD ответных данных отправленным данным) (3) Передать значение таймера контроля безопасности
Ведомое устройство безопасности	(1) Подтвердить, что ведущее устройство является ведущим устройством безопасности (подтверждается передачей циклических данных безопасности) (2) Получить значение таймера контроля безопасности и зарегистрировать это значение внутри

Ведущая станция безопасности передает RNO = 0, отправляя команду установления соединения.

8.3 Верификация ведомого устройства безопасности

8.3.1 Общие положения

Выполнение верификации информации об изделии подтверждает, что действительно подключенные ведомые станции безопасности соответствуют ведомым станциям безопасности, которые на текущий момент настроены на параметры сети ведущей станции безопасности для обнаружения неправильных соединений и конфигураций. Заменяющее ведомое устройство, не являющееся устройством безопасности, обнаруживается и отключается во время запуска.

8.3.2 Процесс верификации информации ведомого устройства безопасности

Процесс верификации информации ведомого устройства безопасности описан в таблице 18.

Таблица 18 — Подробное рассмотрение выполнения верификации информации ведомого устройства

Тип SAREP	Подробность выполнения
Ведущее устройство безопасности	(1) Считывание информации об изделии с ведомых устройств и верификация этой информации, сравнением ее с информацией об изделии, настроенной на параметры сети. (2) После верификации — отправка информации об изделии на ведомые станции безопасности

Окончание таблицы 18

Тип SAREP	Подробность выполнения
Ведомое устройство безопасности	(1) Верификация информации об изделии для ведомого устройства, сравнением ее с информацией об изделии, полученной от ведущего устройства безопасности

Выполнение верификации информации ведомого устройства верифицирует информацию об изделии для ведомого устройства безопасности.

8.3.3 Передача параметров ведомому устройству безопасности

Параметры конфигурации ведомого устройства безопасности передаются от ведущего устройства безопасности каждому ведомому устройству безопасности. Процесс описан в таблице 19.

Таблица 19 — Подробное рассмотрение передачи параметров ведомого устройства безопасности

Тип SAREP	Подробность обработки
Ведущее устройство безопасности	(1) Считывание CRC 32 параметров ROM хранилища с ведомых станций безопасности и верификация этого CRC 32 с CRC 32 параметров хранилища ROM, зарегистрированных пользователем КУБ. (2) Отправление параметров ведомого устройства безопасности ведомому устройству безопасности
Ведомое устройство безопасности	(1) Принятие параметров ведомого устройства безопасности от ведущего устройства, подтверждение значений настроек и выполнение обработки внутренней регистрации

9 Системные требования

9.1 Индикаторы и коммутаторы

9.1.1 Коммутаторы

Каждое устройство безопасности должно предоставлять физические средства для настройки следующего:

- онлайн — настроить этот режим на установление канала данных;
- номер станции: 0 — ведущее устройство безопасности, 1—64 — ведомое устройство безопасности и требуется только для ведомого устройства безопасности;
- ID канала — от 0 до 7;
- скорость в бодах — 156 кбит/ч, 625 кбит/с, 2,5 Мбит/с, 5 Мбит/с, 10 Мбит/с — требуется только для ведущего устройства безопасности;
- сброс — требуется только для ведомого устройства безопасности.

Каждое устройство безопасности не обязательно предоставляет физические средства для настройки следующего:

- число занятых слотов — слоты станций (1 или 2), занятые одной ведомой станцией безопасности;
- линейный тест 1 — верифицирует, что ведущее устройство способно соединяться со всеми ведомыми станциями;
- линейный тест 2 — верифицирует, что ведущее устройство способно соединяться с определенной ведомой станцией;
- тест контроля параметров — верифицирует содержание параметров;
- испытание аппаратуры — верифицирует каждый индивидуальный модуль на нормальное функционирование.

9.1.2 Индикаторы

Требования к индикатору описаны в таблице 20, используя следующие обозначения:

О — обязательно;

Д — дополнительно.

Тип индикатора, цвет и форма не установлены. Также, в случаях использования компьютеров или других устройств с экранами, может поддерживаться индикация на экране.

Таблица 20 — Светодиоды монитора (устройства контроля)

Порядковый номер	Название светодиода	Описание	Ведущая станция безопасности	Удаленная станция устройства безопасности	Удаленная I/O станция безопасности
1	RUN	Горит: нормальный модуль. Не горит: ошибка сторожевого таймера	О	Д	Д
2	ERR	Горит: ошибка коммуникации со всеми станциями. Этот светодиод загорается, когда случается одно из следующих событий: - ошибка настройки коммутатора; - дуплицирование ведущей станции на одной линии; - ошибка содержания параметра; - активирован таймер контроля канала данных; - повреждение кабеля; - кабель зашумлен на пути передачи данных. Мигает: ошибка коммуникаций	О	Д	Д
3	L RUN	Горит: Осуществляется выполнение передачи в канале данных	О	Д	Д
4	L ERR	Горит: Ошибка коммуникаций (сама станция). Мигает: Настройка типа коммутатора изменилась при включении питания	О	Д	Д

9.2 Руководство по установке

Настоящий стандарт описывает протокол и услуги для системы коммуникаций безопасности, основанной на МЭК 61158, Тип 18.Тем не менее, использование устройств безопасности вместе с протоколом безопасности, описанном в настоящем стандарте, требует надлежащей установки. Все устройства соединенные с системой коммуникаций безопасности, заданной в настоящем стандарте, должны выполнять требования SELV/PELV, описанные в соответственных стандартах МЭК, таких как МЭК 60204-1.

Дополнительную информацию по установке можно также найти в [43] и [44].

9.3 Время реакции функции безопасности

9.3.1 Общие положения

Как упоминалось в 5.3, встроенный сторожевой таймер используется для предоставления временного ожидания каждого канала вывода на каждом ведомом выводном устройстве безопасности. Он обеспечивает время реакции функции безопасности, являющееся временем между обнаружением события на ведомом устройстве ввода безопасности и реакцией соответствующего канала(ов) вывода на ведомом устройстве(ах) вывода безопасности.

Время реакции функции безопасности состоит из времени передачи по полевой шине от ведомого устройства ввода безопасности ведущему устройству и от ведущего устройства безопасности ведомому устройству вывода безопасности, включая возможные повторения PDU безопасности, вызванные ошибками передачи, время на обработку на каждом ведомом устройстве безопасности (ввода и вывода) и время на обработку в SRC.

Если время реакции функции безопасности конкретного канала вывода ведомого выводного устройства безопасности превышено, то соответствующий канал вывода переводится в его безопасное состояние, которое, как правило, является обесточенным состоянием.

9.3.2 Вычисление времени

Встроенный сторожевой таймер, предоставляющий временное ожидание каждого канала вывода на каждом ведомом выводном устройстве безопасности, обеспечивает время реакции функции безопасности, являющееся временем между обнаружением события на ведомом вводном устройстве безопасности и реакцией соответствующего канала(ов) вывода на ведомом выводном устройстве(ах) безопасности, исключая время на обработку ввода безопасности.

Время реакции функции безопасности состоит из времени передачи по полевой шине от ведомого вводного устройства безопасности ведущему устройству и от ведущего устройства безопасности ведомому выводному устройству безопасности, включая возможные повторения PDU безопасности, вызванные ошибками передачи, время на обработку на каждом ведомом устройстве безопасности (ввода и вывода) и время на обработку в SRC.

Время реакции функции безопасности вычисляется, как сумма элементов с (a) по (e) из таблицы 21, учитывая термины, заданные в таблице 22.

Примечания

1 Ведущее устройство безопасности вычисляет время тайм-аута на основе времени контроля обновления данных безопасности — ((WDT x n) x 2).

2 (WDT x n) x 2 — это время, требующееся для ведущего устройства безопасности, чтобы отправить коммуникационные данные.

Таблица 21 — Вычисление времени реакции функции безопасности

Элемент	Максимум
(a) Время реакции устройства ввода	DT1
(b) Время обработки ведомого вводного устройства безопасности	Время фильтрации шума + Время обработки удаленной станции ввода
(c) Время контроля от ввода данных безопасности до вывода данных безопасности	Время контроля данных безопасности
(d) Время обработки ведомого выводного устройства безопасности	Время обработки удаленной станции вывода
(e) Время реакции устройства вывода	DT2
Общее значение	(a)+(b)+(c)+(d)+(e)

Таблица 22 — Определение терминов времени реакции функции безопасности

Элемент	Определение
LS	Время сканирования канала (Link Scan Time), установленное производителем
n	Значение после запятой в LS/WDT (округленное)
SRRP	Время обработки ответа обновления данных безопасности. Установлено производителем
m	Значение после запятой в SRRP/(WDT x n) (округленное)
Время фильтрации шума	Конфигурируется в настройках удаленной станции безопасности (значения настроек: от 1 до 50 мс)
DT1, DT2	Время реакции датчика или устройства управления назначением выходного сигнала. Установлено производителем.
Время контроля данных безопасности	Время, установленное в сетевом параметре. В качестве меры используется значение, полученное из следующей формулы: Время контроля обновления данных безопасности x 2 – ((WDT x n) xm) — 10 [мс]
Время контроля обновления данных безопасности	Время, устанавливаемое в сетевом параметре. В качестве меры используется значение, полученное из следующей формулы. В пусковом режиме (triggered mode): (WDT x n) x 3 + (WDT x n) x m x 2 + (WDT x α) [мс] В автономном режиме: (WDT x n) x 3 + LS + (WDT x n) x m x 2 + (WDT x α) [мс], где: α = 0 для LS ≤ 1,5 мс и α = 1 для LS > 1,5 мс

Окончание таблицы 22

Элемент	Определение
WDT (Сторожевой таймер)	Время, устанавливаемое параметром конфигурации
Пусковой режим	Режим, который выполняет канал данных, когда сканирование последовательности и сканирование канала синхронизированы и начинаются одновременно
Автономный режим	Режим, который выполняет канал данных без синхронизации с программой последовательности

9.4 Длительность запросов на обслуживание

Длительность запроса на обслуживание приложением, связанным с безопасностью, на коммуникационном уровне безопасности должна быть достаточной по продолжительности для того, чтобы запрос был обнаружен приложением в течение наибольшего времени реакции функции безопасности.

9.5 Ограничения на вычисление системных характеристик

9.5.1 Системные характеристики

Должны быть учтены следующие базовые данные:

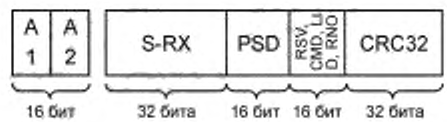
- МЭК 61158, Тип 18: без ограничений;
- максимальное число слотов безопасности: 64;
- минимальное время цикла сканнера: 10 мс;
- максимальное число бит I/O, относящихся к безопасности, приходящееся на один PDU безопасности — ведущий к ведомому: 208;
- максимальное число бит I/O, относящихся к безопасности, приходящееся на один PDU безопасности — ведомый к ведущему: 7168.

9.5.2 Частота возникновения остаточных ошибок (Λ)

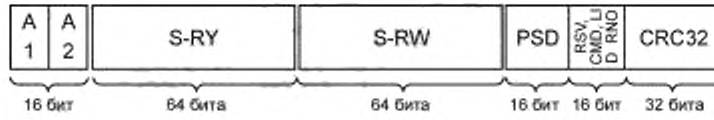
Частота возникновения остаточных ошибок, Λ, для системы безопасности непосредственно связана с числом ведомых устройств безопасности и соответствующим им числом занятых слотов в конфигурации системы.

В таблице 23 показано влияние числа занятых слотов ведомых устройств безопасности на результирующую длину кадра для соответствующего PDU безопасности.

Таблица 23 — Число занятых слотов и данные безопасности

Занятый слот	Структура PDU безопасности		Длина кадра, бит
	SAR	Структура	
1	Ведущая станция безопасности → Ведомая станция безопасности		112
1	Ведомая станция безопасности → Ведущая станция безопасности		112

Окончание таблицы 23

Занятый слот	Структура PDU безопасности		Длина кадра, бит
	SAR	Структура	
2	Ведущая станция безопасности → Ведомая станция безопасности		208
	Ведомая станция безопасности → Ведущая станция безопасности		208

Λ можно получить из таблиц 24 и 25, основываясь на длине кадра и числе ведомых устройств безопасности в системе безопасности.

Таблица 24 — Частота возникновения остаточных ошибок Λ (занятые слоты: 1)

Вероятность частоты возникновения остаточных ошибок, R_{pCRC32}	Число ведомых устройств безопасности	Минимальное время цикла,мс	Частота возникновения остаточных ошибок, Λ
$1{,}01 \times 10^{-24}$	1	10,0	$7{,}27 \times 10^{-17}$
	8	10,0	$5{,}81 \times 10^{-16}$
	16	10,0	$1{,}16 \times 10^{-15}$
	32	10,0	$2{,}33 \times 10^{-15}$
	42	10,0	$3{,}05 \times 10^{-15}$

Таблица 25 — Частота возникновения остаточных ошибок Λ (занятые слоты: 2)

Вероятность частоты возникновения остаточных ошибок, R_{pCRC32}	Число ведомых устройств безопасности	Минимальное время цикла,мс	Частота возникновения остаточных ошибок, Λ
$2{,}05 \times 10^{-19}$	1	10,0	$1{,}47 \times 10^{-11}$
	8	10,0	$1{,}18 \times 10^{-10}$
	16	10,0	$2{,}36 \times 10^{-10}$
	32	10,0	$4{,}72 \times 10^{-10}$

Результирующая частота возникновения остаточных ошибок для всех описанных конфигураций FSCP 8/1 поддерживается на уровне ниже 10^{-7} (10^{-9} в зависимости от сети), что удовлетворяет требованиям УПБ 3 и категории 4.

9.6 Техническое обслуживание

Не существует никаких конкретных требований к техническому обслуживанию, зависящих от КУБ.

Примечания

1 Спецификации для системного поведения в случае ремонта и замены устройства не охватываются настоящим стандартом. Спецификация данных действий и ответственностей не отражается на спецификации услуг и

протоколов. Как правило, она является частью плана менеджмента функциональной безопасности. Тем не менее, ремонт, замена, также как и техническое обслуживание, общее подтверждение соответствия безопасности, общее функционирование, модификации, усовершенствования и списывание или удаление, в соответствии с МЭК 61508 являются важными проблемами, которые следует учитывать. Также рекомендуется обратиться к поставщику устройства или системы.

2 Для получения информации о программировании SRP и настройке параметров устройств безопасности настоятельно рекомендуется обратится к поставщику устройства или системы. Кроме того, рекомендуется учесть документы [43] и [44], в которых для пользователя системы CC-LINK-Safety представлена дополнительная информация, например, контрольные списки.

3 Дополнительные требования для технического обслуживания, как и другие требования, описаны в МЭК 61508, МЭК 61511 и/или МЭК 62061.

9.7 Руководство по безопасности

Поставщик ведомых устройств безопасности, использующий КУБ в соответствии со спецификациями КУБ, предоставленными в настоящем стандарте, должен подготовить надлежащее руководство по безопасности в соответствии с МЭК 61508. Данное руководство по безопасности должно также включать требования к установке, как это определено в 9.2, также как и руководящие указания для конфигурирования коммутаторов устройств. Кроме коммутаторов, соответствующих МЭК 61158, Тип 18, данные руководящие указания должны включать в себя утверждение о том, что все устройства безопасности в одной сети должны быть сконфигурированы, используя один ID канала. См. 9.1.1.

Для коммуникационной системы безопасности, основанной на МЭК 61158, Тип 18, настоятельно рекомендуется учитывать спецификации [43]—[45].

Примечание — Хорошей инженерной практикой перед началом внедрения устройства безопасности является общение с CLPA для установления поправок к руководству по внедрению и/или требованиям к внедрению.

10 Оценка

За разработку устройства в соответствии с надлежащим процессом разработки и в соответствии со стандартами безопасности (см. МЭК 61508, МЭК 61511, МЭК 62061, ...) и значимыми правовыми нормами (например, Европейскими указаниями по охране труда в машиностроении) ответственность несет производитель этого устройства.

Приложение А
(справочное)

Дополнительная информация для удовлетворяющих функциональной безопасности профилей коммуникаций CPF 8

А.1 Вычисление хэш-функции

CRC32 для FSCP 8/1 вычисляют, используя следующий алгоритм:

$$G(x) = x32 + x26 + x23 + x22 + x16 + x12 + x11 + x10 + x8 + x7 + x5 + x4 + x2 + x + 1$$

Этот алгоритм определен в ИИЭР 802.3 [28].

Приложение В
(справочное)

Информация для оценки удовлетворяющих функциональной безопасности профилей коммуникаций CPF 8

Информация о тестовых лабораториях, которые испытывают и подтверждают соответствие изделий FSCP8/1 стандарту МЭК 61784-3-8, может быть получена у национальных комитетов МЭК или у следующих организаций:

CC-Link Partner Association
6F Meiji Yasuda Seimei Ozone Bldg.
3-15-58, Ozone, Kita-ku
Nagoya 462-0825
JAPAN
Телефон: +81 52 919 1588
Факс: +81 52 916 8655
E-mail: gost.e-ecolog.ru
URL: gost.e-ecolog.ru

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60204-1	IDT	ГОСТ Р МЭК 60204-1—2007 «Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования»
IEC 61131-2	IDT	ГОСТ IEC 61131-2—2012 «Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания»
IEC 61158 (все части)	—	*
IEC 61158-2	—	*
IEC 61158-3-18	—	*
IEC 61158-4-18	—	*
IEC 61158-5-18	—	*
IEC 61158-5-10	—	*
IEC 61158-6-18	—	*
IEC 61326-3-1	—	*
IEC 61326-3-2	—	*
IEC 61508 (все части)	IDT	ГОСТ Р МЭК 61508—2012 (все части) «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
IEC 61511 (все части)	IDT	ГОСТ Р МЭК 61511-1—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов»
IEC 61784-1	—	*
IEC 61784-3:2010	—	*
IEC 62061	IDT	ГОСТ Р МЭК 62061—2013 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью»

* Соответствующий национальный стандарт отсутствует.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] IEC 60050 (all parts), International Electrotechnical Vocabulary

Примечание — См. также Многоязыковой словарь — Электричество, Электроника и Телекоммуникации (доступен на CD-ROM и по адресу <gost.e-ecolog.ru >).

[2] IEC/TS 61000-1-2, Electromagnetic compatibility (EMC) — Part 1-2: General — Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena

[3] IEC 61131-6, Programmable controllers — Part 6: Functional safety

[4] IEC 61496 (all parts), Safety of machinery — Electro-sensitive protective equipment

[5] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

[6] IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

[7] IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels

[8] IEC 61784-2, Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3

[9] IEC 61784-4 Industrial communication networks — Profiles — Part 4: Secure communications for fieldbuses

[10] IEC 61784-5 (all parts), Industrial communication networks — Profiles — Part 5: Installation of fieldbuses — Installation profiles for CPF x

[11] IEC 61800-5-2, Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional

[12] IEC 61918, Industrial communication networks — Installation of communication networks in industrial premises

[13] IEC/TR 62059-11, Electricity metering equipment — Dependability — Part 11: General concepts

[14] IEC/TR 62210, Power system control and associated communications — Data and communication security

[15] IEC 62280-1, Railway applications — Communication, signalling and processing systems — Part 1: Safety-related communication in closed transmission systems

[16] IEC 62280-2, Railway applications — Communication, signalling and processing systems — Part 2: Safety-related communication in open transmission systems

[17] IEC 62443 (all parts), Industrial communication networks — Network and system security

[18] ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards

[19] ISO/IEC 2382-14, Information technology — Vocabulary — Part 14: Reliability,maintainability and availability

[20] ISO/IEC 2382-16, Information technology — Vocabulary — Part 16: Information theory

[21] ISO/IEC 7498 (all parts), Information technology — Open Systems Interconnection — Basic Reference Model

[22] ISO 10218-1, Robots for industrial environments — Safety requirements — Part 1: Robot

[23] ISO 12100-1, Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology

[24] ISO 13849-1, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

[25] ISO 13849-2, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

[26] ISO 14121, Safety of machinery — Principles of risk assessment

[27] EN 954-1:1996,Safety of machinery — Safety related parts of control systems — General principles for design

[28] IEEE 802.3, IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks –Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[29] ANSI/ISA-84.00.01—2004 (all parts), Functional Safety: Safety Instrumented Systems for the Process Industry Sector

[30] VDI/VDE 2180 (all parts), Safeguarding of industrial process plants by means of process control engineering

[31] GS-ET-26, Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("Principles for Test and Certification of Bus Systems for Safety relevant Communication")

[32] ANDREW S. TANENBAUM, Computer Networks, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029

[33] W. WESLEY PETERSON, Error-Correcting Codes, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0

[34] BRUCE P. DOUGLASS, Doing Hard Time, 1999, Addison-Wesley, ISBN 0-201 49837-5

[35] New concepts for safety-related bus systems, 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications ", May 1998, from Dr. Michael Schäfer, BG-Institute for Occupational Safety and Health.

[36] DIETER CONRADS, Datenkommunikation, 3rd Edition 1996, Vieweg, ISBN 3-528 245891

[37] German IEC subgroup DKE AK 767.0.4: EMC and Functional Safety, Spring 2002

[38] NFPA79 (2002), Electrical Standard for Industrial Machinery

[39] GUY E. CASTAGNOLI, On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland

[40] GUY E. CASTAGNOLI, STEFAN BRÄUER, AND MARTIN HERRMANN, Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits, June 1993, IEEE Transactions On Communications, Volume 41, No. 6

[41] SCHILLER F and MATTES T: An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57—80, Technical University Press, Łódź,Poland, 2006

[42] SCHILLER F and MATTES T: Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006

[43] CC-Link Safety Specifications, Overview/Protocol, BAP-C1603-001, CLPA

[44] CC-Link Safety Specifications, Implementation, BAP-C1603-002, CLPA

[45] CC-Link Safety Specifications, Profiles, BAP-C1603-003, CLPA

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 Т51

Ключевые слова: промышленные сети, профили, функциональная безопасность полевых шин, спецификации для CPF 8

Редактор *Д.Е. Титов*
Технический редактор *В.Н. Прусакова*
Корректор *С.В. Смирнова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 19.12.2016. Подписано в печать 28.12.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21. Тираж 27 экз. Зак. 3325

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru