ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61784-3— 2015

Промышленные сети

ПРОФИЛИ

Часть 3

Функциональная безопасность полевых шин. Общие правила и определения профилей

(IEC 61784-3:2010, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного перевода на русский язык англоязычной версии 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 28 декабря 2015 г. № 2220-ст

4 Настоящий стандарт идентичен международному стандарту IEC 61784-3:2010 «Промышленные сети. Профили. Часть 3. Функциональная безопасность полевых шин. Общие правила и определения профилей» (Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definition, IDT).

Международный стандарт разработан техническим комитетом IEC 65C.

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0–2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в годовом (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

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

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины, определения и сокращения ... 3
3.1 Термины и определения ... 3
3.2 Сокращения ... 7
4 Соответствие ... 8
5 Основные представления о связанных с безопасностью системах полевых шин ... 9
5.1 Декомпозиция функции безопасности ... 9
5.2 Коммуникационная система ... 9
5.3 Ошибки коммуникаций ... 11
5.4 Меры по устранению детерминированных неисправностей ... 12
5.5 Взаимоотношения между ошибками и мерами безопасности ... 14
5.6 Полнота данных ... 14
5.7 Связь между функциональной безопасностью и защищенностью ... 16
5.8 Предельные условия и ограничения ... 16
5.9 Руководство по установке ... 17
5.10 Руководство по безопасности ... 17
5.11 Политика безопасности ... 17
6 Семейство 1 коммуникационных профилей (Полевая шина FOUNDATION™). Профили для функциональной безопасности ... 18
6.1 Коммуникационный профиль 1/1, удовлетворяющий требованиям функциональной безопасности ... 18
6.2 Технический обзор ... 18
7 Семейство 2 коммуникационных профилей (CIP™). Профили для функциональной безопасности ... 19
7.1 Коммуникационный профиль 2/1, удовлетворяющий требованиям функциональной безопасности ... 19
7.2 Технический обзор ... 19
8 Семейство 3 коммуникационных профилей (PROFIBUS™, PROFINET™). Профили для функциональной безопасности ... 20
8.1 Коммуникационный профиль 3/1, удовлетворяющий требованиям функциональной безопасности ... 20
8.2 Технический обзор ... 21
9 Семейство 6 коммуникационных профилей (INTERBUS®). Профили для функциональной безопасности ... 23
9.1 Коммуникационный профиль 6/7, удовлетворяющий требованиям функциональной безопасности ... 23
9.2 Технический обзор ... 23
10 Семейство 8 коммуникационных профилей (CC-Link™). Профили для функциональной безопасности ... 25
10.1 Коммуникационный профиль 8/1, удовлетворяющий требованиям функциональной безопасности ... 25
10.2 Технический обзор ... 25
11 Семейство 12 коммуникационных профилей (EtherCAT™). Профили для функциональной безопасности ... 25
11.1 Коммуникационный профиль 12/1, удовлетворяющий требованиям функциональной безопасности ... 25
11.2 Технический обзор ... 26
12 Семейство 13 коммуникационных профилей (Ethernet POWERLINKTM). Профили для функциональной безопасности ... 27
12.1 Коммуникационный профиль 13/1, удовлетворяющий требованиям функциональной безопасности ... 27
12.2 Технический обзор ... 27
13 Семейство 14 коммуникационных профилей (EPA®). Профили для функциональной безопасности ... 28

13.1 Коммуникационный профиль 14/1, удовлетворяющий требованиям функциональной безопасности 28
13.2 Технический обзор 28
Приложение А (справочное) Примеры моделей коммуникаций, удовлетворяющих функциональной безопасности 30
Приложение В (справочное) Модель коммуникационного канала безопасности с проверкой ошибок, основанной на CRC 33
Приложение С (справочное) Структура стандартов, связанных с конкретными технологиями 37
Приложение D (справочное) Руководство по оценке 40
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 44
Библиография 45

Введение

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 приложениями автоматизации. В настоящее время технология полевых шин используется достаточно широко и хорошо себя зарекомендовала. Именно поэтому ее пока еще не стандартизированные применения появляются во многих областях, таких как системы реального времени, системы, связанные с безопасностью и защитой.

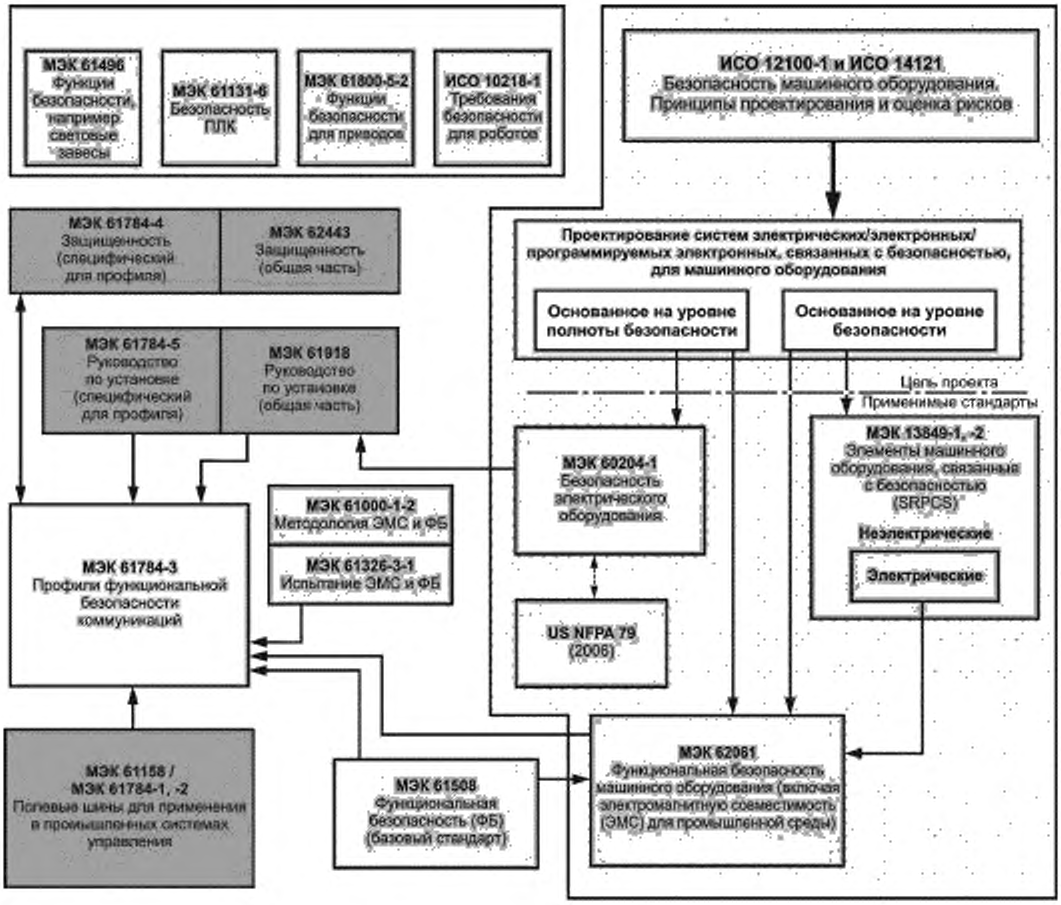
Настоящий стандарт рассматривает важные принципы функциональной безопасности коммуникаций, на основе подхода, представленного в комплексе стандартов МЭК 61508, и определяет несколько коммуникационных уровней безопасности (профилей и соответствующих протоколов) на основе профилей передачи данных и уровней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

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

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

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

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



Обозначения:

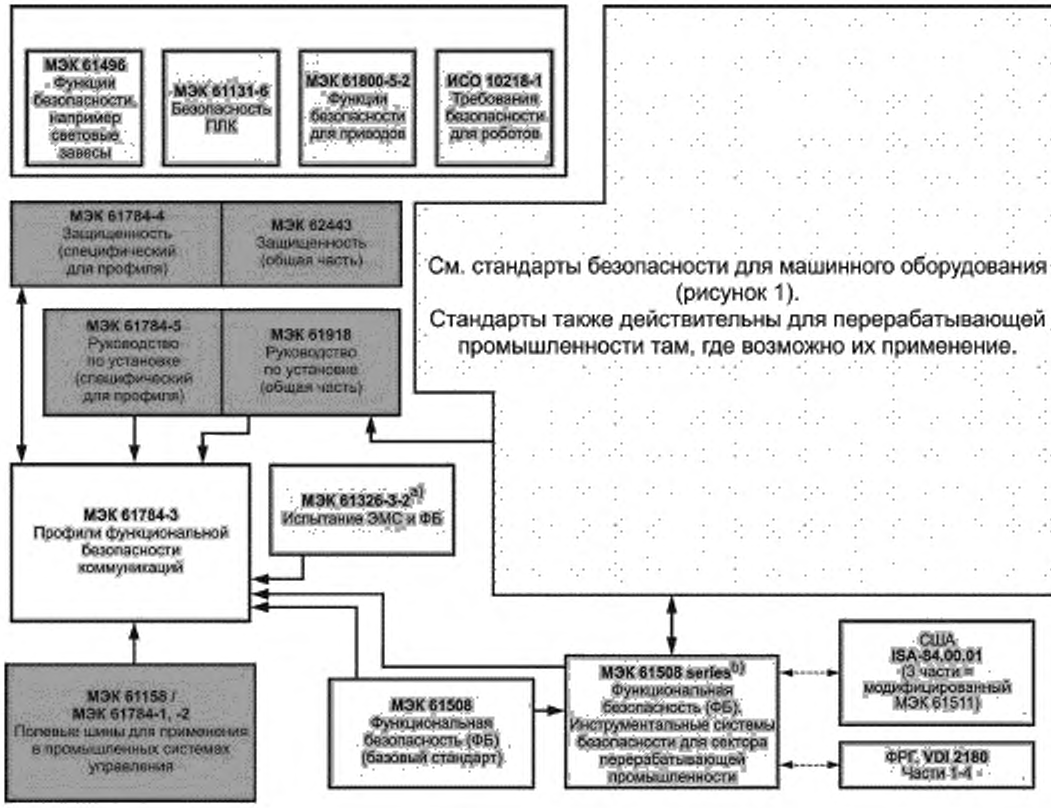
(Желтый) Стандарты, связаные с безопасностью.

(Голубой) Стандарты, связанные с полевыми шинами.

(Бледно-желтый) Настоящий стандарт.

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 безопасности (Категорией) и УПБ.

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



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 ЕН.

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

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

Настоящий стандарт описывает:

- основные принципы реализации требований комплекса стандартов МЭК 61508 для связанной с безопасностью передачи данных, включая возможные сбои при передаче данных, меры по устранению неисправностей и факторы, влияющие на полноту данных;

- индивидуальные описания профилей, удовлетворяющих требованиям функциональной безопасности, для нескольких семейств профилей передачи данных, представленных в МЭК 61784-1 и МЭК 61784-2;

- расширения уровня безопасности до служб передачи данных и разделов протоколов в стандартах комплекса МЭК 61158.

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, описанным в МЭК 61784-3-1, МЭК 61784-3-2, МЭК 61784-3-3, МЭК 61784-3-4, МЭК 61784-3-6, МЭК 61784-3-12, МЭК 61784-3-13, МЭК 61784-3-14.

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 не дискриминационных условиях и положениях с заявителями по всему миру. Такие заявления обладателей прав на данные патенты зарегистрированы в МЭК.

Примечание — Детали патента и соответствующая контактная информация может быть найдена в МЭК 61784-3-1, МЭК 61784-3-2, МЭК 61784-3-3, МЭК 61784-3-4, МЭК 61784-3-6, МЭК 61784-3-12, МЭК 61784-3-13 и МЭК 61784-3-14.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Промышленные сети

ПРОФИЛИ

Часть 3

Функциональная безопасность полевых шин. Общие правила и определения профилей

Industrial communications networks. Profiles. Part 3. Functional safety fieldbuses. General rules and profile definitions

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт рассматривает некоторые общие принципы, которые используются при передаче связанных с безопасностью сообщений между участниками распределенной сети, применяя технологию полевых шин в соответствии с требованиями комплекса[1)] МЭК 61784, для обеспечения функциональной безопасности. Эти принципы могут быть использованы в различных промышленных применениях таких, как управление процессами, автоматизация производства и машинное оборудование.

Настоящий стандарт устанавливает несколько профилей коммуникаций, удовлетворяющих требованиям функциональной безопасности, на основе уровней профилей коммуникаций и уровней протокола технологий полевых шин, представленных в МЭК 61784-1, МЭК 61784-2 и комплексе МЭК 61158.

Примечания

1 Могут существовать другие системы коммуникаций, связанные с безопасностью, соответствующие требованиям МЭК 61508, которые не были включены в настоящий стандарт.

2 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.

На той или иной стадии жизненного цикла все системы подвергаются несанкционированному доступу. Необходимо предусматривать дополнительные меры для защиты любого связанного с безопасностью применения, чтобы защитить системы полевых шин от несанкционированного доступа. Комплекс стандартов МЭК 62443 рассматривает много подобных проблем. Связь настоящего стандарта с МЭК 62443 подробно рассмотрена в посвященном ему подразделе настоящего стандарта.

Примечания

1 Дополнительные, характерные для профиля требования к защите информации могут быть также установлены в МЭК 61784-4 [10].

2 В соответствии с настоящим стандартом реализации в устройстве профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, не достаточно для того, чтобы устройство считалось безопасным, как определено в комплексе стандартов МЭК 61508.

3 Результирующий УПБ, заявляемый для системы, зависит от реализации выбранного профиля коммуникации, удовлетворяющего требованиям функциональной безопасности, внутри этой системы.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты и документы (для датированных ссылок следует использовать указанное издание, для недатированных ссылок — последнее издание указанного документа, включая все поправки к нему):

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

Издание официальное

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

IEC 61158 (all parts) Digital data communications for measurement and control — Fieldbus for use in industrial control systems (МЭК 61158 (все части) Передача цифровых данных для измерения и управления. Полевая шина для систем автоматического регулирования и управления технологическими процессами)

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 (МЭК 61326-3-1 Электрооборудование для измерения, управления и лабораторного использования. Требования ЭМС. Часть 3-1. Требования устойчивости для систем, связанных с безопасностью, и оборудования для выполнения функций, связанных с безопасностью (функциональная безопасность). Общепромышленное применение)

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 (МЭК 61326-3-2 Электрооборудование для измерения, управления и лабораторного использования. Требования ЭМС. Часть 3-2. Требования устойчивости для систем, связанных с безопасностью, и оборудования для выполнения функций, связанных с безопасностью (функциональная безопасность). Общепромышленное применение. Общие промышленные применения в заданной электромагнитной среде)

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems (МЭК 61508 (все части) 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 (МЭК 61508-1:2010 Функциональная безопасность систем электрических/ электронных/программируемых электронных, связанных с безопасностью. Часть 1. Общие требования)

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

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

IEC 61784-2, Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ИСО/МЭК 8802-3 (МЭК 61784-2 Промышленные сети. Профили. Часть 2. Дополнительные профили полевых шин для сетей реального времени, на основе ИСО/МЭК 8802-3)

IEC 61784-3-1, Industrial communication networks — Profiles — Part 3-1: Functional safety fieldbuses — Additional specifications for CPF 1 (МЭК 61784-3-1 Промышленные сети. Профили. Части 3-1. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 1)

IEC 61784-3-2, Industrial communication networks — Profiles — Part 3-2: Functional safety fieldbuses — Additional specifications for CPF 2 (МЭК 61784-3-2 Промышленные сети. Профили. Части 3-2. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 2)

IEC 61784-3-3, Industrial communication networks — Profiles — Part 3-3: Functional safety fieldbuses — Additional specifications for CPF 3 (МЭК 61784-3-3 Промышленные сети. Профили. Части 3-2. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 3)

IEC 61784-3-6, Industrial communication networks — Profiles — Part 3-6: Functional safety fieldbuses — Additional specifications for CPF 6 (МЭК 61784-3-6 Промышленные сети. Профили. Части 3-6. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 6)

IEC 61784-3-8, Industrial communication networks — Profiles — Part 3-8: Functional safety fieldbuses — Additional specifications for CPF 8 (МЭК 61784-3-8 Промышленные сети. Профили. Части 3-8. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 8)

IEC 61784-3-12, Industrial communication networks — Profiles — Part 3-12: Functional safety fieldbuses — Additional specifications for CPF 12 (МЭК 61784-3-12 Промышленные сети. Профили. Части 3-12. Функциональная безопасность полевых шин.Дополнительные спецификации для CPF 12)

IEC 61784-3-13, Industrial communication networks — Profiles — Part 3-13: Functional safety fieldbuses — Additional specifications for CPF 13 (МЭК 61784-3-13 Промышленные сети. Профили. Части 3-13. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 13)

IEC 61784-3-14, Industrial communication networks — Profiles — Part 3-14: Functional safety fieldbuses — Additional specifications for CPF 14 (МЭК 61784-3-14 Промышленные сети. Профили. Части 3-14. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 14)

IEC 61784-5 (all parts), Industrial communication networks — Profiles — Part 5: Installation of fieldbuses — Installation profiles for CPF X (МЭК 61784-5 (все части) Промышленные сети. Профили. Часть 5. Установка полевых шин. Профили установки для CPF X)

IEC 61918, Industrial communication networks — Installation of communication networks in industrial premises (МЭК 61918 Промышленные сети. 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 (МЭК 62280-1:2002 Железные дороги. Системы связи, сигнализации и обработки данных. Часть 2. Экстренная связь в открытых системах передачи. Часть 2. Обеспечение безопасности связи в закрытых системах передачи)

IEC 62443 (all parts), Industrial communication networks — Network and system security (МЭК 62443 (все части) Промышленные сети. Защищенность (кибербезопасность) сети и системы)

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 Общепринятые термины и определения

3.1.1.1

абсолютная метка времени (absolute time stamp): Метка времени, привязанная к глобальному времени, которая является общей для группы устройств, использующих полевые шины.

[МЭК 62280-2, модифицировано]

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

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

3.1.1.4 **мост** (bridge): Абстрактное устройство, соединяющее многочисленные сегменты сети для всего уровня канала передачи данных.

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

3.1.1.6 **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.

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

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

Примечания

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

2 См. также [29], [30].

3.1.1.9

разнообразие (diversity): Различные средства выполнения требуемой функции.

Примечание — Разнообразие может достигаться использованием различных физических методов или различных подходов к проектированию.

[МЭК 61508-4:2010]

3.1.1.10

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.

3.1.1.11

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.

3.1.1.12

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

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

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

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

3.1.1.14 **система полевых шин** (fieldbus system): Система, использующая полевую шину с подключенными устройствами.

3.1.1.15 **кадр** (frame): Упрощенный синоним для DLPDU (Блок Данных Протокола Канала Передачи Данных).

3.1.1.16 **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 [29] и [30].

3.1.1.17

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

Примечания

1 Хеш-функции могут применяться для обнаружения искажений данных.

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

[МЭК/ТО 62210, модифицировано]

3.1.1.18 **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.

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

3.1.1.20

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

[ИСО/МЭК 2382-16.02.01, модифицировано]

3.1.1.21

приемник сообщений (message sink): Часть коммуникационной системы, в которую, как предполагалось, поступают сообщения.

[ИСО/МЭК 2382-16.02.03]

3.1.1.22

источник сообщения (message source): Часть коммуникационной системы, в которой, как предполагалось, возникают сообщения.

[ИСО/МЭК 2382-16.02.02]

3.1.1.23 **ложное срабатывание** (nuisance trip): Ложное аварийное отключение, не причиняющее никакого вреда.

Примечание — В коммуникационных системах таких, как системы беспроводной передачи данных могут возникать внутренние аномальные ошибки, например, вследствие слишком большого количества повторных попыток при наличии помех.

3.1.1.24

уровень безопасности (performance level, PL): Дискретный уровень, применяющийся для определения способности связанных с безопасностью частей системы управления выполнять функцию безопасности в заранее предполагаемых условиях.

[ИСО 13849-1]

3.1.1.25

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

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

[МЭК 61131-2]

3.1.1.26

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

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

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

3.1.1.27

относительная временная метка (relative time stamp): Метка времени, привязанная к локальному времени объекта.

Примечание — В общем случае не существует связи с часами других объектов.

[МЭК 62280-2, модифицировано]

3.1.1.28

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

Примечания

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

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

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

4 Надежность отличается от готовности.

[МЭК 62059-11, модифицирован]

3.1.1.29

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

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

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

3.1.1.30 **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.

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

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

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

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

3.1.1.34

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

Примечание — Цепь SELV не подсоединена к защитному заземлению.

[МЭК 61131-2]

3.1.1.35 **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 УО по отношению к конкретному опасному событию.

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

3.1.1.36 **время реакции функции безопасности** (safety function response time): Наихудшее время выполнения, начинающееся после срабатывания датчика системы безопасности, подключенного к полевой шине, которое может пройти до того, как было достигнуто соответствующее безопасное состояние с помощью исполнительного устройства этой системы безопасности, при наличии ошибок или отказов в канале функции безопасности.

Примечание — Данная концепция введена в 5.2.4 и реализуется профилем коммуникации, удовлетворяющим требованиям функциональной безопасности, определенным в настоящем стандарте.

3.1.1.37

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

Примечания

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

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

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

[МЭК 61508-4:2010]

3.1.1.38 **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 5.3 и 5.4.

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

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

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

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

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

3.1.1.44 **белый канал** (white channel): Канал связи, в котором все соответствующие компоненты аппаратных средств и программного обеспечения спроектированы, реализованы и имеют подтверждение соответствия в соответствии с МЭК 61508.

3.1.2 CPF 1. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.3 CPF 2. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.4 CPF 3. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.5 CPF 6. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.6 CPF 8. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.7 CPF 12. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.8 CPF 13. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.1.9 CPF 14. Дополнительные термины и определения

Не требуются в настоящем стандарте.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения.

3.2.1 Общие сокращения терминов

Сокращение	Полное выражение	Источник
CP	Профиль коммуникаций	[МЭК 61784-1]
CPF	Семейство профилей коммуникации	[МЭК 61784-1]
CRC	Циклический контроль избыточности	
DLL	Уровень канала данных	[ИСО/МЭК 7498-1]
DLPDU	Блок данных протокола канала передачи данных	
ЭМС	Электромагнитная совместимость	
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 (Fieldbus Application Layer)	[МЭК 61158-5]
FCS	Последовательность проверки кадра	

Сокращение	Полное выражение	Источник
ФБ	Функциональная безопасность	
FSCP	Профиль коммуникации, удовлетворяющий требованиям функциональной безопасности	
MTBF	Среднее время между отказами	
MTTF	Среднее время до отказа	
NSR	Несвязанный с безопасностью (Non Safety Relevant)	
PDU	Блока данных протокола	[ИСО/МЭК 7498-1]
PELV	Защитное сверхнизкое напряжение	
PES	Программируемая электронная система	[МЭК 61508-4:2010]
PFD	Средняя вероятность опасных отказов по запросу	[МЭК 61508-6:2010]
PFH	Средняя частота опасных отказов (h^{-1}) в час	[МЭК 61508-6:2010]
PhL	Физический уровень	[ИСО/МЭК 7498-1]
PL	Уровень безопасности	[ИСО 13849-1]
PLC	Программируемый логический контроллер	
SCL	Коммуникационный уровень безопасности	
SELV	Безопасное сверхнизкое напряжение	
УПБ	Уровень полноты безопасности	[МЭК 61508-4:2010]
SR	Связанный с безопасностью	

3.2.2 CPF 1. Дополнительные сокращения терминов

SIS — Инструментальная система безопасности (safety instrumented systems).

3.2.3 CPF 2. Дополнительные сокращения терминов

CIP™ — Общий промышленный протокол [Common Industrial Protocol (application framework shared among CPF 2 communication profiles)].

3.2.4 CPF 3. Дополнительные сокращения терминов

DP — Децентрализованное периферийное устройство (Decentralized Peripherals).

3.2.5 CPF 6. Дополнительные сокращения терминов

Не требуются в настоящем стандарте.

3.2.6 CPF 8. Дополнительные сокращения терминов

ASE — Прикладной сервисный элемент (Application Service Element);

SASE — Безопасный прикладной сервисный элемент (Safety Application Service Element).

3.2.7 CPF 12. Дополнительные сокращения терминов

FSoE — Отказоустойчивый по CPF 12.

3.2.8 CPF 13. Дополнительные сокращения терминов

Не требуются в настоящем стандарте.

3.2.9 CPF 14. Дополнительные сокращения терминов

IP — Протокол сети Интернет (Internet Protocol);

UDP — Протокол пользовательских датаграм (User Datagram Protocol).

4 Соответствие

В настоящем стандарте каждый из профилей коммуникации, удовлетворяющий требованиям функциональной безопасности, основан на профилях коммуникаций стандартов МЭК 61784-1 и МЭК 61784-2, а также уровнях протоколов, представленных в МЭК 61158.

Соответствие профилю коммуникации, удовлетворяющему требованиям функциональной безопасности (FSCP), настоящего стандарта должно устанавливаться как соответствие МЭК 61784-3:20xx FSCP n/m <Тип> или как соответствие МЭК 61784-3 (Ed.2.0) FSCP n/m <Тип>, где Тип, заключенный в скобки, является необязательным и скобки не должны использоваться.

В противном случае соответствие может устанавливаться как ссоответствие МЭК 61784-3-N:20xx или как соответствие МЭК 61784-3-*N* (Ed.2.0), где *N* — это номер, назначенный соответствующему CPF.

Соответствие МЭК 61784-3-*N* означает, что все обязательные требования соответствующего(их) FSCP для конкретного устройства, системы или приложения должны быть выполнены.

Стандарты на изделие не должны включать в себя никаких других аспектов оценки соответствия (включая положения управления качеством), нормативных или информативных, кроме положений об испытании изделия (оценке и проверке).

5 Основные представления о связанных с безопасностью системах полевых шин

5.1 Декомпозиция функции безопасности

В соответствии с МЭК 61508 в результате анализа рисков определяются функции безопасности. Эти функции безопасности могут быть декомпозированы на части, которые вносят свой вклад в функции безопасности всей системы (например, Датчик (датчики) — Безопасный коммуникационный канал — Программируемая(ые) электронная(ые) система(ы) — Безопасный коммуникационный канал — Исполнительное(ые) устройство(а).

В настоящем стандарте рассматривается коммуникационная система, которая сама выполняет функцию безопасно передаваемых данных. При этом настоятельно рекомендуется, чтобы значения PFD или PFH безопасного коммуникационного канала составляли не более 1 % максимального значения PFD или PFH заданного значением УПБ, для которого был разработан данный коммуникационный профиль (см. рисунок 3).

Пример — На рисунке 3 значение PFH функции безопасности равно $PFH_{датчика}$ + $PFH_{ПЭС}$ + $PFH_{исполнительного\ устройства}$ + 2 x $PFH_{безопасного\ коммуникационного\ канала}$.

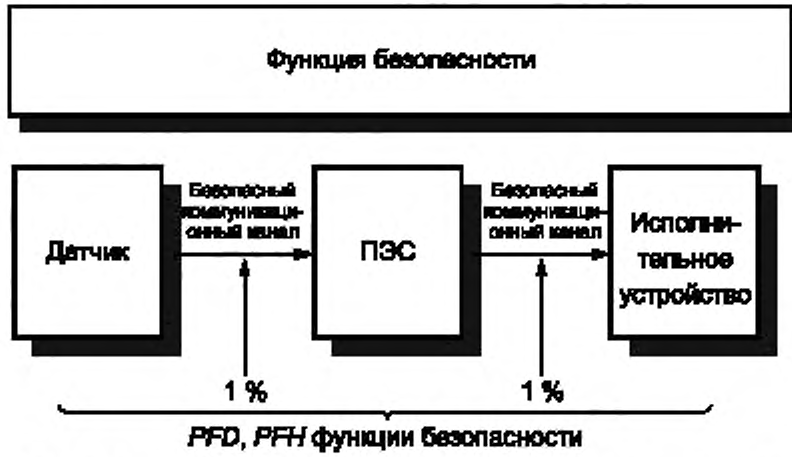


Рисунок 3 — Безопасная коммуникация является частью функции безопасности

5.2 Коммуникационная система

5.2.1 Общие положения

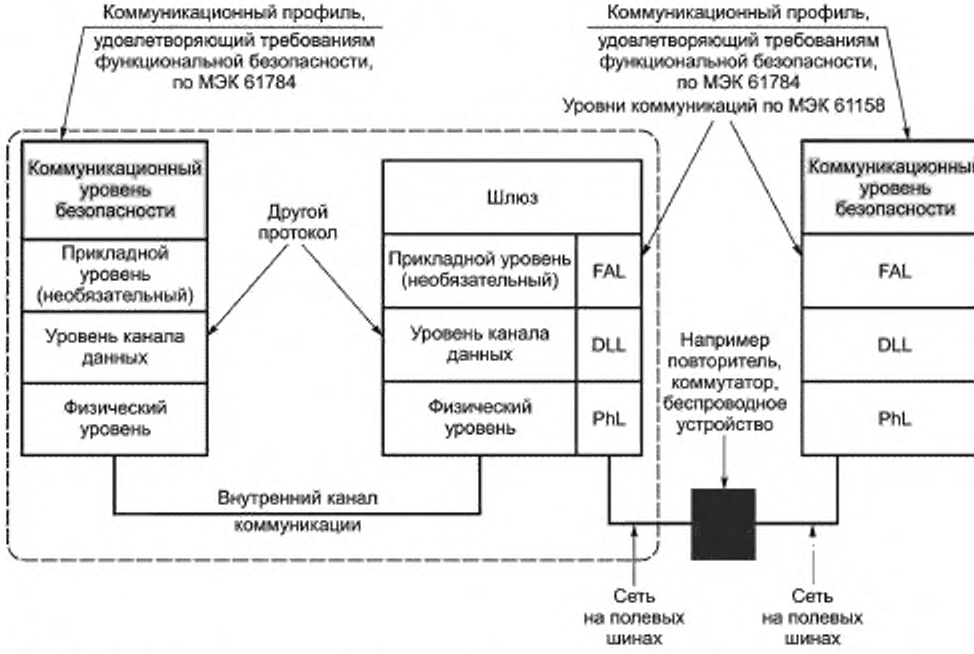
Ниже приведена информация для общего понимания технологии и понятий.

Примечание — Бóльшая часть информации заимствована из [28].

5.2.2 Полевые шины в МЭК 61158

Хотя в МЭК 61508 нет ограничений на использование коммуникационных технологий, основное внимание в настоящем стандарте уделено использованию функциональной безопасности коммуникационных систем на основе полевых шин. На рисунке 4 представлен пример модели применения функциональной безопасности для коммуникаций с полевыми шинами, используя подход на основе черного канала.

Руководствуясь МЭК 61158 при использовании структур полевых шин без изменений при задании каждого уровня коммуникации, все меры, необходимые для выполнения безопасно передаваемых данных в соответствии с требованиями МЭК 61508, должны быть выполнены на дополнительном «коммуникационном уровне безопасности», расположенном, как показано на рисунке 4.



Примечания

1 Для внутренних каналов связи устройства требуется реализация прикладного уровня полевой шины (FAL), в то время как прикладным уровнем (AL) можно пренебречь.

2 Функции пользовательского уровня, не связанные с безопасностью, могут пропускать коммуникационный уровень безопасности и прямо обращаться к FAL.

Рисунок 4 — Пример модели коммуникационной системы, удовлетворяющей требованиям функциональной безопасности

5.2.3 Типы коммуникационных каналов

МЭК 61508 использует концепцию так называемого «черного канала» или «белого канала», чтобы определить требования к базовой полевой шине для передачи безопасных данных. Какой будет канал, черный или белый, определяется тем, где реализованы меры безопасности относительно базовой полевой шины. Настоящий стандарт устанавливает коммуникационные профили, удовлетворяющие требованиям функциональной безопасности, для черного канала.

В таком контексте считается, что безопасный коммуникационный канал начинается на верхнем коммуникационном уровне безопасности источника и завершается на верхнем коммуникационном уровне безопасности приемника (см. рисунок 4).

5.2.4 Время реакции функции безопасности

Время реакции функции безопасности — это наихудшее затраченное время, начинающееся от срабатывания датчика системы безопасности (например, сетевого коммутатора, датчика избыточного давления, световой завесы), подключенного к полевой шине, до соответствующего безопасного состояния, достигаемого исполнительным(ыми) устройством(ами) системы безопасности (например, реле, клапан, двигатель) при наличии ошибок или отказов в канале функции безопасности.

Запрос на срабатывание функции безопасности вызывается или аналоговым сигналом, пересекающим пограничное значение, или цифровым сигналом, меняющим состояние.

На рисунке 5 показан пример типичных компонентов, формирующих время реакции функции безопасности.



Рисунок 5 — Пример компонентов, составляющих время реакции функции безопасности

Конкретные коммуникационные профили, удовлетворяющие требованиям функциональной безопасности, могу обладать отличающимся набором компонентов, но при оценке времени реакции функции безопасности должны учитываться все значимые компоненты.

5.3 Ошибки коммуникаций

5.3.1 Общие положения

Следующие разделы устанавливают возможные ошибки коммуникаций. Также приведены дополнительные примечания, описывающие типичное поведение черного канала.

5.3.2 Искажение

Сообщения могут быть искажены из-за ошибок одного из участников шины, ошибок среды передачи данных или влияния помех на сообщения.

Примечания

1 Ошибки сообщения во время пересылки являются нормальным событием для любой коммуникационной системы, такие события с высокой вероятностью обнаруживаются приемниками при помощи хеш-функции, и сообщение игнорируется.

2 Большинство систем коммуникаций включают в себя протоколы для восстановления ошибок в сообщениях, поэтому эти сообщения не должны классифицироваться как «потери» до тех пор, пока не были предприняты процедуры восстановления или повторной передачи.

3 Если процедуры восстановления или повторной передачи превышают установленные сроки выполнения, сообщение классифицируется как «недопустимая задержка».

4 В событии с очень низкой вероятностью, в котором множественные ошибки приводят к новому сообщению с правильной структурой (например, адресация, длина, хеш-функция, такая как CRC и т. д.), сообщение будет принято и передано на дальнейшую обработку. Оценки, основывающиеся на порядковом номере сообщения или временной метке, могут классифицировать сбои, такие как «непреднамеренный повтор», «ошибочная последовательность», «недопустимая задержка», «появление неизвестного сообщения».

5.3.3 Непреднамеренный повтор

В связи с ошибкой, сбоем или помехами старые необновленные сообщения повторяются в не соответствующий момент времени.

Примечание — Повторения отправителем является нормальной процедурой, когда от станции, для которой предназначалось сообщение, не получено ожидаемое подтверждение/ответ или когда принимающая станция обнаруживает пропажу сообщения и запрашивает его повторную отправку.

В некоторых случаях может быть обнаружено отсутствие ответа и сообщение передается повторно с минимальной задержкой и без нарушения последовательности, в других случаях повторение происходит позже и приходит вне последовательности с другими сообщениями.

Примечание — Некоторые полевые шины используют избыточность и отправляют одно и то же сообщение несколько раз или несколькими альтернативными маршрутами, чтобы повысить вероятность хорошего приема.

5.3.4 Ошибочная последовательность

В связи с ошибкой, сбоем или помехами предопределенная последовательность (например, натуральных чисел, временных ссылок), связанная с сообщениями из конкретного источника, оказывается ошибочной.

Примечания

1 Системы полевых шин могут содержать элементы, хранящие сообщения [например, элементы FIFO (первым пришел — первым вышел) в сетевых коммутаторах, мостах и маршрутизаторах], или могут использовать протоколы, способные изменить последовательность (например, позволяя сообщениям с более высоким приоритетом обгонять сообщения с более низким).

2 Если активны несколько их последовательностей, такие как сообщения из разных источников или отчетов, связанных с различными типами объектов, то такие последовательности контролируются по отдельности и оповещения об ошибках поступают от каждой из них.

5.3.5 Потеря

Из-за ошибки, сбоя или помехи сообщение не принимается и не подтверждается.

5.3.6 Недопустимая задержка

Задержка сообщений может превышать допустимое временное окно их доставки, например, из-за ошибок в среде передачи, перегруженных линий передачи, помех или из-за того, что участники шины посылают сообщения таким образом, что службы обрабатывают их с задержкой или отказываются обрабатывать (например, FIFO в сетевых коммутаторах, мостах и маршрутизаторах).

Примечание — В описанных ниже полевых шинах, использующих планируемое или циклическое сканирование, восстановление после ошибки может быть осуществлено одним из следующих способов:

a) немедленное повторение;

b) повторение, использующее резервное время в конце цикла;

c) обращение с сообщением как с потерянным и ожидание следующего цикла, чтобы получить следующее значение;

В случае a) все последующие сообщения в цикле немного задерживаются, в то время как при b) задерживается только текущее сообщение.

Случаи a) и b) обычно не классифицируются как недопустимая задержка.

Случай c) не будет считаться недопустимой задержкой, если интервал повторения цикла настолько короткий, что задержки между циклами незначительны, и следующее значение цикла может быть принято как замена потерянного предыдущего значения.

5.3.7 Появление неизвестного сообщения

Из-за сбоя или помехи появляется сообщение, связанное с непредвиденным или неизвестным источником.

Примечание — Такие сообщения являются дополнением к основному потоку сообщений и, так как у них нет ожидаемых источников, такие сообщения не могут быть классифицированы как «верное», «непреднамеренный повтор» или «ошибочная последовательность».

5.3.8 Подмена

Из-за сбоя или помехи появляется сообщение, связанное с надежным источником, в результате чего сообщение, не относящееся к безопасности, может быть принято относящимся к безопасности участником, который затем обрабатывает это сообщение, как относящееся к безопасности.

Примечание — Коммуникационным системам, применяющимся для приложений, связанных с безопасностью, могут потребоваться дополнительные проверки, чтобы выявить подмену. Такие проверки могут быть основаны на: разрешенных идентификаторах источников, парольных фразах, криптографии.

5.3.9 Адресация

Из-за сбоя или помехи сообщение, относящиеся к безопасности, отправлено неверному участнику, относящемуся к безопасности, который затем воспринимает принятое сообщение как правильное.

5.4 Меры по устранению детерминированных неисправностей

5.4.1 Общие положения

В данном разделе перечислены меры, применяющиеся для обнаружения детерминированных ошибок и отказов в коммуникационной системе, такие ошибки принципиально отличаются от стохастических ошибок, таких как искажение сообщения из-за помех.

5.4.2 Порядковый номер

Порядковый номер интегрирован в сообщения, которыми обменивается источник и приемник сообщений. Он может быть реализован как дополнительное поле данных, содержащее номер, определенным образом изменяющийся от сообщения к сообщению.

5.4.3 Временная метка

В большинстве случаев содержание сообщения имеет значимость только в определенный момент времени. Временная метка может быть временем или временем и датой, включенными в сообщение отправителем.

Примечания

1 Применяются относительные и абсолютные временные метки.

2 Для временных меток обязательна синхронизация временной базы. Для приложений безопасности требуется, чтобы синхронизация контролировалась.

5.4.4 Время ожидания

Во время передачи сообщения приемник сообщения проверяет, не превысила ли величина задержки между приемом двух последовательных сообщений заранее определенное значение. И если превышение произошло, то полагается считать, что возникла ошибка.

Пример — Метод доступа ориентирован на временные слоты.

Обмен сообщениями осуществляется в пределах постоянных циклов и заранее определенных слотов времени для каждого участника.

Необязательно: каждый участник должен отправлять свои данные в пределах данного ему слота времени, даже если не было изменений значения (это пример циклической коммуникации).

Для определения участника, который не совершил передачу в заданный для него слот времени, добавляется идентификатор источника.

5.4.5 Проверка подлинности соединения

Сообщения могут обладать уникальным идентификатором источника и/или получателя, который описывает логический адрес участника, относящегося к безопасности.

5.4.6 Сообщение обратной связи

Приемник сообщений возвращает сообщение обратной связи источнику, чтобы подтвердить получение начального сообщения. Сообщение обратной связи должно быть обработано на коммуникационных уровнях безопасности.

Примечания

1 Некоторые спецификации полевых шин используют слова «эхо» (echo) и «подтверждение получения» (receipt) как синонимы.

2 Такое вернувшееся сообщение обратной связи может содержать, например, только короткое подтверждение или также с исходными данными, а также любую другую информацию, позволяющую источнику проверить правильность приема.

5.4.7 Обеспечение полноты данных

Прикладной процесс, связанный с безопасностью, не должен полагаться на методы обеспечения полноты данных, если они не были спроектированы с точки зрения функциональной безопасности. Таким образом, в сообщение добавляются избыточные данные, чтобы стало возможным обнаружение искаженных данных с помощью контроля избыточным кодом.

Примечание — Коммуникационные системы, применяющиеся для приложений, связанных с безопасностью, могут прибегать к методам, таким как криптография, для обеспечения полноты данных, как к альтернативе типичным методам, таким как CRC проверки.

5.4.8 Избыточность с перекрестной проверкой

В приложениях полевых шин, связанных с безопасностью, безопасно передаваемые данные могут отправляться дважды одним или двумя отдельными сообщениями, использующими идентичные или различающиеся меры полноты, независимые от нижележащей шины.

Примечание — Дополнительные избыточные модели коммуникаций, удовлетворяющих требованиям функциональной безопасности, приведены в приложении А.

Безопасно передаваемые данные дополнительно проходят перекрестную проверку на достоверность в полевой шине или в отдельном блоке источника или приемника соединения. Если были обнаружены различия, то это означает, что произошла ошибка в процессе передачи, в блоке обработки источника или блоке обработки приемника.

Если применяются избыточные способы связи, то предполагается, что обычный режим защиты использует подходящие меры (например, разнообразие).

5.4.9 Различные системы обеспечения полноты данных

Если данные, относящиеся к безопасности (SR), и данные, не относящиеся к безопасности (NSR), передаются через одну шину, то применяются разные системы обеспечения полноты данных или принципы кодирования (разные хеш-функции, например, разные полиномы и алгоритмы, генерирующие CRC), чтобы воспрепятствовать влиянию любых NSR сообщений на функцию безопасности SR приемника.

Примечание — Допустимо иметь дополнительную систему обеспечения полноты данных для SR сообщений и не иметь ни одной такой системы для NSR сообщений.

5.5 Взаимоотношения между ошибками и мерами безопасности

Можно провести связь между мерами безопасности, выделенными в 5.4, и набором возможных ошибок в 5.3. Эта связь продемонстрирована в таблице 1. Каждая из мер безопасности предоставляет защиту от одной или нескольких ошибок передачи данных. Должно быть продемонстрировано, что существует хотя бы одна соответствующая мера безопасности или комбинация мер безопасности для определенных возможных ошибок в соответствии с таблицей 1.

Фактическая защита меры безопасности от ошибок зависит от конкретной реализации данной меры.

Примечание — Мера безопасности может быть внесена в соответствующую таблицу для заданного FSCP, только если данная мера вступает в силу до окончания гарантированного времени реакции функции безопасности полевой шины.

Таблица 1 — Анализ эффективности применения различных мер к возможным ошибкам

Ошибка коммуникации	Меры безопасности							
	Номер последовательности (см. 5.4.2)	Временная метка (см. 5.4.3)	Время ожидания (см. 5.4.4)	Проверка подлинности соединения (см. 5.4.5)	Сообщение обратной связи (см 5.4.6)	Обеспечение полноты данных (см. 5.4.7)	Избыточность с перекрестной проверкой (см. 5.4.8)	Различные системы обеспечения полноты данных (см. 5.4.9)
Искажение (см. 5.3.2)					x[d]	x	Только для последовательной шины[c]	
Непреднамеренный повтор (см. 5.3.3)	x	x					x	
Ошибочная последовательность (см. 5.3.4)	x	x					x	
Потеря (см. 5.3.5)	x				x		x	
Недопустимая задержка (см. 5.3.6)		x	x[b]					
Появление неизвестного сообщения (см. 5.3.7)	x			x[a]	x		x	
Подмена (см. 5.3.8)				x	x			x
Адресация (см. 5.3.9)				x				

Примечание — Таблица заимствована из МЭК 62280-2 [15] и [28].

[a] Только для идентификации отправителя. Обнаруживает только появление неверного источника.
[b] Необходимо для всех случаев.
[c] Данная мера сопоставима с механизмом обеспечения высокого качества данных, только если вычисление может показать, что частота появления остаточных ошибок Λ достигла значения, требующегося в 5.4.9, когда два сообщения посылаются через независимые передатчики.
[d] Эффективно, только если сообщение обратной связи содержит начальные данные или информацию о начальных данных.

5.6 Полнота данных

5.6.1 Вычисление интенсивности остаточных ошибок

Даже когда сообщения поступают правильно (детерминировано), безопасно передаваемые данные по-прежнему могут быть искажены. Таким образом, обеспечение полноты данных является фун-

даментальным компонентом коммуникационного уровня безопасности, необходимым для достижения уровня полноты безопасности. В таких случаях должны применяться подходящие хеш-функции, такие как биты честности, циклический избыточный код (CRC), повторение сообщений и другие методы избыточности сообщений.

Коммуникационный канал не должен использовать ту же хеш-функцию, что и добавленный сверху коммуникационный уровень безопасности (см. также МЭК 62280-1), если для таких случаев не применены специальные меры. Безопасный код должен быть функционально независимым от передаваемого кода.

Примечание — Если CRC используется в качестве хеш-функции, то коммуникационный канал не должен использовать тот же полином CRC, что и добавленный сверху коммуникационный уровень безопасности.

Все эти методы предоставляют средства для обеспечения низкой интенсивности появления остаточных ошибок. Все меры обеспечения полноты данных должны реализовываться в добавленных сверху уровнях (коммуникационных уровнях безопасности) средств управления, спроектированных с расчетом на соответствие УПБ.

Поставщик может выбрать различные методов вычисления оценочных данных для механизмов обеспечения полноты данных сетей полевых шин. Результаты таких вычислений ведут либо к необходимости приложить больше усилий при проектировании аппаратных средств и программного обеспечения для обеспечения полноты, либо к необходимости приложить больше усилий при вычислениях и предоставлении доказательств безотказности всей системы управления.

Интенсивность остаточных ошибок вычисляется из вероятности остаточных ошибок добавленного сверху механизма обеспечения полноты (безопасно передаваемых) данных и скорости передачи безопасных сообщений. Для оценки дополнительно следует учитывать максимальное число приемников данных (m), допустимое для одной функции безопасности.

Показанное ниже уравнение (1) должно использоваться, чтобы вычислить интенсивность остаточных ошибок из R_{SL} (Pe), если не применяется основная модель или если другой метод может быть более подходящим. Параметры уравнения определены в таблице 2.

$$\Lambda_{SL}(Pe) = R_{SL}(Pe) \cdot v \cdot m. \quad (1)$$

Примечание — Данная формула предполагает циклическую передачу безопасных сообщений.

Таблица 2 — Определение параметров, используемых для вычисления интенсивности остаточных ошибок

Параметр уравнения	Определение
$\Lambda_{SL}(Pe)$	Частота интенсивности ошибок в час коммуникационного уровня безопасности относительно вероятности битовой ошибки
Pe	Вероятность битовой ошибки. Если не доказана лучшая вероятность ошибки, следует использовать значение 10^{-2} [a]
$R_{SL}(Pe)$	Вероятность остаточной ошибки в безопасном сообщении
v	Максимальное число безопасных сообщений в час
m	Максимальное число приемников данных, допустимое для одной функции безопасности (см. рисунок 6)

[a] Значение вероятности битовой ошибки (Pe), равное 10^{-4}, в присутствии непрерывных магнитных помех приводит к прекращению коммуникаций (ложному срабатыванию) при циклическом обмене данными (например, время сторожевого таймера истекает из-за слишком большого количества повторных попыток). Используя правильную установку (экранирование, уравнивание потенциалов), можно уменьшить вероятность ложных срабатываний.

Проектирование уровня безопасности не может основываться на таком предположении, так как одиночный всплеск помех с множеством искаженных бит является распространенным явлением в промышленной среде.

Для того чтобы обнаружить такие нарушения, необходимы мощные механизмы обнаружения ошибок, достаточные для достижения требующейся вероятности остаточных ошибок $R_{SL}(Pe)$ при стократно более высоком значении P_e, то есть равном 10^{-2}.

Рисунок 6 демонстрирует применение при $m = 4$.



Рисунок 6 — Пример применения

5.6.2 Интенсивность остаточных ошибок и УПБ

Коммуникационная система, удовлетворяющая требованиям функциональной безопасности, должна обеспечивать интенсивность остаточных ошибок, установленную в таблице 3.

Как для систем, работающих в режиме с низкой частотой запросов, так и систем, работающих в режиме с высокой частотой запросов, должно быть задано время реакции функции безопасности, чтобы гарантировать необходимое число безопасных сообщений в секунду. Вычисление интенсивности ошибок основано на режиме с высокой частотой запросов и, таким образом, может всегда применяться и для режима с низкой частотой запросов.

Таблица 3 — Связь между интенсивностью остаточных ошибок и УПБ

Применимо для функций безопасности вплоть до УПБ	Вероятность возникновения опасного отказа в час для коммуникационной системы удовлетворяющей требованиям функциональной безопасности	Максимальная допустимая частота возникновения остаточных ошибок для коммуникационной системы, удовлетворяющей требованиям функциональной безопасности
4	$< 10^{-10}$ / ч	$\Lambda < 10^{-10}$ / ч
3	$< 10^{-9}$ / ч	$\Lambda < 10^{-9}$ / ч
2	$< 10^{-8}$ / ч	$\Lambda < 10^{-8}$ / ч
1	$< 10^{-7}$ / ч	$\Lambda < 10^{-7}$ / ч
Примечание — Значения в данной таблице основываются на предположении о том, что отказы коммуникационной системы, удовлетворяющей требованиям функциональной безопасности, составляют 1 % общих отказов функции безопасности.		

5.7 Связь между функциональной безопасностью и защищенностью

Примечание — Оценка угроз защите и оценка рисков обычно необходимы для защиты применений, связанных с безопасностью, от преднамеренных атак или случайных изменений. Защищенность может быть достигнута установлением соответствующих политик безопасности и мер безопасности, таких как физические (например, механические, электронные) или организационные меры.

Когда приложению требуются электронные меры защиты, защищенность должна быть реализована в черном канале. Функция безопасности может быть реализована как внутри устройств, так и на внешних точках доступа. Некоторые требования защищенности подробно рассматриваются в комплексе МЭК 62443.

Примечание — Дополнительные конкретные для профиля требования могут также быть установлены в МЭК 61784-4 [10].

5.8 Предельные условия и ограничения

5.8.1 Электрическая безопасность

Электрическая безопасность является предварительным условием для коммуникационной системы, удовлетворяющей требованиям функциональной безопасности. Таким образом, все устройства,

подключенные к такой коммуникационной системе, должны соответствовать требованиям соответствующим спецификациям МЭК для SELV/PELV (например, МЭК 61131-2).

Примечания

1 Требующиеся дополнения к руководству по установке (например, кабели, прокладка кабеля, экраны, заземление, выравнивание потенциалов) установлены в МЭК 61918 и МЭК 61784-5.

2 Требования для блоков питания (например, устойчивость к одиночным сбоям, использование раздельных блоков питания, SELV/PELV, специфические для страны ограничения по току и т. д.) установлены в МЭК 61918 и МЭК 61784-5.

3 Требования для стандартных устройств шины (например, оценка) специфичны для профилей коммуникаций, удовлетворяющих требованиям функциональной безопасности.

5.8.2 Электромагнитная совместимость (ЭМС)

МЭК 61508 требует «повышения помехозащищенности», но не устанавливает, как этого можно достичь. В настоящем стандарте профили коммуникаций, удовлетворяющие требованиям функциональной безопасности, используют для этой цели повышенные уровни тестирования и соответствующие критерии качества работы, установленные в МЭК 61326-3-1. МЭК 61326-3-2 может использоваться, как исключение, если предполагаемое применение в точности подходит под область применения и предварительные условия МЭК 61326-3-2.

Примечание — Отдельные приложения могут требовать более высокий уровень, чем установленный в МЭК 61326-3-1, согласно спецификациям требований к безопасности (SRS).

5.9 Руководство по установке

Требования к установке оборудования, использующего коммуникационные технологии, установленные в настоящем стандарте, определены в МЭК 61918 и в частях МЭК 61784-5 для конкретных профилей, как и в любых других соответствующих дополнительных стандартах, требующихся для этих конкретных профилей.

Неподдерживаемые устройства, подключенные к шине, могут серьезно помешать выполнению работы и, таким образом, негативно сказаться на готовности (по причине ложных аварийных отключений, включая ложное срабатывание), приводя к отключению пользователем службы безопасности.

Поэтому настоятельно рекомендуется, чтобы все изделия, соединенные с полевой шиной в приложении, связанном с безопасностью (даже стандартные), предоставляли требующееся подтверждение соответствия связанному с ними протоколу полевой шины (например, декларацию изготовителя или подтверждение соответствия третьей стороны).

Примечание — Дополнительная информация может быть найдена в разделах настоящего стандарта, рассматривающих конкретные технологии, если это необходимо.

5.10 Руководство по безопасности

Согласно с МЭК 61508-2 поставщики устройства должны предоставлять руководство по безопасности. Описание минимума информации, включение в руководство которой требуется профилем, предоставлено в соответствующих частях специфичных для профиля.

5.11 Политика безопасности

Пользователи настоящего стандарта должны принять во внимание следующие ограничения во избежание недопонимания, неоправданных ожиданий или судебных исков по вопросам разработок и приложений, связанных с безопасностью.

Примечание — Их обсуждают, например, при обучении, на семинарах, симпозиумах и в процессе консультирования.

Использование установленных в настоящем стандарте коммуникационных технологий в устройстве не гарантирует, что все необходимые технические, организационные и нормативные требования устройства, используемого в приложении, связанном с безопасностью, были выполнены в соответствии с требованиями МЭК 61508.

Чтобы устройство, удовлетворяющее требованиям настоящего стандарта, было пригодно для использования в приложениях, связанных с безопасностью, должны соблюдаться надлежащие процессы менеджмента функциональной безопасности для всего жизненного цикла устройства, которые

должны соответствовать стандартам безопасности и соответствующим законодательствам/нормам. Это должно быть оценено в соответствии с требованиями независимости и компетентности, описанными в МЭК 61508-1.

В контексте полноты безопасности аппаратных средств, наивысший уровень полноты безопасности, который может быть заявлен для функции безопасности, ограничен предельными значениями полноты безопасности аппаратных средств, которые достигаются способом 1_H, описанным в МЭК 61508-2, основанным на концепциях отказоустойчивости аппаратных средств и доле безопасных отказов (реализующихся на уровне системы или подсистемы).

Изготовитель устройства, использующего коммуникационные технологии, определенные в настоящем стандарте, несет ответственность за правильную реализацию требований настоящего стандарта, правильность и полноту документации на устройство и информации.

Настоятельно рекомендуется, чтобы разработчики конкретного профиля выполняли надлежащие испытания на соответствие и проверки в соответствующей организации, компетентной в конкретной реализуемой технологии. Информация о тестовых лабораториях, проводящих тесты на соответствие и подтверждение соответствия в согласии с требованиями данного раздела, приведена в приложении В каждой индивидуальной части профиля.

Примечание — Эти требования и рекомендации включены, потому что неправильные реализации могут повлечь за собой серьезные телесные повреждения или гибель.

6 Семейство 1 коммуникационных профилей (Полевая шина FOUNDATION™). Профили для функциональной безопасности

6.1 Коммуникационный профиль 1/1, удовлетворяющий требованиям функциональной безопасности

Семейство 1 коммуникационных профилей (общеизвестное как полевые шины Foundation™[2]) определяет коммуникационные профили, основанные 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 CP 1/1, CP 1/2 и CP 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 CP 1/1, представленном в МЭК 61784-1, и спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-1.

6.2 Технический обзор

Существуют приложения, требующие уровень полноты безопасности с первого по четвертый, как определено в МЭК 61508.

Примечание — Такие приложения, связанные с безопасностью, также называются инструментальными системами безопасности (SIS) (см. МЭК 61511 [9]).

Коммуникационный уровень безопасности FSCP 1/1, установленный в МЭК 61784-3-1, дает возможность использовать интеллектуальные устройства в системах, связанных с безопасностью, и тем самым расширяет возможности системы, позволяя системе соответствовать требованиям ее уровня полноты безопасности. Коммуникационный уровень безопасности, определенный в IEC 61784-3-1, применим только к CP 1/1, как описано в IEC 61784-1.

В МЭК 61784-3-1 не определены требования для инструментальных средств или функционала измерений внутреннего состояния устройств. Коммуникационный уровень безопасности гарантирует, что конфигурация, созданная при помощи инструментальных средств, загружается в устройства безопасности без негативного влияния протокола на уровень полноты безопасности. Область применения МЭК 61784-3-1 определена на рисунке 7.

---

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

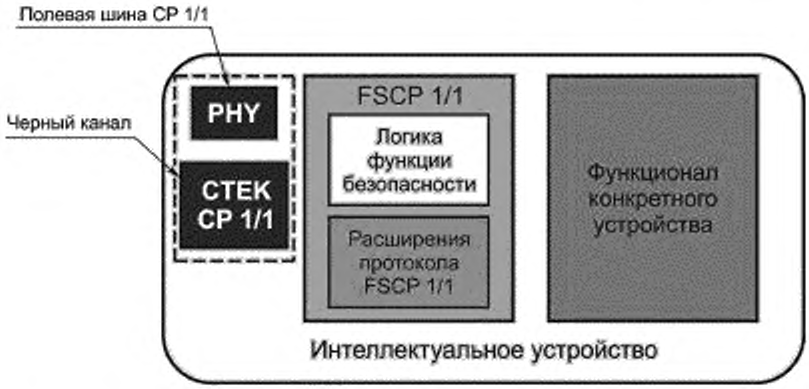


Рисунок 7 — Область применения FSCP 1/1

Сам по себе FSCP 1/1 не обеспечивает функциональную безопасность. Помимо 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.

Дополнительная информация приведена в МЭК 61784-3-1.

7 Семейство 2 коммуникационных профилей (CIP™). Профили для функциональной безопасности

7.1 Коммуникационный профиль 2/1, удовлетворяющий требованиям функциональной безопасности

Семейство 2 коммуникационных профилей (общеизвестное как CIP™[3]) определяет коммуникационные профили, основанные на МЭК 61158-2 Тип 2, МЭК 61158-3-2, МЭК 61158-4-2, МЭК 61158-5-2 и МЭК 61158-6-2.

Базовые профили CP 2/1, CP 2/2 и CP 2/3 определены в МЭК 61784-1 и МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 2/1 (CIP Safety™[3]) семейства 2 коммуникационных профилей (CPF 2) основан на базовых профилях CPF 2 из МЭК 61784-1 и МЭК 61784-2, а также спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-2.

7.2 Технический обзор

FSCP 2/1 основан на модели CPF 2 отправителя/получателя. Объединение отправителей и получателей является важной частью взаимоотношения, которое обеспечивает высокий уровень полноты, необходимый для приложений, связанных с безопасностью.

Коммуникационный уровень безопасности профиля FSCP 2/1 устанавливается при помощи объекта Safety Validator (подтверждение соответствия требованиям безопасности). Данный объект отвечает за управление безопасными соединениями FSCP 2/1 и служит интерфейсом между прикладными объектами, связанными с безопасностью, и соединениями канального уровня, как это показано на рисунке 8. Объект Safety Validator обеспечивает полноту безопасно передаваемых данных.

[3] CIP™ (Общий промышленный протокол) и CIP Safety™ являются торговыми марками некоммерческой организации ODVA, Inc. Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований CIP™ или CIP Safety™. Использование торговых марок CIP™ или CIP Safety™ требует разрешения со стороны ODVA.

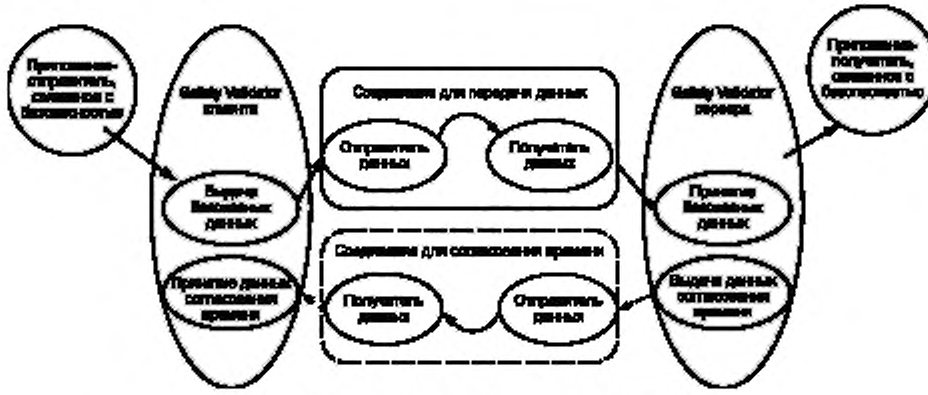


Рисунок 8 — Связи между объектами Safety Validator

Полнота безопасно передаваемых данных обеспечивается следующим образом:

- отправитель связанного с безопасностью приложения использует экземпляр объекта Safety Validator на стороне клиента, чтобы выдать безопасно передаваемые данные и обеспечить временное согласование;
- клиент взаимодействует с отправителем данных канала передачи данных для передачи данных и с получателем данных канала передачи данных для получения сообщений согласования времени;
- отправитель связанного с безопасностью приложения использует экземпляр объекта Safety Validator на стороне сервера для получения и проверки данных;
- сервер взаимодействует с получателем данных канала передачи данных для получения данных и с отправителем данных канала передачи данных для передачи сообщений согласования времени.

FSCP 2/1 применяет концепцию черного канала. Отправители и получатели данных канала передачи данных не обладают никакими знаниями о содержании пакета безопасно передаваемых данных и не реализует никаких функций безопасности. Ответственность за высокий уровень полноты передачи и проверки безопасно передаваемых данных лежит на экземплярах объекта Safety Validator.

FSCP 2/1 использует следующие меры для обеспечения полноты обмена безопасных сообщений:

- временную метку;
- проверку подлинности соединения;
- обеспечение полноты данных;
- избыточность с перекрестной проверкой;
- различные системы обеспечения полноты данных.

Сообщения отправляются с временной меткой, которая позволяет получателю проверить «возраст» посылаемых данных. Идентификация кодируется в каждом сообщении, связанном с безопасностью, чтобы обеспечить использование сообщения правильным получателем. Все сообщения, связанные с безопасностью, используют уникальный CRC. Данные, связанные с безопасностью, отправляются с дополнительной информацией. При отправлении сообщений, связанных с безопасностью, используются разнообразные средства, чтобы стандартные сообщения CPF 2 не воспринимались как сообщения безопасности.

Дополнительная информация приведена в МЭК 61784-3-2.

8 Семейство 3 коммуникационных профилей (PROFIBUS™, PROFINET™). Профили для функциональной безопасности

8.1 Коммуникационный профиль 3/1, удовлетворяющий требованиям функциональной безопасности

Семейство 3 коммуникационных профилей (общеизвестное как PROFIBUS™, PROFINET™[4]) определяет коммуникационные профили, основанные на МЭК 61158-2 Тип 3, МЭК 61158-3-3, МЭК 61158-4-3, МЭК 61158-5-3, МЭК 61158-5-10, МЭК 61158-6-3, и МЭК 61158-6-10.

[4] PROFIBUS™, PROFINET™ и PROFIsafe™ являются торговыми марками некоммерческой организации PROFIBUS Nutzerorganisation e.V. (PNO). Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований PROFIBUS™, PROFINET™ или PROFIsafe™. Использование торговых марок PROFIBUS™, PROFINET™ и PROFIsafe™ требует разрешения со стороны PNO.

Базовые профили CP 3/1 и CP 3/2 определены в МЭК 61784-1. CP 3/4, CP 3/5 и CP 3/6 определены в МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 3/1 (PROFIBUS™, PROFINET™[5]) семейства 3 коммуникационных профилей (CPF 3) основан на базовых профилях CPF 3 из МЭК 61784-1 и МЭК 61784-2, а также на спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-3.

8.2 Технический обзор

FSCP 3/1 основан на циклическом обмене данным между контроллером (шиной) и связанными с ним (полевыми) устройствами, используя непосредственную коммуникационную связь (см. рисунок 9). Один контроллер может управлять любым набором стандартных устройств и устройств, связанных с безопасностью, соединенных с сетью. Также возможно разным контроллерам назначать задачи безопасности и стандартные задачи. Любые из так называемых ациклических коммуникаций между устройствами и контроллерами или диспетчерами, такими как программируемые устройства, предназначены для целей конфигурирования, параметризации, диагностики и поддержания работоспособности.

Для реализации FSCP 3/1 были выбраны следующие четыре меры:

- (виртуальная) последовательная нумерация;
- контроль времени сторожевым таймером с уведомлением;
- кодовое имя для каждого коммуникационного отношения;
- проверка полноты данных циклическим избыточным кодом.

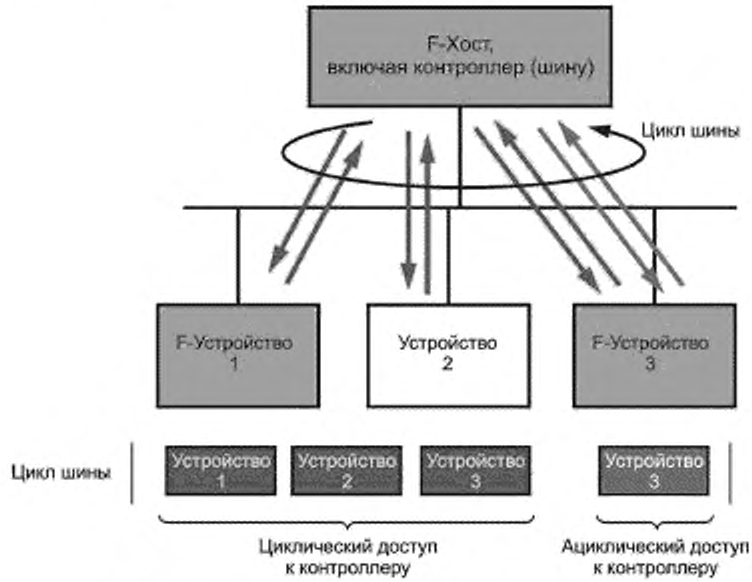


Рисунок 9 — Базовые предварительные условия коммуникации для FSCP 3/1

Для защиты от любого неправильного функционирования, вызванного элементами сети, хранящимися в сообщении, используется достаточно большой диапазон последовательной нумерации. Каждое устройство безопасности в качестве уведомления возвращает сообщение с PDU безопасности, даже если нет данных процесса. Для каждой непосредственной коммуникационной связи устанавливается отдельный сторожевой таймер как на стороне отправителя, так и на стороне получателя. Устанавливается уникальное кодовое имя на каждое коммуникационное отношение для проверки подлинности, которое кодируется в исходном значении сигнатуры CRC для циклически рассчитываемой и передаваемой сигнатуры CRC2 (см. рисунок 10).

[5] PROFIBUS™, PROFINET™ и PROFIsafe™ являются торговыми марками некоммерческой организации PROFIBUS Nutzerorganisation e.V. (PNO). Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований PROFIBUS™, PROFINET™ или PROFIsafe™. Использование торговых марок PROFIBUS™, PROFINET™ и PROFIsafe™ требует разрешения со стороны PNO.

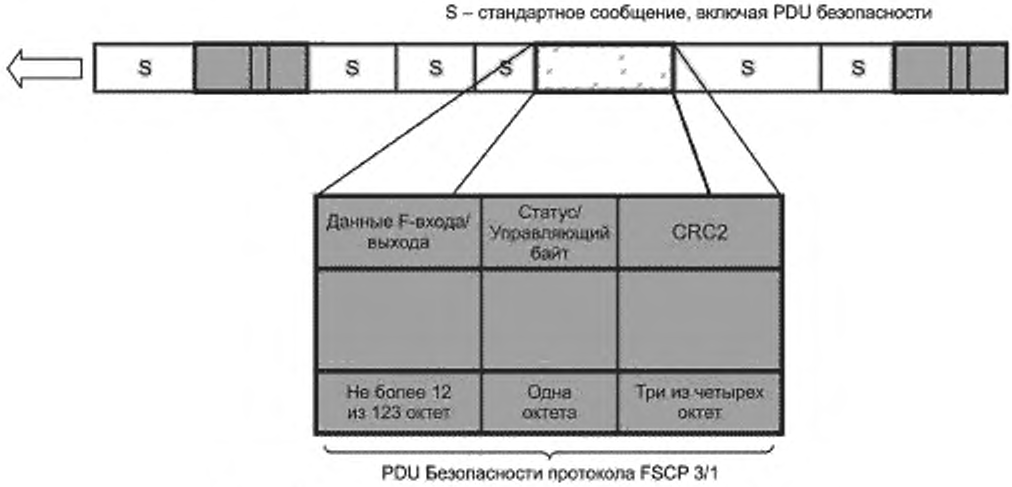


Рисунок 10 — Структура PDU безопасности профиля FSCP 3/1

FSCP 3/1 обеспечивает два режима работы: режим V1 и режим V2. В то время как мер режима V1 достаточно для безопасной передачи данных на сетях CP 3/1 без расширений, более «щедрые свойства» Ethernet / CP 3/4 по CP 3/6, такие как более широкое пространство адресов и буферизация компонентов маршрутизатора, требуют некоторых расширений к протоколу FSCP 3/1, тем самым приводя к режиму V2. Режим V1 ограничивается протоколом CP 3/1, в то время как режим V2 требуется для протоколов с CP 3/4 по CP 3/6 и/или CP 3/1. МЭК 61784-3-3 подробно описывает только расширенный функционал так называемого режима V2. Безопасная коммуникация между компонентами PROFINET CBA (см. PC 3/3) еще не была определена. Обзор FSCP 3/1 в рамках архитектур CP 3/1 и CP 3/4 по CP 3/6 приведен на рисунке 11.

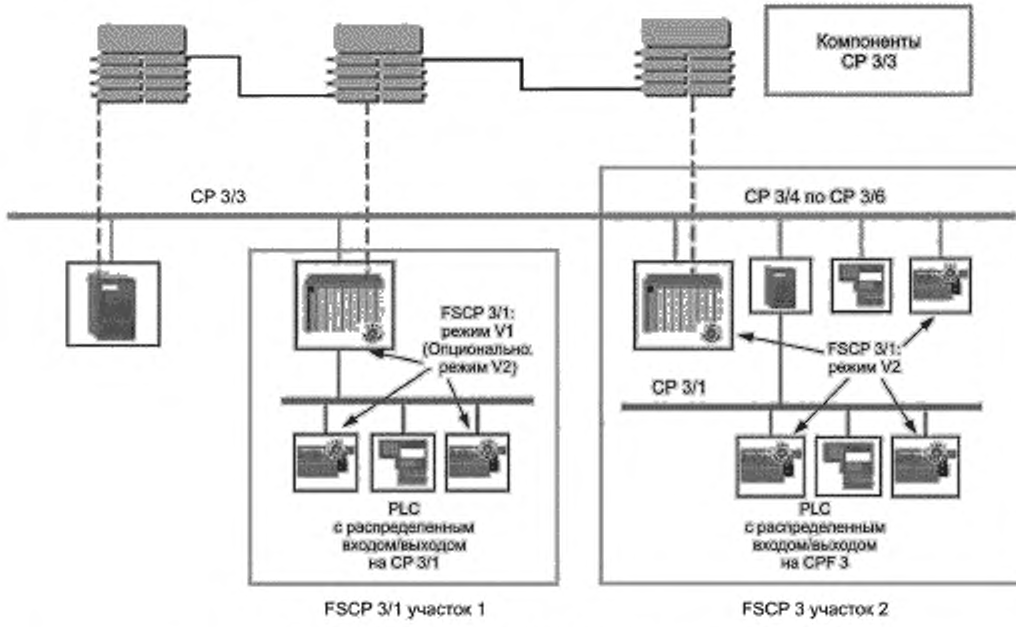


Рисунок 11 — Режимы безопасных коммуникаций

Дополнительная информация приведена в МЭК 61784-3-3.

9 Семейство 6 коммуникационных профилей (INTERBUS®). Профили для функциональной безопасности

9.1 Коммуникационный профиль 6/7, удовлетворяющий требованиям функциональной безопасности

Семейство 6 коммуникационных профилей (общеизвестное как INTERBUS®[6]) определяет коммуникационные профили, основанные на МЭК 61158-2 Тип 8, МЭК 61158-3-8, МЭК 61158-4-8, МЭК 61158-5-8 и МЭК 61158-6-8.

Базовые профили CP 6/1, CP 6/2, CP 6/3 определены в МЭК 61784-1. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 6/7 (INTERBUS Safety™[6]) семейства 6 коммуникационных профилей (CPF 6) основан на базовых профилях CPF 6 из МЭК 61784-1, а также на спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-6.

Профили CP 6/1, CP 6/2 и CP 6/3 содержат необязательные службы, устанавливаемые идентификаторами профиля. Идентификаторы профиля, подходящие для CP 6/7, представлены в таблице 4.

Таблица 4 — Идентификаторы профиля, используемые для FSCP 6/7

Профиль	Ведущее устройство		Ведомое устройство		
	цикличное	цикличное и нецикличное	цикличное	нецикличное	цикличное и нецикличное
Профиль 6/1	618	619	611	—	613
Профиль 6/2	—	629	—	—	623
Профиль 6/3	—	639	—	—	633

Спецификация уровня коммуникаций безопасности, данная в МЭК 61784-6, применима в полной мере.

9.2 Технический обзор

FSCP 6/7 использует существующий тракт передачи для циклической передачи данных (для данных процесса). По сути это является концепций ведущий/ведомый с топологией «физическое кольцо» и логическими непосредственными связями между одним ведущим устройством и каждым из ведомых (см. рисунок 12). Данные передаются с помощью блока PDU (известного как суммарный кадр), из которого каждое из ведомых устройств извлекает свои выходные данные и вносит свои входные данные.

[6] INTERBUS® и INTERBUS Safety™ являются торговыми марками Phoenix Contact GmbH & Co. KG, управление торговыми марками передано некоммерческой организации INTERBUS Club. Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований INTERBUS® и INTERBUS Safety™. Использование торговых марок INTERBUS® и INTERBUS Safety™ требует разрешения со стороны INTERBUS Club.

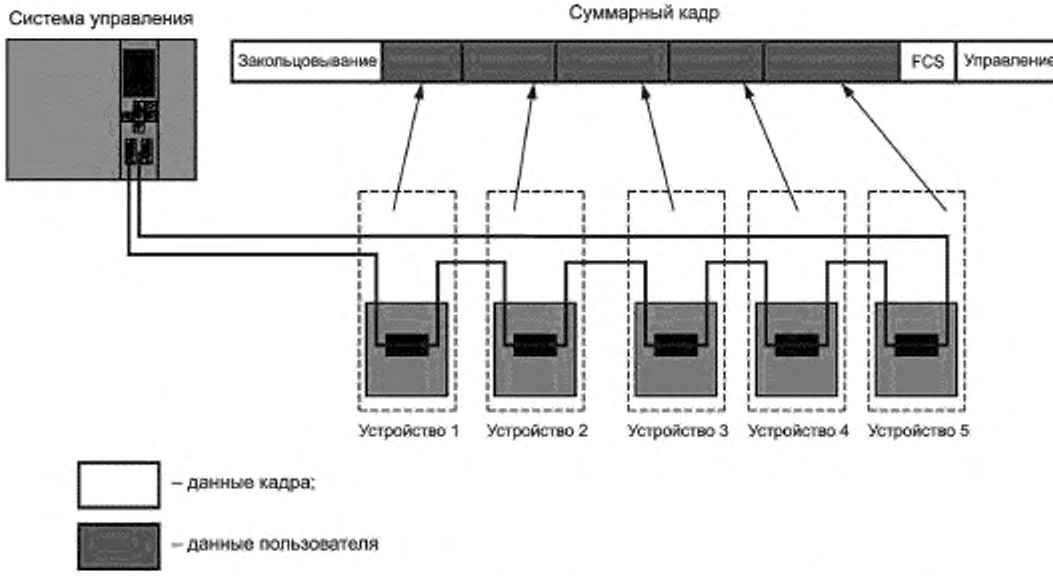


Рисунок 12 — Входные условия для коммуникации FSCP 6/7

Коммуникационный уровень безопасности FSCP 6/7 предоставляет следующие меры безопасности для реализации коммуникационного уровня безопасности:

- порядковый номер;
- временная метка;
- проверка подлинности соединения;
- проверка полноты безопасных данных циклическим избыточным кодом.

Нумерация последовательности использует диапазон от 001 до 111 без 000. Проверка подлинности соединения (информация отправителя/получателя) использует семь бит, поэтому с полевой шиной безопасности может быть интегрировано до 126 ведомых устройств. Безопасно передаваемые данные могут передаваться от ведущего устройства безопасности каждому ведомому устройству безопасности и от каждого ведомого устройства безопасности каждому ведущему устройству безопасности в рамках одного цикла данных. Отдельный сторожевой таймер, установленный на каждом выходе ведомого устройства безопасности, обеспечивает время реакции функции безопасности для каждой функции безопасности и может широко регулироваться. Сторожевой таймер можно настроить для каждого выходного канала безопасности выходного ведомого устройства безопасности.

Коммуникационный уровень безопасности профиля FSCP 6/7 может применяться для функций безопасности уровнем до УПБ 3. Поэтому полевая шина безопасности составляет максимум 1 % всей PFH (средней частоты опасных отказов). Для полевой шины достигается значение $\Lambda < 10^{-7}$. Встроенный сторожевой таймер, обеспечивая время ожидания каждого выходного канала каждого выходного ведомого устройства безопасности, гарантирует время реакции функции безопасности. Время реакции функции безопасности включает:

- время передачи данных по полевой шине от входного ведомого устройства безопасности ведущему устройству и от ведущего устройства выходному ведомому устройству безопасности, включая также возможные повторения PDU безопасности, возникающие по причине ошибок передачи данных;
- время обработки на каждом ведомом устройстве безопасности (входном и выходном) и время обработки в ПЭС (обычно используется безопасный ПЛК, на котором реализовано ведущее устройство);
- время торможения машины.

Если установленное время встроенного сторожевого таймера конкретного выходного канала выходного ведомого устройства безопасности превышено, то соответствующий выходной канал переводится в свое безопасное состояние, которое, как правило, является состоянием с отключенным питанием.

Структура PDU безопасности включает меры безопасности (порядковый номер, временную метку, проверку подлинности соединения, CRC) и безопасно передаваемые данные. Безопасно передаваемые данные и меры безопасности для каждого ведомого устройства безопасности будут интегрированы в суммарный кадр.

Дополнительная информация приведена в МЭК 61784-3-6.

10 Семейство 8 коммуникационных профилей (CC-Link™). Профили для функциональной безопасности

10.1 Коммуникационный профиль 8/1, удовлетворяющий требованиям функциональной безопасности

Семейство 8 коммуникационных профилей (общеизвестное как CC-Link™[7]) определяет коммуникационные профили, основанные на МЭК 61158-2 Type 18, МЭК 61158-3-18, МЭК 61158-4-18, МЭК 61158-5-18 и МЭК 61158-6-18.

Базовые профили CP 8/1, CP 8/2, CP 8/3 определены в МЭК 61784-1. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 8/1 (CC-Link Safety™[7]) семейства 8 коммуникационных профилей (CPF 8) основан на базовых профилях CPF 8 из МЭК 61784-1, а также на спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-8.

10.2 Технический обзор

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

Протокол FSCP 8/1 спроектирован для поддержки УПБЗ (МЭК 61508) на основе CPF 8 при помощи дополнительно установленных механизмов, реализующих порядковый номер, время ожидания, проверку подлинности соединения, сообщения обратной связи, обеспечение полноты данных и различные меры безопасности, гарантирующие обеспечения полноты данных.

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

Дополнительная информация приведена в МЭК 61784-3-8.

11 Семейство 12 коммуникационных профилей (EtherCAT™). Профили для функциональной безопасности

11.1 Коммуникационный профиль 12/1, удовлетворяющий требованиям функциональной безопасности

Семейство 12 коммуникационных профилей (общеизвестное как EtherCAT™[8]) определяет коммуникационные профили, основанные на МЭК 61158-2 Type 12, МЭК 61158-3-12, МЭК 61158-4-12, МЭК 61158-5-12 и МЭК 61158-6-12.

---

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

[8] EtherCAT™ и Safety-over-EtherCAT™ являются торговыми марками Beckhoff, Verl. Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований EtherCAT™ и Safety-over-EtherCAT™. Использование торговых марок EtherCAT™ и Safety-over-EtherCAT™ требует разрешения со стороны Beckhoff, Verl.

Базовые профили CP 12/1 и CP 12/2 определены в МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 12/1 (Safety-over-EtherCAT™) семейства 12 коммуникационных профилей (CPF 12) основан на базовых профилях CPF 12 из МЭК 61784-2, а также на спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-12.

11.2 Технический обзор

FSCP 12/1 описывает протокол для передачи безопасных данных до уровня УПБЗ между устройствами FSCP 12/1. PDU безопасности пересылаются подчиненной полевой шиной, на которую не распространяются требования обеспечения безопасности, так как она может считаться черным каналом. PDU безопасности, которыми обмениваются два партнера по коммуникации, воспринимаются подчиненной полевой шиной как данные процесса, которыми обмениваются циклически.

FSCP 12/1 использует уникальную связь ведущий/ведомый между ведущим и ведомым устройствами FSoE, которая называется соединение FSoE (см. рисунок 13). В соединении FSoE каждое устройство, как только получает новое сообщение от устройства-партнера, возвращает только свое собственное новое сообщение. Весь путь передачи между ведомым устройством FSoE и ведущим устройством FSoE контролируется отдельными сторожевыми таймерами, установленными на обоих устройствах в каждом цикле FSoE.

Ведущее устройство FSoE может обрабатывать более одного соединения FSoE для поддержки нескольких ведомых устройств FSoE.

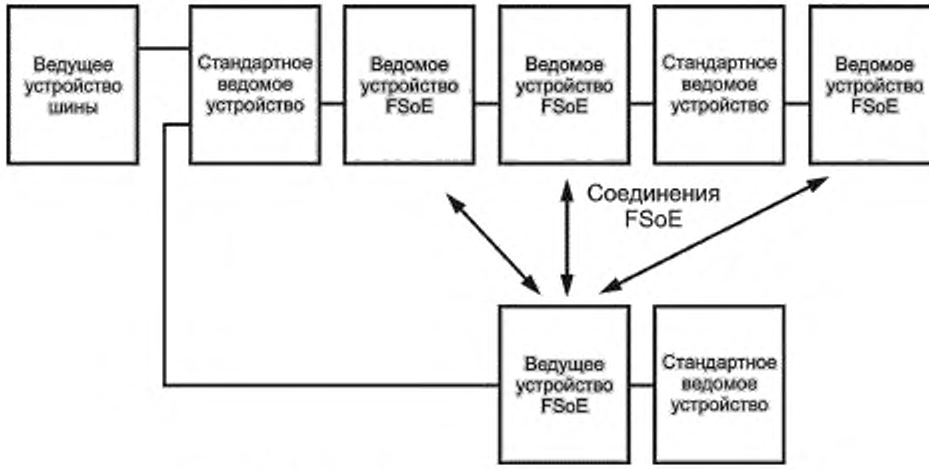


Рисунок 13 — Базовая система FSCP 12/1

Полнота передачи безопасных данных обеспечивается при помощи:

- номера сеанса для обнаружения буферизации полной последовательности загрузки;
- порядкового номера для обнаружения обмена, повторения, появления или потери целого сообщения;
- уникальной идентификации соединения для безопасного обнаружения неправильно маршрутизированного сообщения из-за уникальной адресной связи;
- контроля сторожевым устройством для безопасного обнаружения недопустимых задержек в коммуникационном пути;
- проверки на полноту данных циклическим избыточным кодом для обнаружения искажения сообщений от источника приемнику.

Смены состояний инициируются ведущим устройством FSoE и подтверждаются ведомым устройством FSoE. Конечный автомат FSoE также включает обмен информацией и ее проверку для коммуникационной связи.

Дополнительная информация предоставлена в МЭК 61784-3-12.

12 Семейство 13 коммуникационных профилей (Ethernet POWERLINK™). Профили для функциональной безопасности.

12.1 Коммуникационный профиль 13/1, удовлетворяющий требованиям функциональной безопасности

Семейство 13 коммуникационных профилей (общеизвестное как Ethernet POWERLINK[9)]) определяет коммуникационные профили, основанные на МЭК 61158-3-13, МЭК 61158-4-13, МЭК 61158-5-13 и МЭК 61158-6-13.

Базовый профиль CP 13/1 определен в МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 13/1 (Ethernet POWERLINK safety[9)]) семейства 13 коммуникационных профилей (CPF 13) основан на базовых профилях CPF 13, представленных в МЭК 61784-2, и спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-13.

12.2 Технический обзор

Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 13/1 спроектирован с целью обеспечения коммуникаций на полевой шине для удовлетворяющих требованиям функциональной безопасности применений в микросекундном диапазоне.

Службы и протокол FSCP 13/1 определяют передачу безопасных данных между устройствами безопасности. Технология протокола FSCP 13/1 спроектирована для реализации функции безопасности с УПБ 3 в соответствии с МЭК 61508.

Определены следующие службы:

- конфигурация сети;
- управление сетью (запуск, оперативная диагностика);
- обмен произвольными данными и
- обмен синхронизированными данными.

Передача синхронизированных данных между устройствами безопасности использует модель «издатель-подписчик» (см. рисунок 14), в то время как передача произвольных данных использует модель «клиент-сервер» (см. рисунок 15).

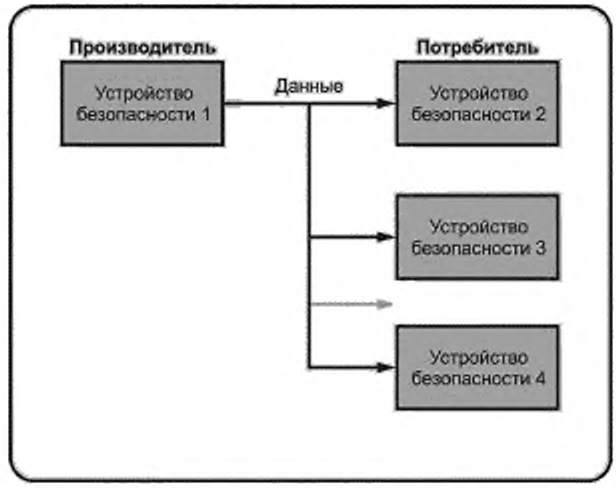


Рисунок 14 — Пример модели «производитель-потребитель»

9) Ethernet POWERLINK and Ethernet POWERLINK являются торговыми марками некоммерческой организации Ethernet POWERLINK Standardization Group (EPSG). Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований Ethernet POWERLINK and Ethernet POWERLINK. Использование торговых марок Ethernet POWERLINK и Ethernet POWERLINK требует разрешения со стороны Ethernet POWERLINK Standardization Group (EPSG).

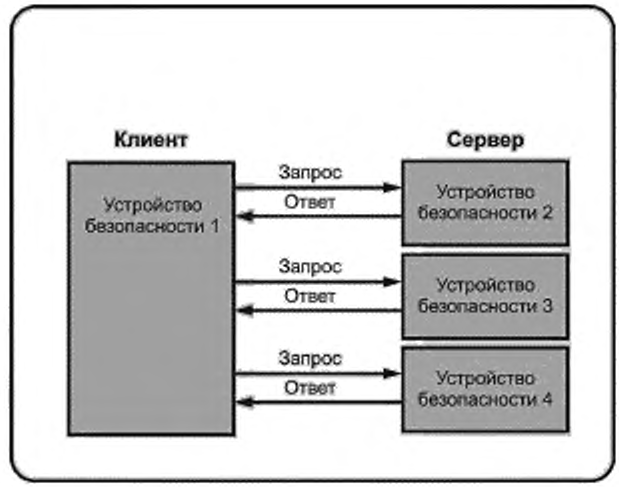


Рисунок 15 — Пример модели «клиент-сервер»

Дополнительная информация представлена в МЭК 61784-3-13.

13 Семейство 14 коммуникационных профилей (EPA®). Профили для функциональной безопасности

13.1 Коммуникационный профиль 14/1, удовлетворяющий требованиям функциональной безопасности

Семейство 14 коммуникационных профилей (общеизвестное как EPA®[10]) определяет коммуникационные профили, основанные на МЭК 61158-3-14, МЭК 61158-4-14, МЭК 61158-5-14 и МЭК 61158-6-14.

Базовые профили CP 14/1 и CP 14/2 определены в МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональной безопасности, FSCP 14/1 (EPASafety®[10]) семейства 14 коммуникационных профилей (CPF 14), основан на базовых профилях CPF 14, представленных в МЭК 61784-2, и спецификациях коммуникационного уровня безопасности, определенных в МЭК 61784-3-14.

13.2 Технический обзор

EPASafety описывает спецификацию безопасной коммуникации, использующуюся для соединения полевых устройств безопасности и контроллеров в EPA системах. Это дополнительная технология, основанная на протоколе EPA, установленном в МЭК 61158 и МЭК 61784-2, для снижения вероятности отказа или ошибки в передаче данных между безопасными передатчиками, исполнительными устройствами и полевыми контроллерами до уровня, установленного соответствующими стандартами или ниже.

Коммуникации EPA основаны на принципе черного канала, как это показано на рисунке 16. Черный канал включает в себя устройства, не относящиеся к безопасности, такие как провода, волоконно-оптические линии связи, повторитель, потенциальный барьер, блоки питания, специализированные интегральные схемы (ASIC), коммуникационный стек, мост EPA, интерфейс. Коммуникационный стек включает в себя следующие уровни: физический, канала данных, сети (IP), транспортный (UDP) и прикладной уровень.

Во время передачи данных в черном канале могут возникать ошибки и сбои по следующим причинам:

- случайный сбой;

[10] EPA® и EPASafety® являются торговыми марками некоммерческой организации Zhejiang SUPCON® Sci&Tech Group Co. Ltd. China. Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его продукцию. Соответствие этому стандарту не требует использования наименований EPA® и EPASafety®. Использование торговых марок EPA® и EPASafety® требует разрешения со стороны Zhejiang SUPCON® Sci&Tech Group Co. Ltd. China.

- отказ/сбой стандартных аппаратных средств;
- отказ системы, вызванный стандартными компонентами аппаратных средств или программного обеспечения.

В системах EPASafety приложения безопасности и стандартные приложения одновременно пользуются одним каналом передачи данных. Функции безопасной передачи данных включает в себя все меры для того, чтобы детерминировано обнаруживать все перечисленные выше отказы/опасности, которые может пропустить стандартная система передачи данных, или же для того, чтобы обеспечить вероятность остаточных ошибок в определенных пределах.

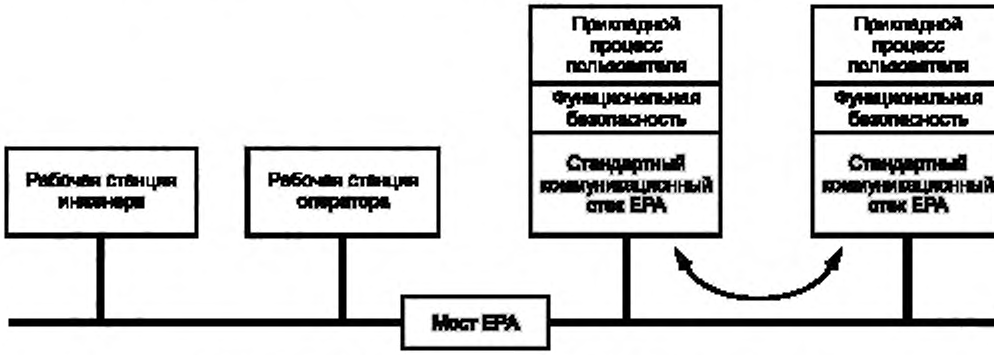


Рисунок 16 — FSCP 14/1 архитектура коммуникации безопасности

Дополнительная информация приведена в МЭК 61784-3-14.

Приложение А
(справочное)

Примеры моделей коммуникаций, удовлетворяющих требованиям функциональной безопасности

А.1 Общие положения

Настоящее приложение рассматривает различные модели структуры реализации устройств полевых шин безопасности. Данные модели предоставляют разные механизмы обнаружения сбоев. Модели, показанные ниже, предназначены только для того, чтобы проиллюстрировать возможные структуры реализации. МЭК 61508 следует использовать для проектирования системы в целом.

Далее приведены некоторые примеры, но могут применяться и другие модели.

А.2 Модель А

Модель А, показанная на рисунке А.1, служит базовой моделью для других моделей. Только один канал подсоединен к шине.

Данные с обоих коммуникационных уровней безопасности проходят проверку безопасности и перекрестную проверку. Оба коммуникационных уровня безопасности принимают участие в формировании сообщения. Если перекрестная проверка показывает отклонение, то предпринимается соответствующее действие для поддержания безопасности.

Примечание — Реализация может быть выполнена, используя разнообразие аппаратных средств и/или программного обеспечения.



Рисунок А.1 — Модель А

А.3 Модель В

Модель В на рисунке А.2 представляет систему, в которой все коммуникационные уровни безопасности, уровни передачи данных и средства передачи данных продублированы.

Сообщения с обоих коммуникационных каналов безопасности проходят проверку безопасности и перекрестную проверку. Если перекрестная проверка показывает отклонение, то предпринимается соответствующее действие для поддержания безопасности.

Примечание — Уровни передачи данных и средства передачи данных могут быть разных типов.

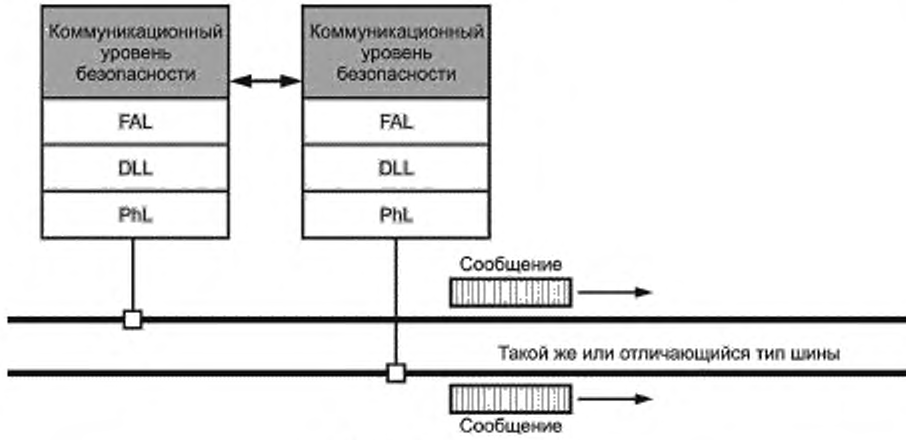


Рисунок А.2 — Модель B

А.4 Модель C

Модель C на рисунке А.3 описывает избыточный подход, подобный модели B. Данная модель использует только одно средство передачи данных.

Сообщения с обоих коммуникационных каналов безопасности проходят проверку безопасности и перекрестную проверку. Если перекрестная проверка показывает отклонение, то предпринимается соответствующее действие для поддержания безопасности.

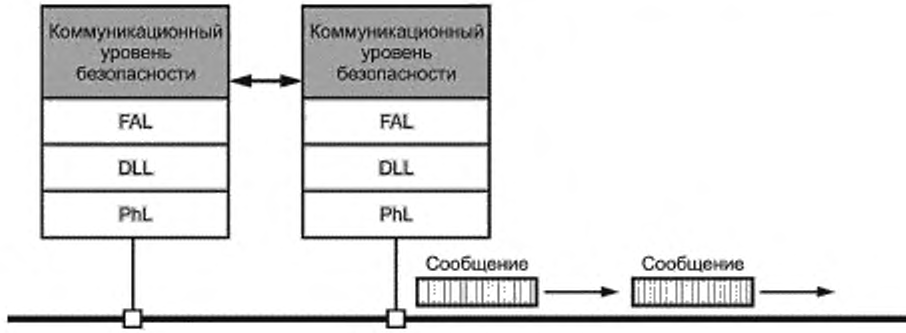


Рисунок А.3 — Модель C

А.5 Модель D

Модель D на рисунке А.4 представляет систему с двойным коммуникационным уровнем безопасности, в то время как уровни передачи данных существуют только в одном экземпляре. Оба коммуникационных уровня безопасности обращаются к уровням передачи независимо друг от друга. Безопасно передаваемые данные могут передаваться одним или двумя сообщениями.

Сообщения с обоих коммуникационных уровней безопасности проходят проверку безопасности и перекрестную проверку. Если перекрестная проверка показывает отклонение, то предпринимается соответствующее действие для поддержания безопасности.

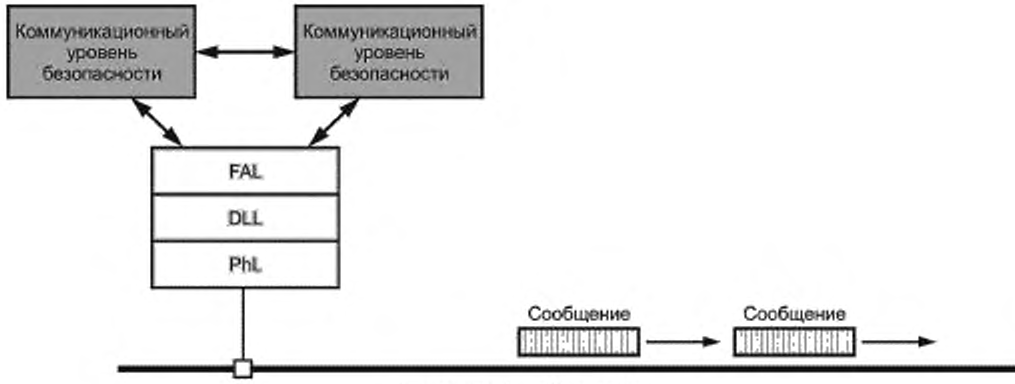


Рисунок А.4 — Модель D

Приложение В
(справочное)

Модель коммуникационного канала безопасности с проверкой ошибок, основанной на CRC

В.1 Обзор

Настоящее приложение описывает модель, созданную для сопоставления методов, которые уже применялись учреждениями, занимающимися оценкой.

Примечание — Рассмотренные в данном разделе аспекты не охватывают всех возможных отказов и ошибок системы передачи данных черного канала. Дополнительные требования приведены в МЭК 62280-1:2002, раздел 7.

В.2 Модель канала для вычислений

Модель, показанная на рисунке В.1, применяется для вычисления/оценки (на первом шаге) вероятности возникновения искаженных бит внутри коммуникационного уровня безопасности. Данный подраздел не затрагивает вопрос возникновения конкретных ошибок внутри черного канала.

Модель предполагает, что и черный канал, и коммуникационный уровень безопасности используют независимые механизмы обнаружения ошибок. Если механизм обнаружения ошибок черного канала не срабатывает, то для определения необходимой интенсивности возникновения остаточных ошибок должно быть достаточно механизма обнаружения ошибок коммуникационного уровня безопасности. Функционирующий в пределах черного канала механизм обнаружения ошибок отфильтровывает определенные виды битовых ошибок, поэтому механизм обнаружения ошибок коммуникационного уровня безопасности должен учитывать определенную модель этих ошибок. Следующие базовые формулы могут использоваться для упрощенной оценки интенсивностей остаточных ошибок или служить основной для других более сложных методов.



Рисунок В.1 — Коммуникационный канал с искажениями

Двоичный канал называется симметричным каналом, когда вероятности P искажения битового элемента в обоих направлениях равны: 1→0 и 0→1 (см. рисунок В.2). В дальнейшем полагается, что все битовые элементы имеют одинаковую вероятность возникновения битовой ошибки $P_e = P$.

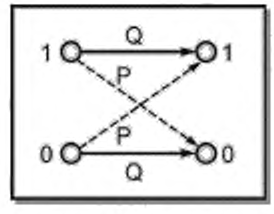


Рисунок В.2 — Двоичный симметричный канал (BSC)

Как правило, безопасно передаваемые данные передаются блоками определенной длины n. В таком случае вероятность возникновения ошибки для числа k искаженных бит (в блоке длиной n) может быть вычислена по формуле

$$P_n(k) = \binom{n}{k} \cdot P_e^k \cdot (1 - P_e)^{n-k}. \quad \text{(B.1)}$$

Если содержимое блока содержит фиктивный код для обнаружения видов ошибок до уровня $d - 1$, как это показано на рисунке B.4, с расстоянием Хемминга d, то верхний предел вероятности возникновения остаточных ошибок $R_{wc}(P_e)$ может быть вычислен по формуле

$$R_{UL}(P_e) = \sum_{k=d}^{n} \binom{n}{k} \cdot P_e^k \cdot (1 - P_e)^{n-k}. \quad \text{(B.2)}$$

Примечание — Подобное кодирование в реальности не используется, поэтому называется «фиктивным».

Тем не менее в этой упрощенной формуле не учитывается, что даже простой бит четности (расстояние Хемминга $d = 2$) позволяет обнаружить больше типов ошибок, чем просто в одном бите. При точном вычислении, если больше нет доступных методов или аппроксимаций, должна использоваться сумма всех индивидуальных не обнаруживаемых типов ошибок.

B.3 Проверка циклическим избыточным кодом

B.3.1 Общие положения

Интенсивность возникновения остаточных ошибок может быть рассчитана на основе метода обнаружения ошибок с применением механизма CRC для двоичного симметричного канала при помощи формулы (B.3) (вероятность возникновения остаточной ошибки для полиномов CRC).

$$R_{CRC}(P_e) = \sum_{i=0}^{n} A_i \cdot P_e^i \cdot (1 - P_e)^{n-i}, \quad \text{(B.3)}$$

где A_i — коэффициент распределения кода (определяемый либо компьютерной симуляцией, либо математическим анализом);

n — число бит в блоке, включая сигнатуру CRC;

P_e — вероятность битовой ошибки.

Анализ метода проверки циклическим избыточным кодом (CRC) показал, что для определенного класса так называемых образующих полиномов CRC в формуле для аппроксимации применим весовой коэффициент 2^{-r} [см. формулу (B.4), описывающую аппроксимацию вероятности возникновения остаточной ошибки для полиномов CRC].

$$R_{CRC}(P_e) \approx 2^{-r} \cdot \sum_{k=d_{min}}^{n} \binom{n}{k} \cdot P_e^k \cdot (1 - P_e)^{n-k}. \quad \text{(B.4)}$$

Функция (кривая) данной аппроксимации (см. формулу B.4) может дать меньшие (лучшие) значения вероятности возникновения остаточных ошибок, чем точные вычисления. Для высокой вероятности возникновения битовых ошибок (значение, близкое к 0,5) наихудшим значением будет 2^{-r}.

Значение r — это число бит CRC, добавленных к сообщению в качестве CRC сигнатуры для обнаружения ошибок, как это показано на рисунке B.3.

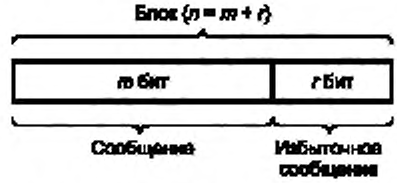


Рисунок B.3 — Пример блока, содержащего сообщение и биты CRC (избыточный код)

На рисунке B.4 представлен контекст для формул (B.2) и (B.4).

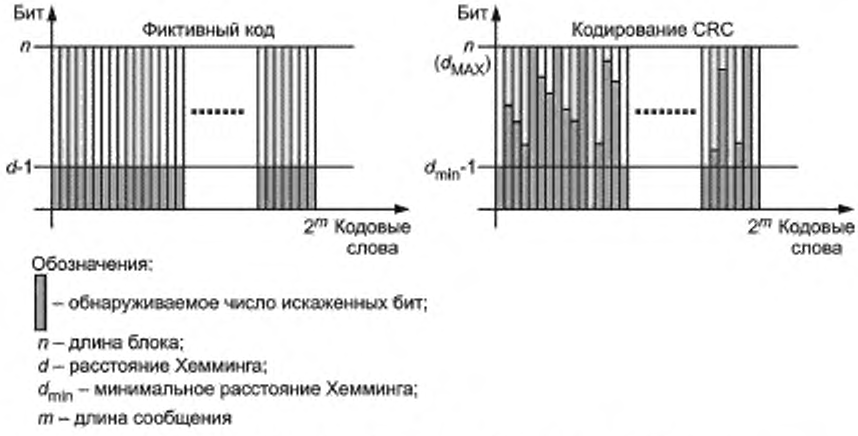


Рисунок В.4 — Коды блоков для обнаружения ошибок

Как правило, при помощи механизма CRC можно получить лучшую вероятность остаточной ошибки чем, если использовать блок меньшей длины n. Таким образом, для образующего полинома CRC существует зависимость между длиной блока n и минимальным расстоянием Хемминга d_{min} (см. таблицу В.1).

Таблица В.1 — Пример зависимости d_{min} и длины блока n

d_{min}	$d_{max} = n$
12	17
8	18...22
6	23...130
4	131...258
2	≥259

В.3.2 О полиномах CRC

Образующие полиномы CRC характеризуются кривой функции вероятности остаточной ошибки, монотонно растущей над кривой вероятности возникновения битовой ошибки. Рисунок В.5 иллюстрирует разницу между образующими и не образующими полиномами CRC. Настоятельно рекомендуется использовать только такие образующие многочлены CRC для упрощения процесса подтверждения достаточной интенсивности возникновения остаточных ошибок. Науке известно несколько методов вычисления подобных функций, например [30], [36] и [37]. Является полином образующим или нет, необходимо проверить для всех предполагаемых размеров блоков безопасности (см. таблицу В.1). Необразующие полиномы могут демонстрировать лучшую вероятность возникновения ошибки при высокой вероятности возникновения битовой ошибки (2^{-r}), чем при меньшей вероятности возникновения битовой ошибки ($> 2^{-r}$). При использовании необразующих полиномов CRC, следует использовать наихудшее значение вероятности возникновения остаточной ошибки ($> 2^{-r}$), в то время как для образующих полиномов при оценке вероятности возникновения остаточной ошибки достаточно значения 2^{-r}.

В некоторых случаях конкретная функция (кривая) выбранного образующего полинома CRC можно обеспечить меньшие (лучшие) значения вероятности возникновения остаточных ошибок вплоть до требующегося предела вероятности возникновения битовых ошибок, равного 10^{-2}. В таком случае настоятельно рекомендуется использовать наихудшие значения 2^{-r} или $>2^{-r}$ соответственно, так как только сообщения с ошибками старших бит (не равно распределенные битовые ошибки) могут достичь коммуникационного уровня безопасности.

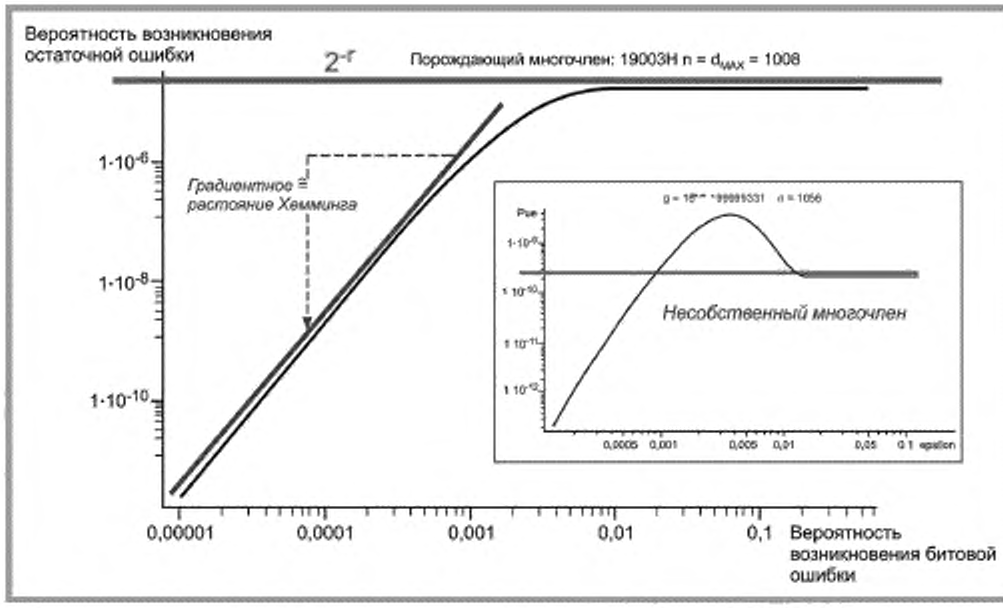


Рисунок В.5 — Образующие и не образующие полиномы CRC

Угол наклона является мерой минимального расстояния Хемминга образующего полинома CRC и размера блока.

Кодирование CRC предоставляет хорошую защиту от электромагнитных помех. Любая ошибка в линии передачи меньшая или равная в битах сигнатуре CRC будет обнаружена.

Приложение С
(справочное)

Структура стандартов, связанных с конкретными технологиями

Все связанные с конкретными технологиями части настоящего стандарта пронумерованы в соответствии с их CPF номером в МЭК 61784-1 или МЭК 61784-2.

Пример — Связанная с конкретной технологией часть стандарта, содержащая спецификации профилей коммуникации семейства CPF 33, удовлетворяющих требованиям функциональной безопасности, имеет номер МЭК 61784-3-33.

Все такие части обладают одной общей структурой для упрощения сравнения разных технологий. Данная структура представлена в таблице С.1.

Таблица С.1 — Общая структура частей стандартов, связанных с конкретной технологией

Номер раздела и подраздела	Заголовок	Содержание
	Введение	Введение одинаково для всех частей МЭК 61784-3
1	Область применения	Область применения стандартизирована для всех частей МЭК 61784-3
2	Нормативные ссылки	Нормативные документы, требующиеся для данной части
3	Термины, определения и сокращения	—
3.1	Термины и определения	—
3.1.1	Термины и определения	Общие термины, использующиеся в данной части
3.1.2	CPF X. Дополнительные термины и определения	Термины, связанные с конкретной технологией, использующиеся в данной части
3.2	Обозначения и сокращения	—
3.2.1	Сокращения	Сокращения, использующиеся в данной части
3.2.2	CPF X. Дополнительные обозначения и сокращения	Обозначения, связанные с конкретной технологией, использующиеся в данной части
3.3	Сокращения	Сокращения, использующиеся для описания разнообразных элементов коммуникационного уровня безопасности (например, таблицы состояний, диаграммы последовательностей)
4	Обзор профилей FSCP X/1 (Safetyname™)	Обзор профиля коммуникаций, удовлетворяющего требованиям функциональной безопасности, и соответствующий вводный материал (включая цели и мотивы, связанные с технологией)
5	Общие положения	—
5.1	Внешние документы, содержащие спецификации для профиля	Список ссылочных документов, требующихся для технологий, в частности те, которые не могут быть внесены в раздел 2 (т. к. они не являются официальными стандартами МЭК или ИСО, например документы консорциумов), поэтому были включены в библиографию вместе со всеми информационными документами
5.2	Требования функциональной безопасности	Может включать описания безопасных состояний (см. МЭК 61508-1:2010, подпункт 7.10.2.6)
5.3	Меры обеспечения безопасности	Может включать меры из 5.4, которые следует принять во внимание
5.4	Структура коммуникационного уровня безопасности	Может включать декомпозицию SCL

Продолжение таблицы С.1

Номер раздела и подраздела	Заголовок	Содержание
5.5	Связи с FAL (и DLL, PhL)	Может включать существующие диагностики, ожидаемые службы, ограничения (например «применять совместно с FSCP x/y»)
5.5.1	Типы данных	Список типов данных МЭК 61158, использующихся в данном профиле
6	Службы коммуникационного уровня безопасности	Может включать использующиеся прикладные объекты, службы диагностики
7	Протокол коммуникационного уровня безопасности	Первый подраздел описан ниже, последующие могут добавляться по мере необходимости. Может включать специальные временные механизмы, конечные автоматы, диаграммы последовательности, реакцию на включение/отключение питания, протокол диагностики и соответствующие диагностики
7.1	Формат PDU безопасности	Включает подробное определение форматов PDU (сообщения) безопасности. Будет включать в себя несколько подразделов для установления элементов формата (например, спецификации CRC безопасности)
8	Управление коммуникационным уровнем безопасности	Включает спецификации для следующих аспектов параметризации: - безопасных данных параметров, предоставленных другим устройством безопасности (например, сервером параметров); - безопасных данных параметров, предоставленных другим инструментом (например, описанием устройства). (При этом включаются любые необходимые меры, чтобы гарантировать хранение, обработку и передачу данных)
9	Системные требования	Первый подраздел описан ниже, последующие могут добавляться по мере необходимости
9.1	Индикаторы и сетевые коммутаторы	Спецификации индикаторов устройств, а также функции и поведения сетевого коммутатора
9.2	Руководство по установке	Подробные ссылки на раздел МЭК 61918 или других соответствующих документов
9.3	Время реакции функции безопасности	Вычисления и связанные с ними примеры времени реакции, связанные с конкретной технологией (например, худшее время реакции контура безопасности)
9.4	Длительность запросов	Спецификации длительности запросов в устройствах
9.5	Ограничения для вычисления системных характеристик	Включает повторные попытки в черном канале, число срочных блоков данных в секунду, число приемников сообщений
9.6	Сопровождение	Спецификации поведения системы в случае ремонта или замены устройства
9.7	Руководство по безопасности	Если необходимо, включает минимум информации, требующийся для включения профиля в руководство по безопасности
9.8	Каналы беспроводной передачи данных	Данный подраздел необязателен. Если необходимо, включает конкретные требования для беспроводной передачи данных
9.9	Классы соответствия	Данный подраздел необязателен. Если необходимо, включает дополнительные требования соответствия для базового протокола полевой шины

Окончание таблицы С.1

Номер раздела и подраздела	Заголовок	Содержание
10	Оценка	Включает информацию о требованиях к оценке
Приложение А (справочное)	Дополнительная информация о профиле коммуникаций, удовлетворяющем требованиям функциональной безопасности, семейства CPF X	Обязательное справочное приложение, предоставляющее дополнительную ненормативную информацию о протоколе. Если такая информация отсутствует, то в приложении должно быть следующее предложение: «Нет дополнительной информации для данного FSCP»
А.1	Вычисление Хэш-функции	Например, алгоритмы для вычисления CRC
Приложение В (справочное)	Информация для оценки профилей коммуникаций, удовлетворяющих требованиям функциональной безопасности, семейства CPF X	Обязательное справочное приложение, предоставляющее информацию о испытательных лабораториях, которые выполняют тестирование и подтверждение соответствия изделий FSCP X/1 стандарту МЭК 61784-3-X
Библиография		Библиографические ссылки для данной части

Приложение D
(справочное)

Руководство по оценке

D.1 Обзор

Данное руководство предназначено для оценки и испытания коммуникационных систем на соответствие задачам передачи сообщений, связанных с безопасностью. Обмен данными безопасности может осуществляться между различными блоками обработки системы обеспечения безопасности и/или между интеллектуальными датчиками/исполнительными устройствами безопасности и блоками обработки системы обеспечения безопасности.

Настоятельно рекомендуется использовать это руководство для оценки определенного коммуникационного профиля безопасности или коммуникационной системы безопасности так же, как и для устройств, связанных с безопасностью, использующих эти профили.

В документации, предоставленной для испытаний и оценки, должны быть установлены точные условия работы в соответствии с 5.8.2. Ни при каких условиях не допускаются отклонения от этих ограничений.

Если коммуникационная система безопасности является составной частью устройства, связанного с безопасностью, для которого существует стандарт на изделие (например, МЭК 61496-1 [5]), то это изделие и связанные с ним компоненты безопасной коммуникации должны соответствовать требованиям в той степени, в которой они определены в области применения соответствующего стандарта или в которой они определены в конкретном коммуникационном профиле безопасности в серии стандартов МЭК 61784-3.

D.2 Типы каналов

D.2.1 Общие положения

Данный подраздел определяет две общие концепции безопасной коммуникации, то есть методы черного и белого каналов. Данное руководство охватывает обе концепции безопасных коммуникаций.

D.2.2 Черный канал

В соответствии с определением 3.1.1.3 для типа безопасной коммуникации черный канал требуется только доказательство выполнения проектирования и подтверждения соответствия для его коммуникационного уровня безопасности (SCL) в соответствии с МЭК 61508. Проектировщик устройства безопасности может воспользоваться заранее оцененным и принятым компонентом аппаратных средств или программного обеспечения, который выполняет функции конкретного SCL. Если проектировщик реализует данный компонент так, как его предусмотрено реализовывать, то в соответствии с МЭК 61508 оценку соответствия безопасности для данного компонента можно опустить. Таким образом, все усилия могут ограничиваться оценкой, связанной с безопасностью технологии устройства и правильной ревлизацией компонента SCL.

Оценка соответствия. Проверка документации и реализации в системе, как было определено; подтверждение соответствия и верификация вычислений, предоставленных изготовителем; верификация параметров, необходимых для этих вычислений.

D.2.3 Белый канал

В соответствии с определением 3.1.1.44 для безопасной коммуникации требуется белый канал, чтобы все соответствующие компоненты аппаратных средств и программного обеспечения были спроектированы, реализованы и для них было выполнено подтверждение соответствия согласно МЭК 61508. В связи с большим количеством возможных решений данное руководство предоставляет помощь только для определенных аспектов обеспечения полноты данных. Дальнейшая информация приведена в МЭК 62280-1.

Как правило, индивидуальные методы белого канала могут быть оценены при помощи одной из моделей, описанных в приложении А.

D.3 Полнота данных для методов белого канала

D.3.1 Общие положения

Для анализа полноты данных можно идентифицировать два класса белого канала, описанных в D.3.2 и D.3.3 соответственно.

D.3.2 Модели B и C

В данном методе каждый канал системы коммуникационных шин не предполагается безопасным. Уровни протоколов избыточны и отправляются два сообщения. Таким образом, меры обеспечения полноты данных системы коммуникационных шин используются в полной мере. Достаточное обнаружение ошибок не возможно в случае, если один из каналов отказывает. Вследствие их архитектуры некоторые известные системы коммуникационных шин дают возможность другим участникам сети проверять каждое сообщение и за счет только этого могут обнаружить большинство возможностей возникновения ошибок.

Примечания

1 Модели B и C могут быть реализованы, как решения для белого, так и для черного каналов.

2 Формулы данного подраздела могут также применяться для систем черного канала.

Следующий метод основан на концепции «избыточности с перекрестной проверкой», описанной в 5.4.8. Это означает, что в случае двукратной передачи безопасного сообщения и побитового сравнения в приемнике сообщения, предпосылкой необнаруженной ошибки будет то, что оба сообщения одинаково искажены. При помощи модели BSC, вероятность остаточной ошибки может быть вычислена по принципам, описанным в приложении B. Вероятность определенной комбинации битовых ошибок в каждом сообщении в данном случае такая же, поэтому выражение возводится в квадрат. Возможности возникновения комбинаций битовых ошибок соответствуют вероятностям возникновения этих ошибок в одиночном сообщении (биноминальные коэффициенты).

Примечание — Протоколы FSCP должны настроить индивидуальные меры таким образом, чтобы был достигнут максимум независимости. В противном случае необходимо использовать более сложные формулы, учитывающие зависимость.

Если предполагается осуществлять обеспечение полноты данных при помощи сигнатуры CRC, то считается эффективным тот же коэффициент 2^{-r} (см. приложение B), а при помощи формулы (D.1) можно получить оценку вероятности возникновения остаточной ошибки.

$$R_{\mathrm{EMC}}(P_e) \approx 2^{-r} \cdot \sum_{k=d_{\min}}^{n} \left(\begin{matrix} n \\ k \end{matrix}\right) \cdot \left(P_e^k \cdot (1-P_e)^{n-k}\right)^2. \qquad \text{(D.1)}$$

Примечание — Данная формула применима только для образующих полиномов (см. B.3.2).

Для полной оценки вероятности возникновения остаточных ошибок для белого канала требуется анализ, проведенный в соответствии с D.3.3, а также расчет по формуле (D.2). МЭК 62280-1 следует учитывать настолько, насколько настоящий стандарт применим.

Вычисление $\Lambda_{\mathrm{SL}}(P_e)$ осуществляется по правилам, описанным в 5.6.1 [формула (1)].

Полная оценка соответствия требованиям безопасности должна быть выполнена в соответствии с МЭК 61508 (например, учитывая и используя анализ видов и последствий отказов, долю безопасных отказов, ошибки по общим причинам).

Оценка соответствия. Проверка документации и реализации в системе, как было специфицировано; подтверждение соответствия и верификация вычислений, предоставленных изготовителем; верификация параметров, необходимых для этих вычислений.

D.3.3 Модели A и D

Для достижения требующегося УПБ данный метод основан на мерах обнаружения ошибок в существующих каналах передачи данных на шинах и дополняет их мерами, реализующимися в добавленном сверху коммуникационном уровне безопасности.

В данном методе в связи с угрозой безопасности из-за отказов в схемах протокола шины необходимо учитывать отказоустойчивость аппаратных средств и, таким образом, ожидаемый их срок службы.

В данном случае анализ Маркова может быть обусловлен тремя фундаментальными возможными проблемами передачи данных (см. рисунок D.1) в соответствии с МЭК 62280-1:

- не обнаруживаемые сбои сообщений в результате отказа аппаратных средств на уровнях передачи данных, которые приводят к распространению искаженных сообщений (R_{HW});
- сбои в сообщениях с не обнаруживаемыми битовыми ошибками, вызванными электромагнитными помехами (ЭМП), которые происходят в процессе нормальной работы (R_{EMC});
- не обнаруживаемые сбои сообщений в результате отказов в соответствующей части, проверяемой шины в канале передачи данных (R_{TC}).

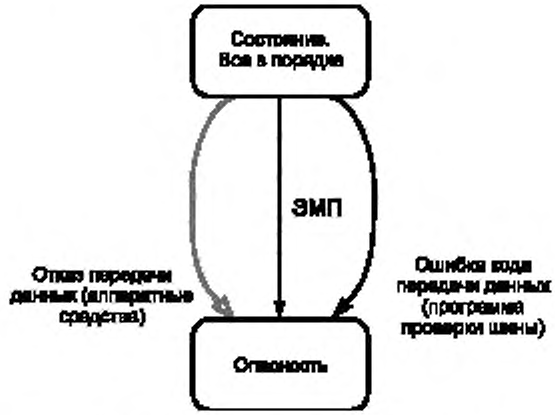


Рисунок D.1 — Базовая модель Маркова

Вероятность возникновения остаточных ошибок R_{AD} в системе определяется суммой индивидуальных вероятностей [формула (D.2)]. Вычисление $\Lambda_{SL}(P_e)$ выполняется в соответствии с 5.6.1, зная значение вероятности возникновения остаточных ошибок:

$$R_{AD} = R_{HW} + R_{EMC} + R_{TC}. \quad (D.2)$$

Полная оценка соответствия требованиям безопасности должна быть выполнена в соответствии с МЭК 61508 (например, учитывая и используя анализ видов и последствий отказов, долю безопасных отказов, ошибки по общим причинам). МЭК 62280-1 должен быть рассмотрен там, где он применим.

Оценка соответствия. Проверка документации и реализации в системе, как было специфицировано; подтверждение соответствия и верификация вычислений, предоставленных изготовителем; верификация параметров, необходимых для этих вычислений.

D.4 Верификация мер безопасности

D.4.1 Общие положения

Данная часть руководства по оценке устанавливает требования для верификации определенного коммуникационного профиля безопасности.

D.4.2 Реализация

Для безопасной передачи сообщений необходимо, чтобы сообщения генерировались безопасным образом (в соответствии с требующимся УПБ). Средство передачи (например, линия шины, включая интерфейс ASIC) само по себе не считается безопасным. Ответственность за меры обеспечения безопасности всецело возлагается на блоки обработки источника и приемника сообщений. Это касается решений черного и белого каналов.

Оценка соответствия. Требования МЭК 61508 или дополнительных стандартов, таких как МЭК 61784-3 должны быть учтены и проверены. Эти требования выходят за рамки области применения данного руководства по оценке и определены нормативно.

D.4.3 Принцип «срабатывание защиты при отключении питания»

Механизм временного ожидания (например, сторожевой таймер) должен применяться во всех случаях.

Оценка соответствия. См. 5.4.4.

D.4.4 Безопасное состояние

В приемнике должен быть установлен механизм обнаружения ошибок и реакции на их возникновение, на котором лежит ответственность за обеспечение связанных с безопасностью действий по достижению безопасного состояния в течение времени невосприимчивости к сбоям.

Оценка соответствия. Проверка документации и реализации; измерение времени реакции устройства безопасности, использующего безопасную передачу данных, при работе системы в наихудших условиях (например, в присутствии ошибок или отказов).

D.4.5 Ошибки передачи данных

Если возникают ошибки, описанные в 5.3, то должна инициироваться определенная реакция на сбой (например, запрос остановки работы).

Оценка соответствия. Проверка документации, реализации и вычислений, если необходимо, а также функциональный тест; расширенные функциональные тесты по принципам, описанным в МЭК 61508.

D.4.6 Время безопасности реакции и время безопасности отклика

Максимальное время реакции функции безопасности, установленное изготовителем, и время, требующееся для завершения связанного с безопасностью действия, не должны быть превышены даже при наличии ошибок и отказов.

Примечание — В некоторых системах шин, интенсивность передачи данных и реакция или отклик зависят от числа участников передачи данных. Если интенсивность передачи данных и реакция или отклик связаны с безопасностью, то может потребоваться снижение числа участников.

Оценка соответствия. Проверка документации и реализации; измерение времени реакции и/или отклика при работе определенной системы в наихудших условиях. Изготовитель или коммуникационный профиль безопасности должны предоставлять определения числа и распределения во времени ошибок, которые необходимо учесть.

D.4.7 Комбинация мер

Для передачи связанных с безопасностью сообщений через системы шин должна быть применена комбинация мер, собранная из мер, приведенных в 5.4, таким образом, чтобы каждая ошибка, описанная в 5.3, была обнаружена в течение времени невосприимчивости к сбоям. Таблица 1 помогает в выборе индивидуальных мер.

Оценка соответствия. Все используемые технические меры должны быть верифицированы на полноту в соответствии с таблицей 1. Реализация мер должна осуществляться в соответствии с требующимся УПБ.

D.4.8 Отсутствие помех

Должно быть доказано, что участники коммуникации, не относящиеся к безопасности, не мешают участникам, связанным с безопасностью.

Оценка соответствия. Проверка документации и реализации должна включать конкретные функциональные тесты, в том числе тесты, например, учитывающие при симуляции персональный компьютер (PC), такие как тестирование нагрузки линий связи или проверка смены адресов при изменении входных данных.

D.4.9 Дополнительные причины сбоев (белый канал)

В дополнение к уже описанным методам, использующим модель BSC для оценки вероятности остаточных ошибок, необходимо учитывать и управлять другими причинами сбоев. Подробности приведены в МЭК 62280-1 или [29].

Оценка соответствия. Все применяющиеся технические меры должны быть проверены на соответствие требованиям, описанным в МЭК 62280-1.

D.4.10 Эталонные испытательные стенды и условия эксплуатации

Все части коммуникационной системы безопасности должны испытываться вместе настолько, насколько это представляется возможным. В противном случае части коммуникационной системы безопасности проходят испытания по отдельности. Во втором случае, эталонные системы (испытательные стенды) и/или симуляторы должны быть созданы для определенного коммуникационного профиля безопасности и реализованы при помощи определенного набора разных устройств, полученных по возможности от разных поставщиков.

Испытательный стенд должен реализовывать наихудшие условия, например, по длине соединения или числу устройств. Сигналы, требующиеся для функции безопасности, должны моделироваться или формироваться другим способом.

Соответствующие режимы работы, такие как циклический обмен данными значений процесса или ациклический обмен данными параметризации, должны быть определены для использования во время испытаний.

Оценка соответствия. Испытание и проверки в соответствии с определениями проверяемого протокола FSCP или спецификациями изготовителя испытуемого оборудования (EUT).

D.4.11 Тестер соответствия параметрам

Соответствие определенному протоколу FSCP должно проверяться тестером соответствия профиля, определенным и предусмотренным отдельным протоколом FSCP.

Примечание — Тестирование на соответствие включает в себя как позитивные, так и негативные тесты.

Оценка соответствия. Испытание и проверки в соответствии с определениями проверяемого протокола FSCP.

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
МЭК 61131-2	IDT	ГОСТ IEC 61131-2—2012 «Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания»
МЭК 61158 (все части)	—	*
МЭК 61326-3-1	—	*
МЭК 61326-3-2	—	*
МЭК 61508 (все части)	IDT	ГОСТ Р МЭК 61508—2012 «Функциональная безопасность систем электрических/ электронных/программируемых электронных, связанных с безопасностью. Части 1—7»
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических/ электронных/программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-2	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических/ электронных/ программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61784-1	—	*
МЭК 61784-2	—	*
МЭК 61784-3-1	—	*
МЭК 61784-3-2	—	*
МЭК 61784-3-3	—	*
МЭК 61784-3-6	—	*
МЭК 61784-3-8	—	*
МЭК 61784-3-12	—	*
МЭК 61784-3-13	—	*
МЭК 61784-3-14	—	*
МЭК 61784-5 (все части)	—	*
МЭК 61918	—	*
МЭК 62280-1:2002	—	*
МЭК 62443 (все части)	—	*

* Соответствующий национальный стандарт отсутствует.

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

- IDT — идентичные стандарты.

Библиография

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

Примечание — См. также IEC Multilingual Dictionary — Electricity, Electronics and Telecommunications (на CD-ROM and at <gost.e-ecolog.ru >)

[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 61496 (all parts), Safety of machinery — Electro-sensitive protective equipment
[6] IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations
[7] IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels
[8] EC 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
[9] IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector
[10] IEC 61784-4, Industrial communication networks — Profiles — Part 4: Secure communications for fieldbuses
[11] IEC 61800-5-2, Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional
[12] IEC/TR 62059-11, Electricity metering equipment — Dependability — Part 11: General concepts
[13] IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems
[14] IEC/TR 62210, Power system control and associated communications — Data and communication security
[15] IEC 62280-2, Railway applications — Communication, signalling and processing systems — Part 2: Safety-related communication in open transmission systems
[16] ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards
[17] ISO/IEC 2382-14, Information technology — Vocabulary — Part 14: Reliability, maintainability and availability
[18] ISO/IEC 2382-16, Information technology — Vocabulary — Part 16: Information theory
[19] ISO/IEC 7498 (all parts), Information technology — Open Systems Interconnection — Basic Reference Model
[20] ISO 10218-1, Robots for industrial environments — Safety requirements — Part 1: Robot
[21] ISO 12100-1, Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology
[22] ISO 13849-1, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
[23] ISO 13849-2, Safety of machinery — Safety-related parts of control systems — Part 2: Validation
[24] ISO 14121, Safety of machinery — Principles of risk assessment
[25] EN 954-1:1996, Safety of machinery — Safety related parts of control systems — General principles for design
[26] ANSI/ISA-84.00.01-2004 (all parts), Functional Safety: Safety Instrumented Systems for the Process Industry Sector
[27] VDI/VDE 2180 (all parts), Safeguarding of industrial process plants by means of process control engineering
[28] GS-ET-26, Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten, May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("Principles for Test and Certification of Bus Systems for Safety relevant Communication")
[29] ANDREW S. TANENBAUM, Computer Networks, 4th Edition, Prentice Hall, N.J., ISBN-10:0130661023, ISBN-13: 978-0130661029
[30] W. WESLEY PETERSON, Error-Correcting Codes, 2nd Edition 1981, MIT-Press, ISBN 0-262-16-039-0
[31] BRUCE P. DOUGLASS, Doing Hard Time, 1999, Addison-Wesley, ISBN 0-201-49837-5
[32] 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
[33] DIETER CONRADS, Datenkommunikation, 3rd Edition 1996, Vieweg, ISBN 3-528-245891
[34] German IEC subgroup DKE AK 767.0.4: EMC and Functional Safety, Spring 2002
[35] NFPA79 (2002), Electrical Standard for Industrial Machinery
[36] GUY E. CASTAGNOLI, On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland
[37] 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
[38] 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
[39] 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

УДК 004:61:006.354 ОКС 35.200 П85

Ключевые слова: промышленные сети, профили, полевые шины, функциональная безопасность, общие правила, определения профилей

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 23.05.2016. Подписано в печать 02.06.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,60. Тираж 33 экз. Зак. 1396.

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

gost.e-ecolog.ru