ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61784-3-3— 2016

Промышленные сети

ПРОФИЛИ

Часть 3-3

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 3

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

Издание официальное

Москва
Стандартинформ
2017

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2016 г. № 1884-ст

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

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном 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 (www.gost.ru)

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины, определения, сокращения и условные обозначения ... 3
3.1 Термины и определения ... 3
3.2 Обозначения и сокращения ... 9
3.3 Условные обозначения ... 11
4 Обзор FSCP 3/1 (PROFIsafe™) ... 11
5 Общие положения ... 14
5.1 Внешние документы, предоставляющие спецификации для профиля ... 14
5.2 Функциональные требования безопасности ... 14
5.3 Меры безопасности ... 14
5.4 Структура коммуникационного уровня безопасности ... 15
5.5 Связи с FAL (и DLL, PhL) ... 19
6 Услуги коммуникационного уровня безопасности ... 23
6.1 Услуги F-хоста ... 23
6.2 Услуги F-устройств ... 26
6.3 Диагностика ... 27
7 Протокол коммуникационного уровня безопасности ... 28
7.1 Формат PDU безопасности ... 28
7.2 Поведение FSCP 3/1 ... 34
7.3 Реакция в случае неисправности ... 53
7.4 Запуск и координация изменений ... 55
8 Управление коммуникационным уровнем безопасности ... 56
8.1 F-Параметр ... 56
8.2 iПараметр и iPar_CRC ... 62
8.3 Параметризация безопасности ... 63
8.4 Конфигурация безопасности ... 67
8.5 Использование информации типов данных ... 70
8.6 Механизмы назначения параметров безопасности ... 73
9 Системные требования ... 86
9.1 Индикаторы и коммутаторы ... 86
9.2 Руководство по установке ... 86
9.3 Время реакции функции безопасности ... 86
9.4 Длительность запросов на обслуживание ... 93
9.5 Ограничения для вычисления системных характеристик ... 93
9.6 Техническое обслуживание ... 96
9.7 Руководство по безопасности ... 97
9.8 Беспроводные каналы передачи данных ... 98
9.9 Классы соответствия ... 101

10 Оценка 102
10.1 Политика безопасности 102
10.2 Обязательства 102
Приложение А (справочное) Дополнительная информация для профиля коммуникаций функциональной безопасности CPF 3 103
Приложение В (справочное) Информация для оценки профилей коммуникаций функциональной безопасности CPF 3 108
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам 109
Библиография 111

Введение

1 Общие положения

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

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

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

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

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

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

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

Настоящий стандарт описывает:

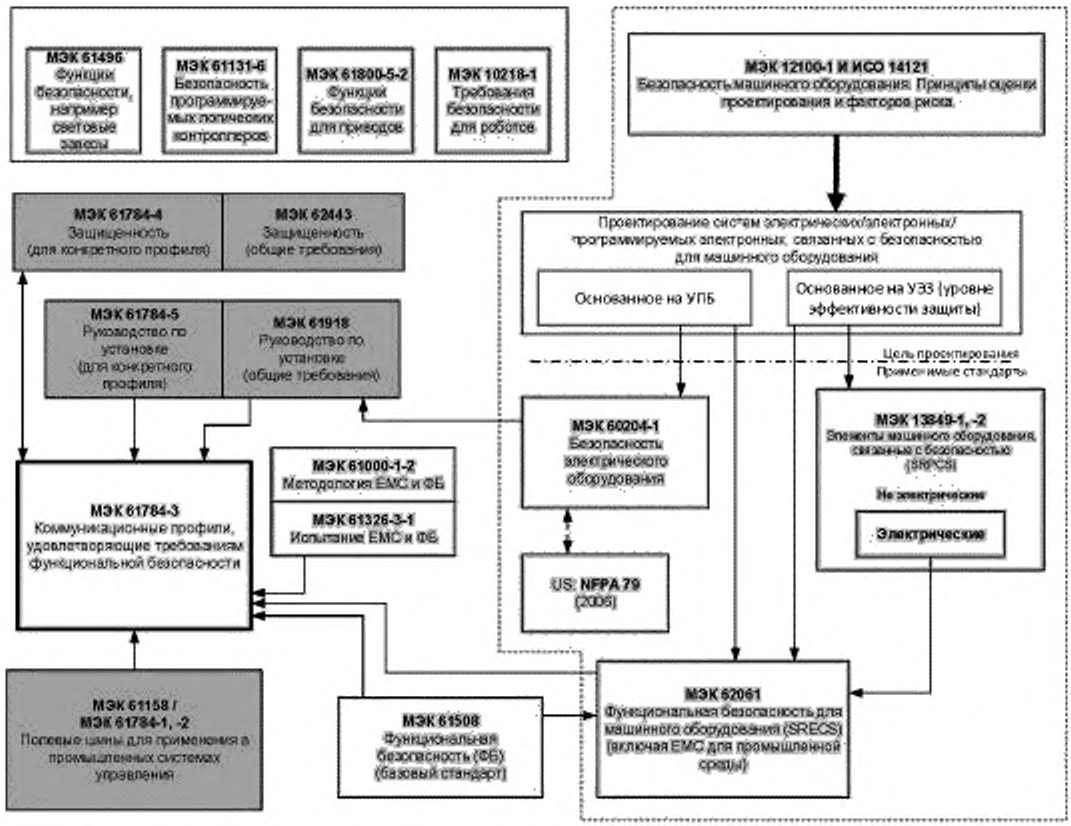
- основные принципы реализации требований комплекса стандартов МЭК 61508 для связанной с безопасностью передачи данных, включая возможные сбои при передаче данных, меры по устранению неисправностей и факторы, влияющие на полноту данных;
- индивидуальные описания профилей, удовлетворяющих требованиям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

2 Патентная декларация

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

EP1267270-A2	[SI]	Метод для передачи данных
WO00/045562-A1	[SI]	Метод и устройство для определения надежности переносчиков данных
WO99/049373-A1	[SI]	Укороченное сообщение с данными системы автоматизации
EP1686732	[SI]	Метод и система для передачи блоков данных протокола
EP1802019	[SI]	Идентификация ошибок в передаче данных
EP1921525-A1	[SI]	Метод для эксплуатации системы, связанной с безопасностью

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



Обозначения:

(желтый) - стандарты, связанные с безопасностью;

(голубой) - стандарты, связанные с полевыми шинами,

(блодно 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 эффективности защиты (Категорией) и УПБ.

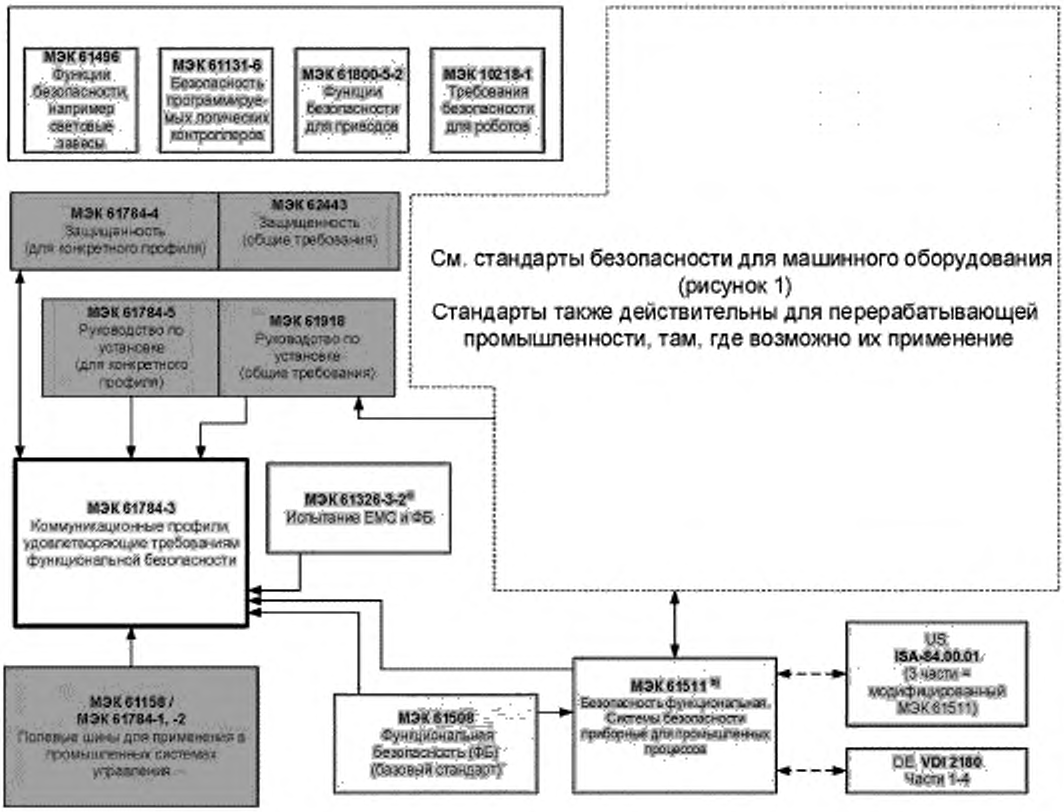
Рисунок 1 — Связь МЭК 61158-3 с другими стандартами (машинное оборудование)

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.

Информация доступна по средством:

[SI] Siemens AG
I IA AS FA TC
76187 Karlsruhe
GERMANY

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



Обозначения:

(желтый) - стандарты, связанные с безопасностью;

(голубой) - стандарты, связанные с полевыми шинами;

(Бледно желтый) - настоящий стандарт

[a] Для установленных электромагнитных сред, в противном случае МЭК 61326-3-1.
[b] Ратифицирован EN

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Промышленные сети

ПРОФИЛИ

Часть 3-3

Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 3

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

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт описывает коммуникационный уровень безопасности (услуги и протокол) на основе CPF 3, представленного в МЭК 61784-1, МЭК 61784-2 (CP 3/1, CP 3/2, CP 3/4, CP 3/5 и CP 3/6) и МЭК 61158, Типы 3 и 10. Настоящий стандарт идентифицирует принципы для осуществления коммуникаций, удовлетворяющих требованиям функциональной безопасности, определенным в МЭК 61784-3 и имеющим важное значение для данного коммуникационного уровня безопасности.

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

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

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

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

2 Нормативные ссылки

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

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

IEC 61000-6-2, Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments (Электромагнитная совместимость (ЭМС) Часть 6-2. Общие стандарты. Помехоустойчивость для промышленных обстановок)

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

Издание официальное

IEC 61010-1, Safety requirements for electrical equipment for measurement, control, and laboratory use Part 1: General requirements (Требования безопасности для электрооборудования, предназначенного для измерения, управления и лабораторного применения. Часть 1. Общие требования)

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

IEC 61131-3, Programmable controllers — Part 3: Programming languages (Программируемые контроллеры. Часть 3. Языки программирования)

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

IEC 61158-3-1, Industrial communication networks — Fieldbus specifications — Part 3-3: Datalink layer service definition — Type 3 elements (Промышленные сети связи. Спецификации полевых шин. Часть 3-1: Определение сервиса канального уровня. Элементы типа 1)

IEC 61158-4-3, Industrial communication networks — Fieldbus specifications — Part 4-3: Datalink layer protocol specification — Type 3 elements (Промышленные сети связи. Спецификации полевых шин. Часть 4-3: Спецификация протокола канального уровня. Элементы типа 3)

IEC 61158-5-5, Industrial communication networks — Fieldbus specifications — Part 5-5: Application layer service definition — Type 5 elements (Промышленные сети связи. Спецификации полевых шин. Часть 5-3: Определение сервиса прикладного уровня. Элементы типа 3)

IEC 61158-5-9, Industrial communication networks — Fieldbus specifications — Part 5-9: Application layer service definition — Type 10 elements (Промышленные сети связи. Спецификации полевых шин. Часть 5-10: Определение сервиса прикладного уровня. Элементы типа 10)

IEC 61158-6-5, Industrial communication networks — Fieldbus specifications — Part 6-5: Application layer protocol specification — Type 3 elements (Промышленные сети связи. Спецификации полевых шин. Часть 6-3: Спецификация протокола прикладного уровня. Элементы типа 3)

IEC 61158-6-10, Industrial communication networks — Fieldbus specifications — Part 6-10: Application layer protocol specification — Type 10 elements (Промышленные сети связи. Спецификации полевых шин. Часть 6-10: Спецификация протокола прикладного уровня. Элементы типа 10)

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

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

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

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

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

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

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

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

IEC 61784-5-3, Industrial communication networks — Profiles — Part 5: Installation of fieldbuses — Installation profiles for CPF 3 (Промышленные сети. Профили. Часть 5. Установка полевых шин. Профили установки для CPF 3)

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

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

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

IEC 62280-2, Railway applications — Communication, signalling and processing systems — Part 2: Safety-related communication in open transmission systems (Железнодорожные приложения. Системы связи, сигнализации и обработки данных. Часть 2. Коммуникации, связанные с безопасностью в открытых системах передачи данных)

IEC/TR 62390, Common automation device — Profile guideline (Обыкновенное автоматическое устройство. Руководящие принципы профиля)

ISO 13849-1, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность оборудования. Части систем управления, связанные с безопасностью. Часть 1. Общие принципы проектирования)

ISO 13849-2, Safety of machinery — Safety-related parts of control systems — Part 2: Validation (Безопасность оборудования. Части систем управления, связанные с безопасностью. Часть 2. Подтверждение соответствия)

ISO 15745-3, Industrial automation systems and integration — Open systems application integration framework — Part 3: Reference description for IEC 61158-based control systems (Промышленные системы автоматизации и интеграция. Прикладная интеграционная среда открытых систем. Часть 3. Эталонное описание систем управления на основе стандарта МЭК 61158)

ISO 15745-4, Industrial automation systems and integration — Open systems application integration framework — Part 4: Reference description for Ethernet-based control systems (Промышленные системы автоматизации и интеграция. Прикладная интеграционная среда открытых систем. Часть 4. Эталонное описание систем управления на основе стандарта Ethernet)

3 Термины, определения, сокращения и условные обозначения

3.1 Термины и определения

В настоящем стандарте используются следующие термины и определения:

3.1.1 Термины и определения

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

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

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

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

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

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

Примечания

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

2 См. также [32], [33].

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

[МЭК 61508-4:2010], [МЭК 61158]

Примечания

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

2 Ошибки не обязательно являются причиной отказов или сбоев.

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

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

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

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

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

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

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

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

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

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

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

Примечания

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

2 См. также [32], [33].

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

Примечания

1 Хеш-функции могут применяться для обнаружения искажений данных.

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

[МЭК/TR 62210, модифицировано]

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

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

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

[ИСО/МЭК 2382-16.02.01, модифицировано]

3.1.1.18 **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.

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

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

[МЭК 61508-4 и МЭК 62061, модифицировано]

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

[ИСО 13849-1]

3.1.1.21 **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]

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

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

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

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

Примечания

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

2 Понятие «надежности» также 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, модифицировано]

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

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

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

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

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

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

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

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

3.1.1.29 **безопасное сверхнизкое напряжение** (safety extra-low-voltage, SELV)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]

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

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

[МЭК 61508-4:2010, модифицировано]

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

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

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

Примечания

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

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

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

[МЭК 61508-4:2010]

3.1.1.33 **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 рассмотрена в МЭК 61784-3:2010, 5.3 и 5.4.

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

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

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

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

3.1.2 CPF 3. Дополнительные термины и определения

3.1.2.1 **бит** (bit): Закодированная двоичная информация без технического модуля.

3.1.2.2 **кодовое имя** (codename): Уникальная идентификация одноранговых коммуникаций безопасности.

3.1.2.3 **конфигурация** (configuration): Определение стандартных коммуникационных соединений и параметров коммуникаций для объектов шины определенного приложения.

Примечание — Конфигурация для коммуникации безопасности включает в себя определение соединений безопасности и F-параметров для объектов шины, связанной с безопасностью, предназначенной для определенного приложения, связанного с безопасностью.

3.1.2.4 **порядковый номер** (consecutive number): Средство для обеспечения завершенности и поддержания правильного порядка передаваемых PDU безопасности.

Примечания

1 Экземпляр порядкового номера описан в МЭК 61784-3.

2 Порядковый номер может передаваться с каждым PDU безопасности (режим-V1) или же защищен только передаваемой сигнатурой CRC (режим-V2).

3.1.2.5 **инструмент-CPD** (CPD-Tool): Специальная программа в обслуживающих компьютерах, соединенная с полевой шиной для целей конфигурирования, параметризации и диагностики определенных полевых устройств.

3.1.2.6 **цикл** (cycle): Интервал, за который повторно и непрерывно выполняется набор команд или действие.

3.1.2.7 **точка доступа к устройству** [device access point (DAP)]: Элемент, использующийся для обращения к модулю ввода-вывода (IO) устройства, как к объекту.

Примечание — Как правило, именуется головной станцией.

3.1.2.8 **время подтверждения устройства,** ВПУ [device acknowledgement time (DAT)]: Затраченное время F-устройства, начиная с принятия в точке доступа к устройству PDU безопасности, включающего новый порядковый номер, и заканчивая генерацией надлежащего ответного PDU безопасности и его возвращением в точку доступа к устройству.

3.1.2.9 **драйвер** (driver): Программный модуль, применяющийся для абстрагирования аппаратных средств от оставшегося прикладного программного обеспечения.

3.1.2.10 **отказоустойчивость,** F [fail-safe (F)]: Способность системы, которая посредством адекватных технических или организационных мер предотвращает опасные ситуации либо детерминировано, либо снижая их риск до допустимого значения.

3.1.2.11 **отказоустойчивые значения,** FV [fail-safe values (FV)]: Значения, которые выдаются вместо значений процесса, когда функция безопасности установлена в отказоустойчивом состоянии.

Примечание — В настоящем стандарте значения отказоустойчивости (FV) должны всегда быть установлены в «0».

3.1.2.12 **отказоустойчивое состояние** (fail-safe state): Режим работы функции безопасности или оконечного элемента (исполнительного устройства), который посредством адекватных технических мер предотвращает опасности либо детерминировано, либо снижая риск до допустимого значения.

Примечание — В зависимости от определенной функции безопасности, отключение питания может быть не единственной возможностью для состояния отказоустойчивости.

3.1.2.13 **F-устройство** (F-Device): Пассивный одноранговый узел коммуникаций CP 3/RTE, способный выполнять протокол FSCP 3/1 и, как правило, вызываемый F-хостом для обмена данными.

3.1.2.14 **F-драйвер** (F-Driver): Программное обеспечение, администрирующее PDU безопасности в F-хостах и F-устройствах в соответствии с спецификациями FSCP 3/1.

3.1.2.15 **F-хост** (F-Host): Блок обработки данных, способный выполнять протокол FSCP 3/1 и обслуживать черный канал.

Примечание — Как правило, это PLC или IPC с адекватной операционной системой.

3.1.2.16 **F-модуль** (F-Module): Пассивный однаранговый узел коммуникаций в модульном F-устройстве или F-ведомом устройстве, способный выполнять протокол FSCP 3/1, обычно вызываемый F-хостом для обмена данными.

Примечание — Как правило, это модуль ввода или вывода, связанный с безопасностью.

3.1.2.17 **F-ведомый** (F-Slave): Пассивный одноранговый узел коммуникаций CP 3/1 или CP 3/2, способный выполнять протокол FSCP 3/1, как правило, вызываемый F-хостом для обмена данными.

3.1.2.18 **реакция на сбой** (fault reaction): Индикация коммуникационной неисправности посредством установки битов сбоя в байте статуса и соответствующей автоматической безопасной реакции в этих компонентах.

Примечание — Как правило, это модуль ввода или вывода, связанный с безопасностью.

В F-выводе:	Закрытие выводов и/или автоматическая безопасная реакция блока исполнительного устройства.
В F-CPU:	Возможна соответствующая реакция пользовательской программы. В F-I/O-данные должны быть установлены значения отказоустойчивости.
В F-вводе:	В случае коммуникационных сбоев, обнаруженных на F-вводе, в байте статуса устанавливаются биты сбоя.

3.1.2.19 **функциональный блок,** ФБ [function block (FB)]: Независимая часть программы, обладающая определенным функционалом.

3.1.2.20 **время подтверждения хоста** [host acknowledgement time (HAT)]: Затраченное время F-хоста, от принятия PDU безопасности, включающего определенный порядковый номер и до генерации надлежащего ответного PDU безопасности, включающего увеличенный порядковый номер, и его возвращения ведущему устройству/контроллеру ввода-вывода.

3.1.2.21 **контроллер ввода-вывода,** IO-контроллер (IO-Controller): Активный объект коммуникаций, способный инициализировать и планировать коммуникационную деятельность CP 3/RTE других объектов, которые могут быть IO-контроллерами или IO-устройствами.

Примечание — В рамках CP 3/1 эта задача соответствует классу 1 ведущего устройства.

3.1.2.22 **устройство ввода-вывода,** IO-устройство (IO-Device): Пассивный объект коммуникаций, способный принимать сообщения и отправлять их в ответ другому объекту коммуникаций CP 3/RTE, который может быть IO-контроллером или IO-устройством.

Примечание — В рамках CP 3/1 данная задача соответствует ведомому устройству.

3.1.2.23 **модуль ввода-вывода,** IO-модуль (IO-Module): Подблок ввода-вывода, имеющий доступный адрес и находящийся в IO-устройстве.

3.1.2.24 **диспетчер ввода-вывода,** IO-диспетчер (IO-Supervisor): Техническая станция, включенная для считывания и записи данных с и в IO-устройство.

Примечание — Диспетчер ввода-вывода используется для ввода в эксплуатацию или диагностики. В отличие от контроллера ввода-вывода он не берет на себя активную роль в процессе работы IO-системы. IO-диспетчер не является частью IO-системы.

3.1.2.25 **система ввода-вывода, IO-система** (IO-System): IO-контроллер и связанные с ним IO-устройства.

3.1.2.26 **iпараметр** (iParameter): Индивидуальные или зависящие от технологии параметры F-устройства.

Примечание — Типичными iпараметрами являются координаты зоны защиты лазерного сканнера.

3.1.2.27 **iпар-сервер** (iPar-Server): Стандартизированный механизм для хранения и извлечения индивидуальных или зависящих от технологии параметров F-устройства в рамках стандартной части F-хоста или управляемой им подсистемы.

3.1.2.28 **ведущее устройство, класс 1** [master (class 1)]: Активный одноранговый узел коммуникаций CP 3/1, инициирующий ведомые устройства для обмена данными.

3.1.2.29 **значения процесса,** ЗП [process values (PV)]: Входные и выходные данные (в PDU безопасности), которые требуются для управления автоматизированным процессом.

3.1.2.30 **квалификатор** (qualifier): Дополнительные указательные биты в *значениях процесса*, демонстрирующие статус каждого индивидуального ввода.

3.1.2.31 **общий ввод-вывод,** общий I/O (shared I/O): Вводы и выводы в полевых устройствах, доступ к которым могут получать несколько контроллеров.

Примечание — Хотя CP 3/RTE и позволяет общий I/O, но он запрещен в FSCP 3/1.

3.1.2.32 **бит-переключатель** (toggle bit): Один бит байта управления и байта статуса для синхронизации (виртуальных) текущих счетчиков как в F-хосте так и в F-устройстве.

3.1.2.33 **универсальная последовательная шина,** USB [universal serial bus (USB)]: Стандарт внешней шины, поддерживающий передачу данных на скорости до 480 Мбит/сек.

Примечание — USB является заменой последовательных и параллельных портов компьютера и применяется для обеспечения быстрых прямых соединений между компьютерами и полевыми устройствами.

3.1.2.34 **режим-V1** (V1-mode): Услуги и протокол FSCP 3/1 в соответствии с [48].

3.1.2.35 **режим-V2** (V2-mode): Услуги и протокол FSCP 3/1 в соответствии с настоящим стандартом.

3.1.2.36 **VLAN-тег** (VLAN tag): Расширение в сообщениях Ethernet, позволяющее определенным группам пользователей в больших сетях вести свою собственную виртуальную сеть посредством приоритетов и идентификаторов VLAN-ID, используя надлежащие коммутаторы и не оказывая влияния на другие группы пользователей и наоборот.

3.2 Обозначения и сокращения

3.2.1 Общие обозначения и сокращения

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	
ФБ	Функциональная безопасность	
FSCP	Профиль коммуникации, удовлетворяющий требованиям функциональной безопасности	
HD	Расстояние Хэмминга	
MTBF	Среднее время между отказами	
MTTF	Среднее время до отказа	
PDU	Блока данных протокола	[ИСО/МЭК 7498-1]
PELV	Защитное сверхнизкое напряжение	
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 эффективности защиты	[ИСО 13849-1]
PLC	Программируемый логический контроллер	
SCL	Коммуникационный уровень безопасности	
SELV	Безопасное сверхнизкое напряжение	
SFRT	Время реакции функции безопасности	
УПБ	Уровень полноты безопасности	[МЭК 61508-4:2010]

3.2.2 CPF 3. Дополнительные термины и определения

SIS — Инструментальная система безопасности (safety instrumented systems)

Сокращение	Полное выражение	Источник
ПП	Прикладной процесс	
API	Идентификатор прикладного процесса	
СП	Связь приложений	
ASE	Прикладной сервисный элемент	
ASIC	Специализированная интегральная схема	
П	Покрытие	
CP 3/1	Коммуникационный профиль общеизвестный как PROFIBUS DP	
CP 3/2	Коммуникационный профиль общеизвестный как PROFIBUS PA	
CP 3/RTE	Коммуникационный профиль общеизвестный как PROFINET IO	
ЦП	Центральный процессор	
КС	Коммуникационная связь	
DAP	Точка доступа устройства	
ВПУ	Время подтверждения устройства	
ДПУ	Децентрализованное периферийное устройство	
F	Идентификатор для элементов безопасности (отказоустойчивость, функциональная безопасность)	
Ф-блок	Функциональный блок	
FV	Отказоустойчивые значения	
GSD	Общее описание станции (файл, ассоциируемый с устройством)	
GSDL	Язык общего описания станции (для устройств CP 3/1 и CP 3/2)	
GSDML	Язык разметки общего описания станции (Для устройств CP 3/RTE)	
HAT	Время подтверждения хоста	
I/O	Ввод-вывод	
СИД	Светоизлучающий диод	
PA	Автоматизация процесса	
PN IO	PROFINET IO = c CP 3/4 по 3/6	
ПВК	Предварительно выданный ключ	
PV	Значения процесса	
RADIUS	Услуга удаленной аутентификации звонящего	
С	Стандарт	
ССБ	Связанный с (функциональной) безопасностью	
SSID	Идентификатор набора услуг	
UML	Унифицированный язык моделирования	[57]
USB	Универсальная последовательная шина	[62]
VLAN	Виртуальная локальная компьютерная сеть	
WCDT	Время задержки в худшем случае	
WD-Время	Время сторожевого таймера	
WPA2	Защищенный доступ Wi-Fi 2	[28]
XML	Расширяемый язык разметки	[59], [60], [61]

3.3 Условные обозначения

В настоящем стандарте нотация UML2 применяется для рисования диаграмм состояний и сжатых схем последовательности [57]. Таблицы переходов изображены, следуя рекомендациям МЭК 62390.

В настоящем стандарте сокращение «F» указывает на элементы, технологии, системы и блоки, связанные с безопасностью (отказоустойчивые, функционально безопасные).

В настоящем стандарте данные по умолчанию, которые должны отправляться в случае отказов или ошибок блока, именуются значениями безопасности и затем они должны устанавливаться в значение «0».

В настоящем стандарте любое вычисление сигнатуры CRC, выдающее значение «0», вместо этого будет использовать значение «1».

В настоящем стандарте аббревиатура «CP 3/RTE» включает в себя три коммуникационных профиля: CP 3/4, CP 3/5 и CP 3/6. CP 3/RTE общеизвестен как PROFINET IO.

4 Обзор FSCP 3/1 (PROFIsafe™)

Семейство 3 коммуникационных профилей (общеизвестное как PROFIBUS™, PROFINET™[2)]) 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.

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™[4)]) 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 настоящем стандарте.

FSCP 3/1 основан на циклическом обмене данными контроллера (шины) со связанными с ним (полевыми) устройствами, используя прямую (один к одному) коммуникационную связь (рисунок 3). Один контроллер может управлять любым набором стандартных устройств и устройств безопасности, соединенных с сетью. Также возможно назначение различным контроллерам задач безопасности и стандартных задач. Любые, так называемые, непериодические коммуникации между устройствами и контроллерами или супервизорами, такими как программирующие устройства, предназначены для целей конфигурирования, параметризации, диагностики и технического обслуживания.

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

- последовательная (виртуальная) нумерация;
- контроль с помощью сторожевого таймера с подтверждением;
- кодовое имя для каждой коммуникационной связи;
- циклический контроль избыточности для поддержания целостности данных.

[2)] 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™, PROFINETT™ и PROFIsafe™ требует разрешения со стороны PNO.

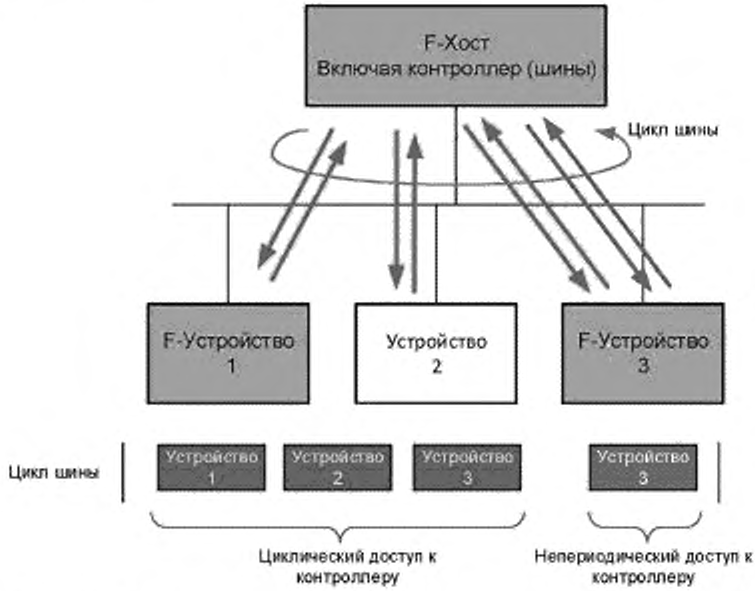


Рисунок 3 — Базовые предварительные условия для коммуникаций в FSCP 3/1

Последовательная нумерация использует достаточно большой диапазон возможностей для защиты от любой неисправности, вызванной элементами сети, хранящими сообщения. Каждое устройство безопасности возвращает сообщение, включающее в себя PDU безопасности для подтверждения, даже если нет никаких данных процесса. Отдельный сторожевой таймер, установленный как на отправителе, так и на получателе, используется для каждой прямой (один-к-одному) коммуникационной связи. Для целей аутентификации на каждую коммуникационную связь устанавливается уникальное кодовое имя. Оно кодируется начальным значением сигнатуры CRC для циклически вычисляемой и передаваемой сигнатуры CRC2 (рисунок 4).

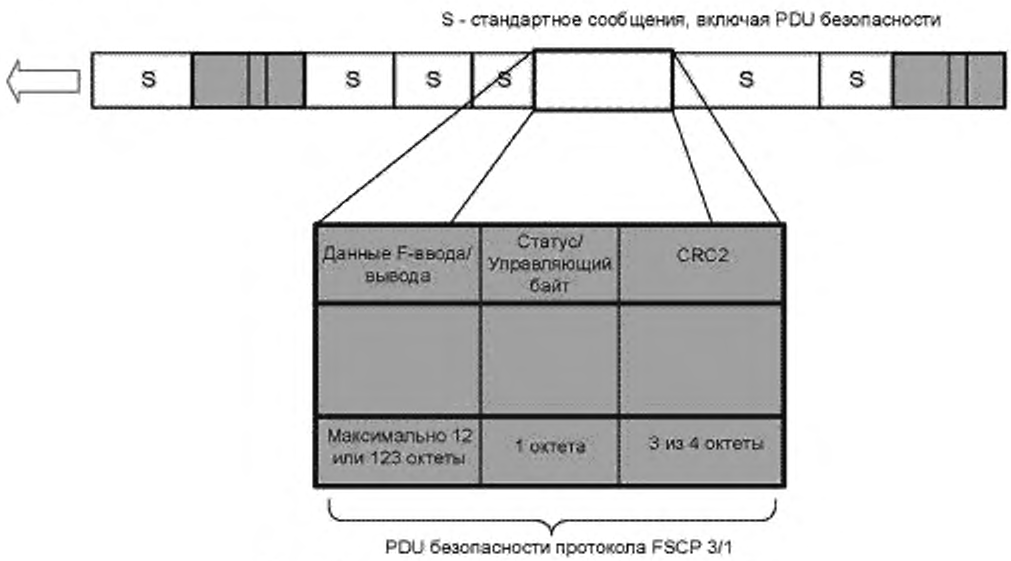


Рисунок 4 — Структура PDU безопасности FSCP 3/1

FSCP 3/1 предоставляет два режима эксплуатации: режим V1 и V2. И хотя средств режима V1 достаточно для передачи данных безопасности в сетях, использующих только CP 3/1, более «щедрые» возможности Ethernet/CP 3/RTE, такие как более широкое адресное пространство и компоненты переключателя буферизации, требуют некоторых расширений протокола FSCP 3/1, таким образом, приводя к режиму V2. Режим V1 ограничивается CP 3/1, в то время как режим V2 необходим для профилей с CP 3/4 по CP 3/6 и/или CP 3/1. Настоящий стандарт подробно описывает только расширенный функционал так называемого режима V2. Коммуникации безопасности между компонентами PROFINET CBA (см. CP 3/3) не определены. На рисунке 5 показан обзор FSCP 3/1 в рамках архитектур CP 3/1 и CP 3/RTE.

В то время как решения автоматизации с распределенными вводами-выводами получили широкое признание в связи с использованием PROFIBUS (CP 3/1 и CP 3/2) и, основанной на Ethernet, промышленной PROFINET (CP 3/RTE), приложения безопасности по-прежнему полагались на второй уровень традиционных электрических методов или на специальные шины, тем самым ограничивая «бесшовную» инженерию и интероперабельность. Кроме того, современные устройства безопасности, такие как лазерные сканнеры или приводы с встроенной системой безопасности, не могли обеспечиваться так, как это требуется, из-за недостающей системной поддержки. Целью настоящего стандарта и связанных с ним документов является предоставление соответствующих поддерживающих технологий.

Следующие за этим введением, подраздел 5.1 содержит дополнительные ссылки для разработки технологии FSCP 3/1, а подраздел 5.2 содержит функциональные требования для этой технологии. Четыре меры безопасности FSCP 3/1 перечислены в 5.3. Сетевые топологии в рамках CP 3/RTE и их пересечения с CP 3/1 и CP 3/2 упоминаются в 5.4. Далее в 5.5 следует небольшое введение в коммуникационные связи и объекты стандарта полевых шин.

Для целей безопасности и эффективности список возможных типов данных полевых шин уменьшен до сокращеного набора и описан в 5.5.4. В подразделах с 6.1 по 6.3 раскрываются услуги F-хоста и F-устройства и возможные сообщения диагностики уровня безопасности.

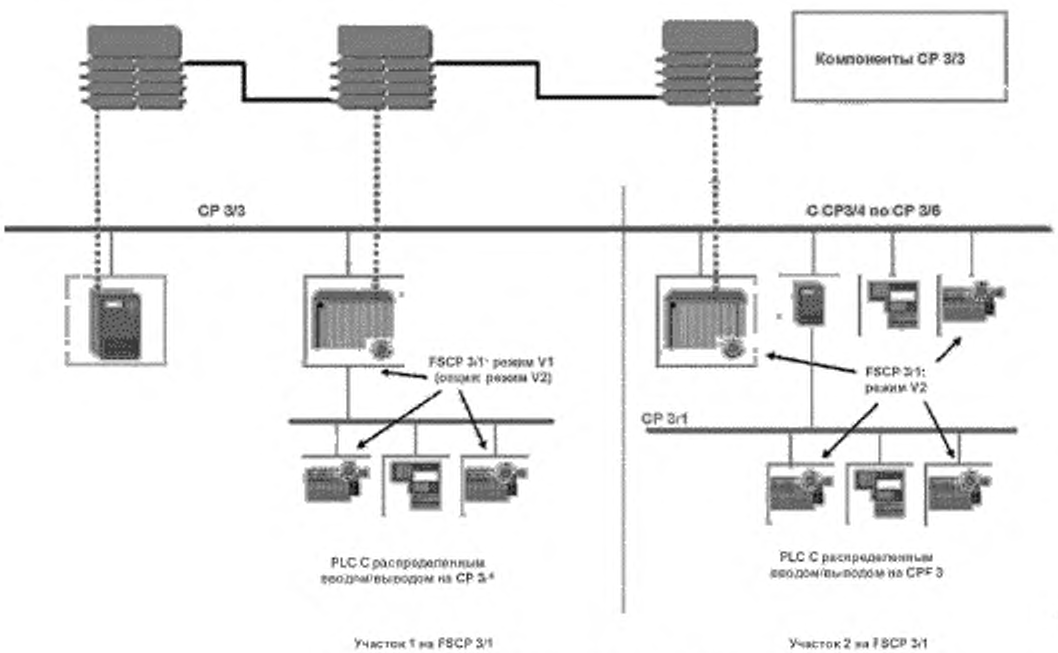


Рисунок 5 — Режимы коммуникаций безопасности

Раздел 7 начинается с обзора PDU безопасности (7.1), за которым следует описание машин состояний в F-хосте и F-устройстве и диаграммы последовательностей в формате унифицированного языка моделирования 2 (с 7.2.2 по 7.2.4). Связанные с ними временные ограничения содержатся в 7.2.5 и 7.2.6. В соответствии с форматом из МЭК 61784-3:2010, приложение D, подраздел 7.3 демонстрирует

реакции системы в случае возможных неисправностей. Другие системные функции, такие, как запуск уровня безопасности, содержаться в 7.4. Управление уровнем устройств безопасности фокусируется на F-параметрах, зависящих от коммуникаций безопасности (8.1) и на индивидуальных iпараметрах, зависящих от устройства (8.2). Требования для обработки и предоставления F-параметров описаны в 8.3. Подраздел 8.4 рассматривает вопрос защиты структур данных, которыми будут обмениваться партнеры коммуникации и которые также представляют конфигурацию устройства. Подраздел 8.5 демонстрирует, как информация о структуре данных может применяться для конфигурирования драйверов F-канала для более сложных F-устройств для того, чтобы избежать излишнее программирование. Требования для интеграции средств и инструментов iпараметризации перечислены в 8.6. Аспекты скоростей реакций, руководства по установке и длительности периода обслуживания, техническое обслуживание, руководство по безопасности, беспроводная передача данных, а также классы соответствия F-хоста — рассмотрены в 9. Аргументация оценки представлена в 10.1, а подробности в 10.2. Справочное приложение содержит примеры для быстрых вычислений CRC сигнатуры и библиографию. Следует ознакомиться с двумя дополнительными руководствами FSCP 3/1 по электрической безопасности и оценке ([44], [45]).

5 Общие положения

5.1 Внешние документы, предоставляющие спецификации для профиля

Кроме нормативных ссылок в разделе 2, технология, представленная в настоящем стандарте, была одобрена в соответствии с GS-ET-26 [31].

FSCP 3/1 соответствует требованиям NE97 [58].

5.2 Функциональные требования безопасности

Следующие требования применяются к разработке технологии FSCP 3/1.

a) Коммуникации безопасности и стандартные коммуникации должны быть независимы. Тем не менее, стандартные устройства и устройства безопасности должны иметь возможность использовать один коммуникационный канал.

b) Коммуникации безопасности должны подходить для уровня полноты безопасности УПБЗ (см. МЭК 61508), категории управления 4 (см EN 954-1 [25]), и PL e (см. ИСО 13849-1).

c) Коммуникация безопасности должна использовать коммуникационную систему, состоящую из одного канала. Дополнительно, но не обязательно, для повышения готовности можно применять избыточность.

d) Реализация протокола передачи данных безопасности должна ограничиваться оконечными устройствами коммуникации (F-хост или F-ЦП — F-устройство и/или F-I/O-модуль).

e) Между F-устройством и его F-хостом всегда должна существовать коммуникационная связь 1:1.

f) Длительности передачи данных должны контролироваться.

g) Окружающие условия должны соответствовать общим требованиям автоматизации, в основном стандартам МЭК 61326-3-1 и МЭК 611326-3-2, если, конечно, нет никаких стандартов для определенных изделий.

h) Оборудование для передачи данных, такое как, контроллеры, ASIC схемы, каналы, соединительные устройства и т. д. должны избегать модификаций (черный канал). Функции безопасности должны занимать уровень выше уровня 7 ВОС (т. е. профиль без каких либо улучшений или изменений стандартного протокола).

i) Коммуникации безопасности не должны уменьшать разрешенное число устройств. В случае приложений CP 3/2 во время отображения можно столкнуться с ограничениями, связанными с ограничениями сообщений (см. CP 3/2 в МЭК 61784-1).

j) Коммуникации безопасности должна подходить для NE97 [58] и соответствовать требованиям МЭК 61784-3:2010, приложение D.

5.3 Меры безопасности

Меры безопасности, упомянутые в таблице 1 для управления возможными ошибками передачи данных, являются одним из значимых компонентов профиля FSCP 3/1. Подборка обычных мер безопасности, перечисленных в МЭК 61784-3:2010, 5.5 и показанная в таблице 1 необходима для FSCP 3/1.

Меры безопасности должны обрабатываться и контролироваться одним блоком безопасности.

Таблица 1 — Меры, примененные для преодоления основных ошибок

Ошибка коммуникаций	Меры безопасности			
	Порядковый (виртуальный) номера[a)]	Перерыв с подтверждением получения[b)]	Кодовое имя для отправителя и получателя[c)]	Проверка данных на непротиворечивость[d)]
Искажение				x
Непреднамеренное повторение	x			
Неверная последовательность	x			
Потеря	x	x		
Недопустимая задержка		x		
Внесение	x	x	x	
Подмена		x	x	x
Адресация			x	
Периодически повторяющие отказы памяти коммутаторов	x			

[a)] Экземпляр «номера последовательности» из МЭК 61784-3.
[b)] Экземпляр «временного ожидания» и «сообщения обратной связи» из МЭК 61784-3.
[c)] Экземпляр «аутентификации соединения» из МЭК 61784-3.
[d)] Экземпляр «обеспечение целостности данных» из МЭК 61784-3.

5.4 Структура коммуникационного уровня безопасности

5.4.1 Принцип коммуникаций безопасности FSCP 3/1

Способ осуществления коммуникаций безопасности FSCP 3/1 основан на опыте, полученном при использовании метода железнодорожной сигнализации, как это было описано в МЭК 62280-1 и МЭК 62280-2.

На этом основании коммуникации безопасности осуществляются:

- стандартной системой передачи данных (рисунок 6), и
- дополнительным протоколом передачи данных безопасности над этой стандартной системой передачи.

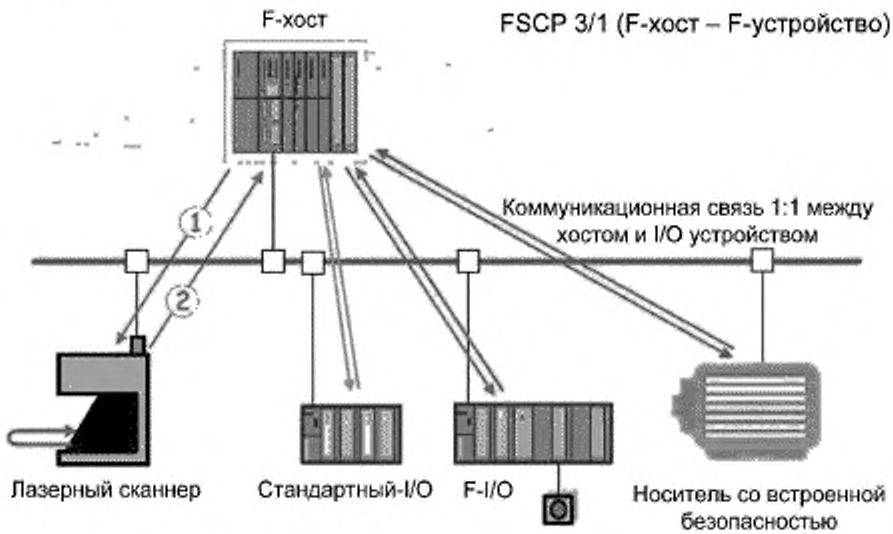


Рисунок 6 — Стандартная система передачи CPF 3

Стандартная система передачи включает в себя все аппаратные средства системы передачи и связанные с ней функции протокола (т. е. уровни 1, 2 и 7 ВОС согласно рисунку 7).

Приложения безопасности и стандартные приложения разделяют одни стандартные коммуникационные системы CPF 3 в одно и то же время. Функция безопасной передачи данных включает в себя все меры для детерминированного обнаружения всех возможных сбоев / опасностей, которые стандартная система передачи может пропускать, или же для того, чтобы поддерживать вероятность остаточной ошибки (сбоя) на допустимом уровне. Такие ошибки включают:

- произвольные неисправности, например, вызванные влиянием ЭМП на канал передачи данных;
- отказы / сбои стандартных аппаратных средств;
- систематические ошибки компонентов стандартных аппаратных средств и программного обеспечения.

Данный подход ограничивает возможности оценки «функций безопасной передачи». «Стандартная система передачи» (черный канал) не нуждается в какой-либо дополнительной оценки безопасности.

Рисунок 7 — Архитектура уровня безопасности

Передача данных осуществляется с помощью электрических или оптических проводников. Допустимые топологии и функции передачи стандартной системы передачи, а также компоненты «черного канала» описаны в 5.4.2.

5.4.2 Структуры коммуникаций CPF 3

Базовые коммуникационные уровни CP 3/RTE показаны на рисунке 8. В то время как циклические коммуникации безопасности FSCP 3/1 используют каналы реального времени RT или IRT (CP 3/RTE стандарта МЭК 61784-2), другие сервисы применяют так называемый открытый канал, работающий посредством TCP/IP или UDP.

Рисунок 8 — Базовые уровни коммуникаций

На рисунке 9 показана типичная топология (звезда) одной возможной схемы монтажа CP 3/RTE с многоканальными коммутаторами в качестве хабов. Одно отказывающее устройство не приведет к выключению всей сети в целом. Тем не менее, усилия по прокладке проводов могут не стоить результата.

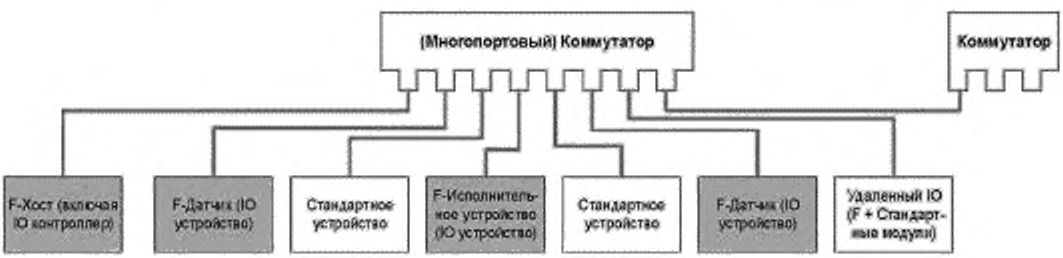


Рисунок 9 — Структура шины многоканального переключателя

CP 3/RTE предоставляет альтернативное решение с помощью коммутатора на база ASIC, где каждое устройство может подключить к своему коммуникационному интерфейсу. Таким образом, становится возможной линейная топология во многом схожая с CP 3/1. Чтобы избежать отключения системы в случае отказывающего устройства, настоятельно рекомендуется кольцевая структура (рисунок 10). Однако в данном случае существуют некоторые ограничения:

- хотя бы один участник в кольце (на рисунке 10 это F-хост) должен осуществлять управление резервированием (избыточностью) для обнаружения любого прерывания и для реорганизации передачи данных в пункты назначения;
- время перенастройки под управлением коммутатора в данном случае не должно превышать минимальное время сторожевого таймера любого F-устройства, находящегося на том же участке.

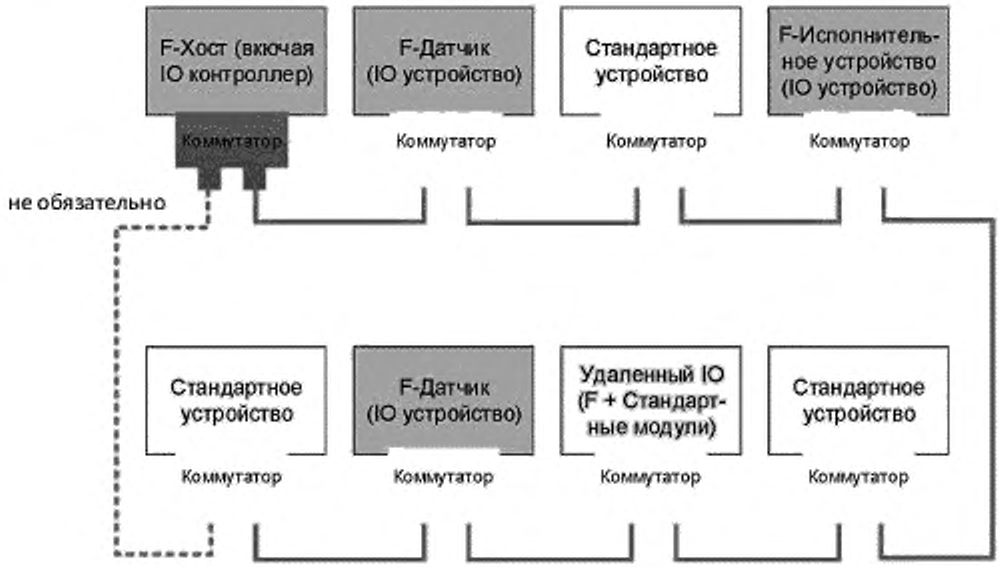


Рисунок 10 — Линейная структура шины

Каждая из сетей, представленных на рисунке 9 и рисунке 10, принадлежат к одной системе CP 3/RTE с одним определенным IP-адресом, так как протокол реального времени (Real-Time, RT или IRT) на уровне 2 не может выходить за рамки данного пространства IP-Адреса (рисунок 8). Задача по перенаправлению сообщений на уровне IP-Адреса (рисунок 11) лежит на маршрутизаторах (уровня 3 ВОС). Таким образом, маршрутизаторы являются естественными границами для CP 3/RTE систем. Следующие ограничения применимы к FSCP 3/1:

- разрешены беспроводные LAN сети. Тем не менее, на территории участков должна гарантироваться уникальность F-адресов;
- запрещены коммутаторы, которые позволяют пересекать границы сети (участка);
- запрещены однопортовые маршрутизаторы (7.3.9).

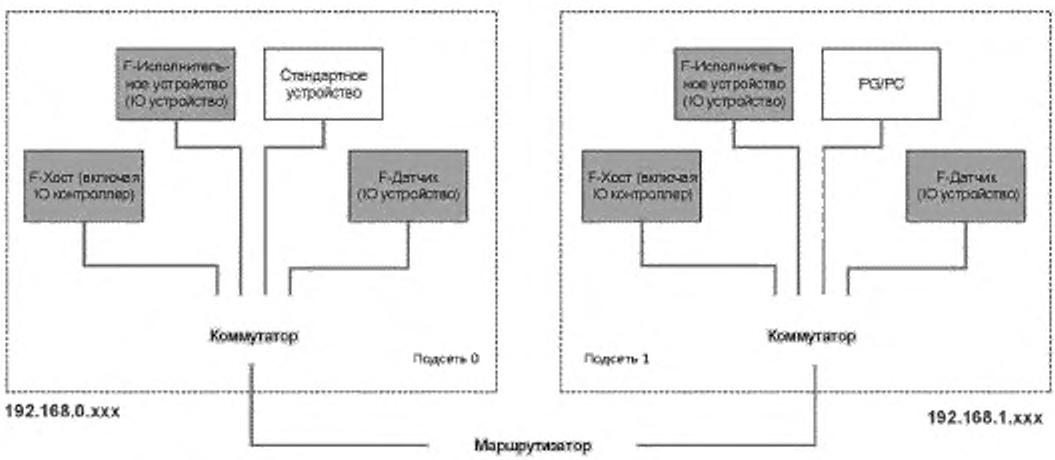
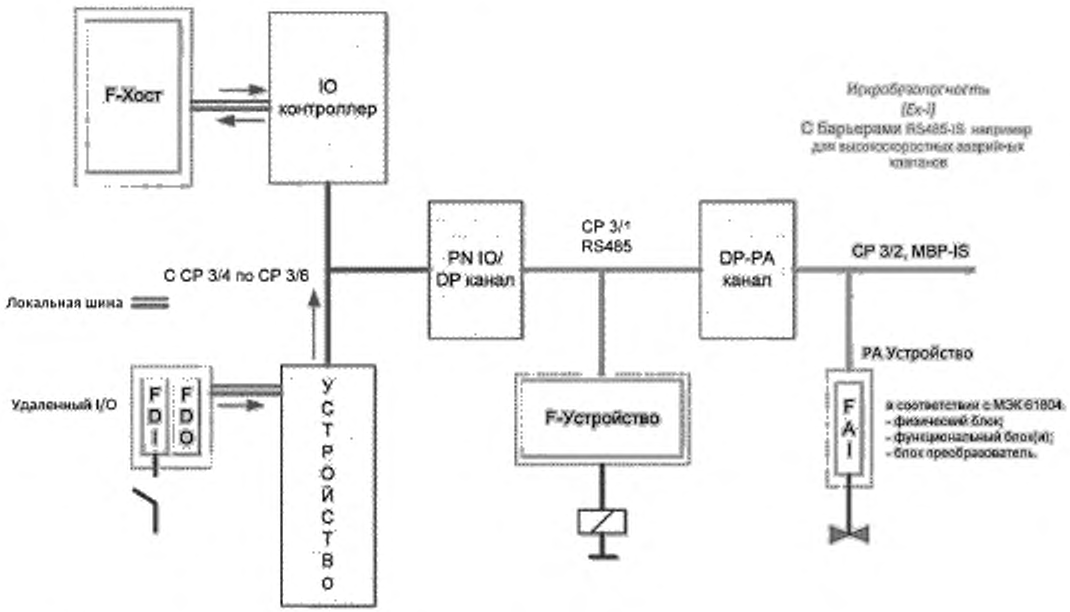


Рисунок 11 — Пересечение границ сети с маршрутизаторами

В отличие от типичной конфигурации системы полевых шин, на рисунке 12 показана возможная структура шины, где профиль безопасности достаточно сильно затрагивает индивидуальные блоки. Например, стандартный удаленный IO может включать в себя F-модуль для присоединения кнопки экстренной остановки. Таким образом, весь путь передачи данных FSCP 3/1 целиком проходит от F-хоста через его шину на объединительной плате, через CP 3/RTE (PN IO) в IO устройство и через возможно другую объединительную плату входит в финальный F-модуль. Уровень безопасности реализуется в пределах этих точек коммуникации.

Разрешено управление F-хостов множеством контроллеров или ведущих устройств (multi-controller / multi-master operation). Запрещены «разделяемые F-Вводы». Возможно совмещение F-хоста и стандартного хоста.

Примечание — Более подробно о режиме V1 в CP 3/1 см. в [48].



Обозначения:

MBP-IS	— передача данных для взрывоопасных областей;
RS485	— высокоскоростная передача данных;
RS485-IS	— специальная RS485 для взрывоопасных областей;
F-DI	— цифровой ввод безопасности;
F-DO	— цифровой вывод безопасности;
F-AI	— аналоговый ввод безопасности;
PA	— устройство в соответствии с моделью устройства автоматизации процесса (МЭК 61804).

Рисунок 12 — Полные пути передачи данных безопасности

5.5 Связи с FAL (и DLL, PhL)

5.5.1 Модель устройства

CP 3/RTE также, как и модель устройства CP 3/1, предполагает один или несколько прикладных процессов (ПП) в устройстве. На рисунке 13 показана внутренняя структура прикладного процесса для модульного полевого устройства. Дополнительно устройство может выполнять несколько из этих ПП. Прикладной процесс подразделяется на столько слотов и подслотов, сколько требуется для представления физических I/O устройства. По сравнению с CP 3/1, CP 3/RTE предоставляет на один иерархический уровень больше: подслоты.

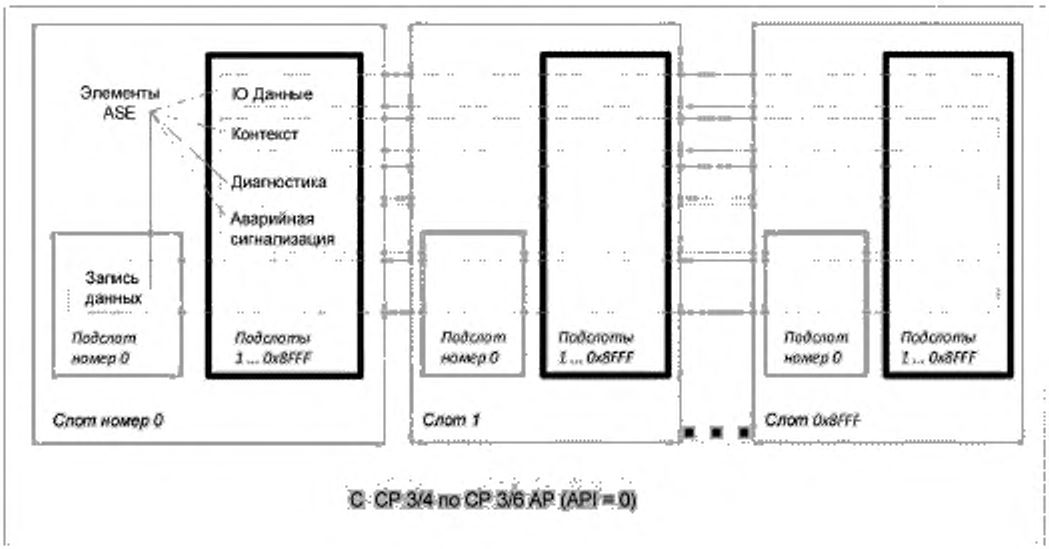


Рисунок 13 — Модель устройства

В рамках подслотов прикладные сервисные элементы (ASE) предоставляют набор стандартизированных услуг для передачи запросов и ответов прикладным процессам и от прикладных процессов, а также для объектов данных ПП, таких как данные IO, контекст (параметризация), диагностика, аварийные сигналы и публикуемые данные. Производитель устройства несет ответственность за фактическое отображение функционала устройства на модель CP 3/RTE устройства (за назначение слотов и подслотов), что осуществляется посредством GSD файла устройства.

5.5.2 Связи приложений и коммуникаций

Необходимым требованием для использования услуг, упомянутых выше, является установление связи приложений (СП), а внутри этой СП — коммуникационной связи (КС), чтобы позволить обмен объектами данных между станциями (устройством, IO-контроллером) посредством ASE элементов. На рисунке 14 показан пример базовой структуры модульного IO-устройства и возможных связей с IO-контроллерами.

IO-контроллер использует кадр «Connect» («Соединить»), отправляемый в специальном CP 3/RTE сообщении, для инициализации установления СП во время запуска системы. Таким образом, он передает устройству следующий набор данных:

- общие параметры коммуникаций этой связи приложений (СП);
- коммуникационные связи (КС), которые необходимо будет установить, включая параметры;
- модель и данные отображения устройства;
- связи КС для аварийных сигналов, которые необходимо будет установить, включая параметры.

IO-устройство проверяет полученные данные и устанавливает требующиеся связи КС. Доклады о возможных возникающих ошибках отправляются IO-контроллеру. Обмен данными начинается с положительного подтверждения ответа устройства на запрос «Соединить». Запрещена установка двух FSCP 3/1 СП связей от разных ПП с одним подслотом.

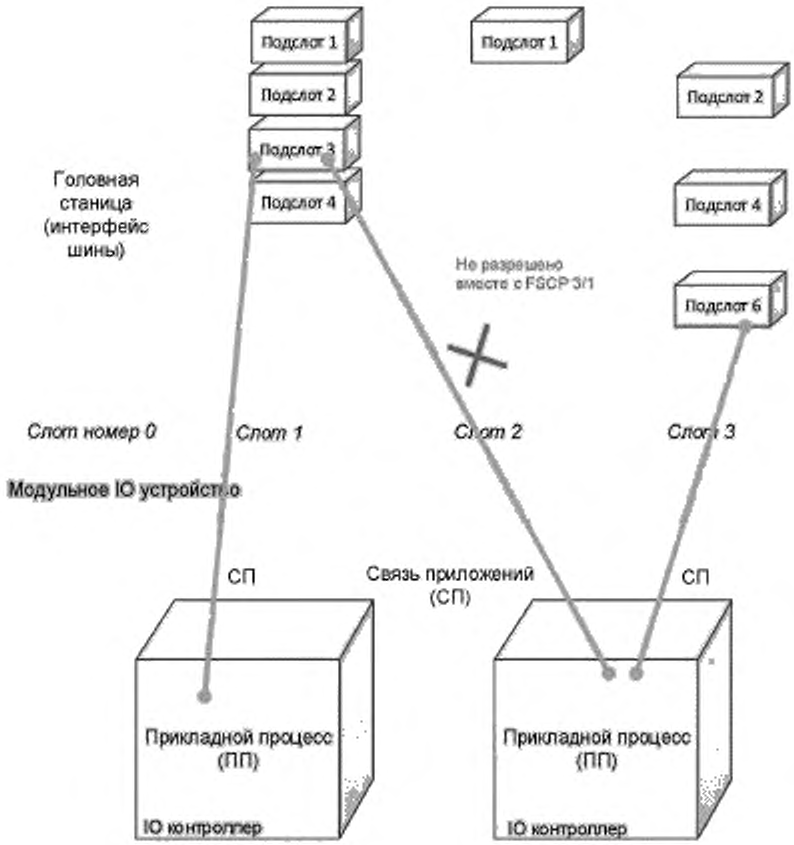


Рисунок 14 — Связи приложений модульного устройства

Рисунок 15 — Связи приложений и коммуникаций (СП/КС)

На этом этапе IO данные по-прежнему могут быть отмечены как ошибочные, так как назначение параметрам запуска IO устройств по-прежнему отсутствует. Следуя за вызовом «Соединить», IO контроллер передает данные назначения параметрам запуска (контекст) IO устройству с помощью КС записи данных (рисунок 15). IO контроллер использует один «кадр записи» для каждого сконфигурированного подмодуля и завершает передачу «концом параметризации». В ответ, IO устройство подтверждает положительное назначение параметрам запуска сообщением «приложение готово». Начиная с этого момента — СП установлена.

5.5.3 Формат сообщения

Формат сообщение CP 3/RTE для обмена данными реального времени показан на рисунке 16. Последовательность проверки кадра (FCS), состоящая из 32 битов, защищает передачу на протяжении всей сети. FSCP 3/1 никак не выигрывает от этой меры.

Обозначения:

Преамбула — AAAAAAAAAAAAAAh;;
SFD — начальный разделитель кадра:: Abh;
DA — адрес назначения (6 octletts);
SA — адрес источника (6 octletts);
Тег VLAN — указывает на определенный приоритет; не обязателен;;
Тип Ether — тип кадра Etthernett:: 8892h для с CP 3//4 по CP 3//6 (2 октета);
ID Кадра — идентификация кадра (типы сообщений с CP 3/4 по CP 3/6);;
IOPS — статус IIO поставщика:: хороший/плохой и местоположениеgood//(не обязательно//GSD);;
IOCS — статус потребителя IIO: хороший//плохой и местоположениеgood//(Не обязательно//GSD);;
Цикл — счетчик цикла (2 октета);; величина,, кратная 31,,25μs;;
Статус данных — информация об избыточности,, соответствии,, состоянии устройства и т..п...;
X Статус — статус передачи (1 октет); всегда "00h";;
FCS — 32-битовый CRC (104C11DB7h)..
*) при VLAN-Tere минимум данных для передачи составляет 36 октетов.

Рисунок 16 — Формат сообщения

5.5.4 Типы данных

CPF 3 использует базовые типы данных, перечисленные в таблице 2. Для целей безопасности только ограниченное число типов данных может быть использовано для FSCP 3/1.

Таблица 2 — Типы данных, использующиеся для FSCP 3/1

Название типа данных	Перевод	Число октет	Используется в
Integer8	8-битовый целочисленный	1	
Integer16	16-битовый целочисленный	2	Режимы V1 и V2
Integer32	32-битовый целочисленный	4	V2-режим
Integer64	64-битовый целочисленный	8	
Unsigned8 (used as bits)	8-битовый без знака (используется в качестве бит)	1	Режимы V1 и V2

Окончание таблицы 2

Название типа данных	Перевод	Число октет	Используется в
Unsigned16 (used as bits)	16-битовый без знака (используется в качестве бит)	2	Режим-V2
Unsigned32 (used as bits)	32-битовый без знака (используется в качестве бит)	4	Режим-V2
Unsigned16	16-битовый без знака	2	
Unsigned32	32-битовый без знака	4	
Unsigned64	64-битовый без знака	8	
Float32	32-битовый с плавающей точкой	4	Режимы V1 и V2
Float64	64-битовый с плавающей точкой	8	
Date	Дата		
TimeOfDay with date indication	Время суток с индикацией даты		
TimeOfDay without date indication	Время суток без индикации данных		
TimeDifference with date indication	Разность времени с индикацией даты		
TimeDifference without date indication	Разность времени без индикации даты		
NetworkTime	Сетевое время		
NetworkTimeDifference	Разность сетевого времени		
Visible String	Видимая строка	1,2,3...	
Unsigned8+Unsigned8	8-битовый без знака+8-битовый без знака	2	Режимы V1 и V2
Float32+Unsigned8 (enumerated)	32-битовый с плавающей точкой+8-битовый без знака (перечислимый)	5	Режимы V1 и V2
F_MessageTrailer4Byte	4-байтовое окончание F_сообщения	4	Режимы V1 и V2
F_MessageTrailer5Byte	5-байтовое окончание F_сообщения	5	Режим-V2

Типы данных для применения в режиме V2 ограничиваются следующими типами: 8-битовый без знака, 16-битовый без знака, 32-битовый без знака, 16-битовый целочисленный, 32-битовый целочисленный, 32-битовый с плавающей точкой и совмещенный тип данных 32-битовый с плавающей точкой+8-битовый без знака. Единичные биты будут закодированы в 8-битовом без знака, 16-битовом без знака или 32-битовом без знака типе данных по причине большей эффективности этих типов в сравнении с Булевым типом.

Общую информацию о типах данных см. в [67].

6 Услуги коммуникационного уровня безопасности

6.1 Услуги F-хоста

На рисунке 17 показано, что каждый F-ввод и каждый F-вывод требует управления блоком PDU безопасности (F-драйвер) для того, чтобы реализовать протокол FSCP 3/1. Соответствующий F-хост работает с экземпляром F-драйвера для каждого F-ввода и F-Вывода соответственно. Таким образом, каждая связь 1:1 между экземпляром F-драйвера и соответствующим партнером в рамках F-устройства идентифицируется уникальным *кодовым именем* (один из F-параметров).

Все стандартное коммуникационное оборудование CPF 3 между F-драйверами принадлежит черному каналу. Стрелочки на рисунке 17 указывают на циклическую передачу данных между F-драйверами: адденда безопасности (статус или контрольный байт и CRC2) передается от F-ввода F-хосту в дополнении к данным F-ввода. В качестве подтверждения, F-ввод всего лишь принимает адденду безопасности (код безопасности). В соответствии с этим, F-вывод принимает адденду безопасности в дополнении к данным F-вывода, и применяет ее для подтверждения.

Управление блоками PDU безопасности и F-параметризация являются задачами F-драйверов в F-хосте и F-устройствах. На рисунке 18 показан F-интерфейс, пользователя находящийся на уровне программы управления безопасностью.

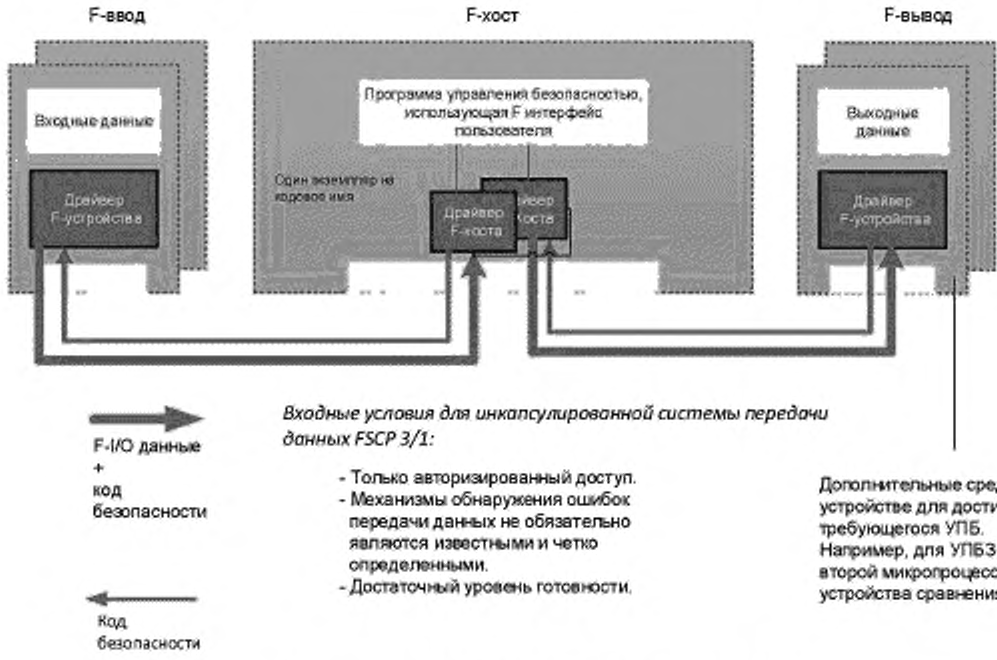


Рисунок 17 — Структура коммуникаций FSCP 3/1

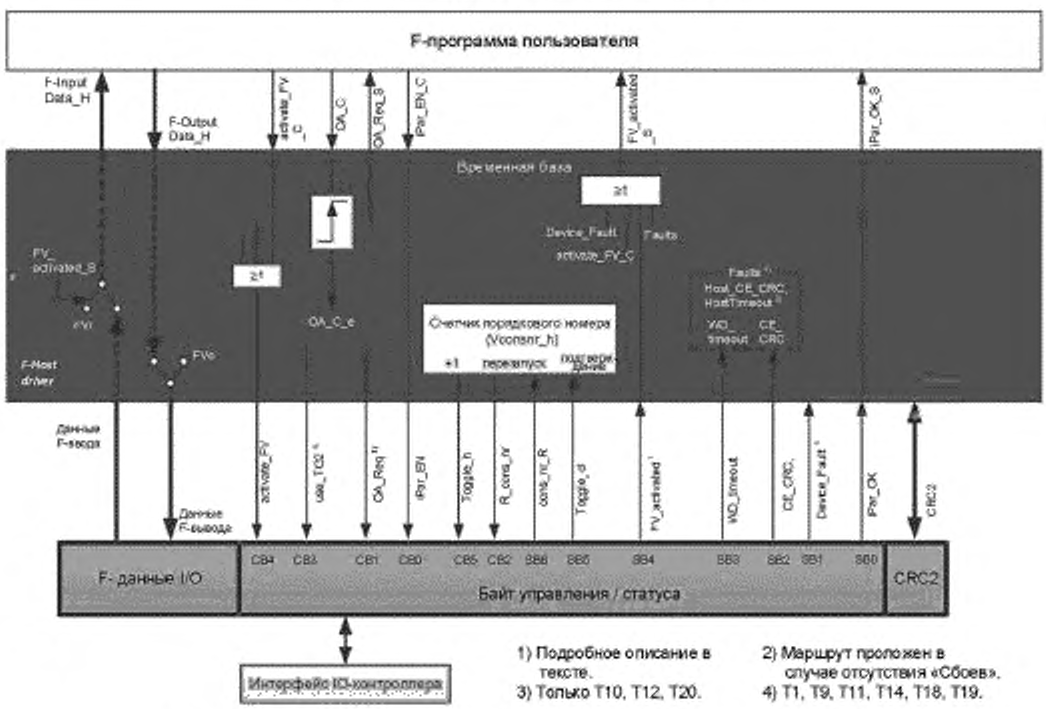


Рисунок 18 — F-интерфейс пользователя для экземпляров драйвера F-хоста

Программисту доступно несколько переменных для того, чтобы манипулировать процессами безопасности в соответствии со стандартами. Эти переменные имеют похожие имена, как правило, расширенные за счет добавления индекса «_C» (Control, т. е. управление) или «_S» (Status, т. е. статус), на подобии соответствующих им битов в байтах статуса и управления, но они также могут нести некоторую логику управления в F-драйвере. См. также 8.5.2 и рисунок 62. Указания по реализации для драйвера F-хоста собраны в 8.5.3.

В соответствии с 9.9 следующие переменные должны быть доступны программисту программы управления F-хоста:

activate_FV_C Каждая программа управления безопасностью, которая работает с соответствующим F-устройством должна использовать эту переменную (тип: двоичная). В случае устройств ввода (например, датчиков) данная переменная, установленная в значение «1» заставляет драйвер доставлять отказоустойчивые значения («0») F-программе управления. В случае устройств вывода (например, исполнительных устройств) эта переменная, установленная в значение «1» вынуждает драйвер отправлять отказоустойчивые значения («0») устройству и установить бит 4 в значение «1». Концепция безопасности устройства вывода определяет тип информации для этих двух случаев, которая должна использоваться для достижения безопасного состояния.

FV_activated_S Каждая программа управления безопасностью, которая работает с соответствующим F-устройством должна использовать эту переменную (тип: двоичная). В случае устройств ввода данная переменная своим значением «1» указывает на то, что драйвер доставляет отказоустойчивые значения («0») программе F-хоста для каждого входного значения. Подсказка: чтобы позволить индивидуальную обработку каждого ввода во вводные данные могут быть добавлены специальные указательные биты. В случае устройств вывода данная переменная указывает своим значением «1» на то, что каждый вывод установлен в отказоустойчивое значение «0» (поведение по умолчанию) или же определенное, зависящее от устройства F-вывода значение, управляемое сигналом «activate_FV» (4-й бит байта управления).
Подсказка: Для того, чтобы обрабатывать каждый вывод индивидуально (например, в случае двигателей) могут быть использованы специальные указательные биты.

iPar_EN_C Данная переменная (тип: двоичная), установленная в значение «1» позволяет F программе управления переключать F-устройство в режим, в ходе которого, оно будет принимать iпараметры. Она непосредственно связана с сигналом управления «iPar_ EN» (бит 0 байта управления) и не влияет на состояния F-хоста. При необходимости, переменная «activate_FV_C» должны быть также установлена в значение «1».

iPar_OK_S Данная переменная (тип: двоичная) указывает F-программе управления на окончание iпараметризации и готовность восстановить обмен данными F-I/O (рисунок 41). Если бит 1 статуса «Сбой устройства» не установлен, она должна обновляться значением «iPar_OK» в переходах T4, T8 и T17 машины состояний F-хоста. В противном случае эта переменная продолжает хранить предыдущее значение. Это не влияет на состояния F-хоста. Переменные «iPar_EN_C» и «activate_FV_C» могут быть переустановлены.

OA _C (Подтверждение оператора) Каждая F программа управления должна применять эту переменную (тип: двоичная). Изменяя значение этой переменной на «1» пользователь получает возможность восстановить функцию безопасности после реакции на сбой (зависит от контура отказоустойчивого управления) посредством пользовательской программы F-хоста.

OA_Req_S Данная переменная (тип: двоичная) указывает на наличие запроса на подтверждение перед возобновлением функции безопасности. В том случае, если драйвер F-хоста или F-устройство обнаруживает коммуникационную ошибку или сбой F-устройства, то будут активированы отказоустойчивые значения. Драйвер F-устройства затем, как только сбой/ошибка была устранена и возможно подтверждение оператора, устанавливает переменную OA_Req_S в ("1"). По завершении подтверждения (OA_C = "1") драйвер F-устройства обнуляет переменную запроса OA_Req_S ("0").

Значения ввода PVi Значения ввода процесса (←F-Input_Data_D, см. рисунок 19).
FVi Отказоустойчивые значения ввода, используемые вместо PVi для F-Input_Data_D (см. рисунок 19).

Значения вывода PVo Значения вывода процесса (→F-Output_Data_D).
FVo Отказоустойчивые значения вывода (=0), используются вместо PVo для FOutput_Data_D.

6.2 Услуги F-устройств

На рисунке 19 подробно проиллюстрирован драйвер F-устройства и то, как он встроен между интерфейсом CP 3/RTE и частью конкретного приложения устройства, связанной с безопасностью. В течение фазы запуска часть конкретного приложения устройства, не связанная с безопасностью, получает F-параметры и передает их драйверу F-устройства. Сам драйвер, после проверки некоторых из F-параметров, передает F-параметры «F_iPar_CRC» и «F_SIL» части конкретного приложения устройства, связанной с безопасностью. Как правило, конкретное приложение устройства предоставляет базу данных времени (1мс) драйверу F-устройства для того, чтобы обеспечивать сторожевые таймеры.

Драйвер F-устройства в основном работает с PDU безопасности, которые принимаются или передаются посредством связи коммуникаций данных IO реального времени, основанной на протоколе CP 3/RTE (5.5.2). F-данные I/O (данные отказоустойчивых вводов-выводов), как правило, пропускаются, за исключением периода запуска (в данном случае проходят значения FVi) или случая сбоев (тогда, это значения FVo). Полученные PDU безопасности содержат байты управления с битами управления (Control Bits) CB0, CB1, CB2, CB3, CB4, и CB5. Некоторые из этих сигналов передаются прикладному интерфейсу без взаимодействия. Для упрощения реализации запросов с достаточной длительностью (как минимум один цикл FSCP 3/1 = двум разным порядковым номерам) предоставляется индикатор нового порядкового номера. В ответ на это для передачи подготавливаются блоки PDU безопасности. Они содержат байты статуса вместе с битами статуса (Status Bits) SB0 …SB5. Один из них пропускается, драйвер генерирует некоторые из них, а некоторые поступают из прикладного интерфейса, подвергаясь манипуляциям драйвера перед входом в PDU безопасности. Driver_Fault устанавливается в случае внутреннего сбоя драйвера.

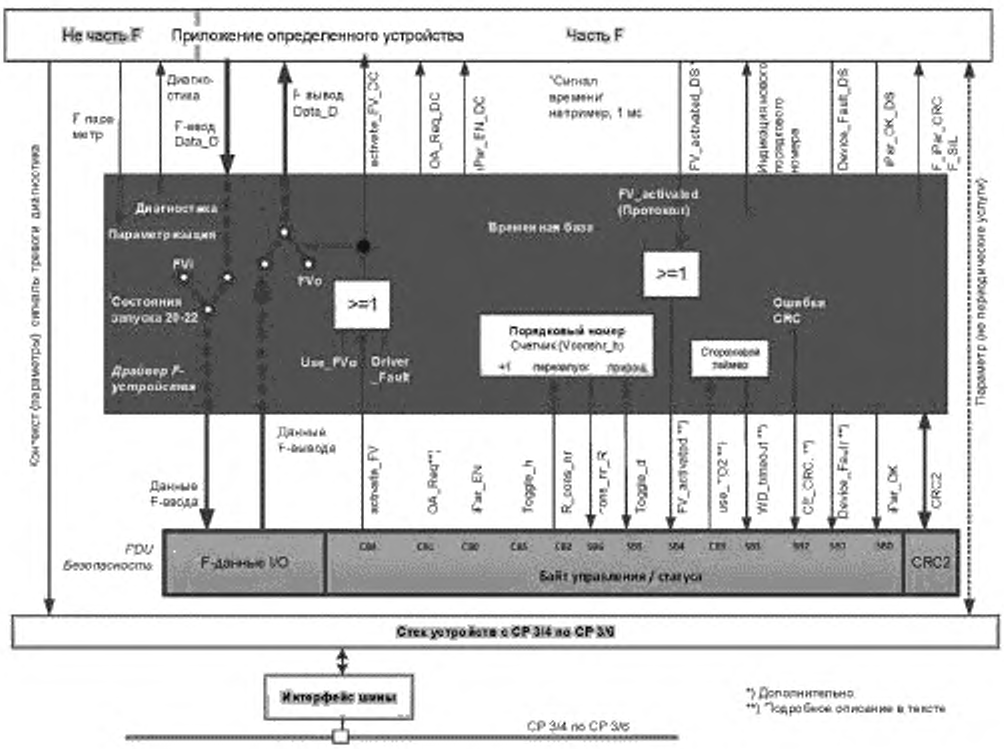


Рисунок 19 — Интерфейсы драйвера F-устройства

Счетчик порядкового номера увеличивается (x+1), когда «Toggle_h» меняет свое состояние (0→1; 1→0). Значение R_cons_nr = «1» обнулит счетчик («0»). Приращение счетчика изменит состояние «Toggle_d» (0→1; 1→0). CRC проверка выполняется при каждом полученном и отправленном PDU безопасности (CRC2).

Следующие переменные доступны конкретному приложению устройства. Эти переменные имеют похожие имена, как правило, расширенные за счет добавления индекса «DC» (device control, т. е. управление устройством) или «DS» (device status, т. е. статус устройства), на подобии соответствующих им битов в байтах статуса и управления.

activate_FV_DC	Эта связанная с безопасностью переменная указывает на то, что данные F-вывода являются отказоустойчивыми значениями (FV = 0). Она может применяться для принуждения выводов F-устройства перейти в сконфигурированные или встроенные отказоустойчивые значения.
FV_activated _DS	В случае устройств ввода эта переменная указывает своим значением «1» на то, что приложение устройства доставляет отказоустойчивые значения («0») драйверу FSCP 3/1 для каждого значения ввода. Подсказка: Для того, чтобы обрабатывать каждый вывод индивидуально к данным ввода могут быть добавлены специальные указательные биты. В случае устройств вывода ярлык указывает с помощью значения «1» на то, что каждый вывод установлен в отказоустойчивые значения. Для случаев совмещения устройств ввода и вывода, данная переменная (тип: двоичная) указывает, с помощью значения «1» на то, что приложение устройства доставляет отказоустойчивые значения («0») драйверу FSCP 3/1 для каждого значения ввода, а каждый вывод установлен в отказоустойчивые значения.
OA_Req_DC	Приложение F-устройства должно использовать эту, не связанную с безопасностью, переменную для того, чтобы локально указывать на присутствие запроса на подтверждение оператора (*OA_C* в F-хосте), как правило, посредством светодиода. Реализация этой переменной является не обязательным для F-устройств.
iPar_EN_DC	Данная переменная, в случае, если она имеет значение «1», указывает на наличие запроса на параметризацию (F-устройство нуждается в новых iпараметрах).
iPar_OK_DS	Данная переменная, в случае, если она имеет значение «1», указывает на то, что F-устройство (его конкретное приложение устройства) обладает новыми назначенными значениями iпараметров.
Device_Fault_DS	Сбой, распознанный конкретным приложением устройства.

6.3 Диагностика

6.3.1 Генерация сигнализации безопасности

Вследствие быстрых циклов опроса пользовательской программы скорость обнаружения изменений F-данных I/O и сигнатуры CRC2 является удовлетворительной.

В случае коммуникационных ошибок система способна вовремя и безопасным способом реагировать, например, используя информацию в байте статуса.

6.3.2 Диагностика уровня безопасности F-устройства, включая iPar-Server

Для того, чтобы отправлять отчеты с информацией о диагностике драйвера F-устройства FSCP 3/1 устройству человеко-машинного интерфейса, драйвер передает свою информацию приложению F-устройства, использующему механизмы стандарта CP 3/RTE для передачи данных IO-контроллеру. Использование каждого стандартного средства диагностики CP 3/RTE является возможным, предпочтительнее диагностика-связанная-с-каналом. В таблице кодирования, в поле «ChannelErrorType» (Тип ОшибкиКанала) хранится место для FSCP 3/1. В таблице 3 показаны различные типы диагностической информации протокольного уровня FSCP 3/1 в F-устройствах.

Таблица 3 — Сообщения диагностики уровня безопасности

Шестнадцатеричный	Номер	Диагностическая информация
0x0040	64	Несоответствие адреса назначения безопасности (F_Dest_Add), см. 8.1.2
0x0041	65	Адрес назначения безопасности недействителен (F_Dest_Add), см. 8.1.2
0x0042	66	Адрес источника безопасности не действителен (F_Source_Add), см. 8.1.2
0x0043	67	Время сторожевого таймера безопасности равно 0 мс (F_WD_Time)
0x0044	68	Параметр «F_SIL» превышает УПБ (SIL) конкретного приложения устройства
0x0045	69	Параметр F_CRC_Length не соответствует сгенерированным значениям
0x0046	70	Установлена неверная версия F-параметра
0x0047	71	Сбой CRC1
0x0048	72	Диагностическая информация, зависящая от устройства, см. руководство
0x0049	73	Время сторожевого таймера для сохранения iпараметра превышено
0x004A	74	Время сторожевого таймера для восстановления iпараметра превышено
0x004B	75	Противоречивые iпараметры (ошибка iParCRC)
0x004C	76	Зарезервировано: не используйте номера, не оценивайте номера
0x004D	77	Зарезервировано: не используйте номера, не оценивайте номера
0x004E	78	Зарезервировано: не используйте номера, не оценивайте номера
0x004F	79	Зарезервировано: не используйте номера, не оценивайте номера

F-устройства, использующие механизм iPar-Server для хранения и извлечения iпараметров в рамках F-хоста или подсистемы, которой он управляет, с помощью дополнительных раздельных кодировок могут создавать отчеты со специализированной диагностической информацией. Настоятельно рекомендуется, в случае F-устройств, использовать эти типы в диагностических сообщениях. Тем не менее, диагностические сообщения могут также переносить итоговую информацию в нескольких индивидуальных случаях.

Примечание — Производитель устройства должен объяснить отображение таких индивидуальных случаев на определенные диагностические сообщения.

7 Протокол коммуникационного уровня безопасности

7.1 Формат PDU безопасности

7.1.1 Структура PDU безопасности

На рисунке 20 показана структура одного единственного блока PDU безопасности, содержащего данные ввода/вывода безопасности, а также дополнительный код безопасности. Сообщение CP 3/RTE может содержать несколько PDU безопасности, например, в случае модульных IO устройств с несколькими модулями.

Автоматизация производства и автоматизация процесса имеют различные требования к системе безопасности. Автоматизация производства использует короткие двоичные (битовые) данные ввода/вывода безопасности, как правило, обрабатываемые на очень высокой скорости; а автоматизация процесса использует более длинные значения I/O («с плавающей точкой»), для обработки которых может потребоваться немного больше времени. Поэтому FSCP 3/1 предлагает две разных длины данных ввода/вывода безопасности, которым требуется защита различной сложности, чтобы соответствовать требованиям УПБ3.

Таким образом, параметризацией могут быть выбраны *два* эксплуатационных *режима*: небольшое количество F-данных I/O длиной до 12 *октетов* вместе с 24-битным CRC2 (3 октета) и F-данные I/O (процесса) до 123 *октетов* вместе с 32-битным CRC2 (4 октета).

Дополнительно, в сумме требуется 4 (5) октетов, включая байт статуса/управления и 3 (4) октета для кода CRC2.

Подразделы с 7.1.2 по 7.1.6 предоставляют подробное описание элементов структуры PDU безопасности.

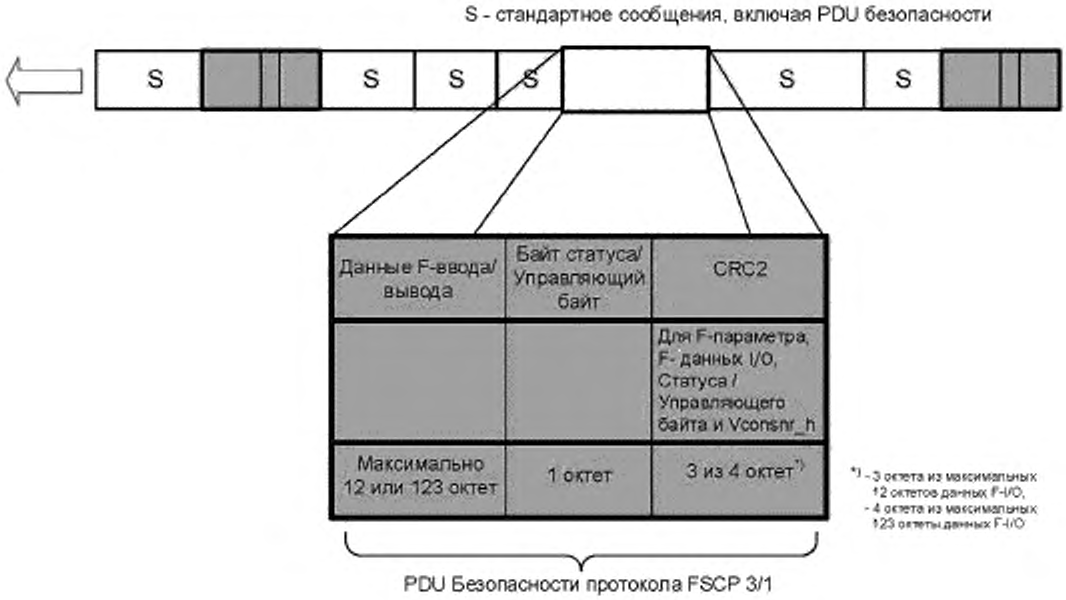


Рисунок 20 — PDU безопасности для CPF 3

7.1.2 Данные I/O безопасности

F-данные I/O периферийных F-модулей I/O содержатся в этой секции PDU безопасности. Кодирование типа данных соответствует одному из кодирований CP 3/RTE и определено для всей системы в стандарте МЭК 61158-5-10. В 8.5.2 рекомендуются и устанавливаются стандартизированные типы данных и структуры данных для нескольких семейств устройств безопасности, таких как удаленные I/O, световые завесы, лазерные сканнеры, приводы и т.д.

В случае, когда используется только небольшое количество F-данных I/O до 12 октетов — опция 24-битового CRC должна быть выбрана параметризацией.

Помимо компактных устройств, имеются также *модульные устройства*, обладающие как F, так и стандартными блоками I/O, а также имеющие подадреса (рисунки 13 и 14). Их головная станция CP 3/RTE (DAP), которую считают частью черного канала, используется для согласования структуры сообщения CP 3/RTE с несколькими PDU безопасности посредством параметризации запуска. Один PDU безопасности соответствует одному подслоту. Количество данных соответствует стандартному количеству данных CP 3/RTE минус 4 или 5 октетов соответственно. Это означает, что для головной станции устройства, обладающей *m* модулями безопасности, требуется сокращение, равное *m*, умноженному на 4 или 5 октет, соответственно.

7.1.3 Байт статуса и управления (Status and Control Byte)

Бит7	Бит6	Бит5	Бит4	Бит3	Бит2	Бит1	Бит0
res	Vconsnr_d был сброшен	Бит переключатель	Активированы отказоустойчивые значения (FV)	Сбой коммуникаций: WD-таймаут	Сбой коммуникаций: CRC	В F-устройстве или F-модуле случился отказ	F-устройству были назначены новые значения параметров
-	cons_nr_R	Toggle_h	FV_activated	WD_timeout	CE_CRC	Device_Fault	iPar_OK

Рисунок 21 — Байт статуса

Байт статуса, показанный на рисунке 21, содержится в каждом PDU безопасности подмодуля CP 3/RTE, передаваемом от устройства контроллеру этого устройства (рисунок 20).

Бит 0 устанавливается, когда F-устройство (его технологическое встроенное программное обеспечение) получило новые значения параметров.

Имя сигнала «iPar_OK».

Бит 1 должен устанавливаться определенным технологическим встроенным программным обеспечением устройства на протяжении хотя бы двух (2) изменений порядкового номера, если F-устройство/модуль либо не предоставляет никаких квалификаторов сигнала, зависящих от канала, и один или более каналов отказывают, либо устройство обнаруживает другую неисправность. Такое поведение позволяет более быструю реакцию в случае события отказа, чем при использовании таймаута (перерыва). Имя сигнала — «Device_Fault».

Бит 2 устанавливается, если F-устройство распознает отказ F-коммуникаций, т.е. если порядковый номер неверен (обнаружено посредством ошибки CRC2 в V2-режиме) или целостность данных нарушена (ошибка CRC). Эта битовая информация позволяет F-хосту подсчитать все ошибочные сообщения в рамках заданного промежутка времени T и вызвать сконфигурированное безопасное состояние системы, если значение превышает определенный предел (максимальная частота остаточных ошибок). Имя сигнала — «CE_CRC».

См. также 9.5.1.

Бит 3 устанавливается, если F-устройство распознает отказ F-коммуникаций, т. е. если время сторожевого таймера в F-устройстве превышено. Имя сигнала — «WD_timeout».

Бит 4 устанавливается протокольным уровнем FSCP 3/1 во время запуска и в случаях любых коммуникационных ошибок (рисунок 19 и 7.2). В дополнение к этому F-часть определенного приложения устройства может также устанавливать этот бит. Имя сигнала — «FV_activated».

Бит 5 это основанный на устройстве бит переключатель (Toggle Bit), указывающий на триггер увеличения виртуального порядкового номера в F-хосте (Vconsnr_h). Имя сигнала — «Toggle_d».

Бит 6 устанавливается, когда F-устройство обнулило свой счетчик порядкового номера Vconsnr_d. Имя сигнала — cons_nr_R.

Бит 7 зарезервирован (res) для будущих выпусков FSCP 3/1.

Бит7	Бит6	Бит5	Бит4	Бит3	Бит2	Бит1	Бит0
res	res	Бит переключатель	Отказоустойчивые значения (FV) ожидающие активации	Использовать F_WD_Time_2 (вторичный сторожевой таймер)	Сбросить Vconsnr_d	Запрошено подтверждение оператором	Назначение iпараметров разблокировано
-	-	Toggle_h	activate_FV	Use_TO2	R_cons_nr	OA_Req	iPar_EN

Рисунок 22 — Байт Управления (Control Byte)

Байт управления, показанный на рисунке 22, отправляется с каждым PDU безопасности подслота от IO контроллера устройству (рисунок 20).

Бит 0 устанавливается F-приложением в F-хосте в случае наличия запроса параметризации (F-устройство нуждается в новых iпараметрах). Имя сигнала — «iPar_EN».

Бит 1 устанавливается драйвером F-хоста, соответствующим переменной «OA_Reg_S». Сигнал не связан с безопасностью и должен использоваться F-устройством для местной индикации запроса для подтверждения оператора (OA_C), как правило, посредством светодиода (9.1). Имя сигнала - «OA_Req».

Бит 2 устанавливается, когда F-хост обнаруживает коммуникационную ошибку, либо с помощью байта статуса, либо самостоятельно. Вследствие этого счетчик виртуального порядкового номера (Vcopnsnr_d) в F-устройстве будет устанавливается в значение «0» (см. 7.1.4 и 7.2.5). Бит 2 должен быть снова обнулен после исчезновения ошибки. После этого последовательная нумерация возобновляется. Имя сигнала — «R_cons_nr».

Бит 3 устанавливается, когда драйвер F-хоста наследственно проинформирован о том, что осуществляется намеренный процесс обновления компонентов полевой шины безопасности для случая «конфигурирования во время выполнения» или «технического обслуживания системы устойчивости к сбоям».

Бит 4 может быть установлен для принуждения выводов F-устройства перейти в сконфигурированные или встроенные отказоустойчивые значения. См. подробности в 6.1. Имя сигнала — «activate_FV».

Бит 5 — это основанный на хосте бит переключатель, указывающий на триггер для приращения виртуального порядкового номера в F-устройстве (Vconsnr_d). Имя сигнала — «Toggle_h». См. подробности в 7.1.4. Имя сигнала — «Toggle_h».

Биты 6 и 7 зарезервированы (res) для будущих выпусков FSCP 3/1.

Подсказка: для того, чтобы избежать неприятностей с будущими версиями устройств FSCP 3/1, биты статуса и управления типа «res» должны быть установлены в значение «0» и приемник должен их игнорировать.

7.1.4 (Виртуальный) порядковый номер

Получатель использует порядковый номер для того, чтобы контролировать, активны ли еще отправитель и коммуникационный канал или нет. Порядковый номер используется в механизме подтверждения для контроля *скорости прохождения* между отправителем и получателем. Значение «0» зарезервировано для первого прогона и для реакции на коммуникационную ошибку. В отличие от режима V1, режим V2 использует 24-*битные счетчики* для последовательной нумерации. Таким образом, порядковый номер вычисляется в циклическом режиме от 1… 0FF FF FFh, возвращаясь назад к 1 в конце.

Примечание — Подробности режима V1 см. в [48].

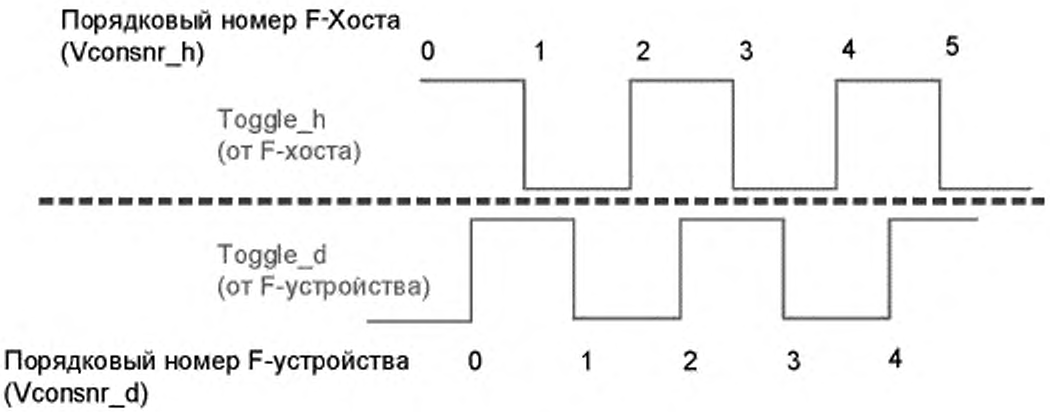


Рисунок 23 — Функция бита переключателя

Также, в отличие от режима V1, режим V2 не передает порядковый номер с каждым из PDU безопасности. Вместо этого он использует виртуальный порядковый номер. Он называется виртуальным потому, что его невозможно увидеть в PDU безопасности. Такой подход использует 24-битные счетчики, размещенные в F-хосте (Vconsnr_h) и F-устройстве (Vconsnr_d), а также бит переключатель в байте статуса и байте управления для синхронного приращения надлежащих счетчиков (рисунок 23). Проверка на корректность и синхронность двух независимых счетчиков выполняется включением порядковых номеров при вычислении CRC2. Затем CRC2 передается с каждым PDU безопасности (рисунок 24).

Передаваемая часть (виртуального) порядкового номера сокращена до бита переключателя, который указывает на приращение местного счетчика. Счетчики в F-хосте и F-устройстве увеличиваются при каждом «крайнем» состоянии битов-переключателей (0→1, 1→0). На рисунке 24 показан механизм для счетчика в F-устройстве. Счетчик обнуляется, когда F-хост отправляет R_cons_nr = "1" в байте управления (см. 7.1.3).

Механизм для счетчика в F-хосте соответствует счетчику в F-устройстве. Тем не менее, счетчик обнуляется каждый раз, когда происходит ошибка (внутри или посредством байта статуса). Этот счетчик называется «Vconsnr_h».

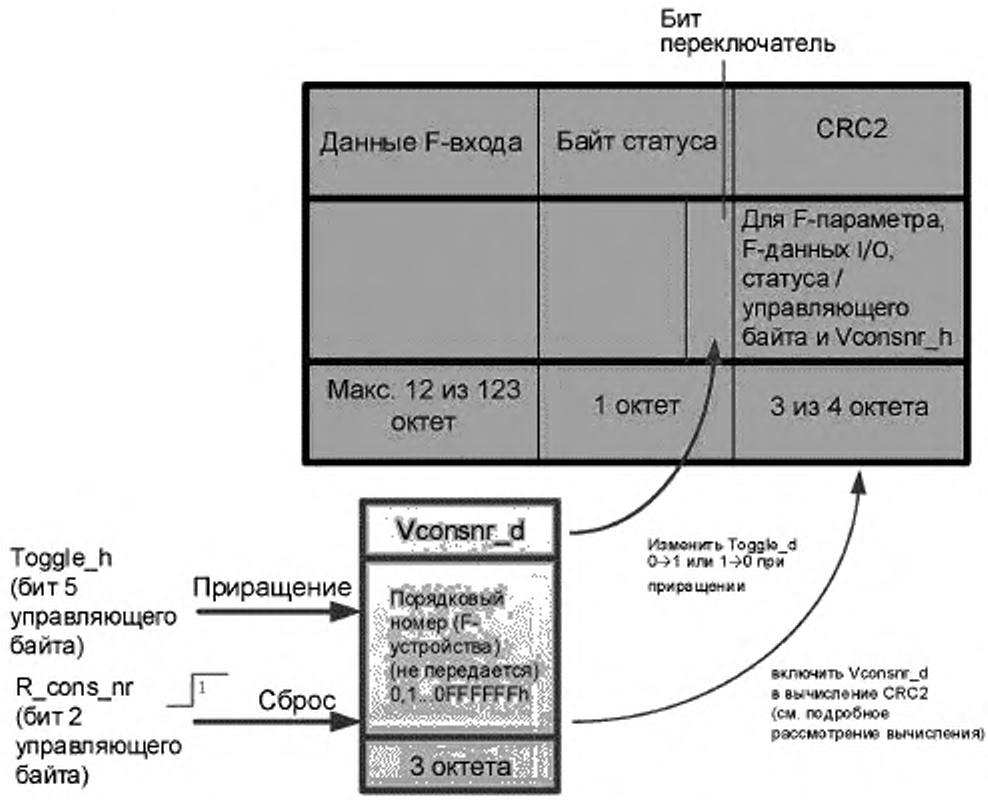


Рисунок 24 — Порядковый номер F-устройства

7.1.5 Сигнатура CRC2

Когда F-параметры (связь источник-назначение или кодовое имя, УПБ, длительности сторожевого таймера и т. п.) передаются F-устройству, те же параметры используются в идентичной процедуре в F-хосте и в F-устройстве/F-модуле для создания CRC1 сигнатуры из двух октетов (верхний октет = 0) (CRC1). См. информацию о построении такого CRC1 в 8.3.3.2. Эта сигнатура CRC1, F-данные I/O, байты статуса и управления и соответствующие порядковый номер (Vconsnr_h или Vconsnr_d) используются для создания другой 3-октетной / 4-октетной сигнатуры CRC2 (*CRC2*) в F-хосте (см. Рисунок 25). Сигнатура CRC1 формирует начальное значение для вычисления CRC2, передающееся циклически. В F-устройстве генерируется идентичная CRC сигнатура и они сравниваются. Последующие циклические передачи требуют только сравнения сигнатур CRC2 (это может выполняться очень быстро).

Любые изменения хранящихся F-параметров должны быть обнаружены и должны приводить к безопасному состояния F-устройства. Механизмы обнаружения зависят от индивидуальной реализации F-устройств и не рассматриваются в настоящем стандарте.

Для лучшего обнаружения ошибок, даже при наличии идентичных CRC полиномов на черном канале и на уровне безопасности, вычисление CRC2 включает в себя октеты рисунка 25 в обратном порядке (рисунок 26). По причинам оптимизации обработки порядковые номера (Vconsnr_h или Vconsnr_d) используются в вычислениях с 4 октетами, дополнительный «заполняющий октет» равен «0». 32-битный счетчик не рекомендуется использовать, так как это может привести к недопустимо длительному тестированию устройств во время процесса тестирования и оценки.

Для того, чтобы предотвратить ситуацию, в которой PDU безопасности несет только значение «0», в данном определенном случае делается исключение: CRC2 устанавливается в значение «1» вместо значения «0».

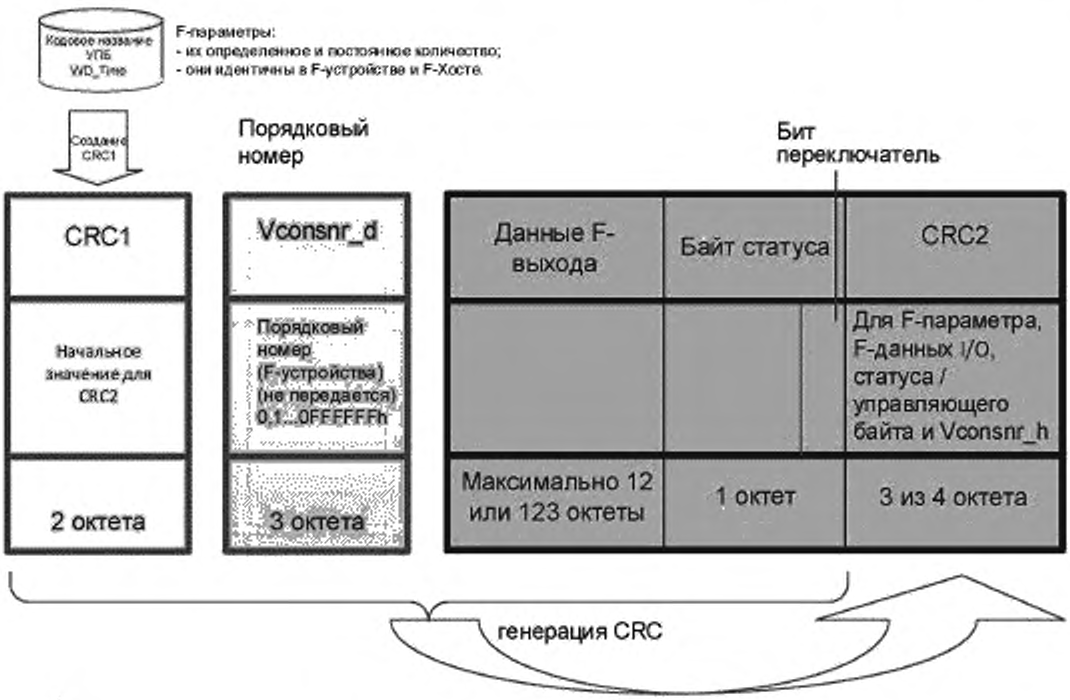


Рисунок 25 — Генерация CRC2 (вывод F-хоста)

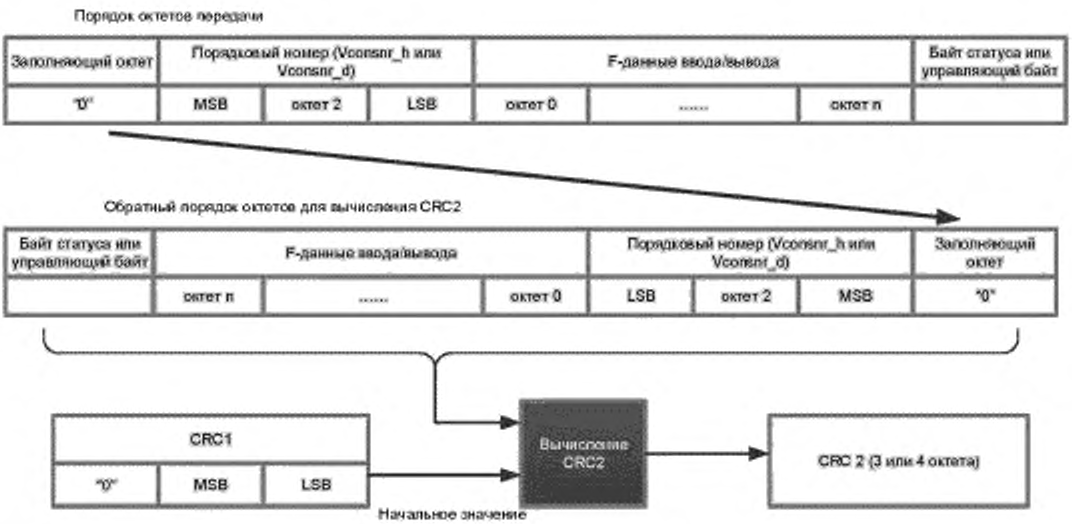


Рисунок 26 — Подробности вычисления CRC2 (обратный порядок)

7.1.6 Добавляемые стандартные данные I/O

Стандартные данные I/O могут быть добавлены к PDU безопасности. Для малогабаритных F-устройств это может быть достигнуто размещением раздельных идентификаций слотов. F-модули в модульных устройствах способны использовать этот механизм в CP 3/RTE по причине моделирования подслота.

7.2 Поведение FSCP 3/1

7.2.1 Общие положения

Ядро уровней безопасности в F-хосте и F-устройстве состоит в каждом случае из конечного автомата, режимы функционирования которого определены диаграммами состояний и диаграммами последовательностей в 7.2.2 и 7.2.3. На рисунке 27 показана упрощенная модель коммуникаций безопасности. Специальная временная диаграмма в 7.2.5 демонстрирует последствия сбоя сигнала обнуления для счетчика порядкового номера. Контроль времени передачи PDU безопасности описан в 7.2.6.

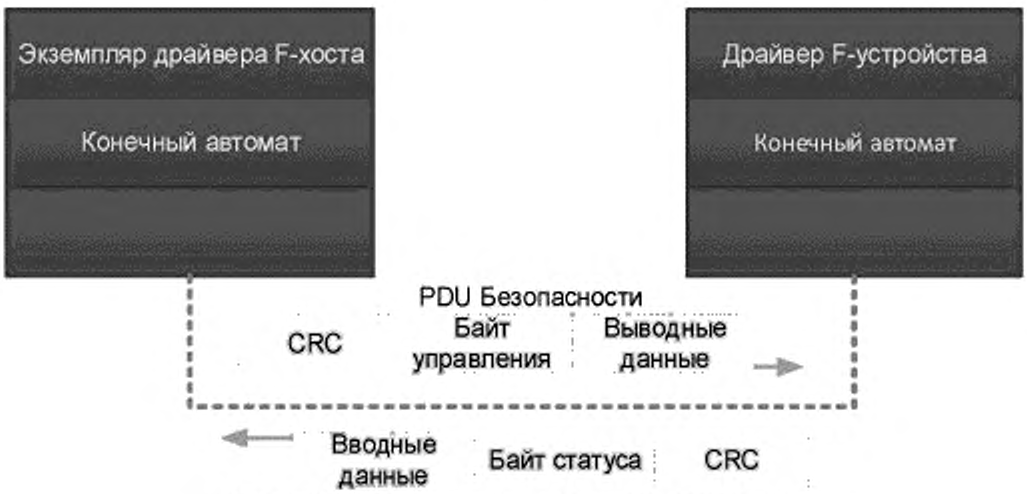


Рисунок 27 — Коммуникационная связь уровня безопасности

7.2.2 Диаграмма состояний F-хоста

На рисунке 28 показана диаграмма состояний F-хоста, а таблица 4 описывает состояния, переходы и внутренние элементы F-хоста. Диаграммы следуют нотации UML2. Переходы активируются в случае события, например, принятия сообщения. В случае нескольких возможных переходов так называемые ограничители [условия] определяют какой переход запустить.

Состояния 4, 7 и 10 (Check Device Ack, т. е. подтверждение проверки устройства) являются так называемыми состояниями изменения, согласно UML2 без «внешнего» события. Соответствующие переходы запускаются после оценки внутренних значений.

Диаграмма состоит из состояний деятельности и действия. Состояния деятельности обведены полужирными линиями, состояния действий — тонкими линиями. Состояния деятельности могут быть прерваны новыми событиями, но это не так для состояний действий. События в рамках состояния действия, такие как, таймауты, полученные сообщения или подтверждения оператора откладываются до достижения следующего состояния деятельности.

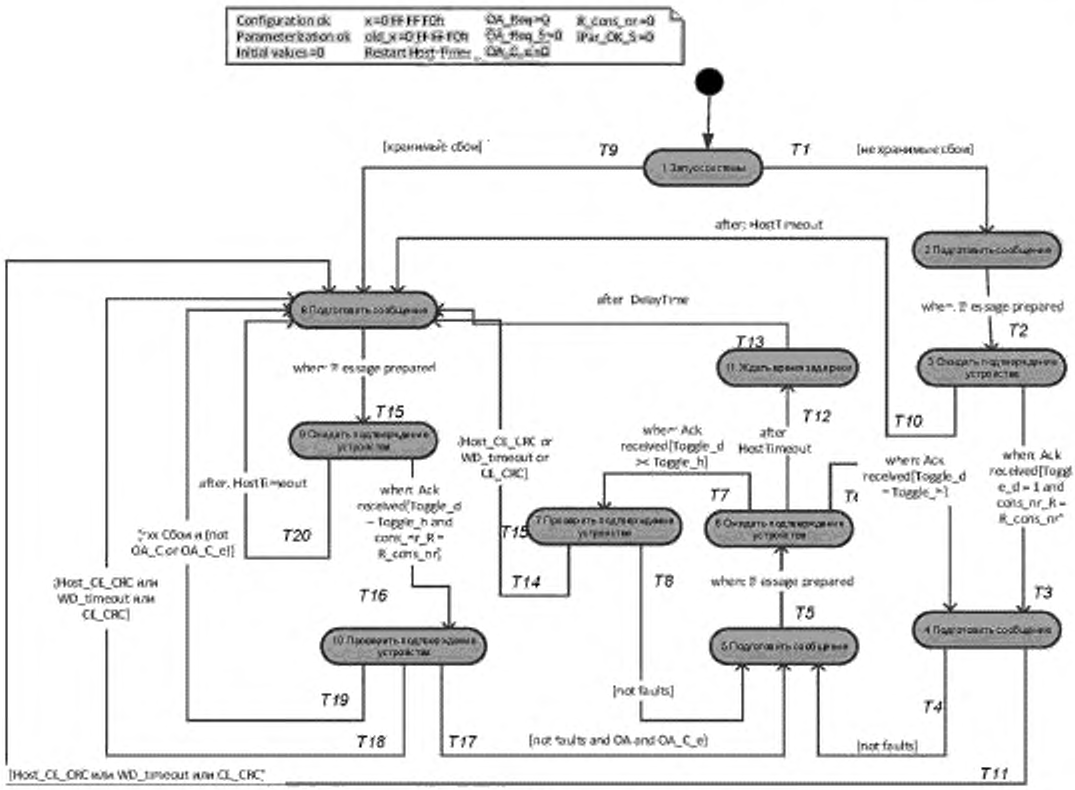


Рисунок 28 — Диаграмма состояний F-хоста

Термины, используемые на рисунке 28, описаны ниже:

Начальные значения — Любые значения PDU безопасности равные «0»;

HostTimeout — F-хост распознает локальный таймаут, ожидая подтверждения F-устройства;

Host_CE_CRC — F-хост распознает сбой CRC, анализируя принятый PDU безопасности;

Device_Fault — F-устройство доложило хосту об отказе; бит статуса = 1;

CE_CRC — F-устройство доложило о CRC сбое F-хосту; Бит Статуса 2 = 1;

OA_C_e — Вспомогательный флаг, указывающий на нарастающий фронт сигнала OA_C (0→1);

WD_timeout — F-устройство доложило о сбое таймаута F-Хосту; Бит Статуса 3 = 1;

[не сбои] — Нотация UML для условия (ограничителя) для запуска перехода. В данном случае данная переменная истинна (1), если не установлены никакие из следующих битов:
- Host_CE_CRC или
- CE_CRC или
- WD_timeout;

[хранимые сбои] — Эта переменная истинна (1), если любые из следующих битов были помещены в хранилище:
- Host_CE_CRC или
- HostTimeout or
- CE_CRC or
- WD_timeout.

Таблица 4 — Состояния и переходы F-хоста

НАЗВАНИЕ СОСТОЯНИЯ	ОПИСАНИЕ СОСТОЯНИЯ
1 System Start (Запуск системы)	Начальное состояние экземпляра драйвера F-хоста при подключении питания. Если система спроектирована для хранения сбоев, то должен быть реализован переход T9. В противном случае система использует только переход T1
2 Prepare message (Подготовить сообщение)	Подготовка *регулярного* PDU безопасности для F-устройства
3 Await Device Ack (Ожидать подтверждение устройства)	Уровень безопасности ожидает новый регулярный PDU от F-устройства (подтверждение)
4 Check Device Ack (Проверить подтверждение устройства)	Проверка принятого PDU безопасности на наличие CRC-ошибки (Host_CE_CRC), включая виртуальный порядковый номер (x) и на возможные *сбои F-устройства* в байте статуса (WD_timeout, CE_CRC)
5 Prepare message	Подготовка *регулярного* PDU безопасности для F-устройства
6 Await Device Ack	Уровень безопасности ожидает новый регулярный PDU от F-устройства (подтверждение)
7 Check Device Ack	Проверка принятого PDU безопасности на наличие CRC-ошибки (Host_CE_CRC), включая предыдущий (old_x) виртуальный порядковый номер (x) и на возможные *сбои F-устройства* в байте статуса (WD_timeout, CE_CRC)
8 Prepare message	Подготовка *регулярного* PDU безопасности для F-устройства (обработка исключений)
9 Await Device Ack	Уровень безопасности ожидает новый нестандартный PDU от F-устройства (подтверждение)
10 Check Device Ack	Проверка принятого PDU безопасности на наличие CRC-ошибки (Host_CE_CRC), включая виртуальный порядковый номер (x) и на возможные *сбои F-устройства* в байте статуса (WD_timeout, CE_CRC). После того как произошел сбой, никакой автоматический перезапуск функции безопасности не разрешен пока не будет получен сигнал подтверждения оператора (OA_C)
11 wait delay time (ждать время задержки)	Это состояние для того, чтобы избежать хранения сбоя таймаута в случаях периодического отключения системы, которое привело бы к формированию запроса на подтверждение оператора (operator acknowledge) при следующем подключении питания. Разрешено время задержки равное 0 мс

Продолжение таблицы 4

ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T1	1	2	использовать FV, activate_FV =1, FV_activated_S =1 Toggle_h =1
T2	2	3	отправить PDU безопасности
T3	3	4	перезапустить хост-таймер
T4	4	5	old_x =x, x =x+1, **if** x =01000000h **then** x =1 Toggle_h = not Toggle_h, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T5	5	6	отправить PDU безопасности

Продолжение таблицы 4

ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T6	6	4	перезапустить хост-таймер
T7	6	7	-
T8	7	5	**if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK
T9[a)]	1	8	use FV, activate_FV =1, FV_activated_S =1, Toggle_h =1, R_cons_nr =1, x =0
T10	3	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T11	4	8	store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T12	6	11	use FV, activate_FV =1, FV_activated_S =1, R_cons_nr =1, x =0
T13	11	8	store faults, Toggle_h = not Toggle_h, restart host-timer
T14	7	8	restart host-timer, store faults, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T15	8	9	отправить PDU безопасности
T16	9	10	перезапустить хост-таймер
T17	10	5	reset stored faults, OA_Req_S =0, OA_Req =0, OA_C_e =0, R_cons_nr =0, old_x =x, x =x+1, **if** x =01000000h **then** x =1 Toggle_h = not Toggle_h, **if** FV_activated =1 or activate_FV_C =1 or Device_Fault =1 **then** use FVi, FV_activated_S =1 **else** use PVi, FV_activated_S =0 **if** activate_FV_C =1 or Device_Fault =1 **then** use FVo, activate_FV =1 **else** use PVo, activate_FV =0 iPar_OK_S =iPar_OK

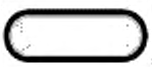
Продолжение таблицы 4

ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T18	10	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0
T19	10	8	OA_Req_S =1, OA_Req =1, **if** OA_C =0 **then** OA_C_e =1 use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =0, old_x =x, x =x+1, **if** x =01000000h **then** x =1
T20	9	8	store faults, OA_Req =0, OA_Req_S =0, OA_C_e =0, use FV, activate_FV =1, FV_activated_S =1, Toggle_h = not Toggle_h, R_cons_nr =1, x =0, restart host-timer
[a] Реализация перехода T9 зависит от концепции проекта безопасности определенного производителя системы.			

Продолжение таблицы 4

ВНУТРЕННИЕ ЭЛЕМЕНТЫ	ТИП	ОПРЕДЕЛЕНИЕ
x	Счетчик	x представляет собой местный порядковый номер в экземпляре драйвера F-хоста. Он не передается своим аналогам в F-устройстве, но синхронизируется с ними посредством бита переключателя в байте управления. Действительное значение счетчика x включено в вычисление CRC2 и потому проверяется на сбои передачи. Диапазон значений — 0 … 0FFFFFFh. Во время запуска этот суммирующий счетчик установлен в значение 0FFFFF0h и начинает отсчет от него. F-хост дает приращение виртуальному порядковому номеру после каждого подтвержденного принятия соответствующего виртуального порядкового номера модуля 0FFFFFFh F-устройства этого хоста, пропуская значение «0» и продолжая с «1»
old_x	Счетчик	Предыдущее значение текущего местного порядкового номера x. Необходимо хранить предыдущее значение порядкового номера для того, чтобы отличать начальный цикл от более поздних циклов
DelayTime	Таймер	Это время задержки предназначено для того, чтобы охватить время регулирования отключения питания во всей системе. Ответственность по определению этого параметра лежит на производителе хоста/системы
host-timer	Таймер	Данный таймер проверяет, прибыл ли вовремя следующий действительный PDU безопасности, поступивший от F-устройства. Инженерный инструмент хоста ответственен за установление времени сторожевого таймера. Диапазон значений — 0 … 65 535 мс
OA_C_e	Флаг	Эта вспомогательная переменная (двоичная) гарантирует то, что безопасное состояние завершается только после смены сигнала OA_C с 0→1 (фронт). Без этого механизма оператор мог бы аннулировать безопасные состояния посредством безвозвратной активации сигнала OA_C

Окончание таблицы 4

ВНУТРЕННИЕ ЭЛЕМЕНТЫ	ТИП	ОПРЕДЕЛЕНИЕ
faults	Флаги	До подтверждения оператора (OA_C), в F-хосте (только в F-Хосте, не требуется от F-устройства) требуется постоянное хранение следующих сбоев: - Host_CE_CRC - HostTimeout - CE_CRC (бит статуса 2) - WD_timeout (бит статуса 3)
	Состояние деятельности	В рамках этих прерываемых состояниях «деятельности» хост ждет новых входных данных таких как таймаут или подтверждение [34]
	Состояние действия	В рамках этих непрерываемых состояний «действия», события, например, таймаут, полученное сообщение или подтверждение оператора откладываются до тех пор, пока не наступит следующее состояние «действия» [34]

7.2.3 Диаграмма состояний F-устройства

На рисунке 29 показана диаграмма состояний F-устройства, а таблица 5 описывает состояния, переходы и внутренние элементы. Диаграммы следуют нотации UML2.

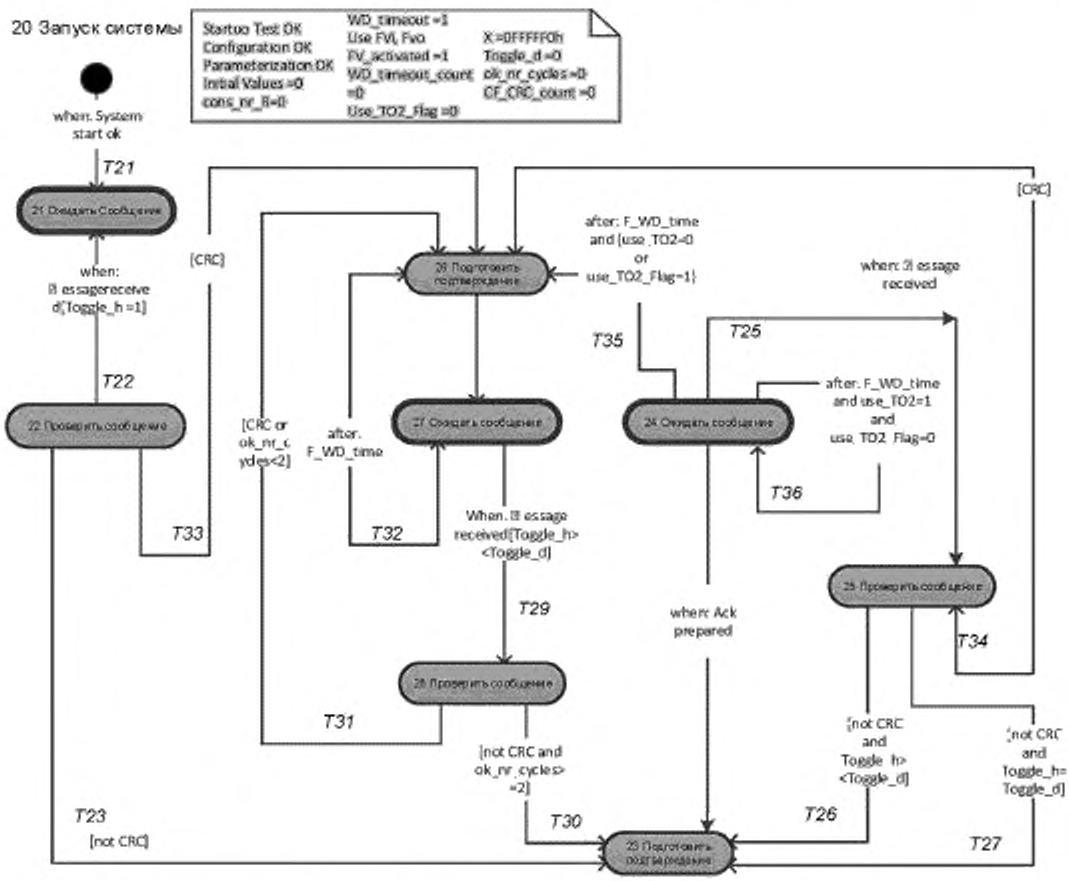


Рисунок 29 — Диаграмма состояний F-устройства

Термины, используемые на рисунке 29, определены ниже:

[Toggle_h = Toggle_d] — нотация UML условия (ограничителя) для запуска перехода. В этом случае это означает, что бит Toggle_h не изменил свое значение («не переключен»);

[Toggle_h >< Toggle_d] — бит Toggle_h изменил свое значение («переключен»);

[CRC] — F-устройство распознает сбой CRC (ошибка коммуникаций и/или порядкового номера);

F_WD_Time — время сторожевого таймера, определенное F-параметром «F_WD_Time»;

use_TO2 — СВ3 в байте управления, указывающий на использование времени вспомогательного сторожевого таймера F_WD_Time2;

use_TO2_Flag — вспомогательный флаг;

Ack — PDU безопасности для подтверждения F-устройства;

Message received — любой новый принятый PDU безопасности; следует игнорировать PDU безопасности, где все значения равны 0.

Таблица 5 — Состояния и переходы F-устройства

НАЗВАНИЕ СОСТОЯНИЯ			ОПИСАНИЕ СОСТОЯНИЯ
20 System Start (Запуск системы)			Начальное состояние устройства при подключении питания. При подключении питания F-устройство *вывода* устанавливает значение «0». Сразу же после F-параметризации оно устанавливает отказоустойчивые значения. При подключении питания F-устройство *ввода* отправляет значение «0». Сразу же после F-параметризации оно отправляет значения процесса
21 Await message (Ожидать сообщение)			Уровень безопасности ожидает новый PDU от F-устройства
22 Check Message (Проверить сообщение)			Проверка принятого PDU безопасности на наличие *CRC-ошибки*, включая виртуальный порядковый номер
23 Prepare Ack (Подготовить подтверждение)			Подготовка *регулярного* PDU безопасности для F-устройства (Подтверждение)
24 Await message			Уровень безопасности ожидает следующий регулярный PDU безопасности от F-устройства
25 Check Message			Проверка принятого PDU безопасности на наличие *CRC-ошибки*, включая виртуальный порядковый номер
26 Prepare Ack			Подготовка *регулярного* PDU безопасности для F-устройства (Подтверждение с битами сбоев)
27 Await Message			Уровень безопасности ожидает следующий PDU безопасности от F-устройства (обработка исключений)
28 Check Message			Проверка принятого PDU Безопасности на наличие *CRC-ошибки*, включая виртуальный порядковый номер
ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T21	20	21	-
T22	21	22	**if** R_cons_nr =1 **then** x=0, cons_nr_R =1
T23	22	23	use PVi, FVo, FV_activated =1, CE_CRC =0, WD_timeout =0, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T24	23	24	send safety PDU

Продолжение таблицы 5

ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T25	24	25	**if** Toggle_h >< Toggle_d **then** restart device-timer x=x+1, **if** x =01000000h **then** x =1, cons_nr_R =0 **if** R_cons_nr =1 **then** x=0, cons_nr_R =1 **if** use_TO2 =0 **then** use_TO2_Flag =0
T26	29	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 ok_nr_cycle =ok_nr_cycle +1 **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo
T27	25	23	Use PVi, Toggle_d = Toggle_h, **if** ok_nr_cycles <4 **then** use FVo, FV_activated =1 **else** use PVo, FV_activated =0 **if** activate_FV =1 **then** use FVo **else** use PVo
T28	26	27	Send safety PDU
T29	27	28	**if** R_cons_nr =1 **then** x=0, cons_nr_R =1 **else** x=x+1, **if** x =01000000h **then** x =1, cons_nr_R =0
T30	28	23	use PVi, FVo, FV_activated =1, Toggle_d = Toggle_h, restart device-timer, ok_nr_cycles =ok_nr_cycles +1
T31	28	26	Toggle_d = Toggle_h, restart device-timer, **if** CRC **then** CE_CRC =1, CE_CRC_count =1, ok_nr_cycles =0, **else** ok_nr_cycles =ok_nr_cycles +1, **if** CE_CRC_count >0 **then** CE_CRC =1, CE_CRC_count = CE_CRC_count -1, **else** CE_CRC =0, **if** WD_timeout_count >0

Продолжение таблицы 5

ПЕРЕХОД	СОСТОЯНИЕ ИСТОЧНИКА	СОСТОЯНИЕ ЦЕЛИ	ДЕЙСТВИЕ
T31	28	26	**then** WD_timeout =1, WD_timeout_count = WD_timeout_count -1 **else** WD_timeout =0
T32	27	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T33	22	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, WD_timeout =0, ok_nr_cycles =0, restart device-timer, Toggle_d = Toggle_h
T34	25	26	Use PVi, FVo, FV_activated =1, CE_CRC =1, CE_CRC_count =1, ok_nr_cycle =0, restart device-timer, Toggle_d = Toggle_h
T35	24	26	Use PVi, FVo, FV_activated =1, WD_timeout =1, WD_timeout_count =1, ok_nr_cycles =0, restart device timer, Toggle_d = Toggle_h
T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1
[a] Реализация перехода T9 зависит от концепции проекта безопасности определенного производителя системы.			
ВНУТРЕННИЕ ЭЛЕМЕНТЫ		ТИП	ОПРЕДЕЛЕНИЕ
x		Счетчик	x представляет собой реальный локальный порядковый номер в F-устройстве. Он не передается своим аналогам в F-хосте, но синхронизируется с ними посредством бита переключателя в байте управления. Это означает, что x увеличивается каждый раз, когда бит переключатель в байте управления изменяет свое состояние с 0→1 или с 1→0, вычисляя модуль 0 FF FF FFh, пропуская значение «0» и продолжая с «1». Значение счетчика x обнуляется в случае, если установлен бит управления «R_cons_nr», т. е. имеет значение (1). Соответствующее значение счетчика x включено в вычисление CRC2 и потому проверяется на сбои передачи. Диапазон значений 0 … 0 FF FF FFh. Во время запуска этот счетчик установлен в значение 0 FF FF F0h и начинает отсчет от него
ok_nr_cycles		Счетчик	Во время запуска и после сбоя, F-устройство должно устанавливать FVo и FV_activated=1 на протяжении минимум 3 циклов. Подсчитать эти циклы от 1 до 3 является задачей данного суммирующего счетчика
CE_CRC_count		Счетчик	Этот счетчик обратного отсчета используется для обеспечения установки бита «CE_CRC» в байте статуса минимум на 1 цикл или максимум на 2. Диапазон значений 0 - 1

Окончание таблицы 5

ВНУТРЕННИЕ ЭЛЕМЕНТЫ	ТИП	ОПРЕДЕЛЕНИЕ
WD_timeout_count	Счетчик	Этот счетчик обратного отсчета используется для обеспечения установки бита «WD_timeout» в байте статуса минимум на 1 цикл или максимум на 2. Диапазон значений 0 —1
device-timer	Таймер	Данный таймер проверяет, поступил ли следующий действительный PDU безопасности вовремя. FПараметр «F_WD_Time» используется для определения времени сторожевого таймера. Диапазон значений 0 … 65 535 мс

7.2.4 Диаграммы последовательностей

Рисунки 30 — 33 демонстрируют сообщения взаимодействия F-хоста и F-устройства, которыми они обмениваются в течении стадии запуска. Рассмотрены три стадии: оба партнера во время запуска, F-хост или F-устройство временно отключают питание в то время как один из них по-прежнему функционирует. Рисунки содержат информацию о состояниях и соответствующих переходах. Числа в кружках представляют состояния, через которые проходят соответствующие F-хост и F-устройство.

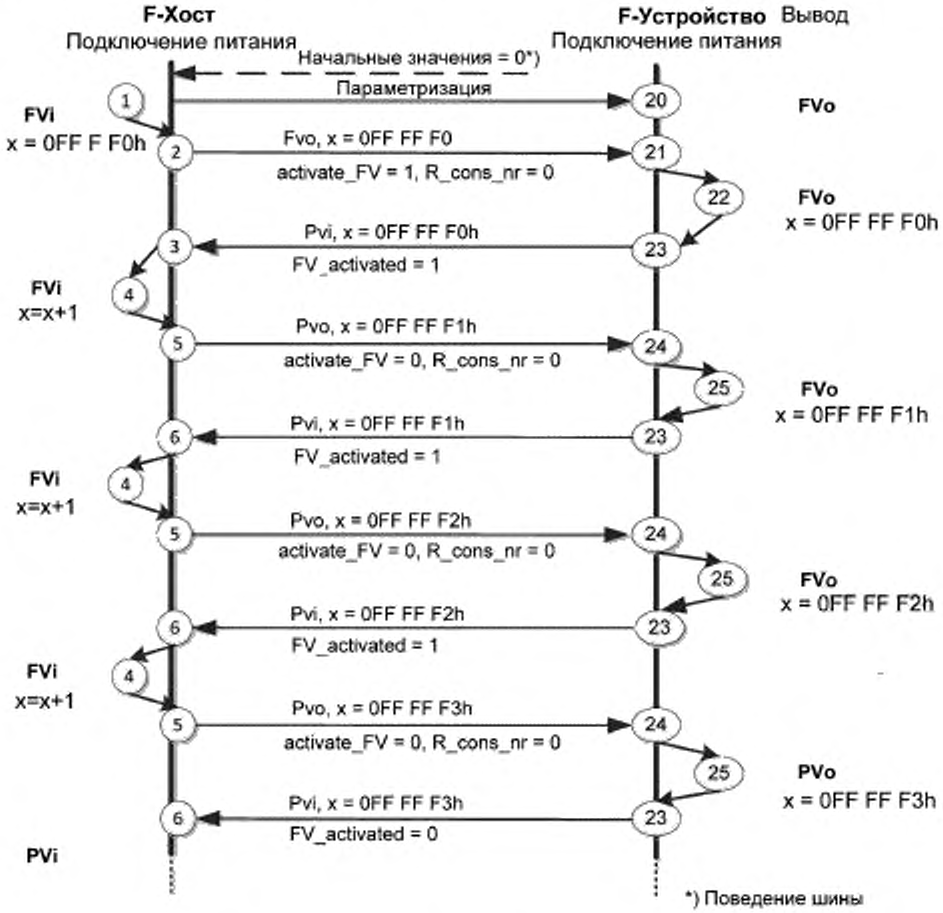


Рисунок 30 — Взаимодействие F-хоста / F-устройства во время запуска

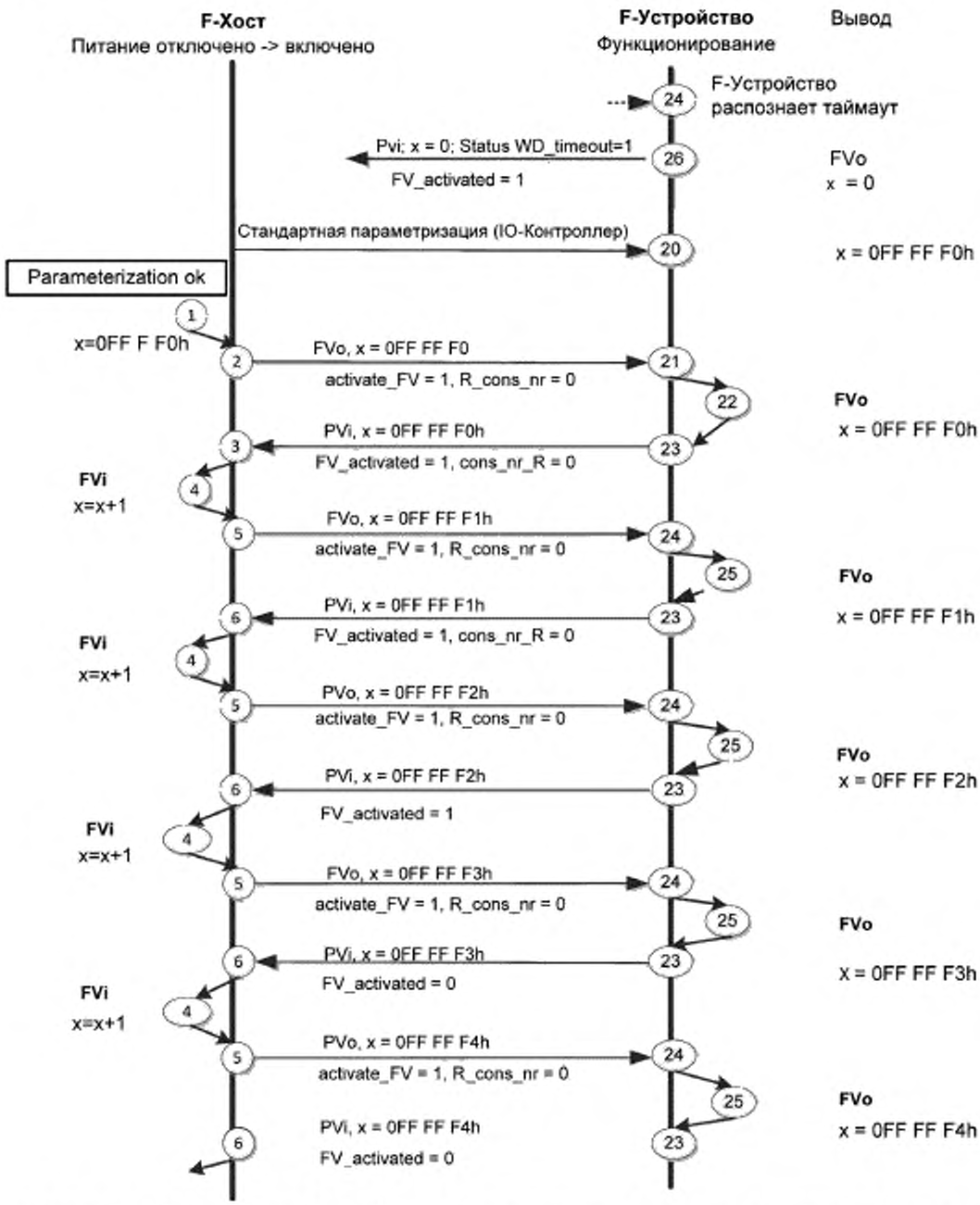


Рисунок 31 — Взаимодействие F-хоста / F-устройства во время отключения→ включения питания F-хоста

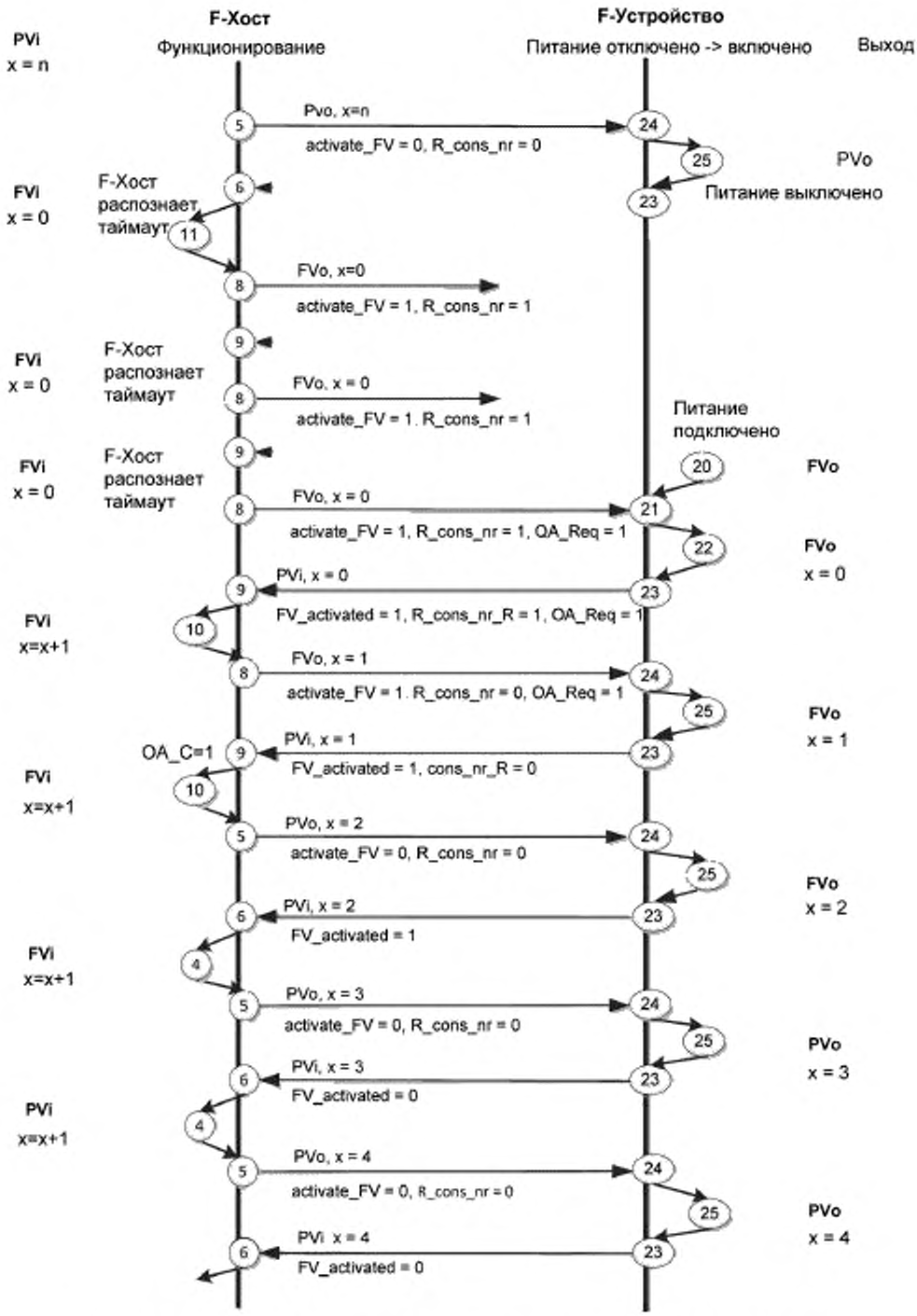


Рисунок 32 — Взаимодействие F-хоста / F-устройства с задержкой включения питания

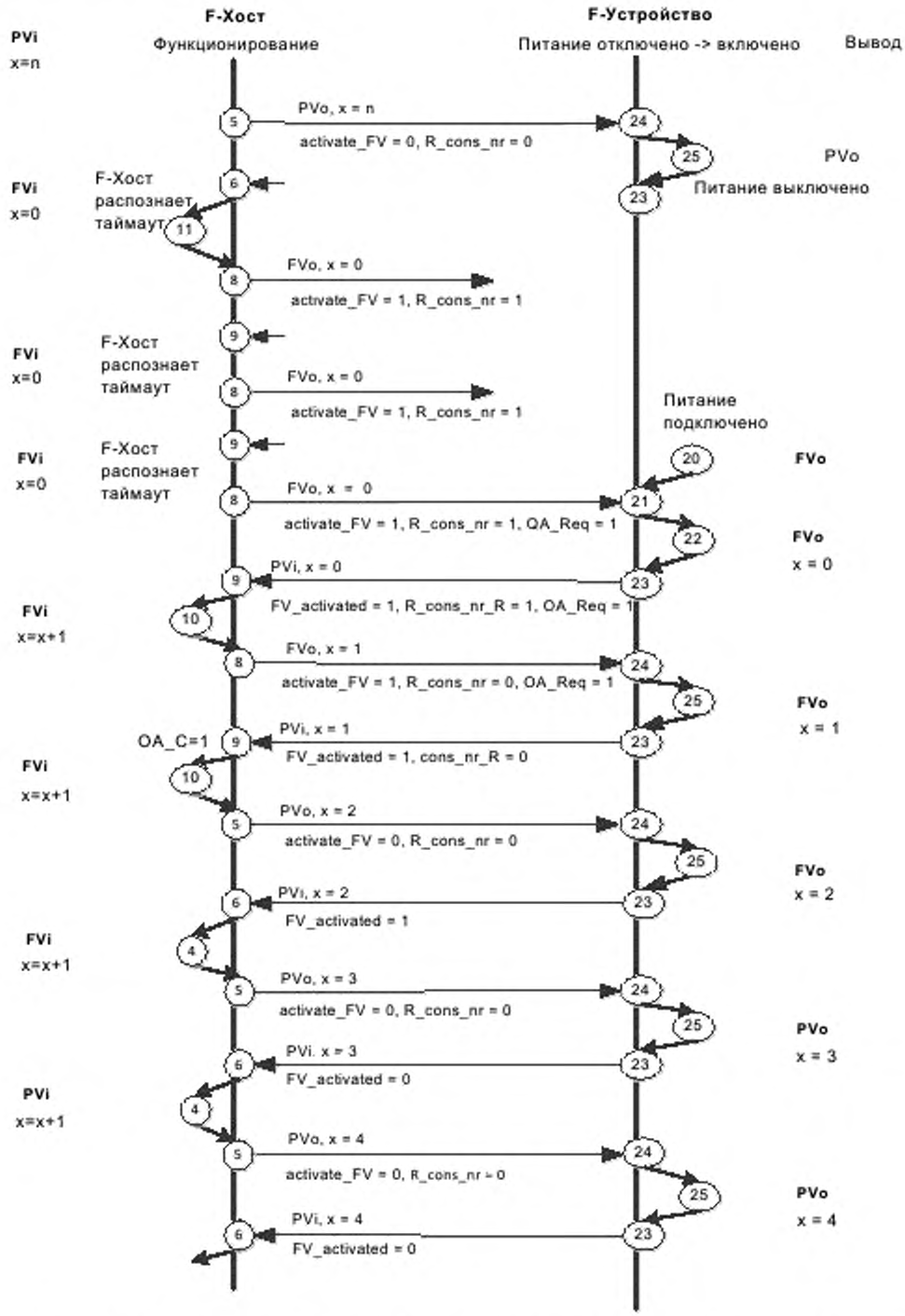


Рисунок 33 — Взаимодействие F-хоста / F-устройства во время отключения→ включения питания

Рисунки 34 и 35 демонстрируют сообщения взаимодействия между F-хостом и F-устройством, в то время как CRC сбои обнаруживаются на каждой стороне взаимодействия.

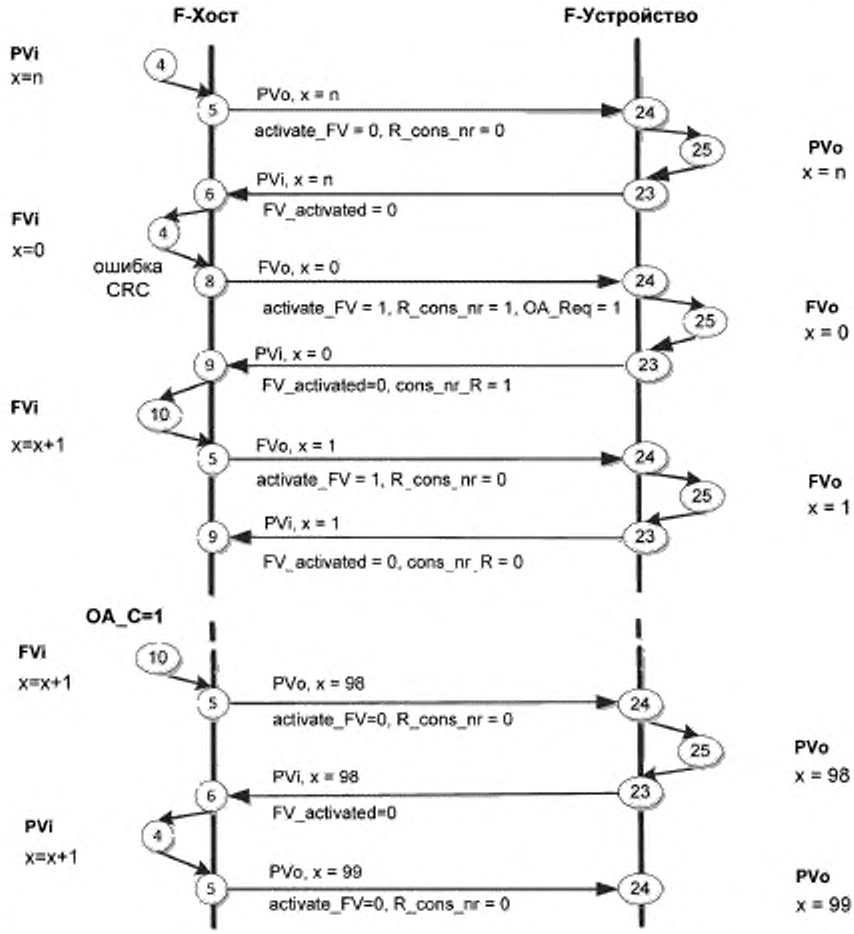


Рисунок 34 — Взаимодействие F-хост / F-устройство, в то время как хост распознает CRC ошибку

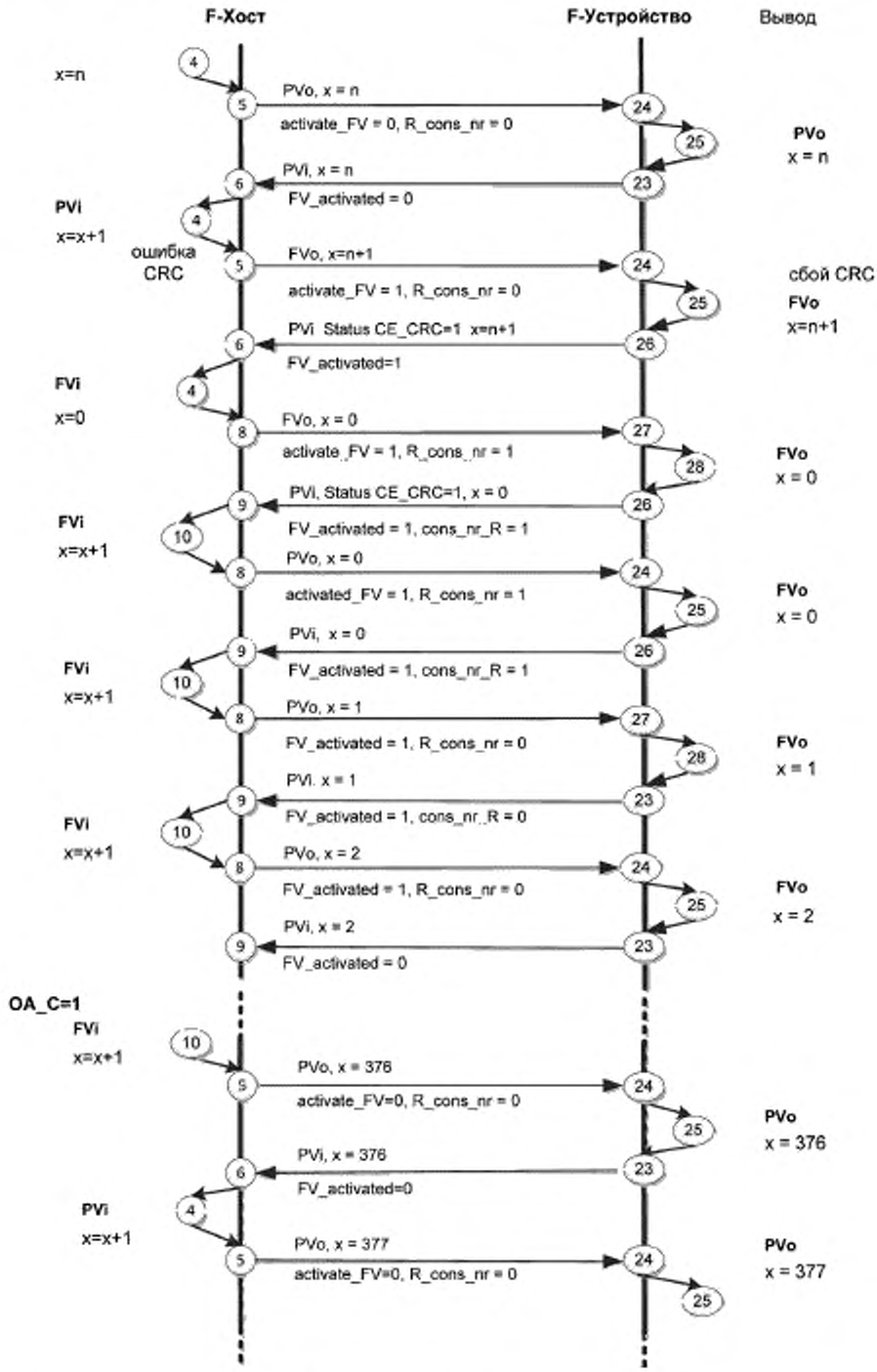


Рисунок 35 — Взаимодействие F-хост / F-устройство, в то время как устройство распознает CRC ошибку

7.2.5 Временная диаграмма для обнуления счетчика

На рисунке 36 показаны последствия сбоя F коммуникаций, произошедшего на счетчике порядкового номера и зависящих от него объектов. Только по происшествию подобного сбоя устанавливается (=1) бит 2 в байте управления "R_cons_nr" и в результате выходные значения F-устройства-вывода устанавливаются в значение «0», а счетчик порядкового номера устанавливается в «0» (Vconsnr_d). В то же время устанавливается в (1) бит 4 «activate_FV» байта управления, тем самым вынуждая F-устройство-вывода настроить свое собственной отказоустойчивое состояние, что делается всякий раз, когда это состояние не может быть достигнуто с помощью обычных значений вывода (FV).

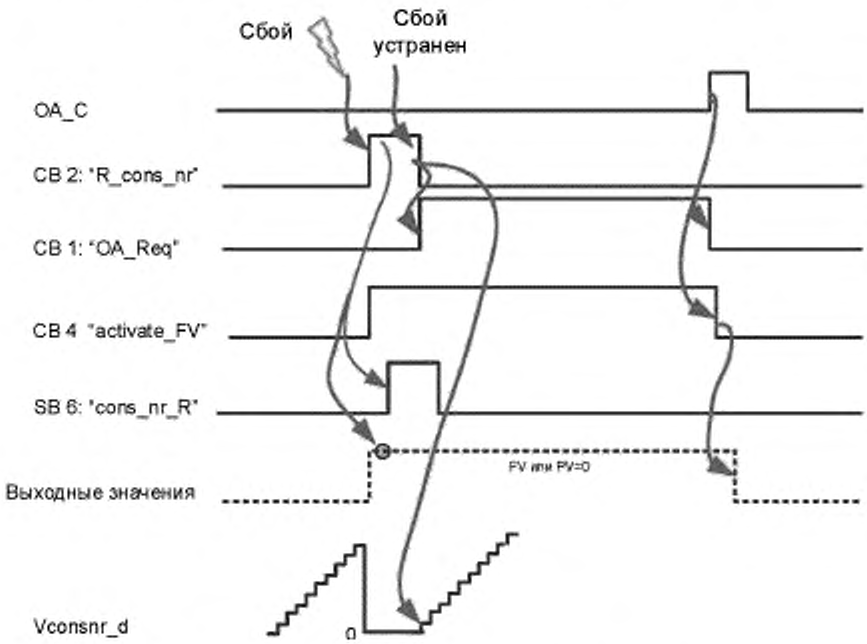


Рисунок 36 — Влияние сигнала сброса счетчика

Тем временем F-хост отправляет F-устройству сигнал «OA_Req» в виде бита 1 байта управления. Этот сигнал может быть использован для того, чтобы указать пользователю посредством светодиода (9.1) на то, что произошла ошибка и запрошено подтверждение оператора (OA_C). Как только сбой устранен, принимаются следующие действия:

- счетчик сброса восстанавливает свое значение по умолчанию (R_cons_nr = 0);
- счетчик порядкового номера продолжает вести отсчет.

Сразу после подтверждения оператора (OA_C = 1) выполняются следующие действия:

- запрос на подтверждение оператора восстанавливает свое значение по умолчанию (OA_Req = 0);
- запрос на активацию состояния отказоустойчивого вывода восстанавливает свое значение по умолчанию (activate_FV = 0);
- выходные значения процесса появляются снова после трех циклов сообщений.

7.2.6 Контроль времен безопасности

7.2.6.1 Нормальное функционирование

На рисунке 37 показано, как F драйвер использует лежащие в основе коммуникации CP 3/RTE и как определяются отдельные времена для контроля. Короткие стрелки означают: в CP 3/RTE IO-контроллер отправляет то же самое PDU безопасности F-устройству более часто, чем новый PDU безопасности генерируется F-драйвером в рамках времени цикла хоста в F-хосте (порядковый номер = n+1). В ответ F-устройство отправляет PDU безопасности (подтверждение) IO-контроллеру более часто, чем F-драйвер в F-устройстве генерирует новый PDU безопасности.

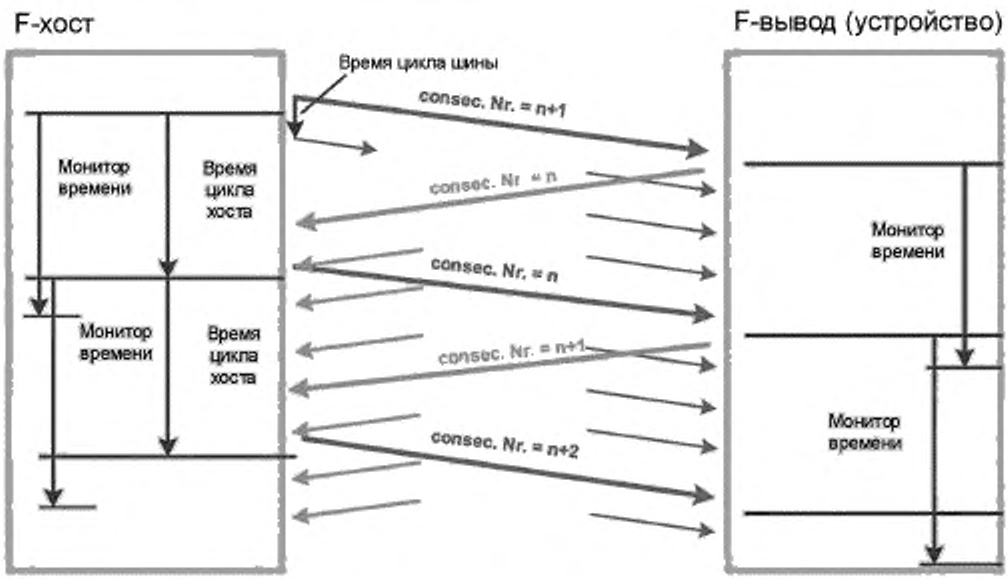


Рисунок 37 — Контроль времени передачи сообщения для передачи F-хост ↔ F-вывод

На рисунке 37 показан контроль времени в F-хосте и F-устройстве вывода. На рисунке 38 показан контроль времени в F-устройстве ввода и F-Хосте. Короткие стрелки на рисунках представляют PDU FSCP 3/1 с подтвержденным на данный момент (виртуальным) порядковым номером, но, вероятно, с различными значениями процесса.

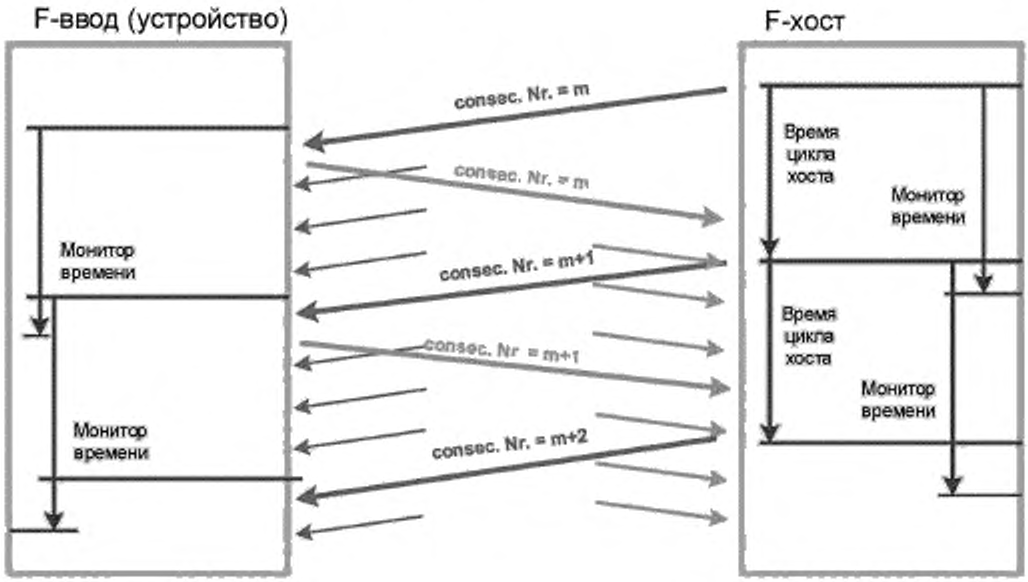


Рисунок 38 — Контроль времени передачи сообщения для передачи F-ввод ↔ F-хост

Другие временные ограничения перечислены ниже:

Запуск (Синхронизация)
Синхронизацию после запуска системы, драйвер F-хоста начинает с порядкового номера «0FFFFF0h». Затем, F-хост увеличивает виртуальный порядковый номер после каждого подтвержденного получения соответствующего виртуального порядкового номера модуля «0FFFFFFh» F-устройства данного хоста, пропуская значение «0» и продолжая с «1». В последний момент перед истечением времени контроля F-ввод/F-вывод ожидает сообщение, содержащее виртуальный порядковый номер, увеличенный на 1. F-вывод предоставляет отказоустойчивые значения (FVo) после того, как получает виртуальный порядковый номер равный «0».

Цикл F-протокола
F-ввод/F-вывод возвращает PDU безопасности F-хосту, содержащее тот же виртуальный порядковый номер (цикл F-протокола) для подтверждения принятия PDU безопасности.
Время цикла F-хоста не должно превышать время цикла F-протокола (но оно может быть короче).

Устройство контроля (монитор) времени (Сторожевой таймер)
Поступление на F-устройство нового корректного PDU безопасности в рамках времени сторожевого таймера контролируется. Подобная верификация может быть выполнена так часто, как это необходимо, но как минимум однажды в конце интервала времени, предназначенного для контроля. Когда время сторожевого таймера истекает, связанный с ним получатель переключается на безопасное состояние.
Самый медленный цикл CP 3/RTE не должен превышать *половины* времени сторожевого таймера. Время цикла F-хоста может быть короче, чем время сторожевого таймера.

Контроль порядкового номера
Новый корректный PDU безопасности характеризуется фактом того, что хотя бы виртуальный порядковый номер был увеличен на 1 и что либо вся остальная часть PDU безопасности целиком не претерпела изменений, либо изменения не привели к сбоям. Это означает, что неверное изменение виртуального порядкового номера прибавлением 1 прямо распознается посредством CRC2. Что в свою очередь приведет к реакции на сбой.

Повторение PDU безопасности
Повторение полноценного PDU безопасности в случае, когда новый корректный PDU безопасности не был получен за время сторожевого таймера, не поддерживается.

Устройство контроля УПБ
Каждое искаженное сообщение (сбоем CRC и виртуального порядкового номера) будет подсчитано за временной период конфигурируемого устройства контроля УПБ (T). Отказоустойчивые значения устанавливаются каждый раз, когда произошло более одного такого сбоя, т.е. одно обнаруженное искаженное сообщение может допускаться (*вариант A*). Случаи, когда целый PDU телеграммы = «0» (например, при запуске), не должны учитываться.
На практике может быть продемонстрировано, что в действительности подсчет всегда остается нулевым. Это служит причиной для оптимизации сложности, приводящей к *варианту B*, в котором время контроля УПБ (T) установлено как бесконечное. В таком случае, упрощенная диаграмма состояний F-хоста на рисунке 28 должна учитываться там, где любое искаженное обнаруженное сообщение не допускается и всегда ведет к состоянию безопасности.
Каждый раз, когда подобное маловероятное событие обнаруженного искаженного сообщения должно произойти во время сдвига производства или операции, то на роль УПБ-устройства контроля (монитора) назначается ответственный оператор, который может допустить индикацию такого события и подтвердить ее. Тем не менее, при любой последующей индикации в рамках того же сдвига, следует предполагать серьезную причину этой индикации, требующую немедленной починки или устранения.
Реализация варианта A лежит на производителе F-хоста. Тем не менее, подробная реализация не рассматривается в настоящем стандарте, ради пользы индивидуальных адаптаций этого варианта под определенные системные среды. Устройство контроля УПБ должно реализовываться только в F-хосте.

Период времени устройства контроля (T)

Временной период *T* устройства контроля УПБ является постоянным измеряемым в часах (h) значением, которое формируется из запрошенного УПБ и длинны сконфигурированного CRC (9.5.1). В таблице 6 установлены времена устройства контроля УПБ.

Таблица 6 — Временные периоды *T* устройства контроля УПБ

УПБ	CRC	Длина PDU безопасности	Временной период (h)
3	24 бита	≤ 16 октетов	>10
2	24 бита	≤ 16 октетов	>1
3	32 бита	≤ 128 октетов	>10
3	32 бита	≤ 128 октетов	>1

7.2.6.1 Расширенное время сторожевого таймера по запросу после взаимодействия с пользователем

Для таких случаев использования, как «конфигурирование во время выполнения» [69] или «техническое обслуживание устойчивых к сбоям систем», требуется определенное время для обновления затронутых устройств. Это время обновления, как правило, дольше, чем обычное основное время сторожевого таймера (F_WD_Time), заданное для приложения безопасности. Для того чтобы избежать ложные срабатывания, драйвер F-хоста может один раз использовать время вспомогательного сторожевого таймера (F_WD_Time_2) для расширения основного времени сторожевого таймера для этих запланированных и контролируемых событий, как это показано на рисунке 39.

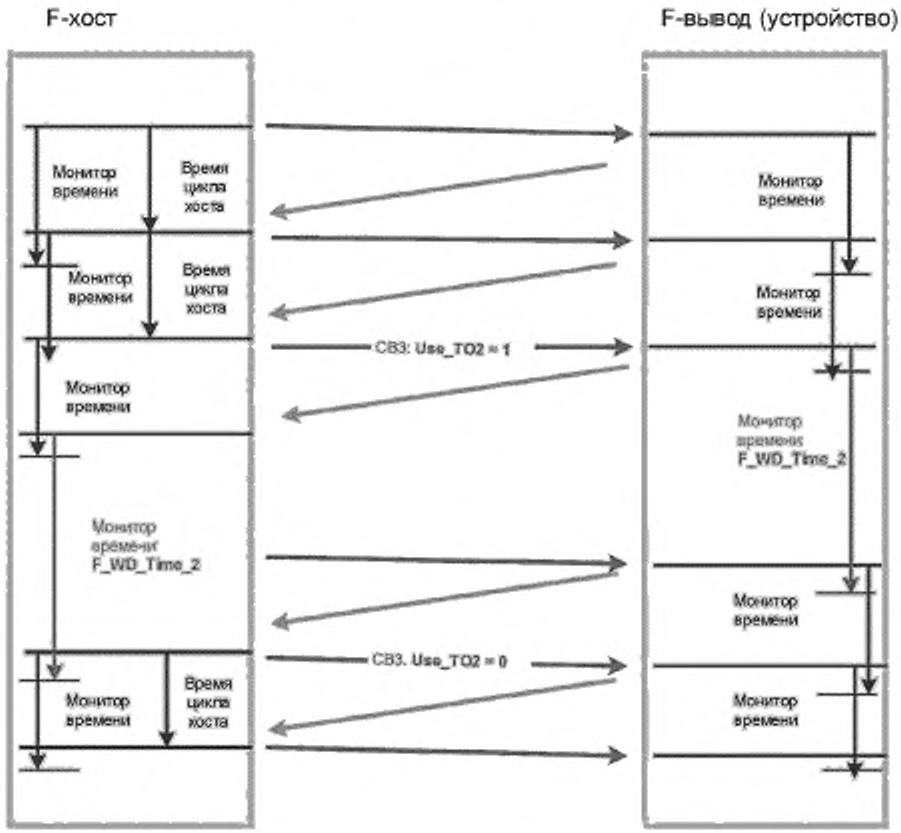


Рисунок 39 — Расширенное время сторожевого таймера по запросу

7.3 Реакция в случае неисправности

7.3.1 Повторение

Цитата: «Неисправность устройства шины приводит к повторению старых и неактуальных сообщений безопасности в неподходящее время так, что получатель может подвергнуться опасности (например, если приходит отчет о закрытии защитной двери в то время, как она уже была открыта).»

Устранение. Данные передаются циклически. Таким образом, неверное сообщение с PDU безопасности введенное однажды будет сразу же заменено правильным сообщением. Таким образом, последующая *возможная задержка* экстренного запроса может быть равна *одному периоду сторожевого таймера*.

7.3.2 Потеря

Цитата: «Неисправность устройства шины удаляет сообщение безопасности (например, запрос «безопасную остановку функционирования»).»

Устранение: Потерянная информации будет обнаружена посредством строгого соблюдения увеличения и анализа порядкового номера.

7.3.3 Внесение

Цитата: «Неисправность устройства шины вносит сообщение безопасности (например, отмена выделения «безопасной остановки функционирования».)».

Устранение: По причине строго последовательного поступления порядкового номера, получатель обнаружит внесенное сообщение.

7.3.4 Неверная последовательность

Цитата: «Неисправность устройства шины модифицирует последовательность сообщений безопасности. Например: Перед инициализацией безопасной остановки функционирования можно выбрать безопасно пониженную скорость. Машина продолжит работу вместо того, чтобы остановиться, когда подобные сообщения перепутаны.».

Устранение: По причине строго последовательного поступления порядкового номера, получатель обнаружит любую неправильную последовательность.

7.3.5 Искажение данных безопасности

Цитата: Неисправность устройства шины или канала передачи зашумляет сообщения безопасности.».

Устранение: Сигнатура CRC2 обнаруживает зашумление данных между отправителем и получателем.

Данные F-параметров
F-параметры: кодовое имя, WD время, УПБ и т. д.

PDU безопасности			
F-данные I/O	Байт статуса или байт управления	(Виртуальный) Порядковый номер	CRC2
			Для F-данных I/O , байта статуса и управления, (виртуального) порядкового номера и F-параметров
m октет	1 октет	3 октета	3 или 4 октета

Рисунок 40 — Данные F-параметра и CRC

Сигнатура CRC2 генерируется для F-параметров (включая кодовое имя), F-данных I/O, виртуального порядкового номера и байта управления/статуса (см. 7.3.5 и рисунок 40). Кодовое имя (связь источник-назначение) F-хоста и F-устройства определено во время стадии конфигурирования при помощи программного инструментария и запоминается с сохранением (не стираясь при выключении).

После исправления, F-адрес F-модуля/устройства должен быть восстановлен / подогнан перед возобновлением действий, связанных с безопасностью.

7.3.6 Задержка

Цитата: «1. Обмен эксплуатационными данными превышает возможности коммуникационного канала. 2. Устройство шины является причиной перегрузки, имитируя неправильные сообщения безопасности так, что услуга, принадлежащая сообщению, задерживается или они не выполняются.»

Устранение:

- порядковый номер в данных отправителя и в данных подтверждения;
- время сторожевого таймера на соответствующем получателе (время сторожевого таймера для F-коммуникаций).

Время сторожевого таймера определено в 9.3.3.

7.3.7 Подмена

Цитата: «Неисправность устройства шины вызывает смешивание сообщений, связанных с безопасностью, и сообщений, не связанных с безопасностью.»

Устранение: Данные поступают от правильного отправителя и направляются правильному получателю (аутентичность). Аутентичность гарантируется посредством включения F-параметров вместе с F-адресом (связь F-источник-назначение) в сигнатуру CRC2.

Принцип безопасной адресации:

Обнаружение взаимосвязи сообщений, связанных и не связанных с безопасностью обеспечивается за счет того, что стандартное устройство не способно создать PDU безопасности с правильным CRC2 и правильным порядковым номером.

Обнаружение данных от другого отправителя или для другого получателя обеспечивается за счет того, что F-отправитель, принадлежащий связи F-источник-назначение (кодовое имя) является единственным генерирующим именно такую совпадающую CRC сигнатуру, которую ожидает F-получатель. В то же самое время, получатель прибегает к CRC сигнатуре для проверки в неявной форме аутентичности адреса F-отправителя (так как он был включен в CRC).

Подборка F-адресов в индивидуальных устройствах с сохранением в долговременной памяти может быть достигнута одним из следующих методов:

- кодовый переключатель в блоке для кодового имени (например, адрес F-устройства малогабаритных устройств);
- одноразовая параметризация устройства посредством программного обеспечения. Необходимо проверять адресует ли это программное обеспечение нужное устройство. Это необходимо повторять при замене данного блока;
- механизмы адресации, независящие от адресации CPF 3.

Саботаж не предполагается.

7.3.8 Отказы памяти в коммутаторах

Цитата: «1. Обмен эксплуатационными данными превышает возможности коммуникационного канала. 2. Устройство шины является причиной перегрузки, имитируя неправильные сообщения так, что услуга, принадлежащая сообщению, задерживается или они не выполняется.»

См. рисунки 9 и 10 в качестве примеров возможных сетей безопасности для следующих соображений. Центральные элементы этих сетей — это коммутаторы, являющиеся достаточно сложными активными компонентами сети. На них могут происходить различные сбои. Сообщения могут отправляться по неправильному назначению или данные сообщений могут быть зашумлены. Более того, коммутатор может продолжать отправлять хранящиеся данные снова и снова даже, когда отправитель уже отключен. Таблица 7 содержит список возможных сбоев коммутатора и меры по их устранению, позволяющие достичь достаточной безопасности.

Таблица 7 — Средства устранения сбоев коммутаторов

Тип сбоя	Обнаружение и контроль (с помощью)
Зашумленные данные	Сигнатура CRC (24 бита)
Неверное назначение	Кодовое имя (2 x 16 бит)
Потерянное сообщение безопасности	Порядковый номер (24 бита) и таймаут
Продублированное сообщение	Порядковый номер (24 бита)
Задержанное сообщение	Таймаут
Ретрансляция хранимых сообщений с менее, чем 3 порядковыми PDU безопасности в партии. F-хост более не подсоединен	Порядковый номер (24 бита) без автоматического перезапуска
Ретрансляции хранимых сообщений с 3 или более порядковыми PDU безопасности в партии. F-хост более не подсоединен	Порядковый номер (24 бита) и реакция на сбой посредством байта управления (рисунок 36)

Следующие сбои подлежат обнаружению / контролю:

- Сбои F-хоста или *его* PDU безопасности не достигают получателя. Вместо этого коммутатор передает сообщения своего автоматически возобновляющегося буфера без правильного порядкового номера. F-устройство распознает сбой порядкового номера и устанавливает отказоустойчивые значения.
- Единичное сообщение буфера коммутатора ретранслируется и несет PDU безопасности с правильным порядковым номером. Этот сбой будет обнаружен по причине 24 битного порядкового номера и того факта, что перезапуск F-устройства-вывода требует OA_C = 1 (подтверждение оператора).
- Коммутатор передает сообщения с блоками PDU безопасности из своего автоматически возобновляющегося буфера с правильными порядковыми номерами и такая последовательность сообщений начинается в рамках времени сторожевого таймера. Этот сбой будет обнаружен по причине 24 битного порядкового номера и того факта, что перезапуск F-устройства-Вывода требует OA_C = 1 (Подтверждение Оператора).

7.3.9 Границы сети и маршрутизатор

Цитата: «1. Обмен эксплуатационными данными превышает возможности коммуникационного канала. 2. Устройство шины является причиной перегрузки, имитируя неправильные сообщения так, что услуга, принадлежащая сообщению, задерживается или они не выполняется.»

Для сетей CP 3/RTE с маршрутизаторами рисунок 11 является применимым, как и соответствующие пояснения. Предположим, что такая система с подсетями объединена с помощью маршрутизаторов. Следующие соображения показывают, что единичная ошибка не направит PDU безопасности к неправильному F-устройству и не заставит его перейти в опасное состояние.

Маршрутизатор соединяет две или более подсети с помощью уровней на уровне 3. Каждый F-хост и F-устройство может быть сконфигурировано на «использование маршрутизатора» вместе с надлежащим адресом маршрутизатора. Маршрутизатор управляет IP адресами подсоединенных подсетей. В таблице 8 содержится список типов сбоев и ограничения для функционирования маршрутизатора, необходимые для обеспечения достаточной безопасности.

Таблица 8 — Границы сети безопасности

Тип сбоя	Последствия	Обнаружение и контроль
Маршрутизатор держит неверный адрес F-устройства	Маршрутизатор получает сообщение для этого определенного F-устройства. Результат: цель не найдена.	Таймаут F-устройства
Два F-устройства с идентичными адресами. Один в подсети 0, другой в подсети 1. Ограничение: 2-портовый-маршрутизатор, как на рисунке 11.	1) F-устройство подсети 0 не найдено в подсети 0; 2) F-устройство подсети 0 не досягаемо в подсети 1; 3) F-устройство подсети 1 не досягаемо в подсети 0; 4) F-устройство подсети 1 правильно в подсети 1	В соответствии со стандартом CP 3/RTE
Два F-устройство с идентичными адресами. Один в подсети 0, другой в подсети 1 Ограничения: Маршрутизатор с одним портом (например, PC, лаптоп)	1) F-устройство подсети 0 не найдено в подсети 0; 2) Дублирование адреса в подсети	Однопортовые маршрутизаторы не создают границы сети (безопасности)

7.4 Запуск и координация изменений

7.4.1 Стандартная процедура запуска

Запуск F-устройств/модулей основан на стандарте CP 3/RTE. Уровни безопасности в F-хосте и F-устройстве запускаются сами по себе каждый раз, когда каналы CP 3/RTE циклически взаимодействуют друг с другом. Предыдущий выполненный запас уровней безопасности вместе с их специальными F-параметрами встраивается в нормальный процесс конфигурации и параметризации («Контекст») для CP 3/RTE. Любое повторение доставки F-параметров с идентичными значениями во время выполнения должно игнорироваться; отклоняющиеся значения приведут к безопасному состоянию.

Примечание — Подробности V1-режима см. в [48].

На рисунке 15 показаны базовые коммуникационные механизмы CP 3/RTE. В МЭК 61158-5-10, МЭК 61158-6-10 и [55] предоставлена информация о последовательностях запуска IO-контроллера и его IO-устройств, являющихся частью F-устройств.

7.4.2 Разблокирование назначения iпараметров

Следуя сообщению диагностики F-устройства, которому требуются дополнительные iпараметры (см. 8.2) или по внешнему запросу, F-хост устанавливает бит 0 («Разблокирование назначения iпараметров») в байте управления своего следующего PDU безопасности. Затем F-устройство принимает, посредством команд «Write-Record» (Записать запись), iпараметры один набор данных за другим, и в конце подтверждает их получение, устанавливая бит 0 («F-устройству были назначены новые значения iпараметров») в байте статуса своего следующего PDU безопасности (рисунок 41).

Разблокирование разрешено только в случае отсутствия состояния опасного процесса. Переменные «iPar_EN_C» и «iPar_OK_S», соотносящиеся с битом 0 байта статуса/управления, могут применяться в контексте Proxy-FB-iParameterization, т. е. прокси-ф-блок-iпараметризации (8.6.2). Они не применимы в контексте iпар-сервера (8.6.4). Последовательность сигналов на рисунке 41 является примером возможного применения.

Рисунок 41 — Разблокировка F-хостом назначения iпараметров

8 Управление коммуникационным уровнем безопасности

8.1 F-параметр

8.1.1 Перечень

Значения параметров устройств CP 3/RTE в черном канале назначаются в соответствии со стандартом CP 3/RTE, т. е. посредством файлов GSD файлов на языках описания GSD (см. [43] и [47]). F-параметры, дополнительно требующиеся для уровня безопасности, могут быть загружены посредством нескольких альтернативных функций параметризации.

Перечень F-параметров:

- F_S/D_Address — «Кодовое имя» для взаимодействий отправителя и получателя;
- F_WD_Time — Время сторожевого таймера F-устройства/модуля (по умолчанию в файле GSD: максимальное время обработки F-устройства/модуля);
- F_WD_Time_2 — дополнительное вспомогательное время сторожевого таймера F-устройств/модулей, спроектированных для «конфигурирования во время выполнения» или для «систем устойчивости к сбоям», чтобы расширить время контроля в случае запланированных обновлений, осуществляемых только авторизованным персоналом (7.2.6.2);
- F_Prm_Flag1 + 2 — Октеты параметра, содержащие несколько параметров для управления профилем;
- F_Check_SeqNr — Режим V2: порядковый номер должен всегда быть частью генерации CRC2;
- F_Check_iPar — Применение, зависящее от производителя, для гомогенных систем;
- F_SIL — Проверка: сконфигурированный УПБ = примененному УПБ?
- F_CRC_Length — Длина CRC2;
- F_Block_ID — Идентификация типа блока параметров;
- F_Par_Version — Номер версии эксплуатационного режима F-параметров/FSCP 3/1;
- F_iPar_CRC — Значение вычисления CRC iпараметра, переданное хотя бы с помощью ручного управления от инструмента CPD программному инструменту;
- F_Par_CRC — Вычисление сигнатуры CRC1 по всем F-параметрам.

8.1.2 F_Source/Destination_Address (кодовое имя)

Адреса F-компонентов контура управления безопасности, таких как F-ввод, F-хост и F-вывод, должны быть точно выражены в рамках подсети. Подсети соединены друг с другом посредством (2-портовых) маршрутизаторов, которые являются естественными границами для CP 3/RTE (5.4.2). Локально каждое F-устройство и его партнер имеют сконфигурированную связь источник-назначение на канале коммуникаций безопасности, («F_Source/Destination_Address» или, сокращенно, «F_S/D_ Adress»). Эта связь запоминается с сохранением в F-устройствах, является частью набора F-параметров и, следовательно, циклически проверяется уровнем безопасности. Параметры F_S/D_Address являются логическими обозначениями адреса, которые могут быть *свободно* и *точно* назначены. Они присваиваются адресам CP 3/RTE во время конфигурирования (7.3.7). Адреса *0* и *0FFFFh* должны быть исключены. Параметр состоит из двух частей: «F_Source_Add» и «F_Dest_Add»: каждая часть является типом данных без знака Unsigned16.

8.1.3 F_WD_Time (время сторожевого F-таймера)

Локально, каждое F-устройство и его аналог в F-хосте поддерживают сконфигурированное время сторожевого F-таймера для каждой связи источник-назначение. Этот таймер запускается уровнем безопасности каждый раз, когда он отправляет PDU безопасности с новым порядковым номером.

Этот параметр F_WD_Time кодируется следующим образом: Unsigned16. Временная база: 1 мс. Диапазон значений: от 1 до 65 535.

Подробности того, как эти временные периоды сторожевого таймера используются при определении времени реакции всей функции безопасности и как эти времена реакции могут быть определены, см. в 9.3.3.

Производитель F-устройства присваивает значение «по умолчанию» параметра F_WD_Time в GSD файле максимальному времени подтверждения устройства (ВПУ). Затем программный инструмент сможет предложить необходимый F_WD_Time для этой конкретной коммуникационной связи 1:1.

Примечание — Затем программный инструмент сможет вычислить скорости реакции функции безопасности, если все другие значения доступны. См. 9.3.2.

8.1.4 F_WD_Time_2 (вспомогательное время сторожевого F-таймера)

Это вспомогательное время сторожевого F-таймера может применяться по желанию для расширения обычного времени сторожевого F-таймера до еще одного периода времени F_WD_Time_2, необходимого для обновления F-устройств/модулей, как это показано на рисунке 42.

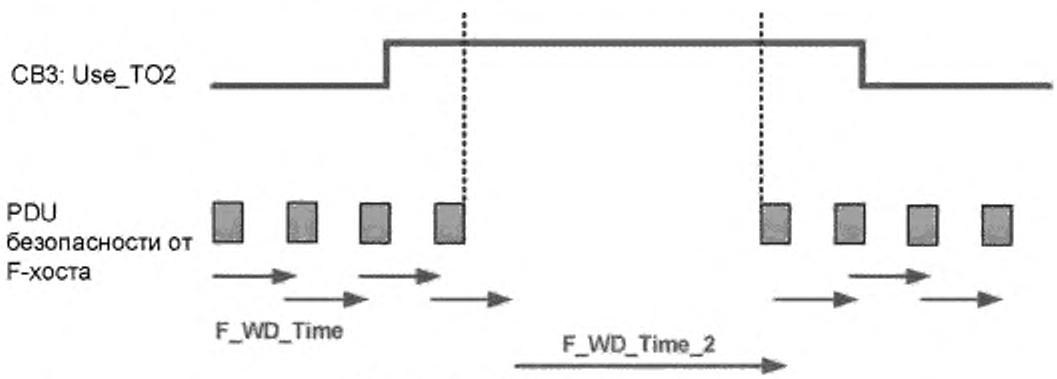


Рисунок 42 — Эффект F_WD_Time_2

Параметр F_WD_Time_2 кодируется следующим образом: Unsigned16. Временная база: 1 мс. Диапазон значений: от 1 до 65 535.

8.1.5 F_Prm_Flag1 (Параметры для управления уровнем безопасности)

8.1.5.1 Структура F_Prm_Flag1

Подразделы 8.1.5.2—8.1.5.5 подробно описывают октеты параметра F_Prm_Flag1. Они обладают структурой, показанной на рисунке 43.

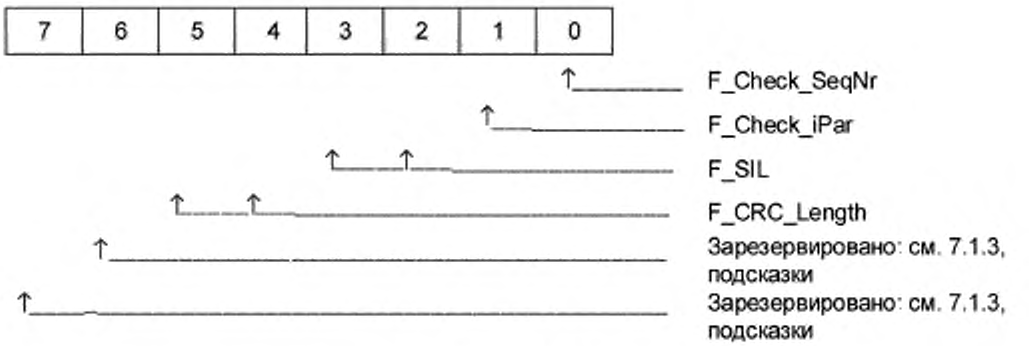


Рисунок 43 — F_Prm_Flag1

8.1.5.2 F_Check_SeqNr (последовательный номер в CRC2)

Этот параметр определяет надо ли включать порядковый номер в сигнатуру CRC2 (см. рисунок 44). Этот параметр распространяется на F-компонент при запуске.

Он кодируется следующим образом: Бит 0 октета параметра «F_Prm_Flag1».

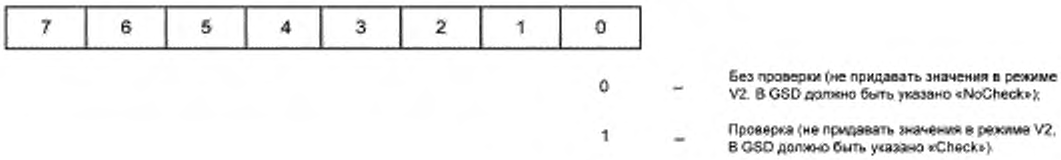


Рисунок 44 — F_Check_SeqNr

8.1.5.3 F_Check_iPar

Для обычного использования этот параметр должен всегда быть установлен в значение «0». Он зарезервирован для использования, зависящего от производителя, в гомогенных системах. Этот параметр не связан с механизмом ipar-сервер.

Он кодируется следующим образом: Бит 1 октета параметра «F_Prm_Flag1».

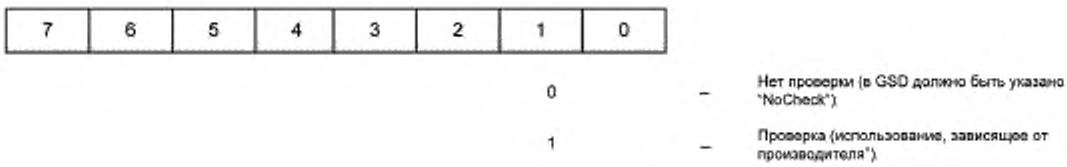


Рисунок 45 — F_Check_iPar

8.1.5.4 F_SIL (стадия УПБ)

FSCP 3/1 разрешает параллельное функционирование как коммуникаций, имеющих значение для безопасности, так и стандартных коммуникаций. Разные функции безопасности, использующие коммуникации, имеющие значение для безопасности, могут нуждаться в разных уровнях полноты безопасности (УПБ 1 … УПБ 3). F-устройства способны сравнивать свой собственный назначенный УПБ и сконфигурированный УПБ (F_SIL). Если он выше чем УПБ подсоединенного F-устройства/модуля, то устанавливается бит статуса «отказ устройства» и срабатывает реакция перехода в безопасное состояние. Существует четыре разные стадии: УПБ 1 … УПБ 3, НетУПБ (см. рисунок 46).

Он кодируется следующим образом: Биты 2 и 3 октета параметра «F_Prm_Flag1».

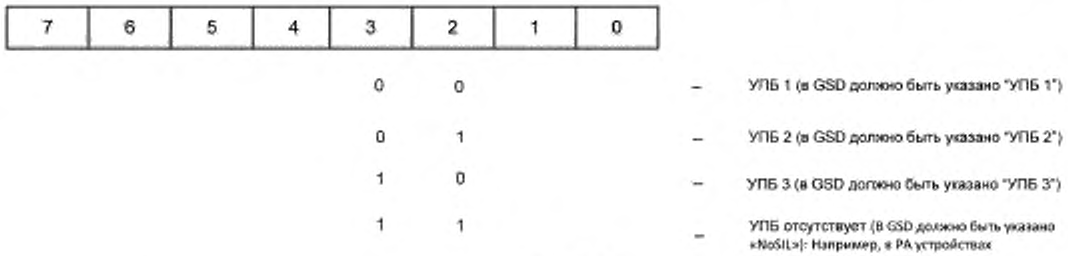


Рисунок 46 — F_SIL

8.1.5.5 F_CRC_Length (длина сигнатуры CRC2)

В зависимости от длины F-данных I/O (12 или 123 октета) и стадии УПБ, требуется CRC из 2, 3 или 4 октетов (см. рисунок 47). Во время запуска этот параметр передает F-компоненту ожидаемую длину сигнатуры CRC2 в PDU безопасности.

Он кодируется следующим образом: биты 4 и 5 октета параметра «F_Prm_Flag1».

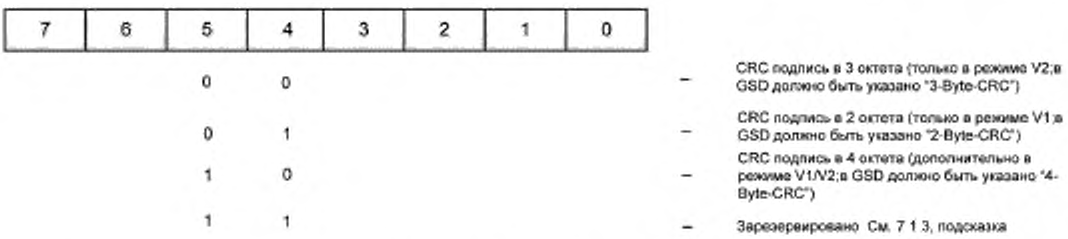


Рисунок 47 — F_CRC_Length

8.1.6 F_Prm_Flag2 (Параметры для управления уровнем безопасности)

8.1.6.1 Структура F_Prm_Flag2

Подразделы 8.1.6.2—8.1.6.3 подробно описывают октеты параметра F_Prm_Flag2.

Он обладает структурой, показанной на рисунке 48.

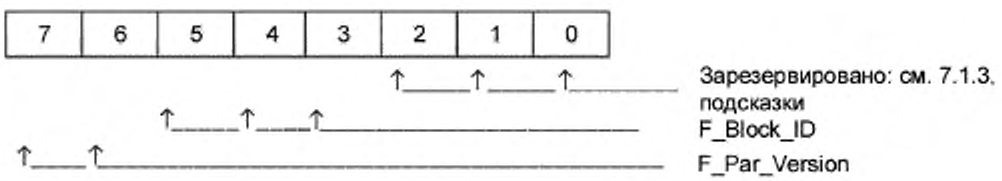


Рисунок 48 — F_Prm_Flag2

8.1.6.2 F_Block_ID (идентификация типа параметров)

Для того, чтобы выделить параметры для будущих режимов FSCP 3/1, идентификация типа параметров «F_Block_ID» кодируется следующим образом: биты 3, 4 и 5 октета параметра «F_Prm_Flag2» (см. рисунок 49). Проверка F_Block_ID является обязательной для уровня безопасности.

7	6	5	4	3	2	1	0		
		0	0	0				–	Нет F_iPar_CRC, Нет F_WD_Time_2
		0	0	1				–	F_iPar_CRC (рисунок 51)
		0	1	0				–	F_WD_Time_2 (рисунок 42), Нет F_iPar_CRC
		0	1	1				–	F_WD_Time_2 и F_iPar_CRC
		1	0	0				–	Зарезервировано
		1	0	1				–	Зарезервировано
		1	1	0				–	Зарезервировано
		1	1	1				–	Зарезервировано

Рисунок 49 — F_Block_ID

8.1.6.3 F_Par_Version (номер версии набора F-параметров)

Целью данного счетчика версий является идентификация новых версий эксплуатационного режима внутри уровня безопасности. В случае если запрошенная версия уровня безопасности не совпадает с реализованной версией, то F-устройство должно отвечать сообщением диагностики, которое зависит от устройства (см 6.3.2 и рисунок 50). Проверка подтверждения соответствия F-параметров должна выполняться уровнем безопасности.

7	6	5	4	3	2	1	0		
0	0							–	Действительно для режима V1 (в GSD должно быть указано "V1-mode")
0	1							–	Действительно для режима V2 (в GSD должно быть указано "V2-mode")
1	0							–	Зарезервировано: см. 7.1.3, подсказки
1	1							–	Зарезервировано. см. 7.1.3, подсказки

Рисунок 50 — F_Par_Version

8.1.7 F_iPar_CRC (значение iPar_CRC для всех iпараметров)

После успешного сеанса параметризации и ввода в эксплуатацию инструмент CPD определенного F-устройства вычисляет сигнатуру CRC (iPar_CRC) для всех iпараметров. Каждый раз, когда вычисления выдают «0», значение должно быть установлено равным «1». Значение в шестнадцатеричном формате должно передаваться, хотя бы с помощью ручного управления, программному инструменту и назначаться полю записи «F_iPar_CRC».

Данный параметр передается F-устройству во время запуска и служит для проверки на непротиворечивость iпараметра в F-устройстве. Его передача осуществляется до запуска обычной операции безопасности. Данный параметр должен быть установлен в значение «0», пока он находится в «FSCP режиме тестирования» (8.6.4.5) F-устройства. В таком случае F-устройство пропустит проверку на непротиворечивость. Каждый раз, когда F-устройство обнаруживает несоответствие между сигнатурой iPar_CRC, вычисленной локально, и значением F_iPar_CRC, оно должно установить отказоустойчивые значение (FV).

Данный параметр не обязателен. Бит 3 F-параметра «F_Prm_Flag2» указывает на его присутствие. Он кодируется как: Unsigned32

8.1.8 F_Par_CRC (CRC1 для всех F-параметров)

Программный инструмент генерирует эту сигнатура CRC1 для всех F-параметров. Начальное значение для CRC1 равно 0. Подробности о порядке F-параметров для использования в генерации сигнатуры CRC1 см. в 8.3.3.2. Используется такой же 16-битный CRC полином (1*4EAB*h). CRC1 является начальным значением для циклического расчета CRC2.

Следующие правила применимы для разных полиномов CRC2:

- В случае 24 битного полинома CRC (1*5D6DCB*h) начальное значение для вычислений CRC2 равно «00xxxx», где xxxx=CRC1.
- В случае 32 битного полинома CRC (1*F4ACFB13*h) начальное значение для вычислений CRC2 равно «0000xxxx», где xxxx=CRC1.

Он кодируется как: Unsigned16.

8.1.9 Структура объекта записи данных (record data object) F-параметра

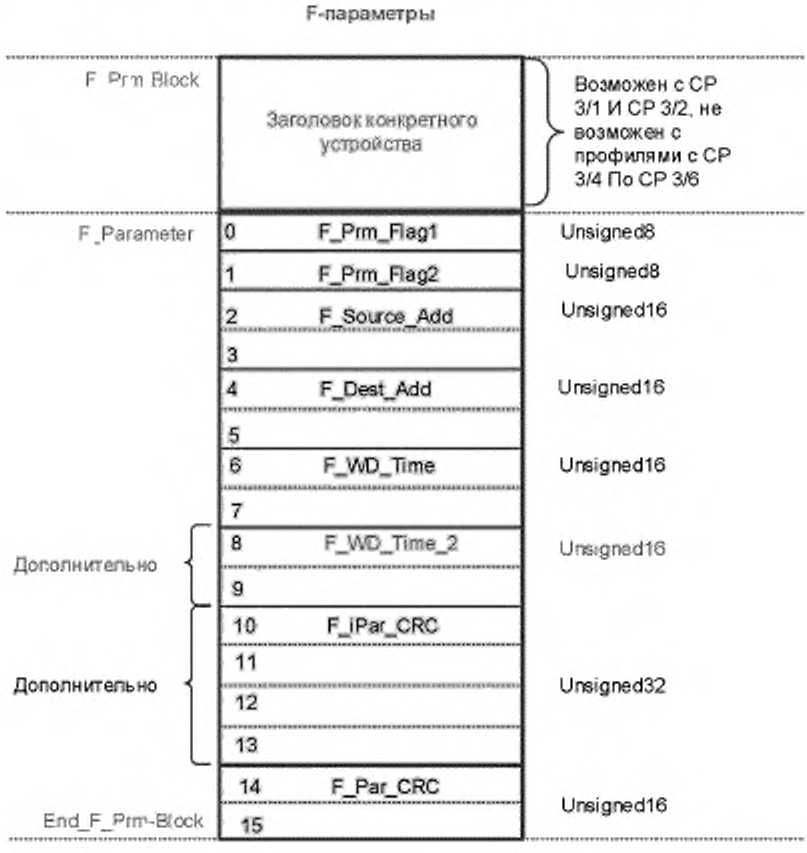


Рисунок 51 — F-параметр

На рисунке 51 показана структура блока F-параметров в объекте записи данных. Упорядочивание октетов выполняется в соответствии со стандартом CP 3/RTE. Следующее применяется к модульным F-устройствам: Для каждого F-подмодуля в контекстное сообщение вводится F_Parameter-Блок (рисунок 13). Присвоение подмодуля F-устройству происходит в выбранном номере подслота.

8.1.10 Доля F-данных

См. 7.1.6.

8.2 iПараметр и iPar_CRC

F-устройства все чаще обеспечиваются интеллектуальными функциями, которые требуют назначения неограниченных индивидуальных значений параметров F-устройства. Эти, связанные с безопасностью, параметры именуются iпараметрами. В частности, в случае замены устройства целесообразно загрузить эти параметры прямо через шину стандартным путем. Эти записи параметров, как правило, выходят за рамки диапазона данных параметризации, основанного на GSD (несколько лазерных сканеров с, приблизительно, 1 кБ на зону защиты могут привести к общим 90 кБ и более) и поэтому данная спецификация FSCP 3/1 предоставляет дополнительные механизмы.

На рисунке 52 показан вариант структуризации большого числа iпараметров для целей загрузки и скачивания. Абсолютный верхний предел для iпараметров это 222-1 октетов; нижний предел это 4 октета. Таким образом, каждый раз, когда общая сумма превышает 240 октетов, для CP 3/1 требуется сегментация, как это показано на рисунке 52. Для CP 3/RTE сегментация не требуется.

Сигнатура CRC («iPar_CRC») должна вычисляться для всех iпараметров (рисунок 52) при помощи любого подходящего CRC полинома, заполнять 4-октетный iPar_CRC в шестнадцатеричном формате и отображаться на CPD-Инструменте. Каждый раз, когда вычисления выдают «0», должно быть установлено значение «1». Включение значения iPar_CRC в iпараметры, как это показано на рисунке 52, является не обязательным. При использование 32-битного CRC полинома для профиля FSCP 3/1 не требуется никакого вычисления достаточной частоты возникновения остаточных ошибок для подтверждения безопасности.

Связь F_source/destination (кодовое имя) позволяет проверять доставку сконфигурированному получателю. Включение iпараметров, как это показано на рисунке 52 не обязательно.

Функции идентификации и технического обслуживания (ИТО) являются обязательными для всех устройств CPF 3. Они предоставляют коды, идентифицирующие тип и версию определенного устройства/модуля. Включение подобной информации в набор iпараметров может быть использовано для проверки подтверждения соответствия заменяющего устройства, обладающего своими собственными ИТО функциями. Включение в iпараметры, как это показано на рисунке 52, не обязательно. Производители устройства могут использовать свои собственные кодировки.

Длина блока iпараметров может пригодиться для эффективной организации процессов загрузки и скачивания, осуществляемых в устройствах. Включение в iпараметры, как это показано на рисунке 52, не обязательно.

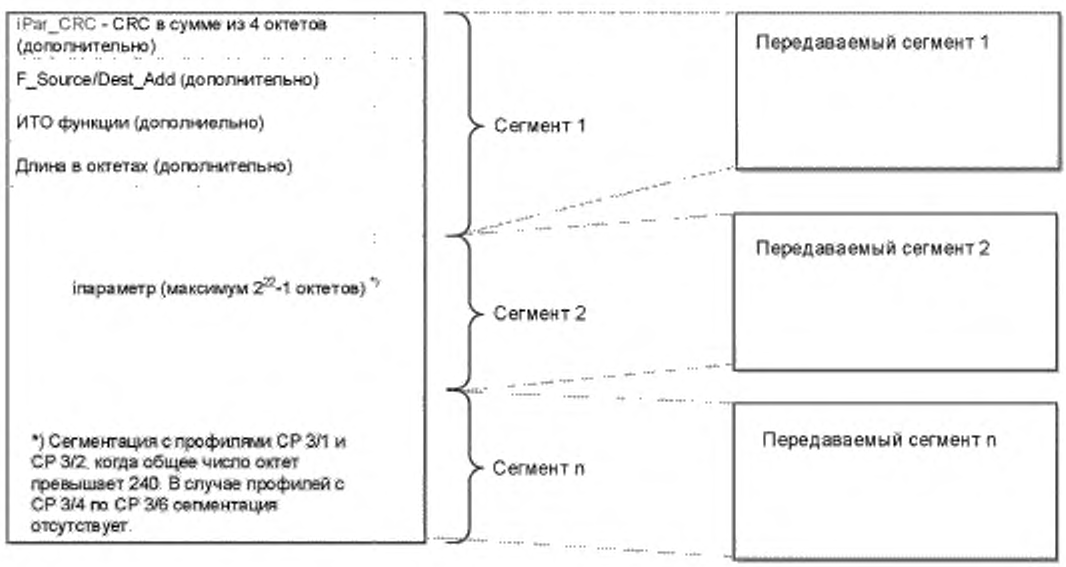


Рисунок 52 — Блок iпараметров

Подробности того, как работать с несколькими сегментами iпараметра, см. в 8.6.

8.3 Параметризация безопасности

8.3.1 Цели

FSCP 3/1 предоставляет «масштабируемые» методы для обеспечения F-устройств F и iпараметрами, так как в производственных и обрабатывающих отраслях полевые устройства применяется по-разному. Одной из основных целей является поддержание в стабильном состоянии небольшого набора F-параметров (коммуникационный уровень) на всех F-устройствах и предоставление интерфейсов для iпараметризации, что позволит минимизировать зависимость между системой и производителем устройства и, тем самым, четко разделить ответственности.

Возможность использования Прокси-ФБлока (Proxy-FB) для iпараметризации определена с самого начала в FSCP 3/1. Прокси-Фблок базируется на рекомендациях из [49] и ответственность за него на себя берет производитель F-устройства. Концепция Прокси-ФБлока описана в 8.6.2.

Для небольшого числа iпараметров, например, для модулей ввода удаленного I/O, концепция Прокси-Фблока подразумевает слишком много логистических издержек, и поэтому в настоящем стандарте определен стандартизированный Прокси-Фблок, «iПар-сервер». В отличие от Прокси-Фблока производитель F-хоста/системы берет на себя ответственность за iпар-сервер и предоставляет это свойство либо включенным в библиотеку стандартного функционального блока, либо в качестве встроенной функции. Концепция iпар-сервера описана в 8.6.4.

Небольшой набор идентичных F-параметров, проходя через все различные F-устройства, передается программному инструменту, отвечающему за конфигурацию сети, связанной с безопасностью, посредством GSD (общее описание станции) и таким образом предоставляет постоянный и не сложный пользовательский интерфейс. Более того, он предотвращает необходимость выбора версии GSD и связанные с этим усилия по одобрению этой версии конфигурационной частью сети.

После проведения настройки F-параметров, которая осуществляется во время конфигурирования сети, составляется запись F-параметра и помещается на хранение в F-хост/IO-контроллер для запуска сети.

F-параметр «F_IO_StructureDescCRC» используется для обеспечения корректного использования F-программой пользователя структуры F-данных I/O и типы данных и поэтому он не передается F-устройству при запуске.

8.3.2 Расширения безопасности GSDL и GSDML

8.3.2.1 Расширения GSDL

FSCP 3/1 поддерживает устройства, ориентированные на физический или виртуальный модуль. Поэтому спецификация язык общего описания станции (GSDL) [43] (см. также ИСО 15745-3) определяет ключевые слова для структурирования и идентификации информацию блока F-параметров F-модулей, показанных на рисунке 51. Возможная выборка значений F-параметров содержится в файле общего описания станции (GSD), ассоциированного с F-ведомым устройством, для которого спроектирован F-модуль. Определены следующие ключевые слова из таблицы 9.

Таблица 9 — Ключевые слова GSDL для F-параметров и структур F-I/O

Ключевое слово GSDL	Описание
F_Ext_Module_Prm_Data_Len	Параметр, ассоциированный с этим ключевым словом, указывает на общую длину F_Prm-Блока, показанного на рисунке 51, которая составляет, как правило, 14 или 18 октетов, в зависимости от F_iPar_CRC
F_Ext_Module_Prm_Data_Const (offset)	При помощи параметра, ассоциированного с этим ключевым словом, фиксированное значение может быть введено в один из 4 октетов заголовка F_Prm-Блока, показанного на рисунке 51. На позицию октета указывает сдвиг 0…3
F_Ext_Module_Prm_Data_Const (0)	Указывает на длину F_Prm_Block, включая F-iPar_CRC, например, 0x12
F_Ext_Module_Prm_Data_Const (1)	Идентификация F_Prm-Блока = 5 (fix)
F_Ext_Module_Prm_Data_Const (2)	Слот F-модуля
F_Ext_Module_Prm_Data_Const (3)	Зарезервировано. Должно быть установлено значение «0».
F_Ext_Module_Prm_Data_Ref (offset)	При помощи параметра, ассоциированного с этим ключевым словом, во время конфигурирования значение выбранное пользователем может быть введено в один из октетов 0… 13 F_Prm-Блока, показанного

Окончание таблицы 9

Ключевое слово GSDL	Описание
F_Ext_Module_Prm_Data_Ref (offset)	на рисунке 51. На позицию октета указывает сдвиг 4… 16. Параметр указывает на определение диапазона ExtUserPrmData в других частях файла GSD
F_ParamDescCRC	Параметр, ассоциированный с этим ключевым словом, закрепляет части описаний F-параметра в GSD файле, связанные с безопасностью. Более подробно, как определить CRC0 сигнатуру, см. 8.3.3.3
F_IO_StructureDescCRC	Параметр, ассоциированный с этим ключевым словом, закрепляет описание структуры F- данных I/O (циклически передающихся значений процесса). Более подробно, как определить сигнатуру CRC7 см. в [43] и 8.4.1
F_IO_StructureDescVersion	Параметр, ассоциированный с ключевым словом, указывает на версию описания структуры F- данных I/O. Значение 1 указывает на 16-битную сигнатуру CRC7, а значение 2 указывает на 32-битную сигнатуру CRC7. Если этот атрибут отсутствует, то предполагается значение 1

Рекомендуется структурированная параметризация. Дальнейшие расширения GSDL см. в 8.6.4.6.

8.3.2.2 Расширения GSDML

F-параметры определенного F-устройства определены с помощью GSD файла. Описание предоставлено при помощи языка разметки общего описания станции (GSDML), основанного на XML (см. ИСО 15745-3, ИСО 15745-4 и [47]).

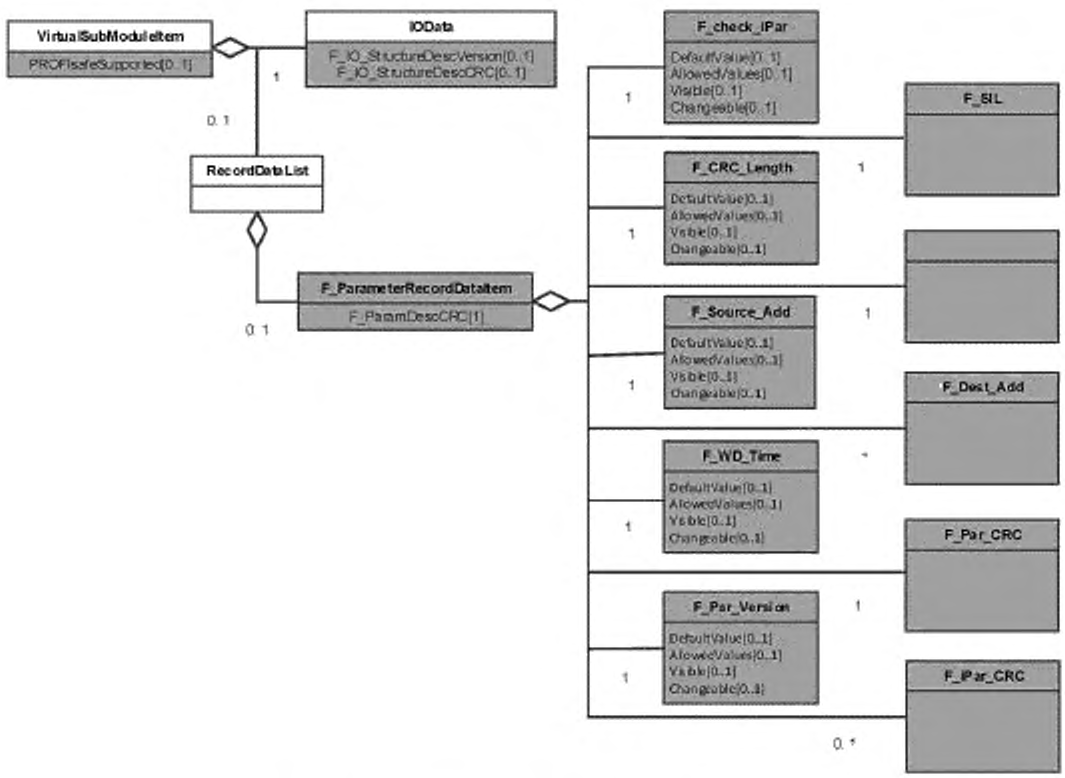


Рисунок 53 — Расширение F-параметра в спецификации GSDML

На рисунке 53 показаны расширения в GSDML. Секция «VirtualSubmoduleItem» (элемент виртуального подмодуля) предоставляет дополнительный атрибут «F_ParamDescCRC». Это CRC сигнатура (CRC0) описания F-параметра на рисунке 53. «F_IO_StructureDescCRC» в секции «IOData» закрепляет форматы данных F-ввода и F-вывода. «F_IO_StructureDescVersion» указывает на версию описания структуры данных F_IO (см. 8.3.3).

8.3.3 Защита параметров безопасности и данных GSD

8.3.3.1 Общие положения

Незаменимым для безопасности системы является защита параметров уровня безопасности (F-параметров), параметров технологии безопасности F-устройства (iпараметров), а также сконфигурированных структур данных безопасности I/O. Это осуществляется посредством CRC сигнатур, постоянной энергонезависимой памяти в F-устройстве и F-хосте и периодического сравнения CRC сигнатур.

Для того чтобы предотвратить использование программным инструментом зашумленных данных описания устройства (GSD), части этих данных, важные для безопасности, также защищаются с помощью CRC сигнатуры.

8.3.3.2 CRC1 и iPar_CRC на всех параметрах безопасности

На рисунке 25 показана только сигнатура CRC1 для всех F-параметров, которые войдут в процесс генерации сигнатуры CRC2. Тем не менее, дополнительно может быть вовлечено больше сигнатур CRC, как показано ниже в данном разделе.

Для защиты F-параметров, программный инструмент F-хоста генерирует сигнатуру *CRC1*, как она описана в 8.1.7. Применимый CRC полином это 1*4EAB*h. Сигнатура *CRC1* строится для всех F-параметров в порядке октетов, показанном на рисунке 51, исключая дополнительный F_iPar_CRC. Каждый раз, когда бит 3 F-параметра «F_Block_ID» устанавливается в значение «1» сигнатура F_iPar_CRC должна включаться в начало вычисления, как это показано на рисунке 54.

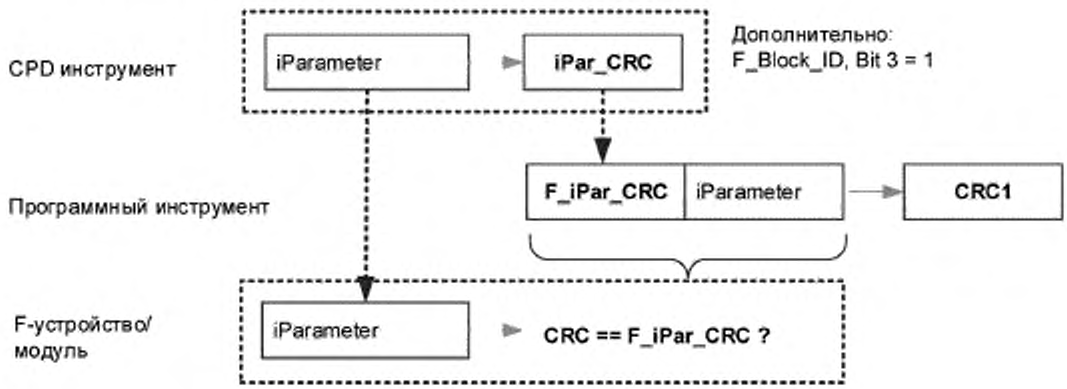


Рисунок 54 — CRC1, включая iPar_CRC

Сгенерированное значение сигнатуры CRC1 (Unsigned16) хранится и используется в дальнейшем в обратном порядке октетов (см. 7.1.5).

8.3.3.3 CRC0 для данных GSD

Для того чтобы гарантировать, что параметры F-устройства, важные для безопасности, не претерпевают незаметных изменений в течение жизни накопителя и могут безопасно считываться в инструмент конфигурирования, все они защищаются с помощью CRC. Параметр «F_ParamDescCRC» содержит 2-октетную сигнатуру CRC (CRC0), сгенерированную при помощи того же 16-битного CRC полинома (14EABh), который используется во всем FSCP 3/1.

В случае файла GSD для F-ведомого устройства (CP 3/1 или CP 3/2) сигнатура CRC0 начинает вычисляться с первым F_Ext_User_Prm_Data_Ref (4) и сканирует все ключевые слова одного типа и их определения F-параметров в описании «ExtUserPrmData» и в выбранных секциях «PrmText». Псевдокод на рисунке 55 показывает алгоритм того, как генерируется 2-октетный CRC0, являющийся практически независимым от структуры GSD файла и комментариев, тем самым, наделяя проектировщика файла максимальной свободой и возможностью вносить изменения.

Подчеркнутые символы включены в вычисление.

```
//Каждая F_Ext_User_Prm_Data_Ref(x) одна за другим в порядке возрастания (байтовый сдвиг  битовый сдвиг)
//Заголовок F_Prm_Block игнорируется
for (F_Par_Ref = 0; F_Para_Ref < number of elements; F_Para_Ref ++)
{
        if (list parameter==TRUE) // PrmText хотя бы с двумя выборками
        {
                // в случае F-параметров с определениями "PrmText"
                // читать имя соответствующего F_Parameter
                // например  ExtUserPrmData = 8 "F_CRC_Length"
                // читать формат данных (0  Bit, 1  Unsigned8, 2  Unsigned16, 3  Unsigned32)
                // читать битовый сдвиг (0 if Unsigned8/Unsigned16/Unsigned32)
                // например  BitArea (4-5) 0 0-2                                   →0, 4
                // читать значение по умолчанию (LoByte, HiByte)
                // например, BitArea(4-5) 0 0-2                                    →0, 0
                // now read corresponding PrmText via the text selections
                // например PrmText        =       3
                // Text(0)                 =       "3-Byte-CRC"
                // Text(1)                 =       "2-Byte-CRC"
                // Text(2)                 =       "4-Byte-CRC"
                // EndPrmText
                for (value = 0; value <= Max (Prmtext), value ++)
                {
                        // читать фактическое значение как текст
                        // например                                               →"3-Byte-CRC"
                        // читать фактическое значение как номер (индекс) (LoByte, HiByte)
                        // например                                               →0, 0
                }
}
else
// в случае F-параметров с полями редактирования.
        {
                // читать наименование соответствующего F_Parameter в порядке возрастания
                // например, ExtUserPrmData = 2 "F_Dest_Add"
                // читать формат данных (0: Bit, 1: Unsigned8, 2: Unsigned16  3  Unsigned32)
                // читать сдвиг битов (0 если Unsigned8/Unsigned16/Unsigned32)
                // например, Unsigned16 1 1-65534                                 →2, 0
                // читать значение по умолчанию (starting with LoByte)
                // Unsigned16 1 1-65534                                           →1, 0
                // читать нижний предел (начиная с LoByte)
                // Unsigned16 1 1-65534                                           →1, 0
                // читать верхний предел (начиная с LoByte)
                // Unsigned16 1 1-65534                                           →254, 255
        }
}
// Конец алгоритма
```

Рисунок 55 — Алгоритм построения CRC0 (GSDL)

Для получения образцов GSD файлов для F-ведомых устройств (CP 3/1 или CP 3/2) следует обратиться к организациям, приведенным в приложении В.

В случае файла GSD для F-устройства (CP 3/RTE) вычисление 2-октетной сигнатуры CRC осуществляется во всех секциях F_ParameterRecordDataItem (рисунок 53), включая все F-параметры и их определения. Псевдокод на рисунке 56 показывает алгоритм построения CRC0 практически независимого от структуры и комментариев файла GSD, что наделяет проектировщика файла максимальной свободой проектирования и возможностью вносить изменения без конфликтов.

Примечание — Некоторые F-параметры могут быть установлены как невидимые в файле GSD для устройств CP 3/RTE, что выполняется с помощью установки Visible (Видим) = «false». F-параметр не будет учитываться в вычислении CRC0 в случае Visible = «false».

Если атрибуты F-параметров в GSD файле не учитываются, то значения схемы GSDML по умолчанию будут по-прежнему применимы и должны включаться в вычисление CRC0.

```
while (F_Parameter_to_read())
{
// секция F_ParameterRecordDataItem должна читать в порядке возрастания (байтовый сдвиг, битовый сдвиг).
// Наименование F-параметра
// DataType F-параметра (0: Bit / BitArea, 1: Unsigned8, 2: Unsigned16, 3: Unsigned32)
// BitOffset F-параметра (0 если Unsigned8/Unsigned16/Unsigned32)
// читать DefaultValue (Начиная с LoByte, два байта для битовых параметров. Unsigned8: Unsigned16:
// четыре байта для Unsigned32)
if (value_range) // Поле редактирования или параметр списка, содержащий только одно значение
{
// читать 1ую цифру AllowedValue (начиная с LoByte: LowerLimit)
// читать 2ую цифру AllowedValue (начиная с LoByte: UpperLimit)
}
else // Перечислить параметры, содержащие хотя бы две текстовые выборки
{
// для каждого AllowedValue в AllowedValueList: читать текстовое описания AllowedValue
// символ за символом, а затем соответствующие числовые значения (LoByte, HiByte)
}
// конец алгорима
```

Рисунок 56 — Алгоритм для построения CRC0 (GSDML)

Для получения образцов GSD файлов для F-устройств (CP 3/RTE) следует обратиться к организациям, приведенным в приложении В. Интерпретация файла GSD: Каждый раз, когда инструмент конфигурирования распознает F-ключевые слова, специальное программное обеспечение F-конфигурирования (как правило, оцененное с точки зрения безопасности) в инструменте конфигурирования может быть запущено для обработки F-параметров связанным с безопасностью образом.

8.4 Конфигурация безопасности

8.4.1 Защита описания данных безопасности I/O (CRC7)

Структура F-данных I/O описана в секции «IOData» файла GSD. Один из атрибутов это «F_IO_StructureDescCRC» = CRC7. CRC7 строится для всех атрибутов в таблице 10 в том порядке, в котором они перечислены (версия 2). Для вычисления сигнатуры должен применяться 32-битный CRC полином (1*F4ACFB13*h). Разрешенные типы данных для FSCP 3/1 перечислены в 5.5.4. Предыдущая версия 1 элемента структуры данных I/O не включала атрибут VERSION («ВЕРСИЯ») и типы данных Integer32 и Unsigned8+Unsigned8. Таким образом, в определенном GSD файле нет ключевого слова VERSION, указывающего на отсутствие типов данных Integer32 и Unsigned8+Unsigned8, сигнатура CRC7 должна вычисляться при помощи 16-битного полинома CRC (1*4EAB*h), а длина сигнатуры CRC7 составляет 2 октета.

Параметр «F_IO_StructureDescCRC» не передается F-устройству во время запуска. Программный инструмент может использовать этот механизм для обеспечения правильной конфигурации.

Таблица 10 — Элементы структуры данных I/O (версия 2)

Имя атрибута	Длина	Описание
VERSION	1 октет	Указывает на определенный набор элементов структуры данных I/O
IN_ADDRESS_RANGE	2 октета	Длина в октетах всей секции IOData Input (включая F_MessageTrailer)
COUNT_PS_INPUT_BYTES_COMPOSITE	2 октета	Ввод. Длина всех элементов данных типа «Float32+Unsigned8» (5 x число элементов)
COUNT_PS_INPUT_BYTES_U8_U8	2 октета	Ввод. Длина всех элементов данных типа «Unsigned8+Unsigned8» (2 x число элементов)
COUNT_PS_INPUT_CHANNELS_BOOL_MAX	2 октета	Ввод. Число всех булевых каналов («используется в качестве битов») в режиме максимума (например, в режиме 1oo1)
COUNT_PS_INPUT_BYTES_BOOL_MAX	2 октета	Ввод. Длина всех булевых элементов данных (в октетах) в режиме максимума (например, в режиме 1oo1)
COUNT_PS_INPUT_CHANNELS_INT	2 октета	Ввод. Число всех элементов данных типа Integer16

Окончание таблицы 10

Имя атрибута	Длина	Описание
COUNT_PS_INPUT_CHANNELS_DINT	2 октета	Ввод. Число всех элементов данных типа Integer32
COUNT_PS_INPUT_CHANNELS_REAL	2 октета	Ввод. Число всех элементов данных типа Float32
OUT_ADDRESS_RANGE	2 октета	Длина в октетах всей секции IOData Output (включая F_MessageTrailer)
COUNT_PS_OUTPUT_BYTES_COMPOSITE	2 октета	Вывод. Длина всех «Float32+Unsigned8» Элементов-Данных (5 х число элементов)
COUNT_PS_OUTPUT_BYTES_U8_U8	2 октета	Вывод: Длина всех «Unsigned8+Unsigned8» элементов данных (2 х число элементов)
COUNT_PS_OUTPUT_CHANNELS_BOOL	2 октета	Ввод. Число всех булевых каналов («используется в качестве битов»)
COUNT_PS_OUTPUT_BYTES_BOOL	2 октета	Вывод: Длина всех булевых элементов данных (в октетах)
COUNT_PS_OUTPUT_CHANNELS_INT	2 октета	Вывод. Число всех элементов данных типа Integer16
COUNT_PS_OUTPUT_CHANNELS_DINT	2 октета	Вывод. Число всех элементов данных типа Integer32
COUNT_PS_OUTPUT_CHANNELS_REAL	2 октета	Вывод. Число всех элементов данных типа Float32
DATA_STRUCTURE_CRC	4 октета	«F_IO_StructureDescCRC» = CRC7

8.4.2 Примеры секций типа данных DataItem

8.4.2.1 Подход

Подразделы 8.4.2.2—8.4.2.5 содержат примеры секций DataItem в соответствии с некоторыми типами драйверов F-канала в 8.5.2, используя атрибуты, описанные в таблице 10.

Разрешенные типы данных для FSCP 3/1 перечислены в 5.5.4. Для 32-битного логического типа данных должен использоваться Unsigned32.

Общую информацию о типах данных см. в [67].

8.4.2.2 F_IN_OUT_1

Ввод: 32-битовый логический.

Вывод: 32-битовый логический.

Пример кодирования секции DataItem для F_Channel_Driver F_IN_OUT_1 показан на рисунке 57. Таблица 10 содержит описание переменных.

```
<IOData>
        <IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Inputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned32" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
</IOData></Output>

VERSION 02                                  02
IN_ADDRESS_RANGE 08                         08
COUNT_PS_INPUT_BYTES_COMPOSITE 00           00
COUNT_PS_INPUT_BYTES_U8_U8 00               00
COUNT_PS_INPUT_CHANNELS_BOOL 32             32
COUNT_PS_INPUT_BYTES_BOOL 04                04
COUNT_PS_INPUT_CHANNELS_INT 00              00
COUNT_PS_INPUT_CHANNELS_DINT 00             00
COUNT_PS_INPUT_CHANNELS_REAL 00             00
OUT_ADDRESS_RANGE 08                        08
COUNT_PS_OUTPUT_BYTES_COMPOSITE 00          00
COUNT_PS_OUTPUT_BYTES_U8_U8 00              00
COUNT_PS_OUTPUT_CHANNELS_BOOL 32            32
COUNT_PS_OUTPUT_BYTES_BOOL 04               04
COUNT_PS_OUTPUT_CHANNELS_ INT 00            00
COUNT_PS_OUTPUT_CHANNELS_DINT 00            00
COUNT_PS_OUTPUT_CHANNELS_ REAL 00           00
DATA STRUCTURE CRC 0x9EBE9328               0x9EBE9328
```

Рисунок 57 — Секция DataItem для F_IN_OUT_1

8.4.2.3 F_IN_OUT_2

Ввод: 16-битовый логический, 16-битовый целочисленный.

Вывод: 16-битовый логический, 16-битовый целочисленный.

Пример кодирования для F_Channel_Driver F_IN_OUT_2 показан на рисунке 58.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Unsigned16" UseAsBits="true" TextId="Inputs" />
                <DataItem DataType="Integer16" UseAsBits="false" TextId="AI channel" />
        <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Unsigned16" UseAsBits="true" TextId="Outputs" />
                <DataItem DataType="Integer16" UseAsBits="false" TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
    </Output>
</IOData>
```

VERSION	02
IN_ADDRESS_RANGE	08
COUNT_PS_INPUT_BYTES_COMPOSITE	00
COUNT_PS_INPUT_BYTES_U8_U8	00
COUNT_PS_INPUT_CHANNELS_BOOL	16
COUNT_PS_INPUT_BYTES_BOOL	02
COUNT_PS_INPUT_CHANNELS_INT	01
COUNT_PS_INPUT_CHANNELS_DINT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	08
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_BYTES_U8_U8	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	16
COUNT_PS_OUTPUT_BYTES_BOOL	02
COUNT_PS_OUTPUT_CHANNELS_ INT	01
COUNT_PS_OUTPUT_CHANNELS_DINT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
DATA STRUCTURE CRC	0x82288330

Рисунок 58 — Секция DataItem для F_IN_OUT_2

8.4.2.4 F_IN_OUT_5

Ввод: Составной (Float32+Unsigned8).

Пример кодирования для F_Channel_Drive F_IN_OUT_5 показан на рисунке 59.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Output>
    </Output>

</IOData>
```

VERSION	01
IN_ADDRESS_RANGE	09
COUNT_PS_INPUT_BYTES_COMPOSITE	05
COUNT_PS_INPUT_CHANNELS_BOOL	00
COUNT_PS_INPUT_BYTES_BOOL	00
COUNT_PS_INPUT_CHANNELS_INT	00
COUNT_PS_INPUT_CHANNELS_REAL	00
OUT_ADDRESS_RANGE	04
COUNT_PS_OUTPUT_BYTES_COMPOSITE	00
COUNT_PS_OUTPUT_CHANNELS_BOOL	00
COUNT_PS_OUTPUT_BYTES_BOOL	00
COUNT_PS_OUTPUT_CHANNELS_ INT	00
COUNT_PS_OUTPUT_CHANNELS_ REAL	00
DATA_STRUCTURE_CRC	0x8CAC

Рисунок 59 — Секция DataItem для F_IN_OUT_5

8.4.2.5 F_IN_OUT_6

Ввод: Составной обратного считывания (Float32 + Unsigned8), статус Unsigned8, статус Unsigned8, статус Unsigned8.

Пример кодирования для секции DataItem для F_Channel_Driver F_IN_OUT_6 показан на рисунке 60. Таблица 10 содержит описание переменных.

```
<IOData>
        <Input Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" TextId="AI channel" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status1" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status2" />
                <DataItem DataType="Unsigned8" UseAsBits="false" TextId="Status3" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
        </Input>
        <Output Consistency="All items consistency">
                <DataItem DataType="Float32+Unsigned8" UseAsBits="false"TextId="AO channel" />
                <DataItem DataType="F_MessageTrailer4Byte" TextId="Safety" />
    </Output>
</IOData>

VERSION                                  01
IN_ADDRESS_RANGE                         12
COUNT_PS_INPUT_BYTES_COMPOSITE           05
COUNT_PS_INPUT_CHANNELS_BOOL             24
COUNT_PS_INPUT_BYTES_BOOL                03
COUNT_PS_INPUT_CHANNELS_INT              00
COUNT_PS_INPUT_CHANNELS_REAL             00
OUT_ADDRESS_RANGE                        09
COUNT_PS_OUTPUT_BYTES_COMPOSITE          05
COUNT_PS_OUTPUT_CHANNELS_BOOL            00
COUNT_PS_OUTPUT_BYTES_BOOL               00
COUNT_PS_OUTPUT_CHANNELS_ INT            00
COUNT_PS_OUTPUT_CHANNELS_ REAL           00
DATA_STRUCTURE_CRC                       0xF33
```

Рисунок 60 — Секция DataItem для F_IN_OUT_6

8.5 Использование информации типов данных

8.5.1 Драйвер F-канала

F-данным I/O, циклически передающимся между F-устройством и F-хостом (канал реального времени), требуется управление посредством пользовательской программы. Программист либо ожидает появления надлежащих Функциональных блоков («драйвера F-канала») в его/ее (программиста) библиотеках инструментов, которые она/он способен встроить в программу клиента. Либо она/он ожидает получения доступа к дискретным, логически адресуемым переменным ввода или вывода (например, для многоступенчатой логики). На рисунке 61 показано как подобный программист видит функциональные блоки «драйвера F-канала».

8.5.2 Правила для стандартных драйверов F-канала

Общая поддержка системы всеми типами F-хостов может быть достигнута, следуя набору правил для проектирования структур F-данных, передающихся циклически:

- структура данных в секции IODataSection файла GSD. Подробное описание см. в 8.3.2;
- сформированная структура данных должна иметь следующий порядок: сначала все смешанные типы Float32 + Unsigned8, если таковые доступны. Затем все переменные типов Unsigned8, Unsigned16, Unsigned32, если таковые доступны. Затем все переменные типа Integer16, если таковые доступны. Затем все переменные с плавающей точкой, если таковые доступны.

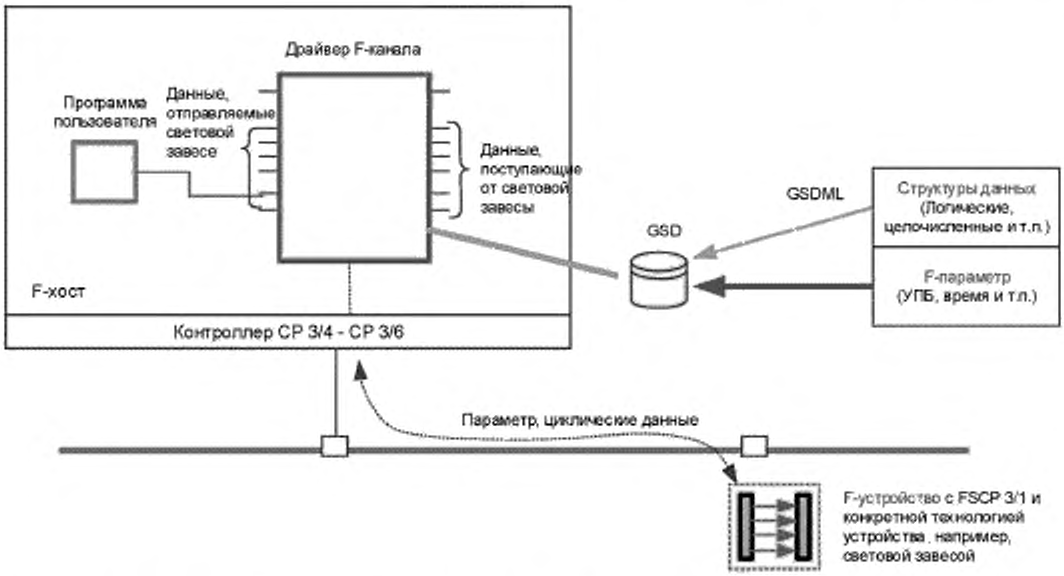


Рисунок 61 — Драйвер F-канала в качестве «клея» между F-устройством и пользовательской программой

Таблица 11 содержит список образцов драйверов F-канала. Драйвера представляют собой разные структуры данных для F-ввода и F-вывода, в соответствии с ассоциированными PDU безопасности. Разрешенные типы данных для FSCP 3/1 перечислены в 5.5.4. Таким образом, 32-битовые логические значения должны быть отображены на тип данных Unsigned32, а 8-битовые на тип данных Unsigned8. Подробности см. в 8.4.2.

Таблица 11 — Образцы драйверов F-канала

Конфигурация драйвера F-канала[a)]	F-ввод (устройством)	F-вывод (для устройства)	Замечания
F_IN_OUT_1	32 логический	32 логический,	например, световая завеса
F_IN_OUT_2	16 логический, 1 Integer16	16 логический, 1 Integer16	например, лазерные сканнеры
F_IN_OUT_5	1 Float32, Unsigned8 (8-битовый «квалификатор»)		например, датчик избыточного давления
F_IN_OUT_6	«обратное считывание»: 1 Float32, 8-битовый «обратная проверка»: 24 бита	«Уставка»: 1 Float32, 8 бит	например, пневмоклапан
[a)] Не обязательно, что нумерация подразумевает различные драйверы. Это может быть один драйвер, параметризованный посредством GSD информации.			

Ограничения:

- неиспользованные биты должны быть установлены в значение «0»;
- индикаторы статуса и сбоя F-устройства должны быть определены в структуре данных ввода, если это необходимо (например, квалификатор).

8.5.3 Рекомендации для драйверов F-канала

На рисунке 62 показан пример макета драйвера хоста F-канала для сложного F-устройства.

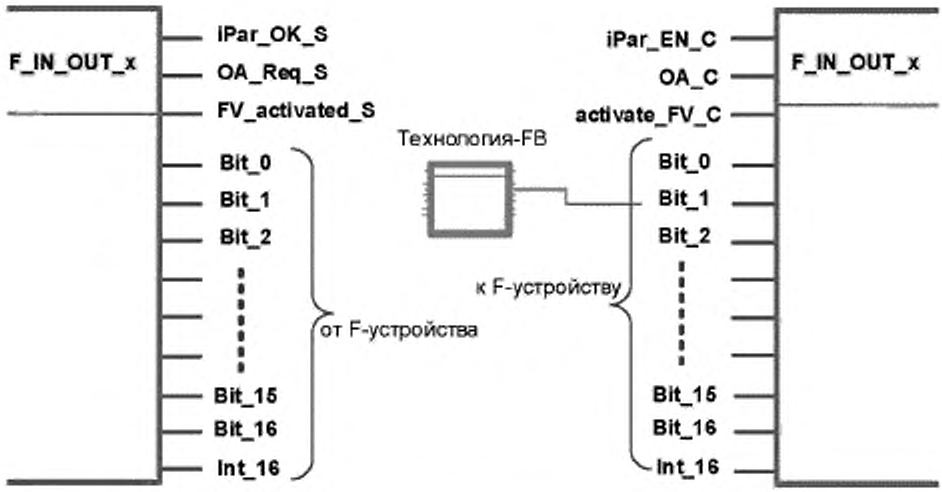


Рисунок 62 — Пример макета драйвера F-канала

Термины, использованные на рисунке 62, а также поведение драйвера описаны ниже:

iPar_EN_C	— включена iпараметризация;
iPar_OK_S	— iпараметризация завершена;
OA_C	— подтверждение оператора (для возобновления после сбоя);
OA_Req_S	— когда сбой (сторожевого таймера, CRC, порядкового номера) был обнаружен и удален;
FV_activated_S	— отказоустойчивые значения, активированные F-устройством;
activate_FV_C	— отказоустойчивые значения, которые будут активированы в F-устройстве;
Фиксированное поведение драйвера F канала	— отказоустойчивые значения, установленные в «0».

В дополнении к структурам данных, зависящим от устройства, существует больше сигналов FSCP 3/1, доступных программисту. Подробную информацию об упомянутых выше сигналах см. в 7.1.3 и 6.1.

По соображениям производительности драйвер F-канала может быть разделен на два функциональных блока, один для вводов, а другой для выводов (рисунок 62). Существует фиксированное поведение драйверов F-канала применительно к отказоустойчивым значениям: независимо от того состоит ли структура данных из битов (Unsigned8), Integer16, Float32 или Float32 + Unsigned8, каждое значение устанавливает в «0». Если исполнительные устройства не могут согласиться с FV = «0», то могут быть реализованы другие значения, либо с жесткой кодировкой, либо посредством iпараметров. Пользовательские программы могут активировать эти, зависящие от устройства, отказоустойчивые значения посредством бита 4 в байте управления (см. 7.1.3). Если датчики не могут признать FV = «0», то дополнительная логика пользовательской программы может преобразовать их в индивидуальные значения, используя ввод «activate_FV_C» драйвера F-канала.

8.6 Механизмы назначения параметров безопасности

8.6.1 Назначение F-параметров

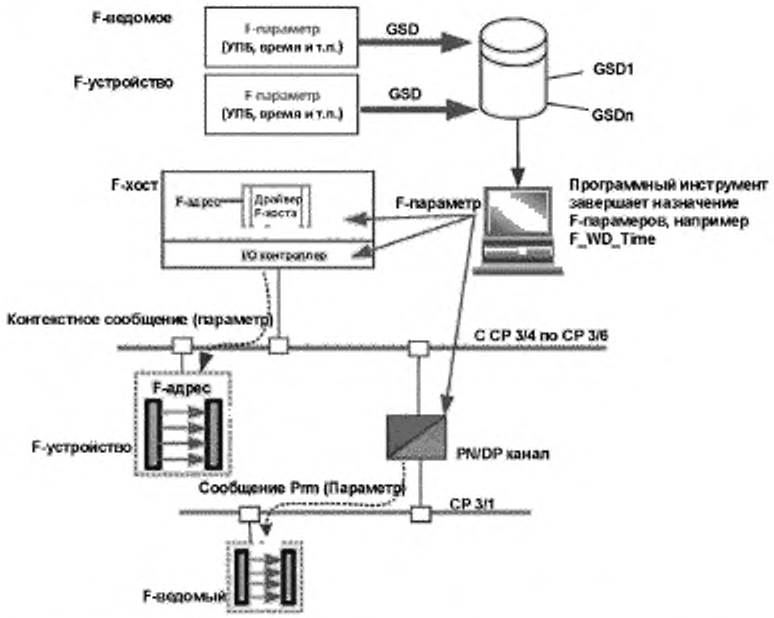


Рисунок 63 — Назначение F-параметров простым F-устройствам и F-ведомым устройствам

Простые F-устройства без iпараметров могут быть обеспечены путем стандартного Контекстного Сообщения. См. МЭК 61158-5-10, МЭК 61158-6-10 и [55]. Общее число F-параметров, таким образом, не может превышать предел в 234 октета (рисунок 63).

8.6.2 Общее назначение iпараметров

Для сложных устройств с iпараметрами должно быть принято решение (по вопросу безопасности) будет ли автоматическое назначение при запуске предпочитаться отдельному назначению, осуществляемому CPD-инструментом для определенного F-устройства, как это предлагается в МЭК 62061. В любом случае F-хост должен разблокировать назначение только, если не наблюдается опасное состояние процесса (7.4.2). В основном возможны два способа, которые могут содействовать друг другу:

- присвоение значений iпараметров посредством специальных прокси функциональных блоков в F-хосте и подходящего набора данных iпараметров;
- присвоение значений iпараметров посредством специального CPD-инструмента через IO-супервизора (программный инструмент/PC).

CPF 3 предлагает стандартную коммуникационную платформу для программного управления через *Коммуникационные функциональные блоки* в соответствии с МЭК 61131-3 и *Прокси Функциональные Блоки* в соответствии с МЭК 61131-3, в частности с помощью языка программирования ST (Структурированного текста), тем самым поддерживая первый способ.

Производителям F-устройства дана возможность предоставить портативное программное обеспечение управления для их устройств.

На рисунке 64 представлен пример того, как стандарты CPF 3 могут использоваться для предоставления очень комфортной и гибкой поддержки системы для F-устройств. Специализированный CPD-инструмент производителя устройства вступает в коммуникации (1) со своим F-устройством (в данном случае со световой завесой) либо, используя прямой и отдельный канал (например, USB), либо посредством непериодических услуг — чтение/запись записанных данных (см. рисунок 15) параллельно, по всей полевой шине, с циклическим обменом данными. После параметризации и ввода в эксплуатацию, Прокси Функциональный Блок может быть активирован для загрузки iпараметров в контроллер (2), где они готовы для скачивания в случае замены (ремонта) устройства.

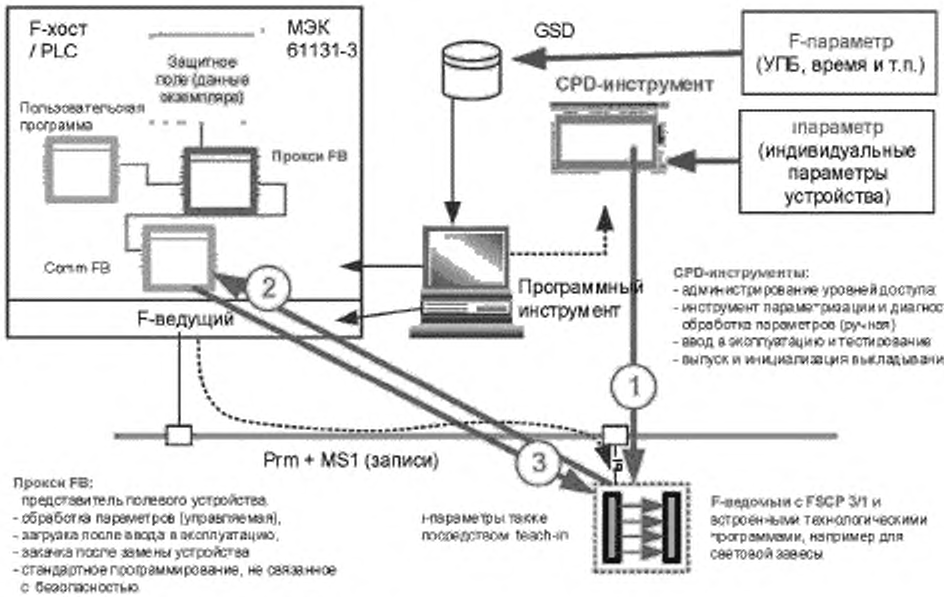


Рисунок 64 — Назначение F и iпараметров для сложных F-устройств

Набор правил, заложенный в программы, посредством управляемого этими программами динамическим назначением iпараметров, может удовлетворить очень гибкие требования в сегодняшних производствах. Таким образом, несколько различных наборов данных или, например, координат для зон обнаружения световой завесы («гашение») могут быть назначены один за другим (рисунок 64). Идентификационный номер действительного набора iпараметров должен сообщаться циклически в рамках F-данных I/O.

8.6.3 Требования интеграции системы для инструментов iпараметризации

В таблице 12 содержится список требований, которые должны быть выполнены процедурами iпараметризации.

Таблица 12 — Требования для iпараметризации

Номер	Системное требование
R1	Должен быть спроектирован CPD-Инструмент для совместимых персональных компьютеров или лаптопов, а также операционных систем от WIN2000 и позднее
R2	Несколько CPD-инструментов или экземпляров CPD-инструментов должно функционировать параллельно
R3	CP 3/1. Интерфейсные платы класса 2 ведущего устройства должны предоставлять унифицированный API (прикладной программный интерфейс) такой, что CPD-инструменты могли бы быть сконфигурированы для работы на разных платах
R4	CP 3/RTE. Интерфейс IO-супервизора должен быть определен таким образом, чтобы «не периодические» услуги CP 3/RTE могли бы использоваться для F-устройства, непосредственно подсоединенного к сети CP 3/RTE
R5	CP 3/RTE. Интерфейс IO-супервизора должен быть определен таким образом, чтобы «не периодические» услуги CP 3/RTE могли бы использоваться для F-устройства, непосредственно подсоединенного к сети CP 3/RTE, или через «Канал» к F-ведомому устройству, подключенному к «дополнительной» сети CP 3/1 (для регистрации инициации, чтения и записи и т.п.)
R6	Соединения R4 и R5 должны быть также возможны посредством порта F-хоста для программистов

Окончание таблицы 12

Номер	Системное требование
R7	«Каналы-PN/DP» должны быть доступны как автономные устройства либо как интегрированные в контроллер
R8	Индикация интерфейса полевой шины. F-устройство должно указывать на свой тип интерфейса полевой шины. Не требуется, если определен унифицированный API (см. R3), подходящий для не периодических коммуникаций CPF 3
R9	Для хранения данных F-устройства внутри всеобщей базы данных проектов, обращение к ней выполняется с помощью параметра «Вызова» или используется интегрированный интерфейс программного инструмента. Должно быть предусмотрено автоматическое управление версиями наборов данных iпараметра
R10	Имя станции/адреса должно быть определено как параметр «Вызова»
R11	Путь к файлу GSD должен быть определен как параметр «Вызова»
R12	Многоязыковая поддержка должна быть определена как параметр «Вызова». Программный инструмент хоста (Host-Engineering-Tool) должен задавать язык по умолчанию при вызове
R13	Авторизация (роли и права доступа) должна наследоваться от программного инструмента хоста и передаваться CPD- инструменту при вызове
R14	Скачивание iпараметров на F-устройство. Поток октетов iпараметров должен определяться таким образом, чтобы его можно было хранить в IO контроллере и передавать F-устройству во время общей параметризации. PROXY-FB по-прежнему является лучшим решением для FSCP 3/1
R15	Версия. Интерфейсы API (см. R3 и R4) должны предоставлять номер версии, такой, чтобы CPD-инструменты могли бы автоматически подстраивать сами себя
R16	Распечатка. Должно быть предусмотрено «удаленное управление» индивидуальными CPD-инструментами из программного инструмента хоста для пакетной печати или для доставки распечаток в стандартизированном формате (например, HTML) программному инструменту хоста
R17	Загрузка и Скачивание iпараметров. Должно быть предусмотрено «удаленное управление» специальными CPD-инструментами из программного инструмента хоста для пакетной «iпараметризации» или доставлять iпараметры в стандартизированном формате программному инструменту хоста (см. R14)
R18	CPD-Инструмент должен быть активирован на предоставление имен символов по умолчанию (например, «OSSD1») программному инструменту хоста и получение взамен финальных назначенных символьных имен проекта в случае диагностики. Предоставление символьных имен по умолчанию возможно в случае GSD файла CP 3/RTE
R19	Для того чтобы достигнуть независимости от лежащего в основе черного канала, должен использоваться тот же принцип защиты передачи данных iпараметра, что используется для циклического обмена данными, который представлен на рисунке 26 и описан в связанном с ним разделе, т. е. вычисление iпар CRC32 должно осуществляться в обратным порядком байтов (начальное значение не должно быть нулем). Производитель может использовать свой собственный метод для защиты iпараметров, если выполняются требующиеся критерии (iпар-сервер, CPD-инструмент)

На рисунке 65 показаны системные аспекты интеграции инструмента CPD (CPD-Tool-Integration). CPD-инструмент может быть подключен к одному из следующего:

- F-Устройству напрямую (например, USB, RS232);
- F-Хосту посредством порта программиста;
- CP 3/RTE и CP 3/1 через Канал;
- CP 3/1 или CP 3/2

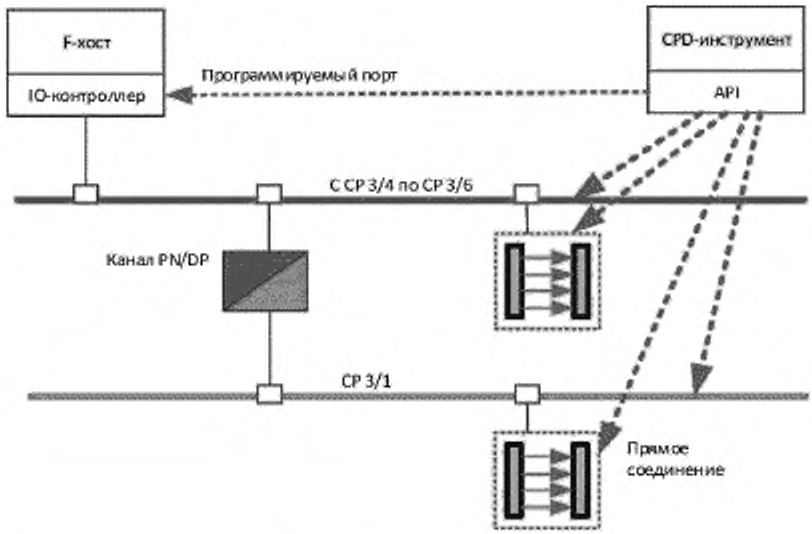


Рисунок 65 — Интеграция системы CPD-инструментов

8.6.4 iПар-сервер

8.6.4.1 Общее описание и ограничения

Концепция iпар-сервера является специализированной формой более общей концепции проксифблока, как это отмечено в 8.3.1. Ответственность за предоставление этой возможности лежит на производителях F-хоста, как это заявлено в таблице 23, независимо от того, реализована ли она в части F-хоста, действующего в качестве ведущего устройства для параметризации, не связанной с безопасностью, в управляемой подсистеме, такой как PLC, не связанной с безопасностью, или на промышленном компьютере в той же сети.

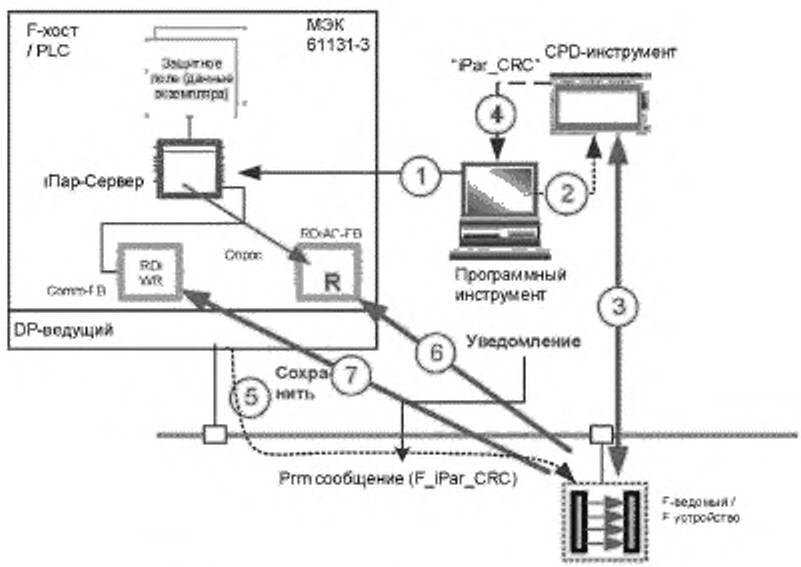


Рисунок 66 — Механизм iпар-сервера (ввод в эксплуатацию)

На рисунке 66 показаны принципиальные шаги механизма iпар-сервера. Вместе с конфигурированием сети и F-параметризацией F-ведомого устройства/F-устройства создается экземпляр и соответствующей функции iпар-сервера (шаг 1). F-ведомое устройство/F-устройство способно входить в режим обмена данными, используя безопасное состояние (FV-значения). Ассоциированный CPD инструмент может быть запущен посредством надлежащего интерфейса (шаг 2) из программного инструмента, распространяя хотя бы адрес узла сконфигурированного устройства. Параметризация, ввод в эксплуатацию, испытание и т. п. может быть выполнено с помощью CPD инструмента (шаг 3). После завершения вычисляется сигнатура iPar_CRC и отображается в шестнадцатеричной форме для, как минимум, копирования и вставки этого значения в поле записи «F_iPar_CRC» конфигурационной части программного инструмента (шаг 4). Перезапуск F-ведомого устройства/F-устройства необходим для передачи параметра «F_iPar_CRC» F-ведомому устройству/F-устройству (шаг 5). После окончательной верификации и выпуска F-ведомое устройство/F-устройство активировано для инициализации уведомления о загрузке (шаг 6) в его экземпляр iпар-сервера. Оно, тем самым, использует средства диагностики CPF 3 (8.6.4.2 и [49]). iпар-сервер опрашивает диагностическую информацию (например, RDIAG Фблока) для интерпретации запроса (R) и для установления процесса загрузки (шаг 7), который хранит iпараметры как экземпляр данных в хосте iпар-сервера.

На рисунке 67 показана вторая часть механизма iпар-сервера. В случае замены дефектного F-ведомого устройства/F-устройства (шаг 1) F-ведомое устройство/F-устройство принимает свои F-параметры, включая «F_iPar_CRC» (шаг 2), при запуске. Так как iпараметры, как правило, отсутствуют при замене или не сохраняются F-ведомым устройством/F-устройством, то оно инициализирует уведомление скачивания (шаг 3) в экземпляр своего iпар-сервера. Тем самым, оно использует средства диагностики CPF 3 (8.6.4.2 и [49]). iпар-сервер опрашивает диагностическую информацию (например, RDIAG Фблока) для интерпретации запроса (R) и для установления процесса скачивания (шаг 4). С помощью этой передачи F-ведомое устройство/F-устройство способно предоставлять исходный функционал без использования дополнительных программных или CPD инструментов.

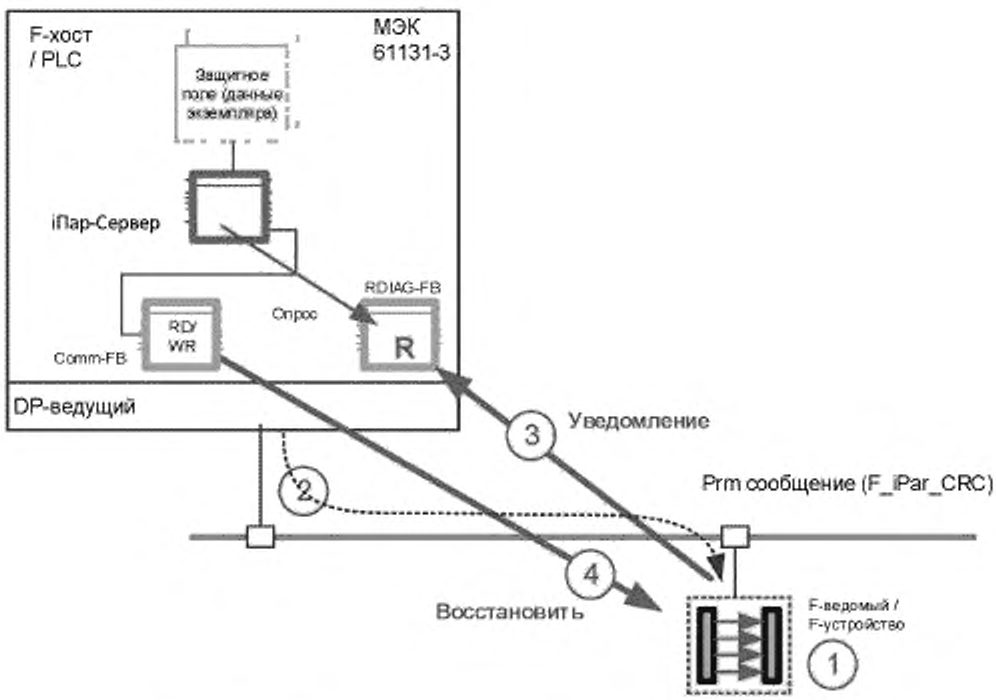


Рисунок 67 — Механизм iпар-сервера (например, замена F-устройства)

Следующие ограничения были определены для механизма iпар-сервера:

- каждый экземпляр iпар-сервера должен поддерживать минимум 2^{15}-1 октетов iпараметров на F_Source/Destination_Address (устройство/подмодуль/модуль);
- iпараметры хранятся как один фиксированный блок данных, как это показано на рисунке 52;
- iпар-сервер не связан с безопасностью. Он может быть реализован или запущен в стандартном хосте или в стандартной части F-хоста (рисунок 67);
- iпар-сервер должен быть доступен только в совокупности с режимом V2 из FSCP 3/1;
- ответственность за то, что скачанный набор iпараметров соответствует, например, корректному типу и версии у заменяющего устройства, лежит на производителе F-ведомого устройства/F-устройства;
- F-модуль/F-ведомое устройство/F-устройство должно инициализировать Запрос-iпар-сервера, когда черный канал гарантирует доставку уведомления;
- разрешено одно повторение каждый раз, когда попытка «Восстановление» не удается (отказ). Соответствующая функция безопасности сохраняет безопасное состояние (FV значения);
- «Восстановление» должно выполняться только при запуске системы/F-устройства.

8.6.4.2 Уведомление

Диагностическое сообщение — это единственный стандартный механизм уведомления iпар-сервера в сетях типа CPF 3, требующийся для F-ведомого устройства/F-модуля. Тем не менее, в отличие от стандартного контекста диагностики, уведомление iпар-сервера не нуждается в передачи информации каким-либо инструментам визуализации для поддержания взаимодействия. Из нескольких разных типов CP 3/1 и CP 3/2, установленных в МЭК 61158-5-3, предпочтительное кодирование диагностической информации связано со «Статусной Моделью» [50]. Для того чтобы избежать конфликтов с уже существующими типами в предварительно зарезервированном диапазоне был определен новый тип статуса «Запрос iпар-сервера» (тип = 7).

Примечание — «Обновленная аварийная сигнализация» (тип=6) не была выбрана в качестве этого типа и, как правило, ведет к отображению аварийной информации и следует другой семантике. Целью FSCP 3/1 является установление кодировок для двух типов диагностических сообщений для CP 3/1, CP 3/2 и CP 3/RTE настолько приближенно насколько возможно, таким образом, чтобы F-модулю внутри удаленного I/O не требовалось знать о своем развертывании.

На рисунке 68 показано кодирование запроса iпар-сервера для CP 3/1 и CP 3/2.

Рисунок 68 — Кодирование запроса iпар-сервера («модель статуса»)

Каждое кодирование «Запроса iпар-сервера» начинается с шести обязательных октетов стандартного диагностического блока. Флаг «Diag.ext.diag» (бит 3 первого октета) не должен подвергаться влиянию, так как ни один светодиодный индикатор не должен быть включен в случае отсутствия отчетов о дефектах. Следующие 4 октета соответствуют стандартному кодированию, описанному в МЭК 61158-5-3 и показанному на рисунке 68. Тип статуса есть новый «Запрос iпар-сервера» (7). Спецификатор статуса должен быть установлен в значение «0». Тело «Запроса iпар-сервера» содержит спецификаторы, определенные в таблице 13.

F-модуль в удаленном I/O всегда использует кодирование, показанное на рисунке 68, или из надлежащего поднабора, для всех случаев, когда он может быть внедрен в удаленное I/O устройство CP 3/1 или CP 3/RTE. Удаленный I/O должен отправлять по одному уведомлению за раз и, тем самым, сохранять или восстанавливать iпараметры F-модуля за F-модулем. Подсказки для проектирования в случаях диагностической перегрузки (например, «Diag.Ext_Diag_Overflow») можно найти в [50].

Примечание — Кодирование передачи информации между модулем и головной станцией не стандартизировано.

Трансформация кодировки запроса iпар-сервера в надлежащий формат актуального коммуникационного профиля является задачей головной станции удаленного I/O устройства (рисунок 68 или 70).

Таблица 13 — Спецификатор для Запроса iпар-сервера

iпар спецификатор	Название	Октет 3	Октет 2	Октет 1	Октет 0	Определение
iPar0	iPar_Req_Header	SR_Version	Reserved	N_Count	SR_Type	Тип запроса iпар-сервера (Unsigned32)
iPar1	Max_Segm_Size	0x00h	0x00h	0x00h	0...234	Максимальный разрешенный размер сегмента в октетах (Unsigned32)
iPar2	Transfer_Index	0x00h	0x00h	0x00h	0...254 (255)	Индекс для передачи регистрации записи/чтения (Unsigned32)
iPar3	Total_iPar_Size					Общая длина октетов iпараметра (Unsigned32)

Примечания

1 Зарезервировано: См. 7.1.3, подсказки.

2 Параметр «Max_Segm_Size» может быть больше, чем 234 октета, в случае CP 3/RTE. Он может включать вплоть до 2^{22}-1 октетов, что вызвано ограничениями FSCP 3/1.

3 «Transfer_Index» в 255 октетов может конфликтовать с другими услугами, такими как, CALL (вызов) ИТО функций.

4 Параметр «Transfer_Index» может быть больше, чем 255 октетов, в случае CP 3/RTE он может достигать до 65 535.

5 Заменяющее устройство может не знать корректного размера iпараметра своего предшественника. В таком случае уведомление для восстановления может содержать «Total_iPar_Size = 0», что означает, что iпар-сервер будет скачивать полный набор данных iпараметров.

6 N_Count является счетчиком последовательности для уведомлений (только для CP 3/1 и CP 3/2), считая от 1 до 15 и сначала.

Параметр «SR_Version» должен быть установлен в 0x01h. Параметр «N_Count» должен начинаться с «1» и увеличиваться с каждым уведомлением (только в случаях CP 3/1 и CP 3/2) до значения 15 и затем продолжаться, начав со значение «1». Параметр «SR_Type» должен кодироваться, как показано на рисунке 69.

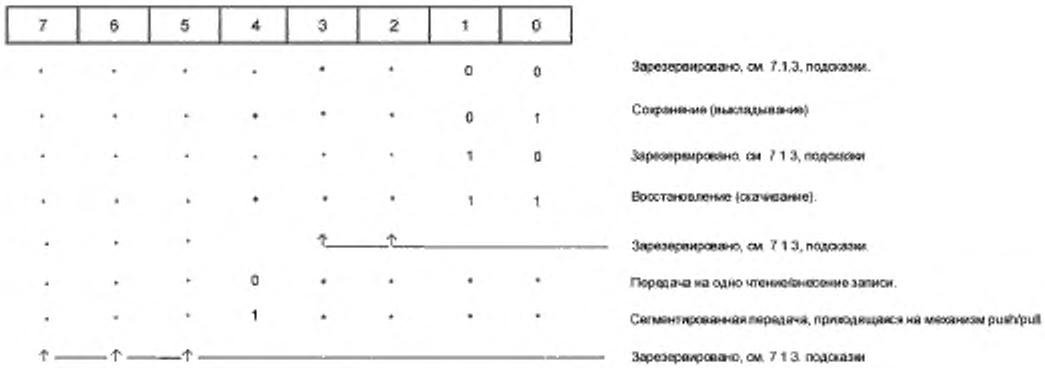


Рисунок 69 — Кодирование SR_Type

Возможная реализация аналога внутри, например, не связанной с безопасностью части F-хоста, описана в [49] и называется функциональным блоком коммуникаций RDIAG.

После отправки запроса iпар-сервера F-ведомое устройство/F-модуль ожидает 2^{18} мс (приблизительно 4,4 минут) полного выполнения услуги «Save» (Сохранить) или «Restore» (Восстановить). По истечению этого времени, он запускает надлежащее диагностическое сообщение в соответствии с 6.3.2. Предпочтительное кодирование диагностической информации в CP 3/RTE для iпар-сервера связано с «Моделью Аварийного сигнала» и со стандартным «Upload&Retrieval» аварийным сигналом, определенным в МЭК 61158-5-10 и МЭК 61158-6-10. На рисунке 70 показано кодирование запроса iпар-сервера для CP 3/RTE (МЭК 61784-2). После отправки запроса iпар-сервера F-устройство/F-модуль ожидает 2^{18} мс (приблизительно 4,4 минуты) для полного завершения сервиса «Сохранить» или «Восстановить». По истечению этого времени, оно запускает надлежащее диагностическое сообщение в соответствии с 6.3.2. В случае запрос iпар-сервера на «Восстановление» и при отсутствии хранимых iпараметров, iпар-сервер должен отправить запись длиной «0».

Рисунок 70 — Кодировка запроса iпар-сервера («модель аварийного сигнала»)

8.6.4.3 Услуги

iпар-сервер является маленькой программой, вызываемой каждый основной цикл, например, внутри не связанной с безопасностью части F-хоста. Он собирает диагностическую информацию, опрашивая определенные F-ведомые устройства/F-модули, в поисках любых запросов двух типов: «Сохранения» и «Восстановления». Для того чтобы выполнить эти запросы он использует стандартные не периодические услуги «читать запись» (read record) и «внести запись» (write record), как это определено в МЭК 61158-5-3. Для небольших наборов iпараметров достаточно обычной несегментированной версии для каждой «записи чтения» и «внесения записи» (таблицы 14 и 15). Возможная реализация этих двух функций, основанная на языках программирования из МЭК 61131-3, описана в [49] и называется функциональными блоками коммуникаций RDREC и WRREC. Настоятельно рекомендуется использовать эту реализацию для F-хост систем для предоставления этих функциональных блоков в рамках библиотеки, предназначенной для части, не связанной с безопасностью.

Таблица 14 — Структура Read_RES_PDU («записи чтения»)

Структура Read_RES_PDU	Размер	Кодирование	Примечания	
Function_Num	1 октет	0x5E	Указывает на «Read», fix	Заголовок
Slot_Number	1 октет	0 … 255	Местоположение модуля	
Index	1 октет	0 … 254	"Transfer_Index"	
Length of net data	1 октет	0 … 240	Длина сегмента iПар	
iParameter (сегмент)	*л* октетов	–	*л* = 240 максимум на запись	Данные
Примечание — Соответствующие структуры для CP 3/RTE можно найти в [49].				

Таблица 15 — Структура Write_REQ_PDU («записи внесения»)

Структура Write_REQ_PDU	Размер	Кодирование	Примечания	
Function_Num	1 октет	0x5F	Указывает на «Write», fix	Заголовок
Slot_Number	1 октет	0 … 255	Местоположение модуля	
Index	1 октет	0 … 254	"Transfer_Index"	
Length of net data	1 октет	0 … 240	Длина сегмента iпар	
iParameter	n октетов	–	n = 240 максимум	Данные

Для наборов iпараметров, превышающих предел записи или буфера определенного F-ведомого устройства/F-модуля может использоваться расширенная версия не периодических услуг «читать запись» и «внести запись», описанная в МЭК 61158-5-3 как услуги «Pull» и «Push» (выталкивание и проталкивание), показанные в таблицах 16 и17.

Таблица 16 — Структура Pull_RES_PDU («Pull»)

Структура Pull_RES_PDU	Размер	Кодирование	Примечания	
Function_Num	1 октет	0x5E	Указывает на «Read», fix	Заголовок
Slot_Number	1 октет	0 … 255	Местоположение модуля	
Index	1 октет	0 … 254 (255)	"Transfer_Index" [a]	
Length of net data	1 октет	0 … 240	Длина сегмента iпар + заголовок области загрузки	
Extended_Function_Num	1 октет	0x02	Указывает на «Pull»	Область загрузки
Options	1 октет	Unsigned8	Управление потоками, см. МЭК 61158-5-3, 6.2.17.2	
Sequence_Number	4 октета	Unsigned32	…текущего iPar сегмента	
iParameter (сегмент)	*л* октетов	Строка октетов	*л* = 240 максимум на запись	Данные

[a] «Transfer_Index» из 255 в данном случае соответствует МЭК 61158-5-3. Тем не менее, конфликты доступа с другими услугами, такими как CALL и функции ИТО, должны рассматриваться при проектировании и реализации. Все другие индексы могут использоваться для услуг «Pull» и «Push».

Таблица 17 — Структура Push_REQ_PDU («Push»)

Структура Pull_RES_PDU	Размер	Кодирование	Примечания	
Function_Num	1 октет	0x5F	Указывает на «Write», fix	Заголовок
Slot_Number	1 октет	0 … 255	Местоположение модуля	
Index	1 октет	0 … 254 (255)	"Transfer_Index" [a]	
Length of net data	1 октет	0 … 240	Длина сегмента iПар + заголовок области загрузки	
Extended_Function_Num		0x01	Указывает на «Push»	Область загрузки
Options	1 октет	Unsigned8	Управление потоками, см. МЭК 61158-5-3, 6.2.17.2	
Sequence_Number	4 октета	Unsigned32	…текущего iPar сегмента	
iParameter (сегмент)	*n* октетов	Octet String	*n* = 240 максимум на запись	Данные

[a] «Transfer_Index» из 255 в данном случае соответствует МЭК 61158-5-3. Тем не менее, конфликты доступа с другими услугами, такими как CALL и функции ИТО, должны рассматриваться при проектировании и реализации. Все другие индексы могут использоваться для услуг «Pull» и «Push».

F-хост или ассоциированная система, не связанная с безопасностью, могут предоставлять механизм iпар-сервер совершенно скрытым от пользователя или в качестве набора функций библиотеки, которые необходимо сконфигурировать для определенного проекта.

Примером для стандартного сервера параметров будет механизм «Upload&Retrieval» (Загрузка и Извлечение) из CP 3/RTE, как это определено в МЭК 61158-5-10, МЭК 61158-6-10 и МЭК 61784-2 (CP 3/RTE).

F-модуль в удаленном I/O всегда использует надлежащее кодирование, всякий раз, когда он может быть внедрен в CP 3/1 или удаленное устройство I/O CP 3/RTE. Преобразование кодировки передачи iпараметров в надлежащий формат актуального коммуникационного профиля и обратно является задачей головной станции удаленного I/O устройства.

Индексы записей для услуг «Сохранить» и «Восстановить» могут отличаться. Также возможно, что услуга «Восстановить» будет читать меньшее число данных, чем было сохранено прежде. Эти сохраненные данные могут содержать информацию о проверке, такую как, тип устройства, длина данных, подпись CRC, и т. п. в дополнение к iпараметрам. Скачивание короткой записи с информацией проверки позволяет верифицировать непротиворечивость данных и их актуальность, не влияя на эффективности.

8.6.4.4 Протокол

На рисунке 71 показана диаграмма состояний iпар-сервера, а в таблице 18 описаны состояния iпар-сервера, а также переходы и внутренние элементы. Общую информацию о нотации UML2 см. в 7.2.2.

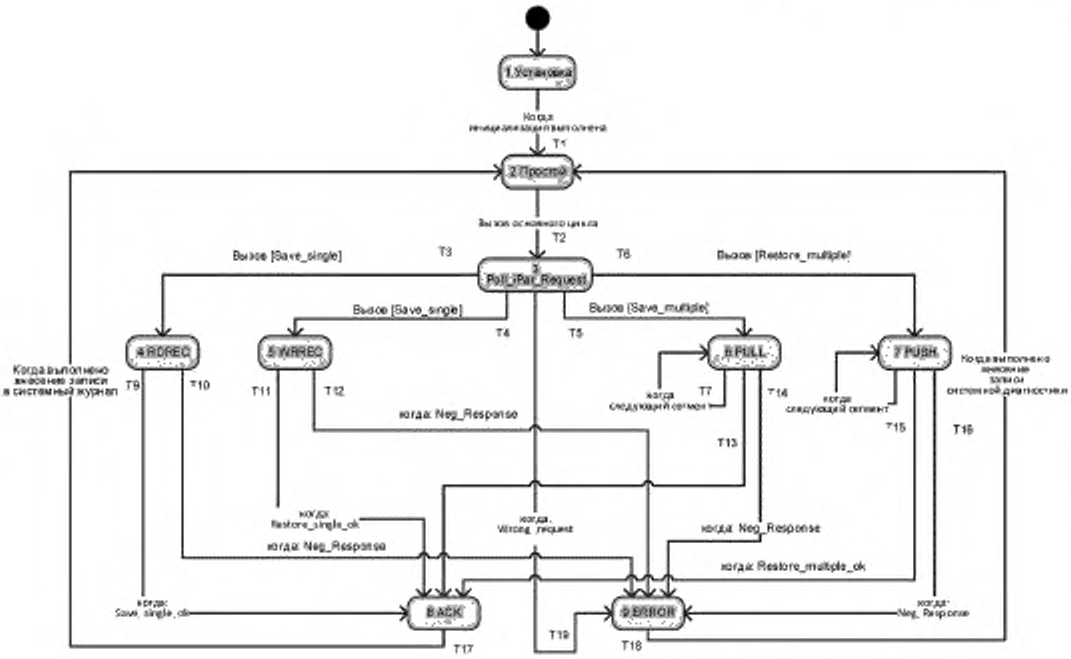


Рисунок 71 — Диаграмма состояний iпар-сервера

Термины, используемые на рисунке 71 описаны ниже:

Save_single — запрос iпар-сервера на сохранение (загрузку) одного блока iпараметров на запись (RDREC);

Restore_single — запрос iпар-сервера на восстановление (скачивание) одного блока iПараметров на запись (WRREC);

Save_multiple — запрос iпар-сервера на восстановление (скачивание) большего блока iпараметров для множества записей (PULL);

Restore_multiple — запрос iпар-сервера на восстановление (скачивание) большего блока iпараметров для множества записей (PUSH);

System log entry (запись в системный журнал) — любое успешное действие сохранения и восстановления может быть записано в файл журнала iпар-сервера (не обязательная функция);

System diagnosis entry (запись системной диагностики) — любое неуспешное действие сохранения или восстановления должно быть зафиксировано в отчете посредством системных средств диагностики;

Neg_Response — каждый раз, когда системная функция, такая как RDREC, WRREC, PULL или PUSH прерывает работу, выдавая ошибку, iпар-сервер должен создавать запись о диагностике системы;

Wrong_request — каждый раз, когда iпар-сервер обнаруживает неверный тип запроса или отсутствие реакции любых вызванных системных функций, он должен прервать действие и создать запись о диагностике системы.

Таблица 18 — Состояния iпар-сервера и переходы

НАИМЕНОВАНИЕ СОСТОЯНИЯ	ОПИСАНИЕ СОСТОЯНИЯ
1. Initialisation (Инициализация)	Состояние холодного запуска; инициализации выводов, если таковые определены
2 Idle (Простой)	Состояние простоя, нет действий
3 Poll_iPar_Request	При вызове основного цикла или другой подобной деятельности в управляемой подсистеме в теле диагностической информации интерпретируется запрос iпар-сервера и запускается соответствующая услуга системы. В случае ошибок, должен быть осуществлен переход в состояние ERROR
4 RDREC	В данном состоянии должна вызываться системная функция RDREC (в соответствии с [49]) или другая подобная функция, выполняющая функцию чтения в соответствии с CP 3/1 или CP 3/2 в МЭК 61158-5-3
5 WRREC	В данном состоянии должна вызываться системная функция WRREC (в соответствии с [49]) или другая подобная функция, выполняющая функцию внесения записи в соответствии с CP 3/1 или CP 3/2 в МЭК 61158-5-3
6 PULL	В данном состоянии должна вызываться системная функция PULL, выполня-ющая функцию множественного чтения посредством «Extended_Function_Num» = 0x02 в соответствии с CP 3/1 или CP 3/2 в МЭК 61158-5-3
7 PUSH	В данном состоянии должна вызываться системная функция PULL, выполня-ющая функцию множественного внесения записей посредством «Extended_Function_Num» = 0x01 в соответствии с CP 3/1 или CP 3/2 в МЭК 61158-5-3
8 ACK	В данном состоянии любое успешное действие сохранения или восстановления может быть записано в «системном файле журнала iпар-сервера» (не обязательная функция)
9 ERROR	Каждый раз, когда системная функция, такая как RDREC, WRREC, PULL, или PUSH прекращает работу, выдавая ошибку, или в случае ошибочного запроса, iпар-сервер должен, в рамках данного состояния, создавать запись о диагностики системы

Продолжение таблицы 18

ПЕРЕХОД	ИСХОДНОЕ СОСТОЯНИЕ	ЦЕЛЕВОЕ СОСТОЯНИЕ	ДЕЙСТВИЕ
T1	1	2	-
T2	2	3	Вызов основного цикла (или другого подобного события в управляемой подсистеме)
T3	3	4	Вызов функции RDREC для загрузки одного блока iпараметров
T4	3	5	Вызов функции WRREC для скачивания одного блока iпараметров
T5	3	6	Вызов функции POLL для множественного скачивания большего сегментированного блока iпараметров
T6	3	7	Вызов функции PUSH для множественного скачивания большего сегментированного блока iпараметров
T7	6	6	Начать читать следующий сегмент
T8	7	7	Начать записывать следующий сегмент
T9	4	8	Начать запись в файл системного журнала об успешном выполнении RDREC (не обязательно)
T10	4	9	Начать запись системной диагностики
T11	5	8	Начать запись в файл системного журнала об успешном выполнении WRREC (не обязательно)
T12	5	9	Начать запись системной диагностики
T13	6	8	Начать запись в файл системного журнала об успешном выполнении POLL (не обязательно)
T14	6	9	Начать запись системной диагностики

Окончание таблицы 18

ПЕРЕХОД	ИСХОДНОЕ СОСТОЯНИЕ	ЦЕЛЕВОЕ СОСТОЯНИЕ	ДЕЙСТВИЕ
T15	7	8	Начать запись в файл системного журнала об успешном выполнении PUSH (не обязательно)
T16	7	9	Начать запись системной диагностики
T17	8	2	Перейти в режим ожидания (Idle)
T18	9	2	Перейти в режим ожидания (Idle)
T19	3	9	Начать запись системной диагностики

8.6.4.5 Управление iпар-сервером

В таблице 19 перечислены средства управления iпар-сервером для обеспечения аутентичности, соответствия и целостности данных iпараметров. Ответственность за предоставление мер безопасности для механизмов сохранения и восстановления лежит на F-модуле, F-ведомом устройстве или F-устройстве. iпар-сервер всего лишь хранит iпараметры в виде потока октетов и может так служить стандартным сервером параметров для устройств, не связанных с безопасностью.

Таблица 19 — Средства управления iпар-сервером

Элемент / стадия	Разделы	Описание
F_S/D_Address	8.1.2 7.3.7 9.1	Использование F_Source/ Destination_Address или короткого F_S/D_Address является обязательным входным условием для обеспечения аутентичности сохраняемых и восстанавливаемых iпараметров. Включение F_S/D_Address в вычисление iPar_CRC или в блок iпараметров не является обязательным. Корректная доставка F_iPar_CRC уже гарантируется посредством F_S/D_Address для того, чтобы ошибочно доставленный блок iпараметров мог быть обнаружен сравнением его iPar_CRC с F_iPar_CRC. В случае, когда посредством кодового переключателя задан F_S/D_Address, заменяющее устройство должно быть отрегулировано для соответствия начальному F_S/D_Address перед запуском. В случае, если F_S/D_Address назначен посредством CPD-инструмента, ответственность за предоставление средств для настройки F_S/D_Address перед перезапуском лежит на производителе устройства
Запуск	8.1.7 8.6.3 9.1	После запуска F-модуль, F-ведомое устройство или F-устройство получает F-параметры для установления коммуникаций CPF 3 (циклического обмена данными). Заданное значение F_iPar_CRC равно «0», что гарантирует нахождение устройства в безопасном состоянии и отправку им значений FV (значений отказоустойчивости). Зеленый светодиод мигает с частотой 2 Гц (два цикла в секунду)
Ввод в эксплуатацию	–	На данном этапе устройство может быть сконфигурировано и параметризовано при помощи CPD-инструмента, подключенного напрямую, или, используя услуги не периодических коммуникаций, такие как, MS2. Ответственность за обеспечение безопасной параметризации на всех этих стандартных коммуникационных каналах и определение безопасности устройства во время нахождения в испытательном режиме FSCP лежит на производителе устройства и соответствующего CPD-инструмента
iPar_CRC / F_iPar_CRC	8.2 8.3.3.2	Использование iPar_CRC и его аналога F_iPar_CRC, передаваемого в разных направлениях, является входным условием для обеспечения целостности данных сохраненных и восстановленных iпараметров. В случае, когда вычисленная iPar_CRC сигнатура в CPD-инструменте выдает «0», должно быть установлено значение «1». Это также применимо для вычисления сигнатуры iPar_CRC в F-модуле, F-ведомом устройстве или F-устройстве перед сравнением со значением F_iPar_CRC, возникающим из параметризации при запуске
Ручное распространение	8.1.7	iPar_CRC вычисляется в режиме безопасности в CPD-инструменте и должна отображаться в шестнадцатеричном формате. Пользователь затем может вручную передать это значение в поле записи «F_iPar_CRC» программного инструмента. Эта передача может быть выполнена автоматически, если доказано, что она достаточно безопасна
ИТО функции	8.2	Соответствие определенного набора iпараметров (блока) для заменяющего устройства дефектному может быть проверено, например, посредством функций

Окончание таблицы 19

Элемент / стадия	Разделы	Описание
ИТО функции	8.2	идентификации и технического обслуживания (ИТО), таких как «order number» (номер заказа), «HW release» (версия аппаратуры) и «SW release» (версия программного обеспечения). Ответственность за выбор правильной информации, необходимой для обеспечения соответствия, лежит на производителе устройства
Верификация	–	Как правило, фаза назначения iпараметров завершается определенным испытанием и шагом верификации, за которым следует действие «отсоединения» и «повторное соединения», приводящее к запуску и передаче правильной F_iPar_CRC
iПар-сервер	–	F-Ммодуль, F-ведомое устройство или F-устройство должны запускать запрос iпар-сервера только после успешной параметризации запуска (F-параметры)
Светодиодная индикация	9.1	До тех пор пока F-модуль, F-ведомое устройство или F-устройство не добьются сохранения своих iпараметров или пока само устройство находится в режиме испытания FSCP, то оно должно указывать на нахождение в этом состоянии посредством светодиодных индикаторов, описанных в 9.1. Чистота мигания в данном случае должна составлять 2 Гц

8.6.4.6 Размер iпараметров в GSD

F-модуль, F-ведомое устройство или F-устройство может указывать максимальный размер своих iпараметров посредством поля ключевого слова «Max_iParameter_Size» в своем GSD файле («Max_iParameterSize» в GSDML). Подробности см. в [43] и [47].

9 Системные требования

9.1 Индикаторы и коммутаторы

В случае сбоя, который можно связать с определенным F-устройством, F-хост устанавливает бит управления 1 «запрошено подтверждение оператора» в байт управления (=1). Этот бит может использоваться для оповещения пользователя о трех начальных действиях:

- проверка оборудования и, если необходимо, его восстановление или замена;
- верификация функции безопасности;
- подтверждение оператора (OA_C).

В случае малогабаритных F-устройств настоятельно рекомендуется использовать индикаторный светодиод (например, имеющийся двухцветных светодиод шины), мигающий с частотой 0,5 Гц в зеленом режиме («коммуникации шины в порядке, но запрошен OA_C»). В случае модульных устройств на каждом модуле должен использоваться, как правило, доступный, светодиод «безопасной операции», мигающий с частотой 0,5 Гц в зеленом режиме («коммуникации шины в порядке, но запрошен OA_C»). Такая реализация не является *обязательной* для F-устройств.

Пока устройство находится в испытательном режиме FSCP или пока F-модуль, F-ведомое устройство или F-устройство не добилось сохранения своих iпараметров, светодиодный индикатор или светодиод «безопасной операции» должен указывать на нахождение в данном состоянии, мигая с частотой 2 Гц в зеленом режиме.

В 7.3.7 и 8.1.2 предоставлена информация о том, как вводить F_S/D_Address F-устройств посредством коммутаторов.

9.2 Руководство по установке

Применяются руководство по установке из МЭК 61918 и поправки, ориентированные на CPF 3 из МЭК 61784-5-3. Дополнительная информация может быть найдена в [44].

9.3 Время реакции функции безопасности

9.3.1 Модель

Функция безопасности может состоять из нескольких датчиков, таких как, световая завеса и кнопки аварийного отключения, логической программы безопасности в F-Хосте и исполнительного устройства, такого как, двигатель (рисунок 72). Для каждого датчика существует свой собственный путь прохождения его сигнала и потому и свое определенное типовое время реакции.

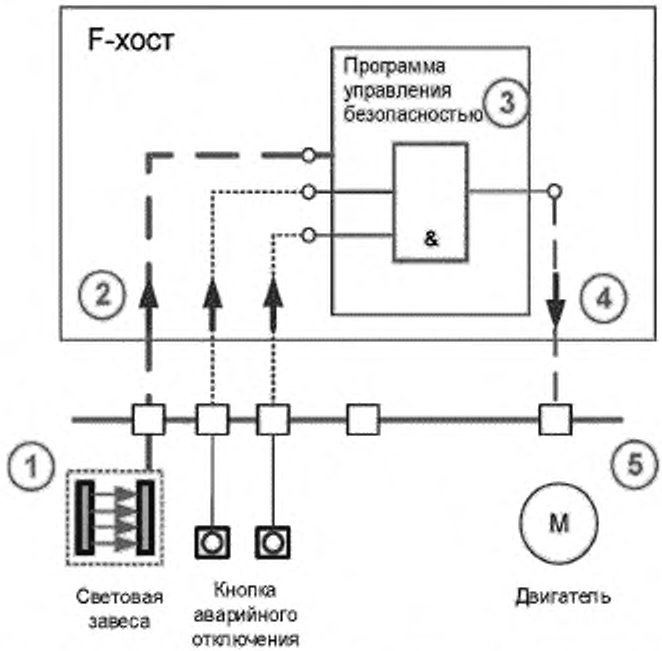


Рисунок 72 — Пример функции безопасности и критический путь ее времени реакции

Это типовое время реакции состоит из нескольких отдельных периодов времени, включая время, затрачиваемое на передачу данных по шине (скорость передачи), как показано в упрощенной модели типового времени реакции на рисунке 73. Пример служит для демонстрации принципа, который может быть заимствован для использования во внутренней модели времени реакции сложного устройства.

	Задержка ввода	Задержка передачи	Задержка обработки*)	Задержка передачи	Задержка вывода
Пример	3, 4, 5, 6 мс	1 2 мс	5, 6, 7, ... 15 мс	1, 2 мс	3, 4, 5. 6 мс

*) мин. время обработки 5 мс, скорость сканирования, управляемая по времени, для это примера = 10 мс

Рисунок 73 — Упрощенная модель типового времени реакции

В примере представлен путь прохождения сигнала, состоящий из устройства датчика, передачи данных по шине F-хосту, обработка данных F-хостом, другая передача данных по шине устройству вывода и устройство вывода (оконечный элемент).

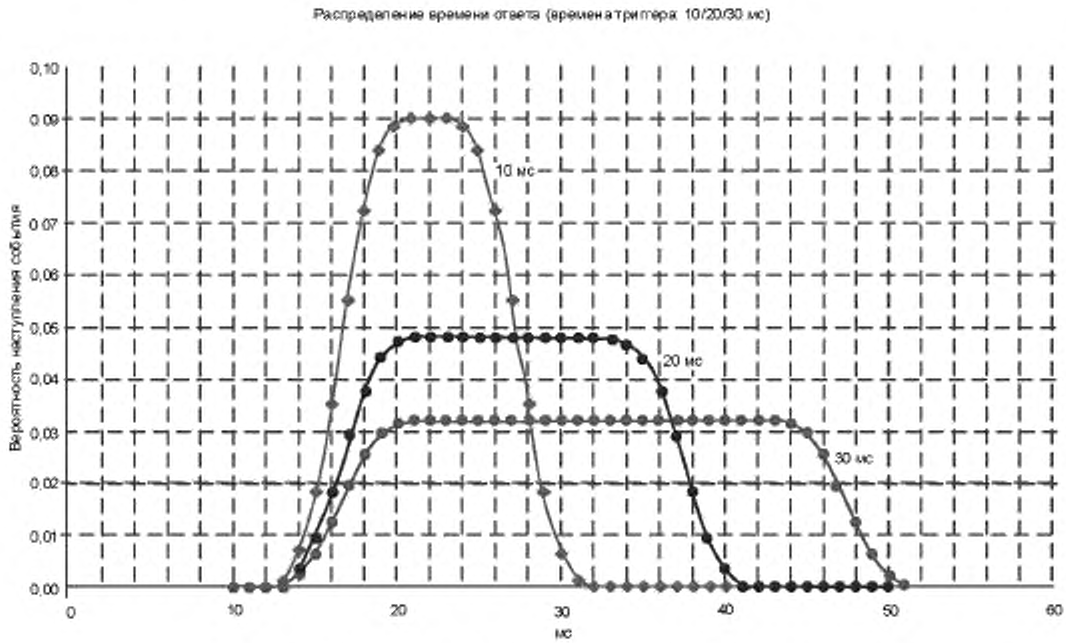
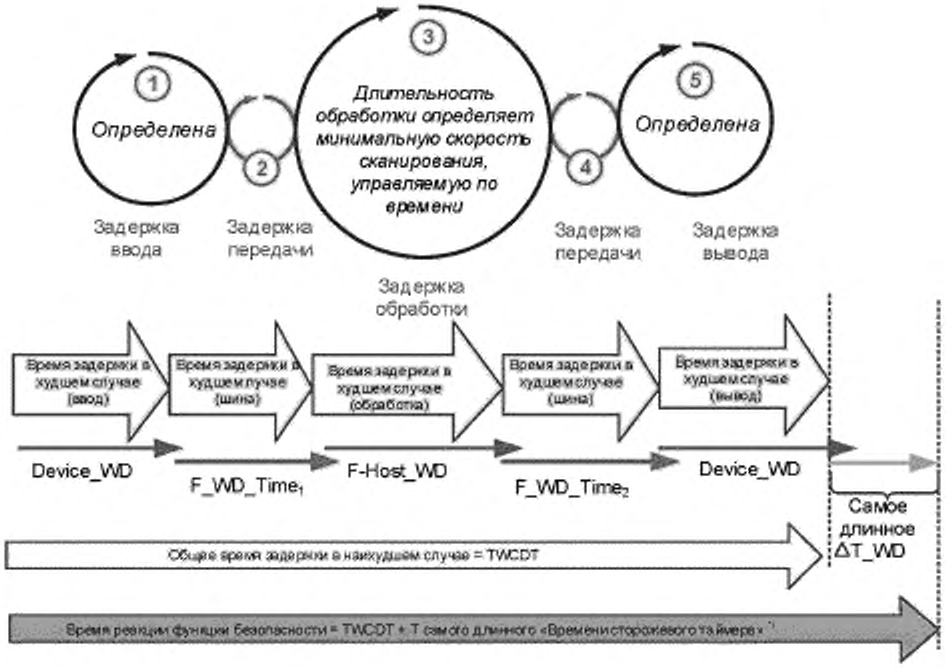


Рисунок 74 — Распределения частот типового времени реакции модели

Любые из этих элементов обладают минимальными (на обработку) и максимальными (обработка + ожидание) временами задержки. Фактическая задержка может быть любым временем (или интервалом) между этими значениями. В данной модели предполагается, что F-хост это комбинированный контроллер для стандартных программ и программ безопасности. Программа безопасности выполняется на отдельном программном уровне, управляемом по времени, и ей может потребоваться время обработки, равное 5 мс. В данном случае триггер срабатывает каждые 10 мс. Это приводит к задержке обработки в минимум 5 мс и максимум 15 мс. В общем, минимальная задержка для этой функции безопасности равна 13 мс. На рисунке 74 показаны распределения частот типового времени реакции модели для триггера, срабатывающего каждые 10 мс, 20 мс и 30 мс.

9.3.2 Вычисление и оптимизация

Модель для определения типового времени реакции в 9.3.1 используется для определения времени реакции функции безопасности. Каждый из циклов в модели может варьироваться от времени задержки в лучшем случае до времени задержки в худшем случае ($WCDT_i$). Для обеспечения безопасности с каждым циклом связан свой сторожевой таймер ($WDTime_i$), который предпринимает необходимые действия для активации безопасного состояния всякий раз, когда в определенном объекте происходит отказ или ошибка. На рисунке 75 показано содержание времен задержки и времен сторожевого таймера в наихудшем случае.



*) Не обязательно для устройства вывода

Рисунок 75 — Контекст для времени задержки и времени сторожевого таймера

Для того чтобы вычислить время реакции функции безопасности необходимо принять, что в рассматриваемой сущности пути сигнала произошла одна ошибка или отказ, который привнес максимальную разность времени между временем задержки в худшем случае и временем сторожевого таймера (WDTime). Соответствующее уравнение (1) показано ниже:

$$SFRT = \sum_{i=1}^{n} WCDT + \max_{i=1,2,..n} (WDTime_i - WCDT_i), \quad (1)$$

где:

SFRT — время реакции функции безопасности;

TD — задержка передачи;

$WCDT_i$ — время задержки в худшем случае для объекта i;

$WDTime_i$ — WDTime охватывает период времени, начиная с принятия PDU безопасности с новым порядковым номером и заканчивая реакцией на истечение времени F_WD_Time. Ниже приведены определенные выражения для объектов i:
- Ввод: $OFDT_{Input}$;
- TD1: $F\_WD\_Time1 + WCDT_{TD1} + Tcy_{F\text{-}Host}$;
- F-хост: $OFDT_{F\text{-}Host}$;
- TD2: $F\_WD\_Time2 + WCDT_{TD2} + DAT_{Output}$;
- Вывод: $OFDT_{Output}$;

OFDT — время задержки объекта в случае одного сбоя, т. е. время задержки в худшем случае при сбое в объекте;

$Tcy_{F\text{-}Host}$ — вемя цикла F-хоста.

В случае необходимости производители системы должны предоставить индивидуальный адаптированный метод вычисления.

9.3.3 Корректировка времени сторожевого таймера для FSCP 3/1

F-Пparameter F_WD_Time определяет время сторожевого таймера для коммуникационной связи 1:1 профиля FSCP 3/1 (8.1.3). На рисунке 76 показано, что минимальное время сторожевого таймера состоит из четырех временных секций (DAT — Шина — HAT — Шина).

Каждый раз, когда F-драйвер (6.2) в малогабаритном F-устройстве или в F-модуле модульного устройства распознает PDU безопасности (кадр FSCP 3/1), содержащий новый порядковый номер (*m*), то он перезапускает сторожевой таймер. Затем драйвер обрабатывает протокол FSCP 3/1, принимая *доступные на данный момент значения процесса*, и готовит новый PDU безопасности. Затраченное время для данной операции называется «DAT = Время подтверждения устройства».

Примечание — В случае модульного F-устройства DAT включает в себя время на внутренние передачи через шину объединительной платы.

Передача нового PDU безопасности F-хосту выполняется в течение следующей временной секции (Шины). Как только F-драйвер в F-хосте получил новый PDU безопасности, он перезапускает свой сторожевой таймер и обрабатывает протокол FSCP 3/1. Он генерирует PDU безопасности со следующим порядковым номером (*m*+1). Затраченное время на эту операцию называется «HAT = Время подтверждения хоста». Передача PDU безопасности F-устройству выполняется в течение последней временной секции (Шины).

Время сторожевого таймера, которое должно быть назначено F-параметру превышает *минимальное время сторожевого таймера*, чтобы обеспечить обнаружение аварийного события.

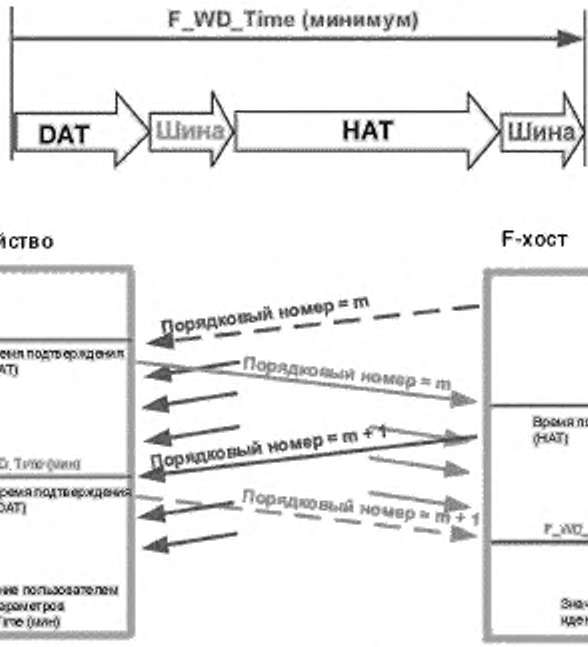


Рисунок 76 — Временные секции, формирующие F_WD_Time профиля FSCP 3/1

Согласно 8.1.3 значение, которое будет назначено F_WD_Time, в примере на рисунке 73 (временной триггер = 10 мс) будет равно два периода времени передачи по шине (2 × 2 мс) плюс DAT устройства (6 мс) и F-хоста (15 мс), в результате F_WD_Time = 4 ms + 6 ms + 15 ms = 25 ms. Корректировка в сторону уменьшения времени сторожевого таймера не скажется на безопасности системы. Она может привести к ложным срабатываниям и тем самым повлиять на готовность.

При резервировании необходимого запаса времени в рамках корректировок сторожевого таймера также должен быть учтен тот факт, что устройство может продлевать передачу данных по шине в случае поступления диагностического сообщения. Дополнительные устройства-супервизоры (или ведущее

устройство класса 2 в рамках СР 3/1) обладают минимумом влияния на время реакции, как это показано на рисунке А.3. Другие влияния описаны в 9.3.5.

Уравнение (1) в 9.3.2 действительно, если временные рамки DAT, HAT и передач по шине могут быть гарантированы. Основной F-параметр F_WD_Time должен получить значение, которое немногим превышает сумму DAT, HAT и помноженного на два времени передачи по шине. Настоятельно рекомендуется, чтобы разница между назначенным значением параметра и суммой не превышала 30 %. Производители системы могут отрегулировать это правило для соответствия их индивидуальным потребностям.

9.3.4 Поддержка программного инструмента

Программные инструменты должны предоставлять средства для того, чтобы сразу предварительно оценить время реакции функции безопасности, на стадии планирования для поддержки расчета расстояний при конструкторском проектировании и во время стадии ввода в эксплуатацию для поддержки назначения параметров сторожевого таймера.

9.3.5 Повторения (повторение сообщений)

В случае высокого уровня электромагнитных помех или устройств, которые не соответствуют стандартам полевых шин, так как они создают в линии передачи данных недопустимые электрические помехи, системы полевых шин, как правило, применяют механизмы повторения для повышения готовности. Хорошей инженерной практикой на стадии ввода в эксплуатацию является проверка каждого соединения со всеми устройствами (стандартными и безопасности) на число повторных попыток и, если необходимо, применить надлежащие меры, такие как, корректное применение руководства по установке или использование проверенных на соответствие устройств (раздел 10). Это не только поможет повысить готовность, но также обеспечит короткое время реакции без ложных срабатываний (рисунок 77).

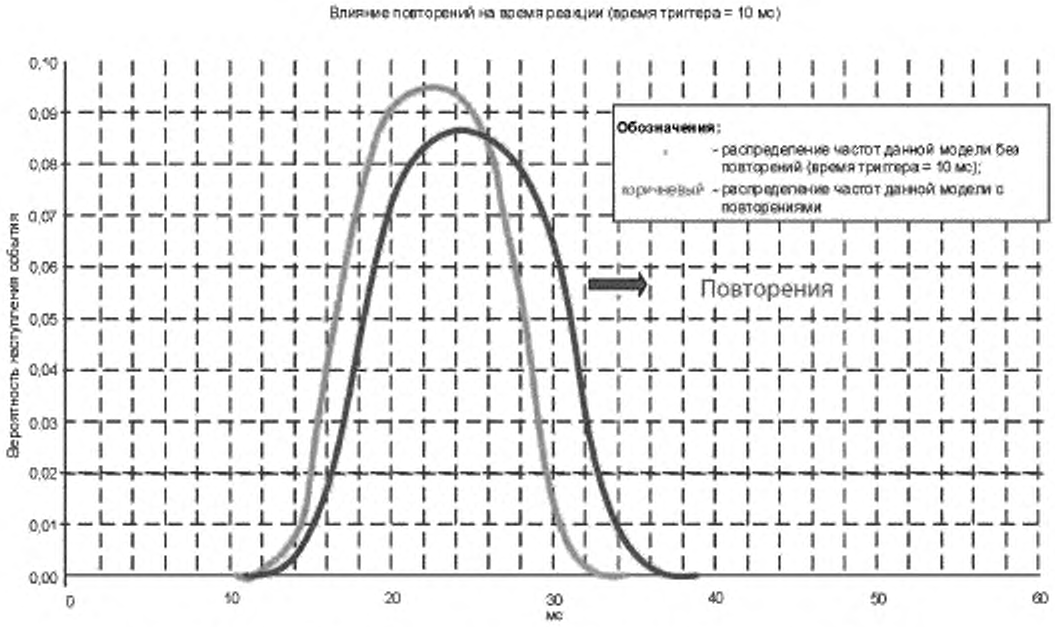


Рисунок 77 — Кривая распределения времени реакции с повторениями сообщений

На рисунке 78 показаны механизмы повторений с СР 3/1, в то время как на рисунке 79 показаны механизмы повторений для СР 3/RTE. Знание поведения черного канала при повторении также может быть необходимо для оценок безопасности.

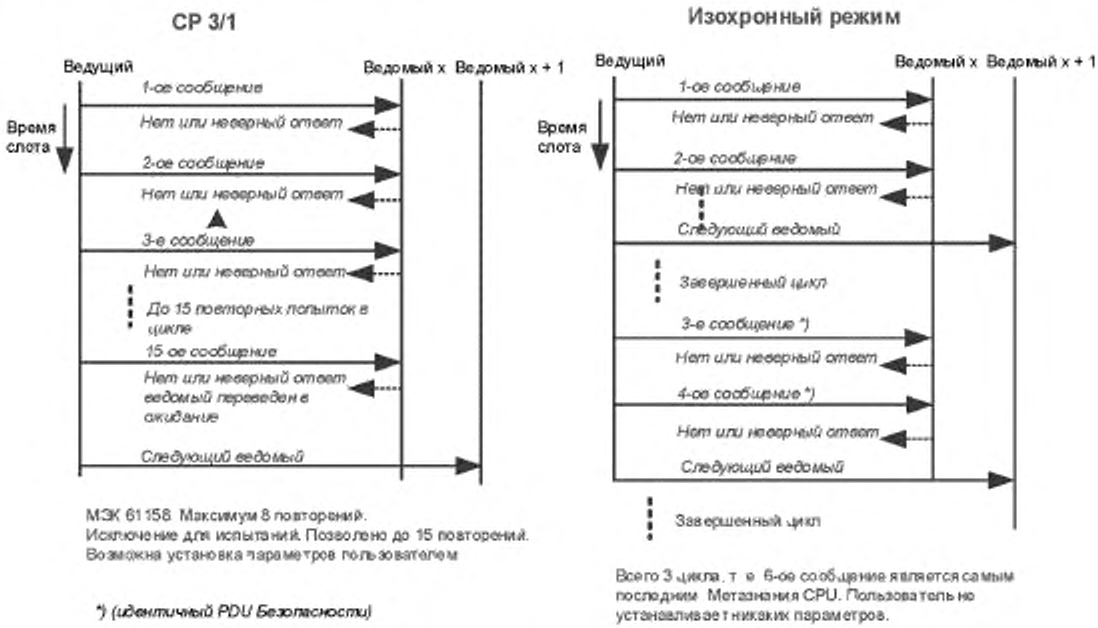
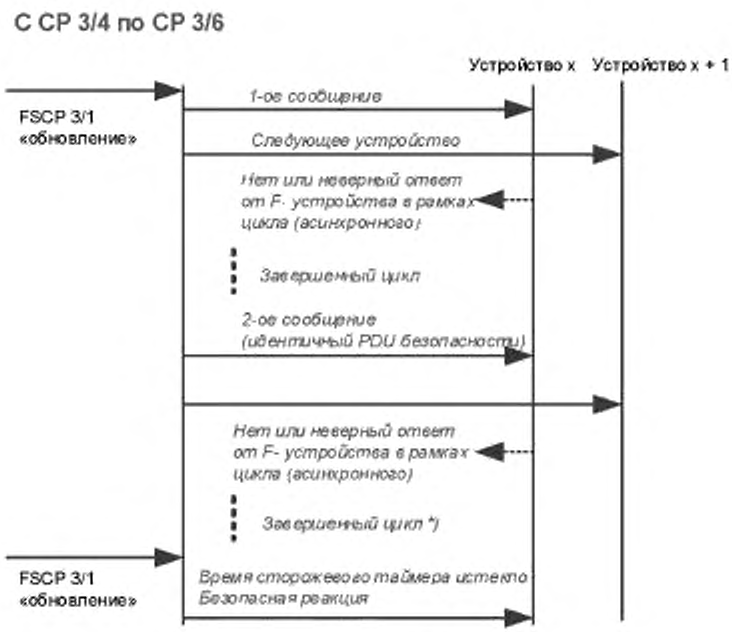


Рисунок 78 — Повторные попытки с CP 3/1



*) Максимальное число повторений см. в CP 3/4

Рисунок 79 — Повторные попытки с CP 3/RTE

9.4 Длительность запросов на обслуживание

«Запрос на безопасную реакцию», как правило, исходят, например, от световой завесы, от защитных ковров безопасности, средств управления от двух рук, рычагов аварийной остановки и тому подобного. Длительность этих сигналов:

- должна быть равна времени безопасности процесса или больше, чем таймаут FSCP 3/1 (F_WD_Time);
- может быть меньше, чем время безопасности процесса или таймаут FSCP 3/1 (F_WD_Time) соответственно. В этом случае возможна реакция безопасности. Например, муха, пролетающая через световую завесу.

В рамках F_WD_Time могут быть приняты PDU безопасности с одинаковым порядковым номером и разными значениями процесса, что происходит из-за переставленных сообщений в черном канале.

9.5 Ограничения для вычисления системных характеристик

9.5.1 Вероятностные соображения

Механизм проверки целостности данных V2-режима профиля FSCP 3/1 совершенно независим от механизмов системы коммуникаций, лежащей в основе и называемой, в таком случае, «черным каналом». Таким образом, он может также быть также использован для каналов коммуникаций на системной плате.

В соответствии с МЭК 62280-1 и МЭК 62280-2 должна быть доказана «годность» применяемых CRC полиномов. Это требует вычислений вероятности возникновения остаточной ошибки в виде функции вероятности битовой ошибки для заданного полинома, в данном случае для 24-битовой версии (*15D6DCB*h), также как и для 32-битовой версии (*1F4ACFB13*h).

На рисунке 80 показаны диаграммы вероятностей возникновения остаточной ошибки для 24-битового полинома. Рассчитанные диаграммы подходят для длины данных, включающей сигнатуру CRC.

Полином будет оценен как «годный», если нет значительного «горба» на кривой с возрастающей вероятностью битовой ошибки, т. е. если она возрастает монотонно.

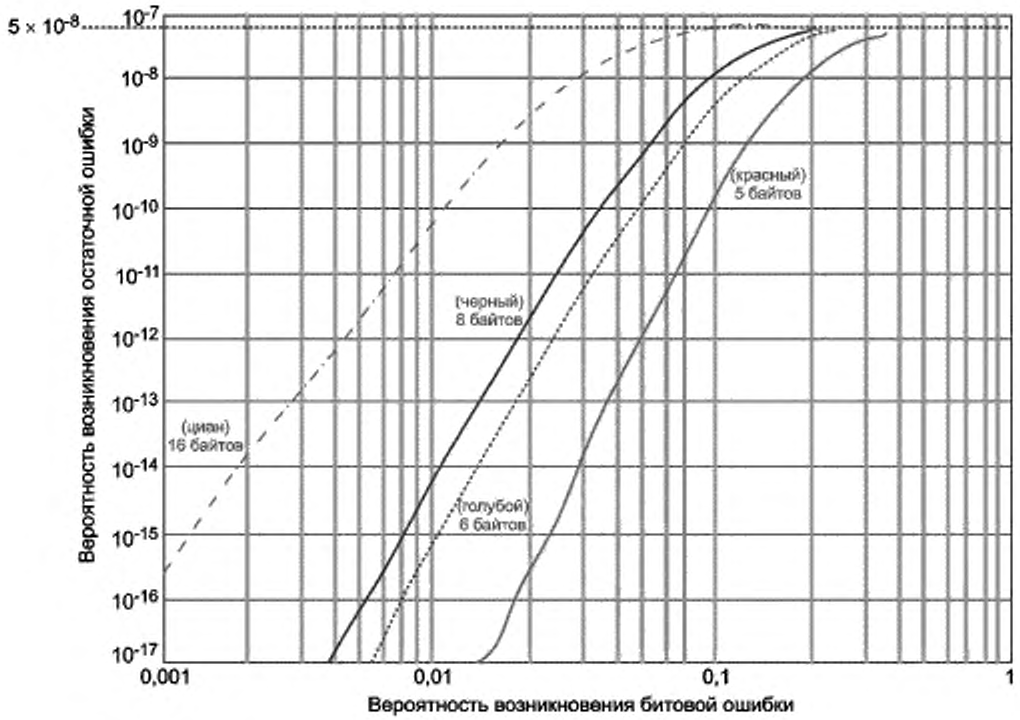


Рисунок 80 — Вероятности возникновения остаточной ошибки для 24-битового полинома

На рисунках 81 и 82 показаны схемы для 32-битового полинома.

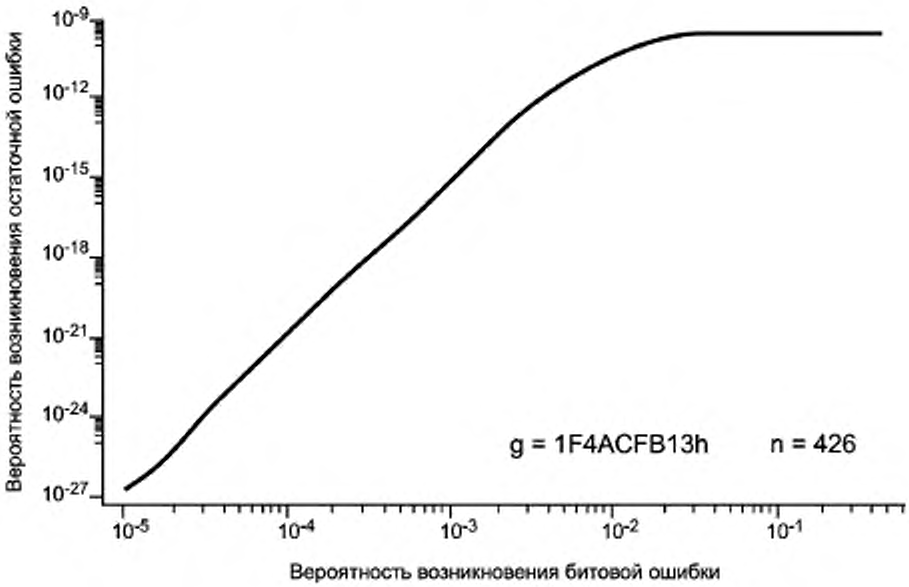


Рисунок 81 — Годность 32-битового полинома для 52 октетов

Термины, использованные на рисунках 81 и 82, описаны ниже:
g = генерирующий полином 1*F4ACFB13*h;
n = битовая длина данных, включая сигнатуру CRC.

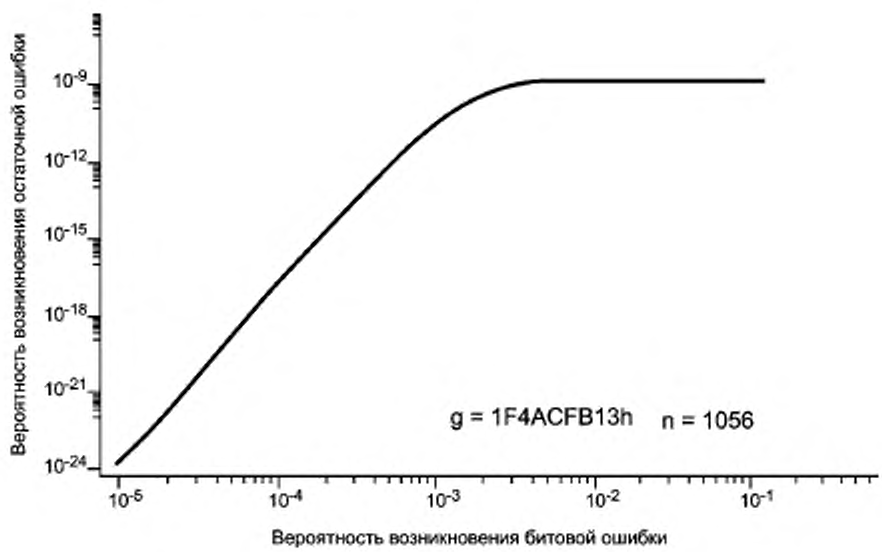


Рисунок 82 — Годность 32-битового полинома для 132 октетов

Результат рассмотрения влияния любых возмущений представлен на рисунке 83. Комбинация причин отказов шины дает (фиктивную) частоту возникновения искаженных сообщений в системе передачи данных. Стандартные механизмы обнаружения ошибок CP 3/RTE (первый Фильтр) распознают каждый сбой вплоть до определенного уровня, тем самым, только специальные комбинации битов достигают механизм уровня безопасности. Для числа необнаруженных искаженных сообщений не должно приниматься значение худшего случая равное 2^{-n} (n = 24 или 32), так как общая частота искаженных PDU безопасности на шине подвергается постоянному контролю.

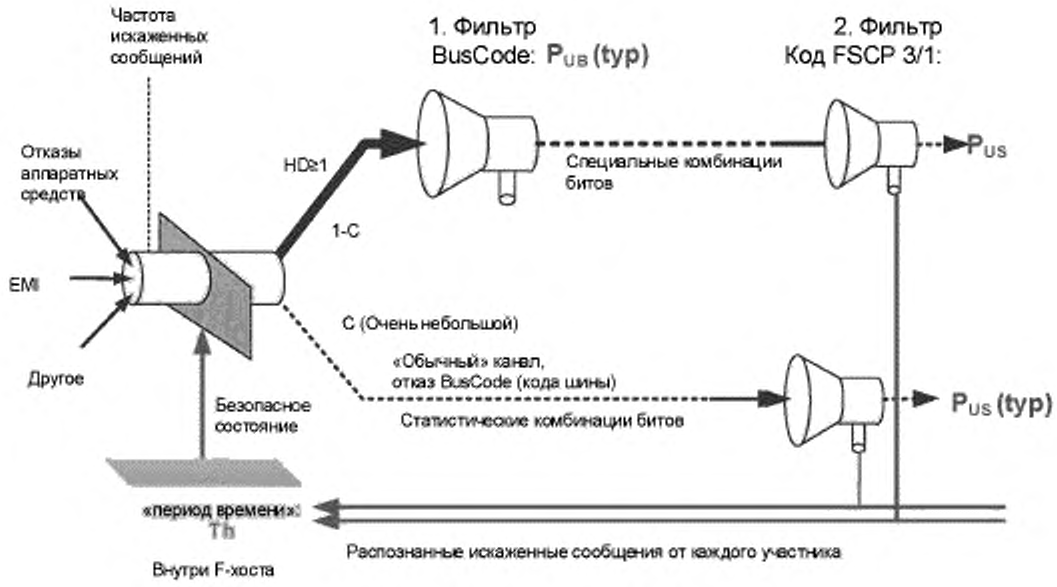


Рисунок 83 — Контроль искаженных сообщений

Термины, использованные на рисунке 83, описаны ниже:
fw — частота отправки искаженных сообщений;
ЭМП — электромагнитные помехи;
HD — расстояние Хемминга;
c — частота возникновения;
T — период измерения в часах (см. 7.2.6).

Если механизмы безопасности в стандартных IO уровнях CP 3/1 и CP 3/RTE отказывают (очень низкая вероятность), то искаженные сообщения со статистическими комбинациями битов достигают механизм уровня безопасности.

Протокол FSCP 3/1 позволяет осуществлять простой контроль каждого искаженного PDU безопасности в F-хосте и, посредством байта статуса, в PDU безопасности подтверждения F-устройства.

9.5.2 Ограничения, связанные с безопасностью

Ниже перечислены граничные условия и ограничения для оценок безопасности и вычислений частоты возникновения остаточных ошибок.

Общие.

- Все устройства обеспечивают SELV/PELV для электрической безопасности и отчет о тестировании на соответствие CPF 3.

- Устройства безопасности спроектированы для обычных промышленных сред в соответствии с МЭК 61000-6-2 или МЭК 61131-2 и обеспечивают повышенную помехоустойчивость в соответствии с МЭК 61326-3-1 и МЭК 61326-3-2.

Режим V1.

- Принятое число сообщений, связанных с безопасностью, поступающих в секунду и приходящихся на коммуникационную связь 1:1 профиля FSCP 3/1:

CP 3/1: 100;
CP 3/2: 10.

- Число повторений, приходящихся на тип канала (см. 9.3.5):

CP 3/1: 15 (МЭК 61158-6-3: максимум 8);
CP 3/2: 15 (МЭК 61158-6-3: максимум 8);
Шина на системной плате: 8 (в хостах или модульных полевых устройствах).

- CRC полиномы черного канала:

Черный канал не должен применять CRC полиномы уровня безопасности 14EABh и 1F4ACFB13h;
Полиномы черного канала не должны делиться на C599h.

- Элементы сети активной буферизации:

CP 3/1: 2 сообщения максимум вместе с каналами и/или повторителем.

- Разбиение PDU безопасности в октетах:

Не разрешено.

Режим V2.

- Принятое число сообщений, связанных с безопасностью, поступающих в секунду и приходящихся на коммуникационную связь 1:1 профиля FSCP 3/1 < 10 000.
- Число повторных попыток приходящихся на тип канала (см. 9.3.5):

Никаких ограничений.

- Число приемников сообщений, связанных с безопасностью, приходящихся на функцию безопасности:

Никаких ограничений.

- CRC полиномы черного канала:

Никаких ограничений.

- Элементы сети активной буферизации:

Никаких ограничений; разрешен любой коммутатор (см. 7.3.8 и 5.4.2).

- Области безопасности:

Не разрешено использовать однопортовые маршрутизаторы на границах области безопасности (см. 7.3.9).

- Разбиение PDU безопасности в октетах:

Никаких ограничений.

9.5.3 Ограничения, не связанные с безопасностью (готовность)

– Циклический обмен данными между хостами и полевыми устройствами в рамках заданного периода времени (признак жизни).

– Гарантированная доставка всех PDU безопасности на уровне безопасности (целостность данных).

Общие:

- CP 3/1: Никаких ответвлений.
- CP 3/RTE: Один F-хост на подмодуль.
- Коммутаторы Ethernet должны подходить для стандартных промышленных сред, как это определено, например, в МЭК 61131-2.

Стандартные устройства и устройства безопасности могут использовать один источник питания в 24В.

9.6 Техническое обслуживание

9.6.1 Ввод в эксплуатацию/замена F-модуля

F-модули могут быть заменены в процессе работы системы. Повторный запуск соответствующего контура управления безопасностью разрешен только в том случае, если не наблюдается никаких состояний опасных процессов и только после подтверждения оператора (OA_C).

9.6.2 Функции идентификации и технического обслуживания

Функции идентификации и технического обслуживания (ИТО) задают набор параметров в F-устройстве для идентификации типов устройств и индивидуальных устройств посредством CPF 3 сети и для поддержания технического обслуживания [46]. Эти функции могут применяться для поддержки iпараметризации, как это определено в 8.2. F-устройства/модули должны реализовывать обязательный

набор ИТО функций. Дополнительно, F-устройства/модули должны заполнять поле IM4 (сигнатура) значением сигнатуры, указывающей на нахождение в состоянии конфигурирования и параметризации безопасности F-устройства/модуля, если эта сигнатура не была включена иначе в общую сигнатуру всего проекта F-хоста.

9.7 Руководство по безопасности

В соответствии с МЭК 61508-2, поставщики F-хоста и F-устройства должны предоставлять руководство по безопасности. В случае FSCP 3/1 в него должны быть включены инструкции, информация и параметры из таблицы 20.

Таблица 20 — Информация, которую необходимо включить в руководство по безопасности

Элемент	Инструкция и/или параметр	Примечание
Работа с безопасностью	Инструкции по конфигурированию, параметризации, вводу в эксплуатацию, испытанию и блокированию этого устройства безопасности в соответствии с МЭК 61508	См. 9.1 (светодиод) и 7.3.7 (F-адрес)
Источник питания	Должны быть определены требования для электрической безопасности (PELV), колебаний, шума, прерываний и т .д.	См. [44] ограничения, зависящие от страны, такие как ограничения на ток
Электрическая безопасность	Все сетевые устройства, используемые в совокупности с этим устройством должны соответствовать требованиями стандарта МЭК 61010-1 или МЭК 61131-2 (например, PELV)	См. [44]
Электромагнитная устойчивость, ЭМП	Применяемые испытания и их результаты (заявление производителя или последний отчет из компетентной тестовой лаборатории)	В соответствии с МЭК 62061, МЭК 61326-3-1 или МЭК 61326-3-2 все, что применимо, или же стандарт на устройство, такой как МЭК 61496 [6]; [44]
Изоляция	Применяемое тестовое напряжение и его длительность на коммуникационном порту шины	См [44]
Компоненты сети	Ограничения на коммутаторы, маршрутизаторы и другие компоненты сети	См. 7.3.8, 7.3.9, 9.5.2, и 9.5.3
Установка	В соответствии с МЭК 61918 и МЭК 61784-5-3	См. также [64]
Ввод в эксплуатацию	Использование контрольного листа из МЭК 61784-5-3, например, для грамотной адресации, проверке повторений, качеству сигнала и т. п.	См. также [65]
iпараметр	Верификация функций безопасности должна включать проверку того, все ли F_iPar_CRC > «0»	См. 8.6.4.5
Техническое обслуживание	Условия и процедуры для замены частей; идентификация	См. 9.6
Жизненный цикл	Значение(ния) интервала контрольных испытаний	В соответствии с МЭК 61508
Время реакции	Значения параметров DAT, WCDT, WDTime	См. 9.3.2 и 9.3.3
Безопасность оборудования (электрическая)	Значения параметров: заявленного УПБ, PFH (вероятность отказа в час)	В соответствии с МЭК 62061
Безопасность оборудования (не электрическая)	Значения параметров для PL (Уровня эффективности защиты), MTTFd (средняя наработка на отказ)	В соответствии с ИСО 13849-1
Безопасность для автоматизации процесса	Значения параметров: заявленного УПБ, PFD (вероятность отказа по запросу), возможности соединения для достижения более высокого УПБ	В соответствии с МЭК 61511 и [30]
Защита	Инструкции по установлению адекватного уровня защиты, зон защиты и защитных ворот	См. 9.8, [44], [53]
Отчеты по оценке	Отчеты о тестировании на соответствие от организации-поставщика полевой шины и отчеты об оценке безопасности от компетентных органов оценки	См. [45] и раздел 10

9.8 Беспроводные каналы передачи данных

9.8.1 Метод черного канала

Беспроводные каналы передачи данных классифицируются как часть черного канала и, тем самым, не нуждаются в оценке безопасности, так как FSCP 3/1 одобрен для вероятности битовых ошибок равной 10^{-2}.

9.8.2 Готовность

Одной из основных трудностей, связанных с беспроводной передачей, является обеспечение достаточной готовности. Пользователь должен установить надлежащие меры для обеспечения достаточной готовности: возможен ли после-базовый тариф в роуминге или возможны ли временные прекращения связи, вызванные отражениями или помехами, или другими причинами ложных срабатываний. Ложные срабатывания могут повлечь за собой отключение или удаление сетевого оборудования (предсказуемое неправильное использование).

9.8.3 Средства защиты

Перед вводом в эксплуатацию приложения безопасности с FSCP 3/1 и беспроводными компонентами должна быть выполнена оценка на наличие опасных угроз таких, как подслушивание или манипуляции данными, как это отмечено в [44]. В случае угрозы не требуется никаких средств защиты.

Существуют две возможные идентифицированные угрозы:

- предумышленные изменения параметров F-устройства и программ безопасности;
- атаки на циклические коммуникации, например, симуляция коммуникации безопасности.

Для того, чтобы защитить беспроводную сеть от подобных случаев следует рассмотреть меры, приведенные в таблице 21, в соответствии с ИИЭР 802.11i [26] для промышленных WLAN, как это отмечено в МЭК 61784-2 для устройств класса А. На рисунке 84 приведен обзор средств обеспечения защиты.

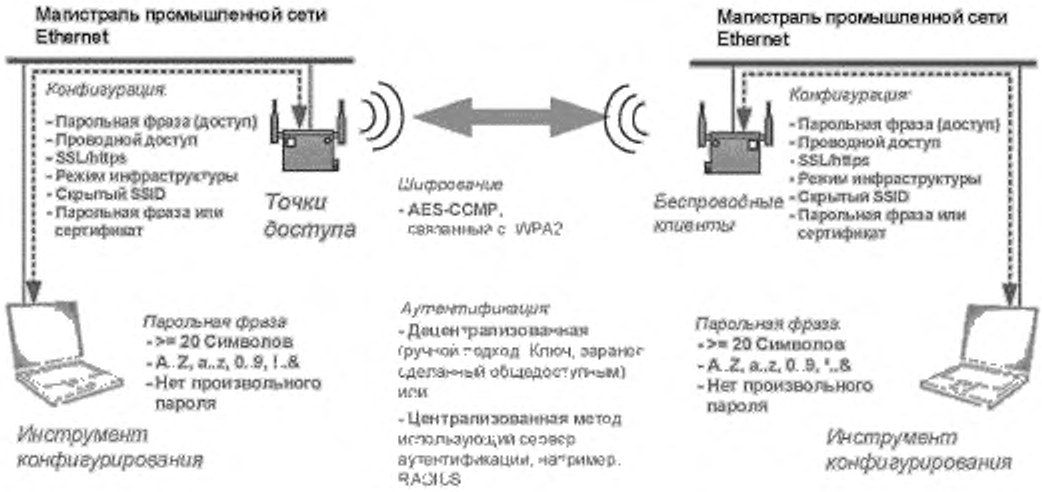


Рисунок 84 — Защита для WLAN сетей

Ниже описаны термины, использованные на рисунке 84:

AES-CCMP — продвинутый стандарт шифрования — протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика;

RADIUS — услуга удаленной аутентификации звонящего;

SSID — идентификатор набора услуг;

SSL — уровень защищенных сокетов;

WPA2 — Wi-Fi защищенный доступ 2 (соответствует ИИЭР 802.11i [26]);

Точка доступа — координационная станция для набора беспроводных услуг в соответствии с ИИЭР 802.11;

Беспроводной клиент — станция, входящая в набор беспроводных сервисов в соответствии с ИИЭР 802.11.

Таблица 21 — Меры обеспечения защиты для WLAN (ИИЭР 802.11i)

№	Элемент	Средство
1	Администрирование беспроводной точки доступа и беспроводного клиента	Разрешен только проводной доступ посредством SSL или https. Пароль/парольная фраза администрации не должен быть паролем по умолчанию
2	Качество парольной фразы для администрации	Длина парольной фразы должна составлять 20 символов. Символы должны представлять собой смесь буквенных, цифровых и специальных знаков
3	Эксплуатационные режимы	Разрешен только *Режим Инфраструктуры*. *Режим прямого подключения* не должен быть задействован
4	Подходы к аутентификации	Разрешен либо *Децентрализованный подход* (ручной ввод в действие ключей аутентификации) или *Централизованный подход* (специализированный сервер аутентификации, например, RADIUS). В случае центральной услуги аутентификации в совокупности с роумингом следует следить за тем, чтобы времена блокировки каналов были меньше, чем их времена циклов
5	Процедуры аутентификации	Для аутентификации разрешен либо *Общедоступный ключ* (Предварительно выданный секрет), либо *Сертификаты*
6	Качество парольной фразы для шифрования	Длина парольной фразы должна быть 20 символов (см. [26] H.4 Предлагаемое отображение парольной фразы на ПВК). Символы должны представлять собой смесь буквенных, цифровых и специальных знаков
7	Шифрование циклического обмена данными (PDU безопасности)	*AES-CCMP* (в соответствии с WPA2) [26] должен быть внедрен в качестве алгоритма шифрования
8	Скрытый SSID	Точка беспроводного доступа должна быть сконфигурирована таким образом, чтобы SSID был скрыт. Внедренный SSID не должен быть SSID по умолчанию
Примечания 1 Длина парольной фразы должна быть доступной, так как пароли или парольные фразы должны вводится только однажды во время сеанса ввода в эксплуатацию. 2 Шифрование циклического обмена данными защищает от манипуляции данных.		

Для того чтобы защитить беспроводную сеть следует рассмотреть средства, представленные в таблице 22 в соответствии с ИИЭР 802.15.1 [27], для Bluetooth, как это отмечено в МЭК 61784-2 для устройств класса А. На рисунке 85 представлен обзор мер защиты.

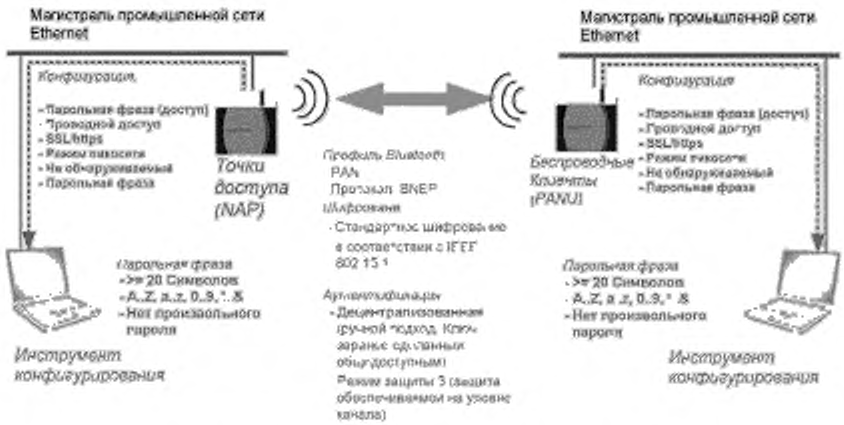


Рисунок 85 — Защита для Bluetooth сетей

Ниже описаны термины, использованные на рисунке 85:

SSL — уровень защищенных сокетов;

PAN — персональная сеть;

BNEP — протокол инкапсуляции сети Bluetooth;

NAP — точка доступа к сети;

PANU — пользователь персональной сети;

Точка доступа — координационная станция (ведущее устройство) беспроводной пикосети в соответствии с ИИЭР 802.11;

Беспроводной клиент — станция (ведомое устройство), входящая в пикосеть в соответствии с ИИЭР 802.11.

Таблица 22 — Средства защиты для Bluetooth (ИИЭР 802.15.1)

№	Элемент	Средство
1	Администрирование беспроводной точки доступа и беспроводного клиента	Разрешен только проводной доступ посредством SSL или https. Пароль/парольная фраза администрации не должен быть паролем по умолчанию
2	Качество парольной фразы для администрации	Длина парольной фразы должна составлять 16 символов. Символы должны представлять собой смесь буквенных, цифровых и специальных знаков
3	Эксплуатационные режимы	Устройства должны функционировать в базовом режиме пикосети, т. е. каждое устройство должно взаимодействовать только с одной пикосетью. Скаттернет сети не должны быть задействованы
4	Подходы к аутентификации	Bluetooth устройства должны использовать защитный режим 3 (принудительная защита канального уровня), как это определено в обязательном для применения ИИЭР 802.15.1. Аутентификация реализуется в децентрализованном подходе при помощи парольной фразы (PIN). Устройства, которые не предоставляют средства для изменения парольной фразы или которые работают только в защитных режимах 1 (никакой защиты) или 2 (защита уровня услуги) не допускаются
5	Качество парольной фразы для шифрования	Длина парольной фразы должна быть 16 символов. Символы должны представлять собой смесь буквенных, цифровых и специальных знаков.
6	Шифрование циклического обмена данными (PDU безопасности)	Шифрование в соответствии с ИИЭР 802.15.1 является обязательным

Окончание таблицы 18

№	Элемент	Средство
7	Открытость	Точка беспроводного доступа и клиенты должны быть сконфигурированы таким образом, чтобы их невозможно было обнаружить (закрытость)
Примечания 1 Длина парольной фразы должна быть доступной, так как пароли или парольные фразы должны вводиться только однажды во время сеанса ввода в эксплуатацию. 2 Шифрование циклического обмена данными защищает от манипуляции данных.		

9.8.4 Стационарные и мобильные приложения

Следует рассмотреть два типа приложений безопасности: «стационарные» приложения безопасности, характеризуемые хорошо определенным местоположением и передвижениями, и «мобильные» приложения безопасности.

Нет никаких ограничений или специальных оценок для стационарных приложений, таких как, циклические системы наполнения и сброса.

Развертывание мобильных беспроводных компонентов несет в себе дополнительные трудности. В частности, должно быть обеспечено однозначное распределение функций безопасности опасным оконечным элементам (например, роботам, см. ИСО 10218-1 [22]).

9.9 Классы соответствия

Производители F-устройств полагаются на некоторые свойства (фукнции), которые их партнеры (производители F-хост), как минимум, должны поддерживать помимо соответствия протоколу FSCP 3/1. Такие свойства перечислены в таблице 23.

Таблица 23 — Классы требований соответствия F-хосту

Элемент	Автоматизация работы предприятия	Автоматизация процесса	Примечание
Поддержка GSD	V5.04 (PB-DP) из [43]; V2.0 (PN-IO) из [47] или более поздние версии	То же самое	Затрагивает только F-параметры
Функциональные блоки коммуникаций в соответствии с МЭК 61131-3	Минимальный набор функциональных коммуникационных блоков это: RDREC, WRREC, RDIAG, RALRM [49]	То же самое	Поддержка MS1 является предусловием. Не обязательно для других прикладных профилей: GETIO_PART, SETIO_PART
iПар-сервер	Производители системы должны предоставлять услуги «iпар-сервера» с минимумом 2^{15} октетов	То же самое	Производителям систем настоятельно рекомендуется предоставлять следующие функциональные блоки коммуникаций: RDREC, WRREC, RDIAG (RALRM) [49]
Количество (биты)	Максимум 64 бита (логический тип), закодированных как Unsigned8, -16, -32	То же самое	Размеры поддерживаемых минимальных структур данных
Количество (типы данных)	12 октетов I/O	То же самое	Размеры поддерживаемых минимальных структур данных
Типы данных	Unsigned8, -16, -32, Integer16, -32, Не Real (Float)	Все типы данных FSCP 3/1: Unsigned8, -16, -32, Integer16, -32, Float32, Unsigned8+Unsigned8, Float32+Unsigned8	Должны соблюдаться правила FSCP 3/1 для драйверов F-канала
Интерфейс драйвера F-хоста	Все сигналы	Все сигналы	

Окончание таблицы 23

Элемент	Автоматизация работы предприятия	Автоматизация процесса	Примечание
Диагностика	Настоятельно рекомендуемые: сообщения об ошибках уровня безопасности (6.3.2)	Настоятельно рекомендуемые: сообщения об ошибках уровня безопасности (6.3.2)	Рекомендуемая литература: [50]
MS1	обязательно	обязательно	В соответствии CP 3/1
MS2	Не через контроллер (PLC)	не обязательно	Малые CPU могут не обеспечить проходную мощность интенсивного трафика
Заявляемый УПБ	3 (в областях специальных приложений, таких как CNC; минимальный уровень 2)	3	
Интеграция инструментальных средств, параметризация	Интерфейс инструментальных средств, соответствующий требованиям таблицы 12	В соответствии с [63] или через интерфейс инструментальных средств, соответствующий требованиям таблицы 12	

10 Оценка

10.1 Политика безопасности

Для того чтобы предотвратить и защитить производителей и поставщиков устройств FSCP 3/1 от возможного неправильного понимания или ложных ожиданий и крайней небрежности по отношению к разработкам и приложениям, связанным с безопасностью, в ходе каждого курса, семинара, практики или консультации следует отмечать и пояснять следующее:

- Не любое устройство будет автоматически применимо к приложениям, связанным с безопасностью, лишь по причине использования им коммуникаций с помощью полевых шин и коммуникационного уровня безопасности.
- Для того чтобы позволить использование изделия для приложений, связанных с безопасностью, должны соблюдаться надлежащие процессы разработки, соответствующие стандартам безопасности (см. МЭК 61508, МЭК 61511, МЭК 60204-1, МЭК 62061, ИСО 13849-2) и/или должна быть получена оценка, выполненная ответственным органом.
- Производитель изделия для систем безопасности несет ответственность за корректную реализацию технологии коммуникационного уровня безопасности, правильность и полноту документации и информации на это изделие.
- Дополнительная важная информация о фактических исправлениях, выполненных в результате завершенных запросов на изменение, должна быть рассмотрена для ее применения и оценки. Подобная информация может быть приобретена у организаций, перечисленных в Приложении В.

Полная информация также доступна в [66].

10.2 Обязательства

Как правило, международные стандарты безопасности принимаются (ратифицируются) по всему миру. Тем не менее, так как технологии безопасности в автоматизации относятся к технике безопасности на производстве и сопутствующим рискам страхования внутри страны, признание правил, выделенных в данном подразделе, по-прежнему является суверенным правом.

Национальные «органы власти» решают вопрос признания отчетов по оценке.

Примечание — Примерами подобных «Органов власти» являются BGIA (Berufsgenossenschaftliches Institut für Arbeitsschutz / BG — Институт профессиональной безопасности и здравоохранения) в Германии, HSE (Инспектор по охране здоровья и безопасности) в Великобритании, FM (Factory Mutual / Организация по страхованию имущества и управлению рисками), UL (Underwriters Laboratories Inc. / Организация тестирования безопасности продукции и сертификации), or the INRS (Institut National de Recherche et de Sécurité) во Франции.

Для FSCP 3/1 применяются правила оценки из МЭК 61784-3. Дополнительную информацию можно получить в [45].

Приложение А
(справочное)

Дополнительная информация для профиля коммуникаций функциональной безопасности CPF 3

А.1 Вычисление хэш функции

Процедура, представленная на рисунке А.1 обнаруживает 99,999 994 % всех ошибок, являющихся результатом модификации данных. С ее помощью также можно обнаруживать последовательные ошибки, так как проверка сигнатуры учитывает последовательность слов.

Для 24-битовой CRC сигнатуры, значение 15D6DCBh используется в качестве генерирующего полинома. Число битов данных может быть четным или нечетным. Значение, генерируемое после последнего октета, соответствует переданной CRC сигнатуре.

```
void crc24_calc(unsigned char x, unsigned long * r)
   int i;
   for (i = 1; i <= 8; i++)
      if ((bool)(*r & 0x800000) != (bool)(x & 0x80))
         /* XOR = 1 => Сдвиг и обработка полинома */
         *r = (*r << 1) ^ 0x5D6DCB;
         else
         /* XOR = 0 => pure shift */
         *r = *r << 1;
      x = x << 1;
/* for */
```

Рисунок А.1 — Типичная «С» процедура циклической проверки избыточностью

Оптимизированный во время выполнения вариант для вычисления сигнатуры CRC требует немного больше памяти. Соответствующая функция (А.1) в языке программирования С для вычислений 24-битовой CRC сигнатуры при помощи справочных таблиц показана ниже:

$$r = \text{crctab24}\,[((r >> 16)\ \hat{}\ *q{+}{+})\ \&\ 0xff]\ \hat{}\ (r << 8)\,, \qquad (A.1)$$

где:

- r представляет собой результат 24-битовой CRC сигнатуры;
- q представляет собой указатель на фактическое значение октета, для которого необходимо вычислить CRC. После считывания значения указатель должен быть увеличен для следующего октета посредством q++;
- начальное значение r равное «0».

Для этого вычисления используется таблица А.1.

Таблица А.1 – Таблица «Crctab24» для вычислений 24-битовой CRC сигнатуры

Т а б л и ц а А.1 — Таблица «Crctab24» для вычислений 24-битовой CRC сигнатуры

Справочная таблица CRC (0...255)							
0x000000	0x5D6DCB	0xBADB96	0xE7B65D	0x28DAE7	0x75B72C	0x920171	0xCF6CBA
0x51B5CE	0x0CD805	0xEB6E58	0xB60393	0x796F29	0x2402E2	0xC3B4BF	0x9ED974
0xA36B9C	0xFE0657	0x19B00A	0x44DDC1	0x8BB17B	0xD6DCB0	0x316AED	0x6C0726
0xF2DE52	0xAFB399	0x4805C4	0x15680F	0xDA04B5	0x87697E	0x60DF23	0x3DB2E8
0x1BBAF3	0x46D738	0xA16165	0xFC0CAE	0x336014	0x6E0DDF	0x89BB82	0xD4D649
0x4A0F3D	0x1762F6	0xF0D4AB	0xADB960	0x62D5DA	0x3FB811	0xD80E4C	0x856387
0xB8D16F	0xE5BCA4	0x020AF9	0x5F6732	0x900B88	0xCD6643	0x2AD01E	0x77BDD5
0xE964A1	0xB4096A	0x53BF37	0x0ED2FC	0xC1BE46	0x9CD38D	0x7B65D0	0x26081B
0x3775E6	0x6A182D	0x8DAE70	0xD0C3BB	0x1FAF01	0x42C2CA	0xA57497	0xF8195C
0x66C028	0x3BADE3	0xDC1BBE	0x817675	0x4E1ACF	0x137704	0xF4C159	0xA9AC92

Окончание таблицы А.1

Справочная таблица CRC (0...255)							
0x941E7A	0xC973B1	0x2EC5EC	0x73A827	0xBCC49D	0xE1A956	0x061F0B	0x5B72C0
0xC5ABB4	0x98C67F	0x7F7022	0x221DE9	0xED7153	0xB01C98	0x57AAC5	0x0AC70E
0x2CCF15	0x71A2DE	0x961483	0xCB7948	0x0415F2	0x597839	0xBECE64	0xE3A3AF
0x7D7ADB	0x201710	0xC7A14D	0x9ACC86	0x55A03C	0x08CDF7	0xEF7BAA	0xB21661
0x8FA489	0xD2C942	0x357F1F	0x6812D4	0xA77E6E	0xFA13A5	0x1DA5F8	0x40C833
0xDE1147	0x837C8C	0x64CAD1	0x39A71A	0xF6CBA0	0xABA66B	0x4C1036	0x117DFD
0x6EEBCC	0x338607	0xD4305A	0x895D91	0x46312B	0x1B5CE0	0xFCEABD	0xA18776
0x3F5E02	0x6233C9	0x858594	0xD8E85F	0x1784E5	0x4AE92E	0xAD5F73	0xF032B8
0xCD8050	0x90ED9B	0x775BC6	0x2A360D	0xE55AB7	0xB8377C	0x5F8121	0x02ECEA
0x9C359E	0xC15855	0x26EE08	0x7B83C3	0xB4EF79	0xE982B2	0x0E34EF	0x535924
0x75513F	0x283CF4	0xCF8AA9	0x92E762	0x5D8BD8	0x00E613	0xE7504E	0xBA3D85
0x24E4F1	0x79893A	0x9E3F67	0xC352AC	0x0C3E16	0x5153DD	0xB6E580	0xEB884B
0xD63AA3	0x8B5768	0x6CE135	0x318CFE	0xFEE044	0xA38D8F	0x443BD2	0x195619
0x878F6D	0xDAE2A6	0x3D54FB	0x603930	0xAF558A	0xF23841	0x158E1C	0x48E3D7
0x599E2A	0x04F3E1	0xE345BC	0xBE2877	0x7144CD	0x2C2906	0xCB9F5B	0x96F290
0x082BE4	0x55462F	0xB2F072	0xEF9DB9	0x20F103	0x7D9CC8	0x9A2A95	0xC7475E
0xFAF5B6	0xA7987D	0x402E20	0x1D43EB	0xD22F51	0x8F429A	0x68F4C7	0x35990C
0xAB4078	0xF62DB3	0x119BEE	0x4CF625	0x839A9F	0xDEF754	0x394109	0x642CC2
0x4224D9	0x1F4912	0xF8FF4F	0xA59284	0x6AFE3E	0x3793F5	0xD025A8	0x8D4863
0x139117	0x4EFCDC	0xA94A81	0xF4274A	0x3B4BF0	0x66263B	0x819066	0xDCFDAD
0xE14F45	0xBC228E	0x5B94D3	0x06F918	0xC995A2	0x94F869	0x734E34	0x2E23FF
0xB0FA8B	0xED9740	0x0A211D	0x574CD6	0x98206C	0xC54DA7	0x22FBFA	0x7F9631
Примечание — Данная таблица содержит 24-битовые значения для каждого значения (0...255) аргумента a в функции crctab24[a]. Таблица должна читаться в восходящем порядке, от верхнего левого (0) до нижнего правого (255).							

Соответствующая функция (А.1) в языке программирования С для вычислений 32-битовой CRC подписи при помощи справочных таблиц показана ниже:

$$r = \text{crctab32}\,[((r >> 24)\ \hat{}\ *q{+}{+})\ \&\ 0\text{xff}]\ \hat{}\ (r << 8). \qquad (A.2)$$

Для этого вычисления используется таблица А.2.

Таблица А.2 — Таблица «Crctab32» для вычислений 32-битовой CRC сигнатуры

Справочная таблица CRC (0...255)							
00000000	F4ACFB13	1DF50D35	E959F626	3BEA1A6A	CF46E179	261F175F	D2B3EC4C
77D434D4	8378CFC7	6A2139E1	9E8DC2F2	4C3E2EBE	B892D5AD	51CB238B	A567D898
EFA869A8	1B0492BB	F25D649D	06F19F8E	D44273C2	20EE88D1	C9B77EF7	3D1B85E4
987C5D7C	6CD0A66F	85895049	7125AB5A	A3964716	573ABC05	BE634A23	4ACFB130
2BFC2843	DF50D350	36092576	C2A5DE65	10163229	E4BAC93A	0DE33F1C	F94FC40F
5C281C97	A884E784	41DD11A2	B571EAB1	67C206FD	936EFDEE	7A370BC8	8E9BF0DB
C45441EB	30F8BAF8	D9A14CDE	2D0DB7CD	FFBE5B81	0B12A092	E24B56B4	16E7ADA7
B380753F	472C8E2C	AE75780A	5AD98319	886A6F55	7CC69446	959F6260	61339973
57F85086	A354AB95	4A0D5DB3	BEA1A6A0	6C124AEC	98BEB1FF	71E747D9	854BBCCA
202C6452	D4809F41	3DD96967	C9759274	1BC67E38	EF6A852B	0633730D	F29F881E

Окончание таблицы А.2

Справочная таблица CRC (0...255)							
B850392E	4CFCC23D	A5A5341B	5109CF08	83BA2344	7716D857	9E4F2E71	6AE3D562
CF840DFA	3B28F6E9	D27100CF	26DDFBDC	F46E1790	00C2EC83	E99B1AA5	1D37E1B6
7C0478C5	88A883D6	61F175F0	955D8EE3	47EE62AF	B34299BC	5A1B6F9A	AEB79489
0BD04C11	FF7CB702	16254124	E289BA37	303A567B	C496AD68	2DCF5B4E	D963A05D
93AC116D	6700EA7E	8E591C58	7AF5E74B	A8460B07	5CEAF014	B5B30632	411FFD21
E47825B9	10D4DEAA	F98D288C	0D21D39F	DF923FD3	2B3EC4C0	C26732E6	36CBC9F5
AFF0A10C	5B5C5A1F	B205AC39	46A9572A	941ABB66	60B64075	89EFB653	7D434D40
D82495D8	2C886ECB	C5D198ED	317D63FE	E3CE8FB2	176274A1	FE3B8287	0A977994
4058C8A4	B4F433B7	5DADC591	A9013E82	7BB2D2CE	8F1E29DD	6647DFFB	92EB24E8
378CFC70	C3200763	2A79F145	DED50A56	0C66E61A	F8CA1D09	1193EB2F	E53F103C
840C894F	70A0725C	99F9847A	6D557F69	BFE69325	4B4A6836	A2139E10	56BF6503
F3D8BD9B	07744688	EE2DB0AE	1A814BBD	C832A7F1	3C9E5CE2	D5C7AAC4	216B51D7
6BA4E0E7	9F081BF4	7651EDD2	82FD16C1	504EFA8D	A4E2019E	4DBBF7B8	B9170CAB
1C70D433	E8DC2F20	0185D906	F5292215	279ACE59	D336354A	3A6FC36C	CEC3387F
F808F18A	0CA40A99	E5FDFCBF	115107AC	C3E2EBE0	374E10F3	DE17E6D5	2ABB1DC6
8FDCC55E	7B703E4D	9229C86B	66853378	B436DF34	409A2427	A9C3D201	5D6F2912
17A09822	E30C6331	0A559517	FEF96E04	2C4A8248	D8E6795B	31BF8F7D	C513746E
6074ACF6	94D857E5	7D81A1C3	892D5AD0	5B9EB69C	AF324D8F	466BBBA9	B2C740BA
D3F4D9C9	275822DA	CE01D4FC	3AAD2FEF	E81EC3A3	1CB238B0	F5EBCE96	01473585
A420ED1D	508C160E	B9D5E028	4D791B3B	9FCAF777	6B660C64	823FFA42	76930151
3C5CB061	C8F04B72	21A9BD54	D5054647	07B6AA0B	F31A5118	1A43A73E	EEEF5C2D
4B8884B5	BF247FA6	567D8980	A2D17293	70629EDF	84CE65CC	6D9793EA	993B68F9

Примечание — Данная таблица содержит 32-битовые значения в шестнадцатеричном представлении для каждого значения (0...255) аргумента a в функции crctab32[a]. Таблица должна читаться в восходящем порядке верхнего левого (0) до нижнего правого (255).

А.2 Измерения времени реакции

В 9.3.1 описана упрощенная модель для типичного времени реакции. Сравнение этой модели и реального приложения, полученного от различных поставщиков, для 15 000 образцовых измерений показано на рисунке А.2. В данном случае скорость передачи была 1,5 Мбит/с и F-хост выполнял приложение, связанное с безопасностью, (программу) каждые 20 мс.

Дополнительные компьютеры, такие как панели программиста и диагностические панели, использующие не периодический доступ к сети (рисунок 3), оказывают мало или никакого влияния на время реакции, если сеть сконфигурирована в соответствии с рекомендациями производителя. На рисунке А.3 показана гистограмма времени реакции настоящего приложения CP 3/1 и FSCP 3/1, полученного от множества поставщиков, при 1,5 Мбит/с и в двух разных стрессовых ситуациях. Синяя кривая представляет собой 22 000 измерений с независимым PLC безопасности. Темно синяя кривая представляет собой 6 500 измерений с тем же PLC, дополнительным программатором (PG), периодически отображающим статус программы, и диагностической панелью (PC), периодически отображающей статус лучей световой завесы. PG и PC взаимодействовали посредством не периодических услуг CP 3/1 (класс 2 ведущего устройства).

Это показывает, что два дополнительных устройства-супервизора, как и ожидалось, оказывают либо небольшое, либо никакого влияния на время реакции. Кривые близки к нормальному распределению (колоколообразная кривая) с минимальным временем реакции 13 мс, максимальным времен реакции 35 мс и средним временем реакции 24 мс.

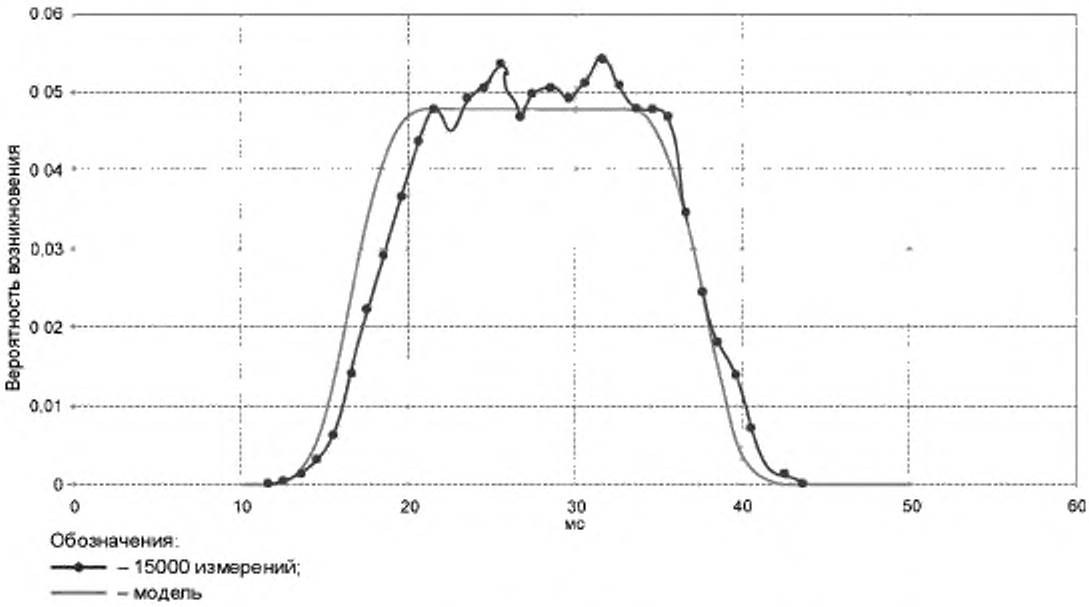


Рисунок А.1 — Сравнение времени реакции модели и реального приложения

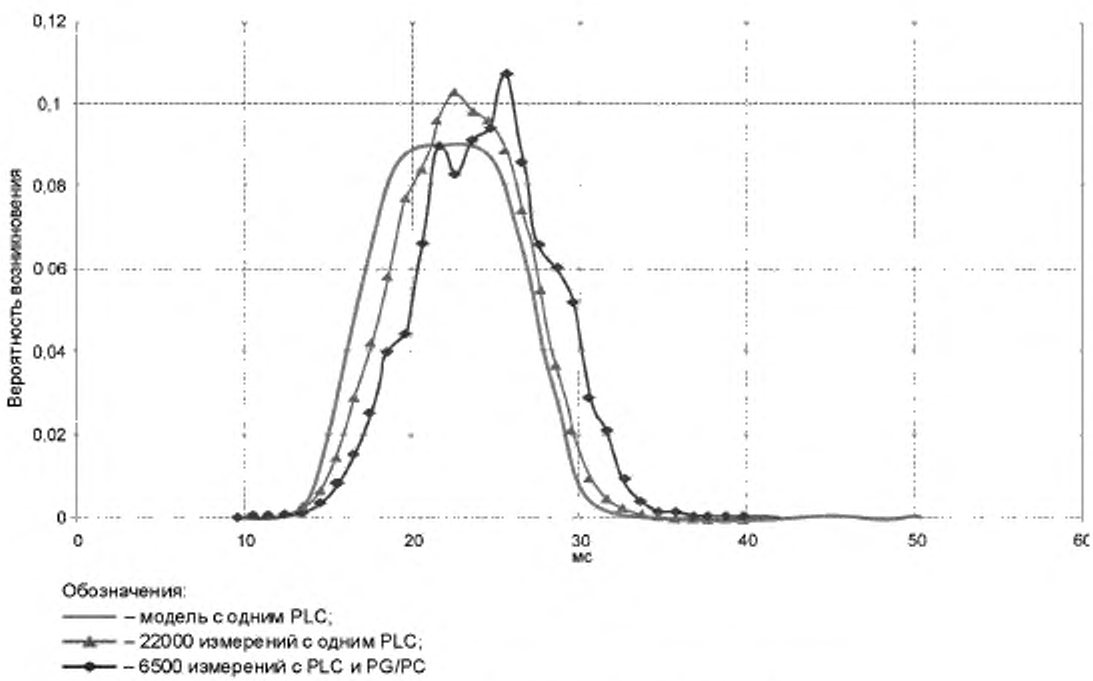


Рисунок А.2 — Распределение частот измеренного времени реакции

Значения цветов, использованных на рисунке А.3, приведены ниже:

циан — модель, включающая один PLC (CPU);

синий — 22 000 измерений времени реакции с приложением от разных поставщиков и одним PLC (F-Хост);

темно-синий — 6 500 измерений времени реакции с приложением от разных поставщиков, используя один PLC (F-хост), плюс один программатор (класс ведущего устройства 2) для функции «циклический статус программы» плюс одна дополнительная диагностическая панель (второй класс 2 ведущего устройства) для функции «циклический статус световой завесы».

F-хост модели использует один CPU для стандартных программ и программ безопасности. Обе программы выполняются на разных уровнях операционной системы для обеспечения логического разделения прикладных программ, связанных с безопасностью, и стандартных программ. На рисунке А.4 показаны примеры разных сегментаций стандартной программы для нескольких значений временного триггера. Это демонстрирует, что изменение в части стандартной программы не сказывается на выполнении программы безопасности. Тем не менее, может быть важно сбалансировать обновление стандартных выводов и выводов безопасности, если необходимо использовать сигналы из другой части для целей координации.

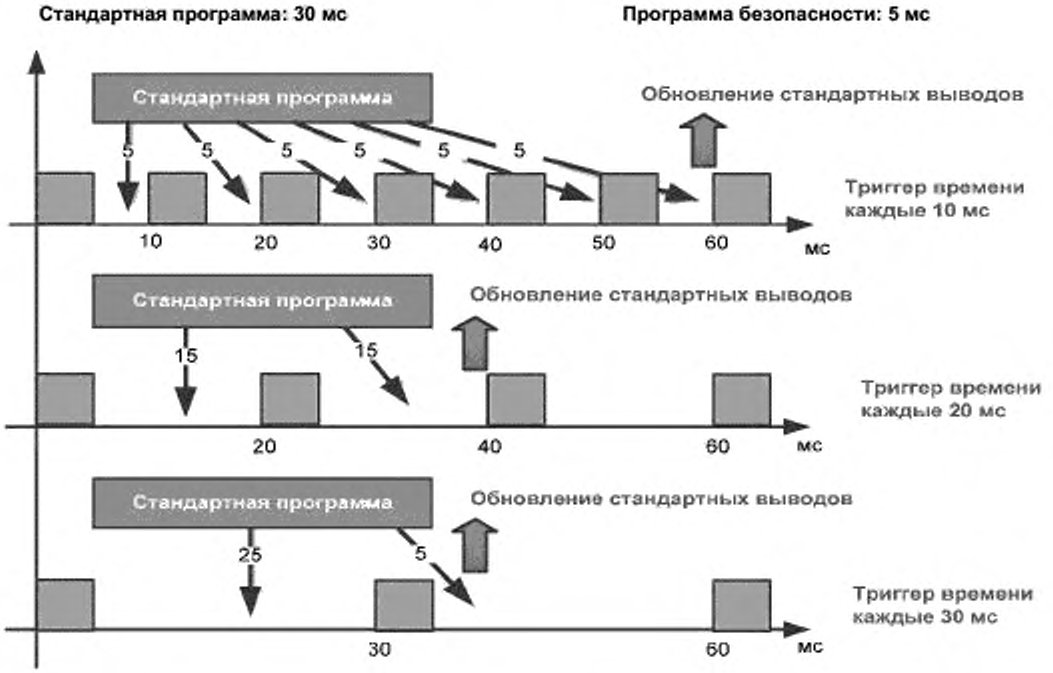


Рисунок А.3 — F-хост со стандартными и связанными с безопасностью прикладными программами

Приложение В
(справочное)

Информация для оценки профилей коммуникаций функциональной безопасности CPF 3

Информация о тестовых лабораториях, которые испытывают и подтверждают соответствие продуктов FSCP 3/1 стандарту МЭК 61784-3-3 может быть получена у Национальных Комитетов МЭК или у следующих организаций:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Str. 7
76131 Karlsruhe
GERMANY

Phone: +49 721 96 58 590
Fax: +49 721 96 58 589
E-mail: info@profibus.com
URL:www.profibus.com or
URL:www.profisafe.net

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 60204-1	IDT	ГОСТ Р МЭК 60204-1—2007 «Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования»
IEC 61000-6-2	MOD	ГОСТ Р 51317.6.2—2007 (МЭК 61000-6-2: 2005) «Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых в промышленных зонах. Требования и методы испытаний»
IEC 61010-1	MOD	ГОСТ 12.2.091—2012 (IEC 61010-1:2001) «Безопасность электрического оборудования для измерения, управления и лабораторного применения. Часть 1. Общие требования»
IEC 61131-2	IDT	ГОСТ IEC 61131-2—2012 «Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания»
IEC 61131-3	–	*
IEC 61158-2	–	*
IEC 61158-3-3	–	*
IEC 61158-4-3	–	*
IEC 61158-5-3	–	*
IEC 61158-5-10	–	*
IEC 61158-6-3	–	*
IEC 61158-6-10	–	*
IEC 61326-3-1	–	*
IEC 61326-3-2	–	*
IEC 61508 (все части)	IDT	ГОСТ Р МЭК 61508—2012 (все части) «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
IEC 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
IEC 61511 (все части)	IDT	ГОСТ Р МЭК 61511-1—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов»
IEC 61784-1	–	*
IEC 61784-2	–	*
IEC 61784-3:2010	–	*
IEC 61784-5-3	–	*
IEC 61918	–	*
IEC 62061	IDT	ГОСТ Р МЭК 62061—2013 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью»
IEC 62280-1	–	*
IEC 62280-2	–	*

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC/TR 62390	–	*
ISO 13849-1	IDT	ГОСТ Р ИСО 13849-1—2003 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования»
ISO 13849-2	–	*
ISO 15745-3	IDT	ГОСТ Р ИСО 15745-3—2010 «Системы промышленной автоматизации и интеграция. Прикладная интеграционная среда открытых систем. Часть 3. Эталонное описание систем управления на основе стандарта МЭК 61158»
ISO 15745-4	IDT	ГОСТ Р ИСО 15745-4—2012 «Системы промышленной автоматизации и интеграция. Прикладная интеграционная среда открытых систем. Часть 4. Эталонное описание систем управления на основе стандарта Ethernet»

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

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичный стандарт;
- MOD — модифицированный стандарт.

Библиография

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

Примечание — См. также IEC Multilingual Dictionary — Electricity, Electronics and Telecommunications (доступно на CD-ROM или at <http://www.electropedia.org>).

[2] IEC 60870-5-1, Telecontrol equipment and systems — Part 5: Transmission protocols — Section One: Transmission frame formats

[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 61131-612, Programmable controllers — Part 6: Functional safety

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

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

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

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

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

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

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

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

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

[14] IEC 61804 (all parts), Function blocks (FB) for process control

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

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

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

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

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

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

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

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

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

[24] ISO 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] IEEE 802.11i-2004 Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003): IEEE Standard for Information technology — Telecommunications and information exchange between system — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications — Amendment 6: Medium Access Control (MAC) Security Enhancements

[27] IEEE 802.15.1-2005: IEEE Standard for Information technology — Telecommunications and information exchange between systems-Local and metropolitan area networks — Specific requirements

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

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

[30] VDI/VDE-Richtlinien 2180, Part 1-4: 2006, Safeguarding of industrial process plants by means of process control engineering, (in German language),

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

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

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

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

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

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

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

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

[39] GUY E. CASTAGNOLI, On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy-Check Codes, 1989, Dissertation No. 8979 of ETH Zurich, Switzerland
[40] GUY E. CASTAGNOLI, STEFAN BRÄUER, and MARTIN HERRMANN, Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits, June 1993, IEEE Transactions On Communications, Volume 41, No. 6
[41] SCHILLER F and MATTES T: An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication, Journal of Applied Computer Science, Vol. 14, No 1, pp. 57-80, Technical University Press, Łódź,Poland, 2006
[42] SCHILLER F and MATTES T: Analysis of CRC-polynomials for Safety-critical Communication by Deterministic and Stochastic Automata, 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, pp. 1003-1008, Beijing, China, 2006
[43] PROFIBUS Guideline: Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.1, July 2008. Order-No. 2.122
[44] PROFIBUS Guideline: PROFIsafe — Environmental Requirements, V2.5, March 2007. Order-No. 2.232
[45] PROFIBUS Guideline: PROFIsafe — Test Specification for F-Slaves, F-Devices, and FHosts, V2.1, March 2007. Order-No. 2.242
[46] PROFIBUS Profile Guideline, Part 1: Identification & Maintenance Functions, V1.2, October 2009. Order-No. 3.502
[47] PROFIBUS Guideline: GSDML Specification for PROFINET IO, Version 2.2, July 2008. Order-No. 2.352
[48] PROFIBUS Guideline: PROFIsafe — Profile for Safety Technology, V1.30, June 2004. Order-No. 3.092
[49] PROFIBUS Guideline: Communication Function Blocks on PROFIBUS DP and PROFINET IO, V2.0, November 2005. Order-No. 2.182
[50] PROFIBUS Profile Guideline, Part 3: Diagnosis, Alarms, and Time Stamping, V1.0, June 2004. Order-No. 3.522
[51] PROFINET Guideline: PROFINET Cabling and Interconnection Technology, Version 2.0, May 2007. Order-No. 2.252
[52] PROFINET Guideline: Installation Guideline PROFINET Part 2, Network Components, Version 1.01, Februar 2004. Order-No. 2.252p2
[53] PROFINET Guideline: PROFINET Security, V1.0, March 2005. Order-No. 7.002
[54] MANFRED POPP, The New Rapid Way to PROFIBUS DP, 2002. Order-No. 4.072
[55] MANFRED POPP, Industrial Communication with PROFINET, 2007. Order-No. 4.182
[56] OPC Foundation, < www.opcfoundation.org >
[57] Object Management Group, Unified Modeling Language: Superstructure, Version 2.0; Formal/05-07-04;available at < www.omg.com >
[58] NAMUR, NE97 — Fieldbus for safety-related uses, 2003; available at < www.namur.de >
[59] REC-xml-20081126, Extensible Markup Language (XML) 1.0 (Fifth Edition) — W3C Recommendation 26 November 2008, available at < www.w3.org/TR/2008/REC-xml-20081126 >
[60] REC-xmlschema-1-20041028, XML Schema Part 1: Structures (Second Edition) — W3C Recommendation 28 October 2004, available at < www.w3.org/TR/2004/REC-xmlschema-1-20041028 >
[61] REC-xmlschema-2-20041028, XML Schema Part 2: Datatypes (Second Edition) — W3C Recommendation 28 October 2004, available at < www.w3.org/TR/2004/REC-xmlschema-2-20041028 >
[62] USB Implementers Forum, Inc , Universal Serial Bus Revision 2.0 specification, available at < http://www.usb.org/developers/docs >
[63] PROFIBUS Specification: Amendment PA-Devices on PROFIsafe, V1.01, March 2009; Order-No. 3.042
[64] PROFIBUS Guideline: Cabling and Assembly, V1.0.6, May 2006. Order No. 8.022
[65] PROFIBUS Guideline: Commissioning, V1.0.2, November 2006. Order No. 8.032
[66] PROFIBUS Guideline: PROFIsafe Policy, V1.3, February 2003. Order No. 2.282
[67] PROFIBUS Profile Guideline, Part 2: Data types, Programming Languages, and Platforms, V1.0, September 2006. Order-N. 3.512
[68] PROFIBUS Specification: Amendment PROFIdrive on PROFIsafe, V2.1, April 2009. Order-No. 3.272
[69] PROFINET Specification: Configuration in Run, dV0.1, August 2009. Order-No. 2.512

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

Ключевые слова: промышленные сети, профили, функциональная безопасность полевых шин, спецификации для CPF 3

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *А.С. Тыртышного*

Сдано в набор 22.12.2016. Подписано в печать 26.01.2017. Формат 60 × 84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 13,95. Уч.-изд. л. 12,62. Тираж 27 экз. Зак. 223.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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