ФЕДЕРАЛЬНОЕ АГЕНТСТВО

**ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**

**Н А Ц И О Н А Л Ь Н Ы Й С Т А Н Д А Р Т Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И**

**ГОСТР**

**МЭК 61784-3-3—**

2016

### Промышленные сети

**ПРОФИЛИ**

Ч а с т ь 3 - 3

### Функциональная безопасность полевых шин.

**Дополнительные спецификации для CPF 3**

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

Издание официальное

Москва Стандартинформ

2017

ГОСТ Р МЭК 61784-3.3—2016

Предисловие

1. ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные си­ стемы» на основе собственного перевода на русский язык англоязычной версии международного стан­ дарта. 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 регу­ лированию и метрологии от 30 ноября 2016 г. № 1884-ст
4. Настоящий стандарт идентичен международному стандарту МЭК 61784-3-3:2010 «Промышлен­ ные сети. Профили. Часть 3-3. Функциональная безопасность полевых шин. Дополнительные специфи­ кации 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 междуна­ родных стандартов соответствуощие им национальные и межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА

1. ВВЕДЕН ВПЕРВЫЕ

*Правила применения наспоящего стандарта установлены е статье 26 Федерального закона от 29 июня 2015 г. N9 162-ФЗ* «О *стандартизации в Российской Федерации». Информация об измене­ ниях к настоящему стандарту публикуется е ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты». а текст изменений и поправок* — е еже­ месячном *информационном укгзателе* «Национальные *стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление* будет *опубликовано в ежеме­ сячном 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*](http://www.gost.ru/)*)*

©Стандартинформ. 2017 Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и рас­

пространен в качестве официального издания без разрешения Федерального агентства по техническо­ му регулированию и метрологии

и

ГОСТ Р МЭК 61784-3-3—2016

Содержание

1. [Область применения. 1](#_bookmark0)
2. [Нормативные ссылки. 1](#_bookmark1)
3. [Термины, определения, сокращения и условные обозначения. 3](#_bookmark2)
   1. Термины и определения. 3
   2. Обозначения и сокращения. 9
   3. Условные обозначения. 11
4. [Обзор FSCP 3/1 (PROFlsafe™). 11](#_bookmark3)
5. [Общие положения. 14](#_bookmark4)
   1. внешние документы, предоставляющие спецификации для профиля. 14
   2. Функциональные требования безопасности. 14
   3. Меры безопасности. 14
   4. [Структура коммуникационного уровня безопасности. 15](#_bookmark5)
   5. Связи с FAL{n DLL. PhL). 19
6. [Услуги коммуникационного уровня безопасности 23](#_bookmark6)
   1. Услуги F-xocra. 23
   2. Услуги F-устройств. 26
   3. Диагностика. 27
7. Протокол коммуникационного уровня безопасности. 28
   1. Формат PDU безопасности. 28
   2. Поведение FSCP 3/1. 34
   3. Реакция в случав неиспраеюсти. 53
   4. Запуск и координация иэмвьвний. 55
8. [Управление коммуникационным уровнем безопасности. 56](#_bookmark7)
   1. F-Параметр. 56

6.2 Шарамеф и iPar\_CRC. 62

* 1. Параметризация безопасности. 63
  2. Конфигурация безопасности. 67
  3. Использование информации типов данных. 70
  4. Механизмы назначения параметров безопасности. 73

1. [Системные требования. 86](#_bookmark8)
   1. Индикаторы и коммутаторы. 86
   2. Руководство по установке. 86
   3. время реакции функции безопасности. 86
   4. Длительность запросов на обслуживание. 93
   5. Ограничения для вычисления системных характеристик. 93
   6. Техническое обслуживание. 96
   7. Руководство по безопасности. 97
   8. Беспроводные каналы передачи данных. 98
   9. Классы соответствия. 101

III

ГОСТ Р МЭК 61784-3.3—2016

1. [Оценка. 102](#_bookmark9)
   1. Политика безопасности. 102
   2. Обязательства. 102

Приложение А (справочное) Дополнительная информация для профиля коммуникаций

функциональной безопасности CPF 3..................................................................................... ЮЗ

Приложение В (справочное) Информация для оценки профилей коммуникаций функциональной

безопасности CPF 3................................................................................................................ Ю8

Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов

национальным и межгосударственным стандартам. 109

Библиография. 111

IV

ГОСТ Р МЭК 61784-3-3—2016

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 осу­ ществлять 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 времена, 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 ком­ муникационных 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 электробеэопасности и искробезопасности.

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

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

Коммуникационные уровни безопасности, реализованные в составе систем, связанных с безопас­ ностью. в соответствии с МЭК 61506 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 которою определен соответствующий ему профиль коммуникации, удовлетворяющий требованиям функциональной безопасности.

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

Настоящий стандарт описывает:

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

1. Патентная декларация

Международный электротехжческий комитет (МЭК) обращает внимание на то. что соблюдение требований настоящею стандарта может включать использование патентов, относящихся к профилям коммуникаций, соответствующих требованиям функциональной безопасности. Для семейства 1 патентов приведено ниже, где обозначение |хх) указывает на держателя патента;

ЕР1267270-А2 (SI) WO00/045562-A1 [SI] WO99/049378-A1 (SI] ЕР1686732 [SI)

ЕР1802019 [SI] ЕР1921525-А1 (SI)

Метзд для передачи данных

Метзд и устройство для определения надежности переносчиков данных Укороченное сообщение с данными системы автоматизации

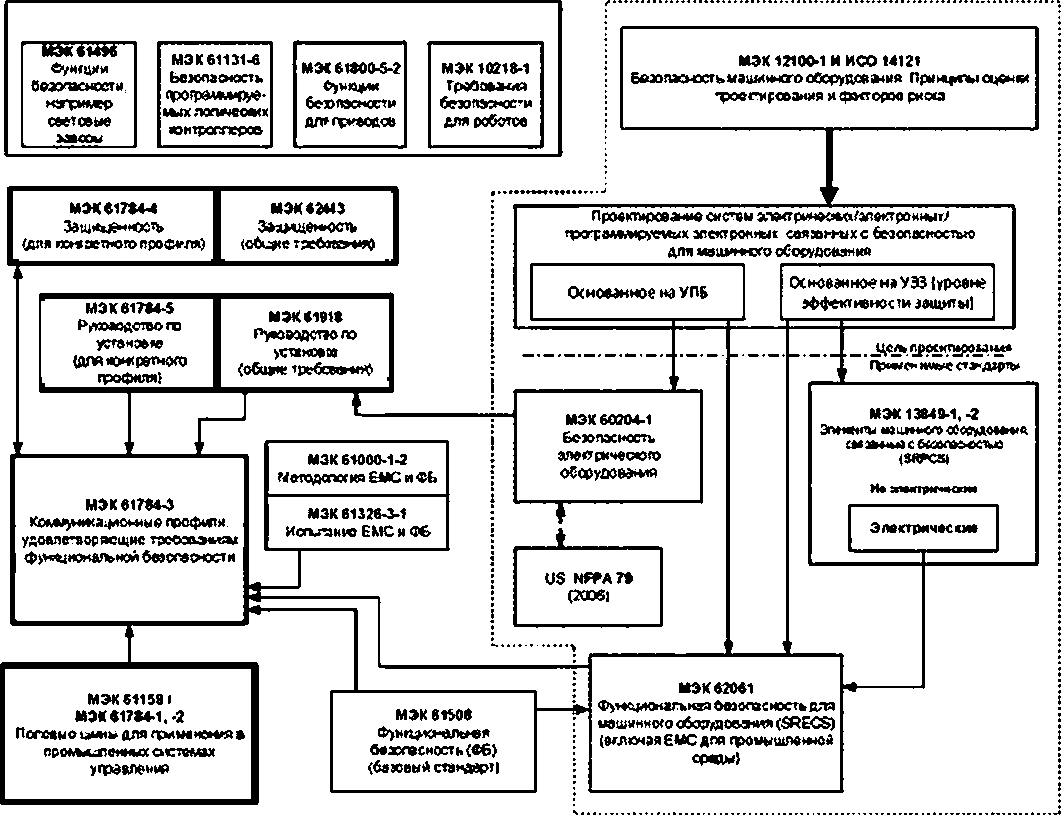
Метзд и система для передачи блоков данных протокола Идентификация ошибок в передаче данных

Метзд для эксплуатации системы, связанной с безопасностью

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

V

ГОСТ Р МЭК 61784-3.3—2016



Обоэдчений:

(волгый) • стандарты. сшаамиыо с безопасностью; (голубой) • стандарты. связанные с л«н\*выми иииамн.

(блодмо жолтмй) - ивсгоеций 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

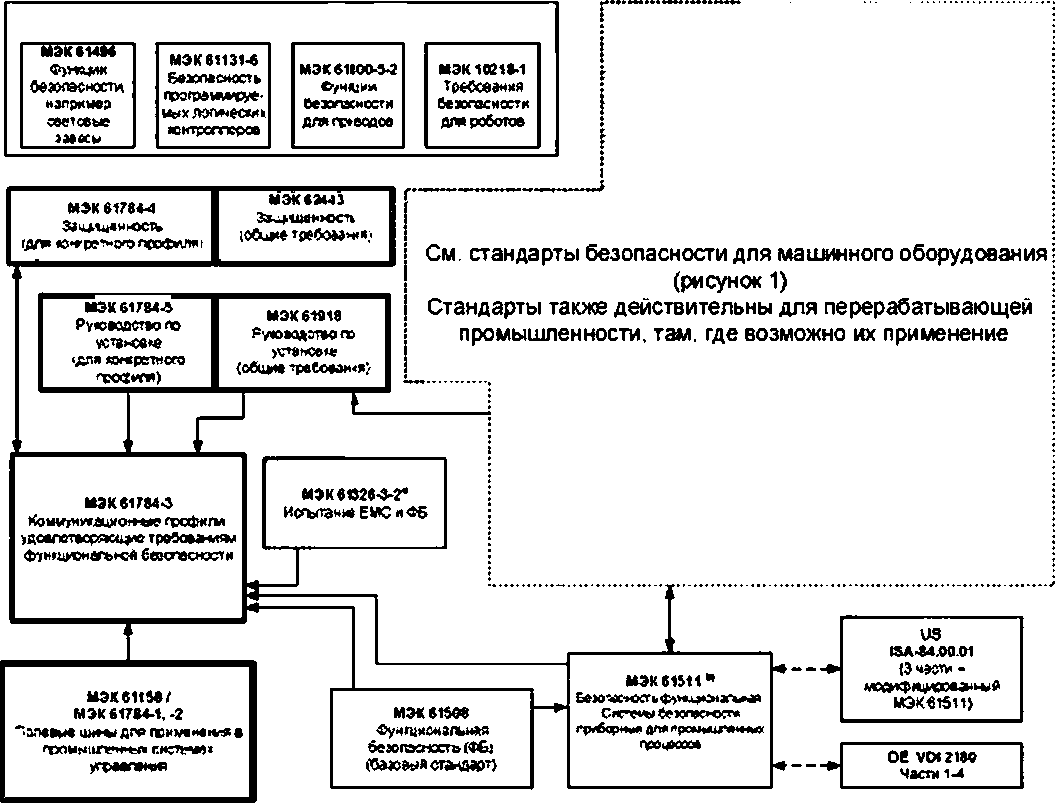
MAAS FA ТС

76187 Karlsruhe GERMANY

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

VI

ГОСТ Р МЭК 61784\*3-3—2016



Обовмачгмия:

(ЖАЛТЫЙ) • СТАНДАРТЫ. СААМ4НЫА с Оаэоласи остью.

J{голубой) - СТАМ ДА рТЫ. СОЯМИ >ШО С ПОПОВЫМИ шинами:

{бледно желтый) - юсгояций стандарт

‘'Дон устаноеленньп эпектроматчптиыа акт. о противной случае МЭК в1326-3-1 "РятифмдооАам EN

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

VII

ГОСТ Р МЭК 61784-3-3—2016

Н А Ц И О Н А Л Ь Н Ы Й С Т А Н Д А Р Т Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И

Промышленные сети

ПРОФИЛИ

Ч а с т ь 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 (СР 3/1, СР 3/2, СР 3/4. СР 3/5 и СР 3/6) и МЭК 61158, Типы 3 и 10. Настоящий стандарт идентифицирует принципы для осуществления комму­ никаций. удовлетворяющих требованиям функциональной безопасности, определенным в МЭК 61784-3 и имеющим важное значение для данного коммуникационного уровня безопасности.

Примечание — Настоящий стандарт не затрагивает вопросы электробеэопасносги и искробеэопасности. Электробеэопэсносгь связана с угрозгми, такими как электрический шок. Искробеэопэсностъ 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 тре­ бованиями функциональной безопасности, представленными в комплексе МЭК 61508”. 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 соответ­ ствующих приборов и систем.

Примечание — Результирующий УПБ. заявляемый для системы, зависит от реализации выбранного профиля коммуникации, удовлетворявшего 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.

1. 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. Помехо­ устойчивость для промышленных обстановок)

” Далее 8 настоящем стандарте используется «МЭК 61508» вместо «комплекс МЭК 61508»

Издание официальное

1

ГОСТ Р МЭК 61784-3.3—2016

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. Programmablecontrollers — 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 кон­ троллеры. 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 канальнсго 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 протскола 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 61156-5-9. 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 61156-6-5. 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 безо­ пасностью (функциональной безопасности) Общие промышленные приложения)

IEC 61326-3-2. Electrical equipment for measurement, control and laboratory use — EMC require­ ments Part 3 2: Immunity requirements for eafety related systems and for equipment intended to perform

safety related functions (functional safety) — Industrial applications with specified electromagnetic environment (Электрооборудование для измерений, управления и лаборатного 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 электрон­ ных. связанных с безопасностью)

IEC 61508-2:2010. Functicnal safety of electrical/electronicfprogrammable electronic safety-related systems — Part 2: Requirements for electrical/electronicfprogrammable electronic safety related systems (Функ­ циональная 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). Functonal 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. Чать 1. Профили полевых шин)

(IEC 61764-2. Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ISOslEC 8802-3 (Промышленные сети. Профили. Часть 2. Дополнительные профили полевых шин для сетей реального времени, основанные на ИСО/МЭК 8802-3)

2

ГОСТ Р МЭК 61784-3-3—2016

IEC 61784-3:2010. Industrial communication networks — Profiles — Part 3: Functional safety fieidbu- ses — 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 comnunication 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 machirery — Functional safety of safety-related electrical, electronic and programmable electronic control systems (Безопасность оборудования. Функциональная безопасность систем управления элвктрических/электронных/программируемых электронных, связанных с безопас­ ностью)

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 свя­ зи. 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 устройст­ во. Руководящие принципы профиля)

IS013849-1. 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 (Безо­

пасность 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 611 S8-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)

1. 1ермины, определения, сокращения и условные оьозначения

3.1 Термины и определения

8 настоящем стандарте используются следующие термины и определения:

* + 1. Термины и определения
       1. готовность (availability): Вероятность того, что в течение заданного промежутка времени в автоматизированной системе не наблюдается неисправных состояний в системе, приводящих к потере производительности.
       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. канал связи (communication channel): Логическое соединение между двумя конечными

точками внутри коммуникационной системы.

* + - 1. коммуникационная система (communication system): Система (устройство), состоящая из технических средств, программчого обеспечения и среды распространения, которая обеспечивает передачу сообщений (прикладной уровень по ИСО/МЭК 7498) от одного приложения другому.
      2. соединение (connection): Логическое связывание между двумя прикладными объектами в

одном или е разных устройствах.

* + - 1. циклический контроль избыточности (Cyclic Redundancy Check. CRC): Получаемые из блока данных (значений) избыточные данные, которые запоминаются и передаются вместе с этим бло­ ком данных для обнаружения искажения данных. Процедура (метод), использующаяся для вычисления избыточных данных.

3

ГОСТ Р МЭК 61784-3.3—2016

Примечания

1 Термины «CRC код» и «CRC подпись» и обозначения, такие как «CRC 1» и «CRC 2». также могут приме­ няться в настоящем стандарте в от-юшвкии избыточных данных.

2 См. также (32]. (33].

* + - 1. ошибка (error): Расхождение между вычисленным, наблюдаемым или измеренным значе­ нием или условием и истинным установленным или теоретически верным значением или условием.

[МЭК 61508-4:2010]. (МЭК 61156]

Примечания

1. Ошибки могут возникнуть вследствие ошибок проектирования аппаратных средств/ программного обеспече­ ния и/или вследствие искажения данных, вызванного электромагнитными помехами и/или другими воздействиями.
2. Ошибки не обязательно являются причиной отхаэое или сбоев.

3.1.1.6 отказ (failure): Пре<ращекие способности функционального блока выполнять необходи­ мую 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]

Примечен и е — Причиной отказа может служить ошибка (например, проблема, связанная с проектиро­ ванием программного обвспечения’алпаратных средств или с нарушением при передаче сообщений).

* + - 1. сбой (fault): Ненормальный режим, который может вызвать снижение или потерю способ­ ности функционального блока выполнять требуемую функцию.

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

(МЭК 61506-4:2010. модифицировано]. (ИСО/МЭК 2382-14.01.10, модифицировано]

* + - 1. полевая шина (fiddbus): Коммуникационная система, основанная на последовательной передаче данных и применяющаяся в промышленной автоматизации или приложениях управления процессами.
      2. система полевых шин (fieldbus system): Система, использующая полевую шину с под­ ключенными устройствами.
      3. кадр (frame): Упрощенный синоним для DLPOU (Блок данных протокола канала переда­

чи данных).

* + - 1. последовательность проверки кадра [frame check sequence (FCS)]: Дополнительные данные, полученные для блока данных DLPOU (кадра) с помощью хеш-функции, которые запоминают­ ся и передаются вместе с этим блоком донных, для обнаружения искажения данных.

Примечания

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

2 См. также (32]. (33].

* + - 1. 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-фучкции включают е себя контроль четности, вычисление контрольной суммы или CRC.

(МЭК/TR 62210. модифицировано]

* + - 1. опасность (hazard): Состояние или набор условий в системе, которые вместе с други­ ми. связанными с этим, условиями неизбежно приведут к причинению вреда человеку, имуществу или окружающей среде.
      2. ведущее устройство (master): Активный объект коммуникации, способный иницииро­ вать и управлять во времени коммуникационной деятельностью других станций, которые могут быть как ведущими, так и ведомыми.
      3. сообщение (message): Упорядоченные последовательности октет, предназначенные для передачи информации.

[ИСО/МЭК 2382-16.02.01. модифицировано]

4

ГОСТ Р МЭК 61784-3-3—2016

* + - 1. ложное срабатывание (nuisance trip): Ложное аварийное отключение, не причиняющее никакого вреда.

Примечание — В коммуникационных системах таких, как системы беспроводной передачи данных мо­ гут возникать внутренние аномальные1 ошибки, например, вследствие слишком большого количества повторных попыток при наличии помех.

* + - 1. 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, гарантируощем установленную полноту безопасности.

(МЭК 61508-4 и МЭК 62061. модифицировано)

* + - 1. уровень эффективности защиты; УЭЗ [performance level (PL)]: Дискретный уровень, применяющийся для определения способности связанных с безопасностью частей системы управле­ ния выполнять функцию безопасности в прогнозируемых условиях.

(ИСО 13849-1]

* + - 1. защитное сверхнизкое напряжение (protective extra-low-voitage. PELV): Электрическая цепь, в которой значение напряжения не может превышать среднеквадратичное значение переменного напряжения в 30 8. пиковое напряжение 42.4 В или постоянное напряжение 60 В при нормальных усло­ виях 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)

* + - 1. избыточность (redundancy): Существование более одного средства выполнения необхо­ димой 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]

* + - 1. надежность (reliability): Вероятность того, что автоматизированная система может выпол­ нять требующуюся функцию в заданных условиях на протяжении заданного промежутка времени (**1** .12).

Примечания

1. Принято считать, что автоматизированная система е состоянии выполнять данную требующуюся функцию 8 начале заданного промежутка времени.
2. Понятие «надежности» также «пользуются для обозначения показателя надежности, измеряемого данной

вероятностью.

1. На протяжении среднего времени между отказами (MTBF) или среднего времени до отказа (MTTF) вероят­ ность того, что автоматизированная система выполнит требующуюся функцию — уменьшается.
2. Надежность отличается от готовности.

[МЭК 62059-11. модифицировано]

* + - 1. 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)

* + - 1. коммуникационный уровень безопасности, КУБ (safety communication layer, SCL): Уро­ вень коммуникации, включающий все необходимые меры для обеспечения безопасной передачи ин­ формации в соответствии с трвбосаниями МЭК 61508.
      2. безопасное соединение (safety connection): Соединение, которое применяет протокол безопасности для транзакций коммуникаций.
      3. данные безопасности (safety data): Данные передаваемые через сеть безопасности, используя протокол безопасности.

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

* + - 1. устройство безопасности (safety device): Устройство, спроектированное в соответствии с МЭК 61508 и реализующее профиль коммуникации, удовлетворяющий требованиям функциональной безопасности.

5

ГОСТ Р МЭК 61784-3.3—2016

* + - 1. безопасное сверхнизкое напряжение (safety extra-low-voltage. SELV)SELV): Электриче­ ская цепь, е которой значение напряжения не может превышать среднеквадратичное значение пере­ менного напряжения в 30 В. пиювое напряжение 42.4 В или постоянное напряжение 60 8 при нормаль­ ных условиях и одиночном сбое, включая короткое замыкание на землю в других цепях.

Примечание — Цепь SELV не подсоединена к защитному заземлению.

[МЭК 61131-2)

* + - 1. функция безопасности (safety function): Функция, реализуемая Э/Э/ЛЭ (электрической, электронной, программируемой электронной) системой, связанной с безопасностью, или другими ме­ рами по снижению риска, предназначенная для достижения или поддержания безопасного состояния управляемого оборудования поотношению к конкретному опасному событию.

Примечание — В МЭК 61506-4 таков же определение, но дополнено примером и примечанием.

(МЭК 61508-4:2010. модифицировано]

* + - 1. время реакции функции безопасности (safety function response time): Наихудшее время между после срабатыванием датчика системы безопасности, подключенного к полевой шине, и дости­ жением соответствующего безопасного состояния с помощью необходимого исполнительного устройст­ ва этой системы безопасности гри наличии ошибок или отказов в канале функции безопасности.

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

* + - 1. 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 61506-4:2010. 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 ло Э/Э/ПЭ системам, связанным с безопасностью.
3. Уровень полноты безопасности (УПБ) не является свойством системы, подсистемы, элемента или компо­ нента. Правильная интерпретация фразы «УПБ системы, связанной с безопасностью, равен *п\** (где л = 1.2.3 или 4) означает: система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до значения, равного *п.*

(МЭК 61508-4:2010]

* + - 1. мера безопасности (safety measure): Средство управления возможными ошибками ком­ муникаций. спроектированное *v* 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 сними меры безопасности подробно рассмотрена в МЭК61764-3:2010. 5.3 и 5.4.
   * + 1. приложение, связанное с безопасностью (safety-related application): Программы, спро­ ектированные в соответствии с МЭК 61508 и удовлетворяющие требованиям УПБ приложения.
       2. система, связанная с безопасностью (safety-related system): Система, выполняющая функцию безопасности в соответствии с МЭК 61508.
       3. ведомое устройство (slave): Пассивный объект коммуникации, способный принимать

сообщения и отправлять их в ответ на другой объект коммуникации, который может быть ведомым или ведущим.

* + - 1. ложное аварийное отключение (spurious trip): Аварийное отключение, вызванное систе­ мой безопасности, без запроса эт процесса.
    1. CPF 3. Дополнительные термины и определения
       1. бит (bit): Закодированная двоичная информация без технического модуля.
       2. кодовое имя (codename): Уникальная идентификация одноранговых коммуникаций без­ опасности.
       3. конфигурация (configuration): Определение стандартных коммуникационных соединений и параметров коммуникаций длч объектов шины определенного приложения.

6

ГОСТ Р МЭК 61784-3-3—2016

Примечание — Конфигурацю для коммуникации безопасности включает в себя определение соединений безопасности и F-параметрое для объе<тов шины, связанной с безопасностью, предназначенной для определенного приложения, связанного с безопасностью.

* + - 1. 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 POU безопасности (режим-VI) или же защищен только передаваемой сигнатурой CRC (рвжимЛ/2).
   * + 1. инструмент-CPD (CPD-Tool): Специальная программа в обслуживающих компьютерах, соединенная с полевой шиной для целей конфигурирования, параметризации и диагностики опреде­ ленных полевых устройств.
       2. цикл (cycle): Интервал, за который повторно и непрерывно выполняется набор команд или действие.
       3. точка доступа к устэойству [device access point (DAP)): Элемент, использующийся для обращения к модулю ввода-вывода (Ю) устройства, как к объекту.

Примечание — Как правило, именуется головной станцией.

* + - 1. время подтверждения устройства. ВПУ [device acknowledgement time (DAT)]: Затрачен­ ное время F-устройства. начиная спринятия е точке доступа к устройству PDU безопасности, включаю­ щего новый порядковый номер, и заканчивая генерацией надлежащего ответного PDU безопасности и его возвращением в точку доступа к устройству.
      2. драйвер (driver): Программный модуль, применяющийся для абстрагирования аппарат­ ных средств от оставшегося прикладного программного обеспечения.
      3. отказоустойчивость. F [fail-safe (F)]: Способность системы, которая посредством адек­ ватных технических или организационных мер предотвращает опасные ситуации либо детерминирова­ но, либо снижая их риск до допустимого значения.
      4. отказоустойчивые значения. FV [fail-safe values (FV)]: Значения, которые выдаются вмес­ то значений процесса, когда функция безопасности установлена в отказоустойчивом состоянии.

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

* + - 1. 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 мажет быть не единственной возможностью для состояния отказоустойчивости.

* + - 1. F-устройство (F-Device): Пассивный одноранговый узел коммуникаций CP 3/RTE. спо­ собный выполнять протокол FSCP 3/1 и. как правило, вызываемый F-хостом для обмена данными.
      2. F-драйвер (F-Driver): Программное обеспечение, администрирующее PDU безопасности в F-хостах и F-устройствах в соответствии с спецификациями FSCP 3/1.
      3. F-хост (F-Host): Блок обработки данных, способный выполнять протокол FSCP 3/1 и об­ служивать черный канал.

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

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

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

* + - 1. F-ведомый (F-Slave): Пассивный одноранговый узел коммуникаций СР 3/1 или СР 3/2, способный выполнять протокол FSCP 3/1. как правило, вызываемый F-хостом для обмена данными.
      2. реакция на сбой (fa jit reaction): Индикация коммуникационной неисправности посредст­ вом установки битов сбоя в байте статуса и соответствующей автоматической безопасной реакции в этих компонентах.

7

ГОСТ Р МЭК 61784-3.3—2016

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-1/О-даннью должны быть установлены значения отказоустойчивости.

В F-вводе: В случае соммуникационных сбоев, обнаруженных на F-вводе. в байте статуса устанав­

ливаются биты сбоя.

* + - 1. функциональный блок, ФБ [function block (FB)J: Независимая часть программы, обла­ дающая определенным функционалом.
      2. время подтверждения хоста [host acknowledgement time (HAT)}: Затраченное время F-хоста. от принятия PDU безопасности, включающего определенный порядковый номер и до генера­ ции надлежащего ответного PDJ безопасности, включающего увеличенный порядковый номер, и его возвращения ведущему устройству/контроллеру ввода-вывода.
      3. контроллер ввода-вывода, Ю-контроллер (Ю-Controller): Активный объект коммуни­ каций. способный инициализировать и планировать коммуникационную деятельность CP 3/RTE дру­ гих объектов, которые могут быть Ю-контроллерами или Ю-устройстеами.

Примечание — В рамка< СР 3/1 эта задача соответствует классу 1 ведущего устройства.

* + - 1. устройство ввода-вывода, Ю-устройство (Ю-Device): Пассивный объект комму­ никаций. способный принимать сообщения и отправлять их в ответ другому объекту коммуникаций CP 3/RTE, который может быть Ю-контроллером или Ю-устройством.

Примечание — В рамка< СР 3/1 данная задача соответствует ведомому устройству.

* + - 1. модуль ввода-вывода, Ю-модуль (IO-Module): Подблок ввода-вывода, имеющий до­ ступный адрес и находящийся е Ю-устройстве.
      2. диспетчер ввода-вывода, Ю-диспетчер (Ю-Supervisor): Техническая станция, вклю­ ченная для считывания и записи данных сив Ю-устройство.

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

* + - 1. система ввода-вывода, Ю-система (Ю-System): Ю-контроллер и связанные с ним Ю-устройства.
      2. (параметр (iParameter): Индивидуальные или зависящие от технологии параметры F-устройства.

Примечание — Типичными i параметрами являются координаты зоны защиты лазерного сканнерэ.

* + - 1. inap-cepsep (iPai-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.
      2. ведущее устройство, класс 1 [master (class 1)]: Активный одноранговый узел коммуни­ каций СР 3/1. инициирующий ведомые устройства для обмена данными.
      3. значения процесса, ЗП [process values (PV)]: Входные и выходные данные (в PDU без­ опасности). которые требуются для управления автоматизированным процессом.
      4. квалификатор (Qualifier): Дополнительные указательные биты в значениях *процесса,*

демонстрирующие статус каждого индивидуального ввода.

* + - 1. общий ввод-выэод, общий I/O (shared I/O): Вводы и выводы в полевых устройствах, доступ к которым могут получать несколько контроллеров.

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

* + - 1. бит-лереключатвль (toggle bit): Один бит байта управления и байта статуса для син­ хронизации (виртуальных) текущих счетчиков как в F-хосте так и в F-устройстве.
      2. 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 портое компьютера и при­ меняется для обеспечения быстрых прямых соединений между компьютерами и полевыми устройствам!.

8

ГОСТ Р МЭК 61784-3-3—2016

* + - 1. режим-VI (V1-mode): Услуги и протокол FSCP 3/1 в соответствии с {48].
      2. режим-У2 (V2-mode) Услуги и протокол FSCP 3/1 в соответствии с настоящим стандартом.
      3. VLAN-тег (VLAN tag): Расширение в сообщениях Ethernet позволяющее определенным группам пользователей в больших сетях вести свою собственную виртуальную сеть посредством при­ оритетов и идентификаторов VLAN-ID. используя надлежащие коммутаторы и не оказывая влияния на другие группы пользователей и наоборот.
  1. Обозначения и сокращения
     1. Общие обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| Сокращение | Полное выражение | Источник |
| СР | Профиль коммуникаций | [МЭК 61784-1] |
| CPF | Семейство профилей коммуникации | [МЭК 61784-1] |
| CRC | Циклический контроль избыточности |  |
| OLL | 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/элекгронные/программируемые электронные | [МЭК 61508-4:2010] |
| FAL | Прикладной уроеень полевой шины (Fieldbus Application Layer) | (МЭК 61158-5] |
| FCS | Последовательность проверки кадра |  |
| ФБ | Функциональная безопасность |  |
| FSCP | Профиль коммуникации, удовлетворяющий требованиям функци­ ональной безопасности |  |
| HD | Расстояние Хэмминга |  |
| MTBF | Сродное время между отказами |  |
| MTTF | Среднее время до отказа |  |
| PDU | Блока данных протокола | [ИСО/МЭК 7498-1] |
| PELV | Защитное сверхнизкое напряжение |  |
| PFD | Средняя верояп-ость опасных отказов по запросу | [МЭК 61508-6:2010] |
| PFH | Средняя частота опасных отказов <h ') 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 полноть безопасности | [МЭК 61506-4:2010] |

9

ГОСТ Р МЭК 61784-3.3—2016

* + 1. CPF 3. Дополнительные термины и определения

SIS — Инструментальная система безопасности (safety instrumented systems)

|  |  |  |
| --- | --- | --- |
| Сокращение | Полное выражение | Источник |
| ПП | Прикладной гроцесс |  |
| API | Идентификатор прикладного процесса |  |
| СП | Связь приложений |  |
| ASE | Прикладной сервисный элемент |  |
| ASIC | Специализированная интеграгьная схема |  |
| П | Покрытие |  |
| СР 3/1 | Коммуникационный профиль общеизвестный как PROFI8US DP |  |
| СР 3/2 | Коммуникационный профиль общеизвестный как PROF1BUS РА |  |
| CP 3/RTE | Коммуникационный профиль общеизвестный как PROFtNET Ю |  |
| ЦП | Центральный процессор |  |
| КС | Коммуникационная связь |  |
| DAP | Точка доступе устройства |  |
| ВПУ | Время подтвфждения устройства |  |
| ДПУ | Децентрализеванное 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 СР 3/1 и СР 3/2) |  |
| GSDML | Язык разметки общего описания станции (Для устройств СР 3/RTE) |  |
| HAT | Время подтвфждения хоста |  |
| I/O | Ввод-вывод |  |
| СИД | Светоизлучающий диод |  |
| РА | Автоматизация процесса |  |
| PN 10 | PROF1NET Ю = С СР 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 | Универсальна 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] |

10

ГОСТ Р МЭК 61784-3-3—2016

* 1. 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 значе­ ние «0».

В настоящем стандарте любсе вычисление сигнатуры CRC. выдающее значение «0». вместо это­ го будет использовать значение «1».

В настоящем стандарте аббревиатура «СР З/RTE» включает в себя три коммуникационных про­ филя: СР 3/4. СР 3/5 и СР 3/6. СР З/RTE общеизвестен как PROFINET Ю.

1. Обзор FSCP 3/1 (PROFIsafe™)

СемействоЗкоммуникационных профилей (общеизвестное KaxPROFIBUS™. PROFINET™2\*)опре­ деляет 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 СР 3/1 и СР 3/2 определены в МЭК 61784-1. СР 3/4. СР 3/5 и СР 3/6 опре­ делены в МЭК 61784-2. Коммуникационный профиль, удовлетворяющий требованиям функциональ­ ной безопасности. FSCP 3/1 (PROFIBUS™. PROFINET™\*') семейства 3 коммуникационных профилей (CPF 3) основан на базовых профипях 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 супервизорам!!, такими как программирующие устройства, предназначены для це­ лей конфигурирования, параметризации, диагностики и технического обслуживания.

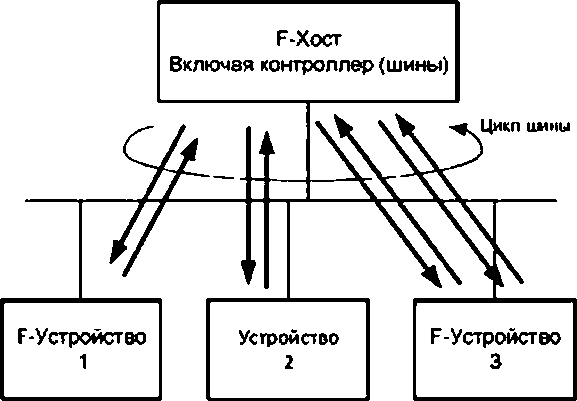
Для реализации FSCP 3/1 были выбраны следующие четыре метода:

* + - 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 Nutzerorgancsation e.V. (PNO). Данная информация приведена для удобства использования данного международного стандарта и не означает, что МЭК поддерживает мнения обладателя торговой марки или его про­ дукцию. Соответствие этому стандарту не требует использования наименований PROFlBUS™.PROFiNET™ или PROFIsafe™. Использование торговых марок PROFIBUS™. PROFINETT™ и PROFIsafe™ требует разрешения со стороны PNO.

11

ГОСТ Р МЭК 61784-3.3—2016



Устройство

Устройство ■ Устройство

2 ■ 3

1

ч . . **\_** *J*

*\*

Циклжеский доступ к Непериодический доступ к контроллеру контроллеру

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

Последовательная нумерация использует достаточно большой диапазон возможностей для защи­ ты от любой неисправности, вьэванной 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).

S - стандартное сообщения, включая PDU безопасности

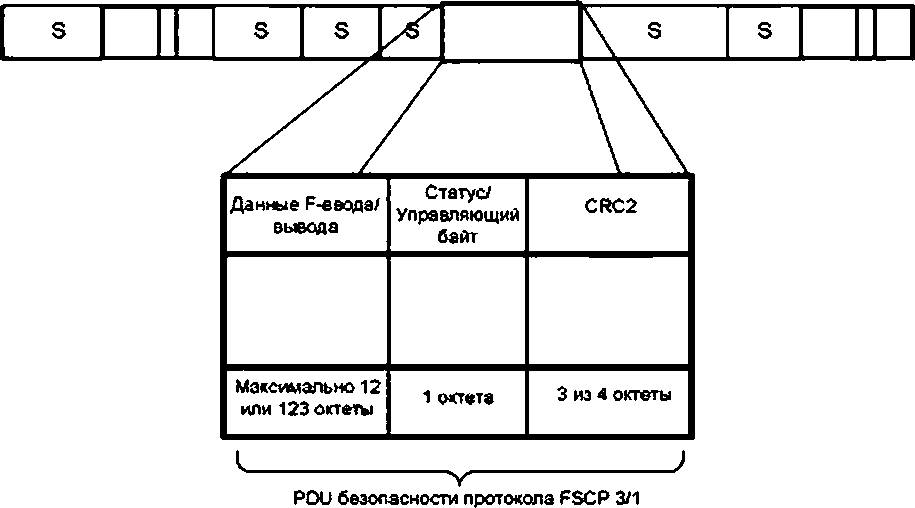


Рисунок 4 — Структура PDU безопасности FSCP 3/1

12

ГОСТ Р МЭК 61784-3-3—2016

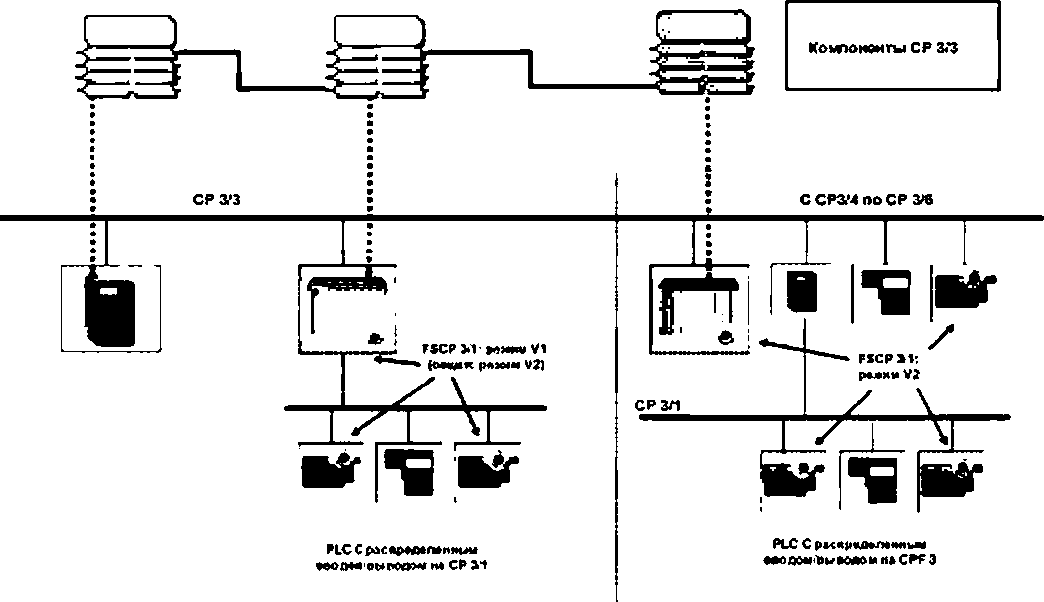
FSCP 3/1 предоставляет два режима эксплуатации: режим V1 и V2. И хотя средств режима V1 достаточно для передачи данных безопасности в сетях, использующих только СР 3/1. более «щедрые» возможности Ethernet/CP 3/RTE. такие как более широкое адресное пространство и компоненты пере­ ключателя буферизации,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

В то время как решения автоматизации с распределенными вводами-выводами получили широкое

признание в связи с использованием PROFIBUS (СР 3/1 и СР 3/2) и. основанной на Ethernet, промыш­ ленной PROFINET (СР 3/RTE), приложения безопасности по-прежнему полагались на второй уровень традиционных электрических методов или на специальные шины, тем самым ограничивая «бесшовную» инженерию и интероперабельности Кроме того, современные устройства безопасности, такие как ла­ зерные 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 подраздет 5.2 содержит функциональные требования для этой технологии. Четыре меры безопасности FSCP 3/1 перечислены в 5.3. Сетевые топологии в рамках СР 3/RTE и их пересечения с СР 3/1 и СР 3/2 упоминаются в 5.4. Далее в 5.5 следует небольшое введение в коммуни­ кационные связи и объекты стандарта полевых шин.

Для целей безопасности и эффективности список возможных типов данных полевых шин умень­ шен 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.



Уж» 1 ш Ужам1м Г\*СР 3.1

Рисунок 5 — Режимы коммуникаций безопасности

Раздел 7 начинается с обзора PDU безопасности (7.1), за которым следует описание машин со­ стояний в F-хосте и F-устройстее 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 форматок! из МЭК 61784-3:2010. приложение D. подраздел 7.3 демонстрирует

13

ГОСТ Р МЭК 61784-3.3—2016

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 тараметрах, зави­ сящих 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 демонстриру­ ет. 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 тараметризации перечислены в 8.6. Аспекты скоростей реакций, ру­ ководства 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 до­ полнительными руководствами FSCP 3/1 ло электрической безопасности и оценке ((44). [45]).

1. Общие положения
   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].

* 1. Функциональные требования безопасности

Следующие требования применяются к разработке технологии FSCP 3/1.

1. Коммуникации безопасности и стандартные коммуникации должны быть независимы. Тем не ме­ нее. стандартные устройства и устройства безопасности должны иметь возможность использовать один коммуникационный канал.
2. Коммуникации безопасности должны подходить для уровня полноты безопасности УПБЗ (см. МЭК 61508). категории управления 4 (см EN 954-1 [25]). и PLe (см. ИСО 13849-1).
3. Коммуникация безопасности должна использовать коммуникационную систему, состоящую из одного канала. Дополнительно, но не обязательно, для повышения готовности можно применять избы­ точность.
4. Реализация протокола передачи данных безопасности должна ограничиваться оконечными устройствами коммуникации (F-хост или F-ЦП — F-yc тронет во и/или F-1/О-модуль).
5. Между F-устройством и его F-хостом всегда должна существовать коммуникационная связь 1:1.
6. Длительности породами данных должны контролироваться.

д) 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.

1. Оборудование для передачи данных, такое как. контроллеры. ASIC схемы, каналы, соединитель­ ные 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 стандарт­ ного протокола).
   1. Коммуникации безопасности не должны уменьшать разрешенное число устройств. 8 случае при­ ложений СР 3/2 во время отображения можно столкнуться с ограничениями, связанными с ограничения­ ми сообщений (см. СР 3/2 в МЭ< 61784-1).

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

* 1. Меры безопасности

Меры безопасности, упомянутые в таблице 1 для управления возможными ошибками передачи дан­ ных. являются одним из значимых компонентов профиля FSCP 3/1. Подборка обычных мер безопаснос­ ти. перечисленных в МЭК 6178^-3:2010, 5.5 и показанная в таблице 1 необходима для FSCP 3/1.

Меры безопасности должны обрабатываться и контролироваться одним блоком безопасности.

14

ГОСТ Р МЭК 61784-3-3—2016

Таблица 1 — Меры, примененные для преодоления основных ошибок

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ошибка коммуникаций | Меры бмоттасиости | | | |
| Порядковый (вирту­ альный) номера\*1 | Перерыв с подтверж­ дением получения\*1 | Кодовое имя для отправителя и полу­ чателя\*1 | Проверка данных на непротиворечивость\*1 |
| 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 |  |  |  |

41 Экземпляр «номера последовательности» из МЭК 61784-3.

Ь| Экземпляр «временного ожидания» и «сообщения обратной связи» из МЭК 61784-3.

с> Экземпляр «аутентификации соединения» из МЭК 61784-3.

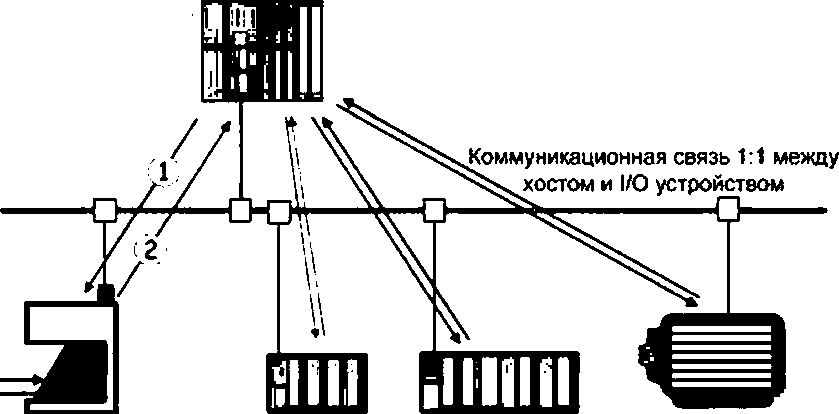
Экземпляр «обеспечение целостности данных» из МЭК 61784-3.

* 1. Структура коммуникационного уровня безопасности
     1. Принцип коммуникацпй 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.

f \*x oc t FSCP 3/1 (F-хост - F-устройство)

Лазерный сканнер Стандартный-I/O F-l/O -1. Носитель со встроенной И\* безопасностью

Рисунок 6 — Стандартная система передачи CPF 3

15

ГОСТ Р МЭК 61784-3.3—2016

Стандартная система передачи включает е 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 коммуника­ ционные 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 стан­ дартная система передачи может пропускать, или же для того, чтобы поддерживать вероятность оста­ точной ошибки (сбоя) на допустимом уровне. Такие ошибки включают:

* + - произвольные неисправности, например, вызванные влиянием ЭМП на канал передачи данных:
* отказы У сбои стандартных аппаратных средств:
* систематические ошибки компонентов стандартных аппаратных средств и программного обес­ печения.

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

Например, диагностические данные

N г

Логическая обработка да>\*м>х безопасности

Урове-ь

***V***

*i* м

|  |  |  |
| --- | --- | --- |
| Стандартный | • | ввод безопасности |
| ооод/оыоод | Ууоье«о |
|  | безопасности |
| 7 | 7 I |
| 2 | 2 *\* | |
| 1 | | *: 1*^ | |

|  |  |
| --- | --- |
| Вывод безопасности | |
| Уровень  безипаемтхли | |
| ***А*** *7* | |
| *Г 2* | |
|  |  |

|  |  |  |
| --- | --- | --- |
| Стандартная логическая | | |
| операция | | |
| 7 | | |
| 2 | | |
|  | 1 |  |

1

# 5 5 5

Обозначения

* «черный канал», схемы ASC. линии, коммутаторы и т.п. не являются компонентами ванными для безопасности

**ЯШ** • функции, не связанные с безопасностью, напри клер, диагностические функции.

I синхронизацию сторожевых таймеров, определение последовательности, сигнатуры и т.п;

TSCP3/1 протокол, саязанмяй с безопасностью включает е себя: адресатам,

1 • функции безопасною I/O и безопасного погического контроллера вачо-ые для

**J** безопасности, но от не являются частью профиля безопасности

Рисунок 7 — Архитектура уровня безопасности

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

* + 1. 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.

16

ГОСТ Р МЭК 61784\*3-3—2016

Открытый канал для TCP/UDP/IP

|  |  |  |  |
| --- | --- | --- | --- |
| ИТ Услуги  -HTTP.   * SNMP. I   •ОНСР | Приложения FSCP 3/1  IP Параметр. 1 Да»\*ые реального | ГГдиалюстщаитд, ] . времени 1 | | |
| TCP или U DP | | £2 | «3 |
| IP | |

* Конфигурирование и параметризация устройства
* Вьеод считываемых данных диагностики
  + - * Перед\*-® взаимосвязей
* Переговоры о коммуникационном канале для данных пользователя

Ethernet

**Канал реального времени RT**

- Высоко аффективная передача циклических данных.

* Сигналы управляемые событиями

Канал реального времени IRT

* высоко-эффективная переда\*-® циклических

данных а иэохрогеюм режиме {< 1мс)

ASIC коммутатора реального времени (налицо не обязательно)

* Джиттер <1цв.
* Требуется ASIC

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 вы­ ключению всей сети в целом. Тем не менее, усилия по прокладке проводов могут не стоить результата.

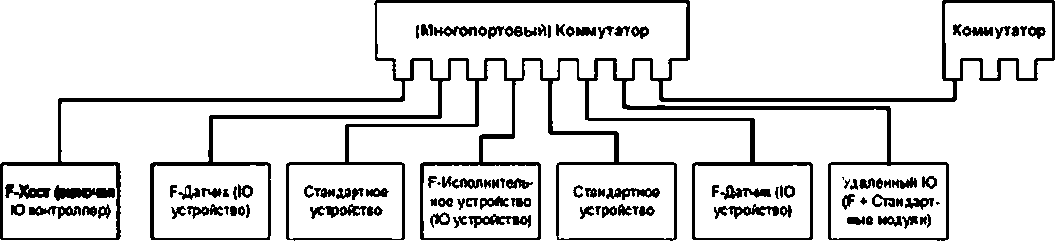


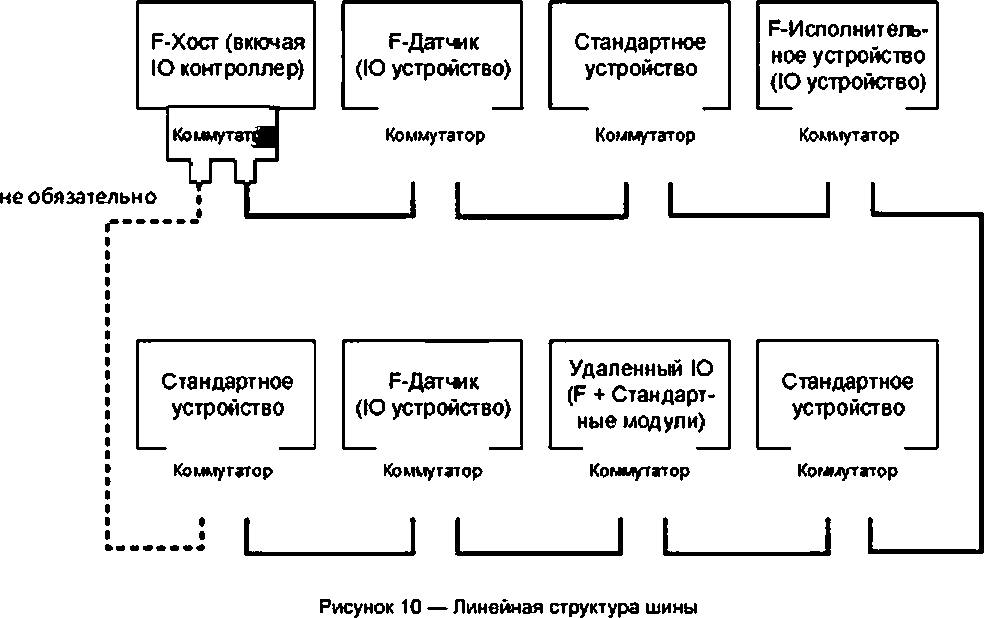
Рисунок 9 —Структура шины многоканального переключателя

CP 3/RTE предоставляет альтернативное решение с помощью коммутатора на база ASIC, где ка­ ждое устройство может подключить к своему коммуникационному интерфейсу. Таким образом, стано­ вится возможной линейная тополо-'ия во многом схожая с СР 3/1. Чтобы избежать отключения системы в случае отказывающего устройства, настоятельно рекомендуется кольцевая структура (рисунок 10). Однако в данном случае существует некоторые ограничения:

* + хотя бы один участник в кольце (на рисунке 10 эго F-хост) должен осуществлять управление ре­ зервированием (избыточностью) для обнаружения любого прерывания и для реорганизации передачи данных е 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.

17

ГОСТ Р МЭК 61784-3.3—2016



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 б). Задача по пе­ ренаправлению сообщений на уровне IP-Адреса (рисунок 11) лежит на маршрутизаторах (уровня 3 ВОС). Таким образом, маршрутизаторы являются естественными границами для CP 3/RTE систем. Следую­ щие ограничения применимы к :SCP 3/1:

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

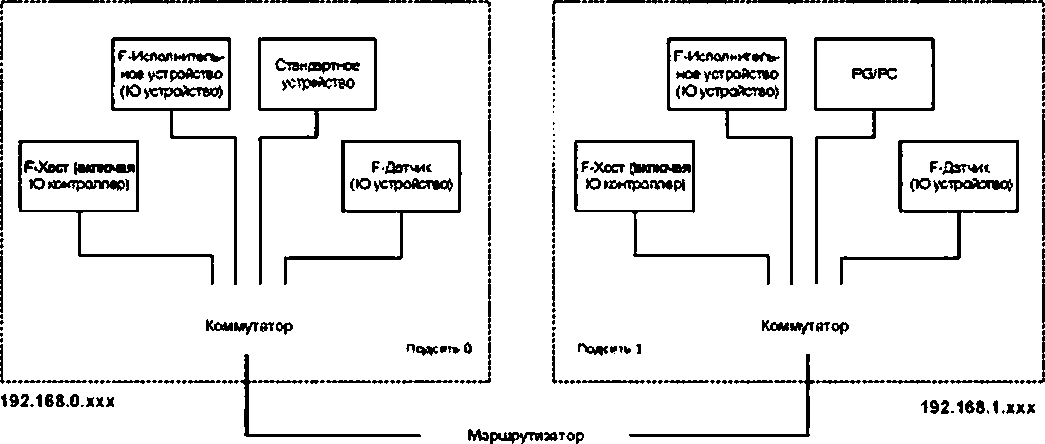


Рисунок 11 — Пересечение границ сети с маршрутизаторами

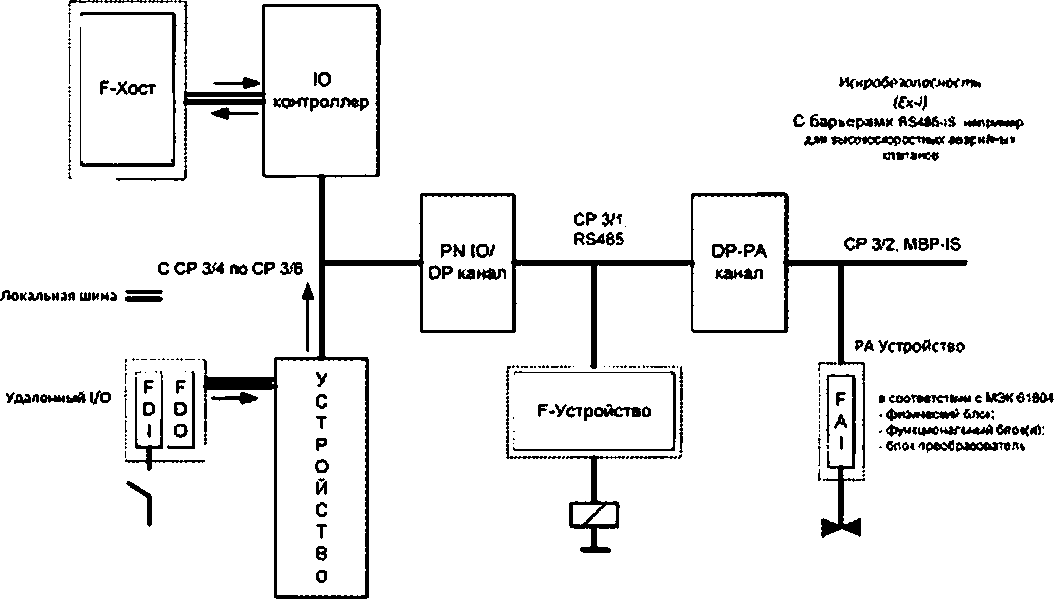
18

ГОСТ Р МЭК 61784-3-3—2016

В отличив от типичной конфигурации системы полевых шин. на рисунке 12 показана возможная структура шины, где профиль безопасности достаточно сильно затрагивает индивидуальные блоки. Например, стандартный удаленный Ю может включать в себя F-модуль для присоединения кнопки экс­ тренной 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 Ю) в Ю устройство и через возможно другую объединительную плату е>одит в финальный F-модуль. Уровень безопасности реализуется в пределах этих точек коммуникации.

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

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



Обозначения

M6P-IS RS46S RS465-IS F-OI

F-0O

F-AI

РА

передача данных для взрывоопасных областей: высокоскоростная передача данных;

специальная RS46S для взрывоопасных областей:

цифровой ввод безотвсности: цифровой вывод безопасности; аналоговый ввод безвпаспости:

устройство в соответствии с моделью устройства автоматизации процесса (МЭК 61604).

Рисунок 12— Полные пути передачи данных безопасности

* 1. Связи с FAL (и DLL, Phi)
     1. Модель устройства

CP 3/RTE также, как и модегь устройства СР 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 представ­ ления физических I/O устройства. По сравнению с СР 3/1, СР 3/RTE предоставляет на один иерархичес­ кий уровень больше: подслоты.

19

ГОСТ Р МЭК 61784-3.3—2016

I

ЭлементыЮДамюГе; •\ 1

AS6 *г.*

##### I

Кои текст

• •

. ... **. ..** с

*1*! 1

Диагност и Аварийная

1 !'

1

##### : 1 —

'1J

t

1

Г сигнали.м**-**ы**-**-м**-** -*i* : *U* С

Запись | г

##### -данных

*0 1***.**

• . ■. *•* t Jl

###### *ПоФспот Подлогом ПоПслотПопоют\** Ло0*\*О*П*1*оПоют*П*\** номер 0 J . QxSfff номере t. \*$rrr номер 0 пат

*Спот номер 0 Спот 1 , Спот (Шее*

С СР 3/4 no СР 3/6 АР (API \* 0)

Рисунок 13 — Модель устройства

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

* + 1. 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 Ю-устройства и возможных связей с Ю-контроллерами.

Ю-контроллер использует кадр «Connect» («Соединить»), отправляемый в специальном CP 3/RTE сообщении, для инициализации установления СП во время запуска системы. Таким образом, он пере­ дает 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.

Ю-устройство проверяет голученные данные и устанавливает требующиеся связи КС. Доклады

* возможных возникающих ошибках отправляются IO-контроллеру. Обмен данными начинается с по­ ложительного подтверждения ответа устройства на запрос «Соединить». Запрещена установка двух FSCP 3/1 СП связей от разных ПП с одним подслотом.

20

ГОСТ Р МЭК 61784\*3-3—2016

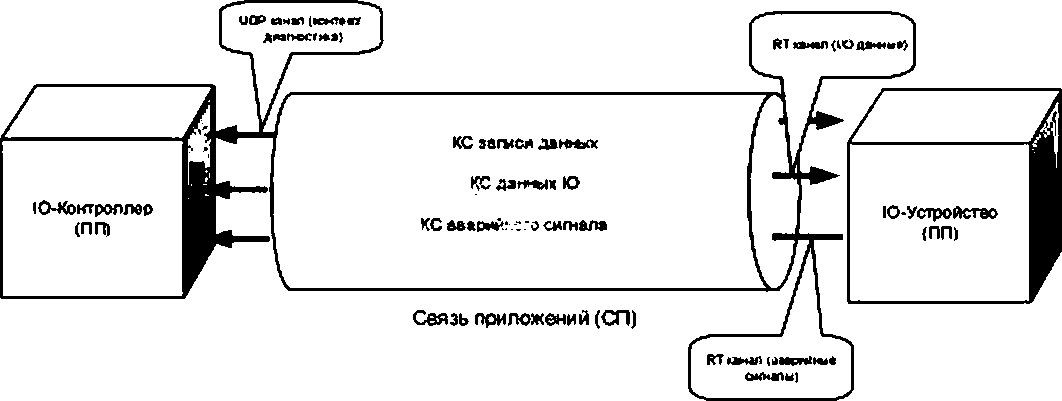
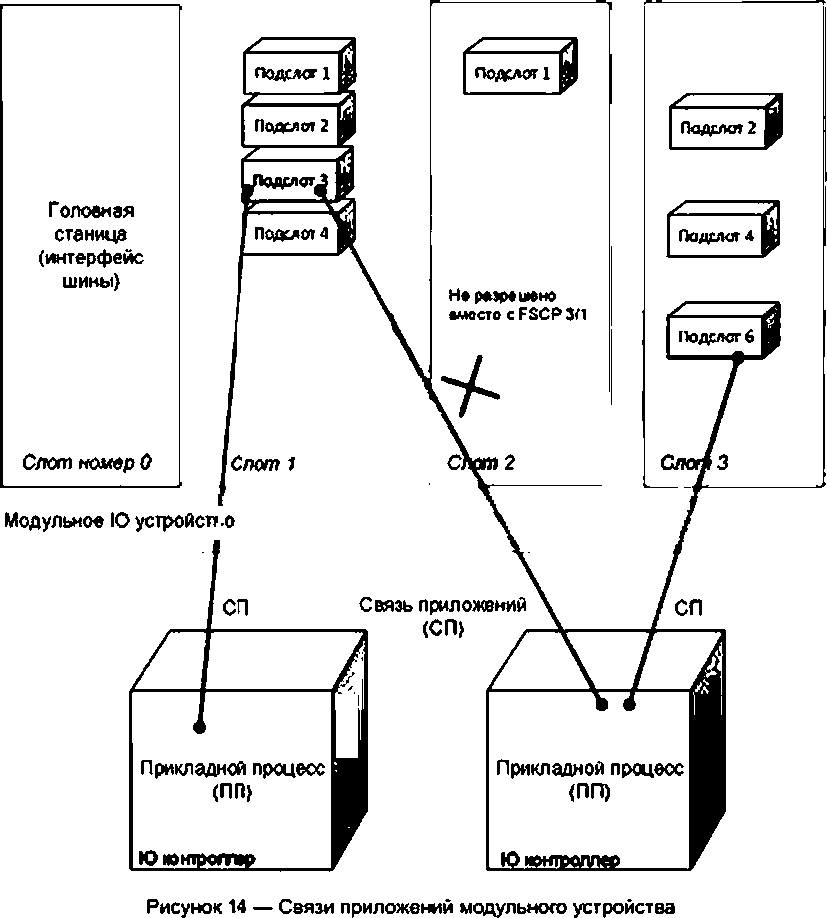


Рисунок 15 — Связи приложений и коммуникаций (СП/КС)

21

ГОСТ Р МЭК 61784-3.3—2016

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

* + 1. 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 — ААААААААдАААААЬ:.

SFD —

OA —

SA -

Тег VLAN —

Тип Elher •—

>D Кадра —

KDPS —

IOCS —

Цикл —

Статус данных —

начальный разделитель садрэ: АЬЬ. адрес назначения {6 ocltetts),

адрес источника (б ocIteTls):

указывает на определенный приоритет, не обязателен.:

тип кадра Е IherneH.; 8892h для с CP ЗМ4 по CP 3//6 (2 октета); идентификация кадра (типы сообщений с CP 3/4 ло СР З/б);;

статус НО п«стаещика:: лороший/ппохон и местололожеииедоо4/(ие обязвтельноМОвО):: статус потребителя НО: хороший№тпокой и иестополежениедооб//(Не обязатепыио//080):: счетчик цикла (2 октета):: величина., кратная 31,,25ps,:

информацит об избыточности., соответствии., состоянии устройства и т..л..;:

У r.fKtyf — гтятуг <1 л<т«г): ИГЛ»ДЯ \*ППЬ\* ;

FCS — Э2-битовыйСЯС (l04C110B7h)..

\*) при VLAN-Tere минимум данных для передачи составляет 36 октетов.

Рисунок 16 — Формат сообщения

* + 1. 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

|  |  |  |  |
| --- | --- | --- | --- |
| Незвание типа данных | Перевод | Число октет | Используется е |
| Integer8 | 6-бкговый целочисленный | 1 |  |
| 1nteger16 | 16-битовый целочисленный | 2 | Режимы VI и V2 |
| Inleger32 | 32-битоаый целочисленный | 4 | V2-режим |
| 1п(едег64 | 64-битовый целочисленный | 8 |  |
| Unsigned8 (used as Ms} | в-бутовый без знака (используется в качестве бит) | 1 | Режимы VI и V2 |

22

ГОСТ Р МЭК 61784-3-3—2016

*Окончание таблицы 2*

|  |  |  |  |
| --- | --- | --- | --- |
| Нанаимо типа данных | Перевод | Число октет | Используется а |
| Unsigned 16 (used as bits) | 16-битовый без знака (используется в качестве бит) | 2 | РежимЛ/2 |
| Unsigned32 (used as bits) | 32-битовый без знака (используется в качестве бит) | 4 | РежимЛ/2 |
| Unsigned 16 | 16-битовый без знака | 2 |  |
| Unsigned32 | 32-битовый без знака | 4 |  |
| Unsigned64 | 64-битовый без знака | 8 |  |
| Floal32 | 32-битовый с плавающей точкой | 4 | Режимы VI и V2 |
| Fk>al64 | 64-битовый с плавающей точкой | 8 |  |
| Date | Дата |  |  |
| TimeOfDay with date indication | Время туток с индикацией даты |  |  |
| TimeOfDay without date indication | Время туток без индикации данных |  |  |
| TimeDifference with date indication | Разность времени с индикацией даты |  |  |
| TimeDifference without date indication | Разность времени без индикации даты |  |  |
| NetworkTime | Сетееоэ время |  |  |
| NehvorkTimeDifference | Разность сетевого времени |  |  |
| Visible String | Видимая строка | 1.2.3... |  |
| UnsignedS+UnsignedB | 8-бигоеый без знака+8-битовый без знака | 2 | Режимы VI и V2 |
| Float32+Unsigned8 (enumerated) | 32-бигсвый с плавающей точсой+8-биговый без знака (перечислимый) | 5 | Режимы VI и V2 |
| F\_MessageTraiter4Byte | 4-байтсеое окончание Р\_сообщения | 4 | Режимы VI и V2 |
| F\_MessageTraiter5Byte | 5-байтсеое окончание Р\_сообщения | 5 | РежимЛ/2 |

Типы данных для применения е режиме V2 ограничиваются следующими типами: 8-битовый без знака. 16-битовый без знака. 32-бмтовый без знака. 16-битоеый целочисленный. 32-битоеый целочис­ ленный. 32-битовый с плавающей точкой и совмещенный тип данных 32-битовый с плавающей точ- кой+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 сравне­ нии с Булевым типом.

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

1. Услуги коммуникационного уровня безопасности
   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-x oc t 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 *кодовый именем* (один из F-параметров).

Все стандартное коммуникационное оборудование CPF 3 между F-драйверами принадлежит чер­

ному каналу. Стрелочки на рисунке 17 указывают на циклическую передачу данных между F-драйве­ рами: адденда безопасности (статус или контрольный байт и CRC2) передается от F-ввода F-хосту в дополнении к данным F-ввода. 3 качестве подтверждения. F-ввод всего лишь принимает адденду безопасности (код безопасности). 3 соответствии с этим. F-вывод принимает адденду безопасности в дополнении к данным F-вывода. и применяет ее для подтверждения.

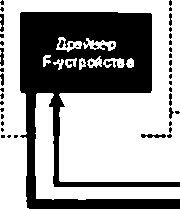
Управление блоками PDU безопасности и F-параметризация являются задачами F-драйверое в F-хосте и F-устройствах. На рисунке 18 показан F-интерфейс. пользователя находящийся на уровне программы управления безопасностью.

23

ГОСТ Р МЭК 61784-3.3—2016

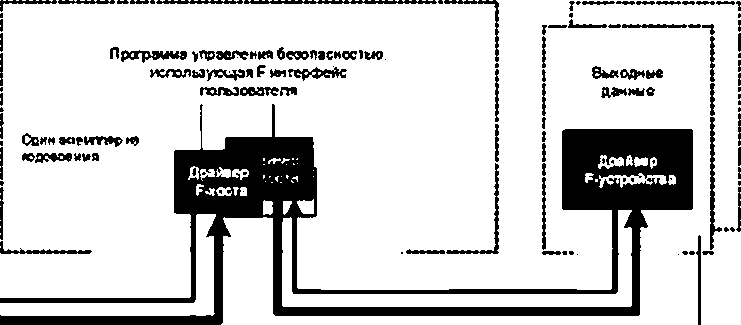
F-ввод

ВхсаныяАатьс



F-I/0 данные

F-x oc t F-вьвад



*Входные условия для инкапсулированной системы передачи данных FSCP 3/1:*

+

КОД

безопасности

код

безопасности

* + - Только авториэироважый доступ.
    - Механизмы обнаружения ошибок передачи дан-ых не обязательно являются известями и четко определенными
    - Достаточен уровень готовности

Дополнительные средства в устройстве для достижения требующегося УПБ Например, для УП63 »то второй микропроцессор и устройства сравнения

Ризунок 17 — Структура коммуникаций FSCP 3/1

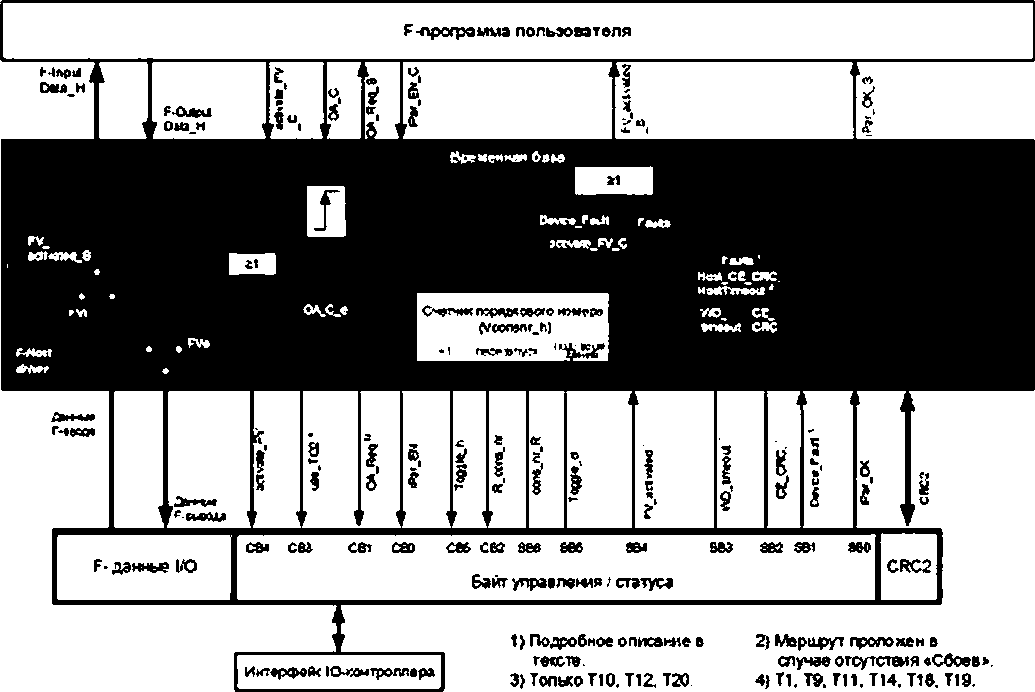


Рисунок 18 — F-интерфейс пользователя для экземпляров драйвера F-хоста

24

ГОСТ Р МЭК 61784-3-3—2016

Программисту доступно несколько переменных для того, чтобы манипулировать процессами без­ опасности в соответствии со стандартами. Эти переменные имеют похожие имена, как правило, рас­ ширенные за счет добавления индекса «\_С» (Control, т. е. управление) или «\_S» (Status, т. е. статус), на подобии соответствующих им битоэ в байтах статуса и управления, но они также могут нести некоторую логику управления в F-драйеере. 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 С*

*FV* activated S

*iPar EN С*

*iPar OK S*

*OA\_C*

(Подтверждение оператора)

*OA\_Req\_S*

*Значения ввода*

Каждая программа управления безопасностью, которая работает с соответствую­ щим F-устройством должна использовать эту переменную (тип: двоичная). В случае устройств вводе (например, датчиков) данная переменная, установленная в значе­ ние «1» заставляет драйвер доставлять отказоустойчивые значения («0») F-програм- ме управления. В случае устройств вывода (например, исполнительных устройств) эта переменная, установленная в значение «1» вынуждает драйвер отправлять от­ казоустойчивые значения («О») устройству и установить бит 4 в значение «1». Кон­ цепция безопасности устройства вывода определяет тип информации для этих двух случаев, которая должна использоваться для достижения безопасного состояния.

Каждая программа управления безопасностью, которая работает с соответствую­ щим F-устройством должна использовать эту переменную (тип: двоичная). В слу­ чае устройств ввода данная переменная своим значением «1» указывает на то. что драйвер доставляет отказоустойчивые значения («0») программе F-хоста для каждо­ го входного значения. Подсказка: чтобы позволить индивидуальную обработку каж­ дого 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» (поведе­ ние по умолчанию) или же определенное, зависящее от устройства F-вывода значе­ ние. 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.

Данная переменная (тип: двоичная), установленная в значение «1» позволяет F про­ грамме управления переключать F-устройство в режим, в ходе которого, оно будет принимать inape метры. Она непосредственно связана с сигналом управления «iPar\_ EN» ( бит 0 байга управления) и не влияет на состояния F-хоста. При необходимо­ сти. переменная «activate\_FV\_C» должны быть также установлена в значение «1». Данная переменная (тип: двоичная) указывает F-программе управления на оконча­ ние тара метризации и готовность восстановить обмен данными F-l/O (рисунок 41). Если бит 1 статуса «Сбой устройства» не установлен, она должна обновляться зна­

чением «iPar\_OK» в переходах Т4, Т8 иТ17 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 пе­ реустановлены.

Каждая F программа управления должна применять эту переменную (тип: двоичная). Изменяя значение этой переменной на «1» пользователь получает возможность вос­ становить функцию безопасности после реакции на сбой (зависит от контура отказо­ устойчивого управления) посредством пользовательской программы F-хоста.

Данная переменная (тип: двоичная) указывает на наличие запроса на подтверждение перед возобновлением функции безопасности. 8 том случае, если драйвер F-хоста или F-устройство обнаруживает коммуникационную ошибку или сбой F-устройстеа. то будут активированы отказоустойчивые значения. Драйвер F-устройстеа затем, как только сбой/ошибка была устранена и возможно подтверждение оператора, уста­ навливает переменную OA\_Req\_S в (’Г). По завершении подтверждения (ОА\_С = "Г) драйвер F-устройстеа обнуляет переменную запроса OA\_Req\_S ("О").

PVi Значения ввода процесса (\*-F-lnput\_Data\_D. см. рисунок 19).

FVi Отказоустойчивые значения ввода, используемые вместо PVi для F\*lnput\_Data\_D (см. рисунок 19).

25

ГОСТ Р МЭК 61784-3.3—2016

*Значения вывода* PVo Значения вывода процесса {—F-Output\_Data\_D).

FVo Отказоустойчивые значения вывода (=0). используются вместо PVo для FOulput\_Dat3\_D.

* 1. Услуги F-устройств

На рисунке 19 подробно троиллюстрирован 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, по­ лучает F-параметры и передает их драйверу F-устройства. Сам драйвер, после проверки некоторых из F-параметрое. передает F-параметры «F\_iPar\_CRC» и «F.SIL» части конкретного приложения устрой­ ства. 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 пе­ редаются посредством связи коммуникаций данных Ю 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) СВО, СВ1. СВ2. СВЗ. СВ4. и С85. 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 но­ вого порядкового номера. В ответ на это для передачи подготавливаются блоки PDU безопасности. Они содержат байты статуса вместе с битами статуса (Status Bits) SBO ...S85. Один из них пропускается, драйвер генерирует некоторые из них. а некоторые поступают из прикладного интерфейса, подверга­ ясь манипуляциям драйвера пеэед входом в PDU безопасности. Oriver\_Fault устанавливается в случае внутреннего сбоя драйвера.

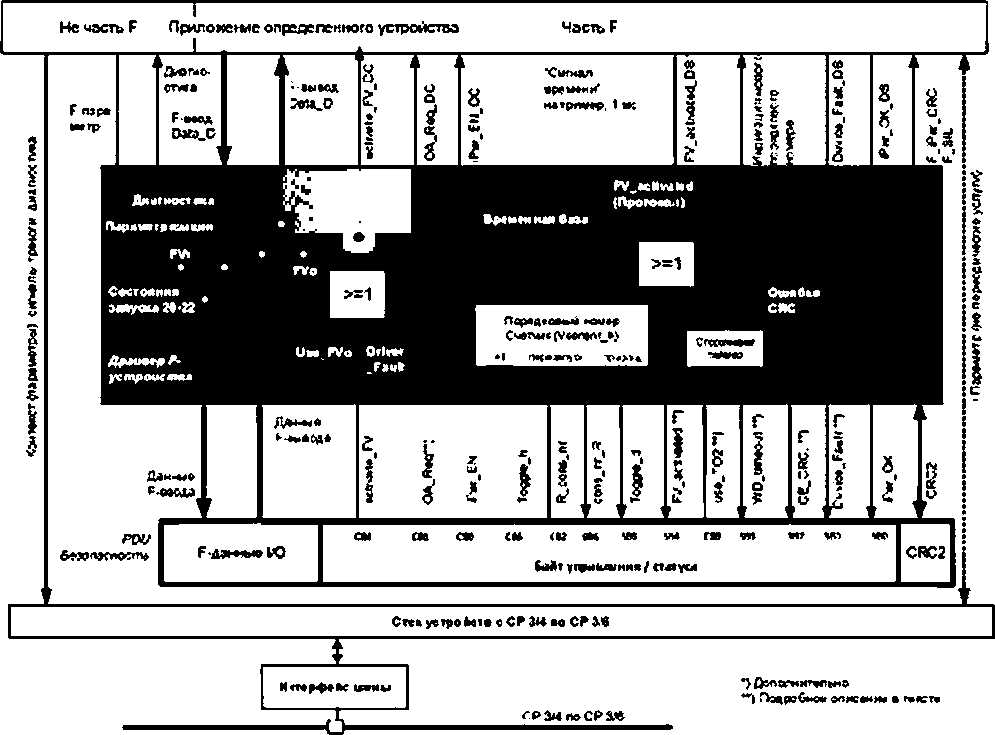


Рисунок 19 — Интерфейсы драйвера F-устройсгва

26

ГОСТ Р МЭК 61784-3-3—2016

Счетчик порядкового номера увеличивается (х+1), когда «Toggte\_h» меняет свое состояние

<0—\*1; 1—0). Значение R\_cons\_nr = «1» обнулит счетчик («0»). Приращение счетчика изменит состоя­ ние «Toggle\_d» {0—1; 1—0). CRC гроверка выполняется при каждом полученном и отправленном PDU безопасности (CRC2).

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

*activate FV DC*

*FV activated DS*

*OA\_Req\_DC*

*iPar EN DC*

*iPar OK DS*

*Device\_Fault\_DS*

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.

В случае устройств ввода эта переменная указывает своим значени­ ем «1» на то. что приложение устройства доставляет отказоустойчи­ вые значения («0») драйверу FSCP 3/1 для каждого значения ввода. Подсказка: Для того, чтобы обрабатывать каждый вывод индиви­ дуально к данным ввода могут быть добавлены специальные ука­ зательные биты. В случае устройств вывода ярлык указывает с по­ мощью значения «1» на то. что каждый вывод установлен в отказоу­ стойчивые значения. Для случаев совмещения устройств ввода и вы­ вода, данная переменная (тип: двоичная) указывает, с помощью значения «1» на то. что приложение устройства доставляет отказоу­ стойчивые значения («0») драйверу FSCP 3/1 для каждого значения ввода, а каждый вывод установлен в отказоустойчивые значения.

Приложение F-устройства должно использовать эту. не связанную с безопасностью, переменную для того, чтобы локально указывать на присутствие запроса на подтверждение оператора (ОА\_С в F-xoc- те), как правило, посредством светодиода. Реализация этой пере­ менной является не обязательным для F-устройств.

Данная переменная, в случае, если она имеет значение «1». указы­ вает на наличие запроса на параметризацию (F-устройство нужда­ ется в новых (параметрах).

Данная переменная, в случае, если она имеет значение «1». указы­ вает на то, что F-устройство (его конкретное приложение устройст­ ва) обладает новыми назначенными значениями (параметров.

Сбой, распознанный конкретным приложением устройства.

* 1. Диагностика
     1. Генерация сигнализации безопасности

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

В случае коммуникационных эщибок система способна вовремя и безопасным способом реагиро­ вать. например, используя информацию в байте статуса.

* + 1. 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 Ю-контроллеру. Использование каждого стандартного средства диагностики CP 3/RTE является возможным, предпоч­ тительнее диагностика-связанная-с-каналом. В таблице кодирования, в поле «ChannelErrorType» (Тип ОшибкиКанала) хранится место для FSCP 3/1. В таблице 3 показаны различные типы диагностичес­ кой информации протокольного урзвня FSCP 3/1 в F-устройствах.

27

ГОСТ Р МЭК 61784-3.3—2016

Таблица 3 — Сообщения диап-остики 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 | Врэмя сторожевого таймера безопасности рвано 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 | Усановлвна неверная версия F-параметра |
| 0x0047 | 71 | Сбой CRC1 |
| 0x0048 | 72 | Диагностическая информация, зависящая от устройства, см. руководство |
| 0x0049 | 73 | Врэмя сторожевого таймера для сохранения ^параметра превышено |
| 0х004А | 74 | Врэмя сторожевого таймера для восстановления {параметра превышено |
| 0x004В | 75 | Противоречивые {параметры (ошибка iParCRC) |
| 0х0О4С | 76 | Заоеэервироаано: не используйте номера, не оценивайте номера |
| 0x0040 | 77 | Заоеэереироеано: не используйте номера, не оценивайте номера |
| Ох0О4Е | 78 | Зарезервировано: не используйте номера, не оценивайте номера |
| 0X0O4F | 79 | Зарезервировано: не используйте номера, не оценивайте номера |

F-устройстеа, использующие механизм iPar-Server для хранения и извлечения шараметров в рам- ках F-хоста или подсистемы, ко'орой он управляет, с помощью дополнительных раздельных кодировок могут создавать отчеты со специализированной диагностической информацией. Настоятельно реко­ мендуется. в случае F-устройсте, использовать эти типы в диагностических сообщениях. Тем не менее, диагностические сообщения могут также переносить итоговую информацию в нескольких индивидуаль­ ных случаях.

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

1. Протокол коммуникационного уровня безопасности
   1. Формат PDU безопасности
      1. Структура POU безопасности

На рисунке 20 показана структура одного единственного блока POU безопасности, содержащего данные авода/еывода безопасности, а также дополнительный код безопасности. Сообщение CP 3/RTE может содержать несколько PDU безопасности, например, в случае модульных Ю устройств с несколь­ кими модулями.

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

Таким образом, параметризацией могут быть выбраны *два* эксплуатационных *режима:* неболь­ шое 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).

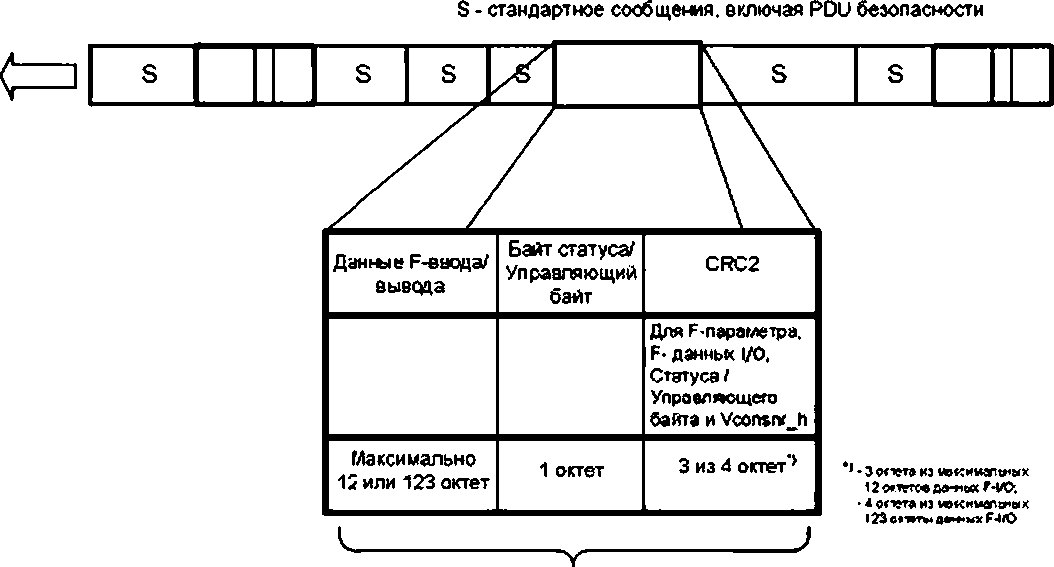
Дополнительно, в сумме требуется 4 (5) октетов, включая байт статуса/управления и 3 (4) октета для кода CRC2.

Подразделы с 7.1.2 по 7.1.6 предоставляют подробное описание элементов структуры PDU безо­

пасности.

28

ГОСТ Р МЭК 61784-3-3—2016



PDU Безопасности протокола FSCP 3/1

Рисунок 20 — PDU безопасности для CPF 3

* + 1. Данные I/O безопасности

F-данные I/O периферийных F-модулей I/O содержатся в этой секции PDU безопасности. Коди­ рование 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.

1. 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 *п* модулями безопасности, требуется сокращение, равное т, умно­ женному на 4 или 5 октет, соответственно.

* + 1. Байт статуса и управления (Status and Control Byte)

Бит4

|  |  |  |
| --- | --- | --- |
| Бит7 | Битв | Бнтб |
| res | VconsoM) | Бит |
| был | переклю- |
|  | сброшен | чатепь |
| • | cons\_nr\_R | ToggleJ» |

Агтивировэны

БитЗ

с&ой

Бит2

Сбой

БиП

В F-устро~~й~~стае

БитО

F-устройству

огкээоустойчюые

коммуникаций: VVD- коммуникаций

или F-модуле

были назначены

значения <FV)

таймаут

CRC

случился отказ

новы\* значения

■ларе метров

FV activated

WD timeout

СЕ CRC

Device\_Fau\*t Par OK

Рисунок 21 — Байт статуса

29

ГОСТ Р МЭК 61784-3.3—2016

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

Бит 0 устанавливается, когда F-устройстео (его технологическое встроенное программное обе­ спечение) получило новые значения параметров.

Имя сигнала «iPar\_OK».

Бит 1 должен устанавливаться определенным технологическим встроенным программным обес­ печением устройства на протяжении хотя бы двух (2) изменений порядкового номера, если F-устройст- во/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 (пере­ рыва). Имя сигнала — «Device\_Fault».

Бит 2 устанавливается, если F-устройстео распознает отказ F-коммуникаций. т.е. если поряд­ ковый номер неверен (обнаружено посредством ошибки CRC2 в У2-режиме) или целостность дан­ ных нарушена (ошибка CRC). Эга битовая информация позволяет F-хосту подсчитать все ошибочные сообщения в рамках заданного промежутка времени Т и вызвать сконфигурированное безопасное состояние системы, если значение превышает определенный предел (максимальная частота остаточ­ ных ошибок). Имя сигнала — «CE\_CRC».

См. также 9.5.1.

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

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 приложе­ ния устройства может также устанавливать этот бит. Имя сигнала — «Reactivated».

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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Бмт7 | Битв | Бит5 | Бит4 | БитЗ | Бит2 | Бит1 | БитО |
| res | res | Бит | Отказоустойчивые | Исяольээеать | Сбросить | Запрошено | Назначение |
|  | течения (FV> | F\_WD\_Tme\_2 |  | подтеержввиие |  |
|  |  | пережлю- | Vcon\*fvj4 | ■параметров |
|  |  | чатель | жидаюшие | (вторичный |  | оператором | рмблокфоввио |
|  |  |  | активации | яорожмой таймеру |  |  |  |
| - |  | Toggle\_h | activaie\_FV | Use\_T02 | R\_cons\_nr | OA\_Req | iPar\_EN |

Рисунок 22 — Байт Управления (Control Byte)

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

Бит 0 устанавливается F-приложением в F-хосте в случае наличия запроса параметризации (F-устройство нуждается в новьх iпараметрах). Имя сигнала — «iPar\_EN».

Бит 1 устанавливается драйвером F-хоста. соответствующим переменной «OA\_Reg\_S\*. Сигнал не связан с безопасностью и дэлжен использоваться F-устройством для местной индикации запро­ са для подтверждения оператора (ОА\_С), 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 возобнов­ ляется. Имя сигнала — «R\_cons\_nr».

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

Бит 4 может быть установлен для принуждения выводов F-устройства перейти в сконфигурирован­ ные или встроенные отказоустойчивые значения. См. подробности в 6.1. Имя сигнала — «activate\_FV».

30

ГОСТ Р МЭК 61784-3-3—2016

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. подроб­ ности в 7.1.4. Имя сигнала — «Toggle\_h».

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

*Подсказка:* для тою. 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.

* + 1. (Виртуальный) порядковый номер

Получатель использует порядковый номер для тою. чтобы контролировать, активны ли еще отправитель и коммуникационный канал или нет. Порядковый номер используется в механизме под­ тверждения 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... OFF FF FFh. возвращаясь назад к 1 в конце.

Примечание — Подробности режима V1 см. 8 (48].

Порядковый номер Р\*Хоста

**(Vconsnr\_h) О** 1 2 3 **4 5**

Toggle\_h (от F-хоста)

**Toggle^d**

**(от F-устройства)**

**Порядковый номер F-устролства** 0 1 2 **3 4**

(Vconsiu\_d)

Рисунок 23 — Функция бита переключателя

Также, в отличие от режима V1, режим V2 не передает порядковый номер с каждым из PDU без­ опасности. Вместо этого он использует виртуальный порядковый номер. Он называется виртуальным потому, что его невозможно увидет» 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 сичхронного приращения надлежащих счетчиков (рисунок 23). Провер­ ка 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 = \*Г в байте управления (см. 7.1.3).

Механизм для счетчика в F-хосте соответствует счетчику в F-устройстве. Тем не менее, счетчик обну­ ляется каждый раз. когда происходит ошибка (внутри или посредством байта статуса). Этот счетчик назы­ вается «Vconsnr\_h».

31

ГОСТ Р МЭК 61784-3.3—2016

Бит переключатель

|  |  |  |  |
| --- | --- | --- | --- |
| **Данные F-входа** | **Байт статуса** | | **CRC2** |
|  |  |  | **Для F-параметра, F-данных I/O, статуса/ управляющего байта и Vconsnr\_h** |
| **Макс. 12 из 123 октет** | **1 октет** *J* | | **3 из 4 октета** |

**Toggle.h (бит 5**

**управляющего байта)**

**R..consjir (бит 2 —**

**управляющего**

**байта)**

**Приращение**

**Сброс**

**Vconsnr d**

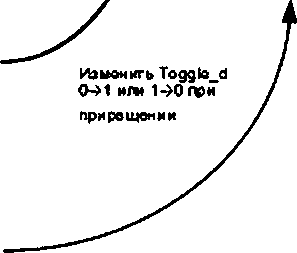
Порядков ЬЙ номер (F- устройства)

{не передается)

0.1. 0FFFFFFH

3 октета

•клочить Vcontrv.d

* + •»числ«чи« CRC2

{см подробное рассмотрение вычисления]

Рисунок 24 — Порядковый номер F-ycтройства

* + 1. Сигнатура CRC2

Когда F-лараметры (связь источник-назначение или кодовое имя. УПБ. длительности стороже­ вого таймера и т. п.) передаются F-устройству, те же параметры используются в идентичной процеду­ ре в F-хосте и в Р-устройстве/Р-иодуле 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. Р-данные I/O. байты статуса и управления и соответствующие порядковый номер (Vconsnr\_h или Vconsnr\_d) используются для создания другой 3-октетной *1*4-октетмои сигнатуры CRC2 (*CRC2*) в F-хосте (см. Рисунок 25). Сигнатура CRC1 формирует начальное значение для вычисления CRC2. передающееся циклически. В F-устройстве генери­ руется идентичная CRC сигнатура и они сравниваются. Последующие циклические передачи требуют только сравнения сигнатур CRC2 (это может выполняться очень быстро).

Любые изменения хранящихся F-napaметров должны быть обнаружены и должны приводить к безопас­ ному 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 е себя октеты рисунка 25 в обратном порядке (рису­ нок 26). По причинам оптимизации обработки порядковые номера (Vconsnr\_h или Vconsnrjj) используются в вычислениях с 4 октетами, дополнительный «заполняющий октет» равен «0». 32-битный счетчик не реко­ мендуется 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 случав делается исключение: CRC2 устанавливается в значение «1» вместо значения «0».

32

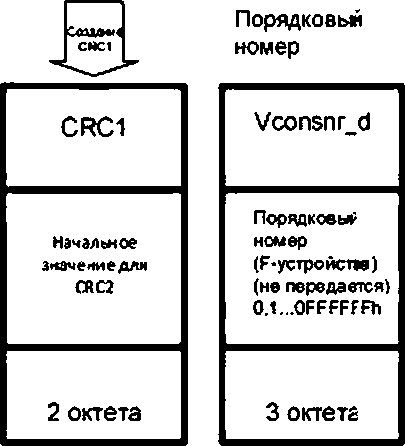
ГОСТ Р МЭК 61784\*3-3—2016

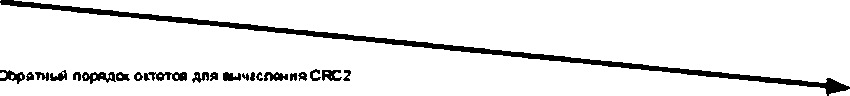
рчиранв,р\*:

yng I ♦ IM СЛрДОЛОоОбИ

1ЧХТО\*ННО« 6ОЛИЧ0С1ПС»;

*WDjm* | • ©ИИ «А6МПМНЫ в Р\*уСТр\*мСТ« И F-Xocre



Порто» октетов перша<и

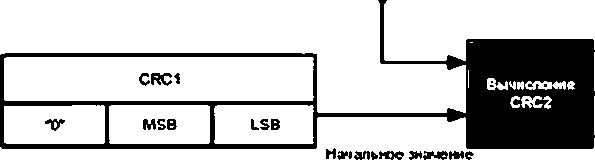
Бит переключатель

h

|  |  |  |  |
| --- | --- | --- | --- |
|  | | |  |
| **Данные F- выхода** | **Байт статуса** | | **CRC2** |
|  |  |  | **Для F-лараметра, F-данных I/O, статуса/ управляющего байта и Vconsnr\_** |
| **Максимально 12**  **или 123 октеты** | **1 октет** | | **3 из 4 октета** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Зеполмаодой омег | Порттдеый номер (Votnenr^h или ViAxa»iNai]) | F-лажме ыодеуыюм | | | байт статус\* ипи у|||ММП)1ДЦ|4 Ом А г |
| *ХГ* | MSB | «хост 2 | LSS | ометО | **I I** | октот п |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| байт сипу» ИНН утаапйктмй бейт | F-АвнмыО Ю0АЛ'\*МСДО | | Пфт»»ы) номер (Vcomnr.b или VeomiM.d) | ЗвЛОЛИНВДИЙ  омет |
|  | onrerп | ометО | LS0 | омет 2 | MS8 | ■о\* |
| i \_ |  |

I\_ *)*

\* СЯС 3 р или 4 о»т\*тв)

Рисунок 26 — Подробности вычисления CRC2 (обратный порядок)

33

ГОСТ Р МЭК 61784-3.3—2016

* + 1. Добавляемые станцартные данные I/O

Стандартные данные I/O могут быть добавлены к PDU безопасности. Для малогабаритных F-устройсте 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.

* 1. Поведение FSCP 3/1
     1. Общие положения

Ядро уровней безопасности в F-хосте и F-устройстве состоит в каждом случае из конечного авто­ мата. режимы функционирования которого определены диаграммами состояний и диаграммами после­ довательностей в 7.2.2 и 7.2.3. На рисунке 27 показана упрощенная модель коммуникаций безопаснос­ ти. 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.

Экземпляр драйвера F-хоста Драйвер F-yc тройства

**Конечный автомат** Конечный автомат

CRC

**PDU Безопасности**

**Байт Выводные управления данные**

**Вводные данные**

**Байт статуса CRC**

**Рису» «ж 27 Комму» (икациопюя солэс уровня боэопасиооти**

* + 1. Диаграмма состояний F-хоста

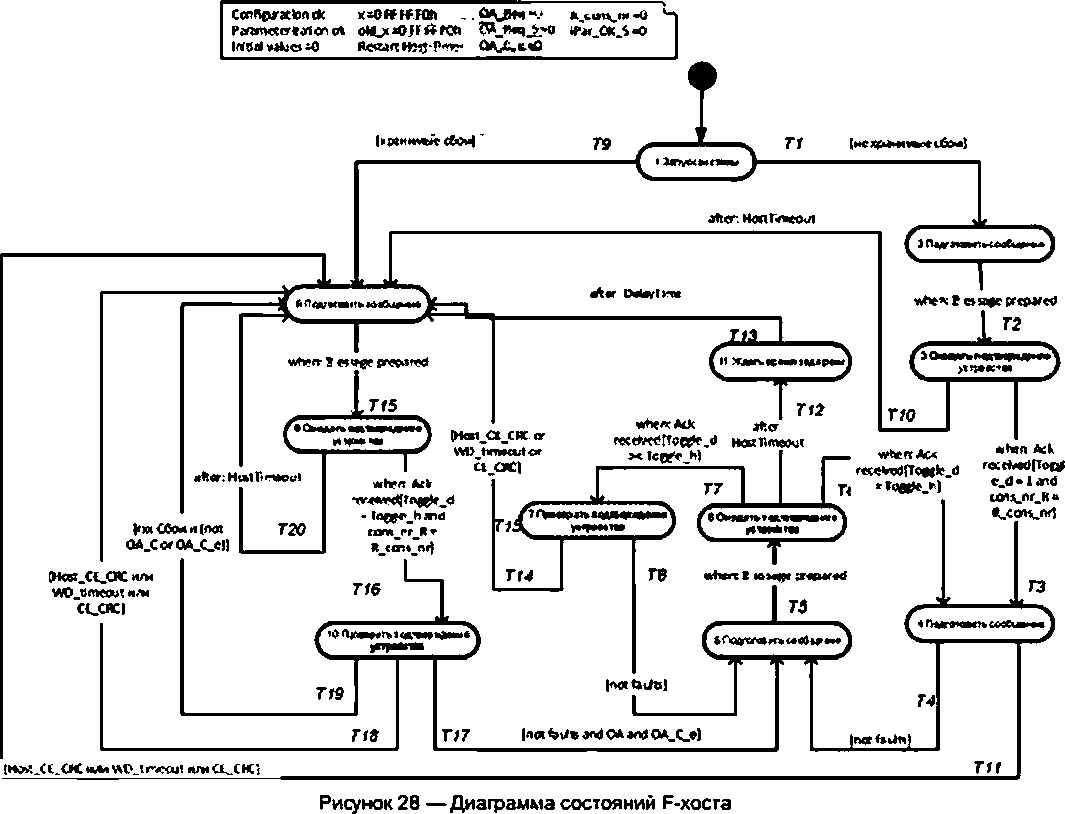
На рисунке 28 показана диаграмма состояний F-хоста. а таблица 4 описывает состояния, пере­ ходы и внутренние элементы F-хоста. Диаграммы следуют нотации UML2. Переходы активируются е случае события, например, принятия сообщения. В случае нескольких возможных переходов так назы­ ваемые ограничители (условия] 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 пе­ реходы 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 дейст­ вия. такие как, таймауты, полученные сообщения или подтверждения оператора откладываются до достижения следующего состоэдия деятельности.

34

ГОСТ Р МЭК 61784\*3-3—2016



Термины, используемые на рлсунке 28. описаны ниже:

Начальные значения — Любые значения PDU безопасности равные «О»:

Host I imeoul Host\_CE\_CRC Oevice\_Fault CE\_CRC

OA\_C\_e

WD\_timeout [не сбои]

[хранимые сбои]

* i-хост распознает локальный таймаут, ожидая подтверждения ьустройства.
* F-хост распознает сбой CRC. анализируя принятый PDU безопасности:
* F-устройство доложило хосту об отказе: бит статуса = 1;
* F-устройство доложило о CRC сбое F-хосту: Бит Статуса 2 = 1:
* Вспомогательный флаг, указывающий на нарастающий фронт сигнала ОА\_С (0—1):
* F-устройство доложило о сбое таймаута F-Хосту; Бит Статуса 3 = 1;
* Нотация UML для условия (ограничителя) для запуска перехода. В данном случае данная переменная истинна (1). если не установлены никакие из сле­ дующих битов:

♦ Host\_CE\_CRC или

♦ CE\_CRC или

- WDjimBOut;

* Эта переиенная истинна (1). если любые из следующих битое были помеще­ ны в хранилище:
  + Host\_CE\_CRC или
* HostTimeout or
* CE\_CRC or
* WDjimeout.

35

ГОСТ Р МЭК 61784-3.3—2016

Таблица 4 — Состояния и переходы F-хоста

|  |  |
| --- | --- |
| НАЗВАНИЕ СОСТОЯНИЯ | ОПИСАНИЕ СОСТОЯНИЯ |
| 1 System Start {Запуск системы) | Начальное состояние экземпляра драйвера F-хоста при подключении пита­ ния. Если система спроектирована для хранения сбоев, то должен быть реа­ лизован переход T9. В противном случае система использует только переход Т1 |
| 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-усгройства (под­ тверждение) |
| 4 Check Device Ack (Проверить подтверждение устройства) | Проверка принятого POU безопасности на наличие CRC-ошибки (Host\_CE\_ SRC). включая виртуальный порядковый номер (х) и на возможные *сбои*  *^•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 (под­ тверждение) |
| 7 Check Device Ack | Проверка принятого PDU безопасности на наличие CRC-ошибки (Host\_CE\_ SRC), включая предыдущий (old\_x) виртуальный порядковый номер (х) и на  возможные сбои F-ycmpoucmea в байте статуса (WDJimeout. CE\_CRC) |
| 8 Prepare message | Подготовка *регулярного* PDU безопасности для F-устройства (обработка ис­ течений) |
| 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\_ SRC), включая виртуальный порядковый номер (х) и на возможные обои  *^•устройства* в байте статуса (WD\_timeoirt. CE\_CRC). После того как произо­ шел сбой, никакой автоматический перезапуск функции безопасности не раз­ решен пока не будет получен сигнал подтверждения оператора (ОА\_С) |
| 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 та проса на подтверждение оператора (operator acknowledge) при следующем подключении питания. Разрешено время задержки равное 0 мс |

*Пройолжоиио таблицы 4*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | СОСТОЯНИЕ ИСТОЧНИКА | СОСТОЯНИЕ ЦЕЛИ | ДЕЙСТВИЕ |
| Т1 | 1 | 2 | испогъзовать FV. activate\_FV «1. FV\_activated\_S =1 Toggle\_h =1 |
| Т2 | 2 | 3 | отправить PDU безопасности |
| ТЗ | 3 | 4 | перезапустить хост-таймер |
| Т4 | 4 | 5 | old\_x =х. х=х+1.  if х =01000000Ь  then х =1 Toggle\_h = not Toggle\_h.  if FV\_activated =1 or activate\_FV\_C \*1 or Devnoa\_Fault =1 then use FVi. FV\_acbvated\_s"=1 else use PVi. FV\_activated\_S \*0 if acbvate\_FV\_C \*1 or Devk»\_Fault =1 then use FVo. activate\_FV =1  else use PVo. activate FV =0 iPar\_OK\_S =iPar\_OK |
| Т5 | 5 | 6 | отправить PDU безопасности |

36

ГОСТ Р МЭК 61784-3-3—2016

*Продолжение таблицы 4*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | СОСТОЯНИЕ ИСТОЧНИКА | СОСТОЯНИЕ ЦЕЛИ | ДЕЙСТВИЕ |
| Тб | 6 | 4 | перезапустить хост-таймер |
| Т7 | 6 | 7 | - |
| Т8 | 7 | 5 | if Reactivated \*1 от activate\_R/\_C =1 or Dev\*ce\_Fault =1 then use FVi, FV\_acbvated\_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 |
| T941 | 1 | 8 | use FV. activate\_FV =1. FV\_activated\_S «1. Toggle\_h \*1.  R cons nr »1, x =0 |
| Т10 | 3 | 8 | restart host-timer, store faults.  use FV. activate\_FV «1. FV\_activated\_S «1, Toggie\_h = not Toggle\_h.  R cons nr=1.  x =0 |
| Т11 | 4 | 8 | store faults. use FV. activate\_FV =1. FV\_activated\_S «1, Toggle\_h = not Toggle\_h,  R cons nr »1, x =0 |
| Т12 | 6 | 11 | use FV. activate\_FV =1. FV\_acbvated\_S «1, R cons nr=1.  x =0 |
| Т13 | 11 | 8 | store faults.  Togg(e\_h = not Toggle\_h, restart host-timer |
| Т14 | 7 | 8 | restart host-timer, elnre fairfts.  use FV. activate\_FV =1. FV\_activated\_S «1, Toggle\_h = not Toggle\_h.  R cons nr=1,  x =0 |
| Т15 | 8 | 9 | отпраеигь PDU безопасности |
| Т16 | 9 | 10 | перезапустить хост-таймер |
| Т17 | 10 | 5 | reset stored faults. OA\_Req\_S \*0. OA\_Req =0. OA\_C\_e =0. R\_cons\_nr =0.  okd\_x =x.  x»x+1. if x s01000000h thenx=1  Toggle\_h = not Toggle\_h. if FV\_activated \*1 or activate\_FV\_C =1 or Dev»ce\_Fault =1 then use FVi. FV\_actcvated\_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 =.Par\_OK |

37

ГОСТ Р МЭК 61784-3.3—2016

Продолжение *таблицы 4*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | СОСТОЯНИЕ ИСТОЧНИКА | СОСТОЯНИЕ ЦЕЛИ | ДЕЙСТВИЕ |
| Т18 | 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 |
| Т19 | 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 Togg»e\_h.  R\_cons\_nr =0.  old\_x =x. x =x+1. if x =01000000h then x =1 |
| Т20 | 9 | в | store fautls. OA\_Req =0. OA\_Req\_S =0. OA\_C\_e \*0. use FV. activate\_FV =1. FV\_activated\_S «1. Toggle\_h = not Toggte\_h.  R\_cons\_nr=1. x =0,  restart host-timer |
| #> Реализация перехода T9 зависи\* от концепции проекта безопасности определенного производителя системы. | | | |

*Продолжение таблицы 4*

|  |  |  |
| --- | --- | --- |
| ВНУТРЕННИЕ ЭЛЕМЕНТЫ | тип | ОПРЕДЕЛЕНИЕ |
| X | Счетчик | х 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 8 байте управления. Действительное чыа^еыия гчвтиииа ж Runinuoun в вычиг.пвыия *C.RC.7* и пптпыу прлшараотгя ыя гЛпм передачи. Диапазон значений — 0 ... OFFFFFFh. Во время запуска этот суммиру­  ющий счетчик установлен в значение OFFFFFOh и начинает отсчет от него. F-xocr дает приращение виртуальному порядковому номеру после каждого подтверж­ денного принятия соответствующего виртуального порядкового номера модуля OFFFFFFh F-устройства этого хоста, пропуская значение «0» и продолжая с «1» |
| old\_x | Счетчик | Предыдущее значение текущего местного порядкового номера х. Необходимо хра­ нить предыдущее значение порядкового номера для того, чтобы отличать началь­ ный 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 хостэ/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 значе­ ний—0 ... 65 535мс |
| OA\_C\_e | Флаг | Эта вспомогательная переменная (двоичная) гарантирует то. что безопасное состояние завершается только после смены сигнала ОА\_С с 0—1 (фронт). Без этого механизма оператор мог бы аннулировать безопасные состояния посред­ ством безвозвратной активации сигнала ОА\_С |

38

ГОСТ Р МЭК 61784-3-3—2016

*Окончание таблицы 4*

|  |  |  |
| --- | --- | --- |
| ВНУТРЕННИЕ ЭЛЕМЕНТЫ | тип | ОПРЕДЕЛЕНИЕ |
| faults | Флаги | До подтверждения оператора (ОА\_С), 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 деятель­  ности | 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, таймау. полученное сообщение или подтверждение оператора откладываются до тех пор. пока не наступит следующее состояние «действия» {34] |

* + 1. Диаграмма состояний F-устройства

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

20Запуск системы

$Mrtuo Тех Ос Configurator ос Pvametcrttaacn OK irrsal Values «О

*104*re В-0

W) tnwouft

U»FVlf»0 XsOffFTR»

**к**

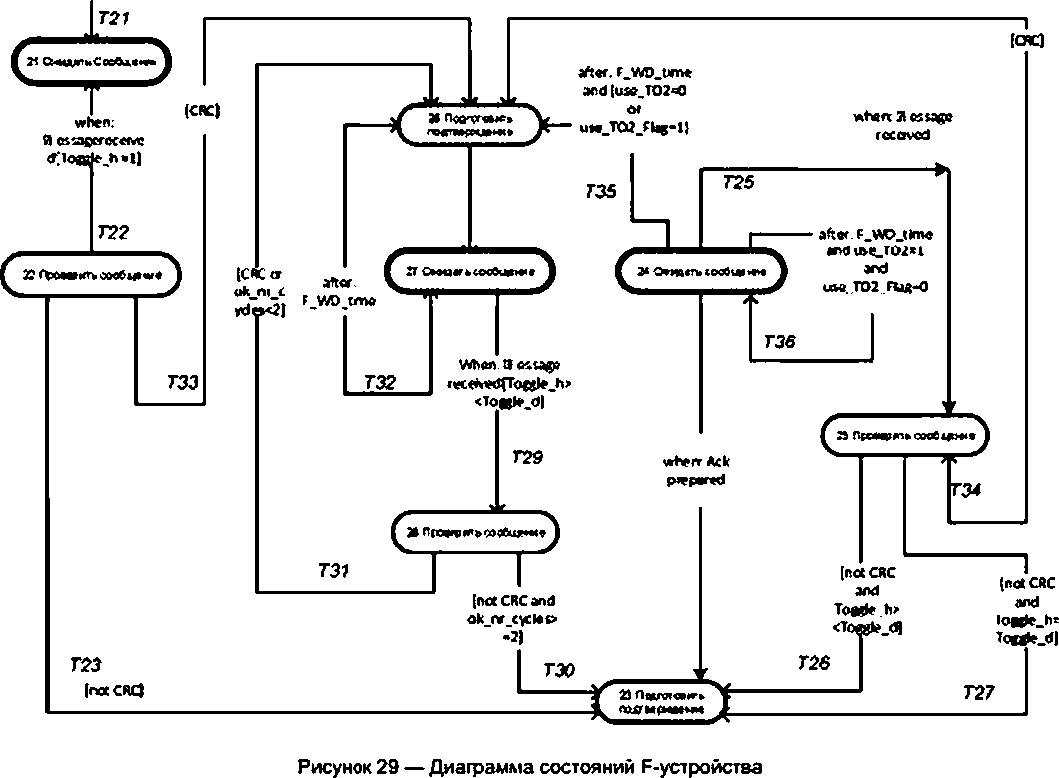
ry.jicavktMi-1 Tng0».d\*4 W>\_t«rwout\_«wr< c\*\_w\_c\*de$ «0

4 CT.CHC.wunt 41

otim SfXsin

$1\*1 Л

UW\_T02\_Tbe »o



39

ГОСТ Р МЭК 61784-3.3—2016

Термины, используемые на рисунке 29. определены ниже:

ffoggle\_h = Toggle\_d]

(Toggle\_h х Togg»e\_d| (CRC)

F\_WD\_Time use\_T02

use\_T02\_Flag Ack Message received

* нотация UML условия (ограничителя} для запуска перехода. В этом случае это означает, что бит Toggie\_h не изменил свое значение (вне переключен»};
* бит Togg\*e\_h изменил свое значение («переключен»);
* F-устройсгво распознает сбой CRC (ошибка коммуникаций и/или порядкового номера):
* время сорокового таймера, определенное F-параметром «F\_WD\_Time»:
* СВЗ в байте управления, указывающий на использование времени вспомогательного сторожевого таймера F\_WD\_Time2;
* вспомогательный флаг;
* POU безопасности для подтверждения F-устройства;
* любой новый принятый PDU безопасности; следует игнорировать PDU безопасности, где все значения равны 0.

Таблица 5 — Состояния и переходы F-усгройства

|  |  |  |  |
| --- | --- | --- | --- |
| НАЗВАНИЕ СОСТОЯНИЯ | | | ОПИСАНИЕ СОСТОЯНИЯ |
| 20 System Start (Запуск системы) | | | Начальное состояние устройства при подключении питания. При подключении литания F-устройство вывода устанавливает значение \*0». Сразу же после F-параметризации оно устанав­ ливает отказоустойчивые значения. При подключении литания F-усгройство *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 POU безопасности от F-устройсгва |
| 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 POU безопасности от F-устройсгва (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 х=0. cons\_nr\_R =1 |
| T23 | 22 | 23 | use PVi. FVo.  FV activated =1.  CE\_CRC =0.  WD\_timeout =0. Toggte\_d = Toggte\_h. restart device-timer. ok\_nr\_cydes =ok\_nr\_cyctes +1 |
| T24 | 23 | 24 | send safety POU |

40

ГОСТ Р МЭК 61784-3-3—2016

*Продолжение таблиц# 5*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | СОСТОЯНИЕ ИСТОЧНИКА | СОСТОЯНИЕ ЦЕЛИ | ДЕЙСТВИЕ |
| Т25 | 24 | 25 | *Н* Toggie\_h >< Toggle\_d then  restart device-timer x=x+1. if x =01000000h thenx=1. cons\_nr\_R \*0  if R\_cons\_nr =1 then x=0. cons\_nr\_R =1 if use\_T02 =0  then use\_T02\_Flag =0 |
| Т26 | 29 | 23 | Use PVi. Toggle\_d = Toggte\_h, if ok\_nr\_cydes <4 ok\_nr\_cycle =ok\_nr\_cyde +1 if ofc\_nr\_cycles <4 then use FVo. FV\_activated =1 else use PVo. FV\_activated =0 if acbvate\_FV =1  then use FVo else use PVo |
| Т27 | 25 | 23 | Use PVi. Toggle\_d = Toggie\_h. if ok\_nr\_cycies <4 then use FVo, FV\_activated =1 else use FVo. FV\_activated =0 if activate\_FV =1  then use FVo else use PVo |
| Т28 | 26 | 27 | Send safety PDU |
| Т29 | 27 | 28 | if R\_cons\_nr =1 then x=0, cons\_nr\_R =1 else x=x+1.  if x =0100000»!  then x =1. cons\_nr\_R =0 |
| ТЗО | 28 | 23 | use PVi. FVo. FV\_activated =1. Toggle\_d = Toggie\_h. restart device-timer. ok\_nr\_cycies =ok\_nr\_cyc\*es +1 |
| Т31 | 28 | 26 | Toggle\_d = Toggie\_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 |

41

ГОСТ Р МЭК 61784-3.3—2016

*Продолжение таблицы 5*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | СОСТОЯНИЕ ИСТОЧНИКА | СОСТОЯНИЕ ЦЕЛИ | ДЕЙСТВИЕ |
| Т31 | 28 | 23 | then  WD\_timeout =1.  WD\_timeout\_count = WD\_timeout\_count -1  else WD.bmeout =0 |
| Т32 | 27 | 25 | Use PVi. FVo. FV.activated =1. WD\_teneout =1.  WD\_timeout\_count =1,  ok\_nr\_cycles =0. restart device timer. Toggle\_d = Toggle\_h |
| ТЗЗ | 22 | 25 | Use PVi. FVo. FV activated =1. CE\_CRC =1,  CE\_CRC\_coont =1, WD\_timeout \*0. ok\_nr\_cycles =0. restart device-timer. Toggle\_d = Toggle\_h |
| Т34 | 25 | 25 | Use PVi. FVo. FV activated =1. CE\_CRC =1,  CE\_CRC\_count =1. ok\_nr\_cycle =0. restart device-timer.  Toggle\_d = Toggle\_h |
| Т35 | 24 | 25 | Use PVi. FVo. FV\_activated =1. WD\_t»meout =1.  WD\_tomeoul\_count =1.  ok\_nr\_cycles =0. restart device timer. Toggle\_d = Toggle\_h |
| Т36 | 24 | 24 | restart device timer with F\_WD\_Time\_2 use\_T02\_Flag =1 |
| 41 Реализация перехода T9 зависит от концепции проекта безопасности определенного производителя системы. | | | |
| внутренние элементы | | тип | определение |
| X | | Очетчик | 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. Эго означает, что х 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 счет­ чика х обнуляется 8 случае, если установлен бит управления  «R\_cons\_nr». т.в. имеет значение(1). Соответствующее значение счетчика х включено в вычисление CRC2 и потому проверяет­ ся 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-устройсгво должно устанав­ ливать FVo и FV\_activated=1 на протяжении минимум 3 циклов. Подсчитать эти циклы от 1 до 3 является задачей данного сум­  мирующего 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 |

42

ГОСТ Р МЭК 61784-3-3—2016

*Окончание таблицы 5*

|  |  |  |
| --- | --- | --- |
| ВНУТРЕННИЕ ЭЛЕМЕНТЫ | тип | ОПРЕДЕЛЕНИЕ |
| WD\_timeout\_count | Счетчик | Этот счетчик обратного отсчета используется для обеспечения установки бита «WCMimeoub\* в байте статуса минимум на 1 цикл или максимум на 2. Диапазон значений 0 —1 |
| devrce-timer | Таймер | Данный таймер проверяет, поступил ли следующий действи­ тельный POU безопасности вовремя. РПараметр «F\_WD\_Time» используется для определения времени сторожевого таймера. Диапазон значений 0 ... 65 535 мс |

* + 1. 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 запу­ ска. 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.

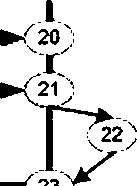
FVI

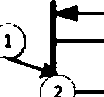
F-Xoc t

Подключение питания

Начальные значения = 0\*) Параметризация

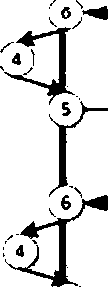
F-Устройство Вывод Подключение литания

FVo

х = OFF F FOh

FVI

х=х+1

FVI

х\*х+1

FVi Х=Х+1

PVi

Fvo, х= OFF FF F0

acbvate\_FV = 1. R\_cons nr = 0

Pvi, x = OFF FF FOh

FV. activated = 1

3vo. x \* OFF FF F1h

activate\_FV = 0. R\_cons\_nr = 0

Pvi. x = OFF FF F1h

FV activated = 1

Pvo, x \* OFF FF F2h activate\_FV • 0. R\_con$\_nr» 0

Pvi. x \* OFF FF F2h fV\_acbvated = 1

Pvo. x = OFF FF F3h

activate\_FV » 0, R\_cons\_nr = 0

Pvi. x = OFF FF F3h

FV activated = 0

VLV

<24

Г25

FVo

x = OFF FF FOh

FVo

x = OFF FF F1h

FVo

x a OFF FF F2h

PVo

x » OFF FF F3h

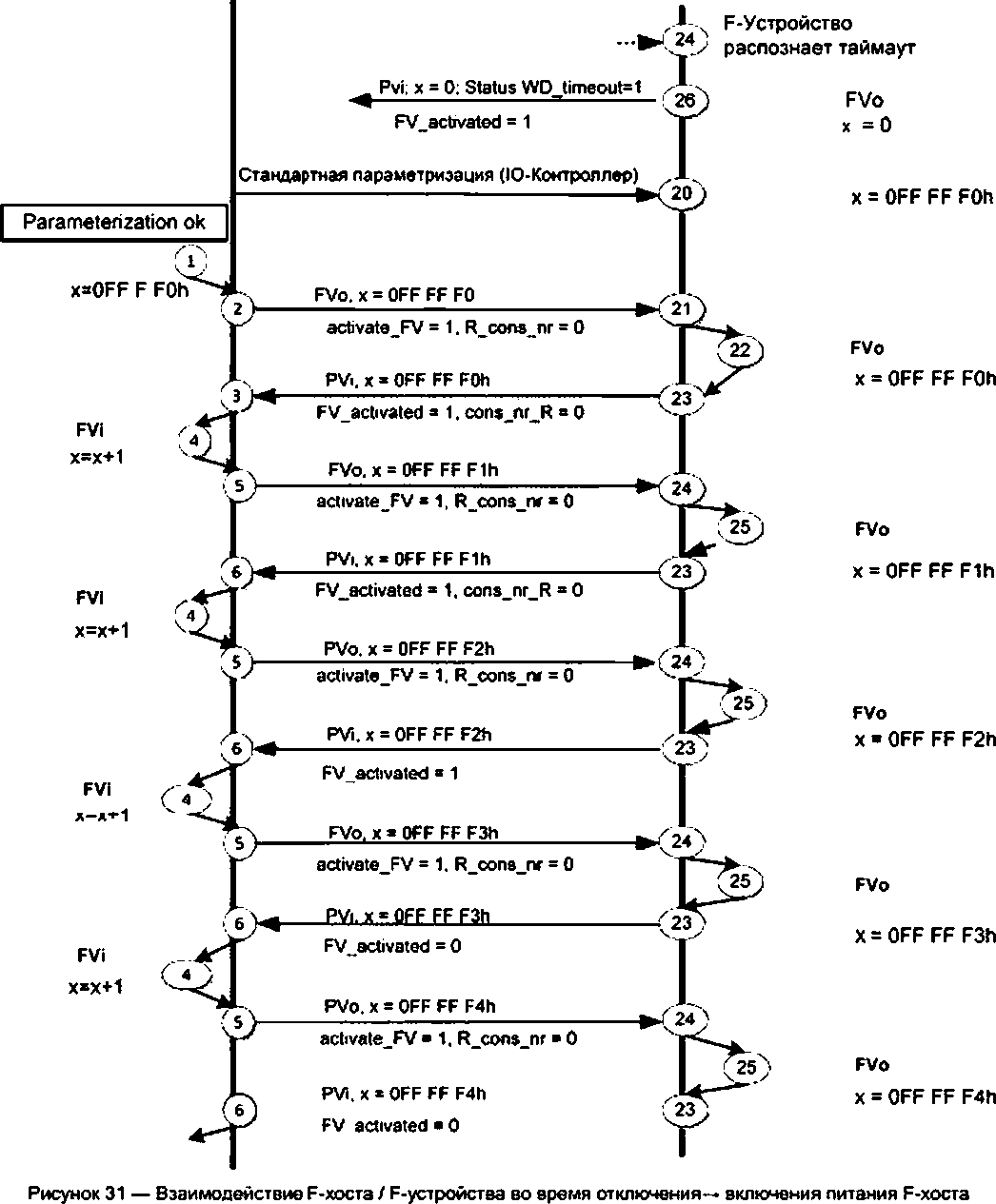
\* \*} Поведение шины

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

43

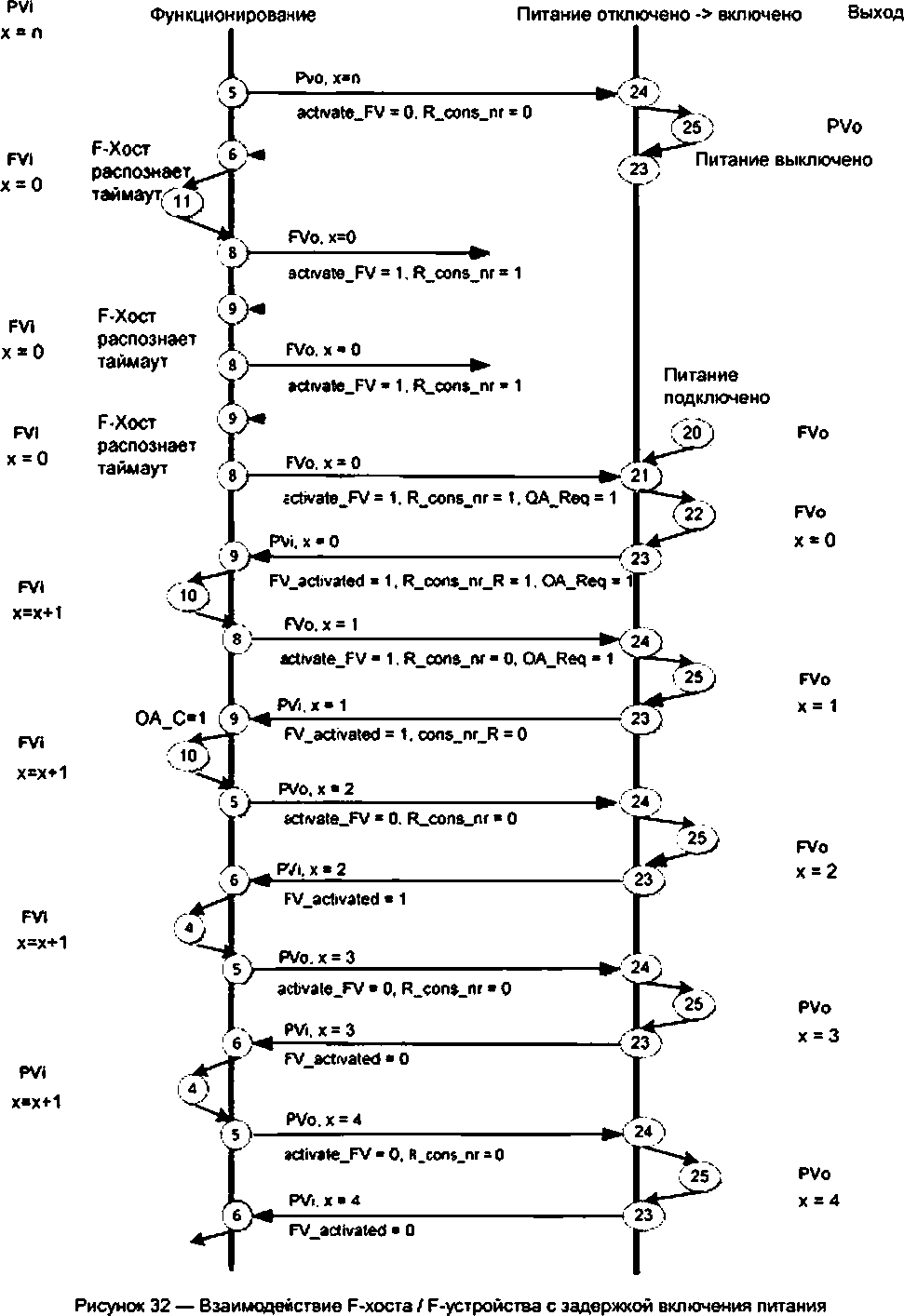
ГОСТ Р МЭК 61784-3.3—2016

F-Xoc t F-Устройство Вывод

Питание отключено -> включено Функционирование

44

ГОСТ Р МЭК 61784\*3-3—2016

F-Xoc t F-Устройство

45

ГОСТ Р МЭК 61784-3.3—2016

PVi Х\*П

FVi Х\*0

FVI

Хв0

FVi

х«0

FVi

х\*х\*1

FVi

х\*х+1

FVi

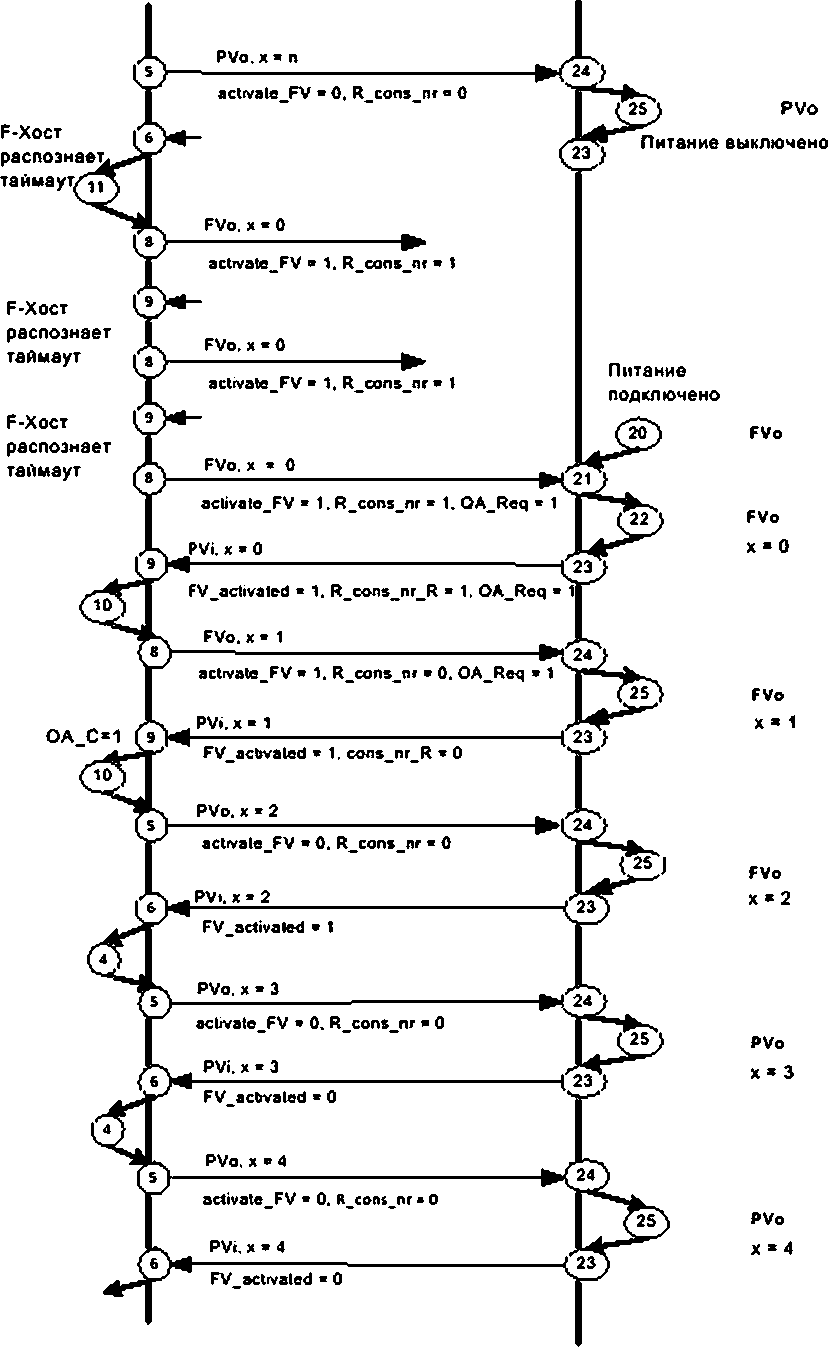
х\*х\*1

PVi

х\*х\*1

F-Xocr Функционирование

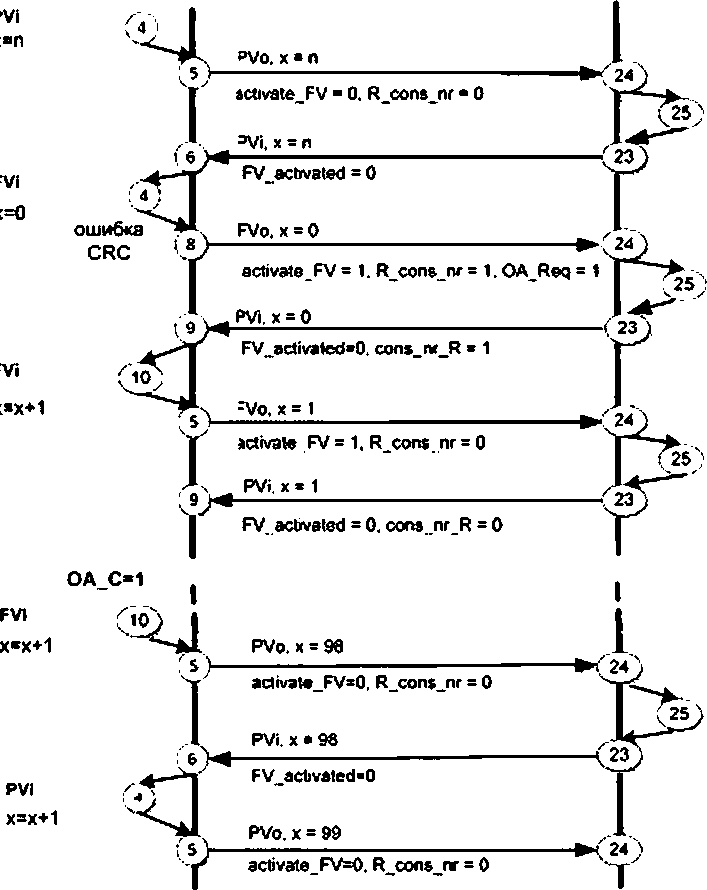
F-Устройство Питание отключено -> включено вывод

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

46

ГОСТ Р МЭК 61784\*3-3—2016

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

F-XOCT F-Устройство

PVo х = n

FVo

х»0

FVo x\* 1

PVo

x\*98

PVo

x \* 99

Рисунок 34 — Взаимодействие F-хосг / F-устройство, 8 то время как хост распознает CRC ошибку

47

ГОСТ Р МЭК 61784-3.3—2016

F-X3CT F-Уетроиство Вывод

х=л

PVI

х=х-Н

FVt

**х=0**

FVI

х=х+1

FVi

х=х+1

ошибка CRC ч!

\*>►

9 re­

pvo . х ■ и

aclivale\_FV • 0, R\_oont.iv ■ О

PV). х = п

FV.adrvaled = О

FVo. х=п»1

activate.FV в 1. R.cons.nr« 0

PVi Status СЕ CRC«1 x\*n\*1

**FV\_ect)V8tee\*l**

**FVo. x ® 0**

activate FV\* 1. R\_oon8.iv • t

PVt. status CE\_CRC=1, x a 0

FV.actwaled = V cons.rr.R = t

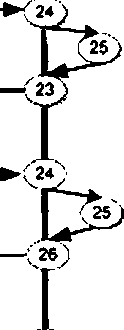
FVo x = 0

actwated.FV ■ 1. R cons rv • 1

PVi. x = 0

FV.acttvaieO = 1. cons.nrR = i

**PVo. x »i**

■►(27/

PVo X = П

сбой CRC

FVo

**x=n+1**

FVo x в 0

FVO

**x = 0**

*1)*----------------------

Г FV.acbvated \* 1

1 PVt. x ■ 1

. R cons nr в 0

-K'20

<23;

FVO

X® 1

FVI

х\*х\*1

**ОА\_С®1**

**FVi**

х=х\*1

**FV.ecbvateO =** 1**. con»\_nr\_R = о**

PVo. x » г

| FV.aciwated • 1. R\_cons\_<v ■ 0 1 PVi. X • 2

()>e---------------------

f FV.actwaied \* 0

PVO. x • 376

actrvate\_FV\*0. R.cons.nr » 0

**i**

*\*(2A*

*i* 23 ;

Y

*A*

*\* 25

FVO X = 2

PVi

х=х+1

PVi. x - 376

FV.aclivaledcO

PVo. X » 377

activate FV\*0, R cons nr • 0

тto

PVo x = 376

PVo X = 377

*ь*

Рисунок 35 — Взаимодействие F-хост ***i*** F-устройство. в то время как устройство распознает CRC ошибку

48

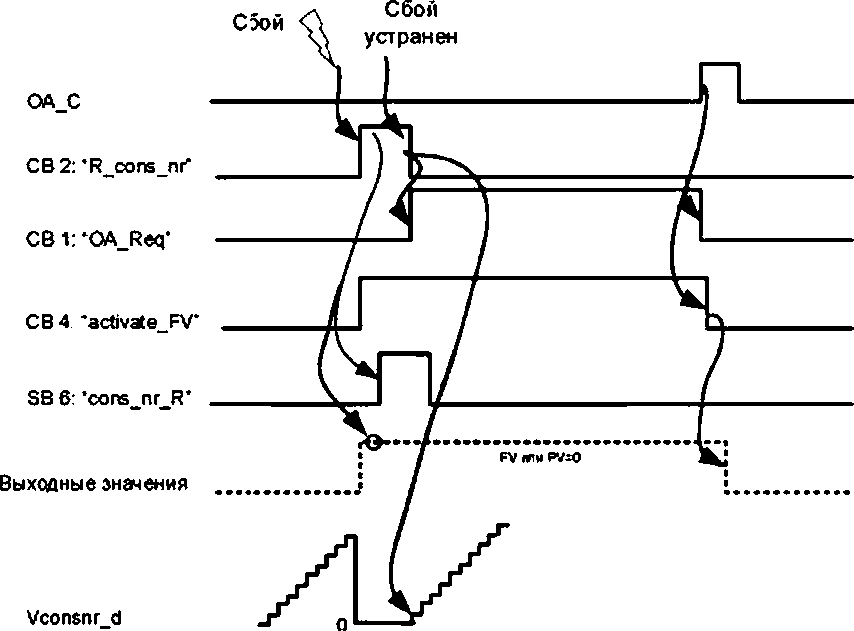
ГОСТ Р МЭК 61784-3-3—2016

* + 1. 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\* *у* в результате выходные значения F-устройства-вывода устанавлива­

ются в значение «0». а счетчик порядкового номера устанавливается в «0» (Vconsnr\_d). В то же время устанавливается в (1) бит 4 «activatB\_FV» байта управления, тем самым вынуждая Р-устройстео-выаода настроить свое собственной отказоустойчивое состояние, что делается всякий раз. когда это состояние не может быть достигнуто с помощью обычных значений вывода (FV).



**Рисумок 36 — Влиаыио сигнала сброса сиагника**

Тем временем F-xocr отправляет F-устройству сигнал «OA\_Req» в виде бита 1 байта управления. Этот сигнал может быть использован для того, чтобы указать пользователю посредством светодио­ да (9.1) на то. что произошла ошибка и запрошено подтверждение оператора (ОА\_С). 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 (ОА\_С = 1) выполняются следующие действия:

* запрос на подтверждение оператора восстанавливает свое значение по умолчанию (OA\_Req = 0);
* запрос на активацию состояния отказоустойчивого вывоза восстанавливает свое значение по умолчанию (activate\_FV = 0);
* выходные значения процесса появляются снова после трех циклов сообщений.
  + 1. Контроль времен безопасности

7.2.6.1 Нормальное функционирование

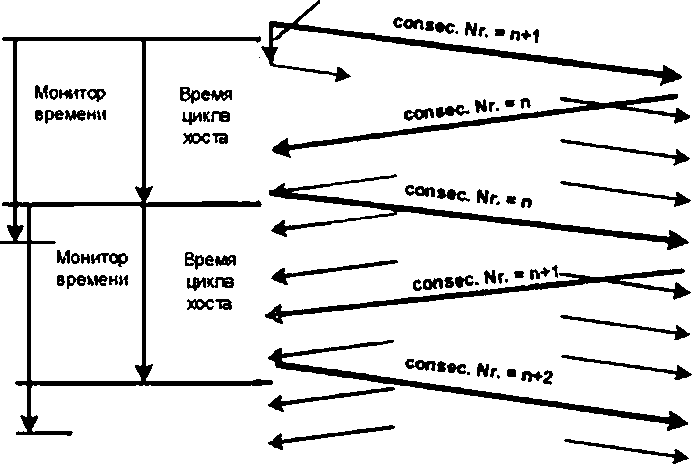
На рисунке 37 показано, как F драйвер использует лежащие в основе коммуникации CP 3/RTE и как определяются отдельные времена для контроля. Короткие стрелки означают: в CP 3/RTE IO-контроллер отправляет то же самое PDU безопасности F-устройству более часто, чем новый POU безопасности генерируется F-драйеером в рамках времени цикла хоста в F-хоств (порядковый номер = п+1). 8 ответ F-устройстео отправляет PDU безопасности (подтверждение) Ю-контроллеру более часто, чем F-драйвер в F-устройстве генерирует новый PDU безопасности.

49

ГОСТ Р МЭК 61784-3.3—2016

1. xocT F-вывсщ (устройство)

Время 1^кпв шины



|  |  |  |
| --- | --- | --- |
| Монитор времени | |  |
| Монитор времен | ' | *'* |
|  | |
|  | *'* | |

Рисунок 37 — Контроль времени передачи сообщения для передачи F-xoc t — 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 представ­ ляют PDU FSCP 3/1 с подтвержденным на данный момент (виртуальным) порядковым номером, но. вероятно, с различными значениями процесса.

**F-ввод (устройство)** F-XOCT

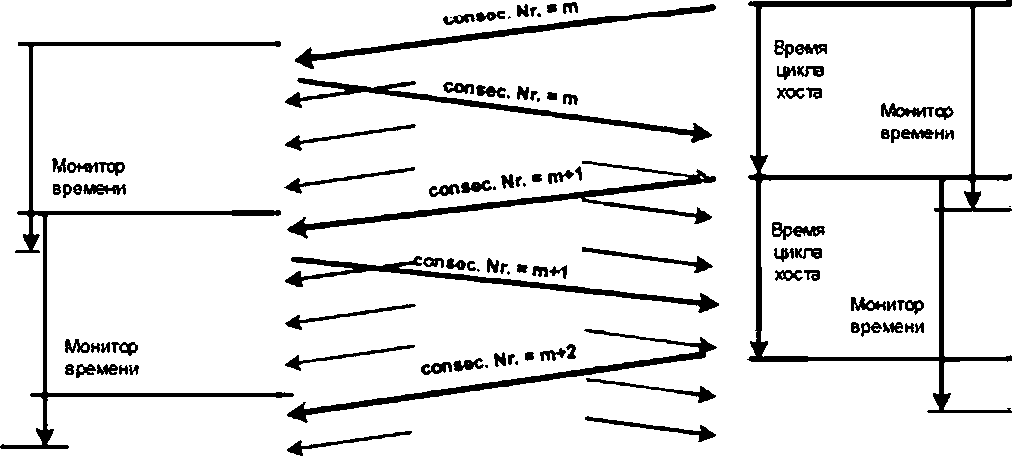


Рисунок 38 — Контрогъ времени передачи сообщения дпя передачи F-ввод •— F-x o c t

50

ГОСТ Р МЭК 61784-3-3—2016

Другие временные ограничения перечислены ниже:

*Запуск*

(Синхронизация)

*Цикл F-протокола*

*Устройство* контроля (монитор) *времени* (Сторожевой таймер)

*Контроль порядкового номера*

*Повторение PDU безопасности*

*Устройство контроля УПБ*

Синхронизацию после запуска системы, драйвер F-xocra начинаете порядкового номера «OFFFFFOh». Затем. F-xocr увеличивает виртуальный порядковый номер после каждого подтвержденного получения соответствующего виртуального по­ рядкового номера модуля «OFFFFFFh» F-устройства данного хоста, пропуская значение «3» и продолжая с «1». В последний момент перед истечением вре­ мени контроля F-eeoA/F-еывод ожидает сообщение, содержащее виртуальный порядковый номер, увеличенный на 1. F-вывод предоставляет отказоустойчи­ вые значения (FVo) после того, как получает виртуальный порядковый номер равный «0к

Р-ввод/Р-вывод возвращает PDU безопасности F-хосту. содержащее тот же вир­ туальный 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).

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.

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

Каждое искаженное сообщение (сбоем CRC и виртуального порядкового номера) будет подсчитано за временной период конфигурируемого устройства контроля УПБ (Т). Отказоустойчивые значения устанавливаются каждый раз. когда прои­ зошло бол€в одного такого сбоя. т.е. одно обнаруженное искаженное сообщение может допускаться {*вариант А).* 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 В.* в котором время контроля УПБ (Т) 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 сообщениядолжно произойти во время сдвига производства или операции, то на роль УПБ-устройства контроля (монитора) назначается ответственный оператор, который межет 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.

Реализации варианта А лежит на производителе F-хоста. Тем не менее, под­ робная 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.

51

ГОСТ Р МЭК 61784-3.3—2016

*Период времени* временной период *Т* устройства контроля УПБ является постоянным иэме-

*устройстеа* ряемым в часах (h) значением, которое формируется из запрошенного УПБ и

*контроля (Т)* длинны сконфигурированного CRC (9.5.1). 8 таблице 6 установлены времена устройства контроля УПБ.

Таблица 6 — Временные периоды Г устройства контроля УПБ

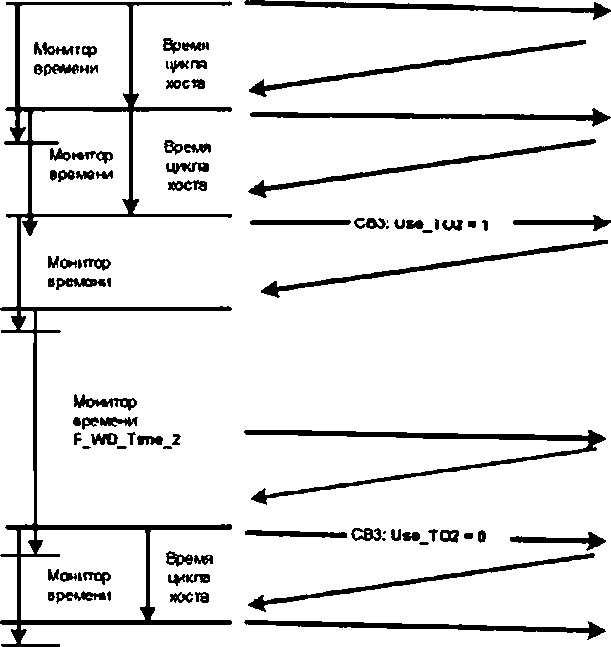
|  |  |  |  |
| --- | --- | --- | --- |
| УПБ | СЯС | Длина POU безопасности | Временной период (h) |
| 3 | 24 бита | S 16 октетов | >10 |
| 2 | 24 бита | $ 16 октетов | >1 |
| 3 | 32 бита | $ 128 октетов | >10 |
| 3 | 32 бита | S 128 октетов | >1 |

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\_Tme), заданное для приложения безопасности. Для того чтобы избежать ложные срабатывания, драйвер F-хоста может один раз использовать время вспомогательного сторожевого таймера (F\_WD\_Tme\_2) для расширения основного времени сторожевого таймера для этих запланированных и контролируемых событий, как это показано на рисунке 39.

F-x oc t F-вьвод (устройство)

Монитор бремени

Монитор

времени

МО\*ИГф

•семени

F.WO\_Tbre\_2

Монитор

времени

Монитор

времени

Рисунок 39 — Расширенное время сторожевого таймера по запросу

52

ГОСТ Р МЭК 61784-3-3—2016

* 1. Реакция в случае неисгравности
     1. Повторение

Цитата: «Неисправность устройства шины приводит к повторению старых и неактуальных сообще­ ний 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 сообщениес PDU безопасно­ сти введенное однажды будет сразу же заменено правильным сообщением. Таким образом, последующая возможная задержка экстренного запроса может быть равна *одному периоду спюрожееого таймера.*

* + 1. Потеря

Цитата: «Неисправность устройства шины удаляет сообщение безопасности (например, запрос

«безопасную остановку функционирования»).»

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

* + 1. 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.

* + 1. 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 перепуганы.».

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

* + 1. Искажение данных безопасности

Цитата: Неисправность устройства шины или канала передачи зашумляет сообщения безопасности.». Устранение: Сигнатура CRC2 обнаруживает зашумление данных между отправителем и получателем.

Денные F-параметров

|  |  |  |  |
| --- | --- | --- | --- |
| PDU безопасности | | | |
| F-денные I/O | Байт статуса или байт управления | (виртуальшй) Порядковый номер | CRC2 |
|  |  |  | Для F-данных WO. бейта статуса и управления, (виртуального) поряа нового номера и F- параметров |
| *т* октет | 1 октет | 3 октета | 3 или 4 октете |

F-пвреметры: кодовое имя.

WD время. УП6 и т. д.

Рисунок 40 — Данные F-параметра и CRC

Сигнатура CRC2 генерируется для F-параметров (включая кодовое имя). F-данных I/O, вир­ туального порядковою номера и байта упрааления/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.

* + 1. Задержка

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

53

ГОСТ Р МЭК 61784-3.3—2016

Устранение:

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

Время сторожевого таймеэа определено в 9.3.3.

* + 1. Подмена

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

Устранение: Данные поступают от правильного отправителя и направляются правильному полу­ чателю (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 POU безопасности с правильным CRC2 и правильным порядковым номером.

Обнаружение данных от дэугого отправителя или для другого получателя обеспечивается за счет того, что F-отлравитель. принадлежащий связи F-источник-назначение (кодовое имя) является единствен­ ным генерирующим именно такую совпадающую CRC сигнатуру, которую ожидает F-лолучатель. 8 то же самое время, получатель прибегает к CRC сигнатуре для проверки в неявной форме аутентичности адреса F-отпраеителя (так какск был включен в CRC).

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

* кодовый переключатель вбпоке для кодовою 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 данною блока;
* механизмы адресации, независящие от адресации CPF 3. Саботаж не предполагается.
  + 1. Отказы памяти в коммутаторах

Цитата: «1. Обмен эксплуатационными данными превышает возможности коммуникационного ка­ нала. 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 соображе­ ний. Центральные элементы этих сетей — это коммутаторы, являющиеся достаточно сложными актив­ ными 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 отклю­ чен. 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 поыощыо) |
| Зашумленные данные | Сигнатура CRC (24 бита) |
| Неверное назначение | Кодовое имя (2 х 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-xocr более не  подсоединен | Порядковый номер (24 бита) без автоматического перезапуска |
| Ретрансляции хранимых сообщений с Э или более порядковыми PDU безопасности в партии. F-xocr более не подсоединен | Порядковый номер (24 бита) и реакция на сбой посредством байга управления (рисунок 36) |

54

ГОСТ Р МЭК 61784-3-3—2016

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 пра­ вильным порядковым номером. Этот сбой будет обнаружен по причине 24 битного порядкового номера и того факта, что перезапуск F-устройства-еывода требует ОА\_С = 1 (подтверждение оператора).
  + Коммутатор передает сообщения с блоками PDU безопасности из своего автоматически возоб­ новляющегося 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 Р-устройства-8ывода требует ОА\_С *-* 1 (Подтверж­ дение Оператора).
    1. Границы сети и маршрутизатор

Цитата: «1. Обмен эксплуатационными данными превышает возможности коммуникационного ка­ нала. 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 непра­ вильному 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

1. содержится список типов сбоев иограничения для функционирования маршрутизатора, необходимые для обеспечения достаточной безопасности.

Таблица в — Границы сети безопасности

|  |  |  |
| --- | --- | --- |
| Тип сбоя | Последствия | Обнаружение и контроль |
| Маршрутизатор держит неверный адрес F-устройства | Маршрутизатор получает сообщение для этого определенного F-устройствэ.  Результат: цель не найдена. | Таймаут F-устройсгва |
| Два F-устройсгва с идентичными адресами. Один в подсети 0, другой в подсети 1.  Ограничение: 2-порго8ый-маршрутиззгор.  как на рисунке 11. | 1. F-устройство подсети 0 не найдено в подсети 0; 2. F-устройство подсети 0 не досягаемо в   подсети 1:   1. F-устройство подсети 1 недосягаемое подсети 0: 2. F-устройство подсети 1 праеипьно в подсети 1 | В соответствии со стандартом CP 3/RTE |
| Дее F-устройсгво с идентичными адресами. Один 8 подсети 0. другой е подсети 1 Ограничения: Маршрутизатор с одним портом (например. PC. лаптоп) | 1. F-устройсгво подсети 0 не найдено в подсети 0; 2. Дублирование адреса в подсети | Однопортовые мар­ шрутизаторы не соз­ дают границы сети (безопасности) |

* 1. Запуск и координация изменений
     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 СР 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 У1-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 Ю-контроллера и его Ю-устройств. являющихся частью F-устройств.

55

ГОСТ Р МЭК 61784-3.3—2016

* + 1. Разблокирование назначения (параметров

Следуя сообщению диагностики F-устройства. которому требуются дополнительные (параметры (см. 8.2} или по внешнему запросу, F-хост устанавливает бит 0 («Разблокирование назначения (пара­ метров)») в байте управления своего следующего PDU безопасности. Затем F-устройство принимает, посредством команд «Write-Record» (Записать запись), (параметры один набор данных за другим, и в конце подтверждает их получение, устанавливая бит 0 («F-устройству были назначены новые значения (параметров») 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 статусаУуправления, могут применяться в контексте Proxy-FB-iParameterization. т. е. прокси-ф-блок-тараметризации (8.6.2). Они не применимы в контексте inap-cepeepa (8.6.4> Последовательность сигналов на рисунке 41 является примером воз­ можного применения.

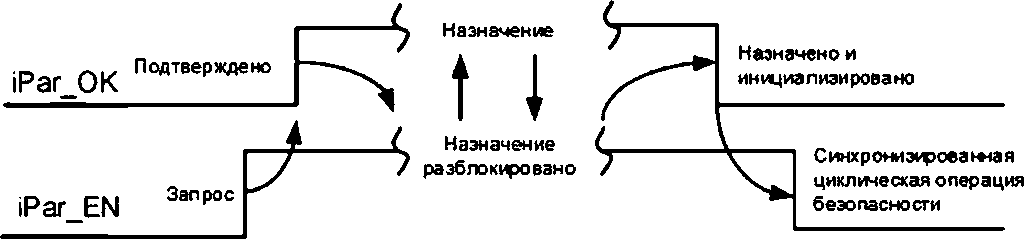


Рисунок 41 — Разблокировка F-хостом назначения (параметров

1. Управление коммуникационным уровнем безопасности
   1. F-параметр
      1. Перечень

Значения параметров усройсте CP 3/RTE в черном канале назначаются е 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
* F WD Time
* F WD Time 2
* F\_Prm\_Flag1 ♦ 2
* F\_Check\_SeqNr
* F\_Check\_iPar
* F\_SIL
* F\_CRC\_Length
* F\_Block\_ID
* F\_Par\_Vers»on
* F\_iPar\_CRC
* F Par CRC

«Кодовое имя» для взаимодействий отправителя и получателя:

Время сторожевого таймера Р-устройства/модуля (по умолчанию в файле GSD: максимальное время обработки F-устройства/модуля):

дополнительное вспомогательное время сторожевого таймера F-устройств/мо- дулей, спроектированных для «конфигурирования во время выполнения» или для «систем устойчивости к сбоям», чтобы расширить время контроля в случав запланированных обновлений, осуществляемых только авторизованным пер­ соналом I7-2.6.2);

Октеты параметра, содержащие несколько параметров для управления про­ филем:

Режим V2: порядковый номер должен всегда быть частью генерации CRC2: Применение, зависящее от производителя, для гомогенных систем; Проверка: сконфигурированный УПБ = примененному УПБ?

Длина CRC2;

Идентификация типа блока параметров;

Номер версии эксплуатационного режима F-napaMerpoa/FSCP 3/1;

Значение вычисления CRC (параметра, переданное хотя бы с помощью ручного управления от инструмента CPD программному инструменту;

Вычисление сигнатуры CRC1 по всем F-параметрам.

56

ГОСТ Р МЭК 61784-3-3—2016

* + 1. F\_Source/Destination\_4ddress (кодовое имя)

Адреса F-компонентов контура управления безопасности, таких как F-ееод. F-хост и F-еывод. должны быть точно выражены е 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 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 *OFFFFh* должны быть исключены. Параметр состоит из двух частей: «F\_Source\_Add» и «F\_Dest\_Add»: каждая часть является типом данных без знака Unsigned16.

* + 1. F\_WD\_Tlme (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 о\*- 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 зти 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 r\_WO\_Time для этой конкретной коммуникационной связи 1:1.

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

* + 1. F\_WD\_Time\_2 (вспомогательное время сторожевого F-таймера)

Это вспомогательное время сторожевого F-таймера может применяться по желанию для расши­ рения обычного времени сторожевого F-таймера до еще одного периода времени F\_WD\_Time\_2. необ­ ходимого для обновления F-устройств/модулей. как это показано на рисунке 42.

СВЗ: U$e\_T02

**PDU**

**безопасности от F-хоста**

**□□ □ 0 d □ □ □**

F WD Time F WD Time 2

Рисунок 42 — Эффект F\_WD\_Time\_2

Параметр F\_WD\_Ttme\_2 кодируется следующим образом: Unsigned16. Временная база: 1 мс.

Диапазон значений: от 1 до 65 535

* + 1. F\_Prm\_Flag1 (Параметры для управления уровнем безопасности)

8.1.5.1 Структура F Prm\_Flac1

Подразделы 8.1.5.2—8.1.5.5 подробно описывают октеты параметра F\_Pmn\_Flag1. Они обладают структурой, показанной на рисунке 43.

57

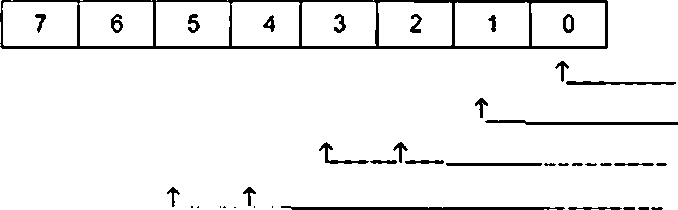
ГОСТ Р МЭК 61784-3.3—2016

т.

т

Рисунок 43 — F\_Prm\_F!ag1

F\_Check\_SeqNr F\_Check\_iPar F\_SIL

**F\_CRC\_Length**

**Зарезервировано см. 7.1.3, подсказки Зарезервировано- см. 7.1.3, подсказки**

8.15.2 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\_Ftag1».

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

без прэмрш (не придавать значения а резюме V2. в G$0 оолмио бе<тъ jxwa-o «ЫэСЬее\*»>.

проварка («а повжвт» « ретме V2. В OSO доило 6м п. усааачо «спаек»)

Рисунок 44 — F\_Check\_SeqNr

* + - 1. F\_Check\_iPar

Для обычного использования э то т параметр должен всегда быть установлен в значение «О». Он зарезервирован для использования, зависящего от производителя, в гомогенных системах. Этот пара­ метр не связан с механизмом inap-cepeep.

Он кодируется следующим образом: Бит 1 октета параметра «F\_Prm\_Flag1«.



0

1

Рисунок 45 — F\_Cbeck\_iPar

Нет лроеерш le GSO доляио быть указано

'МоСпдео

Проверка {иепольаоеэмм. mo hc suj oo от про«з»Ойиг«ля‘)

* + - 1. F\_SIL (стадия УПБ)

FSCP 3/1 разрешает параллельное функционирование как коммуникаций, имеющих значение для безопасности, так и стандартных коммуникаций. Разные функции безопасности, использующие ком­ муникации. имеющие значение для безопасности, могут нуждаться в разных уровнях полноты безо­ пасности (УПБ 1 ... УПБ 3). F-устройства способны сравнивать свой собственный назначенный УПБ и сконфигурированный УПБ (F\_S1L). Если он выше чем УПБ подсоединенного F-устройства/модуля, то устанавливается бит статуса «отказ устройства» и срабатывает реакция перехода в безопасное сос­ тояние. 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».

58

ГОСТ Р МЭК 61784-3-3—2016

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | в | 5 | 4 | 3 | 2 | 1 | 0 |
|  |  |  |  | 0 | 0 |  |  |
|  |  |  |  | 0 | 1 |  |  |
|  |  |  |  | 1 | 0 |  |  |

УПЬ 1 (eGSO оопямобыть дамио'уПБ t\*>

УП6 2 (о 6S0 аопммо быь утамно \*УП6 2’J УП6 3 (а ОЗО догмио Сьль yi\*»«o 'УП6 У)

1 1 УПБеГСуТСТаует(в<&>ДОжиобм1ьу>ИЬМО

* + - * + Мс6и»|- К|приы»р. • Pt>Tq»4cnM

Рисунок 46 — F\_SIL

* + - 1. F\_CRC\_Lenglh (длина сигнатуры CRC2)

В зависимости от длины F-да-жых 1/0(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-комлоненту ожидаемую длину сигнатуры CRC2 в POU безопасности.

Он кодируется следующим образом: биты 4 и 5 октета параметра «F\_Prm\_Flag1».



CRC кдексь а э октета <толь\*о а реамио W а CSD догмаовытьухамно '3-ByteCRC‘i

CRC подпись а 2 оггета (тогыю а рекмые VI а ОЗОдопхко быть унэапо ■2-Byie-CRC’)

|  |  |
| --- | --- |
| 0 | 0 |
| 0 | 1 |
| 1 | 0 |
| 1 | 1 |

CRC подпись «4 окг«тв (дополиитально • доомв V1SV2.Q OSD долм<обитъ утзаамв ‘4. вуй-СНС)

Зарюараироодио Сы 71 3. п о д«а»4

Рисунок 47 — F\_CRC\_Lenglh

* + 1. F\_Prm\_Flag2 (Параметры для управления уровнем безопасности)
       1. Структура F\_Prm\_Flac2

Подразделы 8.1.6.2—8.1.6.3 подробно описывают октеты параметра F\_Prm\_Flag2. Он обладает структурой, показанной на рисунке 48.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Т Т\_

т t т

? Т т

Зарезервировано: см. 7.1.3. подсказки

F\_BlockJO F Par Version

Рисунок 48 — F\_Prm\_Flag2

* + - 1. F\_Block\_ID (идентификация типа параметров)

Для того, чтобы выделить параметры для будущих режимов FSCP 3/1. идентификация типа пара­ метров «F\_BtockJD» кодируется следующим образом: биты 3. 4 и 5 октета параметра «F\_Prm\_Flag2» (см. рисунок 49). Проверка F\_Block\_tD является обязательной для уровня безопасности.

59

ГОСТ Р МЭК 61784-3.3—2016

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 0 | 0 | Нет F\_iPaf\_CRC. Нет F\_WO\_Time\_2 |
| 0 | 0 | 1 | F Par CRC (рисунок 51) |
| 0 | 1 | 0 | F\_WD\_Time\_2 (рисунок 42) Нот F\_tPaf\_CRC |
| 0 | 1 | 1 | F\_WO\_Tm\*\_2 и F\_#>ar\_CRC |
| 1 | 0 | 0 | Зарезервировано |
| 1 | 0 | 1 | ЗзосмрвирФммо |
| 1 | 1 | 0 | Зэрвюрвфсваио |
| 1 | 1 | 1 | Зарезервировано |
|  |  | Рисунок 49 — F\_Block\_lD |  |
| 8.1.6.3 F\_Par\_Version (номер версии набора F-параметров) Целью данного счетчика версий является идентификация | | | новых версий эксплуатационного |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

режима внутри уровня безопасности. В случае если запрошенная версия уровня безопасности не совпадает с реализованной версией, то F-устройство должно отвечать сообщением диагностики, ко­ торое зависит от устройства (см 6.3.2 и рисунок 50). Проверка подтверждения соответствия Р-пара- метров должна выполняться уровнем безопасности.



Действительно до реямиа VI (в OSD должно

1. 0 бить указано ‘Vl-moOe')

Дебета итвгъыо для ранимо V2 (о GSO должно быть укмаио V2-mooen

0 1 -

1. 0 - Зарезервировало см 7.13, пмекаош

1 1 Зарезервировано си *7*1.3. подскажи

Рисунок 50 — F\_Par\_V®rsion

* + 1. F\_iPar\_CRC (значение iPar.CRC для всех {параметров)

После успешного сеанса гараметризации и ввода в эксплуатацию инструмент CPD определенного F-устройства вычисляет сигнатуру CRC (iPar\_CRC) для всех {параметров. Каждый раз. когда вычисления выдают «0». значение должно быть установлено равным «1». Значение в шестнадцатеричном формате должно передаваться, хотя бы спомощью ручного управления, программному инструменту и назначаться полю записи «FJPar\_CRC».

Данный параметр передается P-устройству во время запуска и служит для проверки на непроти­

воречивость {параметра 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.S) F-устройства. В таком случае F-устройство пропустит проверку на непро­ тиворечивость. 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 присутст­ вие. Он кодируется как: Unsigned32

60

ГОСТ Р МЭК 61784-3-3—2016

* + 1. F\_Par\_CRC (CRC1 для всех Р-лараметров)

Программный инструмент генерирует эту сигнатура CRC1 для всех F-параметров. Начальное зна­ чение для CRC1 равно 0. Подробности о порядке Р-параметров для использования в генерации сиг­ натуры CRC1 см. в 8.3.3.2. Используется такой же 16-битный CRC полином (14£A8h). CRC1 является начальным значением для циклического расчета CRC2.

Следующие правила применимы для разных полиномов CRC2:

* В случае 24 битного полинома CRC (15D6DCSh) начальное значение для вычислений CRC2 равно «ООхххх». где xxxx=CRC1.
* В случае 32 битного полинома CRC (1*F4ACFB13h*) начальное значение для вычислений CRC2 равно «0000хххх», где xxxx=CRC1.

Он кодируется как: Uns»gned16.

* + 1. Структура объекта записи данных (record data object) Р-лараметра

F-параметры

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| F\_Prm-B)ock | | Заголовок кои кратного | | I Возможен c CP I 3/1 И CP 3/2. не  > возможем с  [ профилями c CP I 3/4 По CP 3/6 |
| F\_Parameter | | 0 | F\_Prm\_Rafll | Unaigned8 |
| 1 | F\_Prm\_Rag2 | Unsigned8 |
| 2 | F Soiree Add | Unsignedi6 |
| 3 | |  |
| 4 | F\_Dest\_Add | Unsignedie |
| 5 | |  |
| 6 | F^VWD.Time | Unsignedie |
| 7 | |  |
| Пополнительно |  | в | F\_V\0\_Time\_2 | Unsignedie |
| 9 | |  |
|  | 10 | FjPar^CRC |  |
| Дополнительно | 11 | | Urwgned32 |
| 12 | |
|  | 13 | |  |
| End\_F\_Prm-Bock | | 14 | F\_Par\_CRC | Unsignedie |
| 15 | |

Рисунок 51 — F-парамегр

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-BnoK (рису­ нок 13). Присвоение подмодуля Р-устройству происходит в выбранном номере подслота.

* + 1. Доля F-данных См. 7.1.6.

61

ГОСТ Р МЭК 61784-3.3—2016

* 1. (Параметр и IPar.CRC

F-устройстеа асе чаще обеспечиваются интеллектуальными функциями, которые требуют назна­ чения неограниченных индивидуальных значений параметров F-устройстеа. Эти. связанные с безопас­ ностью. параметры именуются параметрами. 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 скам- неров 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 (параметров для целей загрузки и скачивания. Абсолютный веркний предел для (параметров это 222-1 октетов; нижний предел это 4 октета. Таким образом, каждый раз. когда общая сумма превышает 240 октетов, для СР 3/1 требуется сегментация, как это показано на рисунке 52. Для CP 3/RTE сегментация не требуется.

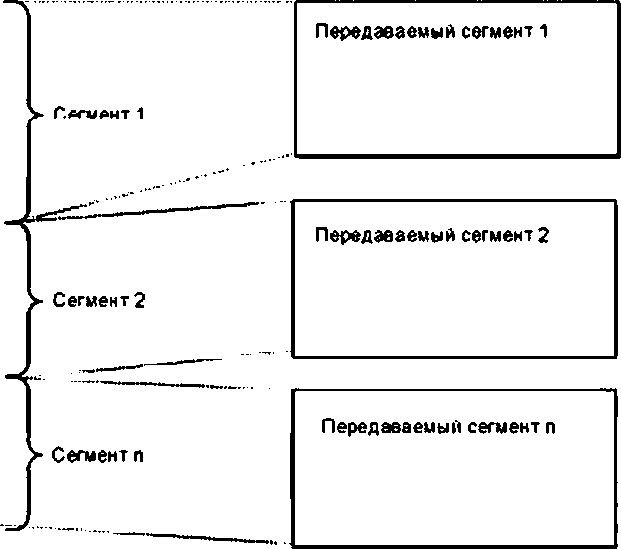
Сигнатура CRC («(Par\_CRC#) должна вычисляться для всех (параметров (рисунок 52) при помощи любого подходящего CRC полинома, заполнять 4-октетный iPar\_CRC в шестнадцатеричном формате и отображаться на СРО-Инструменте. Каждый раз, когда вычисления выдают «0». должно быть установлено значение «1». Включение значения iPar\_CRC в (параметры, как это показано на рисунке 52. является не обязательным. При использование 32-битного CRC полинома для профиля FSCP3/1 не требуется никакого вычисления достаточной частоты возникновения остаточных ошибок для подтверждения безопасности.

Связь F\_source/destination (кодовое имя) позволяет проверять доставку сконфигурированному

получателю. Включение (параметров, как это показано на рисунке 52 не обязательно.

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

Длина блока (параметров иожет пригодиться для эффективной организации процессов загрузки и скачивания, осуществляемых в устройствах. Включение в (параметры, как это показано на рисунке 52. не обязательно.

>Pat\_CRC • CRC в сумм\* из 4 октетов (дологмиельно)

F\_Soirce/Oest\_Add (Дополнительно) ИТО Функции 1допол»н\*льио) Длина в октетах (допогеителью)

'параметр (максимум 2®-1 октетов)

\*) Сегментация с грофплягум СР ЗЛ и СРЗ/2 когда обще\* число октет превышает 240 В случае профилей с СР 3/4 по СР 3/6 сегментация отсутствует

Рисунок 52 — Блок (параметров

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

62

ГОСТ Р МЭК 61784-3-3—2016

* 1. Параметризация безопасности
     1. Цели

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

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

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

Небольшой набор идентичных F-параметров. проходя через все различные F-устройстеа. пере­ дается 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 свя­ занные с этим усилия по одобрений этой версии конфигурационной частью сети.

После проведения настройки F-параметров. которая осуществляется во время конфигурирования сети, составляется запись F-napaMe~pa и помещается на хранение в F-хост/Ю-коитроллер для запуска сети.

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

* + 1. 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 ИС0 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-парэметроа и структур F-l/O

|  |  |
| --- | --- |
| Ключевое слово GSDL | Описание |
| F\_Ext\_Module\_Prm\_Data\_Len | Параметр, ассоциированный с этим ключевым словом, указывает на общую длину F\_Prm-BnoKa. показанного на рисунка 51. которая состав­ ляет. как правило. 14 или 18 октетов, в зависимости от F\_iPar\_CRC |
| F\_Ex1\_Module\_Prm\_Dala\_Consl (offse) | При помощи параметра, ассоциированного с этим ключевым словом, фиксированное значение может быть введено в один из 4 октетов заголовка F\_Prm-EnoKa. показанного на рисунке 51. На позицию октета  указывает сдвиг 0...3 |
| F\_Ext\_Module\_Prm\_Data\_Const (0) | Указывает на длину F\_Prm\_Btock. включая F-iPar\_CRC. например. 0x12 |
| F\_Ext\_Modu!e\_Prm\_Data\_Consl (1) | Идентификация F\_Prm-Блока = 5 (fix) |
| F\_Ext\_Module\_Prm\_Data\_Const (2) | Слот F-модуля |
| F\_Exl\_Modute\_Prm\_Data\_Const (3) | Зарезервировано. Должно быть установлено значение «0». |
| F\_Exl\_Module\_Prm\_Data\_Rel (offset) | При помощи параметра, ассоциированного с этим ключевым словом, ео время конфигурирования значение выбранное пользователем может быть введено в один изоктеговО... 13 F\_Prm-BnoKa. показанного |

63

ГОСТ Р МЭК 61784-3.3—2016

*Окончание* таблицы 9

|  |  |
| --- | --- |
| Ключевое слово 6S0L | 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 GSO |
| 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. 6.3.3.3 |
| 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\_StructufeQescVersion | Параметр, ассоциированный с ключевым словом, указывает на версию описания структуры F- данных I/O. Значение 1 указывает на 16-битную силчатуру CRC7. а значение 2 указывает на 32-битную сигнатуру CRC7. Если этот атрибут отсутствует, то предполагается значение 1 |

Рекомендуется структурированная параметризация. Дальнейшие расширения GSDLc m. в 8.6.4.6.

* 1. 2.2 Расширения GSDML

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

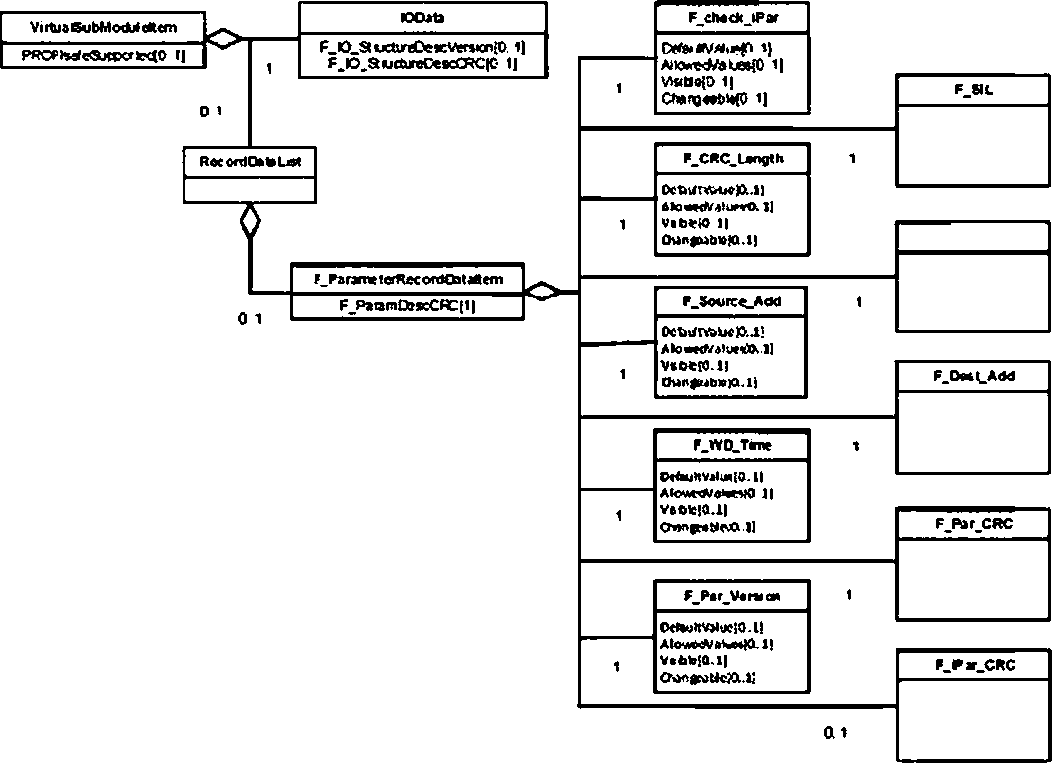


Рисунок 55 — Расширение F-парамегра в спецификации GSDML

64

ГОСТ Р МЭК 61784-3-3—2016

На рисунке S3 показаны расширения в GSDML. Секция «VirtuaiSubmoduieltem» (элемент вирту­ ального подмодуля) предоставляет дополнительный атрибут «F.ParamDescCRC». Это CRC сигнатура (CRC0) описания F-параметра на рисунке S3. «F\_lO\_StructureDescCRC» в секции «lOData» закрепляет форматы данных F-ввода и F-вызода. «F\_10\_StructureDescVereion» указывает на версию описания структуры данных FJO (см. 8.3.3).

* + 1. Защита параметров безопасности и данных GSO
       1. Общие положения

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

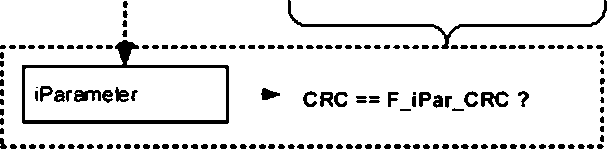
Для того чтобы предотвратить использование программным инструментом зашумленных данных описания устройства (GSD), части этих данных, важные для безопасности, также защищаются с помо­ щью CRC сигнатуры.

* + - 1. 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*4EABh.* Сигнатура *CRC1* строится для всех F-пара­ метров в порядке октетов, показашом на рисунке 51. исключая дополнительный F\_iPar\_CRC. Каждый раз. когда бит 3 F-параметра «F\_Btock\_ID» устанавливается в значение «1» сигнатура F\_iPar\_CRC должна включаться в начало вычисления, как это показано на рисунке 54.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| •  1  CPD инструмент | | iParameier | ► | iPar\_CRC | * MUMUimniCiiDrv * F\_Block\_ID, Bit 3   a | = 1 |
| 1 | • |  |  | a |  |
|  | •  а  а а а |  | а а  **Т** |  |  |
| \*в  \*  Программный инструмент • | |  | FJPar.CRC | IParameier | CRC1 |

F-устр ой ств о/ модуль

Вюунок 54 — CRC1, включая iPar\_CRC

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

* + - 1. CRC0 для данных GSD

Для того чтобы гарантировать, что параметры F-устройства. важные для безопасности, не пре­ терпевают незаметных изменений в течение жизни накопителя и могут безопасно считываться в ин­ струмент конфигурирования, все эни защищаются с помощью CRC. Параметр «F\_ParamDescCRCn 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 (СР 3/1 или СР 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-параметроа в описании «ExtUserPrmData» и в выбранных секциях «PrmText». Псевдо­ код на рисунке 55 показывает алгоритм того, как генерируется 2-октетный CRC0. являющийся практи­ чески независимым от структуры GSO файла и комментариев, тем самым, наделяя проектировщика файла максимальной свободой и возможностью вносить изменения.

Подчеркнутые символы включены в вычисление.

65

ГОСТ Р МЭК 61784-3.3—2016

**«Каждв» F\_Exi\_Us\*r\_Prm\_0\*U\_Ref{x) одна** *за* **другим в поредев возрастай!» (байтовый сдвиг битовый с дв уг }**

**•тзвгопэвок F\_Prm-Blod<mtopvpy«TCfl**

**tor(F Par RafsChF Para Ref«numberofelements,F Pare Ret\*-\*)**

<

if(li\*lp«fjnieter==TRU;)//PrmT«xl хотя бысдвумявыборгакм

{

*U* в случае F-пз par\* трое с определениям\* “АгтТехГ

* + - * + читать ^^соответствующего F\_Parameter
* нагример, ExlUsorPimDala \* 8 "F CRC Lcoaft"
  + - * + читать формат данное (0 Bit. 1: Un»sned8. 2 Unsign ей1б. 3 Unsgned32) читать битовый q\*»r (0 jf Ure»gred8>Uns«gn«J16/Un6igried32j

*•t* налрьмер ilArea(4-5)0i>2

«читать зна^еже no умзлчажю(Lo&/te, HiByle)

*О* например. 3itArea{4-S) *Q* 0-2 now reed corresponding PrmTexT via thetext selections жгргмерЧтТ©с1 = 3

*U* ТекТ(О) • "3-Byt«\*-CRC‘

*H* TextQ) • "2-BvteCRC'

*»* TexlC2) • "4-Bvte-CRG"

ErdPrmTel

fer (value \*C. value <\* Max (Prmlexl). value +♦)

<

->0. 4

**•XX 0**

)

else

* «ттвть фа кпнеекое значение как текст

.• ю гример -»'3-Byte-CRC‘

* «тать фактическое значение как номер (ждехс} (LoByte. HiByte)

.«пример -XX О

}

а случае F-пареметровсподемт редактирования

*{*

читать жичеиоеа же соответствующего F\_Paremeter в парадке воарастанж

«npm^.ExtLherPimDaia ■ 2\*£^2tiLflfld‘

. ' читать формат данных (0: at 1 ur&grtedB, 2: Unsjgned16.3 Unstgnea32)

.v читать сдое Битое (0 если Unsign ed8<Unsignedi6'Unsigned 32) hanpiT^ee Unaipnadlfi 1 1-65534 ->2,0 читать зныеже no yMorNaHmolstaflhgwith loByle)

Uneignediei 1-05634 -Л.О

*■>* читать ж»\*ий гредеп (>«чии\*я с LoByte)

л' Uratpredie 11-65534 -\*1.0

*и* читать вергжй предел (ж ж на» с LoByte)

**л-Une>enedlS 1 t-ffiSy ->254.255**

}

)

* ' Конец алгоритме

Рисунок 55 — Алгоритм построения CRC0 (GSDL)

Для получения образцов GSD файлов для F-ввдомых устройств (СР 3/1 или СР 3/2) следует обра­ титься к организациям, приведенным е приложении В.

В случае файла GSD для F-устройства (СР 3/RTE) вычисление 2-октетной сигнатуры CRC осу­

ществляется во всех секциях F.ParameterRecordDataltem (рисунок 53). включая все F-параметры и их определения. Псевдокод на рисунке 56 показывает алгоритм построения CRC0 практически независи­ мого от структуры и комментариев файла GSD, что наделяет проектировщика файла максимальной свободой проектирования и возможностью вносить изменения без конфликтов.

П р и м е ч а н и е — Некоторые F-параметры могут быть установлены как невидимые а файле GSO для устройств СР 3/RTE. что выполняв'ся с помощью установки Visible (Видим) = «false». F-параметр не будет учиты­ ваться в вычислении CRC0 в случае Visible = «false».

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

66

ГОСТ Р МЭК 61784-3-3—2016

while (F Parameter to read(0

<

секции F\_Parame6eiPecof0OalaKtai делима читать e пор ваге вожастанхя (байтовый сдвиг, битовым сдвиг).

*а* Наихемзвамие F-параметра

*t:* ОаСаТуре F-параметра (0: Bil / ВсЛгса. 1. Uns>gned8. 2. Unsigned 16. 3 Urwifyied32>

*и* BitORsel F-параметра (0 если Unsigned №UnsignedieAJn»>gne632)

*И* читать DefauKVaiue (Начиная с LoByte. два байта для битов ьа параметров. Unsigned8. Unsigned 16. четыре байта для Unsigned32)

if (value range}# Попе ред акт кроет ни я и гм параметр списка, соде ржа ими тотыс одно значеше

<

*;/* читать 1уто цифру AtonedVHue (точимая с LoByte Lowefbmil)

'.'читать 2у«цифру ABowedValue (•в-иил с LoByto Upperbmil)

)

dse *t)*Перечтсшть параметры, содержащие хотя бы две тестовые выборки

<

*II* дл> сажа ого AilowedValue я AliowedValueLisI: читать текстовое описания AllowedValue

*It* символ за символом, а а затем соответствующие числовые значения (LoByte. HiByle)

)

*//*конец алгориыа

Рисунок £6 — Алгоритм для построения CRCO (GSDML)

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

* 1. Конфигурация безопасности
     1. Защита описания данных безопасности I/O (CRC7)

Структура F-данных I/O описана в секции «lOData» файла GSO. Один из атрибутов это \*F\_IO\_ StructureDescCRC» = CRC7. CRC7 строится для всех атрибутов в таблице 10 в том порядке, е котором они перечислены (версия 2). Для вычисления сигнатуры должен применяться 32-битный CRC полином *(lF4ACFB13h).* Разрешенные типы данных для FSCP 3/1 перечислены е 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 (14ЕАВЛ). а длина сигнатуры CRC7 составляет 2 октета.

Параметр «FJO.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 струк­ туры данных I/O |
| IN.ADDRESS.RANGE | 2 октета | Длина в октетах всей секции lOData Input (включая F\_MessageTrailer) |
| COUNT\_PS\_!NPUT\_BYTES\_COMPOSITE | 2 октета | Ввод. Дгына всех элементов данных типа  «Float32+Unsigned8» {5 х число элементов) |
| COUNT\_PS\_lNPUT\_BYTES\_U8\_U8 | 2 октета | Ввод. Длина всех элементов данных типа  \*Unsigned8+Unsigr>e(i8» (2 х число элементов) |
| COUNT\_PS\_INPUT\_CHANNELS\_BOOL\_MAX | 2 октета | Ввод. Число всех булевых каналов («используется в качестве битое») в режиме максимума (например, в режиме 1оо1) |
| COUNT\_PS\_INPUT\_BYTES\_BOOL\_M4X | 2 октета | Ввод. Длина всех булевых элементов данных (в окте­ тах) в режиме максимума (например, в режиме 1оо1) |
| COUNT.PSJNPUT.CHANNELSJNT | 2 октета | Ввод. Число всех элементов данных типа Integer 16 |

67

ГОСТ Р МЭК 61784-3.3—2016

*Окончание таблицы 10*

|  |  |  |
| --- | --- | --- |
| Имя атрибута | Длина | Описание |
| COUNT\_PS\_INPUT\_CHANNELS\_DINT | 2 октега | Ввод. Число всех элементов данных типа Integer32 |
| COUNT\_PS\_JNPUT\_CHANNELS\_REAL | 2 октега | Вв о д . Чи с ло всех элементов данных типа Ftoat32 |
| OUT\_ADDRESS\_RANGE | 2 октега | Длина в октетах всей секции lOOata Output (включая F\_MessageTraler) |
| COUNT\_PS\_OUTPUT\_BYTES\_COMPOSITE | 2 октега | Вывод. Длина всех «Float32+Uns«gned8» Элементов- Данных (5 х число элементов) |
| COUNT\_PS\_OUTPUT\_BYTES\_U8\_U8 | 2 октега | Вывод: Длина всех « Unsigned8+Unsigned8» элемен­ тов данных (2 х число элементов) |
| COUNT\_PS\_OUTPUT\_CHANNELS\_BOOL | 2 октега | Ввод. Число всех булевых каналов («используется в качестве битс»») |
| COUNT\_PS\_OUTPUT\_BYTES\_BODL | 2 октега | Вывод: Длина всех булевых элементов данных (в октетах) |
| COUNT\_PS\_OUTPUT\_CHANNELS\_INT | 2 октега | Вывод. Число всех элементов данных типа Integer16 |
| COUNT\_PS\_OUTPUT\_CHANNELS\_DINT | 2 октета | Вывод. Число всех элементов данных типа tnteger32 |
| COUNT\_PS\_OUTPUT\_CHANNELS\_REAL | 2 октега | Вывод. Число всех элементов данных типа Float32 |
| DATA\_STRUCTURE\_CRC | 4 октега | \*F\_IO\_StructureOescCRC» = CRC7 |

* + 1. Примеры секций типа данных Dataltem
       1. Подход

Подразделы 8.4.2.2—8.4.25 содержат примеры секций Dataltem в соответствии с некоторыми ти­ пами 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].

* + - 1. FJN\_OUT\_1

Ввод: 32-битовый логический. Вывод: 32-битовый логический.

Пример кодирования секции Dataltem для F\_Channel\_Driver FJNjDUT\_1 показан на рисунке 57.

Таблица 10 содержит описание переменных.

|  |  |
| --- | --- |
| <юоав> |  |
| <ЮОа»: |  |
| <input C«mtStBA«y^AKiMaM («пИНажУ» |  |
| <Оа14М<П OataTyo»=\*Wntitn\*dSr UWA»IB£\*I>im' Toi1d:’\*ip«U'/> | |
| <OaiM«m DaiaTrt»oz~f \_ы»ыя\*Тгаа>>4вуы’ Тывв^ЫМ/ *t>* | |
| <Ouiput Corals Hncys'Atitaim юмМапсУ? |  |
| <Oaiaa«<n DaiaT>'pe='unt<t»«dsz' им А«в>в ;\*««»• Taifd^Owipatt\* *f>* | |
| «OalMem ОМаТума\*Г.М«»ма\*Т'«1»14атН\* Т«»ввг\*А»1«у’> | |
| <лооаь>‘,оыеи> |  |
| VERSION 02 | 02 |
| IN ADORESS RANGE 08 | 08 |
| COUNT PS INPUT BYTES COUPOSITEOO | 00 |
| COUNT PS INPUT BYTES US U8 00 | 00 |
| COUNT PS INPUT CHANNELS BOOL 32 | Э2 |
| COUNT PS INPUT BYTES BOOL 04 | 04 |
| COUNT PS INPUT CHANNELS MT 00 | 00 |
| COUNT PS INPUT CHANNELS ONTOO | 00 |
| COUNT PS INPUT CHANNELS REALOO | 00 |
| OUT ADDRESS RANСE 08 | 08 |
| COUNT PS OUTPUT BYTES COMPOSITE 00 | 00 |
| COUNT PS OUTPUT BYTES U8 USOO | 00 |
| COUNT PS OUTPUT CHANNELS BOOL 32 | Э2 |
| COUNT PS OUTPUT BYTES BOOL 04 | 04 |
| COUNT PS OUTPUT CHANNELS INT » | 00 |
| COUNT PS OUTPUT CHANNELS DMT 00 | 00 |
| COUNT PS OUTPUT CHANNELS REAL 09 | 00 |
| OATA STRUCTURE CRC 0к9Е8Е«Э2в | 0к9ЕВЕЯ32в |

Рисунок 57 — Секция Dataltem для F\_IN\_OUT\_l

68

ГОСТ Р МЭК 61784\*3-3—2016

* + - 1. FJN\_OUT\_2

Ввод: 16-6итоеый логический. 16-битовый целочисленный. Вывод: 1 байтовый логический. 16-битовый целочисленный.

Пример кодирования для F\_Channel\_Driver FJN\_OUT\_2 показан на рисунке 58.

|  |  |  |
| --- | --- | --- |
| «ЮОаа» | <lnpul Consiilcney:\*AI>t\*a» ccmnt\*<K/> |  |
|  | «Oaatam Оа1аТур»:\*им||м41\*‘ | UAOA\*BiB :\*№«•\* Texdd:\*«iput»\* *»* |
| <OsUKem Оа1аТ>с»:\*Ы<|«>М\* UsaAtBi»:\*MM\* Твх1№\*А1с1иппаГ *t>* | | |
|  | «Oautem OauTypevj\_M«»\*saio\*«r«ayt«‘  «•input»  «Output ConaHWncy:\*AI>t«Bt comht«iKy\*> | Taxtids'bfety\* *f>* |
|  | «OiiaUm OaiaTypaz'uufeMdii\* | UaaAsBittx'Pvd\* Texdd\*\*<Mpvb\* f\* |
| «Oaatam ОаиТуро:’Ыч«'>4' имА«В4»:\*ГМи\* TtxBdx'AO chtnnN" 1»  «Oaatam Оа1аТур\*г'(.м«>«р\*1ги1н>«\*ум\* т exflex\* Wat/ *i>* | | |
| «^Output» | | |
| «<№Oe«> | | |
| VERSION | | 02 |
| IN.ADORESS .RANGE | |
| os |
| COUNT PS INPUT BYTES COMPOSITE | | 00 |
| COUNT PS INPUT BYTES US US | | 00 |
| COUNT PS INPUT CHANNELS BOOL | | IS |
| COUNT PS INPUT BYTES BOOL | | *02* |
| COUNT PS INPUT CHANNELS INT | | 01 |
| COUNT PS INPUT CHANNELS OMT | | 00 |
| COUNT .PS JNPUT.CHANNELS.REAL | | 00 |
| OUT ADORESS RANOE | | OS |
| COUNT PS OUTPUT BYTES COMPOSITE | | 00 |
| COUNT PS OUTPUT BYTES US US | | 00 |
| COUNT PS OUTPUT CHAAHELS BOOL | | IS |
| COUNT PS OUTPUT BYTES BOOL | | 02 |
| COUNT PS OUTPUT CHAWELS INT | | 01 |
| COUNT PS OUTPUT CHAW1ELS OMT | | 00 |
| COUNT\_PS\_OUTPUT\_CHAM4ELS. REAL | |
| 00 |
| OATASTRUCTURE CSC | | OxS22SS330 |

* + - 1. FJN\_OUT\_5

Рисуюк 58 — Секция Datallem для F\_IN\_OUT\_2

Ввод: Составной (Float32+Unsigned8).

Пример кодирования для F\_Channel\_Drive F\_IN\_OUT\_5 показан на рисунке 59.

<ЮОав>

<1пр4 СОПМВЛ eys'AlhMm\* <oniittan(Y\*>

«Dataltem 04(aTtM:\*HoM32»«lm\*iwd(’ T6i\*d:\*AI cb4iw>\*<’ *l>*

«Datallem ОаиТура:'Г\_М«»\*Ч«1г«\*а14#у1\*\* T<udd:'S«t\*ty\* *»*

«ли*tu>*

<OUpulCenMBncya\*AlliMm<oi»ht«iuv’>

«Datallem OataTypaa\*r\_M«»wa«i'\*fe'Mri\*\* *»*

«/Output»

«>100ва>

VERSION IN ADORE S3 RANGE

COUNT PS INPUT BYTES COMPOSITE

co unt 'ps'input ~c hannel s BOOL

co unt .ps ]input ~8yt e8\_bo 6l

COUNT PS INPUT CHANNELS INT

co unt ps'input 'c kannel s'r eal

OUT AO ORE SS RANGE COUNT PS OUTPUT BYTES COMPOSITE

co unt 'ps'o ut put 'c haw el s BOOL co unt ‘ps'o ut put 'byt es boo l co unt 'psJo ut put 'c kakmeis\_ int

COUNT PS OUTPUT CHAM4ELS REAL DATA. STRUCTURE .CRC

01

09

09

00

00

00

00

04

00

00

00

00

00

OxSCAC

Рисунок 59 — Секция Datallem для F\_IN\_OUT\_5

69

ГОСТ Р МЭК 61784-3.3—2016

* + - 1. FJN\_OUT\_6

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

Пример кодирования для секции Dataltem для F\_Channel\_Driver F\_IN\_OUT\_6 показан на рисун­ ке 60. Таблица 10 содержит описание переменных.

«ЮОав»

«Input Consetenc^'AB items consistency\*»

«DatStam DetdType\*\*Float32\*Unsig»ed&\* Textl d=\* Al cha nnd' *f>*

«Datalem DataType=\*Urui\*r»ed8’ UseAs8iS="f\*be~ Textld-\*St»tujr *f>*

«Datalem DataTypes‘Uniigned8’ UseAs8itSs"f»be" TextldB\*St«tus2'/>

«Catalan DataType=\*Unsignede’ UseAs8itSi\_fabe' Textld=\*St\*tus3’ *f>*

«Datalem DataTypea’F\_MesufeTrailer4Byte\* TextJd^Sefety\* /»

«/Input»

«Output Conelstencya\*AII items consbtencV»

«Catalan DataTypes\*Flost32+Unsig»ed8\* UseAs8ltS="false"Texdda\*A0 channel\* .»

«Catalan DetaTypea\*F\_MesssgeTrailer4Byte\* Texdd=\*Safety' />

«/Output»

«/lOData»

|  |  |
| --- | --- |
| VERSION | 01 |
| IN ADDRESS RANGE | 12 |
| C6UWT\_PS\_INPUT\_BYTES\_COMPOSITE | 05 |
| COUNT PS INPUT CHANNELS 800L | 24 |
| COUNT PS INPUT BYTES BOOL | 03 |
| COUNT J>SJNPUT\_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 I NT | 00 |
| COUNT\_PS\_OUTPUT\_CHANNELS\_ REAL | *QO* |
| DATA\_STRUCTURE\_CRC | 0xF33 |

Рисунок 60 — Секция Dataltem для F\_IN\_OUT\_6

* 1. Использование информации типов данных
     1. Драйвер F-канала

F-данным I/O. циклически передающимся между F-устройством и F-хостом (канал реального вре­ мени). требуется управление посредством пользовательской программы. Программист либо ожидает появления надлежащих Функциональных блоков («драйвера F-канала») в его/ее (программиста) библи­ отеках инструментов, которые она/он способен встроить в программу клиента. Либо она/он ожидает по­ лучения 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».

* + 1. Правила для стандартных драйверов F-канала

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

* структура данных в секции lODataSection файла GSD. Подробное описание см. в 8.3.2;
* сформированная структура данных должна иметь следующий порядок: сначала все смешан­ ные типы Float32 + Unsigned8. если таковые доступны. Затем все переменные типов Unsigned8, Unsigned16, Unsigned32. если таковые доступны. Затем все переменные типа lnteger16. если таковые доступны. Затем все переменные с плавающей точкой, если таковые доступны.

70

ГОСТ Р МЭК 61784-3-3—2016

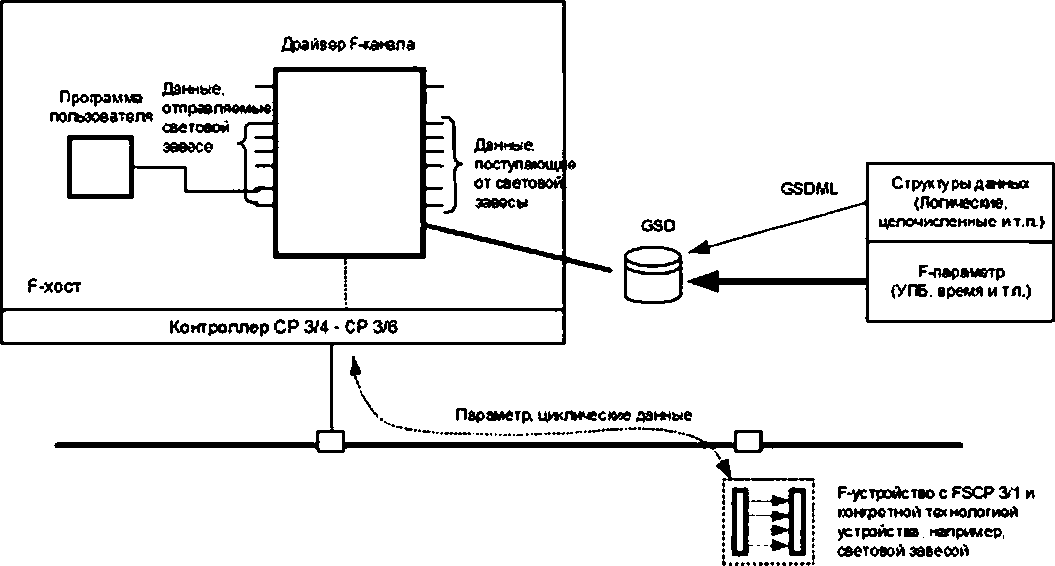


Рисунок 61 — Драйвер F-канала в качестве «клея\* между F-устройстэом и пользовательской программой

Таблица 11 содержит список образцов драйверов F-канала. Драйвера представляют собой раз­ ные структуры данных для F-ввода и F-еыеода. 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-битоеые на тип данных Uneigned8. Подробности см. е 8.4.2.

Таблица 11 — Образцы драйверов F-канала

|  |  |  |  |
| --- | --- | --- | --- |
| Конфигурация  драйвера F ••i-eno\*' | F-веод (устройством) | F-аывод (для устройства) | Замечания |
| F\_IN\_OUT\_1 | 32 логический | 32 логический. | например, световая завеса |
| F\_IN\_OUT\_2 | 16 логический. 1Integer16 | 16 логический. 11nteger16 | например, лазерные сханквры |
| F\_IN\_OUT\_5 | 1 Floa(32. Unsigned8 (В-биговьы  «квалификатора) |  | например, датчик избыточного давления |
| F\_IN\_OUT\_6 | «обратное считывание»: 1 Float32. 8-битовый «обратнаяпроверка»: 24 бита | «Уставка»: 1 F!oat32, 8 бит | например, пневмоклзлан |
| w He обязательно, что нумерация подразумевает различные драйверы. Это может быть один драйвер,  параметризованный посредством GS3 информации. | | | |

Ограничения:

* неиспользованные биты должны быть установлены е значение «0»:
* индикаторы статуса и сбоя F-устройства должны быть определены в структуре данных ввода, если зто необходимо (например, квалификатор).
  + 1. Рекомендации для драйверов F-канала

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

71

ГОСТ Р МЭК 61784-3.3—2016

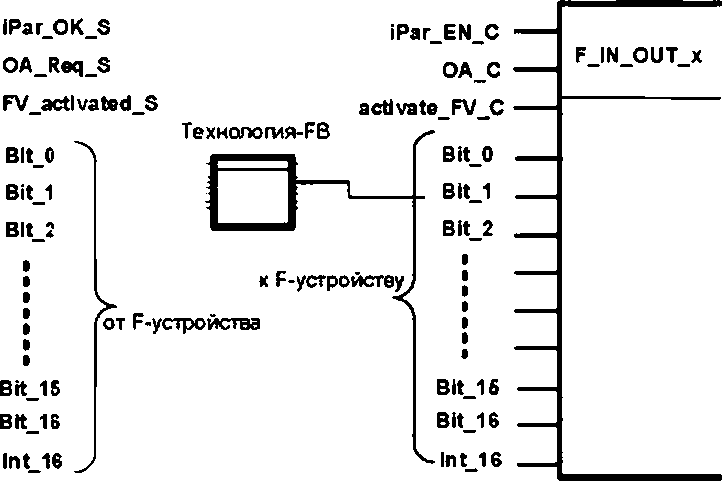
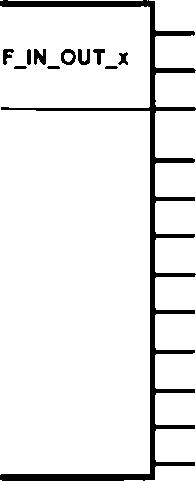


Рисунок 62 — Пример макета драйвера F-канала

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

iPar\_EN\_C iPar\_OK\_S ОА\_С

OA\_Req\_S

FV\_activateO\_S

activate\_FV\_C

Фиксированное поведение драй­ вера F канала

* включена (параметризация;
* Параметризация завершена;
* подтверждение оператора (для возобновления после сбоя);
* когда сбой (сторожевого таймера. CRC, порядкового номера) был обнаружен и удален.
* отказоустойчивые значения, активированные F-устройством;
* отказоустойчивые значения, которые будут активированы в F-устройстве:
* отказоустойчивые значения, установленные в «О».

В дополнении кструктурам 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 функцио­ нальных блока, один для вводов, а другой для выводов (рисунок 62). Существует фиксированное пове­ дение драйверов F-канала применительно к отказоустойчивым значениям: независимо от того состоит ли структура данных из битов (Unsigned8), Integer16. Floal32 или Float32 + Unsigned, каждое значение устанавливает в «О». Если исполнительные устройства не могут согласиться с FV = «О», то могут быть реализованы другие значения, либо с жесткой кодировкой, либо посредством Параметров. Пользова­ тельские 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 = «О», то допол­ нительная логика пользовательской программы может преобразовать их в индивидуальные значения, используя ввод «activate\_FV\_C\* драйвера F-канала.

72

ГОСТ Р МЭК 61784-3-3—2016

* 1. Механизмы назначения параметров безопасности
     1. Назначение F-параметров

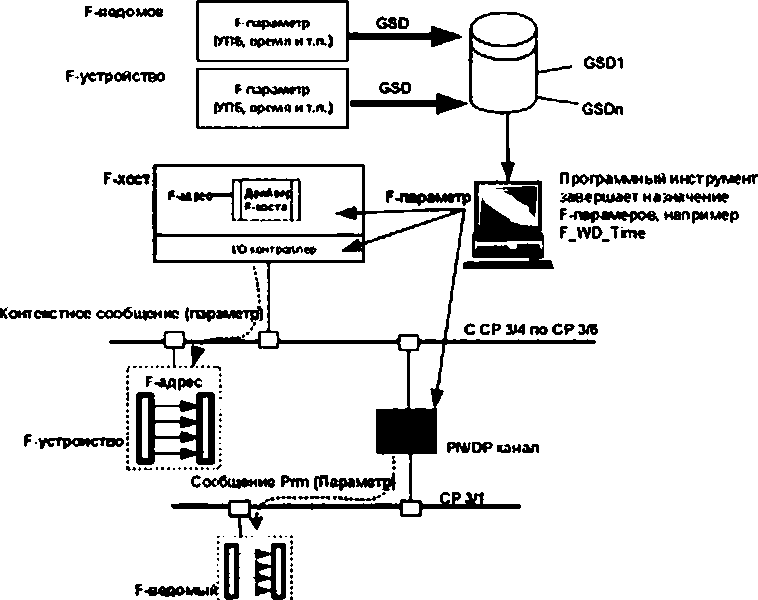


Рисунок 63 — Назначение F-параметров простым F-устройсгвам и F-ведомым устройствам

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

* + 1. Общее назначение {параметров

Для сложных устройств с {параметрами должно быть принято решение (по вопросу безопасности)

буЛАТ ПИ ЛАТПиЯТИЧАПКАА МЯ/ШЯЧАМИА При 1ЯЛуПКА ПрАДГЮЧИТЯТКГЯ ОТДАПКИПМу МЯТначАНИЮ. ПЛуЩАСТАПЯ-

емому СРО-инструментом для определенного F-устройства. как это предлагается в МЭК 62061. В любом случае F-хост должен разблокировав назначение только, если не наблюдается опасное состояние про­ цесса (7.4.2). В основном возможны два способа, которые могут содействовать друг другу:

* + присвоение значений {параметров посредством специальных прокси функциональных блоков в F-хосте и подходящего набора данных {параметров:
  + присвоение значений {параметров посредством специального СРО-инструмента через Ю-супер- виэора (программный инструмент/РС).

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.

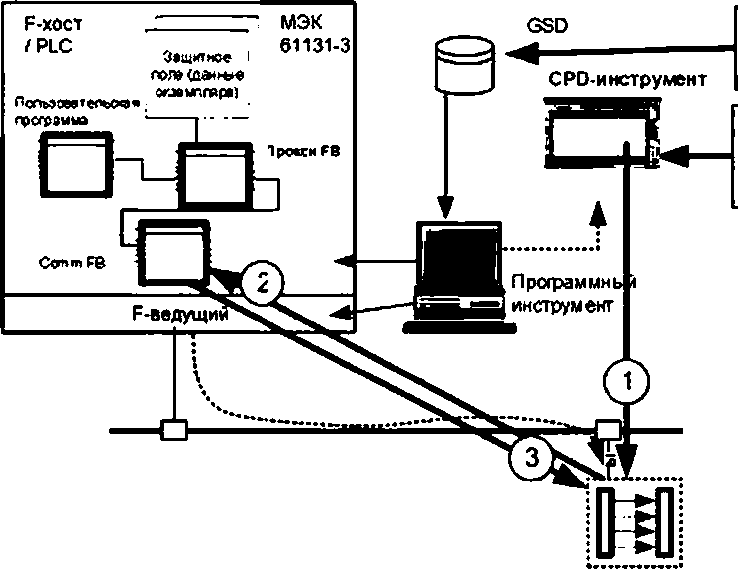
Производителям F-устройства дана возможность предоставить портативное программное обеспе­ чение управления для их устройств.

На рисунке 64 представлен пример того, как стандарты CPF 3 могут использоваться для предостав­

ления очень комфортной и гибкой поддержки системы для F-устройств. Специализированный СРО-инстру- мент 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 по­ левой шине, с циклическим обменом данными. После параметризации и ввода в эксплуатацию. Прокси Функциональный Блок может быть активирован для загрузки {параметров в контроллер (2). где они готовы для скачивания в случае замены (ремонта) устройства.

73

ГОСТ Р МЭК 61784-3.3—2016

F-параметр (УГБ. время и т.п.)

шарамегр (индивидуальные

параметры

устройства)

СЯО-яяструмопии:

•авми-иетскрсв\*"\* у»»«Зйоступа

* м<стоуи»ит параштомачияидмгыэсптм.

овребетга параметров (донец,

* акт а доттгагациоитосжоое»\*\*
  + - аноми титмтя^ваьелкиеачяа

Пр««ем PS:

пресс\* зол nj/iaro/ewo

Prm \* М$1 (записи)

Г-авдоиыис«ЗСРЗЛи

**- обс\*6сг«а пдалегдо (утомляем\*. ■ параметр»' теме**

- мгдом после eectu • амплузгецис. твдодетятм uunh-ari

астро\*».-\*\*\* тв!нол(ги>асхт>и

ТО^рэммаии. кэтоимер ал»

задо-а после «мныус'сьйртаа

* стаилзотнезпсоФМ>мров»<и».

С бОМЛККОСТМ»

на да»»\*.\*

свечам *ж«»*

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

Набор правил, заложенньй в программы, посредством управляемого этими программами дина­ мическим назначением тараметров. 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). Иден­ тификационный номер действительного набора (параметров должен сообщаться циклически в рамках F-данных I/O.

* + 1. Требования интеграции системы для инструментов (параметризации

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

inepe метризации.

Таблица 12 — Требования для (параметризации

|  |  |
| --- | --- |
| Номер | Системное требование |
| R1 | Должен быть спроектирован CPD-Инструменг для совместимых персональных компьютеров или лапто­ пов. а также операционных систем от WIN2000 и позднее |
| R2 | Несколько СРО-инструментов или экземпляров CPD-инструментов должно функционировать параллельно |
| R3 | СР 3/1. Интерфейсные платы класса 2 ведущего устройства должны предоставлять унифицированный API (прикладной программный интерфейс) такой, что CPD-инструменгы могли бы быть сконфигуриро­ ваны для работы на разтых платах |
| R4 | CP 3/RTE. Интерфейс (С-супервизора должен быть определен таким образом, чтобы «не периодиче­ ские» услуги CP 3/RTE могли бы использоваться для F-устройсгва. непосредственно подсоединенного коетиСР 3/RTE |
| R5 | CP 3/RTE. Интерфейс iO-супереиэорв должен быть определен таким образом, чтобы «не периодичес­ кие» услуги CP 3/RTE МОТ1И бы использоваться для F-усгройства. непосредственно подсоединенного к сети CP 3/RTE. или через «Канал» к F-ведомому устройству, подключенному к «дополнительной» сети СР 3/1 (для регистрации инициации, чтения и записи и т.п.) |
| R6 | Соединения R4 и R5 долкны быть также возможны посредством порта F-хоста для программистов |

74

ГОСТ Р МЭК 61784-3-3—2016

*Окончание* таблицы *12*

|  |  |
| --- | --- |
| Номер | Системное требование |
| R7 | «Каналы-PN/DP» должны быть достутыы как автономные устройства либо как интегрированные в кон­ троллер |
| R8 | Индикация интерфейса полевой шиш. F-устройсгео 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 инстру­ мента. Должно быть предусмотрено автоматическое управление версиями наборов данных (параметра |
| R10 | Имя станции'адреса долям 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 пере­ даваться CPD- инструменту при вызове |
| R14 | Скачивание ^параметров на F-устройство. Поток октетов (параметров должен определяться таким образом, чтобы его можно было хранить в IO контроллере и передавать F-устройству во время общей параметризации.  PROXY-FB по-прежнему яагается лучшим решением для FSCP 3/1 |
| R15 | Версия. Интерфейсы API (cw. R3m R4) должны предоставлять номер версии, такой, чтобы CPD-инстру­ менты 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 стандартизиро­ ванном формате (например, HTML) программному инструменту хоста |
| R17 | Загрузка и Скачивание (параметров. Должно быть предусмотрено «удаленное управление» специаль­ ными CPD-инструменгами из программного инструмента хоста для пакетной «{параметризации» или доставлять {параметры в стандартизированном формате программному инструменту хоста (см. R14) |
| R18 | CPD-Инструмент должен бы\*ь активирован на предоставление имен символов по умолчанию (например.  «OSSD1»} программному инструменту хоста и получение взамен финальных назначенных символьных имен проекта в случае диагнэ стики. Предоставление символьных имен по умолчанию возможно в случае GSD файла СР 3/RTE |
| R19 | Для того чтобы достигнуть нззависимости от лежащего в основе черного канала, должен использовать­ ся 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 inap CRC32 должно осуществляться в обратным порядком байтов (начальное значение не должно быть нулем). Производитель может использовать свой собственный метод для защиты {параметров, если выполняются требующиеся критерии (inap-cepeep. CPD-инструмент) |

На рисунке 65 показаны системные аспекты интеграции инструмента CPD (CPD-Tool-Integration).

CPD-инструмент может быть подключен к одному из следующего:

* + F-Устройстеу напрямую (нгпример. USB. RS232);
  + F-Хосту посредством порта программиста:
  + CP 3/RTE и СР 3/1 через Канал:
  + СР 3/1 или СР 3/2

75

ГОСТ Р МЭК 61784-3.3—2016

о. ССРЗЯпоСР 3/6 *J3*

I

#### :а

------ > м ' # I

« »

|  |  |  |
| --- | --- | --- |
| F-x oc t |  | СРО-ииструмемт |
|  | программ чэуемый порт |  |
| ■О-контроллер |  | API |

*уУ* » I

*U-*

Кеи&л РЦ/ОР

**.**

о

CP 3/1

### ■5:

\*

# \*

#

# «

f

« I

**DpiMne**

соединение

* + 1. Шар-сервер

Рисунок 65 — Интеграция системы CPD-инструмектов

* + - 1. Общее описание и ограничения

Концепция inap-cepaepa является специализированной формой более общей концепции прокси- фблока. как это отмечено в 8.3.1. Ответственность за предоставление этой возможности лежит на про­ изводителях F-хоста, как это запалено в таблице 23. независимо от того, реализована ли она в части F-хоста. действующего в качестве ведущего устройства для параметризации, не связанной с безопасно­ стью. в управляемой подсистеме, такой как PLC. не связанной с безопасностью, или на промышленном компьютере в той же сети.

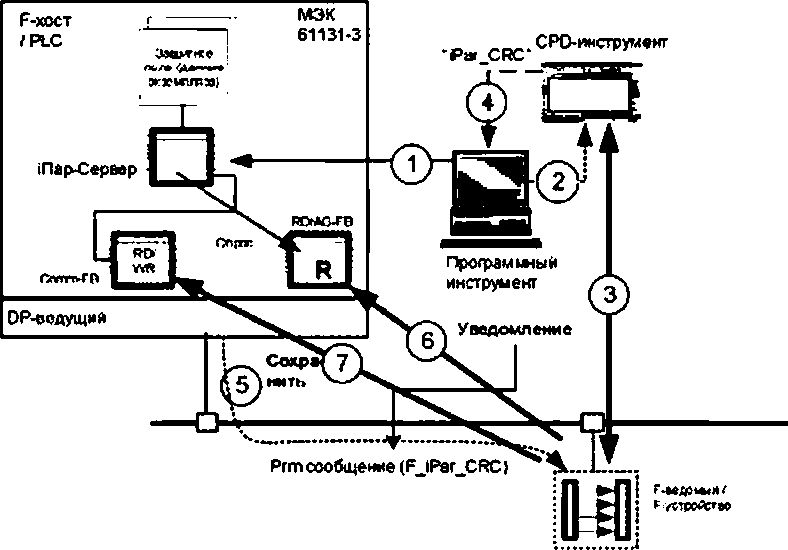


Рисунок 66 — Механизм inap-cepeepa (ввод в эксплуатацию)

76

ГОСТ Р МЭК 61784-3-3—2016

На рисунке 66 показаны принципиальные шаги механизма inap-cepeepa. Вместе с конфигури­ рованием сети и F-параметризацуей F-ведомого устройства/Р-устройства создается экземпляр и со­ ответствующей функции inap-cepeepa (шаг 1). F-ведомое устройство/Р-устройство способно входить в режим обмена данными, используя безопасное состояние (PV-эначения). Ассоциированный СРО 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. л. может быть выполнено с помощью СРО 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/Р-устройства необходим для передачи параметра «FJPar\_CRC» P-ведомому устройству/Р-устройстеу (шаг 5). После оконча­ тельной верификации и выпуска Р-еедомое устройство/Р-устройство активировано для инициализации уведомления о загрузке (шаг 6) в его экземпляр inap-cepeepa. Оно. тем самым, использует средства диагностики CPF 3 (в.6.4.2 и [49]). inap-cepeep опрашивает диагностическую информацию (например. RDIAG Фблока) для интерпретации запроса (R) и для установления процесса загрузки (шаг 7). который хранит тараметры как экземпляр данных в хосте inap-cepeepa.

На рисунке 67 показана вторая часть механизма inap-cepeepa. В случае замены дефектного F-ведо­ мого устройства/Р-устройства (шаг 1) F-ведомое устройство/Р-устройство принимает свои Р-параметры. включая «FJPar.CRC» (шаг 2), np/i запуске. Так как тараметры. как правило, отсутствуют при замене или не сохраняются P-ведомым устзойством/Р-устройством. то оно инициализирует уведомление скачи­ вания (шаг 3) в экземпляр своего inap-cepeepa. Тем самым, оно использует средства диагностики СРР 3 (8.6.4.2 и (49)). inap-cepeep опрашивает диагностическую информацию (например. RDIAG Фблока) для интерпретации запроса (R) и для установления процесса скачивания (шаг 4). С помощью этой передачи F-ведомое устройство/Р-устройство способно предоставлять исходный функционал без использования дополнительных программных и лу CPD инструментов.

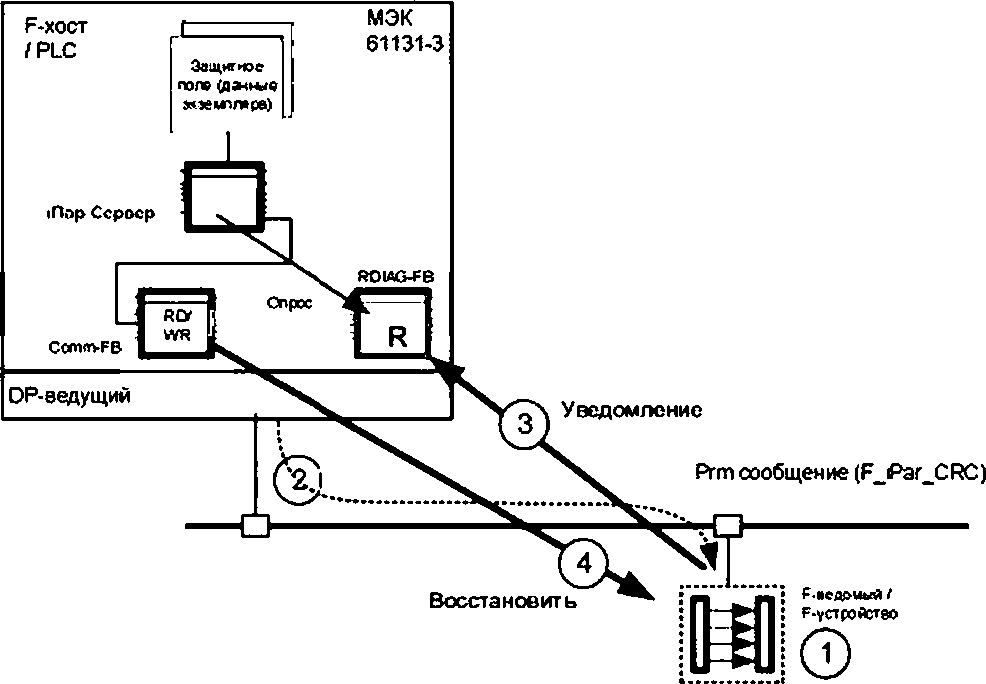


Рисунок 67 — Механизм inap-cepeepa (например, замена F-устройства)

77

ГОСТ Р МЭК 61784-3.3—2016

Следующие ограничения были определены для механизма iпар-сервера:

* каждый экземпляр inap-cepeepa должен поддерживать минимум 215-1 октетов параметров на F\_Source/Destination\_Address (устройство/подмодуль/модуль):
* тараметры хранятся как один фиксированный блок данных, как это показано на рисунке 52:
* inap-cepeep не связан сбезопасностью. Он может быть реализован или запущен в стандартном хосте или в стандартной части F-хоста (рисунок 67):
* inap-cepeep должен быть доступен только в совокупности с режимом V2 из FSCP 3/1:
* ответственность за то. что скачанный набор (параметров соответствует, например, корректному типу и версии у заменяющего устройства, лежит на производителе F-ведомого устройства/Я-устройства;
  + F-модуль/Р-ведомое ус"ройство/Р-устройство должно инициализировать 3anpoc-inap-cepeepa,

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/Я-устройства.
  + - 1. Уведомление

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

«Запрос inap-cepeepa» (тип *- 7).*

Примечание — «Обновленная аварийная сигнализация» (тип=6) не была выбрана в качестве этого типа и, как правило, ведет к отображение аварийной информации и следует другой семантике. Целью FSCP 3/1 являет­ ся установление кодировок для дв/х типов диагностических сообщений для СР 3/1. СР 3/2 и СР 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 inap-cepeepa для СР 3/1 и СР 3/2.

Ш8 БигЗ 158

|  |  |
| --- | --- |
| Ост» | Стандартная диагностика Блок заголовка (6 октетов) |
| Ост 2 |
| Ост 3 |
| Ост 4 |
| Ост S |
| 0<т 6 |
| НыОВТ |  |
| - W-Ser-»-\*) | *Щ*—Иаеити»ма<ор MSB - 1 |
| Skxnumtwr |  |
| •~--к |  |
| •B\*rO iH»f\_Hcq\_Heoeer (UR»fcre<l3h | 1Раг уведомление Блок на затронутый модуль (20 октетов на блок) |
| •Pari Mw\_Seein.Se»  <Un»vwl32) |
| ■Per? Ti»n»bi\_ir\*6w lUncqnnlSZ) |  |
| ■Pars Toaijibr.see  <Vn»gned32i |  |
|  | |

Рисунок 68 — Кодирование запроса inap-cepeepa («модель статуса»)

78

ГОСТ Р МЭК 61784-3-3—2016

Каждое кодирование «Запроса inap-cepeepa» начинается с шести обязательных октетов стандарт­ ного диагностического блока. Флаг «Diag.ext.diag» (бит 3 первого октета) не должен подвергаться вли­ янию. 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 inap-cepeepa» (7). Спецификатор стату­ са должен быть установлен в значение «0». Тело «Запроса inap-cepeepa» 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 СР 3/1 или CP 3/RTE. Удаленный ЬО должен отправлять по одному уведомлению за раз и. тем самым, сохранять или восстанавливать параметры 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 стандар­ тизировано.

Трансформация кодировки запроса inap-cepeepa в надлежащий формат актуального коммуника­ ционного профиля является задачей головной станции удаленного I/O устройства (рисунок 68 или 70).

Таблица 13 —Спецификатор для Запроса inap-cepeepa

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *\па* р сп«ии\* фикатэр | Немение | Oner з | Октет 2 | Октет 1 | Октет 0 | Определение |
| iParO | iPar\_Req\_Header | SR\_V3fsion | Reserved | N.Count | SR\_Type | Тил запроса inap-cepeepa (Unsigned32) |
| iParl | Max\_Segm\_Size | OxOOh | OxOOh | OxOOh | 0...234 | Максимальный разрешенный размер сегмента в октетах (Unsigned32) |
| iPar2 | Transferjndex | OxOOh | OxOOh | OxOOh | 0...254  (255) | Индекс для передачи регистрации записи/чтения (Unsigned32) |
| «РагЗ | Total\_iPar\_Stze |  |  |  |  | Общая длина октетов 1лпараметра (Uns»goed32) |
| Примечания 1 Зарезервировано: см. 7.1.3, подсказки.   1. Параметр «Max\_Segm\_Size» может быть больше, чем 234 октета, в случае СР 3/RTE. Он может включать вплоть до *2Р-\* октетов, что вызвано ограничениями FSCP 3/1. 2. «Transfer\_lndex» в 255 октетоэ может конфликтовать с другими услугами, такими как. CALL (вызов) ИТО функций. 3. Параметр «Transfer Index» может быть больше, чем 255 октетов, в случае СР 3/RTE он может достигать   до 65 535.   1. Заменяющее устройство может не знать корректного размера (параметра своего предшественника. В таком случае уведомление для восстановления может содержать «Total\_iPar\_S<ze = 0». что означает, что inap- сервер будет скачивать полный набор данных inapaMerpoe. 2. N.Count является счетчюсом последовательности для уведомлений (только для СР 3/1 и СР 3/2). считая от 1 до 15 и сначала. | | | | | | |

Пара метр «SR.Version» должен быть установлен e0x01h. Пара метр «N\_Count» должен начинаться с «1» и увеличиваться с каждым уведомлением (только в случаях СР 3/1 и СР 3/2) до значения 15 и затем продолжаться, начав со значение «1». Параметр «SR\_Type» должен кодироваться, как показано на рисунке 69.

79

ГОСТ Р МЭК 61784-3.3—2016

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I ’ | *ь* | 5 | 4 | э | г |  | 0 |
|  |  |  |  |  | • | 0 | 0 |
| • |  |  | • |  |  | 0 |  |
|  |  | • | • |  |  | 3 | 0 |
| • |  | • | е | • | « | 1 | 1 |
| • |  | - |  | ■г | t |  |  |
| • |  | • | 0 |  | « | • | • |
| . |  |  |  | 4 |  | • | а |

**Здонммговьо. «м глэ.псюээш**

Софмми »»)

Зярюрмраино <м *}* 1 Э.псдож\*\* Весспгоом'ме )сал'\*то\*>«1

Эя««мфо<эаи»п ей 7 1Э. положим

п«р«\*в «а мно -де~~нн~~ое всич» пики

Соомчясиюти-мрииа. прласиямис\* *\*в* mo miw .hh puMput

ЗлрвМСМРСЖ.СМ Т1Д OMCUUM

Рисунок 69 — Кодирование SR\_Type

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

После отправки запроса inap-cepeepa F-ведомое устройство/Р-модупь ожидает *21\** мс (приб­ лизительно 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 inap-cepeepa связано с «Моделью Аварийного сигнала» и со стандартным «Upload&Retrieval» аварийным сигналом, определенным в МЭК61158-5-10 и МЭК 61158-6-10. На рисунке 70 показано кодирование запроса inap- cepeepa для CP 3/RTE (МЭК 61784-2). После отправки запроса inap-cepeepa Р-устройство/Р-модуль ожидает 218 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 случав запрос inap-cepeepa на «Восстановление» и при отсутствии хранимых шараметров. inap-сервер должен отправить запись длиной «0».

шп ей» к»

|  |  |  |
| --- | --- | --- |
| CVtH 1 | 1 |  |
| ami | 1 | А 1а (т Notification |
| Оси\* | 1 | (VJpted&Relneval - |
| Оси 4 | 1 | Выкпадмммиа и |
|  | 1 | •тцвидпмт) |
| (Ий« | 1 |  |
| ■мим- | с |  |
|  |  |  |
| API | 4 |  |
| Мам.\*\* | *?* |  |
| liMH *шьш* | *i* |  |
| ком штамм» | *А* |  |
| »1>мч1Ш»|||П|» | 4 | >Раг |
|  | 7 | блок не звтронугьй |
|  | > | модель |
| —ынма» | 0 | (52 октета на |
|  | 1 | 6f»0 |
|  | J |  |
| *г\*\** г».«\*ч.\*\*«\*\* | *4* |  |
| Игч | *4* |  |
| Ат? IUHtfMgl | 4 |  |
| ftr} Тоо.Ав.Ак lUHspWX; | *4* |  |
|  | | |

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

80

ГОСТ Р МЭК 61784-3-3—2016

* + - 1. Услуги

inap-cepeep является маленэхой программой, вызываемой каждый основной цикл, например, внутри не связанной с безопасностью части F-хоста. Он собирает диагностическую информацию, опрашивая определенные F-ведомые устройстваУР-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), какэтоопределено в МЭК 61158-5-3. Для небольших наборов тараметров 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 ROREC и WRREC. Настоятельно рекомендуется использо­ вать 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»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Структуре Read\_RES\_ PDU | Размер | Кодирование | Примечания |  |
| FunctionJMum | 1 октет | 0х5Е | Указывает на «Read», fix | Заголовок |
| Slot.Number | 1 октет | 0... 255 | Местоположение модуля |
| Index | 1 октет | 0... 254 | “Transfefjndex" |
| Length of net data | 1 октет | 0... 240 | Длина сегмента (Пар |
| 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 Wrile\_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 | Transferjndex" |
| Length of net data | 1 октет | 0 ... 240 | Длина сегмента inap |
| iParameter | п октетов | - | п = 240 максимум | Данные |

Для наборов {параметров, 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 PuR.RES.PDU | Размер | Кодирование | Примечания |  |
| Function\_Num | 1 октет | 0х5Е | Указывает на «Read», fix | Заголо- вок |
| Slot\_Number | 1 октет | 0... 255 | Местоположение модуля |
| index | 1 октет | 0... 254 (255) | “Т ransferjndex’ а) |
| Length of net data | 1 октет | 0... 240 | Дгмна сегмента inap + заголовок облас­ ти загрузки |
| Extended\_Function\_Num | 1 октет | 0x02 | Указывает на «Puli» | Область загрузки |
| Options | 1 октет | Unsigned8 | Управление потоками, см. МЭК 61158- 5-3. 6.2.17.2 |
| Sequence.Number | 4 октета | Unsigned32 | .. .текущего «Раг сегмента |
| iParameter (сегмент) | л октетов | Строка октетов | *п* = 240 максимум на запись | Данные |

al «Transfer Jndex\* из 255 в данной случае соответствует МЭК 61158-5-3. Тем не менее, конфликты доступа с другими услугами, такими как CALL и функции И ТО. должны рассматриваться при проектировании и реализации. Все другие индексы могут ис по гьзо ветьс я для услуг «РиН» и «Push».

81

ГОСТ Р МЭК 61784-3.3—2016

Таблица 17 — Структура Push\_REQ\_PDU («Push»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Структура Pull\_RES\_PDU | Размер | Кодирование | Примечание |  |
| Funclion\_Num | 1 октет | 0x5F | Указывает на «Write\*, fix | Заголовок |
| Stot\_Number | 1 октет | 0... 255 | Местоположение модуля |
| Index | 1 октет | 0... 254 (255) | “TransferJndex" *a* |
| Length of net data | 1 октет | 0... 240 | Длина сегмента !Пар + заголовок области загрузки |
| Extended\_Function\_Num |  | 0x01 | Указывает на «Push» | Область |
| Options | 1 октет | Unsigned8 | Управление потоками, см. МЭК 61158- 5-3.6.2.17.2 |  |
| Sequence\_Number | 4 октета | Unsigned32 | ...текущего iPar сегмента |
| iParameter (сетемг) | л октетсв | Octet String | л = 240 максимум на запись | Данные |

41 «Transfer Jndex» из 255 в данном случав соответствует МЭК 61158-5-3. Тем не менее, конфликты доступа с другими услугами, такими как CAL. и функции ИТО. должны рассматриваться при проектировании и реализации. Все другие индексы могут испольювагься для услуг «Pull» и «Push».

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

Примером для стандартного сервера параметров будет механизм «Uptoad&Retneval» (Загрузка и Извлечение) из CP3/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 эсегда использует надлежащее кодирование, всякий раз. когда он может быть внедрен в СР 3/1 или удатенное устройство I/O CP 3/RTE. Преобразование кодировки передачи шараметров 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 параметрам. Скачивание короткой записи с информацией проверки позволяет верифицировать непротиворечивость данных и их актуальность, не влияя на эффективности.

* + - 1. Протокол

На рисунке 71 показана диаграмма состояний inap-сервера.аетаблице 18 описаны состояния inap\* сервера. а также переходы и внутренние элементы. Общую информацию о нотации UML2 см. в 7.2.2.

82



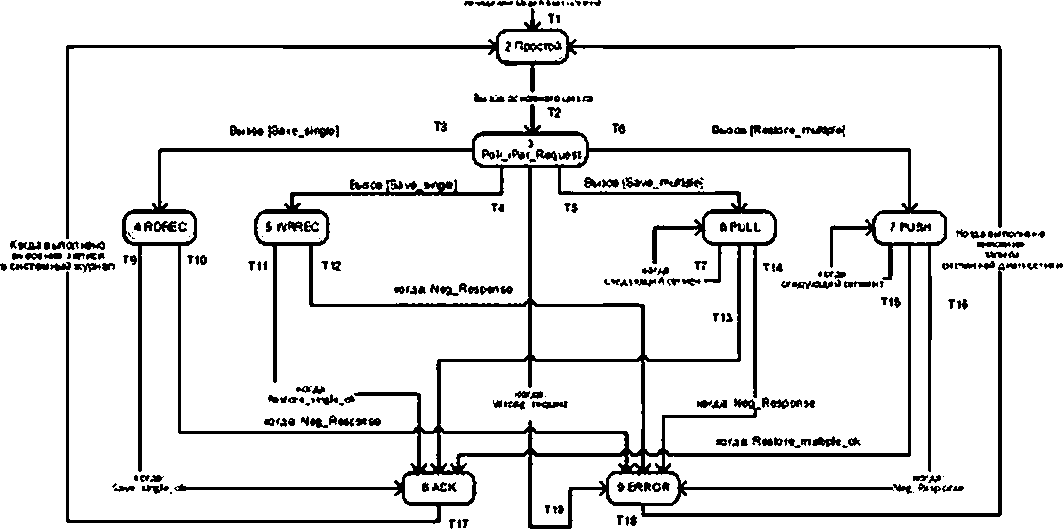
«ОД

Рисунок 71 — Диаграмма состояний iпар-сервера

Термины, используемые на рисунке 71 описаны ниже:

ГОСТ Р МЭК 61784-3-3—2016

Save\_singte Restore\_single Save\_mu1tip!e Restore\_multiple

* запрос inap-cepeepa на сохранение (загрузку) одного блока тараметров на запись (RDREC);
* запрос inap-cepeepa на восстановление (скачивание) одного блока Параметров на запись (WRREC);
* запрос inap-cepeepa на восстановление (скачивание) большего блока тараметров для множества записей (PULL);
* запрос inap-cepeepa на восстановление (скачивание) большего блока тараметров для множества записей (PUSH);

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

System diagnosis entry (за- — лобое неуспешное действие сохранения или восстановления должно пись системной диагностики) быть зафиксировано в отчете посредством системных средств диагно­

стики:

Neg\_Response — каждый раз. когда системная функция, такая как RDREC. WRREC. PULL

иг и PUSH прерывает работу, выдавая ошибку, inap-сервер должен создавать запись о диагностике системы;

Wrong\_request — каждый раз. когда inap-cepeep обнаруживает неверный тип запроса или

отсутствие реакции любых вызванных системных функций, он должен прервать действие и создать запись о диагностике системы.

83

ГОСТ Р МЭК 61784-3.3—2016

Таблица 18 — Состояния inap-cepsepa и переходы

|  |  |
| --- | --- |
| НАИМЕНОВАНИЕ СОСТОЯНИЯ | ОПИСАНИЕ СОСТОЯНИЯ |
| 1. Initialisation ((Инициализация) | Состояh&ie холодного запуска: инициализации выводов, если таковые определены |
| 2 Idle (Простой) | Состояние пэостоя. нет действий |
| 3 Poll\_iPar\_Request | При вызове основного цикла или другой подобной деятельности в управляемой подсистеме в геле диагностической информации интерпретируется запрос inap-cepaepa 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 СР 3/1 или СР 3/2 в МЭК 61158-5-3 |
| 5WRREC | В данном состоянии должна вызываться системная функция WRREC (в соответствии с (49)) или другая подобная функция, выполняющая функцию внесения записи в соответствии с СР 3/1 или СР 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» =0х028соответствии сСРЭ/1 или СР 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\_Funct»on\_Num» = 0x01 в соот­ ветствии с СР 3/1 или СР 3/2 в МЭК 61158-5-3 |
| SACK | В данном состоянии любое успешное действие сохранения или восстановления может быть записано в «системном файле журнала шар-сервера» (не обязательная функция) |
| 9 ERROR | Каждый раз. когда системная функция, такая как RDREC. WRREC. PULL, или PUSH пре­ кращает работу, выдавая ошибку, или в случае ошибочного запроса, iпар-сервер должен, в рамках даннзго состояния, создавать запись о диатостики системы |

*Продолжение* таблицы *18*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | ИСХОДНОЕ СОСТОЯНИЕ | ЦЕЛЕВОЕ СОСТОЯНИЕ | ДЕЙСТВИЕ |
| Т1 | 1 | 2 | - |
| Т2 | 2 | 3 | Вызов основного цикла (или другого подобного события в управляемой подсистеме) |
| ТЗ | 3 | 4 | Вызов функции RDREC для загрузки одного блока (параметров |
| Т4 | 3 | 5 | Вызов функции WRREC для скачивания одного блока (параметров |
| Т5 | 3 | 6 | Вызов функции POLL для множественного скачивания большего сегмен­ тированного блока (параметров |
| Тб | 3 | 7 | Вызов функции PUSH для множественного скачивания большего сепией- тированного блока (параметров |
| Т7 | 6 | 6 | Начать читать следующий сегмент |
| Т8 | 7 | 7 | Начать записывать следующий сегмент |
| T9 | 4 | 8 | Начать запись в файл системного журнала об успешном выполнении RDREC (не обязательно) |
| Т10 | 4 | 9 | Начать запись системной диагностики |
| Т11 | 5 | 8 | Начать запись в файл системного журнала об успешном выполнении WRREC (не обязательно) |
| Т12 | 5 | 9 | Начать запись системной диагностики |
| Т13 | 6 | 8 | Начать запись в файл системного журнала об успешном выполнении POLL (не обязательно) |
| Т14 | 6 | 9 | Начать запись системной диагностики |

84

ГОСТ Р МЭК 61784-3-3—2016

Окончание таблицы *18*

|  |  |  |  |
| --- | --- | --- | --- |
| ПЕРЕХОД | ИСХОДНОЕ СОСТОЯНИЕ | ЦЕЛЕВОЕ СОСТОЯНИЕ | ДЕЙСТВИЕ |
| Т15 | 7 | 8 | Начать запись в файл системного журнала об успешном выполнении PUSH (не обязательно) |
| Т16 | 7 | 9 | Начать запись системной диагностики |
| Т17 | 8 | 2 | Перейти в режим ожидания {Idle} |
| Т18 | 9 | 2 | Перейти в режим ожидания (Idle) |
| Т19 | 3 | 9 | Начать запись системной диагностики |

* + - 1. Управление inap-сереером

В таблице 19 перечислены средства управления inap-сервером для обеспечения аутентичности, соответствия и целостности данных {параметров. Ответственность за предоставление мер безопасности для механизмов сохранения и сосстановления лежит на F-модуле. F-ведомом устройстве или F-устройстве. inap-cepeep всего лишь хранит {параметры в виде потока октетов и может гак служить стандартным сервером параметров для устройств, не связанных с безопасностью.

Таблица 19 — Средства управления inap-сервером

|  |  |  |
| --- | --- | --- |
| Элемент*!* стадия | Разделы | Описание |
| F\_S/D\_Address | 8.1.2  7.3.7  9.1 | Испольэозание F\_Sourcе/ Destination\_Address или короткого F\_S,D\_Address является обязательным входным условием для обеспечения аутентичности сохраняемых и восстанавливаемых {параметров. Включение F\_S/D\_Address в вычисление iPar\_CRC или в блок {параметров не является обязательным. Корректная доставка F\_iPar\_CRC уже гарантируется посредством F\_S/D\_Address для того, чтобы ошибочно доставлен­ ный бпокшараметров мог быть обнаружен сравнением его iPar\_CRC с FjPar\_CRC. В случае, когда посредством кодового переключателя задан F\_S/D\_Address. за­ меняющее устройство должно быть отрегулировано для соответствия начальному F\_S/D\_Address перед запуском. В случае, если F\_S/D\_Address назначен посред­ ством СРЭ-инструмента. ответственность за предоставление средств для настройки  F\_S/D\_Acdress 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-na- раметры 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 I ц (два цикла в секунду) |
| Ввод в эксплуатацию |  | На данной этапе устройство может быть сконфигурировано и параметризовано при помощи СРО-инструмекта. подключенного напрямую, или. испогьзуя услуги не пе- риодичесшх коммуникаций, такие как. MS2. Ответственность за обеспечение без­ опасной параметризации на всех этих стандартных коммуникационных каналах и определение безопасности устройства ео время нахождения в исгытзтельном режи­  ме FSCP лежит на производителе устройства и соответствующего CPD-инструмента |
| iPar CRC / FJPar.CRC | 8.2  8.3.Э.2 | Испольэозание iPar\_CRC и его аналога FjPar\_CRC. передаваемого в разных на­ правлениях. является входным условием для обеспечения целостности данных со­ храненных и восстановленных {параметров. В случае, когда вычисленная iPar\_CRC сигнатург в CPD-инструменге 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. возника­  ющим из параметризации при запуске |
| Ручное распро­ странение | 8.1.7 | iPar\_CRC вычисляется в режиме безопасности в CPD-инсгрументе и должна ото­ бражаться а шестнадцатеричном формате. Пользователь затем может вручную пе­ редать 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 {параметров (блока) для заменяющего устройстаа дефектному может быть проверено, например, посредством функций |

85

ГОСТ Р МЭК 61784-3.3—2016

Окончание таблицы *19*

|  |  |  |
| --- | --- | --- |
| Элеыеит / стадия | Ра мели | Описание |
| ИТО функции | 8.2 | идентяфжации и технического обслуживания (ИТО). таких как «order number» (номер заказе), «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 (параметров завершается определенным испытанием и шагом верификации, за которым следует действие «отсоединения» и «повторное соеджения». приводящее к запуску и передаче правильной F\_iPar\_CRC |
| inap-cepaep | - | F-Ммсдупь. F-ведомое устройство или F-устройсгво должны запускать запрос inap- еврвера только после успешной параметризации запуска (F-параметры) |
| Светодиодная индикация | 9.1 | До тех пор пока F-модуль. F-ведомое устройство или F-усгройсгво на добьются сохра­ нения своих (параметров или пока само устройство находится в режиме испытания FSCP, то оно должно указывать на нахождение в этом состоянии посредством све­ тодиодных индикаторов, описанных в 9.1. Чистота мигания в данном случае должна составлять 2 Гц |

* + - 1. Размер (параметров в GSD

F-модуль. F-ведомое устройство или F-устройство может указывать максимальный размер своих (параметров посредством поля ключевою слова «Max\_iParameter\_Size» в своем GSO файле

{«MaxJParameterSize» в GSDML). Подробности см. в [43] и [47].

1. Системные требования
   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 (ОА\_С).

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 е порядке, но запрошен ОА\_С>). 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 ОА\_С»). 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 (параметров, 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 посред­ ством коммутаторов.

* 1. Руководство по установке

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

* 1. Время реакции функции безопасности
     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 прохожде­ ния его сигнала и потому и свое определенное типовое время реакции.

86

ГОСТ Р МЭК 61784-3-3—2016

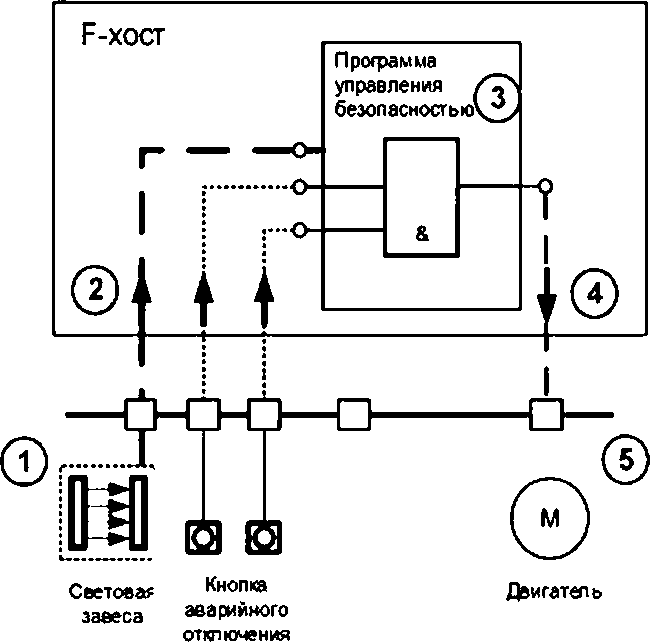
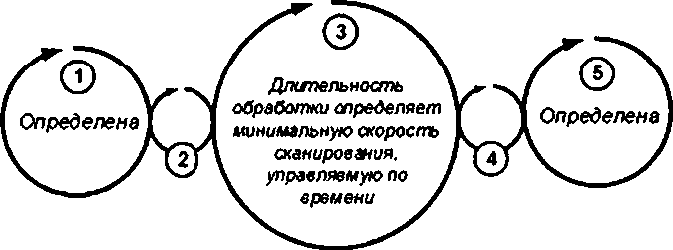


Рисунок 72 — Пример функции безопасности и критический путь ее времени реакции

Это типовое время реакции оостоит из нескольких отдельных периодов времени, включая время, затрачиваемое на передачу данньх 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.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Задерккэ ввода | Задеркка передачи | Задеркка обработки'! | Задеркка передачи | Задеркка вьеода |
| Пример 3. | 1. | 5. | 1. | 3. |
| *4.* | *2м* | 6. | 2 те | *4.* |
| 5. |  | 7. |  | 5, |
| бме |  |  |  | 6 те |
|  |  | 15 те |  |  |

\*)мин время обработки 5те. сюрость сканирования. управляемая го времени, для зтопримерв « Юме

Рисунок 73— Упрощенная модель типового времени реакции

87

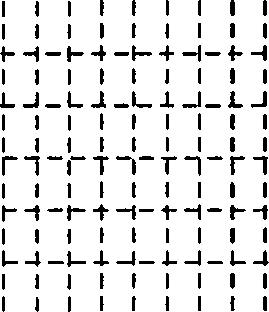
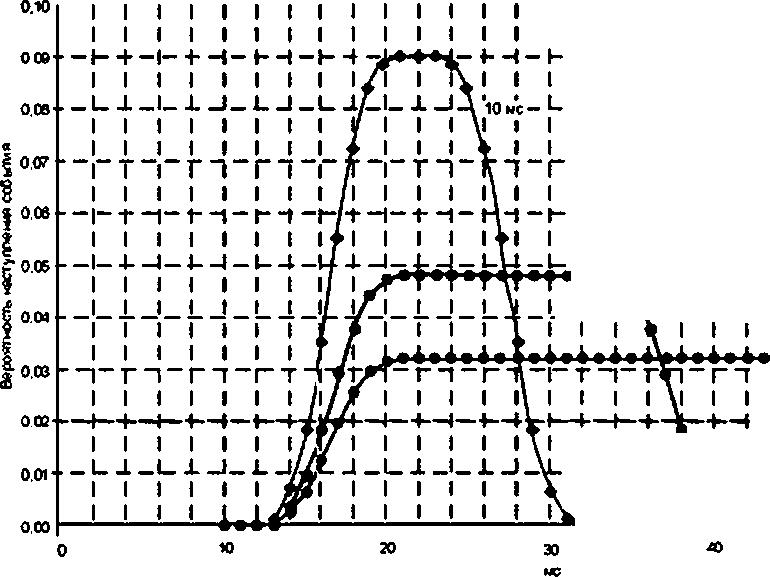
ГОСТ Р МЭК 61784-3.3—2016

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).

PrtnpwneMiw ерм«п> cram (вр«ивиат|мгг«ра юдооз ис)

|  |  |  |  |
| --- | --- | --- | --- |
|  | 1 I I I | 1 1 t | 1 |
| t i l l | 1 1 |
|  | tT-rr-r | П-Г |
| \»ме 1 1 | 1 1 1 |
| *L. U* -U- | o\_i**\_** X |

Рисунок 74 — Распределения частот типового времени реакции модели



I I I I I I

I I I I I I I 4-h-M-fH-

I I I I I I

i \_ L l \_l\_ *L* \_l\_ I I I I I I

тI I

I I

I I I I

IтIтIгI г

-г —I— 1—I— 1—I — I I I I I I

I—i--l —

I I | | I iV"? i I

I I

I Л I

I

I I \1 I

J-L i-lii J-L JJ \_

i I I i V I

I♦I♦*I*♦1

\_ и

i

I г

во

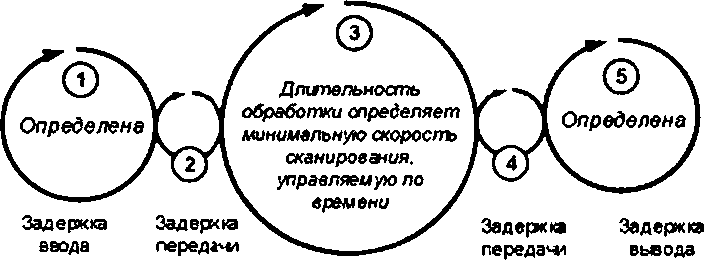
Любые из этих элементов обладают минимальными (на обработку) и максимальными (обработка ♦ ожидание) временами задержки. Фактическая задержка может быть любым временем (или интервалом) между этими значениями. В данной модели предполагается, что F-хостэто комбинированный контроллер для стандартных программ 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. 8 общем, минимальная задержка для этой функции безопасности равна 13 мс. На рисунке 74 показаны распределения частот типового времени реакции модели для триггера, срабаты­ вающего каждые 10 мс. 20 мс и 30 мс.

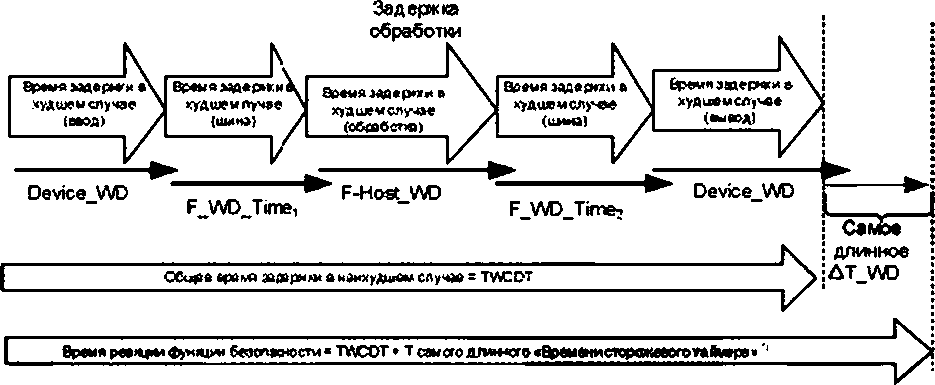
* + 1. Вычисление и оптимизация

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 задерж­ ки в лучшем случае до времеш задержки в худшем случае (WCDT,). Для обеспечения безопасности с каждым циклом связан свой сторожевой таймер (WDTimej, 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.

88

ГОСТ Р МЭК 61784-3-3—2016





\*) Не обязательно для устрой:та вьеода

Рисунок 75 — Контекст для времени задержки и времени сторожевого таймера

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

SFRT “ £ е, WCDT \* max 2 n (WDTime, WCDT,),

где: SFRT ТО WCDT,

WOTime,

OFDT

* время реакции функции безопасности;
* задержка передачи;
* время задержки в худшем случае для объекта i;
* WDTlme охватывает период времени, начиная с принятия PDU безопасности с новым порядковым номером и заканчивая реакцией на истечение времени F\_WDjnme. Ниже при­ ведены определенные выражения для объектов i:

|  |  |
| --- | --- |
| — Ввод: | OFDTlnpul. |
| — TD1: | F\_WD\_Time1 ♦ WCDTT01 + TcyF>W4,; |
| — F-x oc t : | o f d t fhmi, |
| — TD2: | F\_WD\_Time2 ♦ WCDTt02 ♦ DAT0u(pul; |
| — Вывод: | OFDTouipoi; |

* время задержки объекта в случае одного сбоя. т. е. время задержки в худшем случае при сбое в объекте;

TcyF.Hes( — еемя цикла F-хоста.

В случае необходимости производители системы должны предоставить индивидуальный адапти­ рованный метод вычисления.

89

ГОСТ Р МЭК 61784-3.3—2016

* + 1. Корректировка времени сторожевого таймера для FSCP 3/1

F-Ппараметр F\_WD\_Time определяет время сторожевого таймера для коммуникационной свя­ зи 1:1 профиля FSCP3/1 (8.1.3) На рисунке 76 показано, что минимальное время сторожевого таймера состоит из четырех временных секций (DAT — Шина — HAT — Шина).

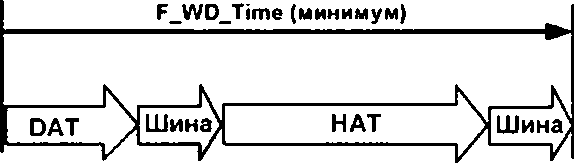
Каждый раз. когда F-драйеер (6.2) в малогабаритном F-устройстве или в F-модуле модульного устройства распознает PDU безопасности (кадр FSCP 3/1), содержащий новый порядковый номер (т). то он перезапускает сторожевой таймер. Затем драйвер обрабатывает протокол FSCP 3/1, принимая *доступные на данный момент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

Примечание — В случае модульного F-устройсгва 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 *[т\** 1). Затраченное время на эту операцию называется «НАТ *-* Время подтверждения хоста». Передача PDU безопасности F-устройству выполняется е течение последней временной секции (Шины).

Время сторожевого таймера, которое должно быть назначено F-napa метру превышает минимальное

*время сторожевого таймера,* чтобы обеспечить обнаружение аварийного события.



F-устройстео F-xoc t

|  |  |
| --- | --- |
| —г- |  |
| I  1  *\* | СОМ) |
| 1  **!’** |  |
|  | {\*миаг>411»«рхд»ма |
| 11 | (DAT] |
| т |  |

Л»ИСМп>»>\*в 1№М№\*»Я|М

\*ОЧ»<И> ПМвМвГ(М

>»F\_Y4Q.T"\*C“»«

— — — —

|  |  |
| --- | --- |
| дмкя лздгеасидо-яя | “1—  1 |
|  | 1 |
|  | 1 |
|  | 1 |
| r.wo.\* г\* (»\*••« 1 | г ! |

1

1

1

Рисунок 76 — Временные секции, формирующие F\_WD\_T\*me 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

90

ГОСТ Р МЭК 61784-3-3—2016

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

* + 1. Поддержка программного инструмента

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

* + 1. 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. ка> правило, применяют механизмы повторения для повышения готов­ ности. 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 повы­ сить готовность, но также обеспечит короткое время реакции без ложных срабатываний (рисунок 77).

ВлтнлеповторсиъНю оасмассвдии (аосмятсмтссаг 10 мс)

О.Ю

**ОМ — I- -f —I-**

**I I I I I I I I I I I I I I I I I { I I I I I I**

I I I I I I 1 t I I I I I I I I I I I I I H-l-t-^ + 4-F4-b4-r

. . /. . — - . .

0бмм<мяий:

•мсвддоние<««!отданное

I/1 I

-J-V

l\

пзатфвмиА {время триггера = 10 м:);

«fv+etoi\* • раарвдегти\* частот дажоймдом в

i i i t i

r

“I “

**r\T**

1—Г

по Stop винти

1 1

/\*

ri-rt

N I I I I

1—I —»--t

— 1—I —

I

•—I—Г—1—1—I

* I—г

-I-

I 1 1 1/ 1/ 1 1 1 I . 1

4--I-U4-1- J# \_1\_ 4—1 -L-i-l

Повторения| | | i i i |

— I-I-I- —I— 4—I— 4—I — I—1-—I—L \_1\_ J—I\_I—I

1 1

1 J

1 1

1 1

1 *V* / I I I

1 ' / 1 1 1

1 1

1 1

/Г ill

h

i i i

1 I; 1

1 it 1

t I

1 1 . 1

I

П“Г7’П 'ТТП “ГТ"1 Г Т

*Л* II/ I I I I

.+.^#.+-+--4-4-

I I I I I

Fl\_ -1 —I\_L \_1. 1 1 1 1

I I I I

2 0 49

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.

91

ГОСТ Р МЭК 61784-3.3—2016

Ведущий

СР 3/1 Изохронный режим

Водоный х Ведо№й х \* 1 Ведущий Ведений х Ведений х + 1

Время

I

спота I

f-ее сосбиргыв

*Нет* или неверный ответ.

*2-ое сообщение*

н«п ши xewpwO ответ,

▲

3-в е»аэйц<в>шв

Нет или нввденый стват^ф—

До 15 повтор/ыл лсгытск в

ч«и\*

iSoococOupruo -

Нет иш наверно отвык ввдоиый т~~рма~~е *д~~о~~не*

*QX(J0AHl#*

*Спеющий* ввДриый

МЭ<в1158 Максимум 8поаторемлй

Иол имение для испытаний. Поют л» но до 15 повторений вожжна установка параметров аогыаоватвпем

\*) (идвилхмвый Р01/ бвлопеоооти!

время слога

т-о» *сосбиение*

*Нет или* /воергыО алеет ,

I

*2-0»* свобирч/в не\*1 *шь*неверны *а*ответ.

**е**

*Ctbbfouvit* ведомый

|  |
| --- |
| { Звеври/еный <«/\*от  • |
| 3-е сообщение\*} |
| Нет ши неверный ответ |
| 4-оо сообиеии\* ‘1 |
| Нет ши «верный ответ |
| СлеСуюшьО вебомый |

Завершенный ркп

Всего 3 цмге, т е 6-ое coo6u#»»me яалаетсяслмым господний МотаэиэиияСРи. Попеаоеательмо устанавливает нм.arm параметров.

Рисунок 78 — Повторные попытки с СР 3/1

С СР 3/4 по СР 3/6

FSCP3/1

«обновление»

f-ое сообщение

*Следующее*устройство

Hem *или*ивеоргрял omeom cm Я- устройства в рохегвл 4 \*

идее /есидеронноео/

Устройство х Устройство х ♦ 1

•tЗавершенный цикл

2-ое *сообшрпие (идентз'+ый POU безопесносп^*

*НетилимееержЛ*ответ

от Я- устройстве *ерэьвох*— цосле (асинхронно\*©/

**а**

а Зев ерше не л/ цикл 7

•

FSCP3/1

«обновление»

бремясторожееоаотвймере ос те ало

бвзолвснаярввкмют

'} Максимальное число повторений см вСРЗ/4

Рисунок 79 — Повторные попытки с СР 3/RTE

92

ГОСТ Р МЭК 61784-3-3—2016

* 1. 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 сиоалов:

* + должна быть равна времени безопасности процесса или больше, чем таймаут FSCP 3/1

{F\_WD\_Tnn6);

- 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 POU безопасности с одинаковым порядковым номером

и разными значениями процесса, «-то происходит из-за переставленных сообщений в черном канале.

* 1. Ограничения для вычисления системных характеристик
     1. Вероятностные соображения

Механизм проверки целостности данных \/2-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.

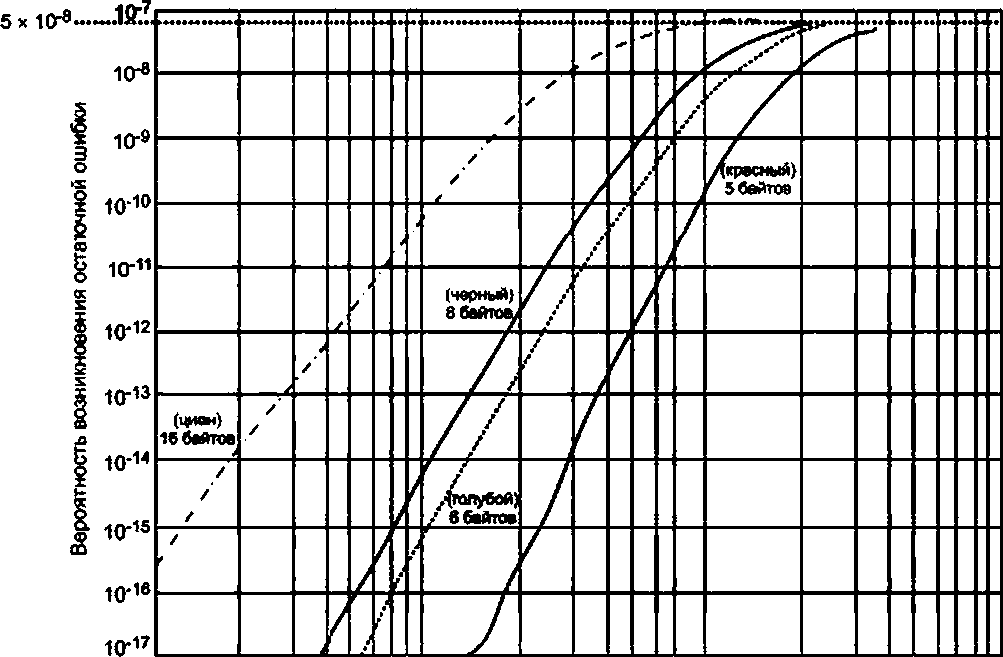
В соответствии с МЭК 62280\*1 и МЭК 62280-2 должна быть доказана «годность» применяемых

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

{15060С8Л). также как и для 32-б^товой версии (1F4ACF0f3h).

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.



   

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

93

ГОСТ Р МЭК 61784-3.3—2016

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

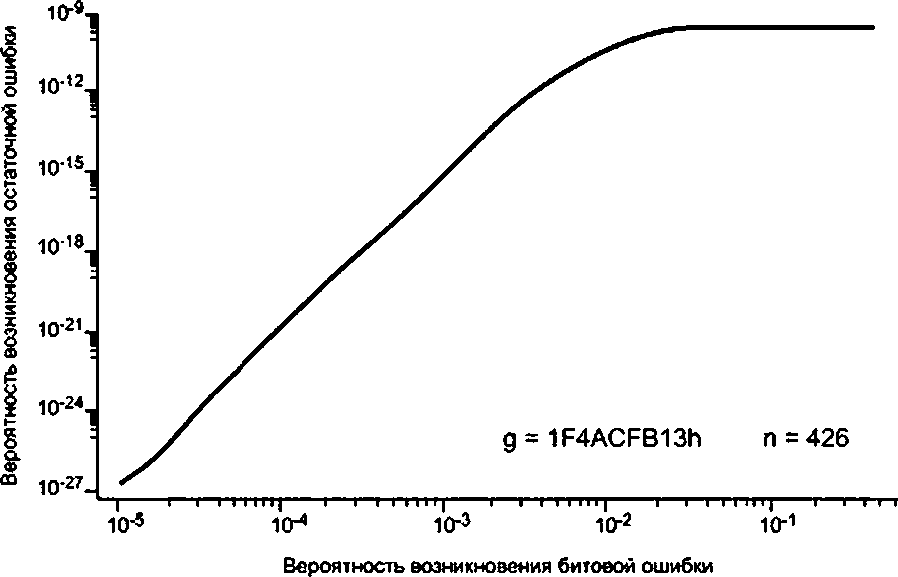
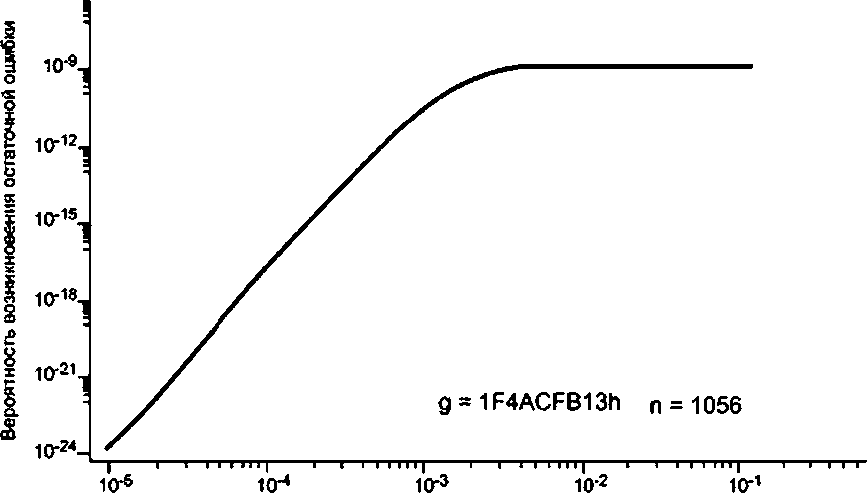


Рисунок 81 — Годность 32-битового полинома для 52 октетов

Термины, использованные на рисунках 81 и 82. описаны ниже:

*д -* генерирующий полином *'\F4ACFB13h:*

*п -* битовая длина данных, включая сигнатуру CRC.



вероятность возникновения битовой ошибки

Рисунок $2 — Годность 32-битового полинома для 132 октетов

94

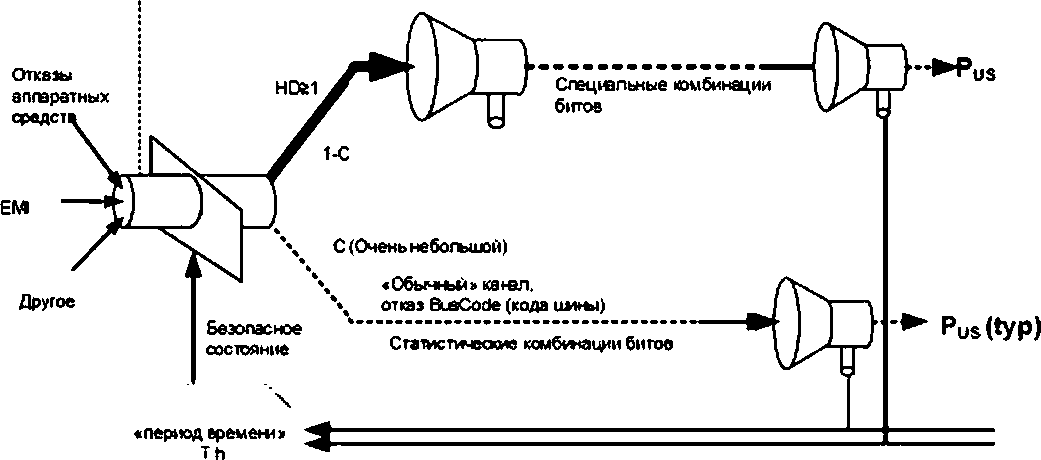
ГОСТ Р МЭК 61784-3-3—2016

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 до­ стигают механизм уровня безопасности. Для числа необнаруженных искаженных сообщений не должно приниматься значение худшего случая равное 2'п (п = 24 или 32). так как общая частота искаженных PDU безопасности на шине подвергается постоянному контролю.

Частота кскажеииоа сообщений

**1 Фильтр 2 Фильтр**

**BusCode:** Pue(typ) **Koa FSCP3/1:**



Внутри F-xocia

Распознанные искаженные сообщаем от каждого у^стнжа

Рисунок 63 — Контроль искаженных сообщений

Термины, использованные нг рисунке 83, описаны ниже: fw — частота отправки искаженных сообщений;

ЭМП — электромагнитные помехи; HD — расстояние Хеммикга: с — частота возникновения;

Т — период измерения в часах (см. 7.2.6).

Если механизмы безопасности в стандартных 10 уровнях СР 3/1 и CP 3/RTE отказывают (очень низкая вероятность), то искаженные сообщения со статистическими комбинациями битое 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.

* + 1. Ограничения, связанные с безопасностью

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

Общие.

* + Все устройства обеспечивают SELV/PELVAAfl электрической безопасности и отчетотестировании 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.

95

ГОСТ Р МЭК 61784-3.3—2016

Режим V1.

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

СР 3/1: 100:

СР 3/2: 10.

* Число повторений, приходящихся на тип канала (см. 9.3.5): СРЗ/1: 15 (МЭК61158-6-3: максимум 8);

СР3/2: 15 (МЭК61158-6-3: 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 1F4ACF813h; Полиномы черного канала не должны делиться на C599h.

* + Элементы сети активной буферизации:

СР 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 безо­ пасности:

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.

* + 1. 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:
* СРЗ/1: Никаких ответвлений.
* СР 3/RTE: Один F->.oc t на подмодуль.
* Коммутаторы Ethernet должны подходить для стандартных промышленных сред, как это опре­ делено, например, в МЭК 61131-2.

Стандартные устройства *а* устройства безопасности могут использовать один источник питания

в 248.

* 1. Техническое обслуживание
     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 v только после подтверждения оператора (ОА\_С).

* + 1. 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

96

ГОСТ Р МЭК 61784-3-3—2016

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

* 1. Руководство по безопасности

В соответствии с МЭК 61508-2. поставщики F-хоста и F-устройства должны предоставлять руко­ водство 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.'ипи параметр | Примечание |
| Работа с безопасностью | Инструкция 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 электричес­ кой безопасности (PELV). колебаний, шума, прерыва­ ний и т .д. | См. (44] ограничения, зави­ сящие от страны, такие как ограничения на ток |
| Электрическая безопас­ ность | Все сетевыэ устройства, используемые в совокупности с этим устройством должны соответствовать требованиями стандарта МЭК61010-1 илиМЭК61131-2(напримвр.РЕ1Л/) | См. (44] |
| Электромагнитная устойчивость. ЭМП | Применяемые испытания и их результаты (заявление производителя или последний огчет из компетентной тестовой лаборатории) | В соответствии с МЭК 62061. МЭК 61326-3-1 или  МЭК 61326-3-2 все. что при­  менимо. 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 эксплуатацюо | Использование контрольного листа из МЭК 61764-5-3. например, для грамотной адресации, проверке повторе­ ний. ка-юстэу оип«ала и т. п. | См. также [65] |
| параметр | Верификацтя функций безопасности должна включать проверку того, все ли F\_iPar\_CRC > «0» | См. 8.6.4.5 |
| Техническое обслужи­ вание | Условия и процедуры для замены частей: идентификация | См. 9.6 |
| Жизненный цикл | Значенив(жя) интервала контрольных испытаний | В соответствии с МЭК 61508 |
| Время реакции | Значения параметров DAT. WCDT. WDTcme | См. 9.3.2 и 9.3.3 |
| Безопасность оборудо­ вания (электрическая) | Значения параметров: заявленного УПБ. PFH (вероят­ ность отказа в час) | В соответствии с МЭК 62061 |
| Безопасность оборудо­ вания (не электричесхая) | Значения гараметров для PL (Уровня эффективности защиты). MTTFd (средняя наработка на отказ) | В соответствии с ИС013849- 1 |
| Безопасность для авто­ матизации процесса | Значения параметров: заявленного УПБ. PFD (вероят­ ность отказа по запросу), возможности соединения для достижения более высокого УПБ | В соответствии с МЭК 61511 и [30] |
| Защита | Инструкциипо установлению адекватного уровня защиты, зон защити 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 безопас­ ности от компетентных органов оценки | См. [45] и раздел 10 |

97

ГОСТ Р МЭК 61784-3.3—2016

* 1. Беспроводные каналы передачи данных
     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.

* + 1. Готовность

Одной из основных трудностей, связанных с беспроводной передачей, является обеспечение до­ статочной 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).

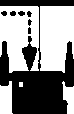
* + 1. Средства защиты

Перед вводом в эксплуатаьию 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-устройстеа и программ безопасности;
* атаки на циклические коммуникации, например, симуляция коммуникации безопасности.

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

Магистраль промышленной се\*и Ethernet

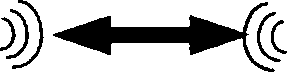
*^конфигурация*

* -гирогъная фрви (доступ)

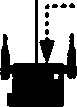
! -Проеоднсждостул

; -ззиъвр»

! -Реж1\*л инфраструктуры

*Шифрование*

Магистраль промышленной сети Ethernet

* + ................................. Т

*Конфигурация* |

- Парольная фраза (доступ! •

* + Проводной доступ •
  + SSLtilpa ;
  + Реаиы инфраструктуры !

! • Скрытый «Ю I • Парольная фра» или

* сертификат

»

I»

*Точки*

*доступа*

-AES-CCMP.

связанный с УУРА2

беспроводные

клиенты

* Скрытый SSD !
* Парольная фреза или !

сертификат |



*Инструмент*

*Парольная* фра»

->• 20Симеолов

* AZ.U, 0..9, !..&
* Нет произаогънол) пароля

*Аут&тифихация*

* + Дяцситрап идо иыыая (ру'аюй подход. Ключ, заранее сделвгыьй общедостугньм) или
  + Централизованная метод использующий сервер

*Парольюя фрааа.*

**->■ 20 Символов**

* + A. .Z. а..2,0.9. !..& *U*
  + Нет проиэвотъного пароля

*IfacmpyiAeHm*

*конфиеурироеания*

аутентификации, например.

RADIUS

*конфи зурироеания*

Рисунок 84 — Защита для WLAN сетей

Ниже описаны термины, использованные на рисунке 84:

AES-CCMP — продвинутый стандарт шифрования — протокол блочного шифрования с кодом аутентич­ ности сообщения и режимом сцепления блоков и счетчика:

RADIUS — услуга удаленной аутентификации звонящего; SSID — идентификатор набора услуг.

SSL — уровень защищенных сокетов;

98

ГОСТ Р МЭК 61784-3-3—2016

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

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

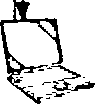
|  |  |  |
| --- | --- | --- |
| № | Элемент | Средство |
| 1 | Администрирование беслроводюй точки доступа и беспроводного клиента | Разрешен только проводной доступ посредством SSL или https. Па- ропь/парольная фраза администрации не должен быть паролем по умолчанию |
| 2 | Качество парольной фразы 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* подк­ лючения не должен быть задействован |
| 4 | Подходы к аутентификации | Разрешен либо *Децентрализованный подход* (ручной ввод в действие ключей аутентификации) или *Централизованный подход* (специализи­ рованный сервер аутентификации, например. RADIUS). В случае цен­ тральной 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 (Предва­ рительно выданный секрет), либо *Сертификаты* |
| 6 | Качество парольной фразы для шифрования | Длина парольной фразы должна быть 20 символов (см. (26] Н.4 Пред­ лагаемое 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 каче­ стве 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, гак 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.

99

ГОСТ Р МЭК 61784-3.3—2016

Магкстраль прамдесчде сети ЕОМЛ144



| И’рмдМмурвим ;1

Мстетраль грочмипвжой сети EVwrwt

ктрыляш\* ‘1

J

| .Mioapt и \_

\* - Парапкая\* «вам М\*сгщ1, L

**^)<3=Кс ^**

n««iiu»Mau И«ет«п|

1ПромвиМ ДК-у»

* + - 1>ММЫММП1«

Точки доступа

ЩмфсМк *8МФШ>*

РАМ

-Про1ММ1 8NEP

ПЮМЖА Oortya !

*(Ьсфю&ь\* • Гшг\* Хмчты* -нв\*\*\*п«мт\*

*(PAMJ)* • Пн«ы«Мш>

1 *(NAP)*

|Мд(ашм

* Стммртмес шиХдоммс
* СОСГМТСШШ С IEEE

nnxv\*"a«4MM

•»• го Снижало\*

* + AZlit.l.'-\*

•Н\*1 орошмлмми

пвропв

Инструмент

*конфиауриоовани\**

«0151

A~~|W»«ul>~~H~~\*~~|iir

* + Двцгнгрвтдовви~~ы~~»

ipV^MlA ГСД>«Д Know шраме wkUMWi 06tWWC<r«>\*\*MI

PiMi Mi^rrw 3 (мцита

обвспг ~~м~~ввамо~~и~~ — уроаж

икала)

Л\*ролым«

•» 30 Символов

• A..Z. • Д, 0.1.' 4

* Her вроювольиоао

пароля

Инструмент

<№Aj>uj>popoee»un

Рисунок 85 — Защита для Bluetooth сетей

SSL PAN BNEP NAP

Ниже описаны термины, использованные на рисунке 85:

* уровень защищенных сокетов;
* персональная сеть;
* протокол инкапсуляции сети Bluetooth;
* точка доступа к сети;

PAN U

Точка доступа

* пользователь персональной сети;
* координационная станция (ведущее устройство) беспроводной пикосети в соответствии с ИИЭР 802.11;

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

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. Скагтврнег сети не должны быть задействованы |
| 4 | Подходы к аутенгификацют | Bluetooth устройства должны использовать защитный режим 3 (при- нудитегъная защита канального уровня), как это определено в обя­ зательном для применения ИИЭР 802.15.1 .Аутентификация реализуется е 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 | Дгына парольной фразы должна быть 16 символов. Символы должны представлять собой смесь буквенных, цифровых и специальных знаков. |
| 6 | Шифрование цикгыческого обмена данными (PDU безопасности) | Шифрование в соответствии с ИИЭР 802.15.1 является обязательным |

100

ГОСТ Р МЭК 61784-3-3—2016

*Окончание таблицы 18*

|  |  |  |
| --- | --- | --- |
| Nt | Элемент | Средство |
| 7 | Открытость | Точка беспроводного доступа и клиенты должш 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 манипулящш данных. | | |

* + 1. Стационарные и мобильные приложения

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

Нет никаких ограничений или специальных оценок для стационарных приложений, таких как. циклические системы наполнения *а* 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 | Аатоматиээцуя работы пред­ приятия | Автоматизация процесса | Примечание |
| Поддержка GSD | V5.04 (PB-DP) из [43J; V2.0  (PN-IO) из (47) или более поздние версии | То же самое | Затрагивает только F-лараметры |
| Функциональные блоки коммуникаций в соответствии с МЭК 61131-3 | Минимальный набор функциональных коммуникационных блоков это: RDREC, WRREC. RD1AG, RALRM  (49) | То же самое | Поддержка MS1 является предусловием. Не обязатель­ но для других прикладных профилей:  GETIO PART.  SETIO.PART |
| iflap-cepeep | Производители системы должны предоставлять услуги «шар-сервера» с минимумом 21S октетов | То же самое | Производителям систем настоятельно рекомендуется предоставлять следующие фукхционагъные блоки ком­  муникаций: RDREC. WRREC. RDIAG (RALRM) (49] |
| Количество (биты) | Максимум 64 бита (логиче­ ский тип), закодированных как Unsigned^. -16. -32 | То же самое | Размеры поддерживаемых ми­ нимальных структур данных |
| Количество (типы данных) | 12 октетов 1/0 | То же самое | Размеры поддерживаемых минимальных структур  данных |
| Тилы данных | Unsigned8. -18. -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-xocra | Все сигналы | Все сигналы |  |

101

ГОСТ Р МЭК 61784-3.3—2016

Окончание *таблицы 23*

|  |  |  |  |
| --- | --- | --- | --- |
| Элемент | Лотомэимаиия работы пред\* приятия | Аотоматимция процесса | Примечание |
| Диагностика | Настоятельно рекомендуе­ мые: сообщения об ошиб­ ках уровня безопасности (6.3.2) | Настоягетъно рекомен­ дуемые: сообщения об ошибках уровня безо­ пасности (6.32) | Рекомендуемая литература: [50] |
| MSI | обязательно | обязательно | В соответствии СР 3/1 |
| MS2 | Не через юнтроллер (PLC) | не обязагвтъно | Малые CPU могут не обес­ печить проходную мощность интенсивного графмса |
| Заявляемый УПБ | 3 (в областях специальных приложений, таких как CNC; минимальный уровень 2) | 3 |  |
| Интеграция инстру­ ментальных средств, параметризация | Интерфейс инструменталь­ ных средств, соответствую­ щий требованиям таблицы 12 | В соответствии с [63] или через интерфейс инстру­ ментальных средств, соответствующий требованиям таблицы 12 |  |

1. Оценка
   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, е 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 надлежащее процессы разработки, соответствующие стандартам безопасности (см. МЭК 61508. МЭК 61511. МЭК 60204-1. МЭК 62061. ИСО 13649-2) 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 е результате завершенных запросов на изменение, должна быть рассмотрена для ее применения и оценки. Подобная информация может быть приобэетена у организаций, перечисленных в Приложении В.

Полная информация также доступна в [66].

* 1. 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 fix Arbertsschutz / BG — Институт профессиональной безопасности и здравоохранения^ 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 da SBcuritB) во Франции.

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

102

ГОСТ Р МЭК 61784-3-3—2016

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 результа­ том модификации данных. С ее помощью также можно обнаруживать последовательные ошибки, так как проверка сигнатуры учитывает последовательность слов.

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

void crc24\_calc(unsigned char х. insigned long \* г) inti;

for (i = 1; i <= 8; i++)

*d* ((boot)(\*r & 0x800000) != (booIXx & 0x80))

*Г* XOR = 1 => Сдвиг и обработка полинома V

•r = ('r« 1) А 0x5D6OCB:

else

*Г* XOR = 0 => pure shift *1*

\*r*s* ’г « 1;

x = x « 1;

*Г* for V

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

Огттикшзированный 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:

г = cxtab24 [((г » 16) А \*g++) & Oxff] Л (г « 8). (А.1)

где:

* *г* представляет собой результат 24-битовой CRC сигнатуры;
* *q* представляет собой указатель на фактическое значение октета, для которого необходимо вычислить

CRC. После считьеания значения указатель должен быть увеличен для следующего октета посредством q++:

- начальное значение г равное х0». Для этого вычисления используется табтца А.1.

Таблица А.1 - Таблица «Сгс1аЬ24в для вычислений 24-битовой CRC сигнатуры Таблица А.1 — Таблица яСгс(аЬ24» для вычислений 24-битовой CRC сигнатуры

Справочная таблица CRC (0...2S5)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0x000000 | 0X5D6DCB | 0хВА0В9б | 0хЕ7В65О | 0х28ОАЕ7 | 0х75В72С | 0x920171 | ОхСРбСВА |
| 0x51 В5СЕ | 0X0CD805 | 0хЕВ6Е58 | ОхВбОЗЭЗ | 0X796F29 | 0х2402Е2 | 0XC3B4BF | 0х9ЕО974 |
| ОхАЗбВЭС | 0XFE0657 | 0х19В03А | 0x44 DDC1 | 0х8ВВ17В | ОхОбОСВО | 0X316AED | 0х6С0726 |
| 0XF2DES2 | 0xAFB399 | 0х4805С4 | 0X15680F | 0хОА04В5 | 0х87697Е | 0x600F 23 | 0X3DB2E8 |
| ОхШВАРЗ | 0x460738 | 0хА16155 | OxFCOCAE | 0x336014 | 0X6E0DDF | 0х89ВВ82 | 0x040649 |
| 0X4A0F3D | 0X1762F6 | 0XF0D4AB | ОхАОВЭбО | 0X62D5DA | 0X3FB811 | 0хО80Е4С | 0x856387 |
| 0XB8D16F | 0хЕ5ВСА4 | 0х020А=9 | 0X5F6732 | Ох900В88 | 0XCD6643 | 0x2 A DO 1Е | 0X77BDD5 |
| 0хЕ964А1 | 0хВ4096А | 0X53BF37 | 0X0ED2FC | 0хС1ВЕ46 | 0x900380 | 0x766500 | 0x26081В |
| 0х3775Е6 | 0X6A182D | 0х8ОАЕ70 | ОхООСЗВВ | 0X1FAF01 | 0х42С2СА | 0хА57497 | 0XF8195C |
| 0х66С028 | ОхЗВАОЕЗ | 0XDC1BBE | 0x817675 | 0х4Е1 ACF | 0x137704 | 0XF4C159 | 0хА9АС92 |

103

ГОСТ Р МЭК 61784-3.3—2016

*Окончание таблицы А. 1*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Справочная таблица CRC{0...2SS) | | | | | | | |
| 0x941Е7А | 0хС973В1 | 0х2ЕС5ЕС | 0х73А827 | 0x800490 | 0хЕ1А956 | 0X061F0B | 0x587200 |
| 0ХС5АВВ4 | 0X98C67F | 0X7F7022 | 0x221DE9 | 0XED7153 | 0хВ01С98 | 0х57ААС5 | 0х0АС70Е |
| 0X2CCF15 | 0x71 A2DE | 0x961483 | 0хСВ7948 | 0x0415F2 | 0x597839 | 0хВЕСЕ64 | 0XE3A3AF |
| 0X7D7ADB | 0x201710 | 0XC7A14D | 0х9АСС86 | 0х55А0ЭС | 0X08CDF7 | 0XEF7BAA | 0хВ21661 |
| 0X8FA489 | 0XD2C942 | 0X357F1F | 0x681204 | 0хА77Е6Е | 0XFA13A5 | 0X1DA5F8 | 0x400833 |
| ОхОЕ1147 | 0х837С8С | 0х64САО1 | 0х39А71А | 0XF6CBA0 | ОхАВАббВ | 0x401036 | 0X117DFD |
| ОхбЕЕВСС | 0x338607 | 0XD4305A | 0x895091 | 0x46312В | 0X1B5CE0 | OxFCEABD | 0хА18776 |
| 0X3F5E02 | 0х6233С9 | 0x858594 | 0XD8E85F | 0х1784Е5 | 0х4АЕ92Е | 0XAD5F73 | 0XF032B8 |
| ОхСОбОбО | ОхЭОЕОЭВ | 0х775ВС6 | 0X2A360D | 0хЕ55АВ7 | 0хВ8377С | 0X5F8121 | 0х02ЕСЕА |
| 0х9С359Е | 0хС15855 | 0х26ЕЕ08 | 0х7В83СЗ | 0XB4EF79 | 0хЕ982В2 | 0X0E34EF | 0x535924 |
| 0X75513F | 0X283CF4 | 0XCF8AA9 | 0х92Е762 | 0x508608 | 0х00Е613 | 0хЕ7504Е | 0XBA3D85 |
| 0X24E4F1 | 0х79693А | 0X9E3F67 | 0хС352АС | 0х0СЗЕ16 | 0x515300 | 0хВ6Е580 | 0хЕВ884В |
| ОхОбЗААЗ | 0х8В5768 | 0х6СЕ135 | 0X318CFE | 0XFEE044 | 0XA38D8F | 0X443BD2 | 0x195619 |
| 0X878F6D | 0XDAE2A6 | 0x3054FВ | 0x603930 | 0XAF5S8A | 0XF23841 | 0х158Е1С | 0X48E3D7 |
| 0х599Е2А | 0X04F3E1 | 0хЕ545ВС | 0хВЕ2877 | 0x714400 | 0x202906 | 0XCB9F5B | 0X96F290 |
| Ох082ВЕ4 | 0X55462F | 0XB2F072 | 0XEF9DB9 | 0X20F103 | 0x709008 | 0х9А2А95 | 0хС7475Е |
| 0XFAFSB6 | 0XA7987D | Ох402Е20 | 0X1D43EB | 0XD22F51 | 0X8F429A | 0X68F4C7 | 0x359900 |
| 0хАВ4078 | 0XF62D83 | 0х119ВЕЕ | 0X4CF625 | 0X839A9F | 0XDEF754 | 0x394109 | 0х642СС2 |
| 0x422409 | 0X1F4912 | 0XF8FF4F | 0хА59284 | ОхбАРЕЭЕ | 0X3793F5 | 0хО025А8 | 0x804863 |
| 0x139117 | 0X4EFCDC | 0хА94А81 | 0XF4274A | 0X3B4BF0 | 0x66263В | 0x819066 | OxDCFDAD |
| 0XE14F45 | 0хВС228Е | 0X5B94D3 | 0X06F918 | 0хС995А2 | 0x94F869 | 0х734Е34 | 0x2E23FF |
| 0XB0FA8B | 0XED9740 | 0х0А2110 | 0x5740 06 | 0x962060 | 0XC54DA7 | 0X22FBFA | 0x7F9631 |
| Примечание — *1* аргумента а в функции сгс до нижнего правого (255). | | энная таблица содержит 24-битовые значения для каждого значения (0...255) 1аЬ24(а]. Таблица должна читаться в восходящем порядке, от верхнего левого (0) | | | | | |

Соответствующая функция (А.1) в языке программирования С для вычислений 32-битовой CRC подписи при Iюмищи ицлиючныл iHGiinq пикамча ниже.

г = сгс1аЬ32 [((г » 24) л \*q ++) & Oxff] А (г « 8). (А.2) Для этого вычисления используется таблица А.2.

Таблица А.2 —Таблица «Сгс1аЬ32» для вычислений 32-битовой CRC сигнатуры

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Справочная таблица CRC (0...2SS) | | | | | | | |
| 00000000 | F4ACFB13 | 1DF50D35 | E959F626 | ЗВЕА1А6А | CF46E179 | 261F175F | 02ВЗЕС4С |
| 77043404 | 8378CFC7 | 6А2139Е1 | 9E80C2F2 | 4СЗЕ2ЕВЕ | B892D5AD | 51СВ238В | A567D898 |
| EFA869A8 | 1В0492В8 | F2506490 | 06F19F8E | D44273C2 | 20EE88D1 | C9B77EF7 | 301В85Е4 |
| 987C5D7C | 6COOA66F | 85895049 | 7125АВ5А | А3964716 | 573АВС05 | ВЕ634А23 | 4ACFB130 |
| 2BFC2843 | OF50O350 | 36092576 | С2А50Е65 | 10163229 | Е4ВАС93А | 0DE33F1C | F94FC40F |
| 50281С97 | А884Е784 | 41DD11A2 | В571ЕАВ1 | 67C206FD | 936EFDEE | 7А370ВС8 | 8E9BFOOB |
| С45441ЕВ | 30F6BAF8 | 09А\*4С0Е | 2D0DB7CD | FFBE5B81 | 0812А092 | Е24В56В4 | 16E7ADA7 |
| B380753F | 472С8Е2С | АЕ75780А | 5А098Э19 | 886A6F55 | 7СС69446 | 959F6260 | 61339973 |
| 57F85086 | А354АВ95 | 4A0D5DB3 | ВЕА1А6А0 | 6С124АЕС | 98BEB1FF | 71E747D9 | 854ВВССА |
| 202С6452 | D4809F41 | 30096967 | С9759274 | 1ВС67Е38 | EF6A852B | 06337300 | F29F881E |

104

ГОСТ Р МЭК 61784-3-3—2016

*Окончание таблицы А.2*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Справочная таблица CRC (0...2SS) | | | | | | | |
| В850392Е | 4CFCC23D | А5А5341В | 5109CF08 | 838А2344 | 7716D857 | 9E4F2E71 | 6АЕ30562 |
| CF840DFA | 3B28F6E9 | D27100CF | 26DDFBDC | F46E1790 | ООС2ЕС83 | Е99В1АА5 | 1D37E1B6 |
| 7С0478С5 | 88A883D6 | 61F175F0 | 95508ЕЕЗ | 47EE62AF | В34299ВС | 5A1B6F9A | АЕВ79489 |
| 06004С11 | FF7CB702 | 16254124 | Е289ВА37 | 303А567В | C496AD6B | 20CF5B4E | D963A050 |
| 93AC116D | 6700ЕА7Е | 8Е591С58 | 7AF5E74B | А8460В07 | 5CEAF014 | В5В30632 | 411FFD21 |
| Е47825В9 | 1004DEAA | F98D283C | 0021D39F | DF923FD3 | 2ВЗЕС4С0 | С26732Е6 | 36CBC9F5 |
| AFF0A10C | 5B5C5A1F | В205АС39 | 46А9572А | 941АВВ66 | 60В64075 | 89EFB653 | 7D434D40 |
| 08249508 | 2С886ЕСВ | C5D198ED | 317D63FE | E3CE8FB2 | 176274А1 | FE3B8287 | 0А977994 |
| 4058СВ А4 | B4F433B7 | 50ADCS91 | А9013Е82 | 7BB2D2CE | 8F1E29DO | 6647DFFB | 92ЕВ24Е8 |
| 378CFC70 | С3200763 | 2A79F145 | DED50A56 | 0С66Е61А | F8CA1D09 | 1193EB2F | E53F103C |
| 840C894F | 70А0725С | 99F984TA | 6D557F69 | BFE69325 | 4В4А6836 | А2139Е10 | 56BF6503 |
| F3D8BD98 | 07744688 | EE2DB0AE | 1A814BBD | C832A7F1 | ЗС9Е5СЕ2 | D5C7AAC4 | 216В5107 |
| 68А4Е0Е7 | 9F081BF4 | 7651EDD2 | 82FD16C1 | 504EFA8D | А4Е2019Е | 4DBBF7B8 | В9170САВ |
| 1C70D433 | E8OC2F20 | 0185D936 | F5292215 | 279АСЕ59 | 0336354А | 3A6FC36C | CEC3387F |
| F808F18A | 0СА40А99 | E5FDFC8F | 115107 АС | СЗЕ2ЕВЕ0 | 374E10F3 | DE17E6D5 | 2ABB1DC6 |
| 8FDCC55E | 7B703E4D | 9229С86В | 66853378 | B436DF34 | 409А2427 | АЭС30201 | 5D6F2912 |
| 17А09822 | Е30С6Э31 | 0А559517 | FEF96E04 | 2С4А8248 | D8E6795B | 31BF8F7D | С513746Е |
| 6074ACF6 | 94D857E5 | 7D81А123 | 892D5AD0 | 569ЕВ69С | AF324D8F | 466ВВВА9 | В2С740ВА |
| D3F4D9C9 | 275822DA | CE01D4FC | 3AAD2FEF | Е81ЕСЗАЗ | 1СВ238В0 | F5EBCE96 | 01473585 |
| A420ED1D | 508С160Е | В9О5Е028 | 40791ВЗВ | 9FCAF777 | 6В660С64 | 823FFA42 | 76930151 |
| ЗС5СВ061 | C8F04B72 | 21A9BD54 | 05054647 | 07В6АА0В | F31A5118 | 1А43А73Е | EEEF5C20 |
| 4В8884В5 | BF247FA6 | 56708930 | A2D17293 | 70629EDF | 84СЕ65СС | 609793ЕА | 993668F9 |

Примечание — Данная таблица содержит 32-битовые значения в шестнадцатеричном представлении для каждого значения (0.. .255) аргумента а в функции сгс(аЬ32(а]. Таблица должна читаться в восходящем поряд­ ке верхнего левого (0) до нижнего правого (255).

А.2 Измерения времени реакции

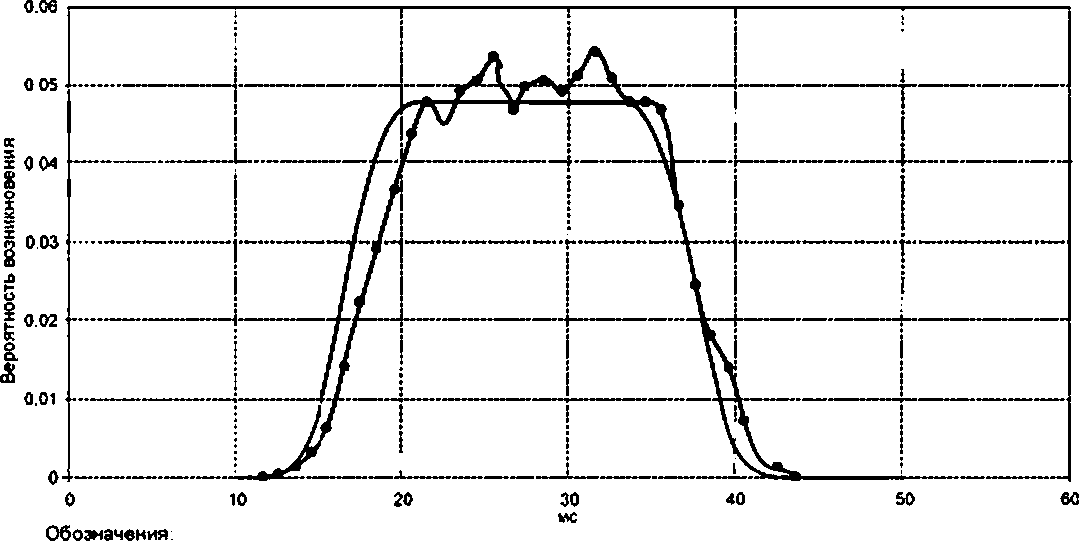
В 9.3.1 описана упрощенная модель для типичного времени реакции. Сравнение этой модели и реального приложения, полученного от различные поставщиков, для 15000 образцовых измерений показано на рисунке А.2. В данном случае скорость передачи была 1.5 Мбит/с и F-xocr выполнял приложение, связанное с безопасностью, (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.З показана гистограмма вре­ мени реакции настоящего приложения СР 3/1 и FSCP 3/1, полученного от множества поставщиков, при 1.5 Мбиг/с и в двух разных стрессовых ситуация».. Синяя кривая представляет собой 22 000 измерений с независимым PLC безопасности. Темно синяя кривая представляет собой б 500 измерений с тем же PLC, дополнительным програм­ матором (PG). периодически отображающим статус программы, и диагностической панелью (PC), периодически отображающей статус лучей световой завесы. PG и PC взаимодействовали посредством не периодических услуг СР 3/1 (класс 2 ведущего устройства).

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

105

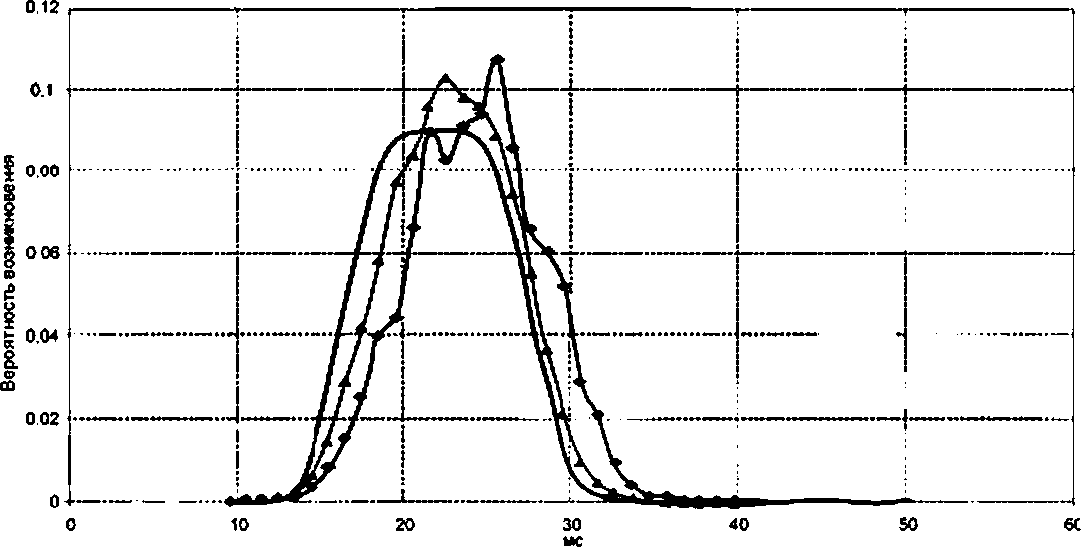
ГОСТ Р МЭК 61784-3.3—2016



-15000 измерений:

-модель

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



Обозначения

-------- --- модель с одкт Р1С,

—\*— - 22000 измерений с одним PLC.

—- 6500 измерена\* с PLC и PG/PC

Рисунок А.2 — Распределение частот измеренного времени реакции

106

ГОСТ Р МЭК 61784-3-3—2016

Значения цветов, использованных на рисунке А.Э. приведены ниже: циан — модель, включающая один PLC (CPU):

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

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 сегмен­ таций стандартной программы для несхольких значений временного триггера. Эго демонстрирует, что изменение в части стандартной программы не сказывается на выполнении программы безопасности. Тем не менее, мажет быть важно сбалансировать обновление стандартных выводов и выводов безопасности, если необходимо использовать сигналы из другой части для целей координации.

Стандартная программа: 30 мс Программа безопасности: 5 мс

Стандартная программа Обновление стандартных выводов

**..........................** *t*

#### Н+ПЧ>Г>~ТРГ>П

ю 20 30 40 SO 60

**Триггер мремеми**

каждые 10 мс

мс

Стандартная программа

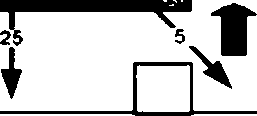
## \*

20

**t**Обновление стандартных выводов

40 60 мс

Триггер времени каждые 20 мс

Стандартная программа Обновление стандартных выводов

30 60 мс

Триггер времени

. каждые 30 мс

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

107

ГОСТ Р МЭК 61784-3.3—2016

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:

PROF18US Nutzerorganisatior e.V. (PNO) Hatd-urtd-Neu-Slr. 7

76131 Karlsruhe GERMANY

Phone: +49 721 96 58 590 Fax: +49 721 96 58 589

E-mai: [info@profibus.com](mailto:info@profibus.com) URL[www.profibus.com](http://www.profibus.com/) or URLwwvv.profisafe.net

108

ГОСТ Р МЭК 61784-3-3—2016

Приложение ДА (справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА. 1

|  |  |  |
| --- | --- | --- |
| Обозначение ссылочного международного стандарта | Степв«< соотеетспия | Обозначение и наименование соответствующего национального, межгосударственного стандарта |
| IEC 60204-1 | IDT | ГОСТ Р МЭК 60204-1—2007 «Безопасность машин. Электрооборудо­ вание 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 электро­  магнитным помехам технических средств, применяемых в промыш­ ленных 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 примене­  ния. 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 | - | в |
| 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 | - | в |
| IEC 61326-3-2 | — | в |
| IEC 61508 (все части) | IDT | ГОСТ Р МЭК 61508—2012 (все части) «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» |
| IEC 61506-2:2010 | IDT | ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связан­ ных с безопасностью. Часть 2. Требования к системам» |
| IEC 61511 (все части) | IDT | ГОСТ Р МЭК61511-1—2011 «Безопасностьфункциональная. Системы безопасности приборные для промышленных процессов» |
| IEC 61784-1 | - | • |
| IEC 61784-2 | - | в |
| IEC 61784-3:2010 | - | в |
| IEC 61784-5-3 | - | в |
| IEC 61918 | - | в |
| IEC 62061 | IDT | ГОСТ Р МЭК 62061—2013 «Безопасность оборудования. Функцио­ нальная безопасность систем управления электрических, электрон­ ных и программируемых электронных, связанных с безопасностью» |
| IEC 62280-1 | - | в |
| IEC 62280-2 | - | в |

109

ГОСТ Р МЭК 61784-3.3—2016

*Окончание таблицы ДА. 1*

|  |  |  |
| --- | --- | --- |
| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального, межгосударственного стандарта |
| IEC/TR 62390 | - | в |
| ISO 13849-1 | IDT | ГОСТ Р ИСО 13849-1—2003 «Безопасность оборудования. Элементы  систем управления, связанные с безопасностью. Часть 1. Общие принцигы 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 | ЮТ | 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.   П р и м е ч а н и е — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:   * 1DT — идентичный стандарт: * MOD — модифицированный стандарт. | | |

110

ГОСТ Р МЭК 61784-3-3—2016

Библиография

[I] IEC 60050 (all parts). International Electrotechnical Vocabulary

Примечание — См. также IEC Multilingual Dictionary — Electricity, Electronics and Telecommunications (доступно на CD-ROM Mat <[http://wwwalectropedia.org](http://wwwalectropedia.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 ard electronic equipment with regard to electromagnetic phenomena

(4] IEC 61131-612. Programmable cor (rollers — 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/eiectronic/programmable electronic safety-related systems — Pari 1: General requirements

{8] IEC 61508-4:2010. Functional safety of eiectrical/electronic/programmable electronic safety-related systems —

Part 4: Definitions and abbreviations

(9] IEC 61508-5:2010. Functional safety of eiectrical/eiectronic/programmable electronic safety-related systems —

Part 5: Examples of methods for tlw 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

(II] IEC 61784-4. Industrial communication networks — Profiles — Part 4: Secure communications for fietdbuses

(12] IEC 61784-5 (all parts). Industrial communication networks — Profiles — Part 5: Installation of fietdbuses — Installa­ tion profiles for CPF x

(13] IEC 61 BOO-5-2. Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional (14] IEC 61804 (alt 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 (alt parts), Industrial communication networks — Network and system security

(18] ISO/1EC Guide 51:1999. Safety aspects — Guidelines for their inclusion in standards

(19] ISO/1EC 2382-14. Information technology — Vocabulary — Part 14: Reliability, maintainability and availability (20] ISO/1EC 2382-16. Information technology — Vocabulary — Part 16: Information theory

(21] ISO/1EC 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 tech­ nology — Telecommunications and information exchange between system — Local and metropolitan area networks

— Specific requirements — Pari 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifi­ cations — Amendment 6: Medium Access Control (MAC) Security Enhancements

(27] IEEE 802.15.1-2005: IEEE Slandaid for Information technology — Telecommunications and information exchange between systems-Loca! and metropolitan area networks — Specific requirements

(28] ANSI/lSA-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] VDl/VDE-Richtiinien 2180. Part 1-4: 2006, Safeguarding of industrial process plants by means of process control engineering, (in German language)

(31] GS-ET-26. Grundsatz fur die Prufung und Zerlifizterung von Bussystemen fur die Obertragung sicherheitsrelevanter Nachrichten. May 2002. HVBG. Gustav-Heinemann-Ufer 130. D-50968 Koln (\*Principles for Test and Certification of Bus Systems for Safety relevant Communication\*)

(32] ANDREW S. TANENBAUM. Computer Networks. 4th Edition. Prentice Hall. N.J.. IS6N-10:0130661023. ISBN-13:

978-0130661029

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

(34] BRUCE P. DOUGLASS. Doing Hard Time. 1999. Adcbson-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 Schafer. BG-lnstitute 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 Standarc for Industrial Machinery

111

ГОСТ Р МЭК 61784-3.3—2016

(39] GUY Е. 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. STEF4N BRAUER. 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: Ar Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communi­

cation. Journal of Applied Computer Science. Vol. 14, No 1. pp. 57-80. Technical University Press. L6di,Poland. 2006

(42] SCHILLER F and MATTES T: Aratysis of CRC-polynomiais for Safety-critical Communication by Deterministic and Sto­ chastic Automata. 6th IFAC Synposium on Fault Detection. Supervision and Safety for Technical Processes. SAFE-

PROCESS 2006. pp. 1003-100®. 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: PROFlsfefe — 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. Or­ der-No. 2.242

(46] PROFIBUS Profile Guideline. Pari 1: Identification & Maintenance Functions. V1.2. October 2009. Order-No. 3.502

(47] PROFIBUS Guideline: GSDML Specification for PROF1NET 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. Pari 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 Raoid 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.opcfoindation.org](http://www.opcfoindation.org/) >

(57] Object Management Group. Untied Modeling Language: Superstructure. Version 2.0: Formal/05-07-04:available at < [www.omg.com](http://www.omg.com/) >

(58] NAMUR. NE97 — FieWbus for safety-related uses. 2003: available at < [www.namur.de](http://www.namur.de/) > (59] REC-xrrt-20081126. Extensible Markup Language (XML) 1.0 (Fifth Edition) — W3C

Recommendation 26 November 2008. available at < [www.w3.org/TR/2008/REC-xml-2008112e](http://www.w3.org/TR/2008/REC-xml-2008112e)>

(60] REC-xmlschema-1-20041028. XML Schema Part 1: Structures {Second Edition) — W3C Recommendation 28 Octo­ ber 2004. available at < [www.w3.org/TR/2004/REC-xmlschema-1](http://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](http://www.w3.org/TR/2004/REC-xmlschema-2-20041028) >

(62] USB Implementors 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. VI .01. March 2009: Order-No. 3.042

(04) PROFIBU3 Guideline. Cabling and Assembly. VI.0.0. May 2000. Oidet No. 0.022

1. PROFIBUS Guideline: Commissioning, VI .0.2. November 2006. Order No. 8.032
2. PROFIBUS Guideline: PROFIsafe Policy. VI .3. February 2003. Order No. 2.282
3. PROFIBUS Profile Guideline. Fart 2: Data types. Programming Languages, and Platforms. V1.0. September 2006.

Order-N. 3.512

1. PROFIBUS Specification: Amendment PROFkJnve on PROFIsafe. V2.1. April 2009. Order-No. 3.272
2. PROFINET Specification: Configuration in Run. dV0.1. August 2009. Order-No. 2.512

112

ГОСТ Р МЭК 61784\*3-3—2016

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

113

Редактор *А.Ф. Котим* Технический редактор *В.И.* Прусакова Корректор *С.И. Фирсова* Компьютерная верстка *А.С. Тыртышмого*

Сдано в набор 22. !2.20'б. Подписано о печать 26.01.2017. Формат 60 \* 64 *1/в.* Гарнитура Ариап.

Усп. п\*ч. n.13.9S. Уч.-иад. л. 12.62. Тира\* 27 эм За\*. 223.

Подготоапеио на основа электронной версии, предоставленной разработчиком стандарта

Издано и отпечатан» во ФГУП «СТЛНДАРТИНФОРМ». 123995 Moctaa. Гранатный пер., 4. [www.90slinto.ruTitoggo 5bnfo.ru](http://www.90slinto.ruTitoggo5bnfo.ru/)