ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61784-3-1— 2016

Промышленные сети

ПРОФИЛИ

Часть 3-1

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 1

(IEC 61784-3-1:2010, IDT)

Издание официальное

Москва
Стандартинформ
2017

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. № 1883-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61784-3-1:2010 «Промышленные сети. Профили. Часть 3-1. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 1» (IEC 61784-3-1:2010 «Industrial communication networks — Profiles — Part 3-1:Functional safety fieldbuses — Additional specifications for CPF 1», 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 (www.gost.ru)

Содержание

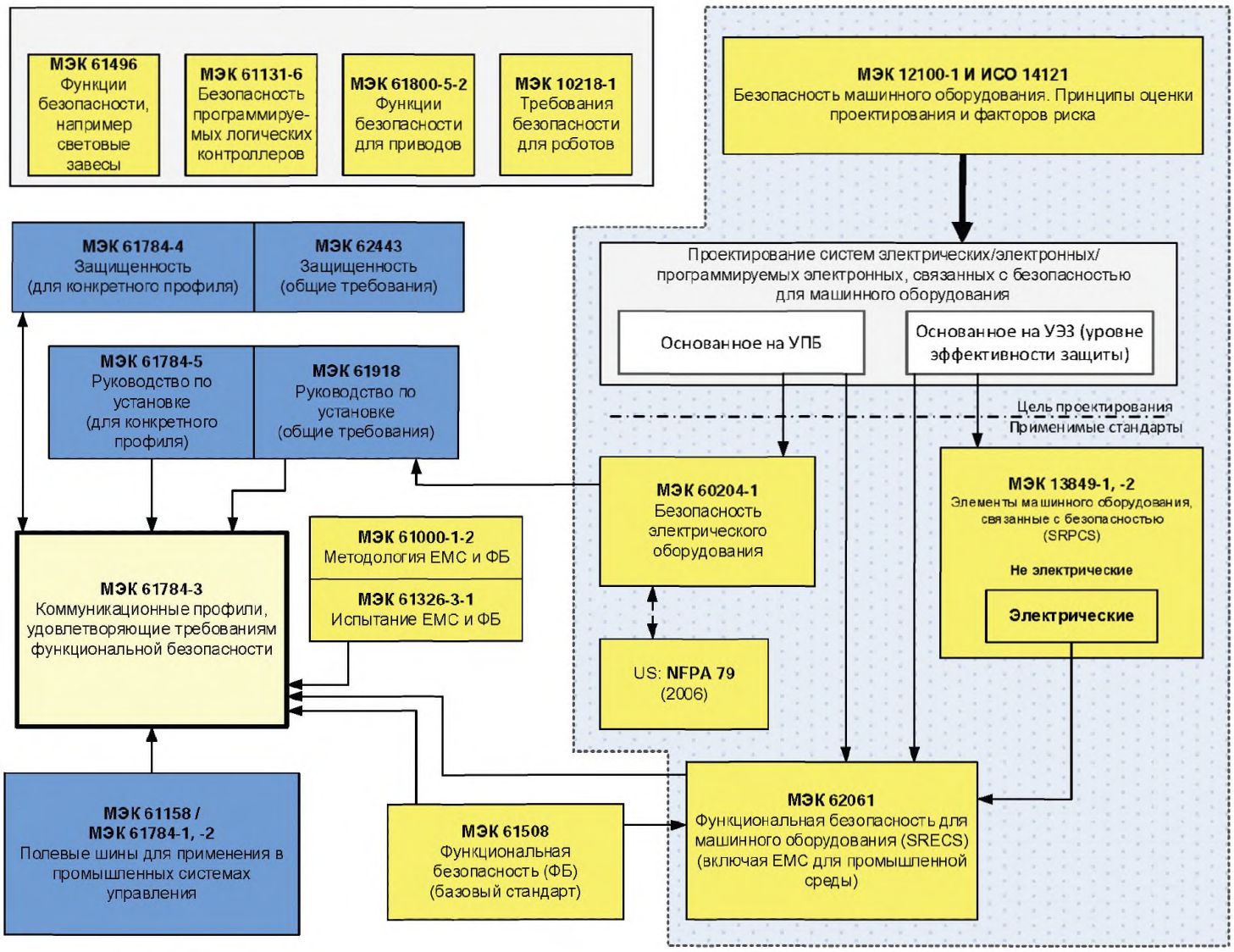
Введение

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.

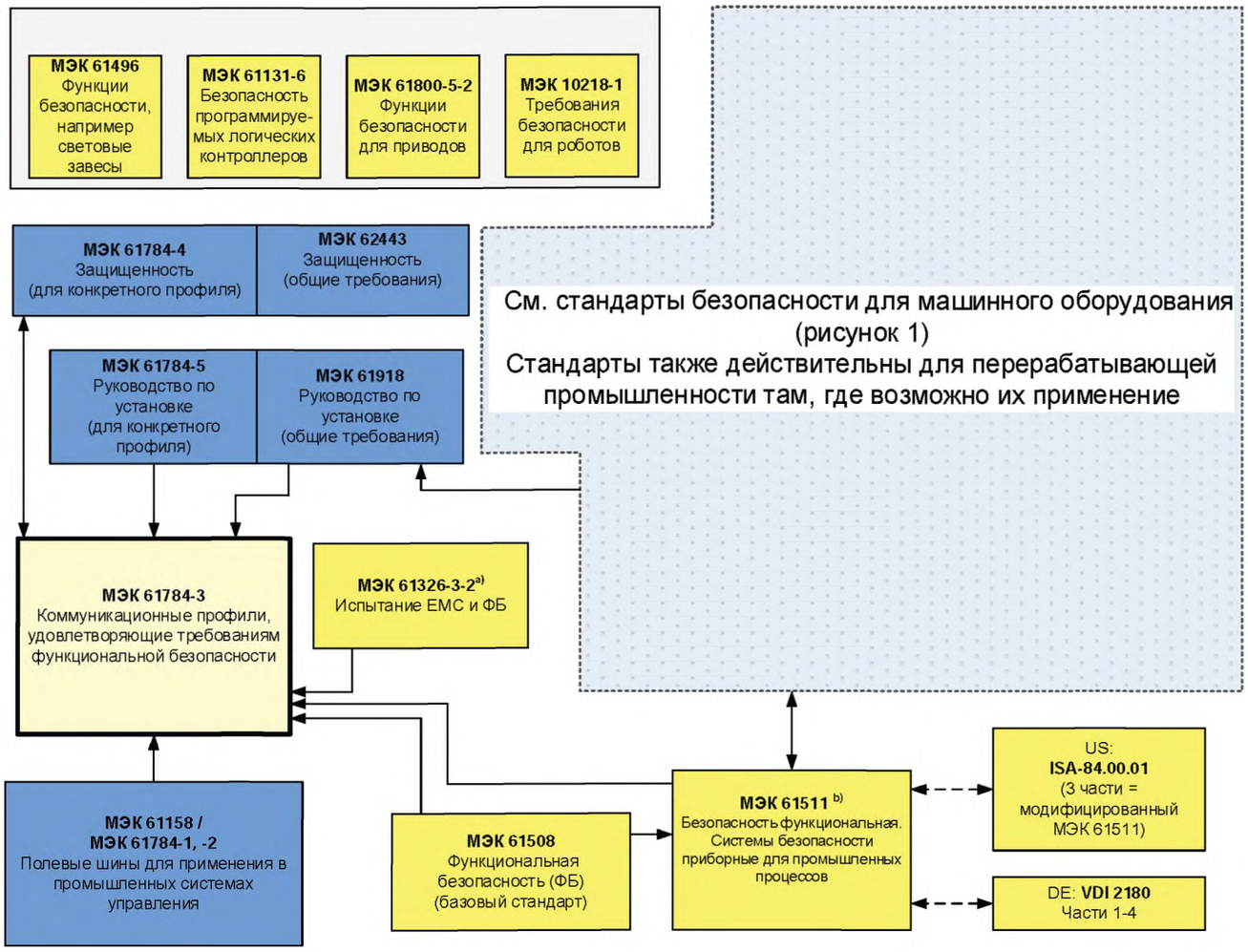
На рисунке 1 представлена связь настоящего стандарта с соответствующими стандартами, посвященными функциональной безопасности и полевым шинам в среде машинного оборудования.



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

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

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



Обозначения:

(желтый) - стандарты, связанные с безопасностью;

(голубой) - стандарты, связанные с полевыми шинами;

(бледно желтый) - настоящий стандарт

a) Для установленных электромагнитных сред; в противном случае МЭК 61326-3-1.
b) Ратифицирован EN.

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

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 обеспечения функциональной безопасности для конкретного уровня полноты функциональной безопасности (УПБ), для которого определен соответствующий ему профиль коммуникации, удовлетворяющий требованиям функциональной безопасности.

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;
- индивидуально профили, удовлетворяющие 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.

2 Патентная декларация

Международный электротехнический комитет (МЭК) обращает внимание на то, что соблюдение требований настоящего стандарта может включать использование патентов, относящихся к профилям коммуникаций, соответствующих требованиям функциональной безопасности. Для семейства 1 патенты приведены ниже, где обозначение [xx] указывает на держателя патента:

US 6,999,824 [FF] Система и метод для реализации приборной системы безопасности в архитектуре полевых шин

МЭК не занимается подтверждением обоснованности, подтверждением соответствия и областью применения прав данных патентов.

Правообладатели на данные патенты заверили МЭК, что они готовы рассмотреть использование лицензий на разумных и недискриминационных условиях и положениях с заявителями по всему миру. Такие заявления обладателей прав на данные патенты зарегистрированы в МЭК.

Информация доступна посредством:

[FF] Fieldbus Foundation
9005 Mountain Ridge Drive
Bowie Bldg. - Suite 190
Austin, TX 78759-5316
USA
Тел.: +1 512 794 8890

Обращаем внимание на то, что некоторые элементы данного документа могут быть субъектом патентных прав, отличных от указанных ранее. МЭК не несет ответственности за идентификацию (частично или полностью) подобных патентных прав.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Промышленные сети

ПРОФИЛИ

Часть 3-1

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 1

Industrial communication networks. Profiles. Part 3-1. Functional safety fieldbuses. Additional specifications for CPF 1

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт описывает коммуникационный уровень безопасности (услуги и протокол) на основе CPF 1, представленного в МЭК 61784-1 и МЭК 61158, Типы 1 и 9. Настоящий стандарт идентифицирует принципы для осуществления коммуникаций, удовлетворяющих требованиям функциональной безопасности, определенным в МЭК 61784-3, что важно для этого 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 управлении 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, удовлетворяющей требованиям функциональной безопасности внутри этой системы. Но в соответствии с настоящим стандартом реализации выбранного профиля коммуникации, удовлетворяющей требованиям функциональной безопасности, в стандартном устройстве не достаточно для того, чтобы устройство считалось устройством безопасности.

2 Нормативные ссылки

В настоящем стандарте используются нормативные ссылки на следующие целые документы или на их части, незаменимые для применения данного документа. В случае датированных ссылок действует только цитируемое издание. Для недатированных ссылок действует самое позднее издание документа, на который производится ссылка (включая любые внесенные в него поправки).

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

---

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

Издание официальное

IEC 61158-2, Industrial communication networks — Fieldbus specifications — Part 2: Physical layer specification and service definition (Сети связи промышленные. Спецификации полевой шины. Часть 2. Спецификация физического уровня и определение сервиса)

IEC 61158-3-1, Industrial communication networks — Fieldbus specifications — Part 3-1: Datalink layer service definition — Type 1 elements (Сети связи промышленные. Спецификации полевой шины. Часть 3-1. Определение сервиса канального уровня. Элементы Типа 1)

IEC 61158-4-1, Industrial communication networks — Fieldbus specifications — Part 4-1: Datalink layer protocol specification — Type 1 elements (Сети связи промышленные. Спецификации полевой шины. Часть 4-1. Спецификация протокола канального уровня. Элементы Типа 1)

IEC 61158-5-5, Industrial communication networks — Fieldbus specifications — Part 5-5: Application layer service definition — Type 5 elements (Сети связи промышленные. Спецификации полевой шины. Часть 5-5. Определение сервиса прикладного уровня. Элементы Типа 5)

IEC 61158-5-9, Industrial communication networks — Fieldbus specifications — Part 5-9: Application layer service definition — Type 9 elements (Сети связи промышленные. Спецификации полевой шины. Часть 5-9. Определение сервиса прикладного уровня. Элементы Типа 9)

IEC 61158-6-5, Industrial communication networks — Fieldbus specifications — Part 6-5: Application layer protocol specification — Type 5 elements (Сети связи промышленные. Спецификации полевой шины. Часть 6-5. Спецификация протокола прикладного уровня. Элементы Типа 5)

IEC 61158-6-9, Industrial communication networks — Fieldbus specifications — Part 6-9: Application layer protocol specification — Type 9 elements (Сети связи промышленные. Спецификации полевой шины. Часть 6-9. Спецификация протокола прикладного уровня. Элементы Типа 9)

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

IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 1: General requirements (Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 1. Общие требования)

IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety related systems (Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью)

IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 3: Software requirements (Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению)

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations (Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения)

IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector (Безопасность функциональная. Системы безопасности приборные для промышленных процессов)

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

IEC 61784-3:2010, Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions (Сети связи промышленные. Профили. Часть 3. Функциональная безопасность полевых шин. Общие правила и определения профиля)

IEC 61918, Industrial communication networks — Installation of communication networks in industrial premises (Сети связи промышленные. Установка сетей связи в промышленных помещениях)

IEC 62280-1:2002, Railway applications — Communication, signalling and processing systems — Part 1: Safety-related communication in closed transmission systems (Железнодорожные приложения. Системы связи, сигнализации и обработки данных. Часть 1. Безопасная связь в закрытых системах передачи)

ISO/IEC 8802-3[1)], Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 3: Carrier sense multiple

[1)] Отменен. Действует ISO/IEC/IEEE 8802-3:2014.

access with collision detection (CSMA/CD) access method and physical layer specifications (Информационные технологии. Телекоммуникации и обмен информацией между системами. Локальные и общегородские сети. Специальные требования. Часть 3. Множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD) и определение физического уровня)

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте используются следующие термины и определения:

3.1.1 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** (black channel): Канал связи, для которого отсутствуют доказательства того, что проектирование и подтверждение соответствия были проведены в соответствии с МЭК 61508.

3.1.1.3 **мост** (bridge): Абстрактное устройство, соединяющее многочисленные сегменты сети на всем протяжении уровня канала данных.

3.1.1.4 **канал связи** (communication channel): Логическое соединение между двумя конечными точками внутри коммуникационной системы.

3.1.1.5 **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.

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

3.1.1.7 **циклический контроль избыточности** (Cyclic Redundancy Check, CRC): Получаемые из блока данных (значений) избыточные данные, 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 настоящем стандарте в отношении избыточных данных.

2 См. также [34], [35].

3.1.1.8 **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.

3.1.1.9 **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.

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

Примечание — Международный электротехнический словарь (IEV 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]

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

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

3.1.1.13 **последовательность проверки кадра** [frame check sequence (FCS)]: Дополнительные данные, полученные для блока данных DLPDU (кадра) с помощью хеш-функции, которые запоминаются и передаются вместе с этим блоком данных, для обнаружения искажения данных.

Примечания

1 Значение FCS может быть получено, используя, например, CRC или другую хеш-функцию.

2 См. также [34], [35].

3.1.1.14 **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/TR 62210, модифицировано]

3.1.1.15 **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.

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

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

[ИСО/МЭК 2382-16.02.01, модифицировано]

3.1.1.18 **приемник сообщений** (message sink): Часть коммуникационной системы, в которую, предполагается, поступают сообщения.

[ИСО/МЭК 2382-16.02.03]

3.1.1.19 **источник сообщения** (message source): Часть коммуникационной системы, из которой, предполагается, возникают сообщения.

[ИСО/МЭК 2382-16.02.02]

3.1.1.20 **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]

3.1.1.21 **контрольная проверка** (proof test): Периодическая проверка, выполняемая для того, чтобы обнаружить отказы в системе, связанной с безопасностью, чтобы, при необходимости, система могла быть возвращена в «исходное» состояние или в наиболее близкое к нему, насколько это практически возможно.

Примечание — Контрольная проверка предназначена подтвердить, находится ли система, связанная с безопасностью, в состоянии, гарантирующем установленную полноту безопасности.

[МЭК 61508-4 и МЭК 62061, модифицировано]

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

Примечание — Такое же определение, как и в МЭК 61508-4, с дополнительным примером и примечаниями.

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

3.1.1.23 **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 используется для обозначения показателя надежности, измеряемого с 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, модифицировано]

3.1.1.24 **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]

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

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

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

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

3.1.1.28 **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, модифицировано]

3.1.1.29 **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 — Данная концепция введена в МЭК 61784-3:2010, 5.2.4, и реализуется профилями коммуникаций, удовлетворяющих требованиям функциональной безопасности, определенным в настоящем стандарте.

3.1.1.30 **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, п. 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]

3.1.1.31 **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.

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

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

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

3.1.1.35 **ложное аварийное отключение** (spurious trip): Аварийное отключение, вызванное системой безопасности, без запроса от процесса.

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

3.1.2 CPF 1. Дополнительные термины и определения

3.1.2.1 **клиент** (client): Объект соединения, запрашивающий информацию от сервера.

3.1.2.2 **перекрестная проверка** (cross-check): Верификация того факта, что избыточно переданные данные идентичны.

3.1.2.3 **H1**: Коммуникационный канал передачи данных, соответствующий стандарту на полевую шину.

3.1.2.4 **хост** (host): Блок обработки информации, способный реализовать механизмы профиля безопасности и услуги черного канала.

3.1.2.5 **макроцикл** (macro cycle): Единичная итерация графика работы канального уровня.

3.1.2.6 **подмена** (masquerade): Ошибка, вызванная неверной идентификационной информацией.

3.1.2.7 **издатель** (publisher): Источник сообщений, периодически передающий сообщения.

3.1.2.8 **организация очереди** (queuing): Последовательная обработка элементов данных.

3.1.2.9 **сервер** (server): Объект соединения, обрабатывающий сообщения, поступающие от клиента.

3.1.2.10 **среда УПБ** (SIL environment): Аппаратные средства и программное обеспечение, обеспечивающие выполнение функций SIS.

3.1.2.11 **подписчик** (subscriber): Приемник сообщений, получающий сообщения от издателя.

3.2 Обозначения и сокращения

3.2.1 Общие обозначения и сокращения

CP — Профиль коммуникаций [МЭК 61784-1];

CPF — Семейство профилей коммуникаций [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;

ЭМП — Электромагнитные помехи;

УО — Управляемое оборудование [МЭК 61508-4:2010];

Э/Э/ПЭ — Электрические/электронные/программируемые электронные [МЭК 61508-4:2010];

FAL — Прикладной уровень полевой шины [МЭК 61158-5];

FCS — Последовательность проверки кадра;

ФБ — Функциональная безопасность;

FSCP — Профиль коммуникаций, удовлетворяющий требованиям функциональной безопасности;

MTBF — Среднее время между отказами;

MTTF — Среднее время до отказа;

NSR — Не относящийся к безопасности (Non Safety Relevant)
PDU — Блок данных протокола [ИСО/МЭК 7498-1];
ЗСНН — Защитное сверхнизкое напряжение;
ПЭС — Программируемая электронная система [МЭК 61508-4:2010];
PFD — Средняя вероятность опасных отказов по запросу [МЭК 61508-6:2010];
PFH — Средняя частота опасных отказов в час [МЭК 61508-6:2010];
PhL — Физический уровень [ИСО/МЭК 7498-1];
УЭЗ — Уровень эффективности защиты [ИСО 13849-1];
ПЛК — Программируемый логический контроллер;
SCL — Коммуникационный уровень безопасности;
БСНН — Безопасное сверхнизкое напряжение;
УПБ — Уровень полноты безопасности [МЭК 61508-4:2010];
SR — Связанный с безопасностью.

3.2.2 CPF 1. Дополнительные обозначения и сокращения

AP — Прикладной процесс;
ASIC — Специализированная интегральная схема;
CAS — Каскад (каскадное размещение);
CF — Общий файл;
CFF — Общий формат файла;
DD — Описание прибора;
DO — Цифровой выход;
FBAP — Функциональный блок прикладного процесса;
FMS — Спецификация сообщения полевой шины:
АПС — Активный планировщик связей;
LO — Локальное переопределение;
LRSN — Последний полученный порядковый номер;
MAU — Блок доступа к среде передачи данных;
MD5 — Алгоритм профиля сообщения 5;
MIB — Информационная база управления;
NMA — Агент сетевого управления;
NMIB — Информационная база управления сетью;
OD — Словарь объектов;
OOS — Неисправный;
SIS — Инструментальная система безопасности;
SMIB — Информационная база управления системой;
SMK — Ядро управления системой;
SMKP — Протокол ядра управления системой;
VCR — Виртуальная коммуникационная связь.

3.3 Условные обозначения

3.3.1 Диаграммы состояний

На рисунке 3 приведен пример диаграммы состояния, использующейся в настоящем стандарте. Состояние показано в виде овала с наименованием состояния в его центре. На рисунке 3 «Не соединен», «Соединен/Хорошее» и «Соединен/Плохое» являются состояниями. Переход представлен в виде линии или кривой, стрелка которой указывает направление перехода. Каждый переход имеет имя. «R1», «R2», «R3» и «R4» на рисунке 3 являются переходами.

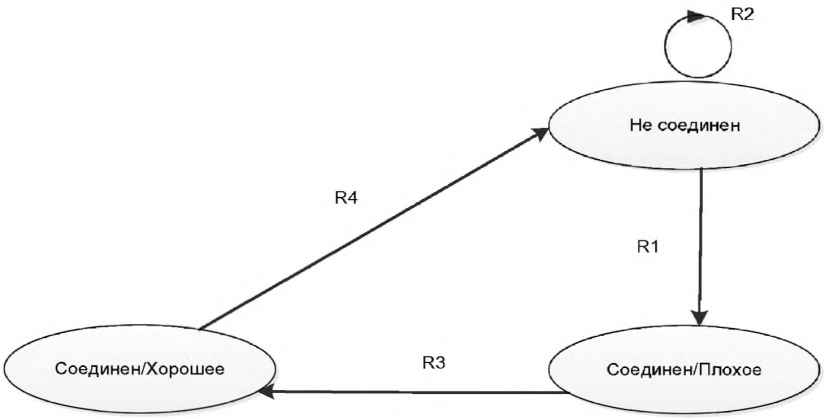


Рисунок 3 — Пример диаграммы состояний

Каждая диаграмма состояний сопровождается таблицей. См. таблицу 1 для диаграммы состояний на рисунке 3. Первый столбец, обозначенный «#», содержит наименование перехода. Следующий столбец «Текущее состояние» содержит состояние, к которому применяется данный переход. Третий столбец, названный «Событие и условные действия», содержит событие, любые условия перехода и любые действия. Действия располагаются в таблице с отступом от условий. «RcvMsg() = "FMS Initiate. cnf"» в таблице 1 является условием, а «SET Sequence Number = MCN» является действием. Четвертый столбец «Следующее состояние» содержит новое состояние, следующее за переходом.

Таблица 1 — Пример таблицы перехода состояний

#	Текущее состояние	Событие условные действия	Следующее состояние
R1	Не соединен	RcvMsg() = "FMS Initiate.cnf" SET Sequence Number = MCN	Соединен/Плохое
R2	Не соединен	RcvMsg() = "Any message (не FMS Initiate.cnf)"	То же самое
R3	Соединен/Хорошее	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен
R4	Соединен/Плохое	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен

3.3.2 Использование цветов в рисунках

Использование цветов в рисунках не является обязательным и применяется только для того, чтобы сделать рисунки более понятными. Что обозначает каждый из цветов, показано на рисунке 4. Любые, не представленные на рисунке, цвета используются только для того, чтобы рисунок был более понятным.

Рисунок 4 — Использование цветов в рисунках

4 Обзор FSCP 1/1 (FOUNDATION Fieldbus™ SIS)

4.1 Общие положения

Семейство 1 коммуникационных профилей (общеизвестное как FOUNDATION™ Fieldbus[1)] определяет коммуникационные профили, основываясь на МЭК 61158-2 Тип 1, МЭК 61158-3-1, МЭК 61158-4-1, МЭК 61158-5-5, МЭК 61158-5-9, МЭК 61158-6-5 и МЭК 61158-6-9.

Базовые профили СР 1/1, СР 1/2 и СР 1/3 определены в МЭК 61784-1. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 1/1 (FF-SIS™) семейства 1 коммуникационных профилей (CPF 1) основан на базовом профиле СР 1/1, представленном в МЭК 61784-1, и спецификациях коммуникационного уровня безопасности, определенных в настоящем стандарте.

Примечание — К данному протоколу применимы следующие спецификации для полевой шины FOUNDATION™: AG-180 [45], FF-807 [46], FF-884 [47] и FF-895 [48].

Существуют применения, требующие, согласно МЭК 61508, от первого до четвертого уровня полноты безопасности.

Примечание — Такие применения, связанные с безопасностью, также называются инструментальными системами безопасности (SIS) (см. МЭК 61511).

Коммуникационный уровень безопасности FSCP 1/1, специфицированный в настоящем стандарте, позволяет использовать интеллектуальные устройства в системах, связанных с безопасностью, тем самым расширяя возможности системы, а также позволяя системе соответствовать требованиям уровня полноты безопасности. Коммуникационный уровень безопасности, установленный в настоящем стандарте, применим только к СР 1/1, как это описано в МЭК 61784-1. Область применения настоящего стандарта определена на рисунке 5.

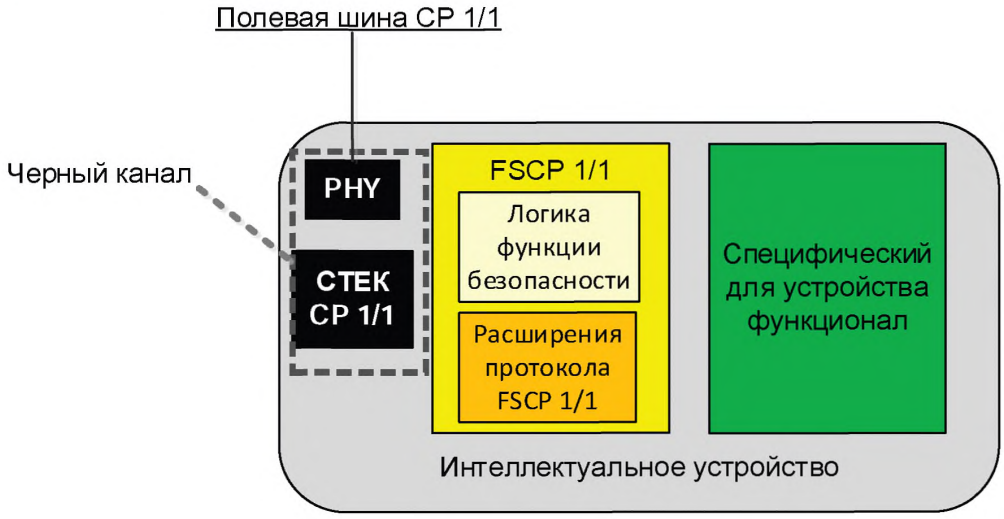


Рисунок 5 — Область применения FSCP 1/1

В настоящем стандарте не определены требования для средств проектирования или функционала собственных измерений устройств. Коммуникационный уровень безопасности обеспечивает загрузку конфигурации, созданной при помощи средств проектирования, в устройства безопасности таким образом, чтобы протокол не оказывал негативного влияния на уровень полноты безопасности.

[1)] Полевые шины FOUNDATION™ и FF-SIS™ являются торговыми марками некоммерческой организации Fieldbus Foundation. Данная информация приведена для удобства использования настоящего международного стандарта и не означает, что МЭК поддерживает мнение обладателя торговой марки или его продукцию. Соответствие настоящему стандарту не требует использования наименований Foundation Fieldbus™ или FF-SIS™. Использование торговых марок FOUNDATION™ Fieldbus или FF-SIS™ требует разрешения со стороны Fieldbus Foundation.

Сам по себе FSCP 1/1 не обеспечивает функциональную безопасность. Кроме регистрации интероперабельности протокола FSCP 1/1 поставщик также получит оценку функциональной безопасности для изделий, систем и программного обеспечения. Пользователю следует удостовериться в том, подходит ли все связанное с безопасностью оборудование для реализации функции безопасности в соответствии с МЭК 61508.

4.2 Основные концепции FSCP 1/1

4.2.1 Черный канал

Данная концепция заключается в использовании недоверенной коммуникационной системы (например, провода, оптоволоконные кабели, повторитель, барьер, ASIC, коммуникационный стек, шлюзовое устройство, интерфейс) для обеспечения надежного коммуникационного канала. Черный канал включает устройство, которое называют средством коммуникаций, а также SMK и SMKP. Система диагностики FSCP 1/1 управляет сбоями в черном канале. Черный канал может отказать в любое время, но отказы коммуникаций выявляются таким образом, чтобы была возможность управлять сбоями в рамках времени безопасности процесса. Диагностики выявления отказов должны соответствовать МЭК 61508, но от черного канала это не требуется. Протокол FSCP 1/1 не основан на 16-битном CRC в FCS уровня канала данных H1.

4.2.2 Ключ соединения

Ключ соединения — это уникальный номер каждого соединения, «кодовое слово» связи источник — адресат, назначаемое хостом каждому объекту канала безопасности во время конфигурации. В отличие от адреса черного канала ключ соединения защищен с помощью CRC коммуникационного уровня безопасности. Ключ соединения уникален в рамках коммуникационного уровня безопасности. При замене устройств может использоваться тот же ключ соединения посредством загрузки его в новое устройство. Конфигурация устройства, включающая ключ соединения, стирается в удаляемом устройстве перед тем, как его подключат снова к FSCP 1/1 сети для другой услуги. Устройства могут автоматически стирать свою конфигурацию при изменении адреса черного канала; альтернативой этому может служить наличие кнопки перезапуска или ее подобия для очистки конфигурации устройства.

4.2.3 Перекрестная проверка

Эта проверка представляет собой сравнение данных приложения, номера последовательности и CRC, которые были избыточно (с резервированием) переданы (дважды в одном сообщении) для подтверждения идентичности двух копий.

4.2.4 FSCP 1/1

FSCP 1/1 обеспечивает закрытую систему передачи, подходящую для использования в системе, связанной с безопасностью. Этот профиль позволяет достичь доверенных коммуникаций между приложениями, связанными с безопасностью (адаптировано из МЭК 62280-1).

4.2.5 Программируемая электронная система (PEC)

Это система для управления, защиты или контроля (мониторинга), основанного на одном или нескольких программируемых электронных устройствах. Она включает в себя все элементы системы, такие как блоки питания, датчики и другие устройства ввода, скоростные линии передачи данных и другие коммуникационные пути, исполнительные устройства и другие устройства вывода. Структура PEC может содержать программируемые электронные элементы в виде модуля не только в датчиках и исполнительных устройствах в управляемом оборудовании и их интерфейсах, программируемые электронные элементы могут присутствовать в нескольких местах в PEC (адаптировано из МЭК 61508-4:2010, 3.3.1).

4.2.6 Задержки в очереди

Один из возможных сбоев — это задержка сообщений в черном канале по причине очередей в коммуникационном стеке устройства или в аппаратном обеспечении интеллектуальной сети, включающей повторители, концентраторы, мосты, коммутаторы и шлюзовые устройства. Не подтвержденные опубликованные сообщения могут успешно проходить через черный канал и даже с приемлемой скоростью, но при этом, по причине долгой очереди или множества очередей на разных этапах на пути черного канала, могут оказаться старее, чем позволяет время безопасности процесса. Этот сбой является сбоем задержки, при котором задержка вызвана устройствами на черном канале, ставящими сообщения в очередь.

4.2.7 Избыточность

Избыточность — это использование дополнительного аппаратного обеспечения, программного обеспечения или данных помимо тех, что требуются в среде, не допускающей ошибки.

Пример — Продублированные функциональные компоненты и дополнение битами четности являются экземплярами избыточности.

Примечание — Избыточность применяется в основном для улучшения надежности или готовности (МЭК 61508-4:2010, 3.4.6).

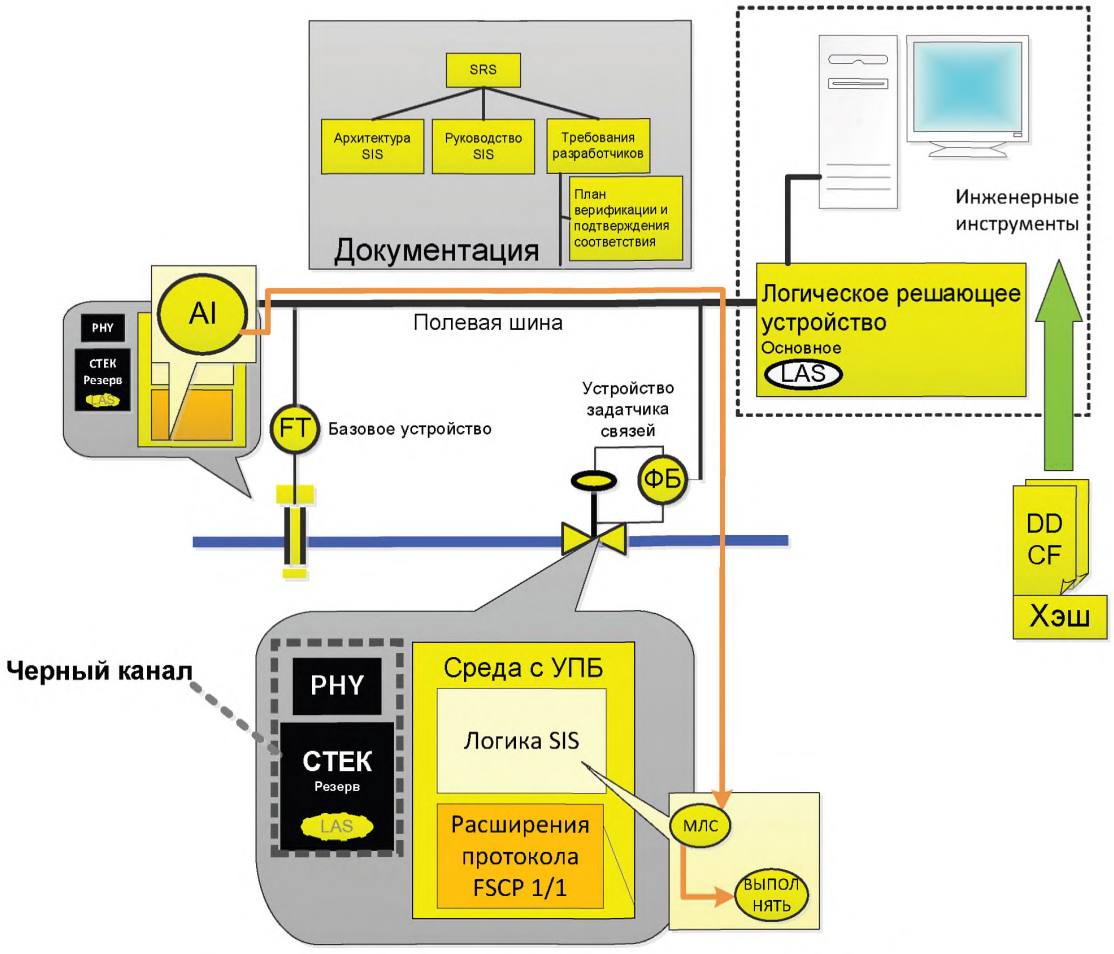
4.2.8 Среда УПБ

Аппаратное обеспечение и компоненты программного обеспечения, соответствующие FSCP 1/1, могут быть встроены в систему, которая является подходящей средой для реализации приложений, связанных с безопасностью.

4.3 Основные компоненты FSCP 1/1

4.3.1 Обзор

Коммуникационное аппаратное обеспечение полевой шины и стек не являются доверенными. Коммуникационный уровень безопасности, находящийся над коммуникационным стеком, обеспечивает доверенные коммуникации через полевую шину, а объект канала безопасности в FBAP содержит дополнительную информацию, требующуюся для протокола FSCP 1/1. Это показано на рисунке 6. В устройстве безопасности прикладной процесс и коммуникационный уровень безопасности будут выполняться в среде с некоторым УПБ. Был создан набор упрощенных функциональных блоков, подходящих для приложений, связанных с безопасностью.



LAS — активный планировщик связей; МЛС — мажоритарная логическая схема

Рисунок 6 — Архитектура (H1) FSCP 1/1

Протокол FSCP 1/1 осуществляет управление отказами, такими как неисправности в устройстве или каналах, а также случайными помехами, такими как ЭМП. Коммуникационный уровень безопасности обнаруживает следующие типы коммуникационных ошибок: повторение, удаление, включение, изменение последовательности, искажение данных, подмена и задержка.

4.3.2 Черный канал

Концепция черного канала, как показано на рисунке 7, позволяет данным безопасности передаваться по недоверенной шине. Необходимость в физическом разделении функций безопасности и аппаратных средств, не связанных с безопасностью, отсутствует. Устройства, связанные и не связанные с безопасностью, а также данные могут разделять шину, как показано на рисунке 7.

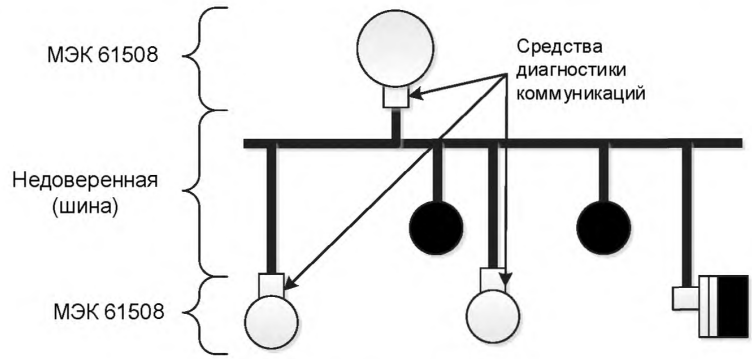


Рисунок 7 — Черный канал

Допустим, что в сети H1 только один LAS, т. е. на одном и том же устройстве могут работать как связанные, так и не связанные с безопасностью приложения. Передача данных по FSCP 1/1 логически отделена от других передач данных. Конфигурация с одним каналом, являющимся не избыточной шиной, является достаточной. Устройство безопасности может предоставлять как связанные, так и не связанные с безопасностью функциональные блоки. Протокол FSCP 1/1 используется в каналах для функциональных блоков безопасности. Обычный CP 1/1 используется в каналах для функциональных блоков, не связанных с безопасностью. Таким образом, устройство безопасности может применяться как для функций, связанных с безопасностью, так и для не связанных с безопасностью функций.

Отказы могут происходить по причинам, отличным от фактических отказов компонентов аппаратного обеспечения (например, электромагнитные помехи, ошибки декодирования), тем не менее подобные отказы считаются случайными отказами в аппаратных средствах (см. МЭК 61508-2:2010, 7.4.5.2).

Для повышения готовности можно применять избыточность, обеспечиваемую шиной горячего резервирования. Между инструментальными устройствами и логическим решающим устройством предполагается использовать один канал. Избыточные каналы предполагается использовать в коммуникациях между логическими решающими устройствами.

4.4 Связь с базовой эталонной моделью ИСО ВОС

Коммуникационный уровень безопасности реализуется над коммуникационным стеком на уровне приложения.

5 Общие положения

5.1 Внешние документы, предоставляющие спецификации для профиля

Следующие документы предоставляют дополнительные спецификации, которые могут играть важную роль в проектировании FSCP 1/1:

- FOUNDATION™ Fieldbus AG-180 [45];
- FOUNDATION™ Fieldbus FF-807 [46];
- FOUNDATION™ Fieldbus FF-884 [47];
- FOUNDATION™ Fieldbus FF-895 [48].

5.2 Функциональные требования безопасности

5.2.1 Требования для функциональной безопасности

Следующий список содержит требования функциональной безопасности, применяемые при разработке протокола FSCP 1/1.

- FSCP 1/1 должен проектироваться таким образом, чтобы поставщики (вендоры) могли разрабатывать продукцию, подходящую для использования в приложениях с УПБ 2 (МЭК 61508), а с УПБ 3 рекомендуется.
- Протокол должен поддерживать соединения издатель/подписчик и клиент/сервер.
- Протокол, связанный с безопасностью, должен предотвращать помехи от устройств, не связанных с безопасностью. Например, не связанному с безопасностью ручному устройству должно быть запрещено изменять параметры в устройстве, связанном с безопасностью.
- Протокол должен защищать от ненамеренных или неавторизованных изменений конфигурации устройства безопасности.
- Вклад протокола FSCP 1/1 в PFD/PFH должен быть менее 1% значения, требуемого для УПБ.
- Вычисления PFD/PFH должны выполняться для режима по запросу и для режима с высокой частотой запросов (в соответствии с определениями в МЭК 61508).
- Протокол должен реализовывать меры по управлению следующими сбоями:
  - отказ/искажение передачи битов;
  - повторная передача;
  - пропуск данных;
  - включение/расширение данных;
  - неверный порядок данных;
  - задержка данных;
  - отказ/искажение адресации;
  - сбои в очередях.

Примечание — Сбои в очередях являются разновидностью сбоя «задержка».

- Должна существовать возможность вычисления времени реакции для приложения.
- Реализация функционального блока для требуемого УПБ должна осуществляться в соответствии с МЭК 61508-3.
- Должно допускаться наличие устройств с различными УПБ в одной сети.
- Должна существовать возможность обхода (by-pass) устройств безопасным образом.

5.2.2 Функциональные ограничения (условия)

Ниже приведен список функциональных ограничений, используемых в разработке FSCP 1/1.

- Должна существовать возможность выполнения коммуникаций безопасности и стандартных коммуникаций средствами стандартных устройств и устройств безопасности на одной шине CP 1/1.

- ASIC, коммуникационный стек, повторители, электромонтажное оборудование, блоки питания и аксессуары не должны модифицировать (черный канал) функции безопасности над уровнем 7 ВОС.

- Протокол должен обладать механизмами, позволяющими хосту обнаруживать несоответствие типа устройства или новой версии устройства, или новой версии DD (описание устройства), или новой версии функциональных возможностей файла, или УПБ.

5.2.3 Требования к производителю устройства

Приведенный ниже список является набором требований, которые FSCP 1/1 выдвигает к поставщику устройства.

- Условия окружающей среды и электрическая безопасность в соответствии с МЭК 61131-2.
- Аппаратные средства должны соответствовать МЭК 61508-2 для требующегося УПБ.
- Программное обеспечение должно соответствовать МЭК 61508-3 для требующегося УПБ.
- Оценка аппаратных средств и программного обеспечения должна выполняться компетентной и независимой испытательной организацией в соответствии с МЭК 61508-1.

5.3 Меры безопасности

5.3.1 Порядковый номер

Каждый блок данных протокола безопасности обладает последовательно формируемым номером, который является номером макроцикла, присвоенным при генерации сообщения.

5.3.2 Временная метка

Последовательно формируемый номер, включенный в блок данных протокола безопасности, также является временной отметкой, так как он является номером макроцикла.

5.3.3 Временное ожидание

Порядковый номер / временная метка используются для проверки того факта, что сообщения доставлены вовремя. Каждое соединение также обладает счетчиком устаревания, обнаруживающим случаи, когда сообщения не были получены в течение времени ожидания.

5.3.4 Аутентификация соединения

С каждым соединением ассоциирован ключ соединения, используемый для проверки того факта, что блок данных протокола безопасности поступил из верного источника сообщений.

5.3.5 Обеспечение целостности данных

Каждый блок данных протокола безопасности содержит CRC для обеспечения целостности данных.

5.3.6 Избыточность с перекрестной проверкой

Каждый блок данных протокола безопасности содержит две копии данных и CRC. Дублирование данных и CRC используются для перекрестной проверки данных.

5.3.7 Различные системы обеспечения целостности данных

Блок данных протокола безопасности содержит дополнительные CRC, отличающиеся от системы целостности данных черного канала.

5.3.8 Связи между ошибками и мерами безопасности

Меры безопасности, выделенные в 5.3.1—5.3.7, можно связать с набором возможных ошибок. Эта связь показана в таблице 2. Каждая мера безопасности может обеспечивать защиту от одной или более ошибок в передаче. С помощью таблицы 2 должно быть продемонстрировано, что существует хотя бы одна соответствующая мера безопасности или комбинация мер безопасности для всех определенных возможных ошибок.

Таблица 2 — Меры безопасности и возможные коммуникационные ошибки

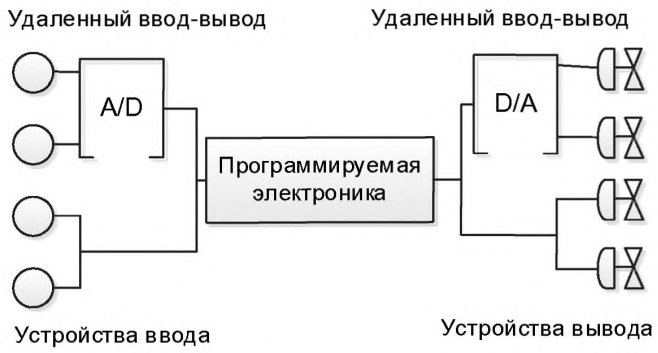
Ошибки коммуникаций	Меры безопасности							
	Порядковый номер	Временная метка	Временное ожидание	Аутентификация соединения	Сообщение обратной связи	Обеспечение полноты данных	Избыточность с перекрестной проверкой	Различные системы обеспечения полноты данных
Искажение						X	X	
Ненамеренное повторение	X	X						
Неправильная последовательность	X	X						
Потеря	X							
Недопустимая задержка		X	X					
Внесение	X							
Подмена								X
Адресация				X				
Примечание — Таблица из МЭК 61784-3.								

5.4 Структура коммуникационного уровня безопасности

5.4.1 Топология сети и связность устройств

5.4.1.1 Общие положения

Устройства, связанные и не связанные с безопасностью, могут разделять общую полевую шину, как показано на рисунке 8. Должна учитываться вся функция безопасности целиком, от датчика до исполнительного устройства. На канал полевой шины по проекту выделяется не более 1 % от PFD (средняя вероятность опасных отказов по запросу) на канал.



A — аналоговый; D — цифровой

Рисунок 8 — FSCP 1/1 в архитектуре системы

Примечание — Программируемые электрические элементы показаны в центре, но могут присутствовать в нескольких местах в ПЭС.

5.4.1.2 Топология отдельного канала H1

Функция безопасности реализуется одним каналом H1. Канал является частью черного канала. Устройства H1, связанные и не связанные с безопасностью, подключаются к сети идентичным образом.

5.4.2 Архитектура устройства

5.4.2.1 Общие положения

Концепция черного канала позволяет коммуникационным аппаратным средствам (включая ASIC и MAU) и стеку коммуникационного программного обеспечения быть недоверенными, тогда как диагностические средства коммуникаций и функциональные блока приложения по протоколу FSCP 1/1 выполняются в среде с УПБ, состоящей из аппаратных средств и программного обеспечения с некоторым УПБ. Коммуникационный уровень безопасности является интерфейсом между прикладным процессом с некоторым УПБ и недоверенными средствами коммуникаций черного канала, как это показано на рисунке 9.

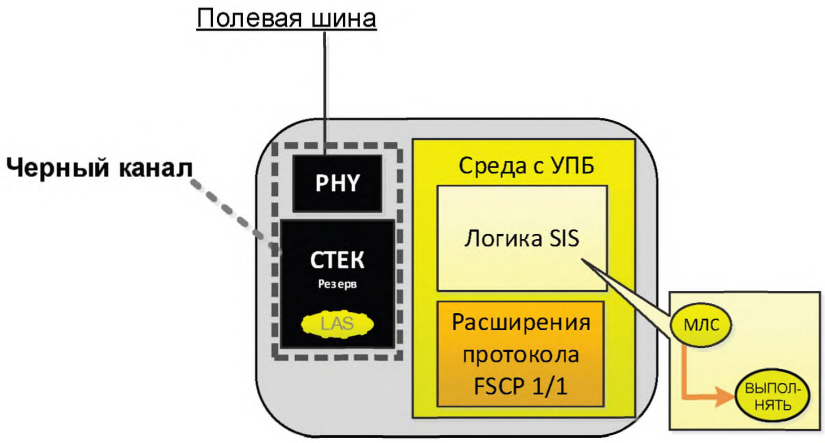


Рисунок 9 — Устройство H1 с FSCP 1/1

Реализация концепции черного канала должна выполняться с осторожностью, чтобы избежать вмешательства не имеющих УПБ аппаратных средств и программного обеспечения в аппаратные средства и программное обеспечение, связанные с УПБ.

5.4.2.2 Архитектура устройства H1

Прикладные процессы связаны с безопасностью и будут выполняться в среде с заданным УПБ. Средство коммуникаций состоит из коммуникационного стека, FMS, NMA и NMIB, являющихся недоверенными. Средство коммуникаций, так же как и SMK и SMKP, входит в состав черного канала. Их связь показана на рисунке 10.

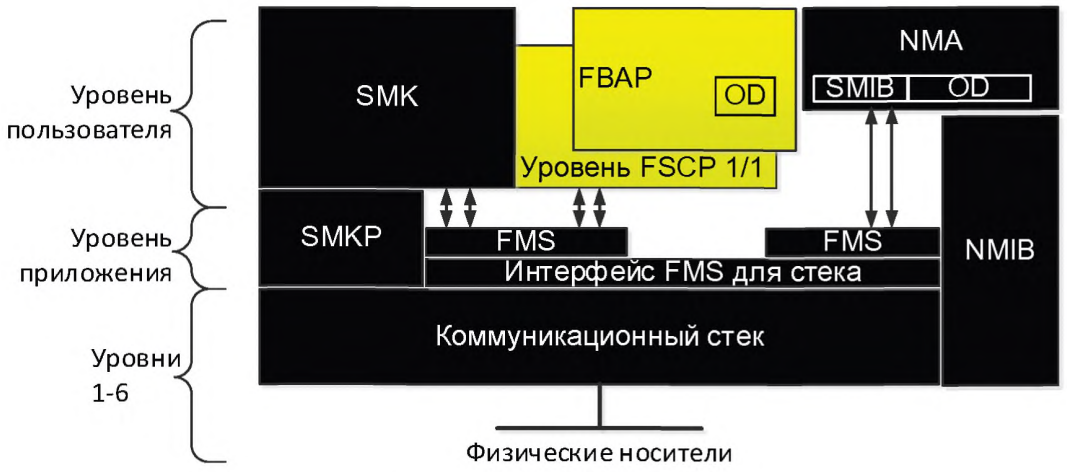


Рисунок 10 — Уровни протокола FSCP 1/1

5.5 Связи с FAL (и DLL, PhL)

5.5.1 Общие положения

На рисунке 11 показана связь между FSCP 1/1 и другими уровнями МЭК 61158, Тип 1.

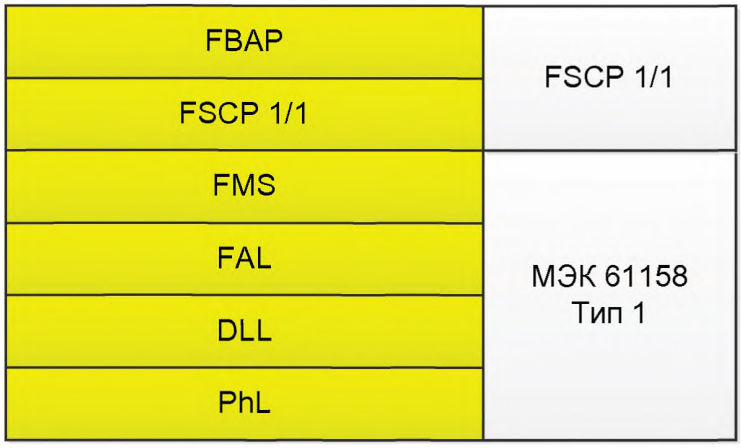


Рисунок 11 — Связь между FSCP 1/1 и другими уровнями МЭК 61158, Тип 1

5.5.2 Типы данных

FSCP 1/1 использует базовые типы данных, перечисленные в таблице 3 согласно CPF 1 в МЭК 61784-1.

Таблица 3 — Типы данных, применяемые в рамках FSCP 1/1

Название типа данных	Перевод	Число октет
Integer8	8-битовый целочисленный	1
Integer16	16-битовый целочисленный	2
Integer32	32-битовый целочисленный	4
Unsigned8 (used as bits)	8-битовый без знака (используется в качестве бит)	1
Unsigned16 (used as bits)	16-битовый без знака (используется в качестве бит)	2
Unsigned32 (used as bits)	32-битовый без знака (используется в качестве бит)	4
Unsigned16	16-битовый без знака	2

Окончание таблицы 3

Название типа данных	Перевод	Число октет
Unsigned32	32-битовый без знака	4
Float32	32-битовый с плавающей точкой	4
Date	Дата	
TimeOfDay with date indication	Время суток с индикацией даты	
TimeOfDay without date indication	Время суток без индикации данных	
TimeDifference with date indication	Разность времени с индикацией даты	
TimeDifference without date indication	Разность времени без индикации даты	
Visible String	Видимая строка	1,2,3…

6 Услуги коммуникационного уровня безопасности

6.1 Прикладной процесс

6.1.1 Обзор

Функции, связанные и не связанные с безопасностью, могут быть размещены в одном или различных прикладных процессах в устройстве. Прикладной процесс (ПП) для функций безопасности требует среду с определенным УПБ и не входит в состав черного канала.

Уровень FSCP 1/1 не зависит от прикладного процесса и, таким образом, может использоваться для передачи функциональных блоков одного прикладного процесса или другого прикладного процесса.

6.1.2 Видимые объекты сети

Прикладной процесс не имеет прямого доступа к прикладному уровню в стеке коммуникаций черного канала, а только через уровень FSCP 1/1.

6.1.3 Интерфейс прикладного уровня

Тот же набор услуг отправки сообщений, который FMS предоставляет для объектов, не связанных с безопасностью, предоставляется коммуникационным уровнем безопасности для объектов безопасности.

6.1.4 Словарь объектов

В словарь объектов полевой шины не вносятся никакие изменения для поддержки черного канала.

6.1.5 Директория прикладных программ

В директорию прикладного процесса не вносятся никакие изменения для поддержки черного канала.

6.2 Функциональные блоки прикладных процессов

6.2.1 Общие положения

Были определены простые функциональные блоки, пригодные для приложений, связанных с безопасностью. FBAP, содержащий объекты безопасности, будет выполняться в среде с УПБ.

Использование функциональных блоков не обязательно. Скорее всего, хост не будет выполнять функциональные блоки.

6.2.2 Модель функционального блока

6.2.2.1 Счетчик устаревания

Проверка счетчиком устаревания для сквозного соединения соответствия номера последовательности, управляет сбоями при планировании (построении графика) и выполнении логической цепи вплоть до выводного функционального блока. После выводного функционального блока таймер устаревания данных управляет сбоями в планировании и выполнении самого выводного функционального блока. Если из-за ошибки планирования или выполнения от выводного функционального блока не получено обновление в заданный промежуток времени, то вывод перейдет в состояние сбоя. Использование таймера устаревания данных после выводного функционального блока является мерой безопасности, независимой от не связанного с УПБ SMK, проверяющего, выполняются ли функциональные блоки. Если функциональный блок не выполняется, то выводы не распространяются по черному каналу. Потерянное сообщение — это сбой управляющего выводного ключевого блока, и несоответствие номера последовательности вызовет действие предварительно сконфигурированного состояния сбоя.

Номер последовательности для канала, используемый в протоколе FSCP 1/1, вычисляется из номера макроцикла, основываясь на времени канала передачи данных, и потому изменяется для каждого нового PDU, передаваемого по черному каналу. Если черный канал работает некорректно и издает старые данные, то номер последовательности не будет соответствовать, что позволяет обнаруживать подобные сбои выводного ключевого блока.

Механизмы проверки сбоев сквозного соединения с помощью счетчика устаревания позволяют обнаружить следующие сбои: остановка выполнения функционального блока, неправильный порядок его выполнения, в неправильное время или со слишком большими флуктуациями сигнала. Подобные сбои могут происходить по причине сбоев в планировании, в самом функциональном блоке, или из-за превышения максимального ожидаемого времени выполнения функционального блока.

6.2.2.2 Имитация

Для запуска имитации в блоке ресурсов выключаются блокировка записи и защита имитации. Если блокировка записи снова включена, то имитация автоматически выключается. Кроме того, запуск имитации должен быть в нестирающейся при перебое питания памяти. Когда питание включено — имитация всегда находится в выключенном состоянии.

Когда имитация активирована, посылается аварийный сигнал от не связанной с безопасностью функции. Хосту требуется периодически проверять, включена имитация или нет в любом из устройств.

6.2.2.3 Блокировка записи

Блокировка записи защищает конфигурацию устройства. Когда блокировка записи установлена в блоке ресурсов устройства безопасности, все внесения записей в ресурс отключены, включая MIB, но исключая саму блокировку записи. Защищенное содержание MIB включает объект (блокировки, каналы, VCR), адрес, параметры и тег устройства.

Функциональный блок предохранительной блокировки (safety lock) в каждом устройстве безопасности способен произвести запись в параметр блокировки записи в блоке ресурсов того же устройства. Функциональный блок предохранительной блокировки имеет вход блокировки записи, который принимает ссылку функционального блока безопасности. Это позволяет включать и отключать возможность ввода в несколько устройств удаленно из центрального устройства. Функциональный блок предохранительной блокировки может активировать и деактивировать блокировку записи в устройстве, используя выключатель с ключом через функциональный блок DI. На рисунке 12 показана архитектура такой предохранительной блокировки.

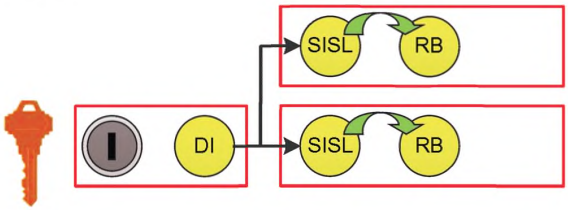
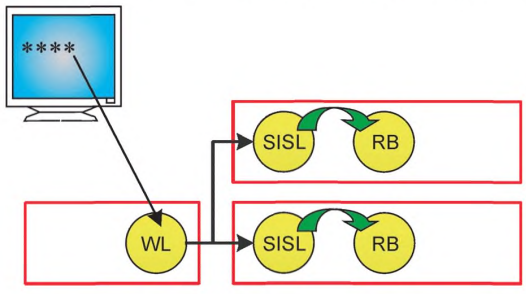


Рисунок 12 — Блокировка записи с помощью ключа

Блокировка записи может также быть активирована и деактивирована записью параметра в функциональный блок предохранительной блокировки. Запись параметра, как правило, защищается на хосте надлежащими паролями. На рисунке 13 показана архитектура подобного замка.



WL — Блокировка записи («Write Lock»)

Рисунок 13 — Блокировка записи с помощью пароля

6.2.2.4 Остановка и перезапуск

Для выводного функционального блока FSCP 1/1 состояние сбоя может быть сконфигурировано как «de-energized-to-trip» (остановлен по отключению питания), или «energized-to-trip» (остановлен по включению питания), или же «hold last value» (держать последнее значение). Если последовательный ввод выводного функционального блока имеет статус «Bad» (плохой), например, по причине потери связи, то это отражается в виде «Bad::non-specific substatus» на выводе обратной связи выводного функционального блока. Физический вывод может срабатывать при непосредственном запросе процесса из логического решающего устройства, из-за коммуникационной или упреждающей ошибки выполнения функционального блока, из-за вмешательства оператора или же по причине сбоя устройства.

Существует различие между предварительно сконфигурированным действием состояния сбоя, отвечающим на запрос процесса, коммуникационную ошибку или упреждающую ошибку выполнения функционального блока, и остановкой по причине сбоя в устройстве подачи питания. Ответ выводного функционального блока на запрос процесса основывается на его входном сигнале, где ноль (0) означает предварительно сконфигурированное действие состояние сбоя, а один (1) всегда означает «можно выполнять» (OK to run). Сигнал для «остановить по включению питания» инвертируется в выводном функциональном блоке. При коммуникационной ошибке выводной функциональный блок не прибегает ни к каким действиям до тех пор, пока не истекло время состояния сбоя, а затем он либо держит свою последнюю позицию, либо переходит к значению сбоя, как это установлено опцией «состояние сбоя» и значением «состояние сбоя».

При нормальном режиме работы выводной функциональный блок выполняется в последовательном режиме. По умолчанию режим останется последовательным по запросу процесса. Дополнительно по запросу процесса и коммуникационной ошибки вывод может быть зафиксирован в состоянии сбоя. Когда включена функция фиксировать состояние сбоя и происходит запрос процесса или ошибка коммуникаций, то функциональный блок DO переходит в режим LO (локального переопределения). Даже если запрос или условие сбоя убраны, вывод остается в состоянии сбоя до тех пор, пока его не перезапустит пользователь. Логическое решающее устройство может контролировать вывод из вывода обратной связи выводного функционального блока и, если необходимо, сигнализировать о статусе Bad. Если зафиксировано, то оператор снимет фиксацию либо через очистку состояния сбоя блока ресурсов, либо через перезапуск ввода выводного функционального блока. Если устройство сконфигурировано для состояния сбоя «по отключению», то аппаратные средства могут, например, выполнить открытие или закрытие клапана. В таблице 4 перечислено подобное поведение.

Если статус ввода «Bad» или «Good::Initiate-fault-state», то вывод также выполнит предварительно сконфигурированное действие состояния сбоя.

Таблица 4 — Поведение состояния сбоя

Условие	Пример	Задержка состояния сбоя DO	Функция состояния сбоя DO	Фиксация состояния сбоя DO	Заметка
Статус «Bad», коммуникационная ошибка или упреждающая ошибка выполнения функционального блока	Плохой последовательный ввод по причине отказа CRC коммуникационного уровня безопасности, несоответствие номера последовательности или несоответствие результатов перекрестной проверки при избыточности	Да	Питание включено		
Питание отключено					
Удержание	Необязательный режим LO				
Инициировать состояние сбоя	От другого функционального блока или логического решающего устройства получен подстатус	Да	Питание включено		
Питание отключено					
Удержание	Необязательный режим LO				

Окончание таблицы 4

Условие	Пример	Задержка состояния сбоя DO	Функция состояния сбоя DO	Фиксация состояния сбоя DO	Заметка
Вмешательство оператора	Установить состояние сбоя из блока ресурсов	Нет	Питание включено		
Питание отключено					
Удержание	Всегда установлен режим LO				
Запрос процесса от логического решающего устройства	Дискретный последовательный ввод равен (0)	Нет	Нет	Необязательный режим LO	Как правило, режим CAS
Отказ черного канала	Ошибка синхронизации времени	Да	Питание включено		
Питание отключено					
Удержание	Необязательный режим LO				

Если условие, вызвавшее предварительно сконфигурированное действие состояния сбоя, убрано, то пользователь может перезапустить зафиксированный вывод, используя параметр очистки состояния сбоя в блоке ресурсов или очистки ввода состояния сбоя в самом выводном функциональном блоке.

6.2.3 Прикладные процессы

6.2.3.1 Общие положения

Определены стандартные функциональные блоки FSCP 1/1. Изготовители могут создавать улучшенные и индивидуальные функциональные блоки безопасности. Все блоки FSCP 1/1 идентифицируются номерами профиля, установленными в рамках определенного диапазона. Это позволяет хосту взаимодействовать с блоками FSCP 1/1 так, как это требуется.

6.2.3.2 Типы блоков

6.2.3.2.1 Общие положения

Для FSCP 1/1 были созданы дополнительные стандартные функциональные блоки и блок ресурсов. Стандартные функциональные блоки FSCP 1/1 идентифицируются номерами профиля, установленными в рамках определенного диапазона. Функциональные блоки FSCP 1/1 имеют меньше допустимых режимов и параметров, чем их обычный аналог. Ручной режим разрешен только когда на устройстве нет блокировки записи, то же самое применяется к автоматическому режиму для выводных функциональных блоков. Когда записи устройства разблокированы, режимы функционального блока будут сменяться на автоматический рабочий и последовательный соответственно.

Поведение состояния сбоя в выводных функциональных блоках безопасности является обязательным.

6.2.3.2.2 Блок ресурсов устройства безопасности

Параметр блокировки записи блока ресурсов обладает важной функцией механизма блокировки, которая предотвращает внесение записей в весь ресурс целиком.

Текущие статистические данные коммуникационного уровня безопасности могут быть оценены посредством блока ресурсов устройства безопасности. Статистические данные протокола FSCP 1/1 состоят из счетчика, обнаруженных плохих сбоев CRC коммуникационного уровня безопасности.

Статистические данные коммуникационного уровня безопасности также содержат параметр ошибки черного канала с флагом, указывающим на произошедший сбой синхронизации времени.

Блок ресурсов устройства безопасности содержит параметр для разблокировки ввода записей на устройстве. Она будет выполняться перед тем, как будет возможно записать параметры и объекты. Функциональный блок предохранительной блокировки упрощает блокировку и разблокировку записей во множестве устройств.

Блок ресурсов устройства безопасности содержит параметр для очистки всех выключенных выводов, которые были зафиксированы в выводе состояния сбоя.

Блок ресурсов устройства безопасности содержит параметр длительности макроцикла, так как на данные черного канала нельзя полагаться.

Блок ресурсов устройства безопасности содержит параметры, оповещающие о выпуске новых версий аппаратных средств и встроенных программ (прошивки), а также о контрольных суммах для встроенных программ и конфигурации.

6.2.3.2.3 Дополнительные функциональные блоки

6.2.3.2.3.1 Общие положения

Приложения безопасности требуют устройства ввода, вывода и логики. Поэтому предоставляется новый набор функциональных блоков безопасности, обеспечивающих эти функциональные возможности. Новый функциональный блок безопасности включает в себя:

- аналоговый ввод безопасности;
- дискретный ввод безопасности;
- предохранительную блокировку;
- дискретный вывод безопасности;
- логику безопасности;
- аналоговый компаратор безопасности.

Функциональные блоки SR-A, SR-DI и SR-DO сократили свою функциональность в сравнении с их обычными аналогами для того, чтобы упростить реализацию для специалистов по внедрению, уменьшить число ошибок, а также облегчить верификацию для пользователей. Упрощение включает в себя уменьшение числа поддерживаемых режимов и отсутствие системы сигналов тревоги.

6.2.3.2.3.2 Выводные функциональные блоки безопасности

Выводные функциональные блоки безопасности важны, так как в них выполняется предварительно сконфигурированное действие состояния сбоя. Помимо предварительно сконфигурированного действия состояния безопасности на значение запроса процесса, полученного на последовательном вводе, выводной функциональный блок также использует предварительно сконфигурированное действие состояния сбоя при плохом статусе, инициации состояния сбоя, упреждающей ошибки выполнения функционального блока и устаревших коммуникаций. Выходной преобразователь остановится по отказу связанного с ним выводного функционального блока функции безопасности, которую необходимо выполнить. Выходной преобразователь управляет планированием и сбоями коммуникаций при выполнении функции безопасности, осуществляя это остановкой в тех случаях, когда он не был обновлен свежими данными в установленные сроки таймера устаревания данных. Если выводной функциональный блок выполняет предварительно сконфигурированное действие состояния сбоя по подлинному запросу процесса, статуса или коммуникационного сбоя, то режим по умолчанию останется последовательным. Выводные функциональные блоки безопасности включают в себя дополнительные функции для фиксации (задержки) остановленных выводов. Вывод обратной связи в выводном функциональном блоке показывает статус «Bad::non-specific», если коммуникации последовательного ввода плохие. Другие сбои в выводе также будут отражены в этом статусе. Кроме того, сигнал тревоги, не связанный с безопасностью, может быть отправлен в ответ на состояние сбоя, если его поддерживает устройство. Подробности статуса обратной связи и аварийного сигнала будут указывать на то, является ли состояние сбоя подлинным запросом процесса или же вызвано сбоем. Используя коммуникации FSCP 1/1, с помощью параметра режима в выводном функциональном блоке можно увидеть, находится ли вывод в условиях состояния сбоя. В отдельном фиксированном выводе состояние сбоя может быть сброшено с помощью параметра перезапуска ввода в каждом выводном функциональном блоке. Перезапуск ввода принимает канал функционального блока безопасности, тем самым позволяя перезапуск состояния сбоя удаленно или с помощью логики другого функционального блока. Во всех остановленных выводах состояние сбоя может быть сброшено посредством параметра, содержащегося в блоке ресурсов.

В блоках преобразователя поставщик должен определенным образом реализовать продвинутые диагностические средства для клапана, такие как испытание клапана при неполном ходе, аналоговая обратная связь по положению для дискретных клапанов и сигнализация об отклонениях позиции. Команды, работающие над будущим профилем блока преобразователя, возможно, определят стандартные параметры для таких устройств.

6.2.3.2.3.3 Функциональный блок предохранительной блокировки

Функциональный блок предохранительной блокировки снимает блокировку с защиты от записи, основываясь на значениях вводов канала, обеспечивающих центральное блокирование и снятие блокировки для нескольких устройств.

Перед тем как появится возможность записывать параметры, ресурс будет разблокирован. Это равносильно блокировке ключом на пульте управления системой безопасности. Так как может работать множество устройств безопасности и так как их часто необдуманно устанавливают в опасных зонах или

как-то иначе делают недоступными, разблокировка и блокировка будут возможны через коммуникации FSCP 1/1. Блокировка записи программного обеспечения обязательна для блока ресурсов безопасности.

6.2.3.2.4 Объект канала безопасности

Расширения протокола FSCP 1/1 отражены в объекте канала безопасности. Другой объект канала, хранящий дополнительную информацию, используется для функциональных блоков каналов FSCP 1/1. Объект канала безопасности содержит ключ соединения и предельное значение непрерывного счетчика устаревания, требующиеся для приложений безопасности. В одной сети, в одном устройстве или в одном логическом решающем устройстве могут существовать множественные независимые цепочки выполнения функции безопасности. Отказ в одной цепи функции безопасности не должен быть причиной отключения других цепей функции безопасности на одной шине, в одном устройстве или логическом решающем устройстве. Для обеспечения интероперабельности с существующим оборудованием в приложениях, не связанных с безопасностью, устройство должно обязательно поддерживать объект канала, не связанный с безопасностью.

6.2.3.2.5 Таймер устаревания данных

Механизм непрерывного счетчика устаревания выявляет ошибки выполнения функционального блока вплоть до выводного функционального блока, но исключая его. Следующий механизм, таймер устаревания данных, останавливает вывод, если блок преобразователя вывода не обновляется выводным функциональным блоком в необходимое время, например, по причине отказа выполнения выводного функционального блока. Таймер устаревания данных вывода конфигурируется через выводной функциональный блок. Следует различать время устаревания данных и время состояния сбоя.

Подобным же образом механизм, зависящий от производителя, контролирует выполнение других блоков, включая блоки преобразователя.

Пример — Если блок преобразователя ввода не выполнен должным образом, то статус вывода вводного функционального блока является плохим.

6.3 Коммуникации устройство—устройство

6.3.1 Общие положения

Коммуникации FSCP 1/1 обеспечиваются для коммуникаций издатель/подписчик и клиент/сервер, но не для рассылки отчетов. Устройство безопасности по-прежнему может использовать VCR рассылки отчетов для передачи сигналов тревоги, но этому механизму нельзя доверять. На рисунке 14 показаны подобные коммуникации.

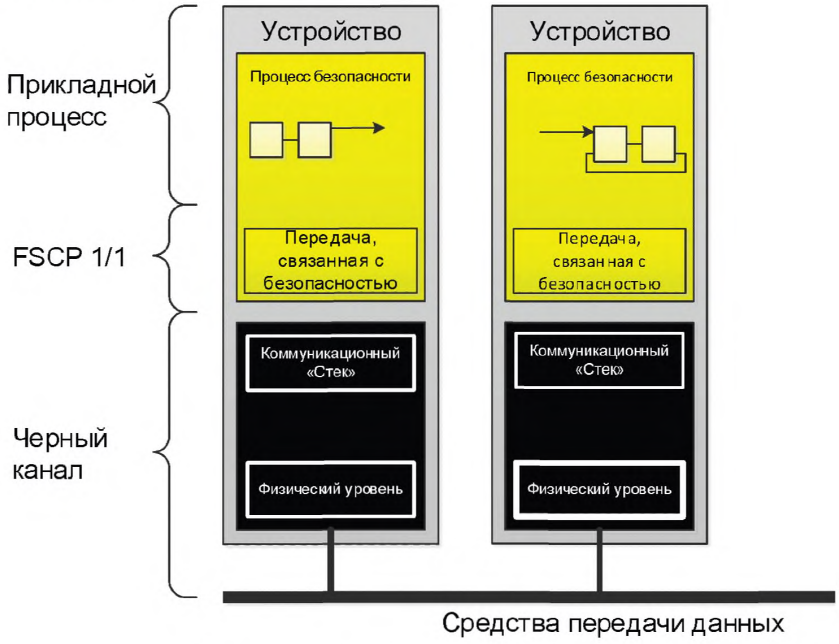


Рисунок 14 — Пример коммуникаций FSCP 1/1

6.3.2 Клиент/сервер

Устройство безопасности поддерживает чтение и запись для коммуникаций клиент/сервер. Клиент/сервер применяется пользователем для записи параметров. После внесения любых изменений пользователь должен выполнить функциональный тест, как это определено в МЭК 61508.

VCR коммуникаций клиент/сервер не является детерминистической и по-настоящему не ограничивается. VCR клиент/сервер не подходит для реализации отключения.

Параметры и объекты могут быть записаны, но для этого требуется, чтобы коммуникации FSCP 1/1 активировали возможность записи. Блокировка записи присутствует в блоке ресурсов, который защищает все объекты в ресурсах. После изменения конфигурации от пользователя требуется осуществить контрольное испытание. Затем коммуникации FSCP 1/1 используют для отключения возможности внесения записей.

«Запросы-на-считывание» и «ответы-на-запись» используют обычный протокол CP 1/1. «Запросы-на-запись» и «ответы-на-чтение» используют протокол FSCP 1/1. Должен быть создан объект канала клиент/сервер (с ключом соединения и т. д.) для каждого клиента (интерфейс), которому будет позволено читать/записывать устройство. Каждое сообщение будет содержать CRC. Ключ соединения включен в виде части виртуального заголовка, который используется при вычислении CRC.

Функциональные блоки FSCP 1/1 обладают каналами FSCP 1/1, сконфигурированными в объектах канала безопасности. Протокол FSCP 1/1 является расширением PDU, а не новым типом данных.

FSCP 1/1 использует избыточную передачу данных, что означает, что данные, номер последовательности и CRC передаются дважды и подвергаются перекрестной проверке в точке получения.

6.3.3 Издатель/подписчик

Функциональные блоки FSCP 1/1 обладают каналами FSCP 1/1, сконфигурированными в объектах канала безопасности. Протокол FSCP 1/1 является расширением PDU, а не новым типом данных. В дополнение к CRC уровня коммуникаций безопасности опубликованный PDU безопасности также включает номер последовательности, разрешающий подписчикам управлять дополнительными сбоями.

FSCP 1/1 использует избыточную передачу данных, что означает, что данные, номер последовательности и CRC передаются дважды и подвергаются перекрестной проверке в точке получения.

6.3.4 Рассылка отчетов

Для VCR рассылки отчетов не существует расширения протокола FSCP 1/1, и потому он не является доверенным. Устройство безопасности может отправлять сигналы тревоги, не связанные с безопасностью.

6.3.5 Операция FBAP в шлюзовом устройстве

Прикладной процесс в шлюзовом устройстве оценивается таким же образом, как и FBAP FSCP 1/1.

6.3.6 Коммуникации протокола ядра управления системой (SMKP)

SMKP является частью черного канала. Сбои в локальном интерфейсе между SMKP и прикладным процессом управляются средствами, определенными изготовителем.

6.4 Профили

6.4.1 Общие положения

Профиль является подмножеством, набором, выбранным из большей общей спецификации. Профиль FSCP 1/1, таким образом, является ограниченной версией полного функционала FSCP 1/1. Для FSCP 1/1 создаются новые профили.

6.4.2 Профиль FSCP 1/1

6.4.2.1 Общие положения

Устройства H1 FSCP 1/1 могут также быть распределены по классам, основываясь на их функциональных возможностях.

Устройства H1 FSCP 1/1 принадлежат одному или нескольким из следующих наборов классов:

- полевые устройства H1 FSCP 1/1 — устройства управления, располагающиеся на каналах H1;
- хост-устройства FSCP 1/1 осуществляют интерфейс пользователя и функции конфигурации — логическое решающее устройство со средствами конфигурации.

6.4.2.2 Параметризация блока

Все параметры в блоках безопасности могут быть записаны либо с помощью VCR клиент/сервер, не связанной с FSCP 1/1, перед тем, как объект канала клиент/сервер FSCP 1/1 был создан, или с помощью VCR клиент/сервер FSCP 1/1 после того, как объект канала клиент/сервер FSCP 1/1 был создан. FSCP 1/1 необходимо, чтобы блок ресурсов был «разблокирован» перед тем, как что-либо будет записано в ресурс. После внесения изменений должен быть выполнен функциональный тест.

6.4.2.3 Блокировка параметризации блока

Перед тем, как появится возможность записывать параметры, ресурс должен быть разблокирован. Это равносильно применению ключа блокировки на пульте управления системой безопасности. Так как может быть несколько устройств безопасности и так как их часто необдуманно устанавливают в опасных зонах или как-то иначе делают недоступными, то разблокировка и блокировка будут также возможны через коммуникации FSCP 1/1. Блокировка записи программного обеспечения обязательна для блока ресурсов безопасности.

Одной из многих возможных подобных реализаций будет функциональный блок, который, при активации ввода, записывает параметр блокировки записи в устройстве для того, чтобы включить возможность конфигурации. Для этой цели предоставляется функциональный блок.

6.4.2.4 Аутентификация пользователя

Программное обеспечение хоста должно гарантировать, что только авторизированные пользователи получают доступ к программированию и параметризации.

6.4.2.5 Блокировка программирования

Перед тем, как появится возможность изменять объекты, ресурс должен быть разблокирован. Это равносильно применению ключа блокировки на пульте управления системой безопасности. Так как может быть несколько устройств безопасности и так как их часто необдуманно устанавливают в опасных зонах или как-то иначе делают недоступными, то разблокировка и блокировка будут возможны через коммуникации FSCP 1/1. Блокировка программирования реализуется параметром блокировки записи в ресурс в блоке ресурсов. Объекты, отличные от блоков, такие как объекты каналов, могут быть записаны только, когда ресурс разблокирован.

Изменения программ должны выполняться в одно время с выключением процесса (устройства по-прежнему будут выполнять блоки), в котором хост взаимодействует с устройствами.

6.5 Описания устройств

Описания устройств являются неотъемлемой частью средств конфигурации. Хэш MD5 будет сгенерирован для каждого из DD и файлов возможностей для обеспечения целостности файлов. Хэш MD5 для файлов DD/CF будет храниться, защищенный специальным ключевым словом в файле возможностей FSCP 1/1. Это показано на рисунке 15.

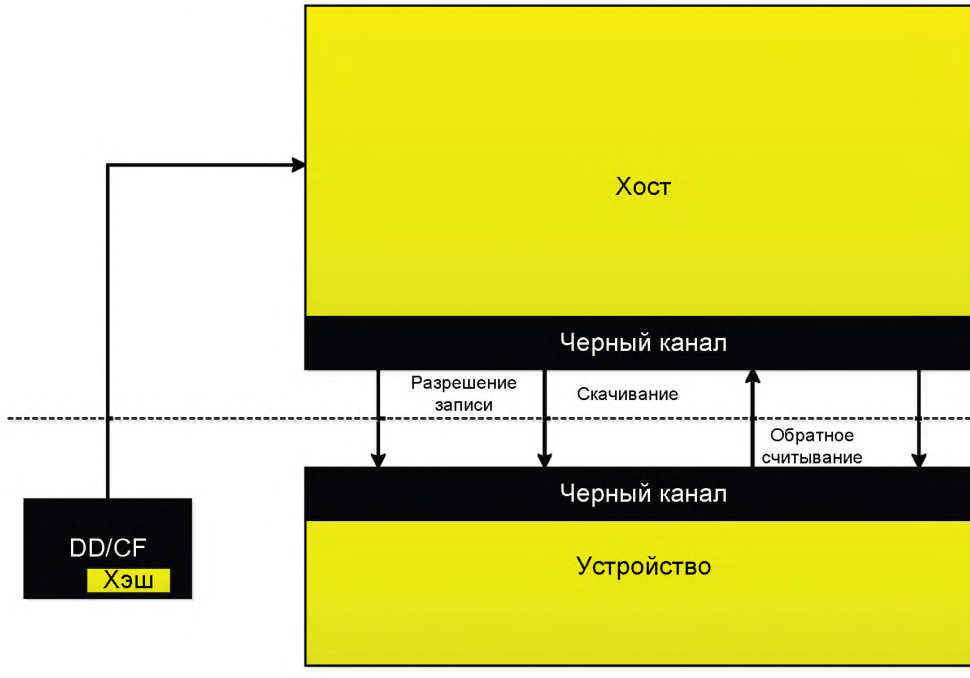


Рисунок 15 — Пример описания устройства

6.6 Распространенные форматы файлов

Файлы возможностей являются неотъемлемой частью средств конфигурации. Механизм хэша описан для DD и будет таким же для CF.

Хэш-сумма MD5 для файлов DD и CFF хранится в конце CFF файла.

Файл возможностей содержит параметры, оповещающие о частоте отказов устройства. Существуют также параметры для уровня проектирования изделия, то есть приобретенное предотвращение сбоев (например, в ходе проектирования требования для УПБ 2 устройства могли выполняться, даже если частоты отказов подходят для УПБ 3).

6.7 Информация о конфигурации

6.7.1 Обзор

Конфигурация FSCP 1/1 в основном не будет отличаться от конфигурации, не связанной с безопасностью, но будет дополнительно включать запись параметров безопасности функционального блока, таких как: таймер устаревания данных, предельное значение непрерывного счетчика устаревания и макроцикл. Ссылки функционального блока FSCP 1/1 используют объект канала безопасности там, где требуется установить ключ соединения. Предполагается, что средства конфигурирования автоматически осуществляют конфигурирование ключа соединения и макроцикла. После того как устройство было приведено в рабочее состояние, внесение изменений в какие-либо функциональные блоки запрещается.

6.7.2 Конфигурация уровня 1. Определение устройства изготовителем

Вопросы реализации устройств безопасности включают в себя меры для физического и логического разделения связанных с безопасностью (прикладной процесс и коммуникационный уровень безопасности) и недоверенных (стек черного канала) функций для того, чтобы обеспечить отсутствие помех. Приложения функционального блока для связанных и не связанных с безопасностью применений могут размещаться в одном или разных VFD (виртуальное полевое устройство).

6.7.3 Конфигурация уровня 2. Определение сети

Конфигурация черного канала не изменена.

6.7.4 Конфигурация уровня 3. Определение распределенного приложения

Для функциональных блоков безопасности используется особый объект канала. Должно быть вычислено ожидаемое время прохождения сигнала для канала.

Пользователь определяет время безопасности процесса. Макроцикл, предельные значения непрерывного счетчика устаревания и таймер устаревания данных должны быть сконфигурированы соответствующим образом.

6.7.5 Конфигурация уровня 4. Конфигурация устройства

Время макроцикла должно быть установлено с помощью параметра из блока ресурсов.

7 Протокол коммуникационного уровня безопасности

7.1 Формат PDU безопасности

7.1.1 Общие положения

Протокол FSCP 1/1 управляет отказами, происходящими во время коммуникаций. Протокол FSCP 1/1 применяется к протоколу коммуникаций FMS. Сбои в локальном интерфейсе между прикладным процессом и SMK, а также SMIB в NMA управляются средствами, определенными изготовителем. Протокол FSCP 1/1 применяется при FMS для коммуникаций на всей полевой шине.

7.1.2 CRC коммуникационного уровня безопасности

Проверка циклически избыточным кодом используется для управления отказами, связанными с искажением данных, происходящими в коммуникациях полевой шины.

Данные передаются вместе с вычисленной контрольной суммой CRC для каждого PDU. CRC коммуникационного уровня безопасности определен в CCITT 32 V.42 и ИСО/МЭК 8802-3 (ИИЭР 802.3). CRC представляет из себя 32-битный полином, вычисляемый следующим образом: ($x^{32} + x^{26} + x^{23} +$ $+ x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$).

Коммуникационный уровень безопасности приемника повторно вычисляет контрольную сумму полученных данных и сравнивает результат с полученной контрольной суммой. Искаженные сообщения отклоняются.

7.1.3 Контроль синхронизации времени на черном канале

Номер последовательности основан на номере макроцикла, полученном из времени канала данных для каждой публикации. Номер последовательности, по сути, является своего рода отметкой времени. Все устройства в сети H1 имеют единое восприятие макроцикла. Таким образом, устройства в сети работают с единым временем, реализуемым корректно функционирующим механизмом синхронизации времени. Синхронизация времени требуется для обеспечения синхронного выполнения функциональных блоков и коммуникаций, тем самым обеспечивая минимально возможное время реакции функции безопасности. Механизм синхронизации времени корректирует время и частоту канала данных и размещается в черном канале, но не контролируется коммуникационным уровнем безопасности. Коммуникационный уровень безопасности обладает независимым источником времени безопасности и обнаруживает потерю синхронизации времени в черном канале, сравнивая частоту синхронизации FSCP 1/1 с частотой синхронизации черного канала при синхронизации часов. Если отклонение превышает допустимое значение, то срабатывает предварительно сконфигурированное действие состояния сбоя, устанавливая статус BAD для вводов и выводов функциональных блоков. Блок ресурсов имеет параметр ошибки черного канала с флажком ошибки синхронизации времени.

На распределение времени от устройства, контролирующего время (LAS), к другим устройствам могут повлиять задержки в очередях коммуникаций, так же как и другие публикации канала. Локальный черный канал включает в себя функцию, которая измеряет двухстороннюю задержку через черный канал для компенсации задержек в очередях. Это выполняется периодически и включает в себя запуск изменения в LAS. Данная функция не является функцией безопасности. Она предназначена для предотвращения ложных аварийных остановок, тем самым гарантируя лучшую готовность.

Устройство контроля синхронизации времени черного канала управляет следующими сбоями:

- быстрое, медленное время LAS или скачок времени LAS;
- сбой очереди (издателя/подписчика или распределения времени);
- перезапуск устройства;
- перезапуск функции безопасности;
- переключение LAS;
- перезапуск LAS;
- нарушение графика (LAS или полевого устройства);
- начальный запуск (конфигурация) (аналогично перезапуску функции безопасности);
- коммуникации (распределение потерь времени, данные взаимоконтроля или публикация).

7.1.4 Номер последовательности

Для связей VCR издателя/подписчика номер последовательности для каждой публикации основывается на номере макроцикла, который вычисляется на коммуникационном уровне безопасности из времени канала данных в начале каждого макроцикла. Функция контроля синхронизации времени черного канала на коммуникационном уровне безопасности обеспечивает правильность времени канала данных. Номер последовательности издателя/подписчика, по сути, является отметкой времени. Все устройства в сети H1 имеют единое восприятие макроцикла. Не должно существовать никаких подпланов, то есть функциональные блоки могут выполняться лишь однажды за макроцикл. В результате в ходе нормального функционирования номер последовательности увеличивается на единицу для каждой новой публикации канала. Номер последовательности включается в сообщение и сравнивается с ожидаемым номером последовательности на коммуникационном уровне безопасности на приемнике. Если превышена максимально допустимая разница, то у функционального блока будет установлен статус BAD для того, чтобы прикладной процесс был осведомлен об устаревании данных.

Если общее время ответа датчика исполнительному устройству нарушено из-за коммуникационных ошибок, выполнения функционального блока, сбоев планирования или по любой другой причине, то на выводе будет выполнено предварительно сконфигурированное действие состояния сбоя. Если имеется цепь связанных функциональных блоков, выполняющих функцию безопасности, то с помощью нескольких счетчиков устаревания канала можно продлить время ответа перед обнаружением сбоя. В отличие от ситуации, когда каждому каналу достается счетчик устаревания, как это используется в коммуникациях, не связанных с FSCP 1/1, счетчики устаревания диагностируются непрерывно («из конца в конец»). Это, по сути, измерение задержки распространения. Максимальное время ответа от датчика к исполнительному устройству, разрешенное приложением (выраженное в единицах макроцикла), должно быть сконфигурировано с помощью непрерывного счетчика устаревания объекта канала. Если предельное значение непрерывного счетчика устаревания превышено, то коммуникационный уровень безопасности устанавливает на функциональном блоке статус «BAD». Так как коммуникационный уро-

вень безопасности извлекает номер последовательности из номера макроцикла только когда выводы функционального блока обновлены и каждый индивидуальный функциональный блок обновляет только свой вывод, если вводные условия верны (последующая публикация, таким образом, вызывает генерацию номера последовательности), то счетчики устаревания изменяются по направлению основного трафика и накапливаются. В таком случае, когда все каналы функционируют и все функциональные блоки выполняются должным образом, номер последовательности (основанный на номере макроцикла на датчике) распространяется из конца в конец и совпадает с макроциклом (ожидаемым номером последовательности) в клапане. При сравнении с макроциклом на устройстве вывода номер указывает на общее число пропущенных коммуникаций и выполнений в цепи функциональных блоков, выполняющих функцию безопасности. Это приводит к гораздо более короткому времени реакции в наихудшем случае. Критерий, определяющий необходимость обновления при новом выводе, зависит от конкретного функционального блока. Новый номер последовательности генерируется коммуникационным уровнем безопасности только во время публикации нового сообщения. Определенным функциональным блокам могут потребоваться все использованные вводы для того, чтобы соответствовать текущему времени, в то время как другие функциональные блоки обладают возможностью выбирать, для чего требуется только определенное число использованных вводов для соответствия текущему времени.

Уровень FSCP 1/1 нуждается в одном счетчике номера последовательности для каждой VCR связи клиент/сервер. Номер последовательности клиент/сервер увеличивается на единицу для каждой передачи. В случае VCR клиента/сервера если номер последовательности не синхронизирован, то соединение обрывается. Номера последовательности устанавливаются повторно, когда устанавливается новое соединение.

7.1.5 Виртуальный заголовок

Заголовок протокола, такой как адрес, находясь в кадре черного канала, не защищен с помощью CRC коммуникационного уровня безопасности, и поэтому в приложениях, связанных с безопасностью, на него нельзя полагаться. Отсюда, таким образом, возникает необходимость использовать другой механизм для уникальной идентификации связи источник—назначение в рамках сообщения FSCP 1/1, но защищенный с помощью CRC коммуникационного уровня безопасности. Для этой цели используется ключ соединения. Но отправка ключа соединения в каждом сообщении приводит к издержкам. Для снижения издержек CRC коммуникационного уровня безопасности вычисляется в данных безопасности и виртуальном заголовке, включая ключ соединения и индекс объекта. Ключ соединения не передается по шине, но CRC коммуникационного уровня безопасности при получении приведет к отказу, если ключ соединения неверен. Объект канала безопасности содержит ключ соединения, что делает возможным вычисление CRC.

7.1.6 Ключ соединения

Протокол содержит механизм для уникальной идентификации сообщений FSCP 1/1 для того, чтобы одно сообщение FSCP 1/1 не подменяло другое сообщение FSCP 1/1: каналы функционального блока FSCP 1/1 будут идентифицированы уникальным 32-битным ключом соединения. Ключ соединения будет принят хостом и записан в объектах канала безопасности. Ключ соединения является частью виртуального заголовка, вложенного в CRC коммуникационного уровня безопасности, но он не сообщается. Любое несоответствие в ключе соединения не проверяется явным образом в подписчике или сервере, но несоответствие вызовет ошибку CRC уровня коммуникаций безопасности. Т. е. ошибка CRC коммуникационного уровня безопасности может указывать на искажение данных или несоответствие ключа соединения.

7.1.7 Избыточность и перекрестная проверка

Протокол коммуникационного уровня безопасности содержит механизм, который передает две копии всех данных целиком, включая номер последовательности и CRC в одном кадре. В точке приемника две копии проходят перекрестную проверку для обнаружения искажений.

Одним из возможных вариантов реализации является устройство, содержащее два избыточных микроконтроллера, каждый из которых строит свое сообщение передачи независимо от другого. Два независимых сообщения с данными совместно добавляются интерфейсом черного канала и совместно передаются в одном кадре. В свою очередь, при получении двух независимых сообщений с данными в кадре, поступившем от черного канала, они распаковываются каждый в соответствующий микроконтроллер, который затем производит перекрестную проверку.

7.2 Расширения протокола для применения в системах, связанных с безопасностью

7.2.1 Обзор

Для того чтобы использовать устройства полевых шин в системе, связанной с безопасностью, необходимо расширить протокол полевой шины для обеспечения перехода процесса в безопасное состояние при возникновении отказов.

FMS и все остальные коммуникационные уровни, включая SMK, обрабатываются как черный канал. В связи с этим все расширения протокола реализуются на уровне пользователя или в прикладном процессе функционального блока.

Кроме объекта канала безопасности, не устанавливаются никакие новые типы данных. Данные, которые передаются с помощью FMS, будут включать в себя расширения протокола. Расширения зависят от типа взаимодействия.

Примечание — CRC 32 описан в 7.1.2.

7.2.2 Взаимодействия издатель—подписчик

7.2.2.1 Общие положения

На весь сегмент H1 приходится только один макроцикл. Все устройства в сегменте H1, включая LAS, должны конфигурироваться с одним счетчиком макроциклов. Функциональный блок в устройстве должен в соответствии с планом выполняться только однажды за макроцикл. В начале выполнения функционального блока текущий номер макроцикла (MCN) должен вычисляться следующим образом:

MCN = DL – время / длительность макроцикла.

MCN должно быть 16-битным целым числом без знака.

Примечание — Если устройство обладает множеством функциональных блоков, то MCN лучше вычислять в начале макроцикла, чем в начале выполнения каждого функционального блока, если это возможно.

7.2.2.2 Издатель

7.2.2.2.1 Установление соединения

На публикацию параметра функционального блока безопасности для использования его в функции безопасности указывает присутствие объекта канала безопасности. Если для публикации имеется объект канала безопасности, то FBAP издателя установит соединение с издателем идентичным образом, как и не связанное с безопасностью соединение с издателем.

7.2.2.2.2 Публикация данных

В конце выполнения функциональный блок безопасности должен определить, какие из его выводных параметров должны быть опубликованы. Выбор параметров для публикации зависит от типа функционального блока и статуса его вводных параметров. Публикуемые параметры не рассматриваются в настоящем стандарте.

Функциональный блок публикует свои выбранные параметры (если такова его конфигурация) с помощью расширенного протокола. На публикацию параметров функционального блока безопасности для использования его в функции безопасности указывает присутствие объекта канала безопасности. Опубликованное значение параметра будет защищено от возможного искажения, дублирования и от приема вне последовательности, вызванных черным каналом. Для защиты данных от искажения используется CRC 32. Виртуальный PDU формируется, как показано на рисунке 16.

Ключ соединения (4 октета)	Индекс объекта (4 октета)	Номер последовательности (4 октета)	Значение и статус объекта (2-120 октет)

Рисунок 16 — PDU безопасности, демонстрирующий виртуальное содержимое

Используются только младшие два октета индекса объекта. Старшие два октета установлены в ноль. CRC 32 вычисляется на основе виртуального PDU безопасности. Данные, предназначенные для информационного отчета, модифицированы для включения в них номера последовательности и CRC 32 и продублированы. Формат данных показан на рисунке 17.

Данные 1			Данные 2		
Исходные данные	Номер последовательности	CRC 32	Исходные данные	Номер последовательности	CRC 32

Рисунок 17 — PDU безопасности, показывающий дублирование данных и добавление CRC

Формат «Исходных данных» идентичен данным, которые бы содержались в части данных информационного отчета для данных, не связанных с безопасностью. Номер последовательности и CRC32 прилагаются к этим данным. Функциональный блок должен установить номер макроцикла как номер последовательности.

Функциональный блок должен установить статус опубликованных выводных параметров как «ad::black channel failure» (отказ черного канала), если синхронизация времени черного канала не работает корректно, т.е. BLK_CHN_ERR отлично от нуля.

Рисунок 18 и таблицы 5, 6 и 7 определяют машину состояний для издателя.

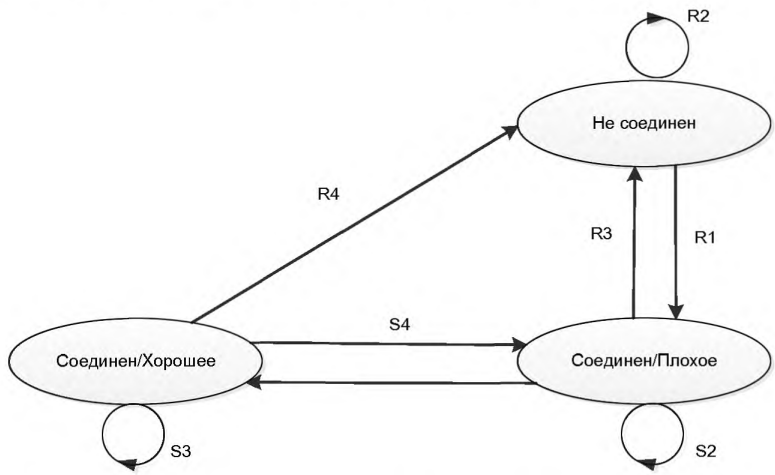


Рисунок 18 — Диаграмма перехода состояний для издателя FSCP 1/1

Таблица 5 — Состояния издателя

Состояние	Описание
Не соединен	Для публикации не установлено никакой VCR
Соединен/Плохое	VCR установлена, но ошибки черного канала не устранены
Соединен/Хорошее	VCR установлена, осуществляются нормальные публикации

Таблица 6 —Таблица состояний издателя. Полученные переходы

#	Текущее состояние	Действие события и условия	Следующее состояние
R1	Не соединен	RcvMsg() = "FMS Initiate.cnf"	Соединен/Плохое
R2	Не соединен	RcvMsg() = "Any message (not FMS Initiate.cnf)"	То же самое
R3	Соединен/ Плохое	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен
R4	Соединен/ Хорошее	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен

Таблица 7 —Таблица состояний издателя. Внутренние переходы

#	Текущее состояние	Действие события и условия	Следующее состояние
R1	Соединен/ Плохое	BLK_CHN_ERR = 0 SET Sequence Number = MCN	Соединен/ Хорошее
R2	Соединен/ Плохое	BLK_CHN_ERR <> 0 SET Black Channel Failure SET Sequence Number = MCN	То же самое
R3	Соединен/ Хорошее	BLK_CHN_ERR = 0 SET Sequence Number = MCN	То же самое
R4	Соединен/ Хорошее	BLK_CHN_ERR <> 0 SET Black Channel Failure SET Sequence Number = MCN Примечание — Функциональный блок определяет, будут ли опубликованы выводные параметры или нет. Логика зависит от номеров последовательности, полученных в его вводных параметрах	Соединен/ Плохое

7.2.2.3 Подписчик

7.2.2.3.1 Установление соединения

На подписку параметра функционального блока безопасности для использования его в функции безопасности указывает присутствие объекта канала безопасности. Если для подписания имеется объект канала безопасности, то FBAP подписчика должен установить соединение с подписчиком идентичным образом, как и не связанное с безопасностью соединение с подписчиком.

7.2.2.3.2 Подписка данных

MCN, вычисляемый в начале выполнения блока, является номером последовательности, ожидаемым от издателя, каждого из соединений издатель—подписчик в блоке. Если опубликованные данные не являются состоянием или если в черном канале нет никаких накопленных задержек, то полученный номер последовательности будет совпадать с MCN.

Когда FBAP получает данные FMS, как показано на рисунке 19, для VCR, ассоциированной с объектом канала безопасности, то:

a) сравниваются две копии исходных данных (Данные 1 и Данные 2), и если они идентичны, то осуществляется переход к b), в противном случае сообщение отклоняется и счетчик устаревания увеличивается на 1;

Данные 1			Данные 2		
Исходные данные	Номер последовательности	CRC 32	Исходные данные	Номер последовательности	CRC 32

Рисунок 19 — PDU безопасности, показывающий дублирование данных и добавление CRC

b) виртуальный PDU безопасности, идентичный VSPDU, используемому в публикации данных, формируется так, как показано на рисунке 20.

Ожидаемый ключ соединения (4 октета)	Ожидаемый индекс объекта (4 октета)	Полученный номер последовательности (4 октета)	Полученные значение и статус объекта (2-120 октет)

Рисунок 20 — PDU безопасности, показывающий виртуальное содержимое

Ожидаемые ключ соединения и индекс объекта извлекаются из объекта канала безопасности. Для H1 используются только два младших октета индекса объекта. Двум старшим октетам устанавливается нулевое значение. Номер последовательности, значение объекта и статус заполняются из

принятых данных. Номер последовательности и индикация дублированных данных, предоставленные черным каналом, игнорируются;

c) CRC 32 вычисляется на основе VSPDU. Затем CRC 32 сравнивается с CRC 32, принятым в части данных PDU FMS. Если вычисленный CRC 32 не соответствует полученному CRC 32, то блок PDU будет отклонен. Если CRC не соответствует, то счетчик устаревания увеличивается на 1;

d) если CRC 32 действителен и номер последовательности соответствует MCN, то полученные данные используются;

e) если CRC 32 действителен, а номер последовательности не соответствует MCN, то счетчик устаревания увеличивается на 1. Данные отклоняются;

f) если счетчик устаревания превышает сконфигурированный предел непрерывного счетчика устаревания, то статус входного параметра должен быть «bad::black channel failure» (отказ черного канал). Данные отклоняются;

g) Если синхронизация времени черного канала не работает, т. е. бит BLK_CHN_SYNC_ERR в параметре BLK_CHN_ERR в блоке ресурсов равен TRUE, то должен быть установлен следующий статус входных параметров «bad::black channel failure». Данные отклоняются.

Таблица 8, рисунок 21 и таблицы 9 и 10 определяют машину состояний для подписчика.

Таблица 8 — Состояния подписчика

Состояние	Описание
Не соединен	Для публикации не установлено никакой VCR
Соединен/Устаревшее	VCR установлена, но ошибки черного канала или счетчик устаревания не очищены
Соединен/Хорошее	VCR установлена, осуществляются нормальные публикации

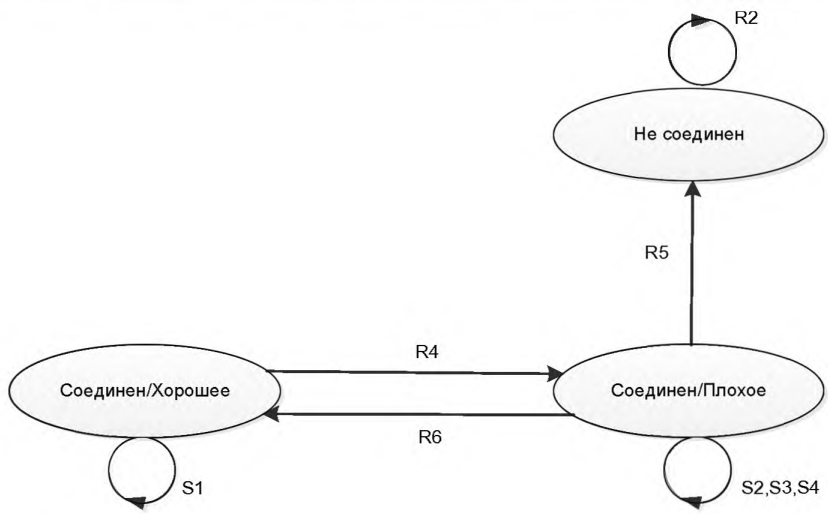


Рисунок 21 — Диаграмма перехода состояний для подписчика FSCP 1/1

Таблица 9 — Таблица состояний подписчика. Полученные переходы

#	Текущее состояние	Действие события и условия	Следующее состояние
R1	Не соединен	RcvMsg() = "FMS Initiate.cnf"	Соединен/Устаревшее
R2	Не соединен	RcvMsg() = "Любое сообщение (не FMS Initiate.cnf)"	То же самое
R3	Соединен/ Устаревшее	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен

Окончание таблицы 9

#	Текущее состояние	Действие события и условия	Следующее состояние
R4	Соединен/ Устаревшее	Sequence Number = MCN И BLK_CHN_ERR = 0 SET Use Data Stale Count = 0	Соединен/Хорошее
R5	Соединен/ Хорошее	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен
R6	Соединен/ Хорошее	Stale Count > End-to-end stale count ИЛИ BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Соединен/Устаревшее

Таблица 10 — Таблица состояний подписчика. Внутренние переходы

#	Текущее состояние	Действие события и условия	Следующее состояние
S1	Соединен/ Устаревшее	Sequence Number = MCN ИЛИ Data 1 <> Data 2 ИЛИ BLK_CHN_ERR <> 0 SET Status = Bad::Black channel failure Discard data	Соединен/Хорошее
S2	Соединен/ Хорошее	(Sequence Number <> MCN OR Data 1 <> Data 2) И Stale Count <= End-to-end stale count И BLK_CHN_ERR = 0 Increment Stale Count Discard data	То же самое
S3	Соединен/ Хорошее	CRC 32 is invalid И BLK_CHN_ERR = 0 Increment Stale Count Discard data	То же самое
S4	Соединен/ Хорошее	Sequence Number = MCN И Data 1 = Data 2 И BLK_CHN_ERR = 0 SET Stale Count = 0 Use data	То же самое

7.2.3 Взаимодействия клиент—сервер

7.2.3.1 Общие положения

VCR клиент—сервер для чтения данных из функциональных блоков безопасности должна быть установлена так, чтобы максимальное значение параллельного доступа было равно 1. Устройство должно отклонять все инициируемые FMS запросы к VCR с установленным значением параллельного доступа больше, чем 1.

7.2.3.2 Чтение

Запрос на чтение для чтения данных из функциональных блоков безопасности (т. е. данных для использования в функции безопасности) идентичен запросу на чтение данных из функциональных блоков, не связанных с безопасностью.

FMS предоставляет индекс объекта (и дополнительный подиндекс), который считывается. Если чтение предназначено для функционального блока, то устройство должно проверять наличие в данном блоке действительного объекта канала безопасности с операцией обслуживания, установленной на SIS_ACCESS. Если действительный объект канала отсутствует, то устройство отвечает на чтение так же, как на чтение параметра функционального блока, не связанного с безопасностью.

Если действительный объект канала безопасности существует и уже существует запрос на чтение или запись, ожидающий ответа, то устройство должно отказать в запросе на чтение или запись и отправить негативный ответ.

Если действительный объект канала безопасности существует и больше нет никаких ожидающих выполнения запросов записи/чтения, то устройство отвечает на данные, используя расширенный протокол. Эти данные будут защищены от возможного искажения, дублирования и приема вне последовательности, вызванных черным каналом. Для защиты данных от искажения используется CRC 32 и для вычисления CRC 32 формируется виртуальный PDU, как показано на рисунке 22. Если чтение является чтением с помощью подиндекса, то подиндекс также используется при вычислении CRC 32. Для H1 используются только два младших октета индекса объекта. Значение старших двух октетов устанавливается в ноль.

Ключ соединения (4 октета)	Индекс объекта (4 октета)	Номер последовательности (4 октета)	Значение и статус объекта (2-120 октет)

Рисунок 22 — PDU безопасности, показывающий виртуальное содержимое

Если чтение осуществляется по подиндексу, то VSPDU должен включать подиндекс. Подиндекс должен быть включен в вычисление CRC 32. Виртуальный PDU показан на рисунке 23.

Ключ соединения (4 октета)	Индекс объекта (4 октета)	Подиндекс (1 октет)	Номер последовательности (4 октета)	Значение и статус объекта (2-120 октет)

Рисунок 23 — PDU безопасности, показывающий виртуальное содержимое с подиндексом

CRC 32 вычисляется из виртуального PDU безопасности. Данные, предназначенные для FMS Read.res, модифицированы для дублирования данных включения номера последовательности и CRC 32. Формат данных показан на рисунке 24.

Данные 1			Данные 2		
Исходные данные	Номер последовательности	CRC 32	Исходные данные	Номер последовательности	CRC 32

Рисунок 24 — PDU безопасности, показывающий дублирование данных, а также добавление номера последовательности и CRC

«Исходные данные» имеют формат, идентичный формату данных, которые бы содержались в поле данных FMS Read.res, предназначенном для функциональных блоков, не связанных с безопасностью. Номер последовательности и CRC 32 прилагаются к этим данным. Номер последовательности увеличивается для каждого PDU, выданного черному каналу для коммуникаций.

Вычисление номера последовательности ведется для каждого соединения коммуникационного уровня безопасности, т. е. ключа соединения. Номер последовательности обнуляется после установления соединения. Номер последовательности увеличивается на 1.

Примечание — ID вызова (Invoke ID) не включено в вычисление CRC 32.

Если устройство дает негативный ответ, то такой ответ будет идентичен негативному ответу для функциональных блоков, не связанных с безопасностью. Другими словами, номер последовательности не увеличивается; не требуется формировать виртуальный PDU безопасности.

Машина состояний для обработки чтений показана в таблице 11, на рисунке 25 и в таблице 12.

Таблица 11 — Состояния сервера во время операций чтения

Состояние	Описание
Не соединен	Не установлено никакого соединения
Соединен	Соединение установлено

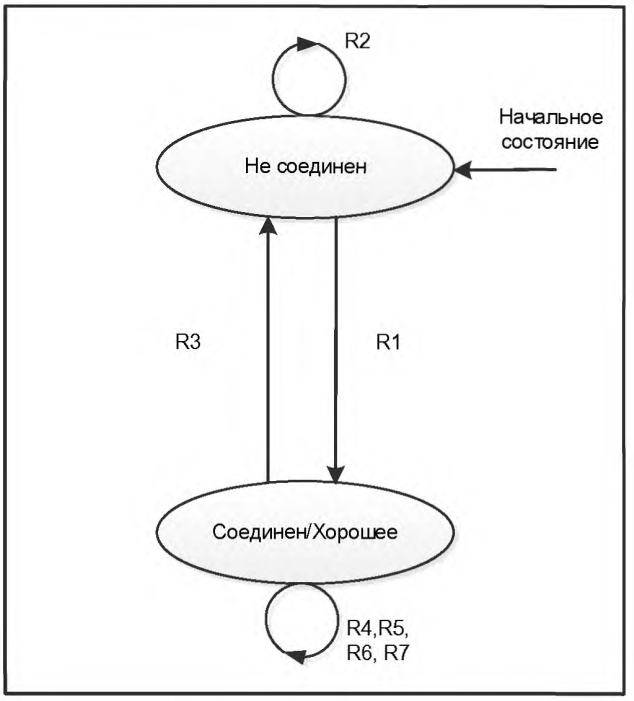


Рисунок 25 — Диаграмма перехода состояний для сервера FSCP 1/1 во время операций чтения

Таблица 12 — Полученные переходы для сервера FSCP 1/1 во время операций чтения

#	Текущее состояние	Действие события и условия	Следующее состояние
R1	Не соединен	RcvMsg() = "Connection Request valid response" Set Sequence number = o	Соединен
R2	Не соединен	RcvMsg() = "Любое сообщение (не connection request valid response)"	То же самое
R3	Соединен	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"	Не соединен
R4	Соединен	Запрос Valid Read И присутствует объект канала безопасности И Никакие запросы FMS не ожидают выполнения Ответить с помощью протокола уровня коммуникаций безопасности	Соединен
R5	Соединен	запрос Valid Read И объект канала безопасности отсутствует Ответить с помощью FMS протокола	Соединен

Окончание таблицы 12

#	Текущее состояние	Действие события и условия	Следующее состояние
R6	Соединен	запрос Valid Read И присутствует объект канала безопасности И Другие запросы FMS ожидают выполнения Вернуть негативный ответ	Соединен
R7	Соединен	Недействительный запрос Вернуть негативный ответ	Соединен

7.2.3.3 Запись

Запрос на запись данных в функциональные блоки безопасности будет следовать расширенному протоколу. Клиенты, инициирующие запрос на запись, должны форматировать данные в соответствии с форматом PDU безопасности, описанным ниже и показанным на рисунке 26.

FMS предоставляет индекс записываемого объекта. Если запись осуществляется для функционального блока безопасности, устройство должно проверять, отформатирована ли запись в соответствии с расширенным протоколом.

Другими словами, устройство проверяет, идентичны ли Данные 1 Данным 2. В случае идентичности устройство определяет, обладает ли пакет действительным номером последовательности и добавленным CRC 32. В случае неидентичности данные отклоняются и возвращается негативный ответ. Последовательность является действительной, если она на 1 (без знака) больше последнего номера последовательности, принятого в этом соединении (LRSN), т. е. номера последовательности должны отслеживаться по ключам соединения. Если номер последовательности неверен, то устройство должно увеличить LRSN.

Данные 1			Данные 2		
Исходные данные	Номер последовательности	CRC 32	Исходные данные	Номер последовательности	CRC 32

Рисунок 26 — PDU безопасности, показывающий дублирование данных и добавление номера последовательности и CRC

«Исходные данные» имеют формат идентичный формату данных, которые бы содержались в части данных FMS Write.ind, предназначенной для функциональных блоков, не связанных с безопасностью.

Устройство затем определяет, имеется ли для функционального блока действительный объект канала безопасности, у которого значение операции обслуживания («Service Operation») равно SIS_ACCESS. Если действительный объект канала безопасности отсутствует, то устройство отклоняет запрос на запись и возвращает негативный ответ.

Если действительный объект канала существует, то устройство конструирует виртуальный PDU безопасности (VSPDU), как показано на рисунке 27. Ожидаемый ключ соединения берется из объекта канала безопасности. Если запись осуществляется с подиндексом, то подиндекс также должен быть включен, как это показано на рисунке 28. Используются два младших октета индекса объекта. Два старших октета обнулены.

Ожидаемый ключ соединения (4 октета)	Индекс объекта (4 октета)	Номер последовательности (4 октета)	Значение и статус объекта (2-120 октет)

Рисунок 27 — Пример записи FSCP 1/1

Ожидаемый ключ соединения (4 октета)	Индекс объекта (4 октета)	Подиндекс (1 октет)	Номер последовательности (4 октета)	Значение и статус объекта (2-120 октет)

Рисунок 28 — Пример записи FSCP 1/1 с подиндексом

CRC 32 вычисляется из виртуального PDU безопасности и сравнивается с CRC 32 в принятых данных. Если CRC не совпадают, то устройство должно отклонить данные и вернуть негативный ответ.

Если все проверки пройдены, то устройство выполняет запрос на запись. Позитивный или негативный ответ возвращается с помощью особого блока, в который ведется запись.

Позитивный или негативный ответ на запись обладает таким же форматом, как и и ответ на запись от функционального блока, не связанного с безопасностью.

Машина состояний для обработки записей показана в таблице 13, на рисунке 29 и в таблице 14.

Таблица 13 — Состояния сервера FSCP 1/1 во время операций записи

Состояние	Описание
Не соединен	Не установлено никакого соединения
Соединен	Соединение установлено

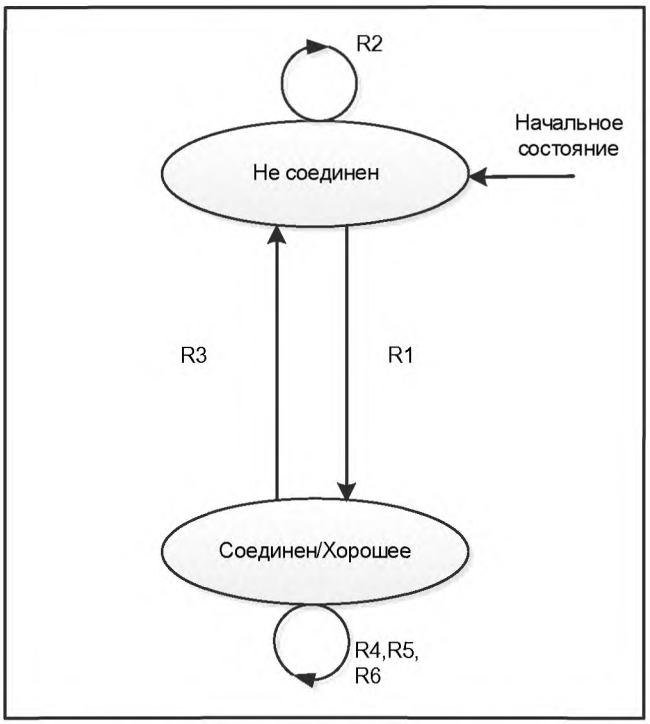


Рисунок 29 — Диаграмма перехода состояний для сервера FSCP 1/1 во время операций записи

Таблица 14 — Принятые переходы для сервера FSCP 1/1 во время операций записи

#	Текущее состояние	Действие события и условия	Следующее состояние
R1	Не соединен	RcvMsg() = "Connection Request valid response" Set LRSN = 0	Соединен
R2	Не соединен	RcvMsg() = "Любое сообщение (не connection request valid response)"	То же самое
R3	Соединен	RcvMsg() = "Abort.ind" ИЛИ RcvMsg() = "Abort.req"OR	Не соединен

Окончание таблицы 14

#	Текущее состояние	Действие события и условия	Следующее состояние
R4	Соединен	запрос Valid Write И объект канала безопасности присутствует И CRC 32 is OK И Номер последовательности OK И Никакие запросы FMS не ожидают выполнения Прирастить LRSN Ответить с помощью протокола уровня коммуникаций, связанного с безопасностью	Соединен
R5	Соединен	Данные 1 не идентичны Данным 2 ИЛИ отсутствует объект канала безопасности ИЛИ CRC 32 not OK ИЛИ Недействительный запрос на запись Вернуть негативный ответ	Соединен
R6	Соединен	Действительный запрос на запись И присутствует объект канала безопасности И Номер последовательности OK И Другие запросы FMS ожидают выполнения Вернуть негативный ответ	Соединен

7.2.3.4 Записи для объекта канала безопасности

Записи в объект канала безопасности должны выполняться в соответствии с расширенным протоколом, как установлено ниже. Запрос на запись данных в функциональные блоки безопасности будет следовать расширенному протоколу. Клиент должен вычислить CRC 32 по индексу объекта канала безопасности и данным объекта канала, именно в такой последовательности.

FMS предоставляет индекс объекта, который записывают. Если запись осуществляется для функционального блока безопасности, устройство должно проверять, отформатирована ли запись в соответствии с расширенным содержанием PDU, как показано на рисунке 30. Другими словами, устройство проверяет, идентичны ли Данные 1 Данным 2. В случае идентичности устройство определяет, обладает ли пакет действительным добавленным CRC 32. В случае неидентичности данные отклоняются и возвращается негативный ответ. CRC 32 вычисляется по индексу объекта канала безопасности и данным объекта канала безопасности, именно в такой последовательности. Если вычисленный CRC не соответствует полученному CRC, то устройство должно отклонить запись и вернуть негативный ответ. Устройство не должно поддерживать запись по подиндексу в объект канала безопасности. Если устройство получает запись по подиндексу, то ему необходимо отклонить запрос и вернуть негативный ответ.

Данные 1		Данные 2	
Данные объекта канала безопасности	CRC 32	Данные объекта канала безопасности	CRC 32

Рисунок 30 — PDU безопасности, показывающий дублирование данных и CRC

Затем устройство определяет, правильно ли отформатирован объект канала безопасности. Если это не так, то устройство должно отклонить запись и вернуть негативный ответ.

Объект безопасности должен быть записан только когда блок ресурсов неисправен (OOS). Если блок ресурсов не находится в состоянии OOS, устройство должно отклонить запись и вернуть негативный ответ.

Если все проверки пройдены, устройство выполняет запрос на запись и возвращает позитивный ответ.

Позитивный или негативный ответ на запись имеет такой же формат, как и ответ на запись от функционального блока, не связанного с безопасностью.

Что касается управления соединением, успешное внесение записи в объект канала безопасности должно вызывать такое же поведение, как и запись в объекты канала, не связанные с безопасностью. В дополнение к этому успешная запись должна перезапустить (установить значение 0) счетчик номера последовательности, связанного с ключом соединения, который записывается.

Устройство должно хранить CRC в своей нестирающейся при перебоях питания памяти как часть объекта канала безопасности. Предполагается, что устройство будет периодически и сразу же после запуска проверять целостность всех своих сконфигурированных объектов канала в соответствии с требованиями МЭК 61508. Если полнота не прошла проверку, устройство должно установить блок ресурсов в состояние OOS.

7.2.4 Синхронизация времени

Время (время канала данных, DL-время) синхронизируется черным каналом. Устройство контроля синхронизации времени коммуникационного уровня безопасности должно контролировать, работает ли синхронизация времени черного канала или нет. Коммуникационный уровень безопасности должен обладать специальным аппаратным таймером на кристалле с точностью хотя бы в 10^{-4} и разрешением минимум 100 мкс.

а) Устройство контроля синхронизации времени коммуникационного уровня безопасности выполняется после того, как черный канал обработает принятый PDU распределения времени. Оно должно определить, превышает ли допустимое значение сдвиг между временем черного канала и временем коммуникационного уровня безопасности. В приведенных ниже вычислениях англоязычные названия обозначают следующее:

Allowable drift — допустимый сдвиг;

Actual drift — действительный сдвиг;

Total Error — суммарная ошибка;

Time Sync Error — ошибка синхронизации времени.

Allowable drift = ($TLCTD_n$ — $TLCTD_{n-1}$) × SF_SYNC_DRIFT) / (60 × 32 000).

Примечания

1 Параметр (60 × 32 000) выражается в (1/32 мс)/мин.

2 Порядок вычисления важен для точности вычислений.

Actual drift = (TTD_n — TTD_{n-1}) - ($TLCTD_n$ — $TLCTD_{n-1}$).

Total Error = Total Error + Actual drift.

```
if [Total Error] > (Allowable Drift + SIF_SYNC_JITTER)
        Time Sync Error = 1
else
        Time Sync Error = 0.
```

В следующих уравнениях учитывается допустимый дрейф в суммарной ошибке.

```
if (|Total Error| > Allowable Drift) then
      if (Total Error > 0) then
            // Total Error положительна
            // Вычесть допустимый сдвиг из суммарной ошибки
            Total Error = Total Error — Allowable Drift
else
            // Добавить допустимый сдвиг к суммарной ошибке
            Total Error = Total Error + Allowable Drift
else
      // Величина Total Error меньше, чем Allowable Drift
      Total Error = 0,
```

где $TLCTD_n$ — время часов коммуникационного уровня безопасности после обработки текущего TD (распределения времени);

$TLCTD_{n-1}$ — время часов коммуникационного уровня безопасности после обработки предыдущего TD;

SIF_SYNC_D — параметр, определяющий допустимую интенсивность дрейфа.

Примечания

1 SIF_SYNC_DRIFT измеряется в (1/32 мс)/мин.

2 Допустимый диапазон для SIF_SYNC_DRIFT — это 100-1000.

3 Значение для SIF_SYNC_DRIFT по умолчанию равно 384. SIF_SYNC_JITTER — это параметр, определяющий допустимое дрожание импульсов синхронизации.

4 SIF_SYNC_JITTER измеряется в 1/32 ms.

5 Значение SIF_SYNC_JITTER по умолчанию равно 160.

6 Допустимый диапазон для SIF_SYNC_JITTER —это 0-320;

TTD_n —это DL — время после обработки текущего TD;

TTD_{n-1} _это DL — время после обработки предыдущего TD;

Total Error — это суммарная накопленная ошибка в 1/32 мс, содержащаяся в 32-битном значении со знаком;

Time Sync Error — это флаг, указывающий на ошибку синхронизации времени.

b) Если Time Sync Error равна 1, то устройство контроля должно установить для бита BLK_CHN_SYNC_ERR, параметра BLK_CHN_ERROR в блоке ресурсов, значение TRUE; в противном случае флаг должен иметь значение FALSE.

c) Если черный канал не получает действительный TD через 6 последовательных периодов распределения времени, то устройство контроля должно установить для бита BLK_CHN_SYNC_ERR, параметра BLK_CHN_ERROR в блоке ресурсов, значение TRUE.

d) Если BLK_CHN_SYNC_ERR имеет значение TRUE, то должно потребоваться устройство контроля синхронизации времени, чтобы черный канал предпринял синхронизацию времени, т. е. должен периодически (один раз в каждом периоде TD) отправлять команду черному каналу отправить CT последовательности.

e) Когда записан CLR_FAULT_STATE блока ресурсов, то примитив DL_RESET должен быть отправлен на уровень канала данных, если BLK_CHN_SYNC_ERR имеет значение TRUE.

7.2.5 Запуск устройства

Блок ресурсов коммуникационного уровня безопасности должен находиться в режиме OOS до тех пор, пока не будет выполнено следующее:

a) Устройство находится в списке действующих узлов (устройство является либо LAS, либо устройство приняло действительную последовательность PDU PN/PR/Активация).

b) DL для черного канала. Время является допустимым. Устройство является планировщиком LAS или же устройство обновило время, основываясь на действительном TD и PDU блоках RR.

7.3 Средство коммуникаций

7.3.1 Общие положения

Средство коммуникаций и SMK являются частями черного канала, которые существуют в устройстве, поэтому от них не требуется работа в среде с УПБ.

В средство коммуникаций не внесено никаких изменений.

7.3.2 Управление сетью

Управление сетью является частью черного канала. Не требуется никаких изменений.

7.3.3 FMS

FMS является частью черного канала. Не требуется никаких изменений.

7.3.4 Стек H1

Стек H1 является частью черного канала. Не требуется никаких изменений.

8 Управление коммуникационным уровнем безопасности

8.1 Обзор

SMK не является проверенным и является частью черного канала. Таким образом, SMK не должно выполняться в среде УПБ. Для любого локального взаимодействия между SMK и прикладным процессом требуются проверки, определяемые производителем, которые соответствуют требованиям МЭК 61508.

Установить адрес возможно только когда блок ресурсов устройства установлен в режим, позволяющий запись. Когда адрес меняется, то объекты канала удаляются. Адрес и тег устройства могут быть записаны только когда ресурс находится в режиме неисправности.

8.2 Коммуникации SMK

SMK является частью черного канала, и его коммуникации с прикладным уровнем не проверены. Коммуникации между SMK и прикладным процессом осуществляются через локальный интерфейс, и верификации выполняются внутри с помощью средств, определенных производителем.

8.3 Услуги FMS

SMIB является частью черного канала, но обменивается информацией с прикладным процессом посредством SMK и через локальный интерфейс. Диагностические средства, определенные производителем, должны верифицировать этот локальный интерфейс. Внутренние сбои могут обрабатываться с помощью определенных производителем средств.

8.4 Услуги SMK

8.4.1 Общие положения

Услуги SMK являются частью черного канала и поэтому не проверены. Верификации выполняются внутри между SMK и прикладным процессом через локальный интерфейс. Внутренние сбои могут обрабатываться с помощью определенных производителем средств.

Блок ресурсов содержит параметр макроцикла, так как на данные в черном канале нельзя полагаться.

8.4.2 Назначение адреса

Адрес является частью черного канала. Сбои, подменяющие дублирование адреса, управляются посредством ключа соединения. Предполагается, что устройства автоматически сбрасывают свою конфигурацию при изменении адреса черного канала.

8.4.3 Синхронизация времени

Синхронизация времени является функцией черного канала. Функция контроля синхронизации времени черного канала на коммуникационном уровне безопасности диагностирует целостность механизма синхронизации времени H1. Расширения протокола FSCP 1/1, таймер устаревания данных и предельное значение непрерывного счетчика устаревания будут косвенно управлять сбоями, вызванными любыми проблемами синхронизации.

8.5 Конфигурация и запуск коммуникационного уровня безопасности

8.5.1 Конфигурация и запуск H1

MIB является частью черного канала. В ее конфигурацию не вносятся никакие изменения. FBAP отличается (см. 8.5.2). Коммуникационный уровень безопасности конфигурируется из данных в объектах канала и блоке ресурсов, передаваемых внутренними средствами, определенными поставщиком.

8.5.2 FBAP FSCP 1/1

Объекты и параметры функционального блока могут быть сконфигурированы в соответствии со спецификацией AP (прикладного процесса) функционального блока.

8.5.3 Тестирование

После изменения конфигурации устройства необходимо испытать и верифицировать корректную функцию.

9 Системные требования

9.1 Индикаторы и коммутаторы

Устройству не требуются никакие индикаторы или коммутаторы.

9.2 Указания по установке

Должны применяться указания по установке МЭК 61918.

Примечание — Определенные поправки к указаниям по установке для МЭК 61918 будут также определены в МЭК 61784-5-1 [13] для CPF 1.

9.3 Время реакции функции безопасности

9.3.1 Обзор

Время реакции функции безопасности — это максимальное время между срабатыванием датчика безопасности (например, коммутатора, датчика избыточного давления, температурного датчика), подключенного к полевой шине, и достижением соответствующего безопасного состояния с помощью исполнительных устройств(а) (например, реле, клапана, привода) этой системы безопасности при наличии ошибок или отказов в канале функции безопасности.

Запрос (на выполнение) функции безопасности вызван либо аналоговым сигналом, пересекающим пороговое значение, или цифровым сигналом, изменяющим состояние.

На рисунке 31 показан пример типичных компонентов, из которых состоит время реакции функции безопасности.

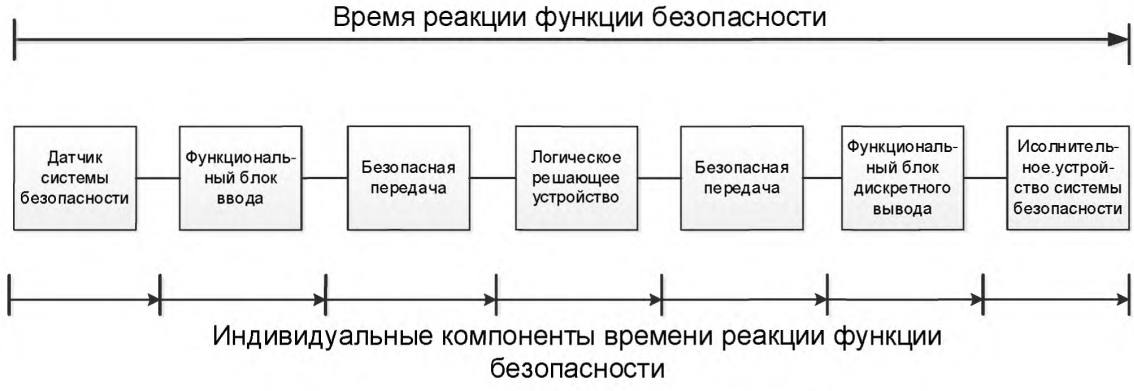


Рисунок 31 — Пример компонентов времени ответа функции безопасности

Время реакции функции безопасности — это сумма всех времен, показанных на рисунке 31.

9.3.2 Датчик системы безопасности

Время реакции датчика системы безопасности будет указано поставщиком датчика.

9.3.3 Функциональный блок ввода

Время реакции функционального блока ввода будет определено в руководстве по безопасности, поставляемом с устройством, включающим функциональный блок ввода.

9.3.4 Безопасная передача

Время безопасной передачи = 2 × (время макроцикла) + ((значение счетчика устаревания) × (время макроцикла)).

9.3.5 Логическое решающее устройство

Время реакции логического решающего устройства будет определено в руководстве по безопасности для логического решающего устройства.

9.3.6 Функциональный блок дискретного вывода

Время реакции функционального блока дискретного вывода будет определено в руководстве по безопасности, поставляемом с устройством, включающим функциональный блок дискретного вывода.

9.3.7 Исполнительное устройство безопасности

Время реакции исполнительного устройства безопасности будет предоставлено вместе с руководством по безопасности для исполнительного устройства безопасности.

9.4 Длительность запросов

Длительность запроса должна быть не менее двух макроциклов, чтобы гарантировать, что система коммуникаций, связанная с функциональной безопасностью, обнаружит этот запрос.

9.5 Ограничения для вычислений характеристик системы

9.5.1 Характеристики системы

На рисунке 32 показана топология сети FSCP 1/1, определенная для FSCP 1/1. В этой топологии все устройства ввода и вывода, соединены с логическим решающим устройством. Устройство ввода

публикует свои данные для подписчика логического решающего устройства. Устройство вывода подпишется на данные, опубликованные логическим решающим устройством.

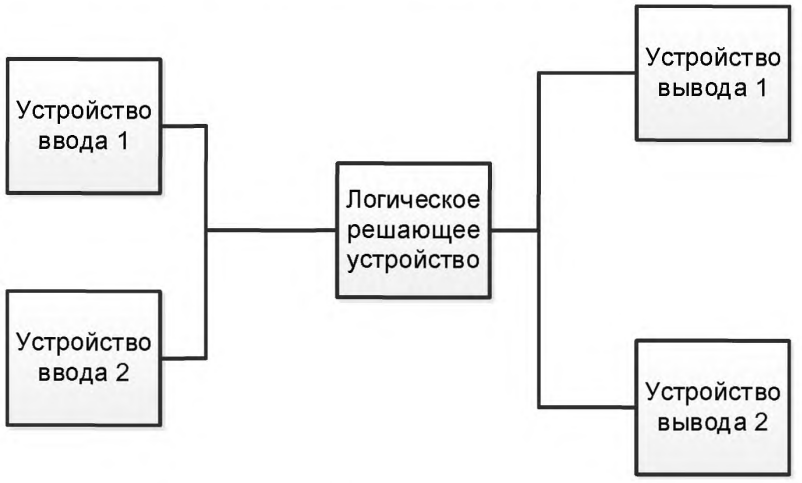


Рисунок 32 — Пример топологии сети FSCP 1/1

9.5.2 Частота отправки сообщений

FSCP 1/1 имеет физическое ограничение на значение максимальной частоты публикации данных, равное 100 сообщениям в секунду. Максимальная частота отправки сообщений, используемая при вычислениях уровня полноты безопасности FSCP 1/1, была равна 10 000 сообщениям в секунду. Так как используемая частота отправки значительно превышает возможную частоту в сегменте H1, не существует никаких ограничений на частоту отправки сообщений в сегменте H1.

9.5.3 Уровень УПБ

Технология протокола FSCP 1/1 спроектирована для реализации функций безопасности с УПБ 3, и разрешено использование не более 1 % значения PFD для всей системы безопасности (1 % от 10^{-7} в режиме с высокой частотой запросов или в режиме с непрерывным запросом). FSCP 1/1 возможно использовать в изделиях, спроектированных для функций безопасности вплоть до УПБ 3, подходящих для логических решающих устройств.

9.5.4 Совмещение устройств FSCP 1/1 и устройств CP 1/1

Протокол FSCP 1/1 был спроектирован с расчетом на возможность совмещения CP 1/1 и FSCP 1/1 в одном сегменте H1. Устройства CP 1/1 не могут повлиять на безопасность протокола FSCP 1/1, но устройства CP 1/1 могут повлиять на готовность сегмента H1. Совмещать устройства CP 1/1 и FSCP 1/1 в одном сегменте H1 не рекомендуется.

9.5.5 Устройства в сегменте

Не существует ограничений сверх тех, которые уже были установлены в CP 1/1 на число устройств в сегменте H1, наложенных протоколом FSCP 1/1.

9.5.6 Вычисления частоты остаточных ошибок

Результаты вычисления частоты остаточных ошибок, выполненные в соответствии с уравнением (1) МЭК 61784-3:2010 и значениями, используемыми для этого вычисления, показаны в таблице 15.

Таблица 15 — Значения, используемые для вычисления частоты возникновения остаточной ошибки

Члены уравнения	Значение FSCP 1/1	Члены уравнения	Значение FSCP 1/1
$\Lambda_{SL}(Pe)$	$1{,}04 \times 10^{-14}$	v	6 000
Pe	10^{-2}	m	32
$R_{SL}(Pe)$	$5{,}42 \times 10^{-20}$	n	от 32 до 1024

$R_{SL}(Pe)$ вычислен с помощью уравнения (D.1) МЭК 61784-3:2010. Результаты показаны в таблице 16.

Таблица 16 — Значения $R_{SL}(Pe)$ для различных значений n

n	$R_{SL}(Pe)$	n	$R_{SL}(Pe)$
32	$5{,}42 \times 10^{-20}$	288	$4{,}68 \times 10^{-97}$
64	$1{,}26 \times 10^{-29}$	320	$1{,}09 \times 10^{-106}$
96	$2{,}94 \times 10^{-39}$	352	$2{,}54 \times 10^{-116}$
128	$6{,}84 \times 10^{-49}$	384	$6{,}99 \times 10^{-127}$
160	$1{,}59 \times 10^{-58}$	416	$3{,}03 \times 10^{-138}$
192	$3{,}70 \times 10^{-68}$	448	$2{,}59 \times 10^{-150}$
224	$8{,}63 \times 10^{-78}$	480	$5{,}51 \times 10^{-163}$
256	$2{,}01 \times 10^{-87}$	512	$3{,}56 \times 10^{-176}$

9.6 Обслуживание

Для FSCP 1/1 не существует никаких определенных требований по обслуживанию.

9.7 Руководство по безопасности

Производитель устройства безопасности должен предоставлять руководство по безопасности, подходящее для устройства. Руководство по безопасности должно включать методы, необходимые для вычисления времени реакции системы, связанной с безопасностью, включающей устройство безопасности.

10 Оценка

FSCP 1/1 сам по себе не образует систему, связанную с безопасностью, или устройство безопасности. Кроме регистрации интероперабельности протокола FSCP 1/1, устройство, системы, программное обеспечение и т. д. будут также оценены с точки зрения применимого УПБ. Пользователь должен удостовериться в том, что каждое устройство безопасности подходит для реализации функции безопасности в соответствии с МЭК 61508. В дополнение к аспектам полевой шины пользователь должен также учесть аспекты безопасности МЭК 61508. На производителе лежит ответственность за разработку устройства и использование при этом только таких процессов разработки, которые соответствуют стандартам безопасности (см. МЭК 61508, МЭК 61511), а также им должна быть получена оценка, выполненная надлежащим органом.

Приложение А
(справочное)

Дополнительная информация для профилей коммуникаций, удовлетворяющих требованиям функциональной безопасности, CPF 1

А.1 Вычисление хэш функции

```
//
// Использование:
// crc32eth [infile]
// вычисляет Ethernet-CRC32 на основе содержания файла [infile]
//
// Компилировать:
// (этот источник должен компилироваться на любом компиляторе C++)
// g++ -Wall -o crc32eth crc32eth.cc #GNU-C++ под Linux
// g++ -Wall -mno-cygwin -o crc32eth.exe crc32eth.cc #with cygwin GNU-C++
//
// ---------------------------------------------------------------------------
// вычисление CRC математически является оцениванием остатка полиноминального
// деления, где порождающий многочлен (полином) является делителем.
// Для Ethernet-CRC32 порождающий многочлен — это 0xedb88320, биты соответствуют
// (f.l.t.r.) коэффициентам fuer x^0, x^1 .. x^31, коэффициент для x^32 не является явно
// 1.
// Этот «неестественный» порядок битов (наименее значащий бит слева) также
// применяется к любому единичному октету блока ввода данных и к результату
// полиноминального деления.
// ---------------------------------------------------------------------------
#include <iostream>
#include <iomanip>
#include <fstream>
// ---------------------------------------------------------------------------
const unsigned long maCRC32Ether[256] = {
  // Таблица для порождающего многочлена 0xedb88320
  0x00000000, 0x77073096, 0xee0e612c, 0x990951ba,
  0x076dc419, 0x706af48f, 0xe963a535, 0x9e6495a3,
  0x0edb8832, 0x79dcb8a4, 0xe0d5e91e, 0x97d2d988,
  0x09b64c2b, 0x7eb17cbd, 0xe7b82d07, 0x90bf1d91,
  0x1db71064, 0x6ab020f2, 0xf3b97148, 0x84be41de,
  0x1adad47d, 0x6ddde4eb, 0xf4d4b551, 0x83d385c7,
  0x136c9856, 0x646ba8c0, 0xfd62f97a, 0x8a65c9ec,
  0x14015c4f, 0x63066cd9, 0xfa0f3d63, 0x8d080df5,
  0x3b6e20c8, 0x4c69105e, 0xd56041e4, 0xa2677172,
  0x3c03e4d1, 0x4b04d447, 0xd20d85fd, 0xa50ab56b,
  0x35b5a8fa, 0x42b2986c, 0xdbbbc9d6, 0xacbcf940,
  0x32d86ce3, 0x45df5c75, 0xdcd60dcf, 0xabd13d59,
  0x26d930ac, 0x51de003a, 0xc8d75180, 0xbfd06116,
  0x21b4f4b5, 0x56b3c423, 0xcfba9599, 0xb8bda50f,
  0x2802b89e, 0x5f058808, 0xc60cd9b2, 0xb10be924,
  0x2f6f7c87, 0x58684c11, 0xc1611dab, 0xb6662d3d,
  0x76dc4190, 0x01db7106, 0x98d220bc, 0xefd5102a,
  0x71b18589, 0x06b6b51f, 0x9fbfe4a5, 0xe8b8d433,
  0x7807c9a2, 0x0f00f934, 0x9609a88e, 0xe10e9818,
  0x7f6a0dbb, 0x086d3d2d, 0x91646c97, 0xe6635c01,
  0x6b6b51f4, 0x1c6c6162, 0x856530d8, 0xf262004e,
  0x6c0695ed, 0x1b01a57b, 0x8208f4c1, 0xf50fc457,
  0x65b0d9c6, 0x12b7e950, 0x8bbeb8ea, 0xfcb9887c,
  0x62dd1ddf, 0x15da2d49, 0x8cd37cf3, 0xfbd44c65,
```

```
  0x4db26158, 0x3ab551ce, 0xa3bc0074, 0xd4bb30e2,
  0x4adfa541, 0x3dd895d7, 0xa4d1c46d, 0xd3d6f4fb,
  0x4369e96a, 0x346ed9fc, 0xad678846, 0xda60b8d0,
  0x44042d73, 0x33031de5, 0xaa0a4c5f, 0xdd0d7cc9,
  0x5005713c, 0x270241aa, 0xbe0b1010, 0xc90c2086,
  0x5768b525, 0x206f85b3, 0xb966d409, 0xce61e49f,
  0x5edef90e, 0x29d9c998, 0xb0d09822, 0xc7d7a8b4,
  0x59b33d17, 0x2eb40d81, 0xb7bd5c3b, 0xc0ba6cad,
  0xedb88320, 0x9abfb3b6, 0x03b6e20c, 0x74b1d29a,
  0xead54739, 0x9dd277af, 0x04db2615, 0x73dc1683,
  0xe3630b12, 0x94643b84, 0x0d6d6a3e, 0x7a6a5aa8,
  0xe40ecf0b, 0x9309ff9d, 0x0a00ae27, 0x7d079eb1,
  0xf00f9344, 0x8708a3d2, 0x1e01f268, 0x6906c2fe,
  0xf762575d, 0x806567cb, 0x196c3671, 0x6e6b06e7,
  0xfed41b76, 0x89d32be0, 0x10da7a5a, 0x67dd4acc,
  0xf9b9df6f, 0x8ebeeff9, 0x17b7be43, 0x60b08ed5,
  0xd6d6a3e8, 0xa1d1937e, 0x38d8c2c4, 0x4fdff252,
  0xd1bb67f1, 0xa6bc5767, 0x3fb506dd, 0x48b2364b,
  0xd80d2bda, 0xaf0a1b4c, 0x36034af6, 0x41047a60,
  0xdf60efc3, 0xa867df55, 0x316e8eef, 0x4669be79,
  0xcb61b38c, 0xbc66831a, 0x256fd2a0, 0x5268e236,
  0xcc0c7795, 0xbb0b4703, 0x220216b9, 0x5505262f,
  0xc5ba3bbe, 0xb2bd0b28, 0x2bb45a92, 0x5cb36a04,
  0xc2d7ffa7, 0xb5d0cf31, 0x2cd99e8b, 0x5bdeae1d,
  0x9b64c2b0, 0xec63f226, 0x756aa39c, 0x026d930a,
  0x9c0906a9, 0xeb0e363f, 0x72076785, 0x05005713,
  0x95bf4a82, 0xe2b87a14, 0x7bb12bae, 0x0cb61b38,
  0x92d28e9b, 0xe5d5be0d, 0x7cdcefb7, 0x0bdbdf21,
  0x86d3d2d4, 0xf1d4e242, 0x68ddb3f8, 0x1fda836e,
  0x81be16cd, 0xf6b9265b, 0x6fb077e1, 0x18b74777,
  0x88085ae6, 0xff0f6a70, 0x66063bca, 0x11010b5c,
  0x8f659eff, 0xf862ae69, 0x616bffd3, 0x166ccf45,
  0xa00ae278, 0xd70dd2ee, 0x4e048354, 0x3903b3c2,
  0xa7672661, 0xd06016f7, 0x4969474d, 0x3e6e77db,
  0xaed16a4a, 0xd9d65adc, 0x40df0b66, 0x37d83bf0,
  0xa9bcae53, 0xdebb9ec5, 0x47b2cf7f, 0x30b5ffe9,
  0xbdbdf21c, 0xcabac28a, 0x53b39330, 0x24b4a3a6,
  0xbad03605, 0xcdd70693, 0x54de5729, 0x23d967bf,
  0xb3667a2e, 0xc4614ab8, 0x5d681b02, 0x2a6f2b94,
  0xb40bbe37, 0xc30c8ea1, 0x5a05df1b, 0x2d02ef8d
};
// GetCRC32Ether() вычисляет CRC для блока данных, расположенного по адресу
// [pStart] размером в [len] октет. GetCRC32Ether() работает с приращением, где
// результат последней части выполняет роль [предварительно установленного]
// значения для последующей части. Для первой части должно использоваться
// предварительно установленное значение, равное 0xffffffff (=CRC32ETHER_PRESET).
// GetCRC32Ether() реализует высокоэффективный табличный метод для вычисления
// CRC.
enum {CRC32ETHER_PRESET= 0xffffffff};
unsigned long GetCRC32Ether(const void* pStart,
                            size_t len,
                            unsigned long preset) {
    size_t bytecount;
    unsigned char * buf= (unsigned char *) pStart;
    unsigned long crcword= preset;
    for (bytecount= len; (bytecount > 0); bytecount--, buf++) {
    — 62 — 61784-3-1 ♥ IEC:2010(E)
    crcword= maCRC32Ether[(crcword ^ *buf) & 0x0ff] ^ ( crcword >> 8L );
  }
  return crcword;
};
```

```
// ----------------------------------------------------------------------
enum {BUFSIZE= 1024}; //Groesse des Read-Buffers

  int main(int argc, char * argv[]) {
    if (argc != 2) {
    std::cerr << "Usage:" << std::endl;
    std::cerr << " " << argv[0] << " infile" << std::endl;
    return 2;
}
  std::ifstream infile;
  infile.open(argv[1], std::ios_base::in | std::ios_base::binary);
  if (!infile) {
    std::cerr << "ERR: unable to open file " << argv[1] << std::endl;
    exit(1);
}
  char buf[BUFSIZE]; //буфер-считывания
  size_t totalCount= 0; //Laenge в байтах
  unsigned long sig= CRC32ETHER_PRESET; //Предварительное значение signatur
  while (infile) {
    infile.read(&buf[0], BUFSIZE);
    size_t portionCount= infile.gcount();
    totalCount+= portionCount;
    sig= GetCRC32Ether(&buf[0], portionCount, sig);
}
  if (!infile.eof()) {
    std::cerr << "ERR: ошибка чтения файла" << argv[1] << std::endl;
    exit(1);
}
  infile.close();
  std::cout << argv[0] << ": байты, считанные из файла " << argv[1] << ": " << totalCount << std::endl;
  std::cout << argv[0] << ": CRC: 0x" << std::hex << std::setw(8) << std::setfill('0') << sig << std::endl;
return 0;
        }
```

А.2 Условия сбоев, возникающие за пределами функционального блока вывода

Когда средства диагностирования на устройстве вывода обнаруживают полевой сбой, возникающий за пределами функционального блока вывода или за пределами самого устройства, например в подсоединенном исполнительном устройстве, то предпринимаемое действие определено не в функциональном блоке вывода, а скорее в блоке преобразователя или в аппаратных средствах. При сбое устройства вывод переходит в обесточенное состояние так, как если бы было отключено питание у самого устройства. Некоторые устройства вывода могут использовать резервное питание для исполнительного устройства, и если эта возможность утрачена, то физическое устройство вывода переходит в обесточенное состояние. Так как эти сбои происходят вне функционального блока вывода, то конфигурация состояния сбоя не применима. В таблице А.1 представлено такое поведение.

Отказ устройства всегда завершается зафиксированным выводом, который пользователю потребуется перезапустить.

Таблица А.1 — Условия сбоя, возникающие за пределами функционального блока вывода

Условие	Пример	Комментарий
Полевой сбой	Отказ при испытании клапана при неполном ходе (сбой клапана или исполнительного устройства), разрыв обмотки или короткое замыкание в соленоиде	Диагностические средства и действия, определенные блоком преобразователя и аппаратными средствами. Обратная связь через функциональный блок вывода
Отказ резервного питания	Потеря поступления воздуха, питания на шине или гидравлического давления	Действие, определенное аппаратными средствами. Обратная связь через функциональный блок вывода
Отказ устройства питания	Питание шины или независимый источник питания утрачены	Действие, определенное аппаратными средствами

Окончание таблицы А.1

Условие	Пример	Комментарий
Отказ устройства	Контроль сторожевым устройством сбоев памяти или работы центрального процессора	Действие, определенное аппаратными средствами
Таймер устаревания данных	Сбой выполнения блока вывода или планирования	Диагностические средства и действия, определенные блоком преобразователя и аппаратными средствами. Обратная связь через функциональный блок вывода

Приложение В
(справочное)

Информация для оценки профилей коммуникаций, удовлетворяющих требованиям функциональной безопасности, CPF 1

Информация о тестовых лабораториях, которые испытывают и подтверждают соответствие реализующих FSCP 1/1 изделий стандарту МЭК 61784-3-1, может быть получена в национальных комитетах МЭК или в следующих организациях:

Fieldbus Foundation
9005 Mountain Ridge Drive
Bowie Bldg - Suite 200
Austin, TX 78759-5316
USA

Телефон: +1 512 794 8890
Факс: +1 512 794 8893
E-mail: info@fieldbus.org
URL:http://www.fieldbus.org

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61131-2	IDT	ГОСТ IEC 61131-2—2012 «Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания»
IEC 61158-2	IDT	
IEC 61158-3-1	—	*
IEC 61158-4-1	—	*
IEC 61158-5-5	—	*
IEC 61158-5-9	—	*
IEC 61158-6-5	—	*
IEC 61158-6-9	—	*
IEC 61508 (все части)	IDT	ГОСТ Р МЭК 61508—2012 (все части) «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
IEC 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
IEC 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
IEC 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
IEC 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
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 61918	—	*
IEC 62280-1	—	*
ISO/IEC 8802-3	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

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

- IDT — идентичные стандарты.

Библиография

[1] IEC 60050 (all parts), International Electrotechnical Vocabulary NOTE See also the IEC Multilingual Dictionary — Electricity, Electronics and Telecommunications (available on CD-ROM and at <http://www.electropedia.org>)

[2] IEC 60204-1, Safety of machinery — Electrical equipment of machines — Part 1: General requirements

[3] 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

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

[5] IEC 61158 (all parts), Industrial communication networks — Fieldbus specifications

[6] 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

[7] 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

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

[9] 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

[10] IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

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

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

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

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

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

[16] IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

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

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

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

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

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

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

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

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

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

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

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

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

[29] ITU-T(CCITT) V.42, Error-correcting procedures for DCEs using asynchronous-tosynchronous conversion, available at < http://www.itu.int/rec/T-REC-V.42/e>

[30] 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

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

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

[33] GS-ET-2616, 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")

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

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

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

[37] 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.

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

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

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

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

[42] 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

[43] 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

[44] 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

[45] Foundation™ Fieldbus AG-180, User Application Guide for FF-SIS

[46] Foundation™ Fieldbus FF-807, FS-SIS Application Model — Phase 1

[47] Foundation™ Fieldbus FF-884, FF-SIS Protocol Specification

[48] Foundation™ Fieldbus FF-895, FF-SIS Function Block Application Process — Phase 1

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 1

Редактор *А.А. Кабанова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 19.12.2016. Подписано в печать 23.01.2017. Формат 60 ×84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 6,31. Тираж 27 экз. Зак. 141.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru