ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61131-6— 2015

КОНТРОЛЛЕРЫ ПРОГРАММИРУЕМЫЕ

Часть 6

Безопасность функциональная

IEC 61131-6:2012
Programmable controllers — Part 6: Functional safety
(IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 18 мая 2015 г. № 363-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61131-6:2012 «Контроллеры программируемые. Часть 6. Безопасность функциональная» (IEC 61131-6:2012 «Programmable controllers — Part 6: Functional safety», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2016

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

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 2
3 Термины и определения ... 4
4 Соответствие настоящему стандарту ... 14
5 Жизненный цикл ПЛК-ФБ ... 15
5.1 Общие положения ... 15
5.2 Требования к функциональной безопасности и предельному значению УПБ ПЛК-ФБ ... 17
5.3 Система менеджмента качества ... 19
5.4 Управление жизненным циклом ПЛК-ФБ ... 19
6 Спецификация требований к проектированию ПЛК-ФБ ... 23
6.1 Общие положения ... 23
6.2 Содержание спецификации требований к проектированию ... 23
6.3 Целевая интенсивность отказов ... 24
7 План проектирования, разработки и подтверждения соответствия ПЛК-ФБ ... 26
7.1 Общие положения ... 26
7.2 Сегментирование требований ... 26
8 Архитектура ПЛК-ФБ ... 26
8.1 Общие положения ... 26
8.2 Архитектуры и подсистемы ... 27
8.3 Передача данных ... 27
9 Планирование проектирования, разработки и подтверждение соответствия аппаратных средств ... 27
9.1 Общие требования к аппаратным средствам ... 27
9.2 Спецификация требований функциональной безопасности аппаратных средств ... 27
9.3 Планирование подтверждения соответствия безопасности аппаратных средств ... 28
9.4 Проектирование и разработка аппаратных средств ... 28
9.5 Аппаратные средства и встроенное программное обеспечение. Их интеграция в ПЛК-ФБ ... 44
9.6 Процедуры эксплуатации и технического обслуживания аппаратных средств ... 45
9.7 Подтверждение соответствия безопасности аппаратных средств ... 46
9.8 Верификация аппаратных средств ... 47
10 Проектирование и разработка программного обеспечения ПЛК-ФБ ... 47
10.1 Общие положения ... 47
10.2 Требования ... 48
10.3 Классификация инструментальных средств ... 48
10.4 Планирование подтверждения соответствия программного обеспечения ... 49
11 Подтверждение соответствия безопасности ПЛК-ФБ ... 49
12 Типовые испытания ПЛК-ФБ ... 50
12.1 Общие положения ... 50
12.2 Требования к типовым испытаниям ... 50
12.3 Требования к климатическим испытаниям ... 52
12.4 Требования к механическим испытаниям ... 52
12.5 Требования к испытаниям на электромагнитную совместимость (ЭМС) ... 53
13 Верификация ПЛК-ФБ ... 56
13.1 План верификации ... 56
13.2 Требования к тестированию с введением неисправности ... 57
13.3 Проверенное изделие по сравнению с поставленным ... 58
14 Оценка функциональной безопасности ... 58
14.1 Цель ... 58
14.2 Требования к оценке ... 58
14.3 Информация об оценке ПЛК-ФБ ... 60
14.4 Независимость ... 61
15 Процедуры эксплуатации, технического обслуживания и модификации ПЛК-ФБ ... 62
15.1 Цель ... 62
15.2 Модификация ПЛК-ФБ ... 62
16 Информация, предоставляемая пользователю производителем ПЛК-ФБ ... 62

16.1 Общие положения 62
16.2 Информация о соответствии настоящему стандарту 62
16.3 Информация о типе и содержании документации 63
16.4 Информация каталогов и спецификаций 63
16.5 Руководство по безопасности 63
Приложение А (справочное) Вычисление безотказности 65
Приложение В (справочное) Типовые архитектуры ПЛК-ФБ 66
Приложение С (справочное) ПЛК-ФБ в системах, реализующих срабатывание защиты при подаче питания 72
Приложение D (справочное) Доступные базы данных интенсивностей отказов 73
Приложение Е (справочное) Методология оценки интенсивности отказов по общей причине в многоканальном ПЛК-ФБ 74
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам 76
Библиография 78

Введение

Общие положения

Комплекс МЭК 61131 имеет общее наименование «Программируемые контроллеры» и состоит из следующих частей:

Часть 1. Общее описание;

Часть 2. Требования и тесты оборудования;

Часть 3. Языки программирования;

Часть 4. Руководства пользователей;

Часть 5. Коммуникации;

Часть 6. Безопасность функциональная;

Часть 7. Программирование управления с нечеткой логикой;

Часть 8. Руководства для применения и реализации языков программирования.

Настоящий стандарт следует применять в сочетании с другими частями комплекса МЭК 61131.

Поскольку настоящий стандарт — это стандарт на изделие, являющееся программируемым логическим контроллером, удовлетворяющим требованиям функциональной безопасности (ПЛК-ФБ), то его положения должны применять к области программируемых контроллеров и связанных с ними периферийных устройств.

О соответствии с настоящим стандартом не может идти речи, если не выполнены требования раздела 4.

Общие термины определены в МЭК 61131-1. Более специальные термины определены в каждой из частей комплекса МЭК 61131.

В соответствии с 1.1 МЭК 61508-1 настоящий стандарт охватывает определенные в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-3 требования к изделиям из области программируемых контроллеров и связанных с ними периферийных устройств.

Принципиальная цель настоящего стандарта состоит в том, чтобы следовать структуре серии стандартов МЭК 61508. Но некоторые аспекты не связаны с МЭК 61508 непосредственно и, таким образом, должны рассматриваться несколько по-другому. Частично это связано с рассмотрением аппаратных средств, программного обеспечения, встроенного микропрограммного обеспечения и т.д. в одном документе.

Общая структура настоящего стандарта

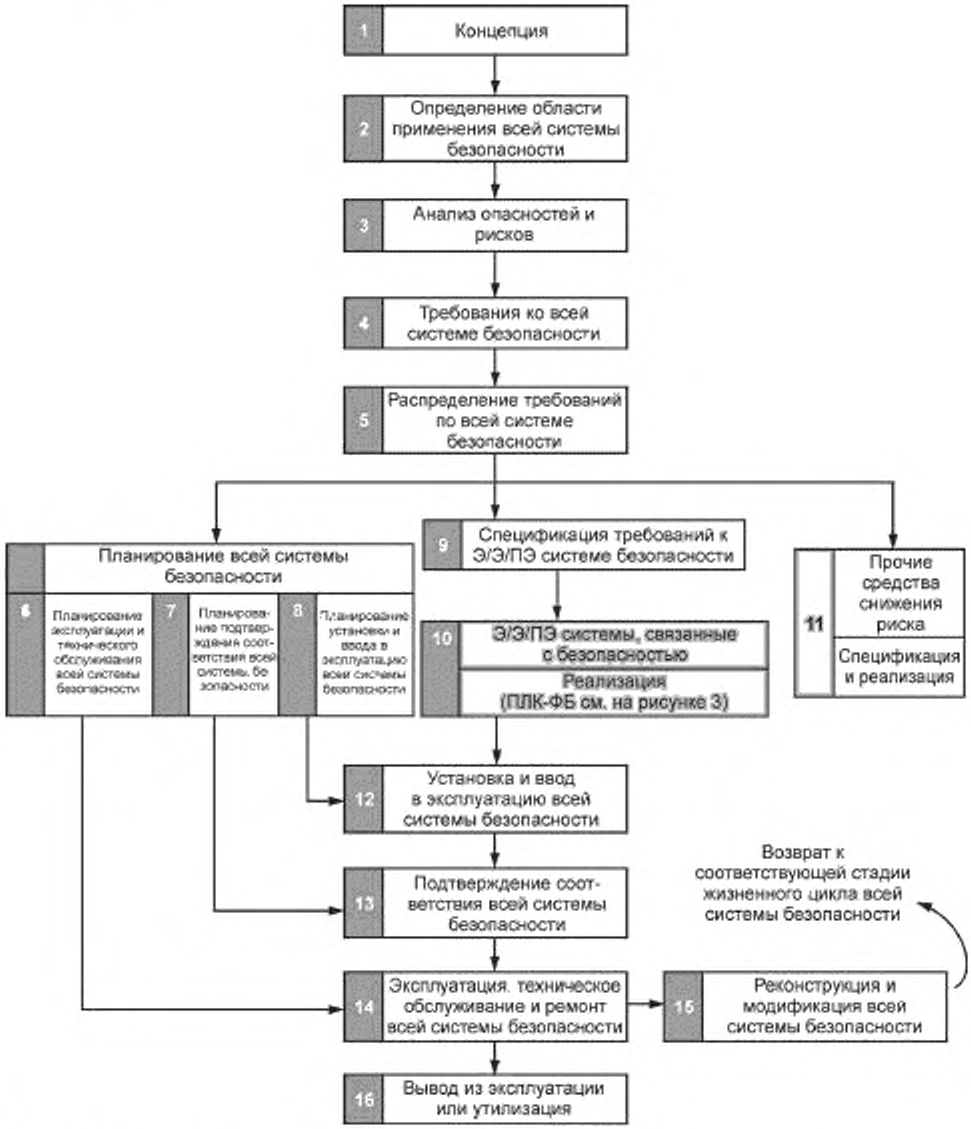
На рисунке 1 представлен рисунок 2 МЭК 61508-1:2010, который был скорректирован, чтобы показать, как ПЛК-ФБ реализуется в связанной с безопасностью Э/Э/ПЭ системе и встраивается в жизненный цикл всей системы безопасности. Хотя согласно МЭК 61508-1 блок 10 на рисунке 1 включает рассмотрение функциональной безопасности датчиков, логической подсистемы и исполнительных элементов (например, приводов), в настоящем стандарте в рамках данного блока рассматривается ПЛК-ФБ с учетом ссылки на рисунок 3.

По этой причине стадия реализации (блок 10 на рисунке 1) в настоящем стандарте рассматривается только для логической подсистемы.

Настоящий стандарт рассматривает управление ПЛК-ФБ на стадиях жизненного цикла системы безопасности, распределение требований к функциональной безопасности и планирование разработки ПЛК-ФБ, уделяя основное внимание стадии реализации (блок 10) жизненного цикла всей системы безопасности, представленного на рисунке 1. В настоящем стандарте предполагается, что ФБ-ПЛК используется в качестве логической подсистемы всей Э/Э/ПЭ системы безопасности.

Стадия реализации (блок 10 на рисунке 1) включает:

- определение характеристик безопасности ПЛК-ФБ для его аппаратных средств, программного обеспечения, или встроенного микропрограммного обеспечения, или любой их комбинации;
- реализацию архитектур аппаратных средств ПЛК-ФБ;
- действия по верификации и подтверждению соответствия на уровне ПЛК-ФБ;
- требования к модификации ПЛК-ФБ;
- информацию по эксплуатации и техническому обслуживанию для специалиста, использующего ПЛК-ФБ;
- информацию, предоставляемую производителем ПЛК-ФБ, для специалиста, использующего ПЛК-ФБ.



Примечания

1 Действия, относящиеся к верификации, управлению функциональной безопасностью и оценке функциональной безопасности, не показаны из соображений ясности рисунков, однако они относятся ко всем стадиям жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

2 Стадии, представленные на рисунке блоком 11, находятся вне области применения настоящего стандарта.

3 МЭК 61508-2 и МЭК 61508-3 относятся к блоку 10 (реализация), но они также относятся, при необходимости, к аспектам блоков 13, 14 и 15 программируемой электроники (аппаратным средствам и программному обеспечению).

4 В таблице 1 МЭК 61508-1 описаны цели и область распространения стадий, представленных каждым блоком.

5 Технические требования, необходимые для эксплуатации, технического обслуживания, ремонта, модификации, модернизации и вывода из эксплуатации или утилизации всей системы безопасности, будут заданы как часть информации, предоставляемой поставщиком Э/Э/ПЭ системы, связанной с безопасностью, и ее элементов и компонентов.

Рисунок 1 — ПЛК-ФБ в связанной с безопасностью Э/Э/ПЭ системе в структуре жизненного цикла всей системы безопасности

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

КОНТРОЛЛЕРЫ ПРОГРАММИРУЕМЫЕ

Часть 6
Безопасность функциональная

Programmable controllers. Part 6. Functional safety

Дата введения — 2016—05—01

1 Область применения

Настоящий стандарт определяет требования для программируемых (логических) контроллеров (ПЛК) и связанных с ними периферийных устройств, как определено в части 1, которые предназначены для использования в качестве логической подсистемы связанной с безопасностью электрической/электронной/программируемой электронной (Э/Э/ПЭ) системы. Программируемый контроллер и связанные с ним периферийные устройства, соответствующие требованиям настоящего стандарта, считают пригодным для применения в Э/Э/ПЭ системе, связанной с безопасностью, и называют программируемым логическим контроллером, удовлетворяющим требованиям функциональной безопасности (ПЛК-ФБ). ПЛК-ФБ — обычно подсистема аппаратных средств (АС) / программного обеспечения. ПЛК-ФБ может также включать элементы программного обеспечения, например предварительно созданные функциональные блоки.

Э/Э/ПЭ система, связанная с безопасностью, обычно состоит из датчиков, исполнительных механизмов, программного обеспечения и логической подсистемы. Настоящий стандарт является реализацией требований стандартов серии МЭК 61508 для конкретного изделия и соответствие настоящему стандарту означает выполнение всех применимых для ПЛК-ФБ требований стандартов МЭК 61508. В то время как МЭК 61508 — это общесистемный стандарт, настоящий стандарт содержит конкретные требования, обеспечивающие применение к ПЛК-ФБ принципов стандартов серии МЭК 61508.

Настоящий стандарт рассматривает только требования функциональной безопасности и полноты безопасности ПЛК-ФБ, если он является частью Э/Э/ПЭ систем, связанных с безопасностью. Определение требований функциональной безопасности ко всей Э/Э/ПЭ системе, связанной с безопасностью, и требований функциональной безопасности к конечному приложению Э/Э/ПЭ системы, связанной с безопасностью, выходит за рамки настоящего стандарта, но для него эти требования являются входной информацией. Информацию для конкретного применения можно получить из стандартов, таких как МЭК 61511, МЭК 62061 и ИСО 13849.

Настоящий стандарт не охватывает общие требования безопасности для ПЛК-ФБ, такие как требования, связанные с поражением электрическим током и пожарооласностью, определенные в МЭК 61131-2.

Настоящий стандарт распространяется на ПЛК-ФБ со значением уровня полноты безопасности (УПБ) не больше, чем 3.

Цель настоящего стандарта:

- установить и описать элементы жизненного цикла ПЛК-ФБ в соответствии с общим жизненным циклом системы безопасности, определенным в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-3;

- для аппаратных средств и программного обеспечения ПЛК-ФБ установить и описать требования, связанные с функциональной безопасностью и полнотой безопасности Э/Э/ПЭ системы, связанной с безопасностью;

- установить методы оценки для следующих параметров/критериев ПЛК-ФБ:

Издание официальное

- заявленное значение уровня полноты безопасности (УПБ), которое может быть достигнуто для ПЛК-ФБ;
- значение вероятности отказа по запросу (PFD);
- значение средней частоты опасных отказов в час (PFH);
- значение доли безопасных отказов (SFF);
- значение отказоустойчивости аппаратных средств (HFT);
- значение охвата диагностикой (DC);
- проверка того, что заданные для ПЛК-ФБ процессы жизненного цикла производителем были осуществлены;
- определенное безопасное состояние;
- меры и методы предотвращения и управления систематическими отказами;
- функциональное поведение в состоянии отказа для каждого вида отказа, рассматриваемого в настоящем стандарте;
- установить определения и идентифицировать основные характеристики, относящиеся к выбору и применению ПЛК-ФБ и связанных с ними периферийных устройств.

Настоящий стандарт, прежде всего, предназначен для производителей ПЛК-ФБ. Он также включает очень важную роль пользователей ПЛК-ФБ с помощью требований в документации для пользователей. Некоторые руководящие указания пользователю ПЛК-ФБ можно найти в МЭК 61131-4.

В настоящий стандарт включены требования Руководства ИСО/МЭК 51 и Руководства МЭК 104, поскольку они имеют отношение к настоящему стандарту.

2 Нормативные ссылки

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

МЭК 60947-5-1:2003 Аппаратура распределения и управления низковольтная. Часть 5. Аппараты и коммутационные элементы цепей управления. Глава 1. Электромеханические аппараты для цепей управления (IEC 60947-5-1:2003, Low-voltage switchgear and control gear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices)

МЭК/ТС 61000-1-2 Электромагнитная совместимость (ЭМС) — Часть 1-2. Основы. Методология обеспечения функциональной безопасности электрического и электронного оборудования в отношении электромагнитных помех (IEC/TS 61000-1-2, Electromagnetic compatibility (EMC) — Part 1-2: General — Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena)

МЭК 61000-4-2:2008 Электромагнитная совместимость (ЭМС). Часть 4-2. Методы испытаний и измерений. Испытания на устойчивость к электростатическим разрядам (IEC 61000-4-2:2008, Electromagnetic compatibility (EMC) — Part 4-2: Testing and measurement techniques — Electrostatic discharge immunity test)

МЭК 61000-4-3:2006 Электромагнитная совместимость (ЭМС). Часть 4-3. Методы тестирования и измерения. Испытания на устойчивость к излученному радиочастотному электромагнитному полю (IEC 61000-4-3:2006, Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test)

МЭК 61000-4-4:2012 Электромагнитная совместимость (ЭМС). Часть 4-4. Методы испытаний и измерений. Испытания на устойчивость к наносекундным импульсным помехам (IEC 61000-4-4:2012, Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques — Electrical fast transient/burst immunity test)

МЭК 61000-4-5:2005 Электромагнитная совместимость. Часть 4-5. Методики испытаний и измерений. Испытание на невосприимчивость к выбросу напряжения (IEC 61000-4-5:2005, Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques — Surge immunity test)

МЭК 61000-4-6:2008 Электромагнитная совместимость (ЭМС). Часть 4-6. Методы тестирования и измерения. Устойчивость от помех, наведенных радиочастотными электромагнитными полями (IEC 61000-4-6:2008, Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields)

МЭК 61000-4-8:2009 Электромагнитная совместимость. Часть 4-8. Методы тестирования и измерения. Испытание на устойчивость к магнитному полю (IEC 61000-4-8:2009, Electromagnetic compatibility (EMC) — Part 4-8: Testing and measurement techniques — Power frequency magnetic field immunity test)

МЭК 61131-1:2003 Контроллеры программируемые. Часть 1. Общие сведения (IEC 61131-1:2003, Programmable controllers — Part 1: General information)

МЭК 61131-2:2007 Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания (IEC 61131-2:2007, Programmable controllers — Part 2: Equipment requirements and tests)

МЭК 61131-4:2004 Контроллеры программируемые. Часть 4. Руководство для пользователя (IEC 61131-4:2004, Programmable controllers — Part 4: User guidelines)

МЭК 61326-3-1:2008 Оборудование электрическое для измерения, управления и лабораторного использования. Требования к электромагнитной совместимости. Часть 3-1.Требования помехоустойчивости к системам, связанным с обеспечением безопасности, и оборудованию для выполнения функций, связанных с обеспечением безопасности (функциональная безопасность). Общее применение в промышленности (IEC 61326-3-1:2008 Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — General industrial applications)

МЭК 61326-3-2:2008 Оборудование электрическое для измерения, управления и лабораторного использования. Требования к электромагнитной совместимости. Часть 3-2. Требования помехоустойчивости к системам, связанным с обеспечением безопасности, и оборудованию для выполнения функций, связанных с обеспечением безопасности (функциональная безопасность). Применение в промышленности с особой электромагнитной средой (IEC 61326-3-2:2008 Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — Industrial applications with specified electromagnetic environment)

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

МЭК 61508-2:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/программируемым электронным, связанным с безопасностью (IEC 61508-4:2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 2. Requirements for electrical / electronic / programmable electronic safety-related systems)

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

МЭК 61508-6:2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3 (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)

МЭК 61784-3 Сети связи промышленные. Профили. Часть 3. Полевые шины для обеспечения функциональной безопасности. Общие правила и определения профилей (IEC 61784-3, Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions)

МЭК 62443 (все части) Сети связи промышленные. Безопасность сетей и систем (IEC 62443 (all parts), Industrial communication networks — Network and system security)

МЭК Руководство 104:1997 Подготовка стандартов по безопасности и использование базовых стандартов по безопасности и стандартов по безопасности групп (IEC Guide 104:1997, The preparation of safety publications and the use of basic safety publications and group safety publications)

ИСО/МЭК Руководство 51:1990 Аспекты безопасности. Руководящие указания по включению в стандарты (ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards)

ЕН 50205:2002 Реле с принудительными контактами (механически связанные) (EN 50205:2002, Relays with forcibly guided (mechanically linked) contacts)

3 Термины и определения

3.1 **прикладное программное обеспечение** (application software, application data, configuration data): Часть программного обеспечения РЕ системы, которая по специфицированным функциям выполняет задачу, связанную с безопасностью УО, но не обеспечивает функционирование и не предоставляет сервисы для самого программируемого устройства.

[МЭК 61508-4:2010, 3.2.7]

3.2 **специализированная заказная интегральная схема**; СИС (application specific integrated circuit, ASIC): Интегральная схема, разработанная и изготовленная для выполнения конкретной функции, которую определяет разработчик изделия.

[МЭК 61508-4:2010, 3.2.15]

3.3 **архитектура** (architecture): Конкретная конфигурация элементов аппаратных средств и системы.

[МЭК 61508-4:2010, 3.3.4]

3.4 **готовность** (availability): Вероятность того, что элемент в состоянии выполнить свою предназначенную функцию, выраженная как десятичное значение от нуля до единицы.

Пример — A = 0,9 означает, что изделие готово выполнить предназначенную для нее функцию в течение 90 % времени его работы.

Примечание — При $\lambda T << 1$, $A = 1 - \lambda T$. См. 3.23.

3.5 **средняя частота опасного отказа в час** (average frequency of a dangerous failure per hour, PFH): Средняя частота опасного отказа Э/Э/ПЭ системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.

Примечания

1 Термин «вероятность опасного отказа в час» в настоящем стандарте не используют, но сокращение PFH сохранено, и если оно используется, то это означает «средняя частота опасного отказа [ч]».

2 Теоретически PFH — среднее значение безусловной интенсивности отказа, также называемой частотой отказов, которое обычно обозначают $w(t)$. Ее не следует путать с интенсивностью отказов (см. приложение В МЭК 61508-6).

3 Если Э/Э/ПЭ система, связанная с безопасностью, является последним слоем безопасности, то PFH вычисляют исходя из ее неотказоустойчивости $F(T) = 1 - R(t)$ (см. выше «интенсивность отказов»). Если Э/Э/ПЭ система, связанная с безопасностью, не является последним слоем безопасности, то ее PFH вычисляют исходя из ее неготовности $U(t)$ (см. PFD, 3.38). Приближения PFH задаются в первом случае как $F(T)/T$ и 1/MTTF и во втором — как 1/MTBF.

4 Если Э/Э/ПЭ система, связанная с безопасностью, подразумевает только быстро восстанавливаемые выявляемые отказы, то асимптотическая интенсивность отказов λ_{as} достигается быстро, что обеспечивает оценку PFH.

[МЭК 61508-4:2010, 3.6.19]

3.6 **черный канал** (black channel): Части канала связи, которые не разработаны или для которых не проведена процедура подтверждения соответствия согласно стандартам серии МЭК 61508.

Примечание — См. 7.4.11.2 МЭК 61508-2.

3.7 **канал** (channel): Элемент или группа элементов, которые независимо реализуют элемент функции безопасности.

Пример — Двухканальная (или дуальная) конфигурация — конфигурация, в которой два канала независимо выполняют одну и ту же функцию.

Примечание — Данный термин можно применять для описания полных систем или частей системы (например, датчиков или исполнительных элементов).

[МЭК 61508-4:2010, 3.3.6]

3.8 **отказ по общей причине** (common cause failure): Отказ, являющийся результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, приводящих к отказу системы.

[МЭК 61508-4:2010, 3.6.10]

3.9 **информационная безопасность** (cyber security): Защита данных в компьютерных и информационных системах от потери или повреждения из-за умышленных или неумышленных действий людьми, не обладающими полномочиями, или злоумышленниками.

Примечание — Данный термин касается защиты от таких действий, реализуемых через сеть или другие коммуникационные интерфейсы.

3.10 **опасный отказ** (dangerous failure): Отказ элемента и/или подсистемы, и/или системы, влияющий на выполнение функции безопасности:

a) препятствует выполнению функции безопасности, если необходимо ее выполнение (в режиме запроса), или вызывает прекращение выполнения функции безопасности (в непрерывном режиме), переводя УО в опасное или потенциально опасное состояние;

b) снижает вероятность корректного выполнения функции безопасности, если необходимо ее выполнение.

[МЭК 61508-4:2010, 3.6.7]

3.11 **опасный сбой** (dangerous fault): Сбой, который может привести к опасному отказу.

Примечание — Если опасный сбой обнаружен, то предпринимают меры по предотвращению опасного отказа.

3.12 **заданное безопасное состояние** (defined safe state): Состояние ПЛК-ФБ, определенное производителем ПЛК-ФБ, в которое переходит ПЛК-ФБ, когда происходит опасный отказ.

Примечание — Как правило, заданное безопасное состояние — состояние по умолчанию всех без исключения выходов ПЛК-ФБ. Для цифровых выходов — это состояние с отключенным питанием, если конкретно не определено иначе. Для аналоговых выходов — это состояние с нулевыми значениями напряжения или нулевыми коэффициентами усиления, если конкретно не определено иначе. Для коммуникационных портов — это состояние определено как отсутствие связи, если, в частности, не определено иначе.

3.13 **обнаруженный отказ** (detected failure): Прекращение способности функционального блока выполнить требуемую функцию, обнаруженное диагностическими проверками, контрольными испытаниями, вмешательством оператора или в процессе нормального функционирования.

Пример — Физический осмотр и проверки, выполняемые вручную.

3.14 **охват диагностикой;** ОД (diagnostic coverage, DC): Часть опасных отказов, выявляемая автоматическими диагностическими тестами в неавтономном режиме. Эту часть опасных отказов вычисляют как отношение интенсивности выявленных диагностическими тестами опасных отказов к общей интенсивности опасных отказов.

Примечания

1 Охват диагностикой опасных отказов определяют с помощью следующего выражения

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{total}},$$

где DC — охват диагностикой;

λ_{DD} — интенсивности выявленных опасных отказов;

λ_{total} — общая интенсивность опасных отказов.

2 Данное определение справедливо при условии, что рассматриваемые компоненты имеют постоянную интенсивность отказов.

[МЭК 61508-4:2010, 3.8.6]

3.15 **Э/Э/ПЭ** (E/E/PE): Электрический / электронный / программируемый электронный.

3.16 **элемент** (element): Часть подсистемы, включающая в себя отдельный компонент или любую группу компонентов, которая выполняет одну или более функций безопасности элемента.

[МЭК 61508-4:2010, 3.8.6, модифицировано]

Примечание — Элемент может включать в себя аппаратные средства и/или программное обеспечение.

[МЭК 61508-4:2010, 3.4.5, модифицировано]

3.17 **функция безопасности элемента** (element safety function): Часть функции безопасности, которая реализуется элементом.

[МЭК 61508-4:2010, 3.5.3, модифицировано]

3.18 **встроенное программное обеспечение, встроенное микропрограммное обеспечение** (embedded software, embedded firmware): Программное обеспечение, управляющее работой ПЛК-ФБ или одной из его подсистем.

Примечания

1 Встроенное программное обеспечение поставляется производителем ПЛК-ФБ установленное в ПЛК-ФБ. У пользователя нет прямого доступа к встроенному программному обеспечению. Производитель ПЛК-ФБ разрабатывает

или пишет встроенное программное обеспечение, чтобы управлять его ПЛК-ФБ. Оно может, например, управлять коммуникационной подсистемой или интерпретацией программы, разработанной пользователем в инструментальных средствах инженерии.

2 Еще один термин для встроенного программного обеспечения.

3 Встроенное микропрограммное обеспечение может быть связанным безопасностью или не связанным с безопасностью.

3.19 **средства проектирования** (engineering tools): Программное обеспечение для разработки прикладной программы.

Пример — Программное обеспечение средств проектирования поставляется производителем ПЛК-ФБ для установки на персональной рабочей станции. В этом программном пакете пользователь разрабатывает или пишет свою прикладную программу для управления процессом. Затем эта прикладная программа загружается в ПЛК-ФБ и осуществляет управление ПЛК-ФБ пользователя, присоединенным оборудованием и, таким образом, процессом.

Примечание — Прикладные программы и программное обеспечение могут быть связанными с безопасностью или не связанными с безопасностью.

3.20 **управляемое оборудование**; УО (equipment under control, EUC): Оборудование, машины, аппараты или установки, используемые для производства, обработки, транспортирования, в медицине или в других областях.

Примечание — Система управления УО представляют собой отдельное отличное от УО понятие.

3.21 **испытуемое техническое средство** (equipment under test, EUT): Определенная(ые) производителем представительная(ые) конфигурация(и), используемая(ые) для типовых испытаний.

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

Примечания

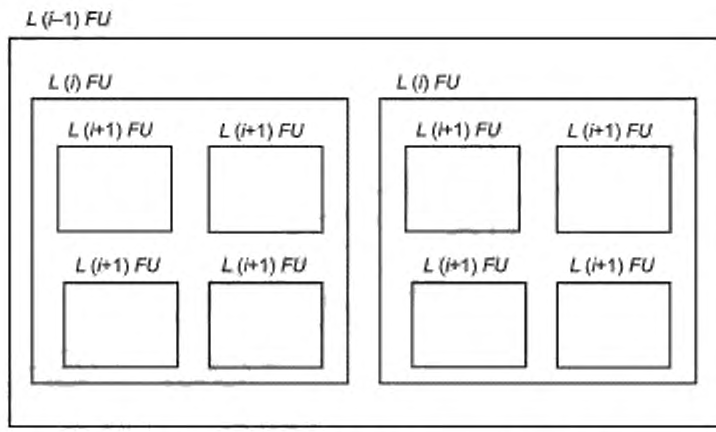
1 Данное определение основано на определении 91-04-01 в МЭК 60050-191 и учитывает изменения, связанные с систематическими отказами, например, вследствие недоработок в спецификации или программном обеспечении.

2 Соотношение между сбоями и отказами см. на рисунке 2.

3 Характеристики требуемых функций неизбежно исключают определенные режимы работы, и некоторые функции могут быть определены путем описания режимов, которых следует избегать. Возникновение таких режимов представляет собой отказ.

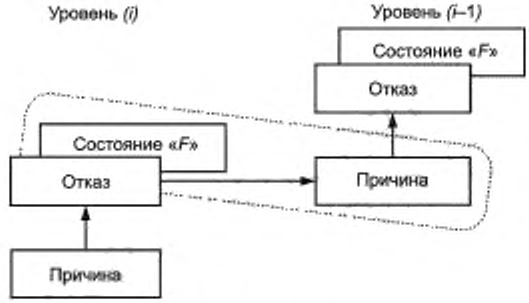
4 Отказы являются либо случайными (в аппаратных средствах), либо систематическими (в аппаратных средствах или в программном обеспечении), см. 3.42 и 3.56.

[МЭК 61508-4:2010, 3.6.4]

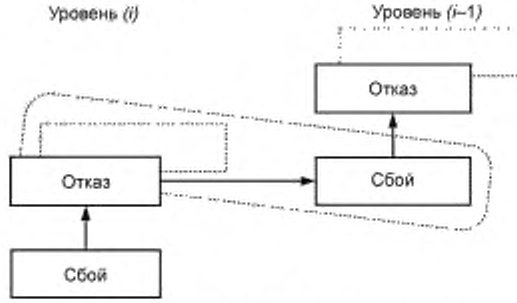


(*L* — уровень: *i* = 1,2,3 и т.д.; *FU* — функциональный блок)

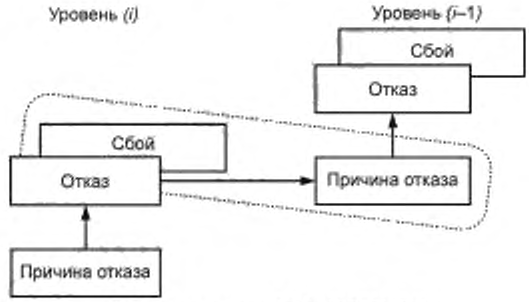
а) Конфигурация функционального блока



b) Обобщенный вид



c) С точки зрения МЭК 61508 и ИСО/МЭК 2382-14.



d) С точки зрения МЭК 60050(191)

Примечания к рисунку 2

1 Как показано на рисунке a), функциональный блок может быть представлен в виде многоуровневой иерархической структуры, каждый из уровней которой может быть в свою очередь назван «функциональный блок». На уровне (*i*) «причина» может проявить себя как ошибка (отклонение от правильного значения или состояния) в пределах функционального блока, соответствующего данному уровню (*i*). Если ошибка не будет исправлена или нейтрализована, то она может привести к отказу данного функционального блока, который в результате перейдет в состояние «F», в котором он более не сможет выполнять необходимую функцию [см. рисунок b)]. Данное состояние «F» уровня (*i*) может в свою очередь проявиться в виде ошибки на уровне функционального блока (*i*–1), которая, если она не будет исправлена или нейтрализована, может привести к отказу функционального блока уровня (*i*–1).

2 В этой причинно-следственной цепочке один и тот же элемент («объект X») может рассматриваться как состояние (состояние «F») функционального блока уровня (*i*), в которое он попадает в результате отказа, а также как причина отказа функционального блока уровня (*i*–1). Данный «объект X» объединяет концепцию «отказа» в МЭК 61508 и ИСО/МЭК 2382-14, в которой внимание акцентируется на причинном аспекте, как показано на рисунке c), и концепцию «отказа», представленную в МЭК 60050(191), в которой основное внимание уделено аспекту состояния, как показано на рисунке d). В МЭК 60050(191) состояние «F» называется «отказом», а в МЭК 61508 и ИСО/МЭК 2382-14 оно не определено.

3 В некоторых случаях отказ или ошибка могут быть вызваны внешним событием, таким, например, как молния или электростатические помехи, а не внутренним отказом. Более того, ошибка (в обоих словарях) может возникать без предшествующего отказа. Примером такой ошибки может быть ошибка проектирования.

Рисунок 2 — Модель отказа

3.23 **интенсивность отказов** (failure rate): Интенсивность отказов $\lambda(t)$ объекта (отдельных компонентов или систем) определяется как вероятность отказа $\lambda(t)dt$ этого объекта на отрезке времени $[t, t+dt]$ при условии, что объект был работоспособен на временном отрезке $[0, t]$.

Примечания

1 Математически $\lambda(t)$ — условная вероятность отказа в единицу времени на временно́м отрезке $[t, t+dt]$. Она тесно связана с функцией безотказности (т. е. вероятности отсутствия отказа от 0 до t), описываемой общей формулой: $R(t) = \exp\left(-\int_0^t \lambda(\tau)d\tau\right)$. Выражение для $\lambda(t)$ через функцию безотказности имеет вид $\lambda(t) = -\frac{dr(t)}{dt}\frac{1}{r(t)}$.

2 Интенсивности отказов и их неопределенности могут быть оценены из стандартных статистических данных об отказах реальных объектов. В течение «срока годности» (т. е. после «выгорания» дефектов и до износа) интенсивность отказов простого элемента можно считать постоянной величиной $\lambda(t) \equiv \lambda$.

3 Среднее значение $\lambda(t)$ в течение заданного отрезка времени $[0, T]$, вычисленное по формуле $\lambda_{avg}(T) = \left(\int_0^T \lambda(\tau)d\tau\right) \Big/ T$, не является интенсивностью отказов, поэтому не может быть использовано для вычисления функции $R(t)$ по формуле в примечании 1. Однако оно может быть интерпретировано как средняя частота отказа за этот отрезок времени (т. е. PFH, см. МЭК 61508-6, приложение В).

4 Интенсивность отказов последовательности элементов — сумма интенсивностей отказов каждого из этих элементов.

5 Интенсивность отказов избыточных систем обычно не является постоянной. Однако если все отказы достаточно быстро выявлены, являются независимыми и быстро исправлены, то $\lambda(t)$ быстро сходится к асимптотическому значению λ_{ss}, которая является эквивалентной интенсивностью отказов систем. Ее не следует путать со средней интенсивностью отказов в соответствии с примечанием 3, которая не обязательно сходится к асимптотическому значению.

[МЭК 61508-4:2010, 3.6.16]

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

[ИСО/МЭК 2382-14:1997, 14.01.10]

Примечание — МЭК 60050-191, 191-05-01 определяет «сбой» как состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая неспособность, возникающую во время профилактических работ или других плановых мероприятий, либо в результате недостатка внешних ресурсов. Иллюстрация к этим двум точкам зрения показана на рисунке 2.

[МЭК 61508-4:2010, 3.6.1]

3.25 **устойчивость к сбоям** (fault tolerance): Способность функционального блока продолжать выполнять необходимую функцию при наличии сбоев или ошибок.

[ИСО/МЭК 2382-14:1997, 14.01.06]

Примечание — Определение МЭК 60050-191, 191-05-05 относится только к сбоям подэлементов. См. примечание к термину «сбой» в 3.24.

[МЭК 61508-4:2010, 3.6.3]

Примечание — В рассматриваемые отказы и ошибки включают те, которые происходят в интерфейсах к ПЛК-ФБ.

3.26 **спецификация требований к функциональной безопасности ПЛК-ФБ** (ПЛК-ФБ functional safety requirements specification): Спецификация, содержащая требования к функциям безопасности и связанным с ними уровням полноты безопасности для ПЛК-ФБ.

3.27 **функциональная безопасность** (functional safety): Часть общей безопасности, обусловленная применением УО и системы управления УО и зависящая от правильности функционирования Э/Э/ПЭ систем, связанных с безопасностью, и других средств по снижению риска.

[МЭК 61508-4:2010, 3.1.12]

Примечание — Функциональная безопасность по существу — способность связанной с безопасностью системы достигать или поддерживать безопасное состояние.

3.28 **технические средства** (hardware, HW): Электрические ПЛК-ФБ, механические или другие физические устройства, которые соединены вместе для выполнения функций.

3.29 **связанная с безопасностью подсистема высокой сложности** (high complexity safety-related subsystem): Такая часть связанной с безопасностью Э/Э/ПЭ системы, для которой:

- или вид отказа, по крайней мере одного компонента, не четко определен; или
- поведение подсистемы в случае неисправности не может быть полностью определено; или
- недостаточно эксплуатационных данных об отказах, чтобы показать, что достигаются требуемые интенсивности отказов.

Пример — ПЛК-ФБ. Получено из определения подсистемы типа B, описанного в МЭК 61508-2, 7.4.4.1.3.

Примечание — Относится к системам типа A (9.4.3.2.2) и типа B (9.4.3.2.3).

3.30 **логическая подсистема** (logic subsystem): Логическая подсистема — это часть связанной с безопасностью Э/Э/ПЭ системы, которая выполняет функциональную логику, но не включает датчики и исполнительные элементы.

Пример — ПЛК-ФБ — логическая подсистема.

3.31 **средняя продолжительность ремонта** (mean repair time, MRT): Ожидаемая полная продолжительность ремонта.

Примечание — MRT охватывает времена b), c) и d) MTTR (см. 3.34).

[МЭК 61508-4:2010, 3.6.22]

3.32 **среднее время между отказами** (mean time between failures, MTBF): Статистический параметр (обычно выражаемый в часах), который позволяет сравнивать надежность различных изделий.

Примечания

1 Математически — это обратная величина интенсивности отказов восстанавливаемого изделия.

2 MTBF — среднее арифметическое значение, определенное для большого количества устройств за длительный период времени.

3 Для сложного изделия, такого как ПЛК, средняя интенсивность отказов аппроксимируется постоянным значением интенсивности отказов экспоненциальной функции надежности: $R(t) = e^{-\lambda t}$.

4 MTBF = MTTF + MTTR.

См. 3.33, примечание 2.

3.33 **среднее время до отказа** (mean time to failure, MTTF): Статистический параметр (обычно выражаемый в часах), который позволяет сравнивать надежность невосстанавливаемых изделий.

Примечания

1 Для невосстанавливаемого изделия с постоянной интенсивностью отказов MTTF — обратная величина интенсивности отказов изделия.

2 MTTF — среднее арифметическое значение, определенное для большого количества устройств за длительный период времени.

3 Несмотря на то, что два термина MTBF и MTTF иногда используют взаимозаменяемо, они, строго говоря, относятся к восстанавливаемым и невосстанавливаемым изделиям соответственно. MTBF следует использовать только для тех изделий, которые обычно восстанавливают и возвращают в работу.

3.34 **среднее время восстановления** (mean time to restoration, MTTR): Ожидаемое время восстановления.

Примечание — MTTR включает в себя:

a) время выявления отказа;

b) время, прошедшее до начала восстановления;

c) время, фактически затраченное на ремонт;

d) время возвращения компонента в работу.

Начало времени перечисления b) совпадает с окончанием времени перечисления a); начало времени перечисления c) совпадает с окончанием времени перечисления b); начало времени перечисления d) совпадает с окончанием времени перечисления c).

[МЭК 61508-4:2010, 3.6.21]

3.35 **режим работы** (mode of operation): Способ выполнения функции безопасности, который может быть в режиме с низкой частотой запросов, с высокой частотой запросов либо в непрерывном режиме.

Примечание — Э/Э/ПЭ система, связанная с безопасностью, выполняющая функцию безопасности, не влияет на работу УО или систему управления УО до тех пор, пока к ней не возникает запрос. Однако если Э/Э/ПЭ

система, связанная с безопасностью, отказывает так, что выполнение функции безопасности невозможно, то она может вызвать переход УО в безопасное состояние (см. МЭК 61508-2, 7.4.6).

[МЭК 61508-4:2010, 3.5.16]

3.35.1 **режим работы с низкой частотой запросов** (low demand mode): Режим, в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов не превышает одного запроса в год.

[МЭК 61508-4:2010, 3.5.16]

3.35.2 **режим работы с высокой частотой запросов** (high demand mode): Режим, в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов превышает один в год.

[МЭК 61508-4:2010, 3.5.16]

3.35.3 **непрерывный режим работы** (continuous mode): Режим, в котором функция безопасности поддерживает УО в безопасном состоянии, как и при нормальном функционировании.

[МЭК 61508-4:2010, 3.5.14]

3.36 **M из N, MooN** (M out of N, MooN): Архитектура, состоящая из *N* независимых каналов, которые соединены так, что, по крайней мере, требуется *M* каналов для выполнения функции безопасности.

3.37 **время безопасности процесса, худший случай** (process safety time, worst case): Промежуток времени между моментом появления отказа, который может вызвать опасное событие в УО или системе управления УО, и моментом времени, к которому в УО должно быть завершено действие по предотвращению появления опасного события.

[МЭК 61508-4:2010, 3.6.20]

3.38 **вероятность опасного отказа по запросу** (probability of dangerous failure on demand, PFD): Неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность (см. МЭК 60050-191), т. е. выполнить заданную функцию безопасности, когда происходит запрос от УО или системы управления УО.

Примечания

1 [Мгновенная] неготовность (согласно МЭК 60050-191) является вероятностью ненахождения элемента в состоянии выполнения необходимой функции при данных условиях в данный момент времени, предполагая, что элемент обеспечен всеми необходимыми внешними ресурсами. Обычно ее обозначают как $U(t)$.

2 [Мгновенная] готовность не зависит от состояний (выполнения или отказа), в которых находился элемент до момента времени t. Она только характеризует элемент, который должен быть в работоспособном состоянии, когда он обязан в нем быть, например Э/Э/ПЭ система, связанная с безопасностью, работающая в режиме с низкой интенсивностью запросов.

3 Если происходит периодическое тестирование, то PFD Э/Э/ПЭ системы, связанной с безопасностью, для заданной функции безопасности представляется в виде зубчатой кривой с большим диапазоном значений вероятностей от низкого, сразу после теста, до максимума, непосредственно перед тестом.

[МЭК 61508-4:2010, 3.6.17]

3.39 **программируемые технические средства** (programmable HW): Технические средства, функциональность или производительность которых могут быть изменены или модифицированы встроенным программным обеспечением.

Пример — Программируемая логическая интегральная схема, устройства флэш-памяти и изделия на базе микропроцессоров.

3.40 **контрольная проверка** (proof test): Периодическая проверка, проводимая для того, чтобы обнаружить опасные скрытые отказы в системе, связанной с безопасностью, с тем чтобы при необходимости система могла быть восстановлена настолько близко к «исходному» состоянию, насколько это возможно в данных условиях.

Примечания

1 В настоящем стандарте использован термин «контрольная проверка», но считается, что он является синонимом термина «периодическая проверка».

2 Эффективность контрольной проверки будет зависеть также от охвата отказов тестами и эффективности восстановления. На практике обнаружить все 100 % скрытых опасных отказов не просто и возможно только для Э/Э/ПЭ системы, связанной с безопасностью, имеющей низкую сложность. Однако к этому необходимо стремиться. По крайней мере все выполняемые функции безопасности должны проверять в соответствии со спецификацией требований к безопасности Э/Э/ПЭ системы. При использовании отдельных каналов эти проверки проводят для каждого канала отдельно. Для сложных элементов, возможно, должен быть проведен анализ, с тем чтобы продемонстрировать, что вероятность скрытого опасного отказа, не обнаруженного контрольными проверками, является незначительной в течение всего срока службы Э/Э/ПЭ системы, связанной с безопасностью.

3 Для проведения контрольной проверки требуется некоторое время. В течение этого времени доступ к Э/Э/ПЭ системе, связанной с безопасностью, может быть частично или полностью запрещен. Продолжительностью контрольной проверки можно пренебречь, только если часть проверяемой Э/Э/ПЭ системы, связанной с безопасностью, останется доступной для запроса на выполнение или если УО будет отключено во время проверки.

4 Во время проведения контрольной проверки Э/Э/ПЭ система, связанная с безопасностью, может быть частично или полностью недоступна для выполнения запроса. В этом случае при вычислении УПБ величиной MTTR можно пренебречь, только если во время ремонта УО был отключен или были использованы другие эквивалентные по эффективности меры по снижению риска.

[МЭК 61508-4:2010, 3.8.5]

3.41 **надлежащая процедура функциональной проверки** (proper function verification procedure, PFVP): Методология тестирования ПЛК-ФБ.

3.42 **случайный отказ аппаратных средств** (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик в аппаратных средствах.

Примечания

1 Существует много механизмов ухудшения характеристик, действующих с различной интенсивностью и в различных компонентах. Поскольку допуски изготовления приводят к тому, что компоненты в результате действия этих механизмов отказывают в разное время и отказы аппаратных средств включают в себя много факторов, то отказы происходят с предсказуемой частотой, но в непредсказуемые (т. е. случайные) моменты времени.

2 Основное различие между случайными отказами аппаратных средств и систематическими отказами (см. 3.6.6) состоит в том, что интенсивность отказов системы (или другие подобные характеристики таких отказов), связанная со случайными отказами аппаратных средств, может прогнозироваться с достаточной степенью точности, но систематические отказы по своей природе не могут быть предсказаны точно. Поэтому интенсивность отказов системы, связанных со случайными отказами аппаратных средств, может быть охарактеризована количественно с достаточной степенью точности, тогда как отказы системы, связанные с систематическими отказами, не могут быть статистически охарактеризованы с достаточной точностью, поскольку события, приводящие к таким отказам, не могут быть предсказаны.

[МЭК 61508-4:2010, 3.6.5]

3.43 **надежность** (reliability, *R*): Вероятность того, что конкретное изделие будет работать в течение конкретного времени *t* без отказа.

Примечания

1 Для сложного изделия, такого как программируемый контроллер, средняя интенсивность отказов аппроксимируется экспоненциальной функцией надежности с постоянным значением интенсивности отказов: $R(t) = e^{-\lambda t} = e^{-(t/\text{MTBF})}$.

2 Если время *t* в последнем уравнении равно значению MTBF, то уравнение дает значение надежности, равное 0,368, подразумевая, что только 36,8 % конкретного изделия будет работать без отказа в течение его значения MTBF.

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

[ИСО/МЭК Руководство 51:1999, определение 3.2].

Примечание — Дальнейшее обсуждение этого определения содержится в МЭК 61508-5, приложение А.

[МЭК 61508-4:2010, 3.1.6]

3.45 **безопасный отказ ПЛК-ФБ** (safe failure): Отказ элемента и/или подсистемы, и/или системы, играющий определенную роль в реализации функции безопасности, который:

a) приводит к ложному выполнению функции безопасности, переводящей УО (или его часть) в безопасное состояние или поддерживающей безопасное состояние, или

b) увеличивает вероятность ложного выполнения функции безопасности, переводящей УО (или его часть) в безопасное состояние или поддерживающей безопасное состояние.

[МЭК 61508-4:2010, 3.6.8]

3.46 **безопасный сбой** (safe fault): Сбой, не вызывающий опасный отказ.

3.47 **доля безопасных отказов**; ДБО (safe failure fraction, SFF): Свойство элемента, связанного с безопасностью, определяемое отношением суммы средних частот безопасных отказов и опасных обнаруженных отказов к сумме средних частот безопасных и опасных отказов.

Примечание — Данное отношение имеет вид:

$$\text{ДБО} = \left(\sum \lambda_{S_{avg}} + \sum \lambda_{Dd_{avg}}\right) \Big/ \left(\sum \lambda_{S_{avg}} + \sum \lambda_{Dd_{avg}} + \sum \lambda_{Du_{avg}}\right).$$

Если частоты отказов являются постоянными величинами, то выражение упрощается и имеет вид:

$$ДБО = \left(\sum \lambda_S + \sum \lambda_{Dd}\right) / \left(\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}\right).$$

[МЭК 61508-4:2010, 3.6.15]

3.48 **безопасное состояние** (safe state): Состояние УО, в котором достигается безопасность.

Примечание — При переходе от потенциально опасного состояния к конечному, безопасному, состоянию УО может пройти через несколько промежуточных безопасных состояний. Для некоторых ситуаций безопасное состояние существует только до тех пор, пока УО остается под непрерывным контролем. Такое непрерывное управление может продолжаться в течение короткого или неопределенного периода времени.

[МЭК 61508-4:2010, 3.1.13]

3.49 **время реакции функции безопасности** (safety function response time): Наихудшее время между срабатыванием датчика системы безопасности и моментом достижения соответствующего безопасного состояния, реализуемого исполнительным(и) устройством(ами) системы безопасности при наличии ошибок или отказов в канале, выполняющем функцию безопасности.

[МЭК 61784-3:2010, 3.1.1.36, модифицировано]

3.50 **полнота безопасности** (safety integrity): Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени.

Примечания

1 Чем выше уровень полноты безопасности, тем ниже вероятность того, что система, связанная с безопасностью, не сможет выполнить указанные функции безопасности или не будет в состоянии, когда потребуется, принять указанное состояние.

2 Существует четыре уровня полноты безопасности для систем (см. МЭК 61508-4, 3.5.8).

3 При определении полноты безопасности должны учитывать все причины отказов (случайных отказов аппаратных средств и систематических отказов), которые приводят к небезопасному состоянию, например, отказы аппаратных средств, отказы, вызванные программным обеспечением, и отказы, вызванные электрическими помехами. Некоторые из этих типов отказов, например случайные отказы аппаратных средств, могут быть охарактеризованы количественно, с использованием таких параметров, как интенсивность отказов в опасном режиме или вероятность того, что система защиты, связанная с безопасностью, не сможет выполнить запрос. Однако полнота безопасности системы также зависит и от многих факторов, которым нельзя дать точную количественную оценку и которые могут быть оценены только качественно.

4 Полнота безопасности включает в себя полноту безопасности аппаратных средств (см. МЭК 61508-4, 3.5.7) и полноту безопасности по отношению к систематическим отказам (см. МЭК 61508-4, 3.5.6).

5 Данное определение основано на определении безотказности (надежности) систем, связанных с безопасностью, при выполнении ими функций безопасности (определение надежности см. МЭК 60050-191, 191-12-01).

[МЭК 61508-4:2010, 3.5.4]

3.51 **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 Меры целевых отказов (см. МЭК 61508-4, 3.5.17) для четырех уровней полноты безопасности указаны в МЭК 61508-1, таблицы 2 и 3.

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

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

[МЭК 61508-4:2010, 3.5.8]

4 Данная схема спецификации применима только к системе, связанной с безопасностью.

5 Целевые меры по отказу для четырех уровней целостности безопасности определены в таблицах 1 и 2.

3.52 **предельное значение УПБ** (SIL capability): Максимальное значение УПБ, которое может быть достигнуто для ПЛК-ФБ с учетом архитектурных ограничений и систематической полноты безопасности.

[МЭК 62061:2005, 3.2.24]

3.53 **система, связанная с безопасностью** (safety-related system): Система, которая:

- реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния УО;

- предназначена для достижения своими средствами или в сочетании с другими Э/Э/ПЭ системами, связанными с безопасностью, и другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности.

Примечания

1 Данный термин относится к системам, обозначенным как системы, связанные с безопасностью, и предназначенным для достижения совместно с внешними средствами снижения риска (см. 3.4.2 МЭК 61508-4) необходимого снижения риска для соответствия требованиям приемлемого риска (см. 3.1.7 МЭК 61508-4). См. также приложение А МЭК 61508-5.

2 Системы, связанные с безопасностью, предназначены для того, чтобы предотвратить переход УО в опасное состояние путем выполнения необходимых действий при обнаружении условий, которые могут привести к опасному событию. Отказ системы, связанной с безопасностью, может быть отнесен к событиям, ведущим к возникновению определенной опасности или опасностей. Хотя могут существовать и другие системы, имеющие функции безопасности, именно системы, связанные с безопасностью, предназначены для достижения требуемого приемлемого риска. В широком смысле системы, связанные с безопасностью, могут быть разделены на две категории: системы управления, связанные с безопасностью, и системы защиты, связанные с безопасностью.

3 Системы, связанные с безопасностью, могут быть составной частью системы управления УО либо связаны с УО с помощью датчиков и/или исполнительных устройств. Это означает, что необходимый уровень полноты безопасности может быть достигнут реализацией функций безопасности в системе управления УО (и, возможно, также дополнительными отдельными и независимыми системами), либо функции безопасности могут быть реализованы отдельными, независимыми системами безопасности.

4 Система, связанная с безопасностью, может быть предназначена:

a) для предотвращения опасного события (т.е. если система, связанная с безопасностью, выполняет свои функции безопасности, то опасного события не происходит);

b) ослабления последствий вредного события, снижая риск путем уменьшения последствий;

c) достижения целей перечислений a) и b).

5 Человек может быть частью системы, связанной с безопасностью (см. 3.4.1 МЭК 61508-4). Например, человек может получать информацию от программируемого электронного устройства и выполнять действие, связанное с безопасностью, основываясь на этой информации, либо выполнять действие, используя программируемое электронное устройство.

6 Система, связанная с безопасностью, включает в себя все аппаратные средства, программное обеспечение и дополнительные средства (например, источники питания), необходимые для выполнения указанных функций безопасности [датчики, другие устройства ввода, исполнительные элементы (устройства привода) и другие устройства вывода включаются в систему, связанную с безопасностью].

7 Система, связанная с безопасностью, может основываться на широком диапазоне технологий, включая Э/Э/ПЭ, гидравлическую и пневматическую технологии.

[МЭК 61508-4:2010, 3.4.1]

3.54 **программное обеспечение** (software): Продукт интеллектуальной деятельности, включающий в себя программы, процедуры, данные, правила и ассоциированную информацию, имеющий отношение к работе системы обработки данных.

Примечания

1 Программное обеспечение является независимым от носителя, на котором оно записано.

2 Данное определение без примечания 1 отличается от представленного в ИСО 9000-3 добавлением слова «данные».

[МЭК 61508-4:2010, 3.2.5]

3.55 **подсистема** (subsystem): Часть ПЛК-ФБ, включающая отдельный компонент или совокупность компонентов, который выполняет одну или более функций.

Примечание — В настоящем стандарте использование термина «подсистема» отличается от его определения в МЭК 61508-4.

3.56 **систематический отказ** (systematic failure): Отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов.

[МЭК 60050-191:1990,191-04-19]

Примечания

1 Корректирующее сопровождение без модификации обычно не устраняет причину отказа.

2 Систематический отказ может быть вызван имитацией причины отказа.

3 Примерами причин систематических отказов являются ошибки человека:

- в спецификации требований к безопасности;
- в проекте, изготовлении, установке или работе аппаратных средств;
- при проектировании, реализации и т.п. программного обеспечения.

4 В настоящем стандарте отказы в системах, связанных с безопасностью, подразделяют на случайные отказы аппаратных средств (см. 3.6.5) и систематические отказы.

[МЭК 61508-4:2010, 3.6.6]

3.57 **полезный срок службы** (useful lifetime, worst case): Минимальный период времени между установкой ПЛК-ФБ и моментом времени, когда интенсивности отказов компонентов ПЛК-ФБ больше не могут быть предсказаны с какой-либо точностью.

Пример — Момент времени, когда вычисленные в начале значения β-факторов по методике, определенной в приложении D МЭК 61508-6, больше не справедливы.

3.58 **подтверждение соответствия** (validation): Подтверждение, путем испытаний и представления объективных свидетельств, выполнения конкретных требований к предусмотренному конкретному использованию.

Примечания

1 Данное определение адаптировано из ИСО 8402 исключением примечаний.

2 В настоящем стандарте рассматриваются три стадии подтверждения соответствия:
- подтверждение соответствия всей системы безопасности (см. рисунок 2 МЭК 61508-1);
- подтверждение соответствия Э/Э/ПЭ системы, связанной с безопасностью (см. рисунок 3 МЭК 61508-1);
- подтверждение соответствия программного обеспечения (см. рисунок 4 МЭК 61508-1).

3 Подтверждение соответствия представляет собой демонстрацию того, что рассматриваемая система, связанная с безопасностью, до или после установки соответствует во всех отношениях спецификации требований к безопасности для этой системы, связанной с безопасностью. Например, подтверждение соответствия программного обеспечения означает подтверждение путем испытаний и предоставления объективных свидетельств того, что программное обеспечение соответствует спецификации требований к программному обеспечению системы безопасности.

[МЭК 61508-4:2010, 3.8.2]

3.59 **верификация** (verification): Подтверждение выполнения требований путем исследования и сбора объективных свидетельств.

Примечания

1 Данное определение адаптировано из ИСО 8402 исключением примечаний.

2 В контексте настоящего стандарта верификация представляет собой выполняемую для каждой стадии жизненного цикла соответствующей системы безопасности (всей системы, ПЛК-ФБ) путем анализа, математических обоснований и/или тестирования демонстрацию того, что для используемых входных данных выходные данные соответствуют во всех отношениях набору задач и требований для рассматриваемой стадии жизненного цикла системы безопасности.

Пример — Процессы верификации включают в себя:

- анализ выходных данных (документов, относящихся ко всем стадиям жизненного цикла безопасности) для того, чтобы убедиться в соответствии задачам и требованиям соответствующей стадии, с учетом конкретных входных данных для этой стадии;

- анализ проекта;

- тестирование, выполняемое для проектируемых изделий, для того, чтобы убедиться в том, что они работают в соответствии с их спецификациями;

- комплексные испытания, выполняемые там, где различные части системы последовательно объединяются, и испытания на воздействие окружающей среды необходимы для того, чтобы убедиться, что все части работают совместно в соответствии с техническими требованиями.

[МЭК 61508-4:2010, 3.8.1]

3 В настоящем стандарте стадия верификации охватывает все действия, которые связаны с разработкой ПЛК-ФБ и доказательством того, что разработанный ПЛК-ФБ соответствует своей спецификации.

4 Соответствие настоящему стандарту

Настоящий стандарт охватывает конкретные требования к изделию из МЭК 61508-1, МЭК 61508-2 и МЭК 61508-3. В то время, как серия МЭК 61508 является системным (базовым) стандартом, настоящий стандарт содержит конкретные требования к изделию, обеспечивающие применение принципов стандартов серии МЭК 61508 к ПЛК-ФБ.

Соответствие настоящему стандарту применимо только в том случае, когда программируемый контроллер и связанные с ним периферийные устройства, как определено в МЭК 61131-1, предназначены для использования в качестве логической подсистемы Э/Э/ПЭ системы, связанной с безопасностью, и программируемый контроллер определен как программируемый логический контроллер, удовлетворяющий требованиям функциональной безопасности (ПЛК-ФБ). ПЛК-ФБ может также включать элементы программного обеспечения, например предварительно созданные функциональные блоки.

Чтобы установить соответствие настоящему стандарту, должно быть продемонстрировано, что требования функциональной безопасности каждого раздела и подраздела настоящего стандарта были удовлетворены.

ПЛК-ФБ должен сначала удовлетворять установленным требованиям МЭК 61131-2, прежде чем рассматривать соответствие с настоящим стандартом. Для соответствия с МЭК 61131-3 никакого эквивалентного требования не существует.

За соответствие разделам и подразделам настоящего стандарта ответственность несет производитель ПЛК-ФБ.

5 Жизненный цикл ПЛК-ФБ

5.1 Общие положения

Для систематизированного рассмотрения всех действий, необходимых для обеспечения требуемой(ых) логической(их) функции(й) ПЛК-ФБ и предельного значения УПБ для ПЛК-ФБ, в настоящем подразделе принят подход, основанный на жизненном цикле ПЛК-ФБ, который представлен на рисунке 3.

Рисунок 3 основывается на рисунках 2—4 из МЭК 61508-1, рисунках 2 и 4 из МЭК 61508-2 и рисунках 2—5 из МЭК 61508-3.

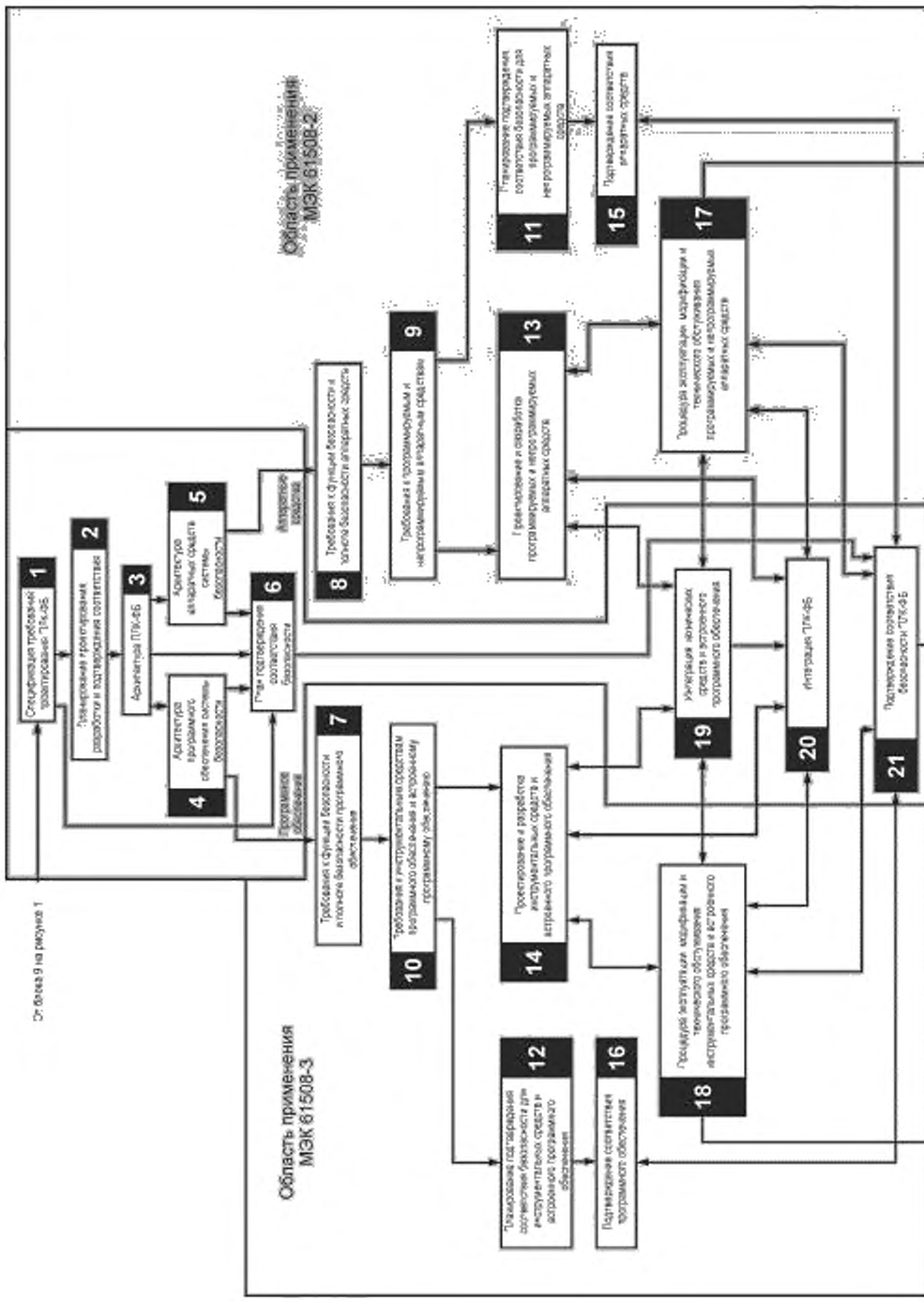


Рисунок 3 — Жизненный цикл ПЛК-ФБ (стадия реализации)

Примечания

1 Ссылки «От блока 9 на рисунке 1» или «К блоку 12 на рисунке 1» подразумевают рисунок 1.

2 Данный рисунок представляет типичные задачи, связанные с разработкой ПЛК-ФБ, но не описывает фиксированную последовательную процедуру при разработке ПЛК-ФБ.

Рисунок 3, лист 2

Для всех стадий жизненного цикла ПЛК-ФБ, представленных на рисунке 3, в разделах 5 — 16 определены требования для ПЛК-ФБ, сформированные в соответствии с МЭК 61508-2 и МЭК 61508-3. Рисунок 3, по сути, не отличается от исходных рисунков МЭК 61508-1, МЭК 61508-2 и МЭК 61508-3, но включает некоторые разъяснения и отличия.

Требования разделов 5 — 16 охватывают все спецификации требований к ПЛК-ФБ: к аппаратным средствам (включая ASIC, FPGA и т.д.) и к программному обеспечению. Рисунок 3 представляет поток принятия архитектурных решений для ПЛК-ФБ, а также демонстрирует, как разделяются требования между спецификациями требований безопасности аппаратных средств ПЛК-ФБ и спецификациями требований безопасности программного обеспечения ПЛК-ФБ.

Для программного обеспечения ПЛК-ФБ рассматриваются два типа средств (инструментальные средства и встроенное программное обеспечение). В то время как их считают программным обеспечением, существуют некоторые явные различия в их влиянии и отношениях с наборами инструментальных средств, с используемыми методами и т. д., используемыми для разработки аппаратных средств.

Для аппаратных средств ПЛК-ФБ показаны три типа средств (программируемые технические средства, специализированные заказные интегральные схемы и непрограммируемые технические средства). В то время как их считают аппаратными средствами, существуют некоторые явные различия в их влиянии и отношениях с наборами инструментальных средств, с используемыми методами и т. д., используемыми для разработки программного обеспечения.

Блоки 17, 18, 19 и 20 на рисунке 3 изображают постепенную интеграцию частей программного обеспечения и аппаратных средств ПЛК-ФБ.

На первом уровне интеграция выполняется между программируемыми аппаратными средствами и встроенным программным обеспечением, предназначенным для данных аппаратных средств. Это хорошо показано на исходных рисунках в МЭК 61508.

На втором уровне интеграция выполняется, когда имеются все части ПЛК-ФБ: программируемые технические средства и их встроенное программное обеспечение, непрограммируемые технические средства и инструментальные средства. На исходных рисунках в МЭК 61508 это показано неявно, а на рисунке 3 рассматривается подробно.

Только после завершения интеграции на втором уровне для ПЛК-ФБ может быть выполнено подтверждение соответствия безопасности.

5.2 Требования к функциональной безопасности и предельному значению УПБ ПЛК-ФБ

5.2.1 Общие положения

Перед выполнением стадии реализации должны быть установлены требования функциональной безопасности и требования к полноте безопасности, определяя логические функции ПЛК-ФБ и его предельное значение УПБ. Затем должно быть выполнено распределение требований функциональной безопасности и для аппаратных средств, или для программного обеспечения, или для тех и других. Это приводит к подробным требованиям для аппаратных средств и программного обеспечения, что определено в разделах 9 и 10, соответственно.

В настоящем стандарте рассмотрены следующие стадии жизненного цикла аппаратных средств и программного обеспечения:

- спецификация требований проектирования ПЛК-ФБ (блок 1 на рисунке 3);
- планирование проектирования, разработки и подтверждения соответствия (блок 2 на рисунке 3);
- архитектура ПЛК-ФБ (блок 3 на рисунке 3);
- архитектура программного обеспечения системы безопасности (блок 4 на рисунке 3);
- архитектура аппаратных средств системы безопасности (блок 5 на рисунке 3);
- планирование подтверждения соответствия безопасности (блок 6 на рисунке 3 раздела 11);
- требования к функции безопасности и полноте безопасности аппаратных средств (блок 7 на рисунке 3),
- требования к функции безопасности и полноте безопасности программного обеспечения (блок 8 на рисунке 3);

- требования к программируемым и непрограммируемым аппаратным средствам (блок 9 на рисунке 3);
- требования к инструментальным средствам и встроенному программному обеспечению (блок 10 на рисунке 3);
- планирование подтверждения соответствия безопасности для программируемых и непрограммируемых аппаратных средств (блок 11 на рисунке 3);
- планирование подтверждения соответствия безопасности для инструментальных средств и встроенного программного обеспечения (блок 12 на рисунке 3);
- проектирование и разработка программируемых и непрограммируемых аппаратных средств (блок 13 на рисунке 3);
- проектирование и разработка инструментальных средств и встроенного программного обеспечения (блок 14 на рисунке 3);
- подтверждение соответствия аппаратных средств (блок 15 на рисунке 3);
- подтверждение соответствия программного обеспечения (блок 16 на рисунке 3);
- процедура эксплуатации и модификации программируемых и непрограммируемых аппаратных средств (блок 17 на рисунке 3);
- процедура эксплуатации и модификации инструментальных средств и встроенного программного обеспечения (блок 18 на рисунке 3);
- интеграция аппаратных средств и встроенного программного обеспечения (блок 19 на рисунке 3);
- интеграция ПЛК-ФБ (блок 20 на рисунке 3);
- подтверждение соответствия безопасности ПЛК-ФБ (блок 21 на рисунке 3).

5.2.2 Безопасность данных

5.2.2.1 Общие положения

Анализ угроз и нарушения безопасности обычно необходимы для связанных с безопасностью применений, чтобы защитить от преднамеренных атак или неумышленных изменений. Безопасность может быть достигнута с помощью установления надлежащей политики безопасности и мер таких, как физические (например, механические средства, электронные средства) или организационные.

Если связанные с безопасностью коммуникации являются частью ПЛК-ФБ, то существует возможность непреднамеренных изменений параметров сетевых устройств. Связанные с безопасностью коммуникационные устройства должны иметь средства защиты от непреднамеренных изменений.

Для обеспечения безопасности всей системы необходимо применять требования, определенные в МЭК 62443, если они применимы.

5.2.2.2 Предположения безопасности для обеспечения функциональной безопасности и предельного значения УПБ

Основная политика безопасности для обеспечения условия(й) безопасности ПЛК-ФБ в соответствии со сложностью оборудования должна предусматривать следующие службы безопасности:

- логическое управление доступом к ПЛК-ФБ и между ними, включая человеко-машинные интерфейсы. Такое логическое управление ограничено известным сообществом пользователей, доступ которых к одному или более устройств санкционирован средствами управления. Обычно логический доступ ограничен небольшой группой пользователей, которые устанавливают, поддерживают и администрируют эти службы, и предоставляет возможность на ролевой основе выборочного доступа, изменения и/или использования определенной информации;
- административное управление, такое, чтобы для конкретного условия безопасности выполнялся общий подход по управлению и администрированию политики обеспечения безопасности на условиях единоначалия с общей ответственностью;
- физическое управление, ограничивающее несанкционированный доступ к ПЛК-ФБ (включая вспомогательные части, кабельные соединения, разъемы).

Производитель ПЛК-ФБ должен обеспечить инструкции по выполнению этих служб, где они применимы.

На основе анализа угроз и нарушения безопасности должны быть применены надлежащие меры, например:

a) управление коммуникационными записями;
b) доступ с механическим или логическим ключом;
c) инструкции по ограничению физического доступа, например посредством закрытых корпусов;
d) инструкции ограниченного доступа по сети;
e) защита встроенным паролем;
f) печать защиты от несанкционированного вскрытия;
g) выявление и отслеживание управления изменениями.

5.3 Система менеджмента качества

При разработке и изготовлении ПЛК-ФБ следует использовать систему управления качеством, которая:

- включает предварительные условия для проектирования и разработки аппаратных средств (включая ASIC, FPGA и т.д.)/программного обеспечения и производства ПЛК-ФБ;
- описывает требования для процессов разработки и создания аппаратных средств (включая ASIC, FPGA и т.д.)/программного обеспечения;
- гарантирует, чтобы ПЛК-ФБ соответствовал требованиям, определенным в настоящем стандарте, и всем нормативным стандартам, на которые ссылается настоящий стандарт;
- гарантирует, что подробно задокументированы результаты разработки и тестирования аппаратных средств (включая ASIC, FPGA и т.д.) / программного обеспечения;
- гарантирует воспроизводимые, подробно задокументированные стадии разработки и изготовления аппаратных средств (включая ASIC, FPGA и т.д.)/программного обеспечения;
- включает систему управления изменениями/управления версиями и систему управления конфигурацией.

Примечание — Пример требований для системы управления качеством описан в ИСО 9001.

5.4 Управление жизненным циклом ПЛК-ФБ

5.4.1 Цели

Первой целью требований настоящего подраздела является определение ответственностей в управлении функциональной безопасностью для тех, кто несет ответственность за ПЛК-ФБ или за одну или более стадий жизненных циклов ПЛК-ФБ и программного обеспечения системы безопасности.

Второй целью требований настоящего подраздела является определение действий, выполняемых ответственными за управление функциональной безопасностью.

Примечание — Организационные мероприятия, относящиеся к данному подразделу, обеспечивают эффективную реализацию технических требований и предназначены исключительно для достижения и поддержания функциональной безопасности ПЛК-ФБ. Технические требования, необходимые для поддержания функциональной безопасности, определены как часть информации, предоставляемой изготовителем ПЛК-ФБ (см. раздел 16).

5.4.2 Требования и процедуры

5.4.2.1 Требования

5.4.2.1.1 Общие положения

Организация, ответственная за реализацию ПЛК-ФБ, или за одну или несколько стадий жизненных циклов всей системы безопасности, ПЛК-ФБ или программного обеспечения системы безопасности, должна выделить одного или более сотрудников, несущих полную ответственность:

- за ПЛК-ФБ и стадии его жизненного цикла;
- координацию действий, связанных с безопасностью, выполняемых на этих стадиях;
- взаимодействие между этими стадиями и другими стадиями, выполняемыми другими организациями;
- выполнение требований 5.4.2.1.2 — 5.4.2.1.11 и 5.4.2.2.2;
- координацию оценки функциональной безопасности (см. перечисление b) 5.4.2.1.11 и раздел 14), особенно на тех стадиях, где выполнение оценки функциональной безопасности различается, включая передачу, планирование и объединение документации, обоснований и рекомендаций;
- удостоверение того, что функциональная безопасность достигнута и продемонстрировано соответствие с целями и требованиями настоящего стандарта.

Ответственность за действия, связанные с безопасностью, или за стадии жизненного цикла безопасности, могут быть делегированы другим сотрудникам, в частности, выполняющим экспертизу. Однако это делегирование должно принадлежать одному или небольшой группе сотрудников с достаточным уровнем административного ресурса.

5.4.2.1.2 Политика и стратегия достижения функциональной безопасности

Должны быть определены политика и стратегия достижения функциональной безопасности, а также средства для оценки ее достижения и средства взаимодействия внутри организации.

5.4.2.1.3 Установление ответственности

Должны быть определены все лица, подразделения и организации, ответственные за выполнение действий на соответствующих стадиях жизненных циклов всей системы безопасности, ПЛК-ФБ и

программного обеспечения системы безопасности (включая отдельных лиц, ответственных за проверку и оценку функциональной безопасности и, где это необходимо, органы лицензирования и органы регулирования в области безопасности), а также до них полностью и ясно должна быть доведена их ответственность.

5.4.2.1.4 Передача информации

Должны быть разработаны процедуры для определения того, какая информация будет передаваться между соответствующими сторонами и как эта передача будет осуществляться.

Примечание — Требования к документации см. раздел 5 МЭК 61508-1.

5.4.2.1.5 Последовательное разрешение рекомендаций

Должны быть разработаны процедуры, предназначенные для обеспечения быстрого последовательного и удовлетворительного разрешения рекомендаций, относящихся к ПЛК-ФБ, сформированных по результатам:

a) оценки функциональной безопасности (см. раздел 14);

b) действий по верификации (см. 13);

c) действий по подтверждению соответствия (см. раздел 11);

d) управления конфигурацией (см. раздел 15).

5.4.2.1.6 Анализ эксплуатационных отказов и информации пользователей

Для анализа эксплуатационных отказов и информации пользователей должны быть разработаны процедуры, включающие:

- распознавание систематических отказов, которые могут подвергать риску функциональную безопасность;

- оценку интенсивности отказов во время эксплуатации и обслуживания в соответствии с требованиями, специфицированными во время определения стадии жизненного цикла, для всей области применения.

5.4.2.1.7 Внутренние аудиты качества

Должны быть определены требования к периодическим внутренним аудитам качества процессов проектирования и производства ПЛК-ФБ, включая:

a) частоту проведения внутренних аудитов качества;

b) уровень независимости стороны, выполняющей аудит;

c) требуемую документацию, корректирующие действия и последующие действия.

5.4.2.1.8 Модификация

Должны быть разработаны процедуры:

a) для инициирования изменений в ПЛК-ФБ;

b) получения полномочий и разрешения для внесения изменений.

5.4.2.1.9 Должны быть разработаны процедуры для поддержания точной информации о неисправностях и отказах ПЛК-ФБ.

5.4.2.1.10 Управление конфигурацией

Должны быть разработаны процедуры для управления конфигурацией ПЛК-ФБ, включая, в частности:

a) указатель на определенные стадии, на которых должен быть реализован формальный контроль конфигурации;

b) процедуры, которые должны быть использованы для уникальной идентификации всех составных частей компонентов (аппаратных средств и программного обеспечения);

c) процедуры для предотвращения использования неутвержденных компонентов.

5.4.2.1.11 Управление конфигурацией программного обеспечения

Должны быть разработаны процедуры для управления конфигурацией программного обеспечения ПЛК-ФБ во время соответствующих стадий жизненного цикла системы безопасности на ПЛК-ФБ. В частности, система управления конфигурацией программного обеспечения должна:

a) использовать административные и технические средства управления на протяжении жизненного цикла программного обеспечения системы безопасности для того, чтобы управлять изменениями в программах и, таким образом, гарантировать непрерывное выполнение указанных в спецификациях требований к программному обеспечению, связанному с безопасностью;

b) гарантировать выполнение всех необходимых операций для того, чтобы продемонстрировать достижение заданной полноты безопасности программным обеспечением, связанным с безопасностью;

c) осуществлять аккуратную поддержку с использованием уникальной идентификации всех элементов конфигурации, которые необходимы для обеспечения требований полноты безопасности ПЛК-ФБ;

d) элементы конфигурации должны включать в себя, как минимум, следующее:

- анализ системы функциональной безопасности и требования к ней;
- спецификация программного обеспечения и проектная документация;
- исходный текст программных модулей;
- план и результаты тестирования;
- ранее разработанные программные элементы и пакеты, которые должны быть включены в ПЛК-ФБ;
- все инструментальные средства и системы разработки, которые использовались при создании, тестировании или выполнении иных действий с программным обеспечением ПЛК-ФБ;

e) использовать процедуры управления изменениями для того, чтобы:

- предотвращать несанкционированные модификации;
- документально оформлять запросы на выполнение модификаций;
- анализировать влияние предлагаемых модификаций;
- утверждать либо отвергать запросы на выполнение модификаций;
- подробно документально оформлять модификации и выдавать полномочия на выполнение всех утвержденных модификаций;
- устанавливать базовую конфигурацию для соответствующих этапов разработки программного обеспечения;
- документально оформлять тестирование (частичное) интеграции системы, обосновывающее базовую конфигурацию;
- гарантировать объединение и встраивание всех базовых конфигураций программного обеспечения (включая переработку более ранних версий базовых конфигураций).

Для ведения и осуществления административных и технических средств управления необходимы наличие полномочий и принятие управленческих решений;

f) иметь процедуру, гарантирующую, что осуществлены соответствующие меры, чтобы корректно загружать прикладное программное обеспечение и данные в ПЛК-ФБ.

Допускается рассматривать отдельные целевые системы, а также общие системы;

g) документально оформлять перечисленную ниже информацию, для того чтобы обеспечить возможность последующего аудита конфигурации:

- состояние конфигурации,
- состояние версии системы,
- обоснование и утверждение всех модификаций,
- подробное описание всех модификаций;

h) строго документально оформлять каждую версию программного обеспечения, связанного с безопасностью. Обеспечить хранение всех версий программного обеспечения и всей относящейся к ним документации, а также версий данных для обеспечения возможности сопровождения и выполнения модификаций на протяжении всего периода использования разработанного программного обеспечения.

Примечание — Дополнительную информацию по управлению конфигурацией см. ИСО/МЭК 12207, IEEE 828, IEEE 1042.

5.4.2.2 Лица, управляющие функциональной безопасностью

5.4.2.2.1 Лица и спецификация их действий

Те лица, которые несут ответственность за одну или более стадий жизненных ПЛК-ФБ или программного обеспечения системы безопасности, должны для тех стадий, за которые они несут ответственность, и в соответствии с процедурами, определенными в 5.4.2.1 и его подпунктах, определить все управленческие и технические действия, необходимые для обеспечения достижения, демонстрации и поддержания функциональной безопасности ПЛК-ФБ, включая:

a) подобранные меры и методы, используемые для удовлетворения требованиям конкретного раздела или подраздела;

b) действия по оценке функциональной безопасности, а также способ, с помощью которого будет продемонстрировано достижение функциональной безопасности для тех, кто осуществляет ее оценку (см. раздел 14).

При оценке функциональной безопасности должны быть использованы соответствующие процедуры:

- для определения выбора соответствующей организации, лица или лиц с надлежащим уровнем независимости;
- составления и внесения изменений при оценке функциональной безопасности;
- замены тех, кто осуществляет оценку функциональной безопасности на каждом этапе жизненного цикла системы;
- разрешения споров с участием лиц, осуществляющих оценку функциональной безопасности.

5.4.2.2.2 Процедуры и лица

Должны быть разработаны процедуры, гарантирующие, что все лица, ответственность которых определена в соответствии с 5.4.2.1 и 5.4.2.3.1 (т. е. все лица, участвующие в любом из жизненных циклов системы безопасности на ПЛК-ФБ или ее программного обеспечения, включая их действия по верификации, управлению функциональной безопасностью и оценке функциональной безопасности), должны иметь соответствующую компетентность (т. е. пройти обучение, обладать техническими знаниями, опытом и квалификацией), относящуюся к конкретным обязанностям, которые они должны выполнять. Такие процедуры должны включать требования к актуализации, обновлению и непрерывности оценки компетентности.

5.4.2.2.3 Компетентность и лица

Соответствие компетентности должны рассматривать для конкретной области применения, с учетом всех факторов, включая:

a) ответственность конкретного лица;

b) уровень необходимого надзора;

c) уровни полноты безопасности ПЛК-ФБ — чем выше уровень полноты безопасности, тем более строгой должна быть спецификация компетентности;

d) новизну проекта, проектных процедур или области применения — чем более новыми или менее проверенными они являются, тем более строгой должна быть спецификация компетентности;

e) предыдущий опыт и его актуальность для конкретных выполняемых обязанностей и используемых технологий — чем больше требуемая компетентность, тем выше должно быть соответствие между компетентностью, полученной из предыдущего опыта, и компетентностью, необходимой для конкретных видов деятельности, которые должны быть выполнены;

f) тип компетентности, соответствующий обстоятельствам (например, квалификация, опыт, соответствующая подготовка и последующая практика, способности к лидерству и принятию решений);

g) инженерные знания, соответствующие области применения и технологии;

h) инженерные знания в области безопасности, соответствующие применяемой технологии;

i) знание законодательной и нормативно-правовой базы в области безопасности;

j) соответствие квалификации конкретным выполняемым действиям.

Компетентность всех лиц и их ответственности, определенные в соответствии с 5.4.2.1 и 5.4.2.1.3, должны быть документально оформлены.

5.4.2.3 Поставщики

Поставщики, предоставляющие продукцию или услуги организациям, несущим полную ответственность за одну или несколько стадий жизненных циклов системы безопасности на ПЛК-ФБ или ее программного обеспечения (см. 5.4.2.1), должны поставлять свою продукцию или услуги в соответствии со спецификациями этих организаций и должны иметь соответствующую систему управления качеством.

У поставщиков должны быть система управления качеством и, кроме того, надлежащая система управления функциональной безопасности.

5.4.2.4 Планирование функциональной безопасности программного обеспечения

Планирование функциональной безопасности должно определять стратегию поставок, разработки, интеграции, верификации, подтверждения соответствия и модификации программного обеспечения в той мере, в какой этого требует уровень полноты безопасности функций, реализуемых ПЛК-ФБ.

Примечание — Идея настоящего подхода состоит в применении планирования функциональной безопасности в качестве возможности для адаптации настоящего стандарта с учетом требуемой полноты безопасности для каждой функции безопасности, реализуемой ПЛК-ФБ.

Если программное обеспечение должно реализовать функции безопасности в ПЛК-ФБ, имеющие различный уровень полноты безопасности, то следует считать, что все программное обеспечение имеет наивысший уровень среди этих уровней, если только в проекте не будет продемонстрирована достаточная независимость реализуемых ПЛК-ФБ функций, имеющих различный уровень полноты безопасности. Обоснование независимости должно быть документально оформлено.

Примечание — Дополнительные требования см. в 6.2.2 МЭК 61508-3.

5.4.3 Выполнение и контроль

Все действия, указанные в 5.4.2, должны быть реализованы, и их выполнение следует контролировать.

5.4.4 Управление функциональной безопасностью

Действия, относящиеся к управлению функциональной безопасностью, должны быть применены на соответствующих стадиях жизненных циклов системы безопасности на ПЛК-ФБ или ее программного обеспечения в соответствии с целевым предельным значением УПБ и МЭК 61508.

6 Спецификация требований к проектированию ПЛК-ФБ

6.1 Общие положения

Первой целью данной стадии является определение требований к функциональной безопасности и полноте безопасности ПЛК-ФБ, содержащихся в спецификации требований к проектированию. Они являются ориентированными на ПЛК-ФБ требованиями к функциональной безопасности и полноте безопасности Э/Э/ПЭ системы, связанной с безопасностью, для предполагаемого(ых) применения(й).

Второй целью данной стадии является определение предельного значения УПБ для ПЛК-ФБ на основе функции, определенной из связанной с безопасностью Э/Э/ПЭ системы, для обеспечения спецификации и разработки ПЛК-ФБ.

6.2 Содержание спецификации требований к проектированию

Спецификация требований к проектированию ПЛК-ФБ должна содержать.

a) определение требования(й) безопасности к аппаратным средствам, программному обеспечению или их комбинации с достаточным уровнем детализации для проектирования и разработки ПЛК-ФБ.

Примечание — Функции безопасности ПЛК-ФБ переводят его выходы в безопасное состояние, определенное производителем, или поддерживают безопасное состояние, определенное производителем;

b) предполагаемое предельное значение УПБ для ПЛК-ФБ;

c) спецификацию безопасного состояния или безопасных состояний ПЛК-ФБ;

d) определение ограничений работы ПЛК-ФБ в режиме низкой частоты запросов и в режиме высокой частоты или с непрерывным запросом.

Примечание — Если ПЛК-ФБ используют в различных конфигурациях, то для этих конфигураций могут применять различные ограничения предельных значений УПБ;

e) описание всех мер и методов, необходимых для достижения требуемой функциональной безопасности. Оно должно включать:

1) значение времени необходимое для ПЛК-ФБ, чтобы обработать внешний(е) сигнал(ы) и активировать заданную(ые) функцию(и), например, функцию безопасности ПЛК-ФБ при нормальных условиях и в условиях сбоя; функцию вход/выход; вычисление, результаты которого будут на выходе; выполнение записи на выходе; сетевые коммуникации; выполнение задач.

Примечание — Наихудшее значение времени отклика для функции безопасности ПЛК-ФБ вносит вклад в наихудшее значение времени отклика функции безопасности всей Э/Э/ПЭ системы, связанной с безопасностью (см. МЭК 61784-3);

2) всю информацию, относящуюся к функциональной безопасности, которая может повлиять на проектирование Э/Э/ПЭ системы, связанной с безопасностью;

3) все интерфейсы с ПЛК-ФБ;

4) внешние диагностические тесты сбоев.

Примечание — Например, для цифровых выходов выявление короткого замыкания или обрыва в нагрузке при отсутствии питания;

5) все соответствующие режимы работы ПЛК-ФБ;

6) все требуемые режимы поведения ПЛК-ФБ — в частности, поведение при обнаружении сбоев;

7) значимость всех взаимодействий аппаратных средств/программного обеспечения и (при необходимости) любые требуемые ограничения между аппаратными средствами и программным обеспечением.

Примечание — Если эти взаимодействия неизвестны до завершения разработки, то устанавливают только общие ограничения;

8) предельные и ограничивающие условия для ПЛК-ФБ и любых связанных с ними подсистем, например ограничения синхронизации;

9) любые специфические требования, относящиеся к процедурам запуска и повторного запуска ПЛК-ФБ;

10) значения целевых интенсивностей случайных отказов аппаратных средств для оценки влияния каждого отказа в процессе анализа видов и последствий отказов;

11) любые требования, ограничения, функции и средства для того, чтобы были выполнены контрольные проверки аппаратных средств ПЛК-ФБ.

Примечание — Как правило, интервал контрольных проверок для ПЛК-ФБ — срок эксплуатации;

12) пределы электромагнитной устойчивости и критерии оценки выполнения испытания в соответствии с требованиями 12.5.

Примечание — На основе соглашения между производителем ПЛК-ФБ и пользователем, для определенных применений используют более высокие пределы, например применение световых завес в соответствии с МЭК 61496-1;

13) требования для управления ошибками в любых внешних, связанных с безопасностью, цифровых средствах коммуникации;

14) используемые меры, ограничивающие работу посторонних лиц (ключи, заблокированные компьютеры, сетевой доступ, пароли, и т.д.);

15) критические не зависящие от применения аварийные сигналы и события, например деградация системы, переполнение при сканировании, перезапуск при сбое питания;

16) информационная безопасность — производитель определяет, может ли ПЛК-ФБ быть соединен с незащищенной сетью и любые конкретные меры, необходимые для информационной безопасности.

Примечание — Например, см. руководство по анализу угроз безопасности в серии стандартов МЭК 62443;

17) описание человеко-машинного интерфейса, библиотек, инструментальных средств и т.д., если они связаны с безопасностью;

18) меры гарантии качества/контроля качества на месте;

19) применяемые методы и меры, представленные в таблице В.1 МЭК 61508-2.

6.3 Целевая интенсивность отказов

На основе целевого значения УПБ для ПЛК-ФБ и режима запросов к нему для ПЛК-ФБ определяется PFD (см. таблицу 1) или PFH (см. таблицу 2).

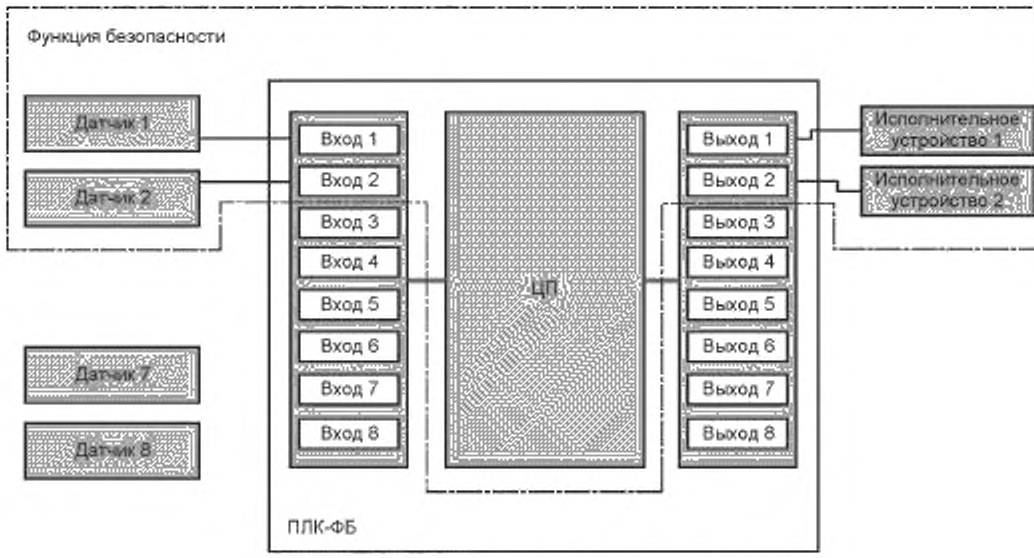


Рисунок 4 — Соответствующие части функции безопасности

Таблица 1 — Уровни полноты безопасности для режима работы с низкой интенсивностью запросов

Уровень полноты безопасности системы, связанной с безопасностью	PFD для функции безопасности	Вклад ПЛК-ФБ в PFD
4[a)]	$> 10^{-5} — < 10^{-4}$	$< k\ 10^{-4}$
3	$> 10^{-4} — < 10^{-3}$	$< k\ 10^{-3}$
2	$> 10^{-3} — < 10^{-2}$	$< k\ 10^{-2}$
1	$> 10^{-2} — < 10^{-1}$	$< k\ 10^{-1}$

[a)] Настоящий стандарт применяют к ПЛК-ФБ для предельных значений УПБ не более, чем УПБ 3. Для предельного значения УПБ 4 к функции безопасности ПЛК-ФБ должны быть применены дополнительные требования серии МЭК 61508.

Примечание — Обычно $0 < k < 0{,}15$.

Таблица 2 — Уровни полноты безопасности для режима работы с высокой интенсивностью запросов или для режима с непрерывным запросом

Уровень полноты безопасности системы, связанной с безопасностью	PFH для функции безопасности	Вклад ПЛК-ФБ в PFH
4[a)]	$> 10^{-9} — < 10^{-8}$	$< k\ 10^{-8}$
3	$> 10^{-8} — < 10^{-7}$	$< k\ 10^{-7}$
2	$> 10^{-7} — < 10^{-6}$	$< k\ 10^{-6}$
1	$> 10^{-6} — < 10^{-5}$	$< k\ 10^{-5}$

[a)] Настоящий стандарт применяют к ПЛК-ФБ для предельных значений УПБ не более, чем УПБ 3. Для предельного значения УПБ 4 к функции безопасности ПЛК-ФБ должны быть применены дополнительные требования комплекса стандартов МЭК 61508.

Примечание — Обычно $0 < k < 0{,}15$.

Требования к полноте безопасности для каждой функции безопасности должны быть сформулированы в терминах PFD или PFH только для случайных отказов аппаратных средств. Если требования к полноте безопасности заданы в терминах PFD, то для достижения этого значения PFD должен быть определен необходимый интервал контрольных проверок.

Примечание — Значения PFD или PFH системы, связанной с безопасностью, определены как сумма значений PFD или значений PFH для датчиков, логической подсистемы и исполнительных устройств, реализующих функцию безопасности. См. рисунок 4.

Для управления систематическими отказами ПЛК-ФБ необходимо использовать методы и меры, представленные в 9.4.6.

Значения PFD или PFH для ПЛК-ФБ должны быть определены производителем ПЛК-ФБ. В соответствии с рекомендациями их значения составляют не более 15 % от значений PFD или PFH для соответствующей Э/Э/ПЭ системы, связанной с безопасностью (коэффициент $k = 0{,}15$ в таблицах 1 и 2).

Цель состоит в том, чтобы разрешить оставшиеся значения PFD или PFH распределить датчикам и исполнительным устройствам.

Значения PFD или PFH для ПЛК-ФБ выше 15%-ного уровня возможны на основе более строгого анализа применения и соглашения между производителем и независимым экспертом после консультаций с пользователем.

Требования функции безопасности и требования полноты безопасности ПЛК-ФБ для Э/Э/ПЭ системы, связанной с безопасностью, для выполнения функции которой ПЛК-ФБ был разработан и специфицирован, должны быть документально оформлены в спецификации требований проектирования ПЛК-ФБ.

7 План проектирования, разработки и подтверждения соответствия ПЛК-ФБ

7.1 Общие положения

В настоящем разделе должно быть выполнено планирование требований к функции безопасности и требований к полноте безопасности ПЛК-ФБ для специфицированной в разделе 6 функции, определенной из связанной с безопасностью Э/Э/ПЭ системы, для обеспечения спецификации и разработки ПЛК-ФБ.

7.2 Разделение требований

Цель настоящей стадии состоит в разделении требований функциональной безопасности и полноты безопасности для ПЛК-ФБ на требования функциональной безопасности и полноты безопасности для программного обеспечения ПЛК-ФБ и требования функциональной безопасности и полноты безопасности для аппаратных средств ПЛК-ФБ, в соответствии с выбранной документально оформленной архитектурой.

После разделения требований функциональной безопасности и полноты для ПЛК-ФБ имеем:

- требования функциональной безопасности и полноты безопасности для программного обеспечения ПЛК-ФБ;
- требования функциональной безопасности и полноты безопасности для аппаратных средств ПЛК-ФБ;
- документально оформленные планы оценок.

В разделах 9 и 10 рассматриваются аппаратные средства ПЛК-ФБ (на стадии реализации) и программное обеспечение ПЛК-ФБ (на стадии реализации), соответственно.

План разработки должен включать план оценки и ряд связанных с аппаратными средствами и программным обеспечением планов проектирования, которые учитывают рекомендации приложения В МЭК 61508-2.

8 Архитектура ПЛК-ФБ

8.1 Общие положения

Цель настоящего раздела состоит в том, чтобы определить удовлетворяющую требованиям безопасности архитектуру аппаратных средств и программного обеспечения ПЛК-ФБ.

На основе спецификации требований функциональной безопасности для системы ПЛК-ФБ может быть выполнена оценка различных архитектур для достижения обязательных требований, установленных в спецификации требований функциональной безопасности. Необходимы компромиссы, чтобы установить и определить, где и как выполнить требуемые функции безопасности ПЛК-ФБ. Эти решения установят общую архитектуру ПЛК-ФБ, а также основанные на ней архитектуры программного обеспечения и аппаратных средств.

Требования к архитектурам программного обеспечения и аппаратных средств должны быть документально оформлены в требованиях к функциональной безопасности программного обеспечения и аппаратных средств, соответственно.

На рисунке 5 блоки, залитые серым цветом, связаны с ПЛК-ФБ и должны быть рассмотрены. Белый блок не является связанной с безопасностью частью ПЛК-ФБ, т.е. помехи на нее не влияют. Заштрихованный блок указывает на возможность этого элемента быть связанным с безопасностью на основе анализа критичности. Если последний будет связан с безопасностью, то он должен быть рассмотрен.

Элементы примера на рисунке 5 в белых и заштрихованных блоках показаны только в иллюстративных целях, и в конкретном применении они могут или не могут быть определены как связанные с безопасностью.

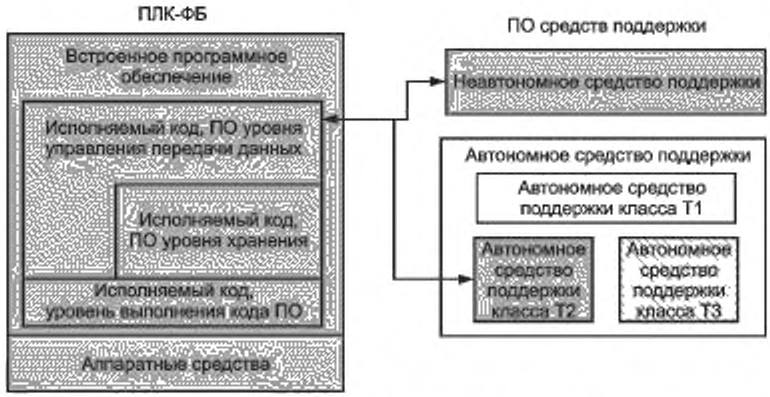


Рисунок 5 — Связь ПЛК-ФБ с инструментальными средствами

8.2 Архитектуры и подсистемы

Подсистемы ПЛК-ФБ могут иметь различные архитектуры.

ПЛК-ФБ использует обозначение архитектуры в виде MooN, означающее, что система состоит из *N* каналов, каждый из которых может выполнять логическую функцию ПЛК-ФБ. По крайней мере, требуется *M* каналов, чтобы выполнять логическую функцию ПЛК-ФБ. Система выполняет логическую функцию ПЛК-ФБ, если *M* каналов функционируют должным образом. (*N*-*M*) определяет отказоустойчивость системы, где (*N*-*M*+1) сбоев в канале будут приводить к отказу логической функции ПЛК-ФБ. Примеры см. в приложении В.

8.3 Передача данных

У системы ПЛК-ФБ обычно есть два типа передачи данных. Один — связанная с безопасностью передача, а другой — не связанная с безопасностью передача.

Коммуникации, связанные с функциональной безопасностью, использующие промышленные шины, должны соответствовать требованиям МЭК 61784-3.

Коммуникации, связанные с безопасностью, использующие отличные от промышленных шин средства передачи, должны соответствовать требованиям 7.4.11 МЭК 61508-2.

Если коммуникации не связаны с безопасностью, то см. МЭК 61131-2.

Должны быть приняты меры по предотвращению любой предсказуемой передачи данных, допустимой или недопустимой от a) оказывающей негативное влияние на корректную работу связанной с безопасностью функции или b) предотвращающей поддержку или достижение заданного безопасного состояния.

9 Планирование проектирования, разработки и подтверждение соответствия аппаратных средств

9.1 Общие требования к аппаратным средствам

Требования 8.3 получены из конкретных требований к аппаратным средствам, содержащихся в спецификации требований функциональной безопасности для ПЛК-ФБ.

9.2 Спецификация требований функциональной безопасности аппаратных средств

Требования функциональной безопасности для аппаратных средств ПЛК-ФБ должны быть определены и/или выведены из спецификации требований функциональной безопасности ПЛК-ФБ.

Если в одном ПЛК-ФБ выполняются связанные с безопасностью функции и не связанные с безопасностью функции, то должны существовать соответствующие меры, предотвращающие негативное влияние не связанных с безопасностью функций на связанные с безопасностью функции.

Требования функциональной безопасности для аппаратных средств ПЛК-ФБ должны быть выражены и структурированы с тем, чтобы они были:

- ясными, точными, недвусмысленными, поддающимися проверке, пригодными для тестирования, поддерживаемыми и реализуемыми;

- оформлены в письменном виде для того, чтобы их лучше понимали те, кто использует эти требования на любой из стадий жизненного цикла системы безопасности на ПЛК-ФБ.

9.3 Планирование подтверждения соответствия безопасности аппаратных средств

Примечание — Данная стадия жизненного цикла ПЛК-ФБ обычно выполняется параллельно с проектированием и разработкой аппаратных средств, см. 9.4.

Планирование подтверждения соответствия аппаратных средств проводят для определения шагов, на которых должно быть продемонстрировано соответствие аппаратных средств спецификации требований функциональной безопасности к аппаратным средствам ПЛК-ФБ (см. 6).

План подтверждения соответствия функциональной безопасности должен включать процедуры, гарантирующие, что каждая функция безопасности корректно реализована и имеет требуемое предельное значение УПБ, описания параметров тестирования и условий окружающей среды, при которых проводят испытания, а также критерии «прошла испытания/не прошла испытания».

Типовые испытания определены в разделе 12.

9.4 Проектирование и разработка аппаратных средств

9.4.1 Общие положения

Проект ПЛК-ФБ должен соответствовать требованиям спецификации требований функциональной безопасности аппаратных средств.

Спроектированные аппаратные средства и документация, появившаяся в процессе проектирования, а также документация рассматриваемой стадии жизненного цикла ПЛК-ФБ должны соответствовать всем следующим требованиям:

a) к предельному значению УПБ (УПБ 1, УПБ 2 или УПБ 3) аппаратных средств на основе подхода отказоустойчивости и доли безопасных отказов аппаратных средств (способ 1_H, описанный в 7.4.4 и 7.4.4.2 МЭК 61508-2), включая архитектурные ограничения на полноту безопасности аппаратных средств (см. 9.4.3, 9.4.3.1.2) и вероятности опасных отказов аппаратных средств (см. 9.4.3.2.4);

b) систематической полноте безопасности, включая требования по предотвращению систематических отказов (см. 9.4.5) и требования по управлению систематическими отказами (см. 9.4.6);

c) поведению ПЛК-ФБ при обнаружении отказов (см. 9.4.2);

d) независимости функций, связанных с безопасностью и не связанных с безопасностью, если все аппаратные средства ПЛК-ФБ не будут рассматриваться как связанные с безопасностью. Независимость должна быть такой, что отказы в частях, не связанных с безопасностью, не должны вызывать опасные отказы в связанной с безопасностью части. Метод достижения такой независимости и обоснование этого метода должны быть документально оформлены.

9.4.2 Требования к поведению ПЛК-ФБ при обнаружении сбоев

Обнаружение опасного сбоя на стадии эксплуатации ПЛК-ФБ должно завершаться:

a) или переходом всех выходов, на которые может повлиять сбой, встроенными в ПЛК-ФБ мерами, например с помощью аппаратных средств или встроенного программного обеспечения, к определенному безопасному состоянию в течение времени реакции на сбой, которое определено производителем;

b) сбоем, уведомляющим (подающим сигнал тревоги) применяемые меры, например определенную производителем прикладную программу во время реакции на сбой, таким образом, чтобы применяемые меры, например прикладная программа, могли бы вызвать надлежащее действие для поддержания безопасности.

Примечание — Какое действие является надлежащим, зависит от применения, и оно определено пользователем, а не производителем ПЛК-ФБ.

Как минимум представленные в таблице 3 сбои должны быть обнаружены, и о них должна быть уведомлена (передан сигнал тревоги) прикладная программа, за исключением тех случаев, когда:

- или сбой не может произойти в ПЛК-ФБ преднамеренно;

- или пропуск отказа обоснован письменно оформленной технической оценкой.

Таблица 3 — Неисправности, которые будут обнаружены и будет уведомлена (передан сигнал тревоги) прикладная программа

Неисправности, которые будут обнаружены и будет уведомлена (передан сигнал тревоги) прикладная программа
Превышено время сканирования — время сканирования больше, чем предварительно установленное максимальное значение
Точки входа или выхода отключены, или на месте существует ручная коррекция при техническом обслуживании
Обнаружение неисправностей отключено
Условие перегрева
Отказ выполнения диагностики
Предпринятый доступ для записи через несанкционированный канал
Режимы работы деградируемой системы — избыточные модули/каналы автономны или неисправны
Потеря питания системы или полевого устройства питания, включая избыточные источники
Потеря или задержка внешних, связанных с безопасностью, средств коммуникации
Деление на ноль или другая обнаруженная логическая ошибка

9.4.3 Полнота безопасности аппаратных средств

9.4.3.1 Отказоустойчивость аппаратных средств

9.4.3.1.1 Общие положения

Во время проектирования ПЛК-ФБ должна быть определена отказоустойчивость аппаратных средств, связанная с функциональной безопасностью. Отказоустойчивость аппаратных средств в сочетании со значением доли безопасных отказов позволяет определить максимально допустимый уровень полноты безопасности (УПБ 1, УПБ 2, или УПБ 3), на который можно претендовать в соответствии со способом 1_H, как описано в МЭК 61508-2.

9.4.3.1.2 Наивысший уровень полноты безопасности, на который можно претендовать

В контексте полноты безопасности аппаратных средств наивысший уровень полноты безопасности, на который может претендовать функция безопасности, ограничен отказоустойчивостью аппаратных средств и составляющей безопасного отказа подсистем, которые выполняют эту функцию безопасности. В таблицах 4 и 5 определяют наивысший уровень полноты безопасности, на который может претендовать функция безопасности ПЛК-ФБ, реализуемая подсистемой, с учетом аппаратной отказоустойчивости и составляющей безопасных отказов этой подсистемы. Требования таблиц 4 и 5 должны быть применены к каждой подсистеме, выполняющей функцию безопасности ПЛК-ФБ и, следовательно, к каждой части ПЛК-ФБ. В 9.4.3.2.2 к 9.4.3.2.4 определяют, какая из таблиц 4 или 5 применяется к любой конкретной подсистеме. В 9.4.3.2.5 и 9.4.3.2.6 определяют, как получить наивысший уровень полноты безопасности, на который можно претендовать функция безопасности ПЛК-ФБ. Что касается данных требований, необходимо учитывать:

a) отказоустойчивость аппаратных средств *N* означает, что *N*+1 сбоев может привести к потере функции безопасности. В определении отказоустойчивости аппаратных средств не должны учитывать другие средства, которые могли бы контролировать последствия сбоев, например диагностика;

b) если один сбой непосредственно приводит к одному или более последующим сбоям, то их рассматривают как одиночный сбой;

c) при определении отказоустойчивости аппаратных средств некоторые сбои могут быть исключены из-за того, что физическое поведение компоненты определяется доминирующим для нее видом отказов. Любые такие исключения сбоев должны быть обоснованы и документально оформлены (см. примечание 3).

Примечание — В ИСО 13849-2 даны примеры исключения сбоев с помощью различных технологий;

d) доля безопасных отказов подсистемы определена отношением суммы средних интенсивностей безопасных отказов и опасных обнаруженных отказов к общей средней интенсивности отказов подсистемы.

Примечания

1 Чтобы достигнуть достаточно устойчивой архитектуры, учитывая уровень сложности подсистемы, включают архитектурные ограничения. Уровень полноты безопасности аппаратных средств для системы ПЛК-ФБ, полученный в результате применения требований настоящего подпункта, является максимальным уровнем из

определенных, на которые может претендовать функция безопасности, даже если в некоторых случаях теоретические расчеты надежности показывают, что мог быть достигнут более высокий уровень полноты безопасности при использовании исключительно математического подхода для анализа системы ПЛК-ФБ.

2 Удовлетворяющие требованиям отказоустойчивости аппаратных средств архитектура и подсистема затем используются при нормальных условиях эксплуатации. Требования отказоустойчивости к аппаратным средствам могут быть снижены, если система ПЛК-ФБ восстанавливается неавтономно. Однако ключевые параметры, связанные с любым снижением требований, должны быть предварительно оценены (например, оценка среднего времени восстановления по отношению к вероятности запроса).

Таблица 4 — Полнота безопасности аппаратных средств. Подсистемы низкой сложности (тип А)

Доля безопасных отказов	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
Менее 60 %	УПБ 1	УПБ 2	УПБ 3
От 60 % до менее 90 %	УПБ 2	УПБ 3	УПБ 4[a)]
От 90 % до менее 99 %	УПБ 3	УПБ 4[a)]	УПБ 4[a)]
Более и равно 99 %	УПБ 3	УПБ 4[a)]	УПБ 4[a)]

[a)] Настоящий стандарт применяют к ПЛК-ФБ с предельным значением УПБ не более чем УПБ 3. Для УПБ 4 применяют особые требования. См. серию МЭК 61508.

Примечание — Данная таблица получена из таблицы 2 МЭК 61508-2.

Таблица 5 — Полнота безопасности аппаратных средств. Подсистемы низкой сложности (тип В)

Доля безопасных отказов	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
Менее 60 %	Не оговаривается	УПБ 1	УПБ 2
От 60 % до менее 90 %	УПБ 1	УПБ 2	УПБ 3
От 90 % до менее 99 %	УПБ 2	УПБ 3	УПБ 4[a)]
Более и равно 99 %	УПБ 2	УПБ 4[a)]	УПБ 4[a)]

[a)] Настоящий стандарт применяется к ПЛК-ФБ с предельным значением УПБ не более чем УПБ 3. Для УПБ 4 применяются особые требования. См. серию МЭК 61508.

Примечание — Данная таблица получена из таблицы 2 МЭК 61508-2.

9.4.3.1.3 Требования к поведению ПЛК-ФБ при обнаружении сбоя

Обнаружение опасного сбоя в ПЛК-ФБ должно завершаться конкретным действием:

a) или для достижения либо поддержания безопасного состояния, определенного производителем;

b) если отказоустойчивость аппаратных средств ПЛК-ФБ больше нуля, то в такой подсистеме следует восстановить дефектную часть в пределах среднего времени продолжительности ремонта MRT, определенного для применения, где разрешена непрерывная эксплуатация, или если отказоустойчивость аппаратных средств ПЛК-ФБ равна нулю и такую подсистему используют в режиме с низкой частотой запросов, то следует восстановить дефектную часть в пределах среднего времени продолжительности ремонта MRT, определенного для применения. Непрерывная эксплуатация подсистемы во время восстановления ПЛК-ФБ должна быть обеспечена дополнительными мерами по снижению риска, выбранными пользователем.

9.4.3.1.4 Независимые сторожевые таймеры

Все подсистемы, которые используют микропроцессор, должны включать функцию сторожевого таймера, которая:

- отделена и работает независимо от состояния микропроцессора;
- не попадает под воздействие механизма общей причины, что может предотвратить неправильную установку сторожевого таймера при установке микропроцессора в исходное состояние.

Необходимо избегать следующих типов механизмов при установке сторожевого таймера в исходное состояние:

a) использовать области памяти или адреса ввода/вывода — должны использовать только единственный адрес;

b) разрешать установку и при операции чтения и при операции записи — только одну операцию должны использовать;

c) использовать адрес, который может быть легко доступен, если микропроцессор «зацикливается»;

d) использовать только максимальное значение тайм-аута, для окна должны быть определены минимальное и максимальное значения.

9.4.3.2 Декомпозиция подсистемы аппаратных средств

9.4.3.2.1 Общие положения

Примечание — Необходимо напомнить, что термин «подсистема», используемый в настоящем стандарте, определен по-другому, чем в МЭК 61508-4. См. 3.55.

В 9.4.3.1 Определены требования для доли безопасных отказов (ДБО) и отказоустойчивости в зависимости от уровня полноты безопасности и типа подсистемы.

Ниже представлена дополнительная информация для двух типов подсистем, определенных в 9.4.3.2.2 и 9.4.3.2.3:

- подсистемы типа А (низкой сложности) обычно создаются из дискретных компонентов (например, резисторов, конденсаторов, диодов, транзисторов), для которых виды сбоев и их влияние на подсистему предсказуемы и четко определены;
- подсистемы типа В (высокой сложности) обычно включают один или несколько сложных или программируемых компонентов (например, микропроцессоры, ASICs, модули ПЛК-ФБ), у которых плохо определены виды сбоев, и их влияние на подсистему непредсказуемо. (Для таких компонентов, в отсутствие лучших данных, можно предположить, что 50% всех сбоев приводят к безопасным сбоям и 50% приводят к опасным сбоям.)

Примечание — Интегральные схемы низкой сложности — это те, у которых известны все виды сбоев и их влияние.

При оценке ПЛК-ФБ ее сначала необходимо декомпозировать на подсистемы. Каждая подсистема должна выполнить требования таблицы 4 или 5 в отношении необходимых ДБО и отказоустойчивости, чтобы достигнуть заданного значения УПБ.

Если две подсистемы зависимы, и одна подсистема обеспечивает диагностику для другой подсистемы, то сначала для подсистемы, обеспечивающей диагностику, необходимо обеспечить выполнение требований таблицы 4 или 5. Затем подсистема, обеспечивающая диагностику, может быть объединена со второй подсистемой, чтобы обеспечить выполнение требований таблицы 4 или 5 для обеих подсистем вместе.

Примечание — Например, модули ввода-вывода ПЛК-ФБ обычно состоят из микропроцессора и подсистемы ввода/вывода, как показано на рисунке 6. Процессор управляет вводом/выводом и часто также выполняет диагностику. В таком случае процессор необходимо рассматривать как подсистему типа В, а ввод/вывод мог быть или подсистемой типа В, или подсистемой типа А в зависимости от компонентов подсистемы.

Рассмотрим случай модуля ввода/вывода, который составлен из двух подсистем; одна — типа А или В, обозначенная подсистема 1, и одна — типа В, обозначенная подсистема 2. Предполагается, что этот модуль ввода-вывода достигает значения уровня полноты безопасности, равного УПБ 3.

Предположим, что подсистема 1 сама по себе имеет отказоустойчивость, равную 1, и ДБО равна 55%. Предположим также, что подсистема 2 сама по себе имеет отказоустойчивость, равную 1, и ДБО равна 95%.

Если подсистема 1 использует процессорный элемент подсистемы 2, чтобы выполнить диагностику, то она может достигнуть высокого значения охвата диагностикой (ОД) и ДБО (около 100%).

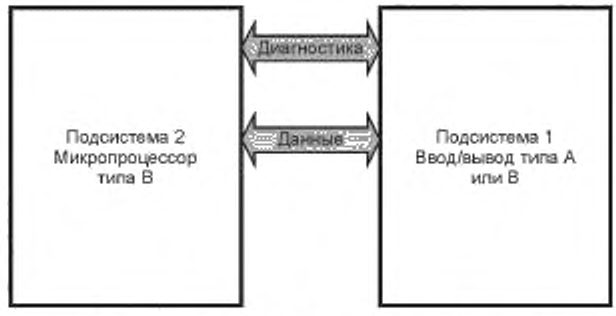


Рисунок 6 — Декомпозиция аппаратных средств

Однако объединение с диагностикой требует рассмотрения ряда вопросов. Поскольку подсистемы 1 и 2 соединены последовательно, обе должны иметь ДБО > 90%. Это означает, что диагностика подсистемы 1 должна составить ≥ 90%, если она содержит компоненты типа В ,и > 60%, если она содержит только компоненты типа А. Обеспечить требование типа А будет трудно, так как линии управления для диагностики приходят из подсистемы типа В. Поэтому интерфейс у этих двух подсистем должен иметь диагностический охват, равный 90%. Требовать конкретный диагностический охват необходимо в соответствии с приложением В МЭК 61508-2.

В соответствии с таблицей 5, чтобы модуль ввода-вывода достиг УПБ 3, требуется, по крайней мере, чтобы ДБО было равно 90%.

До использования подсистемой 1 процессора подсистемы 2 для диагностики, комбинация подсистем 1 и 2 не могла достигнуть значения ДБО более чем 90%. При использовании подсистемой 1 процессора подсистемы 2 для диагностики, комбинация подсистем 1 и 2 может теперь достигнуть значения ДБО более чем 90%, и следовательно модуль ввода/вывода может достигнуть УПБ 3.

9.4.3.2.2 Подсистема типа А

Подсистема может быть отнесена к типу А, если для ее компонентов, необходимых для части функции безопасности, реализуемой ПЛК-ФБ, одновременно выполняются следующие условия:

a) виды отказов всех составляющих компонентов точно определены;

b) поведение элемента в условиях сбоя может быть полностью определено;

c) имеются достаточные надежные данные об отказах из опыта эксплуатации, демонстрирующие, что предъявленные интенсивности отказов для обнаруженных и необнаруженных опасных отказов удовлетворяют требованиям (см. 9.4.8).

9.4.3.2.3 Подсистема типа В

Подсистема может быть отнесена к типу В, если для ее компонентов, необходимых для части функции безопасности, реализуемой ПЛК-ФБ, выполняется хотя бы одно из следующих условий:

a) вид отказа по крайней мере одного составляющего компонента не определен;

b) поведение подсистемы в условиях сбоев не может быть полностью определено;

c) имеются недостаточно надежные данные об отказах из опыта эксплуатации, чтобы поддержать требования по интенсивностям отказов для обнаруживаемых и необнаруживаемых опасных отказов (см. 9.4.8).

Примечания

1 Это означает, что если по крайней мере один из компонентов самой подсистемы соответствует условиям для подсистемы типа В, то такая подсистема должна быть отнесена к типу В, а не к типу А.

2 ПЛК-ФБ является сложной (тип В) подсистемой. В то же время ПЛК-ФБ может состоять из подсистем, которые имеют тип А или тип В.

9.4.3.2.4 Архитектурные ограничения подсистем типа А и типа В

Таблицы 4 и 5 определяют значение ДБО, которое требуется, чтобы выполнить спецификацию требования по УПБ 1, УПБ 2 или УПБ 3, на основе аппаратной отказоустойчивости. Архитектурные ограничения в таблице 4 или таблице 5 должны применять к каждой подсистеме, выполняющей часть функции безопасности, реализуемой ПЛК-ФБ, так, чтобы:

a) требования отказоустойчивости аппаратных средств были достигнуты для всей системы ПЛК-ФБ;

b) таблица 4 применялась для каждой подсистемы типа А, являющейся частью системы ПЛК-ФБ;

c) таблица 5 применялась для каждой подсистемы типа В, являющейся частью системы ПЛК-ФБ;

d) обе таблицы 4 и 5 применялись к системе ПЛК-ФБ, включающей подсистемы типа А и типа В, так как требования таблицы 4 должны применять для подсистем типа А, а требования таблицы 5 — для подсистем типа В.

9.4.3.2.5 Последовательное соединение подсистем

В системе ПЛК-ФБ, в которой некоторое число элементов функций безопасности реализуется с помощью последовательности элементов (как показано на рисунке 7), максимальный уровень полноты безопасности, на который может претендовать рассматриваемая функция безопасности, должен определяться элементом, который имеет самый низкий уровень полноты безопасности для достигнутой им доли безопасных отказов и отказоустойчивости аппаратных средств, равной 0. Чтобы проиллюстрировать этот метод, примем архитектуру, как показано на рисунке 5, и рассмотрим далее пример.

Пример — Пусть архитектура (рисунок 7), где некоторое число элементов функций безопасности реализуется подсистемами 1, 2 и 3, выполненными по одноканальной архитектуре, которые соответствуют требованиям таблиц 4 и 5 следующим образом:

- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 1;

- подсистемы 2 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 2;

- подсистемы 3 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 1.

Обе подсистемы 1 и 3 ограничивают максимальный уровень полноты безопасности, на который можно претендовать для соответствия отказоустойчивости аппаратных средств и доле безопасных отказов, до УПБ 1.



Рисунок 7 — Пример определения максимального значения УПБ для заданной архитектуры

9.4.3.2.6 Параллельное соединение подсистем

В системе ПЛК-ФБ, в которой функция безопасности реализована в многоканальной архитектуре (такой, как на рисунке 8), максимальный уровень полноты безопасности аппаратных средств, на который может претендовать рассматриваемая функция безопасности, должен быть определен:

a) группированием последовательно соединенных элементов для каждого канала и затем определением максимального уровня полноты безопасности, на который может претендовать рассматриваемая функция безопасности для каждого канала (см. 9.4.3.2.5);

b) выбором канала с самым высоким уровнем полноты безопасности, на который может претендовать рассматриваемая функция безопасности, и затем добавлением единицы к значению уровня полноты безопасности для определения максимального уровня полноты безопасности для всей комбинации подсистем;

c) по крайней мере, должны быть выполнены следующие требования:

- функция безопасности должна выполняться в каждой подсистеме,
- анализ отказов по общей причине должен выполняться согласно требуемому УПБ,
- средство голосования на выходе подсистем должно быть разработано согласно требуемому УПБ,
- реакция на отказ объединенной системы должна удовлетворять требованиям 7.4.8 МЭК 61508-2,
- значение охвата диагностикой ПЛК-ФБ соответствует требованиям УПБ объединенной системы,
- программное обеспечение/встроенное микропрограммное обеспечение, используемое в ПЛК-ФБ, должно соответствовать требованиям УПБ объединенной системы;

d) предположениями:

- систематический сбой этой подсистемы не вызовет отказ специфицированной функции безопасности, но сделает это только в сочетании со вторым систематическим сбоем другой подсистемы,
- существует достаточная независимость между этими двумя подсистемами (обоснованная анализом отказов по общей причине).

Пример — Группирование и анализ этих комбинаций может быть выполнено разными способами. Для иллюстрации одного из возможных способов принимают архитектуру, в которой конкретная функция безопасности ПЛК-ФБ реализована двумя подсистемами X и Y, где подсистема X состоит из подсистем 1, 2, 3 и 4, а подсистема Y — из одной подсистемы 5, как показано на рисунке 8. Использование параллельных каналов в подсистеме X гарантирует, что подсистемы 1 и 2 реализуют требуемую часть функции безопасности подсистемы X ПЛК-ФБ независимо от подсистем 3 и 4 и наоборот. Функцию безопасности считают выполненной:

- или при событии сбоя в подсистеме 1 или 2 (поскольку комбинация подсистем 3 и 4 позволяет реализовать требуемую часть функции безопасности ПЛК-ФБ);

- или при событии сбоя в подсистеме 3 или 4 (поскольку комбинация подсистем 1 и 2 позволяет реализовать требуемую часть функции безопасности ПЛК-ФБ).

Далее подробно рассматривается процедура определения максимального уровня полноты безопасности, на который может претендовать рассматриваемая функция безопасности.

В подсистеме X при заданной функции безопасности ПЛК-ФБ каждая подсистема соответствует требованиям таблиц 4 и 5 следующим образом:

- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 3;

- подсистемы 2 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 2;

- подсистемы 3 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 2;

- подсистемы 4 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 1.

Для того, чтобы получить максимальный уровень полноты безопасности аппаратных средств для рассматриваемой функции безопасности ПЛК-ФБ элементы подсистемы X объединяют следующим образом:

a) Объединение подсистем 1 и 2. Отказоустойчивость аппаратных средств и доля безопасных отказов, обеспеченная комбинацией подсистем 1 и 2 (каждая в отдельности соответствует требованиям для УПБ 3 и УПБ 2, соответственно), соответствует требованиям УПБ 2 (определенным подсистемой 2, см. 9.4.3.2.5).

b) Объединение подсистем 3 и 4. Отказоустойчивость аппаратных средств и доля безопасных отказов, обеспеченная комбинацией подсистем 3 и 4 (каждая в отдельности соответствует требованиям для УПБ 2 и УПБ 1, соответственно), соответствует требованиям УПБ 1 (определенным подсистемой 5, см. 9.4.3.2.5).

c) Дальнейшее объединение комбинации подсистем 1 и 2 с комбинацией подсистем 3 и 4. Максимальный уровень полноты безопасности аппаратных средств, на который может претендовать рассматриваемая функция безопасности ПЛК-ФБ, определяется выбором канала с самым высоким уровнем полноты безопасности, который был достигнут, и затем увеличением уровня полноты безопасности на единицу для определения максимального уровня полноты безопасности для всей комбинации подсистем. В данном случае подсистема включает в себя два параллельных канала с отказоустойчивостью аппаратных средств, равной 1. Каналом с самым высоким уровнем полноты безопасности для рассматриваемой функции безопасности ПЛК-ФБ является канал, включающий в себя подсистемы 1 и 2 и соответствующий требованиям для УПБ 2. Поэтому максимальный уровень полноты безопасности для подсистемы при отказоустойчивости аппаратных средств, равной 1, будет УПБ 2 + 1 = = УПБ 3 (см. 9.4.3.2.6).

В подсистеме Y для подсистемы 5 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равной 0, и доле безопасных отказов, равен УПБ 2.

Для полной системы ПЛК-ФБ (включающей в себя две подсистемы X и Y, которые достигли требований для рассматриваемой функции безопасности УПБ 3 и УПБ 2 соответственно), максимальный уровень полноты безопасности, на который может претендовать система ПЛК-ФБ, определен подсистемой с самым низким уровнем полноты безопасности, на который она претендует (9.4.3.1.2). Поэтому для настоящего примера максимальным уровнем полноты безопасности, на который может претендовать Э/Э/ПЭ система, связанная с безопасностью, для рассматриваемой функции безопасности ПЛК-ФБ является УПБ 2.

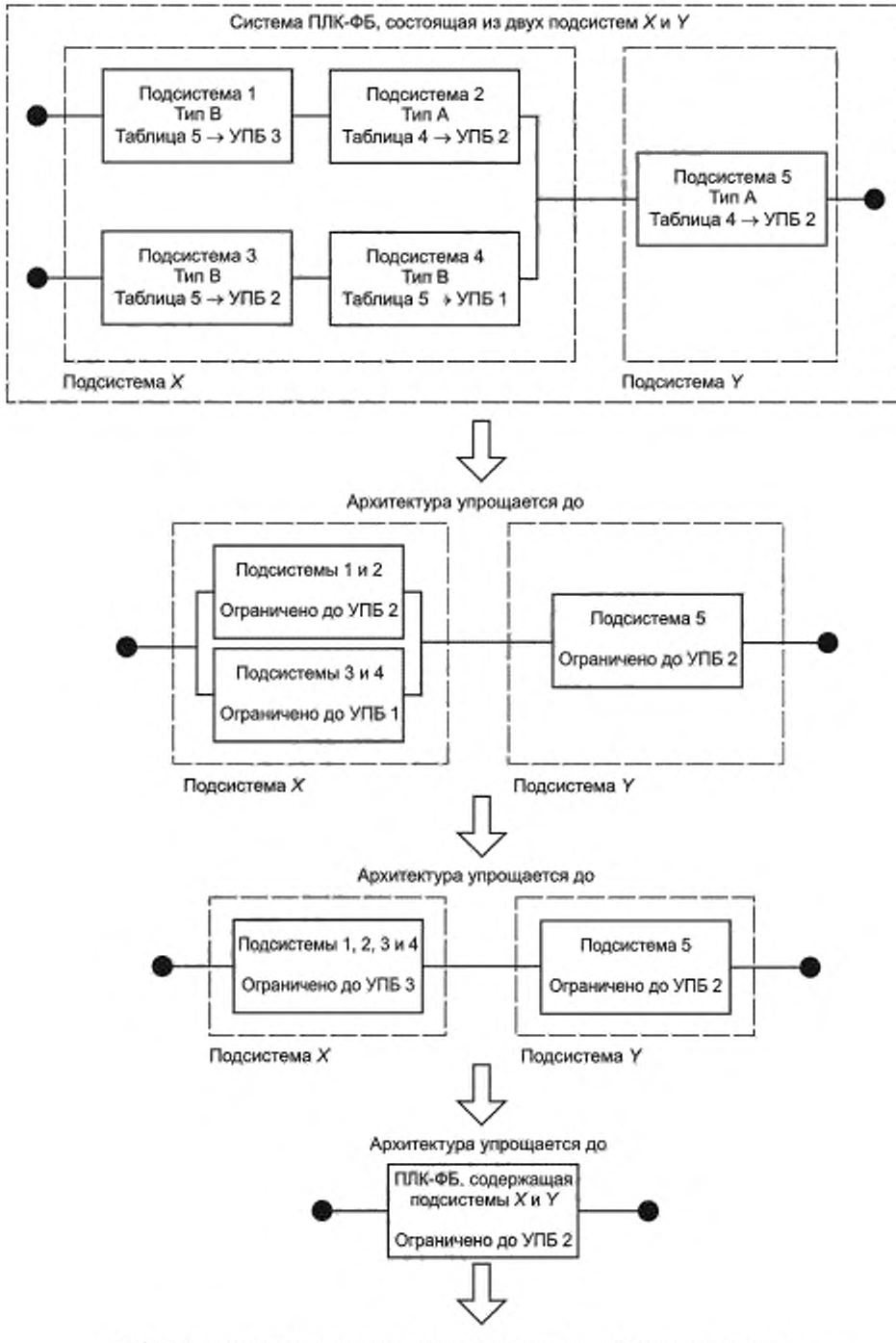


Рисунок 8 — Пример ограничения полноты безопасности аппаратных средств для многоканальной реализации функции безопасности

Примечания

1 Подсистемы 1 и 2 реализуют требуемую часть функции безопасности подсистемы *X* независимо от подсистем 3 и 4, и наоборот.

2 Подсистемы, выполняющие функцию безопасности ПЛК-ФБ, считают полной системой ПЛК-ФБ, включая все элементы — от входов до логического решателя и выходов.

3 Для получения дополнительной информации при интерпретации данного рисунка, см. пример, описанный выше.

4 Тип А могут иметь только подсистемы ПЛК-ФБ. Тип В могут иметь подсистемы ПЛК-ФБ или сам ПЛК-ФБ.

Рисунок 8 — Лист 2

9.4.4 Случайные отказы аппаратных средств

9.4.4.1 Общие положения

Вероятность опасного отказа из-за случайных отказов аппаратных средств должна быть равна или менее целевой меры отказов, определенной в спецификации требований к функциональной безопасности.

Случайные отказы аппаратных средств для проекта должны быть определены и проанализированы с помощью методов анализа видов и последствий отказов (FMEA), анализа дерева отказа или других приемлемых методов (см. приложение А). Интенсивности отказов для каждого компонента должны быть оценены с помощью общепризнанной базы данных надежности. Используя анализ охвата диагностикой, каждый отказ должен быть классифицирован в одну из следующих категорий:

- безопасный обнаруживаемый;
- безопасный не обнаруживаемый;
- опасный обнаруживаемый;
- опасный не обнаруживаемый;
- не влияющий.

Все вычисления надежности необходимо использовать один-единственный источник для данных надежности компонента. Данные из различных источников могут использоваться, только если можно показать, что данные были получены при близких условиях. Для получения дополнительной информации см. приложение D.

Как только определены интенсивности этих отказов, для ПЛК-ФБ должна быть сформирована модель надежности и должен быть выбран метод ее расчета. Это является предварительным условием для определения значения PFD или PFH подсистем и ПЛК-ФБ. В приложении В МЭК 61508-6 рассматривается вычисление PFD и PFH для различных архитектур ПЛК-ФБ; например 1oo1, 1oo2, 1oo2D (с диагностикой), 2oo2, и 2oo3, и т.д.

Для сложных систем, подобных ПЛК-ФБ, вычисление надежности рекомендуется выполнять на основе блок-схем надежности или модели Маркова.

Примечание — Если доступны подходящие данные, то отказы распределяются между преобладающими видами отказов: короткое замыкание, разрыв цепи, изменение значения и т.д.

9.4.4.2 Отказы по общей причине аппаратных средств

Если архитектура ПЛК-ФБ включает несколько каналов, например архитектуры 1oo2 или 2oo3, то необходимо рассмотреть отказы по общей причине.

Отказ по общей причине является результатом одного или более событий, которые вызывают совпадающий или почти совпадающий отказ двух или больше отдельных каналов в многоканальной системе, которые могут привести к потере функции безопасности. Отказы по общей причине могут происходить в результате систематических сбоев (например, из-за ошибки проектирования или спецификации) или внешних воздействий, приводящих к отказу аппаратных средств (например, аномально высокая температура).

Интенсивность отказов по общей причине должна оцениваться, используя общепризнанный метод. Как правило, такие методы применяют определенную часть интенсивности случайных отказов аппаратных средств для одного канала в качестве интенсивности отказов по общей причине для многоканальной системы. Значение этой части (β-фактор) определяется системой оценки, основанной на степени независимости каналов и возможности обнаружения неисправностей, прежде чем они повлияют на все каналы.

Пригодность метода, выбранного для оценки отказов по общей причине в проекте ПЛК-ФБ, должна быть обоснована.

Примечание — В приложении Е представлен один из возможных методов для оценки отказов по общей причине. Для получения дополнительной информации см. приложение D МЭК 61508-6.

9.4.4.3 Охват диагностикой (ОД) аппаратных средств

ОД системы ПЛК-ФБ можно определить следующим образом:

- создать модель надежности ПЛК-ФБ, используя подходящие подсистемы;
- для каждого компонента каждой подсистемы выполнить анализ видов и последствий отказов FMEA;
- классифицировать каждый вид отказа в соответствии с тем, приводит ли он к безопасному или опасному последствию, согласно определенному безопасному состоянию и предназначенным применениям ПЛК-ФБ, как заявлено производителем.

Примечание — Если для компонентов высокой сложности данные не доступны, можно предположить, что 50% случайных отказов аппаратных средств являются безопасными, и 50 % — опасными. Такое предположение также может быть применено к подсистемам, но обычно не используется;

- вычислить интенсивность отказов, для безопасных отказов λ_S и интенсивность отказов для опасных отказов λ_D для каждой подсистемы;
- оценить интенсивность отказов для тех опасных отказов, которые будут обнаружены диагностическими проверками λ_{DD} для каждой подсистемы;
- вычислить интенсивность отказов для тех опасных отказов, которые не будут обнаружены диагностическими проверками λ_{DU} для каждой подсистемы.

Примечание — $\lambda_D = \lambda_{DD} + \lambda_{DU}$;

- вычислить ОД (среднее значение ОД) и долю безопасных отказов (среднее значение ДБО) для каждой подсистемы:

$ОД = \Sigma \lambda_{DD} / \Sigma \lambda_D = \Sigma \lambda_{DD} / [\Sigma \lambda_{DU} + \Sigma \lambda_{DD}]$;

- если одна из этих интенсивностей отказов не будет иметь постоянного значения, то необходимо оценить ее среднее число за конкретный период времени и использовать для вычислений ОД и ДБО.

Для того чтобы претендовать на более высокий ОД, чем обычно позволяет серия МЭК 61508, для его вычисления можно использовать два или более различных методов. Эти различные методы должны быть независимыми и не иметь отказов по общей причине.

В таблице 6 перечислены сбои или отказы, которые, как минимум, должны быть обнаружены, чтобы достигнуть указанного ОД.

Для более полного рассмотрения методов и мер, которые, если они применимы, должны быть включены в ПЛК-ФБ для управления случайными отказами аппаратных средств, систематическими отказами, отказами из-за воздействия окружающей среды и отказами эксплуатации, см. приложение А МЭК 61508-2:2010, в котором также дается объяснение этих методов и мер.

Таблица 6 — Сбои и отказы, которые подлежат рассмотрению при количественной оценке случайных отказов аппаратных средств или учитываются при определении доли безопасных отказов

Компонент	См таблицу МЭК 61508-2, приложение А	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Электромеханические устройства	А.2	Невключение или неотключение Приваренные контакты	Невключение или неотключение Отдельные приваренные контакты	Невключение или неотключение Отдельные приваренные контакты Отсутствует принудительное управление контактами (для реле этот отказ не предполагается, если они изготовлены и испытаны в соответствии с ЕН 50205 или эквивалентными нормами)

Продолжение таблицы 6

Компонент	См. таблицу МЭК 61508-2, приложение А	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
				Отсутствует принудительное включение (для положений переключателей этот отказ не рассматривается, если они изготовлены и испытаны в соответствии с МЭК 60947-5-1 или эквивалентными нормами)
Дискретные аппаратные средства: - цифровой вход/выход - аналоговый вход/выход - источник питания	A.3, A.7, A.9	Константный отказ (см. примечание 2) Константный отказ (см. примечание 2) Константный отказ (см. примечание 2)	Неисправности при постоянном токе (см. примечание 3) Неисправности при постоянном токе (см. примечание 3) Отказы типа отклонений и колебаний при постоянном токе Неисправности при постоянном токе (см. примечание 3) Отказы типа отклонений и колебаний при постоянном токе	Неисправности при постоянном токе (см. примечание 3) Отказы типа отклонений и колебаний при постоянном токе Отказы типа отклонений и колебаний при постоянном токе Отказы типа отклонений и колебаний при постоянном токе Неисправности при постоянном токе (см. примечание 3) Отказы типа отклонений и колебаний при постоянном токе
Шина: - общая шина - диспетчер памяти - прямой доступ к памяти - управление доступом к шине (см. примечание 1)	A.3, A.7, A.8	Константный отказ адресов (см. примечание 2) Константный отказ данных или адресов (см. примечание 2) Нет доступа или непрерывный доступ Константный отказ сигналов управления доступом к шине (см. примечание 2)	Временная потеря работоспособности Неверное декодирование адреса Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти (см. примечания 4 и 5) Неисправности данных и адресов при постоянном токе (см. примечания 3) Изменение информа-ции, вызванное кратко-временными ошибками в регистрах памяти прямого доступа. Не-верное время доступа. Отсутствует или непрерывный доступ к шине	Временная потеря работоспособности Неверное декодирование адреса Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти (см. примечания 4 и 5) Все отказы, влияющие на данные в памяти Неверное время доступа Отсутствует или непрерывный, или неправильный доступ к шине

Продолжение таблицы 6

Компонент	См. таблицу МЭК 61508-2, приложение А	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Процессор: - регистр, внутреннее ОЗУ	А.4, А.10	Константный отказ данных или адресов (см. примечание 2)	Неисправности данных и адресов при постоянном токе (см. примечание 3) Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе (см. примечание 3). Перекрестные помехи в ячейках памяти. Изменение информации, вызванное исправимыми ошибками. Отсутствует, неверная или множественная адресация.
- устройство кодирования и выполнения, включая регистр признаков		Неверное кодирование или невыполнение	Неверное кодирование или неверное выполнение	Отсутствует определение предполагаемого отказа
- устройство вычисления адреса		Константный отказ (см. примечание 2)	Неисправности при постоянном токе (см. примечание 3). Изменение адресов, вызванное исправимыми ошибками	Отсутствует определение предполагаемого отказа
- счетчик команд, указатель стека		Константный отказ (см. примечание 2)	Неисправности при постоянном токе (см. примечание 3). Изменение адресов, выз-ванное исправимыми ошибками	Неисправности при постоянном токе (см. примечание 3). Изменение адресов, вызванное исправимыми ошибками
Устройство обработки прерываний: - устройство преры-вания	А.4	Отсутствуют или непрерывные прерывания (см. примечание 6)	Отсутствуют или непрерывные прерывания. (см. примечание 6). Пересечение прерываний	Отсутствуют или непрерывные прерывания (см. примечание 6). Пересечение прерываний
- схема возврата		Константный отказ. Отдельные компоненты не инициализируют состояние возврата	Неисправности при по-стоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата	Неисправности при постоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата
Постоянная память	А.5	Константный отказ данных или адресов (см. примечание 2)	Неисправности данных и адресов при постоян-ном токе (см. примечание 3)	Все отказы, влияющие на данные в памяти

Окончание таблицы 6

Компонент	См. таблицу МЭК 61508-2, приложение А	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Память с произвольным доступом	А.6	Константный отказ данных или адресов (см. примечание 2)	Неисправности данных и адресов при постоянном токе (см. примечание 3) Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе (см. примечание 3) Перекрестные помехи в ячейках памяти Изменение информации, вызванное исправимыми ошибками Отсутствует, неверная или множественная адресация
Устройство синхронизации (кварцевое)	А.11	Нижняя или верхняя гармоника. Неустойчивость периода синхронизации	Неверная частота. Неустойчивость периода синхронизации	Неверная частота. Неустойчивость периода синхронизации
Устройство связи и запоминающее устройство большой емкости	А.12	Неверные данные или адреса Отсутствует передача данных	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверна последовательность передачи	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверная последовательность передачи

Примечания

1 Управление доступом к шине — это механизм, который определяет, какое из устройств может управлять шиной.

2 «Константный» — это вид отказа, который может быть описан постоянными «0» или «1» либо «включено» на выводах компонента.

3 «Неисправности при постоянном токе» включают в себя следующие виды отказов: константные отказы, открытые константные выходы, открытые выходы или выходы с высоким сопротивлением, а также короткие замыкания между линиями связи. Для интегральных схем — это короткое замыкание между любыми двумя соединениями (выводами).

4 Интенсивность исправимых ошибок SER для полупроводниковых приборов с низким напряжением питания, как известно, более чем на порядок (50—500 раз), превышает интенсивность устойчивых неисправностей (постоянное повреждение устройства). См. МЭК 61508-7.

5 Причинами исправимых ошибок являются: альфа-частицы, образовавшиеся в результате процесса распада, нейтроны, внешний источник электромагнитного излучения и внутренние перекрестные помехи. Результаты исправимых ошибок могут быть обработаны только функционирующими средствами обеспечения полноты безопасности. Но такие средства обеспечения полноты безопасности эффективны для случайных отказов аппаратных средств и могут оказаться неэффективными для исправимых ошибок.

Пример — Для ОЗУ такие тесты, как «блуждающая траектория», GALPAT и т.д., не эффективны, тогда как методы, использующие контроль четности и коды с исправлением ошибок, возвращающие содержимое ячеек памяти, или методы, использующие избыточность (и сравнение или голосование), могут быть эффективны.

6 Отсутствие прерываний означает, что прерывания не выполняются, если они должны происходить. Непрерывные прерывания означают, что выполняются непрерывные прерывания, если они не должны происходить.

7 Для ASIC настоящая таблица и таблицы А.2 — А.18 МЭК 61508-2 применяют в соответствующих случаях.

9.4.4.4 Доля безопасных отказов (ДБО) аппаратных средств

Для сложных подсистем или элементов деление отказов на 50% безопасных и 50% опасных является общепринятым, например для подсистем или элементов без диагностики.

Компоненты, которые «не влияют», не должны учитывать при вычислениях, например, светодиоды, конденсаторы многоступенчатого фильтра.

В таблице 6 перечислены сбои или отказы, которые будут обнаружены во время эксплуатации или проанализированы, чтобы получить долю безопасных отказов.

9.4.4.5 Вычисления предельного значения УПБ

Для того чтобы заявить конкретное предельное значение УПБ для ПЛК-ФБ, необходимы соответствующие как качественные методы и меры, определенные в приложении В МЭК 61508-2, так и количественные значения, вычисляемые с помощью уравнений приложения В МЭК 61508-6.

Включение этих конкретных методов и мер в течение жизненного цикла ПЛК-ФБ позволяют решать вопросы, связанные с систематическими отказами. Выполнение вычислений в соответствии с приложением В МЭК 61508-6 позволяют решать вопросы, связанные со случайными отказами аппаратных средств.

Ниже рассмотрены количественные вычисления предельного значения УПБ для ПЛК-ФБ. Эта последовательность действий, выполняемая производителем ПЛК-ФБ, упрощает процесс вычисления УПБ:

a) определить значение УПБ, специфицированное для предназначенной(ых) области(ей) применения — «целевой УПБ»;

b) определить требуется ли для предназначенной(ых) области(ей) применения функция безопасности, действующая в режиме низкой частоты запросов, или функция безопасности, действующая в режиме высокой частоты запросов или с непрерывными запросами, или они требуются обе, так как для режима низкой частоты запросов необходимо вычислять PFD, а для режима высокой частоты запросов или режима с непрерывными запросами — PFH;

c) специфицировать архитектуру ПЛК-ФБ;

d) установить тот процент PFD или PFH, связанный с УПБ системы, который будет определен для ПЛК-ФБ (см. 6.3);

e) установить значения среднего времени восстановления MTTR и средней продолжительности ремонта MRT для ПЛК-ФБ в случае отказа;

f) рекомендовать один или несколько интервалов контрольных проверок T_1 для ПЛК-ФБ;

g) определить интенсивность опасных отказов для ПЛК-ФБ (для обнаруживаемых λ_{DD} и необнаруживаемых λ_{DU} отказов) на основе интенсивностей отказов компонентов аппаратных средств (см. 9.4.4.3) и соответствующих вычислений (см. приложение В МЭК 61508-6);

h) вычислить проценты отказов по общей причине, которые обнаружены β_D и не обнаружены β, (см. приложение Е, а также приложение D МЭК 61508-6);

i) использовать вышеупомянутые параметры, чтобы вычислить PFD и/или PFH согласно приложению В МЭК 61508-6;

j) проверить, что расчетное(ые) значение(я) не выходит(ят) за пределы соответствующих диапазонов таблиц В.2, В.3, В.4, В.5, В.10, В11, В.12 и В.13 МЭК 61508-6.

9.4.5 Требования по предотвращению систематических отказов аппаратных средств

Должны использовать методы и меры, чтобы избежать систематических отказов во время разработки аппаратных средств, описанные в приложении В МЭК 61508-2.

9.4.6 Требования по управлению систематическими сбоями аппаратных средств

9.4.6.1 Общие положения

Систематические сбои — это такие сбои, которые связаны с причиной, которая может быть устранена только модификацией проекта или производственного процесса, эксплуатационных процедур, документации или других соответствующих факторов.

9.4.6.2 Управление систематическими сбоями

Для управления систематическими сбоями проектирование ПЛК-ФБ должно обладать особенностями проектирования, которые делают системы ПЛК-ФБ, связанные с безопасностью, устойчивыми:

- к любым остаточным сбоям проектирования аппаратных средств, если вероятность ошибок проектирования аппаратных средств не может быть исключена (см. таблицу А.15 МЭК 61508-2);
- внешним влияниям, включая электромагнитные воздействия (см. таблицу А.16 МЭК 61508-2);
- ошибкам оператора управляемого оборудования (см. таблицу А.17 МЭК 61508-2);
- любым остаточным сбоям в программном обеспечении;
- любым ошибкам, возникающим в результате выполнения любого процесса передачи данных (см. 8.3).

9.4.6.3 Пригодность для обслуживания и тестируемость

Пригодность для обслуживания и тестируемость необходимо рассмотреть при выполнении действий по проектированию и разработке, чтобы упростить реализацию этих процедур для окончательных, связанных с безопасностью, систем, включающих ПЛК-ФБ.

9.4.6.4 Интерфейсы с человеком

Проект ПЛК-ФБ должен учитывать способности и ограничения человека при формировании действий, которые должны выполнять операторы и обслуживающий персонал. Проект всех интерфейсов

должен принимать во внимание современную практику учета человеческого фактора и определить вероятный уровень подготовки или осведомленности операторов, например в областях массового производства, где оператор имеет ограниченный опыт.

Примечание — Цель проекта состоит в том, что предсказуемые критические ошибки, сделанные операторами или обслуживающим персоналом, были предотвращены или устранены по мере возможности в проекте либо должно существовать повторное подтверждение действия перед его завершением.

9.4.7 Классификация сбоев аппаратных средств

Сбои приводят к отказам. Цель состоит в том, чтобы обнаружить сбои и предупредить о них, прежде чем сбои могли бы привести к отказу с опасным последствием. Ключевая концепция заключается в обнаружении неисправности, прежде чем произойдут многократные сбои, поскольку сценарии многократных сбоев не всегда возможно проанализировать.

Если явно не определено, сценарии многократных сбоев не рассматривают при анализе сбоя, например при анализе дерева отказов FTA, анализе видов и последствий отказов FMEA.

В общем случае существует пять различных типов отказов, которые необходимо рассмотреть при анализе ПЛК-ФБ. Классификация этих пяти отказов зависит от функции безопасности ПЛК-ФБ и его архитектуры.

Первый тип сбоя (не влияющий сбой) никак не влияет на функцию безопасности ПЛК-ФБ (например, световой индикатор). Такие сбои не учитываются при вычислении PFD, PFH и других характеристик и не вносят вклад в ДБО.

Если отказ не влияет на функцию безопасности ПЛК-ФБ, он классифицируется как «не влияющий отказ». «Не влияющий отказ» не учитывается при вычислении ДБО.

Оставшиеся четыре типа отказов учитываются при рассмотрении функции безопасности ПЛК-ФБ. Они должны быть включены в вычисление PFD, PFH и т.д.

Цель рисунка 9 состоит в том, чтобы помочь или указать разработчику ПЛК-ФБ, как необходимо классифицировать сбои при анализе отказов, например, применяя FMEA, FTA.

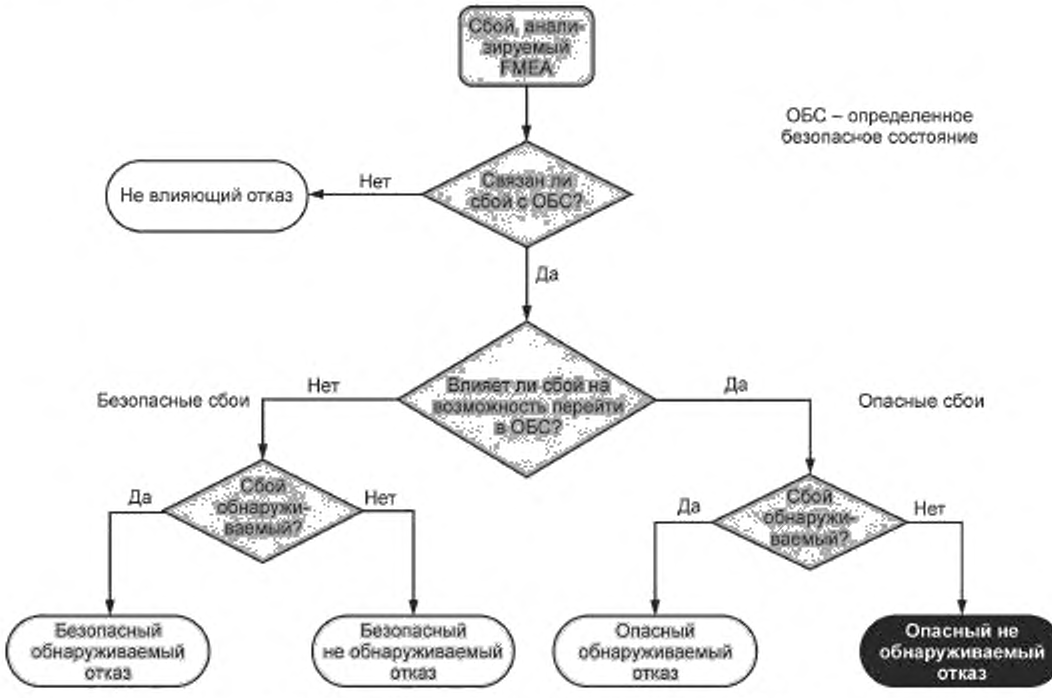


Рисунок 9 — Классификация сбоев и поведение ПЛК-ФБ

Предполагается, что для обнаружения и формирования реакции на опасный(ые) и/или безопасный(ые) сбой(и) существуют диагностические средства.

Если отказ непреднамеренно выполняет функцию безопасности ПЛК-ФБ, то такой отказ считается безопасным, не обнаруживаемым отказом. С другой стороны, если отказ выполняет функцию безопасности ПЛК-ФБ преднамеренно, но обнаруживается диагностическими мерами, то предполагается, что диагностика приводит к соответствующей реакции системы в соответствии с требованиями 7.4.8 МЭК 61508-2 или что отказ будет восстановлен (безопасный обнаруживаемый отказ). В случае режима с высокой частотой запросов диагностируемый отказ должен автоматически привести к выполнению функции безопасности ПЛК-ФБ или к безопасному состоянию. В случае режима с низкой частотой запросов достаточно уведомление оператору, чтобы запустить восстановление системы.

Если система неумышленно не выполняет функцию безопасности ПЛК-ФБ или не достигает безопасного состояния, отказ классифицируется как опасный не обнаруживаемый отказ. Опасный отказ также может быть диагностирован (опасный обнаруживаемый отказ). В зависимости от режима работы о конкретных действиях в случае отказа см. 9.4.3.1.3.

9.4.8 Реализация аппаратных средств

ПЛК-ФБ должен быть реализован в соответствии с проектом аппаратных средств ПЛК-ФБ.

В процессе проектирования и разработки производителем ПЛК-ФБ должно быть собрано и доступно для оценки следующее:

a) спецификация функций и интерфейсов, которые могут использоваться функциями безопасности, например ограничения применения, коммуникационные ограничения;

b) оценки интенсивностей случайных отказов аппаратных средств, которые могут вызвать опасный отказ системы, но обнаружены диагностическими тестами, см. 9.4.4;

c) оценки интенсивностей случайных отказа аппаратных средств, которые могут вызвать опасный отказ системы, но не обнаружены диагностическими тестами, см. 9.4.4;

d) ограничения внешней среды, чтобы поддержать легитимность интенсивности отказов;

e) механические условия окружающей среды и климатические условия (например, вибрация, ударное воздействие, температура, влажность), предусмотренные для ПЛК-ФБ;

f) объявленный производителем максимальный полезный срок службы ПЛК-ФБ, который должен составить 20 лет или меньше, если производитель ПЛК-ФБ не сможет обосновать более продолжительный срок службы, представляя свидетельства, на основе вычислений, показывающих, что данные по надежности обосновывают более продолжительный срок службы.

Примечание — Некоторые отдельные компоненты в ПЛК-ФБ имеют известный срок службы, который менее чем 20 лет. Например, батареи, электролитические конденсаторы, светодиоды и т.д. По мере необходимости, периодическая замена этих компонентов рассматривается как часть обычных процедур технического обслуживания, определенных производителем ПЛК-ФБ. Максимальный полезный предел срока службы, равный 20 годам, предназначен, чтобы охватить большую часть компонентов ПЛК-ФБ, для которых не известен срок службы;

g) метод периодической контрольной проверки и интервал контрольной проверки (с обоснованием) и/или требования по техническому обслуживанию;

h) охват диагностикой, внутренней для ПЛК-ФБ;

i) интервал диагностических проверок, внутренний для ПЛК-ФБ;

j) среднее время восстановления MTTR и средняя продолжительность ремонта MRT, если применимо;

k) доля безопасных отказов SFF;

l) отказоустойчивость аппаратных средств;

m) рекомендуемые ограничения применения для предотвращения систематических отказов;

n) снижение номинальных характеристик, применяемое к используемым компонентам (см. 9.4.9);

o) значения УПБ, на которые может претендовать связанные с безопасностью системы, для которых подойдет использование ПЛК-ФБ;

p) версия аппаратных средств ПЛК-ФБ;

q) документально оформленное доказательство, что для ПЛК-ФБ было выполнено подтверждение соответствия (см. 9.7).

9.4.9 Снижение номинальных характеристик компонент

Предполагается, что производитель демонстрирует хорошую инженерно-техническую практику и принципы снижения номинальных характеристик, включая снижение номинальных характеристик для компонентов.

Номинальные рабочие характеристики компонентов должны быть меньше, чем указанные производителем их максимальные значения при наихудших случаях условий эксплуатации: напряжении,

токе, температуре, параметров синхронизации и т. д. В тех случаях, где это невыполнимо, требуется проверка пригодности выбранного (или только доступного) компонента для предполагаемого(ых) применения(й). Компонент считается неподходящим, пока не квалифицирована его пригодность.

9.4.10 Проектирование и разработка специализированной интегральной схемы (СИС)

На рисунке 10 представлена подробная V-модель жизненного цикла разработки СИС. Если будет использоваться другой жизненный цикл разработки СИС, то он должен быть определен как часть действий по управлению функциональной безопасностью (см. 5.4).

9.4.11 Методы и меры, предотвращающие введение сбоев в СИС

Необходимо использовать соответствующую группу методов и средств, которые важны в процессе проектирования и разработки СИС для предотвращения появления неисправностей. В зависимости от технической реализации необходимо разделение между полностью и не полностью специализированными цифровыми СИС и ИС и программируемыми пользователем (FPGA/PLD/CPLD). Подходящие методы и средства, которые поддерживают обеспечение получения соответствующих свойств, определены в МЭК 61508-2.

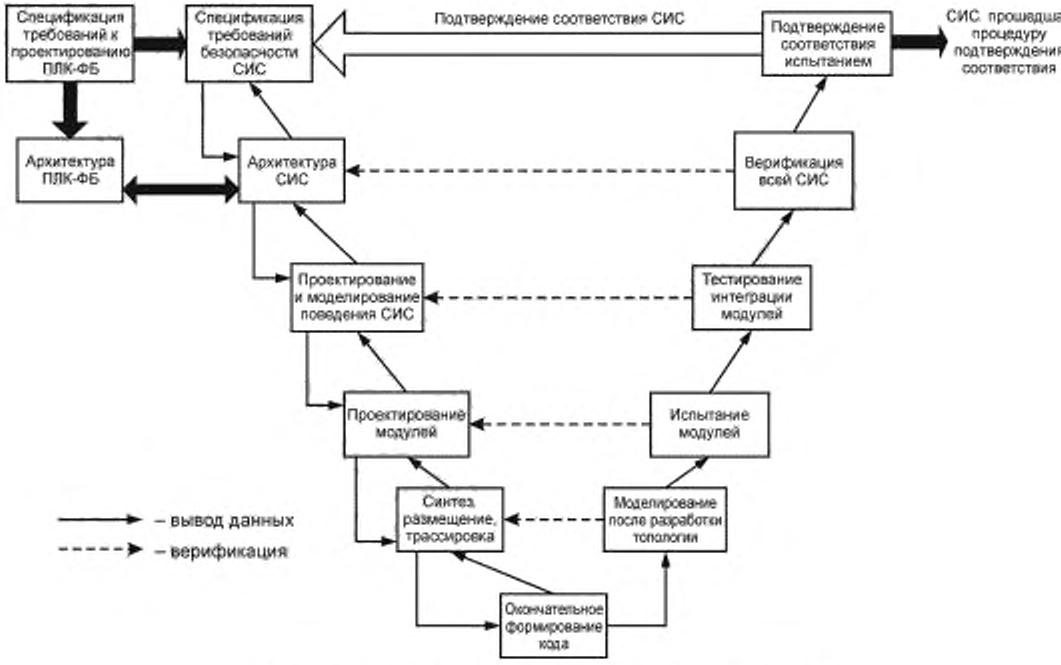


Рисунок 10 — Жизненный цикл разработки СИС (V-модель)

9.5 Аппаратные средства, встроенное программное обеспечение. Их интеграция в ПЛК-ФБ

Стадия интеграции жизненного цикла ПЛК-ФБ состоит, прежде всего, из функционального испытания, и тестирования методом «черного ящика» или статистическим методом. Эти испытания должны показать, что все модули и их части взаимодействуют правильно и выполняют предназначенные для них функции.

При испытаниях интеграции ПЛК-ФБ должна быть документально оформлена следующая информация:

- используемая версия спецификации испытаний;
- критерии принятия испытаний интеграции;
- версия испытуемого ПЛК-ФБ;
- используемые средства испытаний и оборудование с датой поверки;
- результаты каждого испытания;
- любое несоответствие между ожидаемыми и фактическими результатами;
- проведенный анализ и принятое решение о продолжении испытаний или выпуске запроса на изменение (при наличии несоответствия).

Результаты проектирования и разработки программируемых аппаратных средств интегрируются со встроенным программным обеспечением (см. блок 19 рисунка 3), если выполняются требования к функции безопасности и УПБ их ПЛК-ФБ.

После того как интегрированы программируемые аппаратные средства и программное обеспечение, интегрируются результаты проектирования и разработки инструментальных средств и непрограммируемых аппаратных средств (см. блок 20 рисунка 3). Во время этой интеграции должны быть выполнены требования к функции безопасности и УПБ ПЛК-ФБ

Указанная последовательность интеграции программируемых аппаратных средств перед непрограммируемыми аппаратными средствами не является требованием. Последовательность должна быть определена в спецификации испытания.

9.6 Процедуры эксплуатации и технического обслуживания аппаратных средств

9.6.1 Цель

Целью требований настоящего подраздела для производителя ПЛК-ФБ является разработка процедур, гарантирующих требуемую функциональную безопасность ПЛК-ФБ во время эксплуатации и технического обслуживания.

9.6.2 Требования

Для эксплуатации и технического обслуживания ПЛК-ФБ должны быть предусмотрены процедуры, специфицирующие следующее:

a) обычные действия, которые должны быть выполнены для поддержания «спроектированной» функциональной безопасности ПЛК-ФБ, включая обычную замену компонентов с предварительно заданными сроками жизни, например вентиляторов, батарей и т.п.:

- обновление и замена встроенного программного обеспечения,
- полная или частичная замена прикладного программного обеспечения,
- обновления и замена аппаратных средств;

b) действия и ограничения, необходимые (например, во время установки, запуска, обычного режима эксплуатации, типовых испытаний, прогнозируемых нарушений в работе, сбоев или отказов, отключений) для предотвращения опасных событий и/или уменьшения последствий опасных состояний;

c) процедуры и документация, если в ПЛК-ФБ происходят сбои или отказы, включая следующее:

- процедуры для обнаружения и восстановления сбоев,
- режим работы при отказе,
- светодиодная/диагностическая индикация,
- регистры состояния/диагностики,
- процедуры для создания отчетов об отказах,
- процедуры для анализа отказов,
- процедуры для повторного подтверждения соответствия;

d) процедуры и документация для технического обслуживания ПЛК-ФБ должны быть специфицированы в требованиях к предоставлению информации о техническом обслуживании;

e) инструментальные средства, необходимые для анализа отказов, технического обслуживания и повторного подтверждения соответствия, а также процедуры для поддержания инструментальных средств и оборудования.

Примечание — В процедуры эксплуатации и технического обслуживания ПЛК-ФБ должны быть включены процедуры модификации программного обеспечения (см. раздел 15).

Производитель, по мере необходимости, должен совершенствовать процедуры эксплуатации и технического обслуживания ПЛК-ФБ на основе вводов, полученных по результатам (1) аудитов функциональной безопасности, выполняемых пользователями ПЛК-ФБ, (2) испытаний ПЛК-ФБ и (3) отчетов с места работы.

Обычные действия по техническому обслуживанию, необходимые для поддержания требуемой (в соответствии с проектом) функциональной безопасности ПЛК-ФБ, должны быть заданы на основе систематического подхода, например с помощью:

- экспертизы деревьев отказов;
- анализа видов и последствий отказов.

Примечания

1 Рассмотрение человеческого фактора является ключевым моментом в определении требуемых действий и соответствующих интерфейсов с ПЛК-ФБ.

2 Частота проведения контрольных проверок должна быть такой, чтобы была достигнута целевая мера отказов.

3 Частота контрольных проверок, интервал диагностических проверок и время последующего ремонта зависят от нескольких факторов (см. приложение В МЭК 61508-6), включая:

- целевую меру отказов, связанную с уровнем полноты безопасности;
- архитектуру;
- охват диагностикой диагностических испытаний и
- ожидаемую частоту запросов.

4 Частота контрольных проверок и интервал диагностических проверок, вероятно, должны иметь решающее влияние на достижение полноты безопасности аппаратных средств. Одна из основных причин проведения анализа надежности аппаратных средств (см. 9.4.3.2.2) состоит в гарантии соответствия частоты проведения этих двух типов испытаний целевой полноте безопасности аппаратных средств.

Процедуры эксплуатации и технической поддержки ПЛК-ФБ должны быть оценены на возможность воздействия, которое они могут оказать на управляемое оборудование.

Для предотвращения сбоев и отказов во время процедур эксплуатации и технического обслуживания ПЛК-ФБ необходимо использовать группу средств и методов в соответствии с таблицей В.4 МЭК 61508-2.

9.7 Подтверждение соответствия безопасности аппаратных средств

9.7.1 Общие положения

Результат стадии подтверждения соответствия должен включать: конкретные ссылки на план подтверждения соответствия (9.3); конкретные требования к ПЛК-ФБ, испытательному оборудованию, используемому во время подтверждения соответствия; даты проверки испытательного оборудования и результаты каждого теста.

Данная стадия жизненного цикла фактически выполняется в течение нескольких других стадий жизненного цикла. Например, во время проектирования и разработки должны быть протестированы выходы, чтобы гарантировать их правильность и непротиворечивость со входами, и должно быть продемонстрировано, что конкретные сбои и отказы, рассмотренные в 9.4.4.3, обнаруживаются.

Цель требований настоящей стадии состоит в подтверждении соответствия, что ПЛК-ФБ удовлетворяет, во всех отношениях, требованиям функциональной безопасности с точки зрения требуемых функций безопасности и полноты безопасности (см. 9.1).

9.7.2 Требования

Подтверждение соответствия ПЛК-ФБ должно проводиться в соответствии с подготовленным планом подтверждения соответствия безопасности (см. 9.3).

Примечание — Подтверждение соответствия программируемой электроники ПЛК-ФБ системы, связанной с безопасностью, включает в себя подтверждение соответствия аппаратных средств и программного обеспечения. Требования к подтверждению соответствия программного обеспечения содержатся в разделе 10.

Испытательное оборудование, используемое для подтверждения соответствия, должно быть откалибровано в соответствии с нормативным документом, по возможности с национальным стандартом, или с общепризнанной процедурой. Все испытательное оборудование должно быть проверено на корректность функционирования.

Для адекватной реализации каждой функции безопасности, определенной в требованиях к ПЛК-ФБ (см. раздел 6), и всех процедур эксплуатации и технического обслуживания ПЛК-ФБ должно быть выполнено подтверждение соответствия испытанием и/или анализом.

Должна быть подготовлена необходимая документация по проведению испытаний на подтверждение соответствия безопасности ПЛК-ФБ, в которой для каждой функции безопасности должны быть указаны:

a) версия используемого плана проведения подтверждения соответствия безопасности ПЛК-ФБ;

b) функция безопасности, подвергаемая испытаниям (или анализу), вместе с конкретной ссылкой на указанные в документации требования к планированию проведения подтверждения соответствия безопасности ПЛК-ФБ;

c) испытательные средства и оборудование с датой поверки;

d) результаты каждого испытания;

e) несоответствие между ожидаемыми и фактическими результатами.

Примечание — Для каждой функции безопасности отдельная документация не требуется, но каждая функция безопасности и каждое отклонение от функции безопасности должны быть отражены в информации, соответствующей перечислениям a) — e). Если для различных функций безопасности информация отличается, то эти различия устанавливаются.

Если фактические результаты отличаются от ожидаемых результатов более, чем это установлено допусками, результаты испытаний на подтверждение соответствия безопасности ПЛК-ФБ должны быть документально оформлены, включая:

1) описание проведенного анализа и

2) принятое решение о продолжении испытаний либо о выпуске извещения об изменении и возвращении к более раннему этапу испытаний на подтверждение соответствия.

Производитель ПЛК-ФБ должен предоставить результаты испытаний подтверждения соответствия безопасности ПЛК-ФБ только, в случае необходимости, разработчику управляемого оборудования или Э/Э/ПЭ системы, связанной с безопасностью, с тем, чтобы позволить им обеспечить выполнение требований подтверждения соответствия всей системы безопасности в соответствии с МЭК 61508-1.

Для предотвращения сбоев при проведении подтверждения соответствия безопасности ПЛК-ФБ необходимо использовать группу методов и средств в соответствии с МЭК 61508-2.

9.8 Верификация аппаратных средств

9.8.1 Цель

Целью требований настоящего подраздела является подтверждение того, что требуемые действия каждой стадии выполняют и результаты регистрируют.

Примечание — Для удобства все действия по верификации аппаратных средств были объединены в подразделе 9.8, но фактически они выполняются на нескольких стадиях.

9.8.2 Требования

Должна быть запланирована, выполнена и документально оформлена верификация конечного результата каждой стадии жизненного цикла, связанной с аппаратными средствами ПЛК-ФБ. Эти проверки должны основываться на заданных входных значениях для стадии жизненного цикла. Методы/инструменты, используемые для верификации, включают, например:

- документально оформленный анализ стадии,
- экспертизы проекта,
- функциональные испытания и
- испытания на воздействие окружающей среды.

Примечание — Верификацию не следует путать с калибровкой или подтверждением соответствия.

10 Проектирование и разработка программного обеспечения ПЛК-ФБ

10.1 Общие положения

Требования настоящего раздела получены из конкретных требований к программному обеспечению, содержащихся в спецификации требований функциональной безопасности ПЛК-ФБ.

Требования настоящего раздела применяют к встроенным в ПЛК-ФБ программному обеспечению и инструментальным средствам, а также к инструментальным программным средствам разработки приложений, но не применяют к прикладному программному обеспечению пользователя.

На рисунке 11 представлена базовая эталонная модель программного обеспечения, используемая в настоящем стандарте. Данная эталонная модель является одним из примеров реализации программного обеспечения, удовлетворяющего требованиям функциональной безопасности, но другие архитектуры также возможны.

Инструментальные средства обычно включают генератор кода приложений функциональной безопасности и человеко-машинный интерфейс для редактирования исходного кода приложений функциональной безопасности и контроля состояния ПЛК-ФБ. Должен быть выполнен анализ соответствующего влияния инструментальных средств на безопасность.

Встроенное в ПЛК-ФБ программное обеспечение получает код приложения функциональной безопасности на уровне передачи кода приложения функциональной безопасности и запоминает его на уровне хранилища приложений функциональной безопасности.

Уровень выполнения кода приложения функциональной безопасности загружает код приложения функциональной безопасности из хранилища приложений функциональной безопасности и выполняет его.

Требования к программному обеспечению ПЛК-ФБ, полученные из конкретных требований к программному обеспечению, содержащихся в спецификации требований функциональной безопасности

ПЛК-ФБ, в большинстве случаев будут достигаться совместной работой встроенного программного обеспечения и инструментальных средств. Именно от комбинации этих компонентов зависит обеспечение характеристик, удовлетворяющих требованиям следующих подразделов. Строгое разделение между встроенным программным обеспечением и инструментальными средствами зависит от выбранной архитектуры системы.

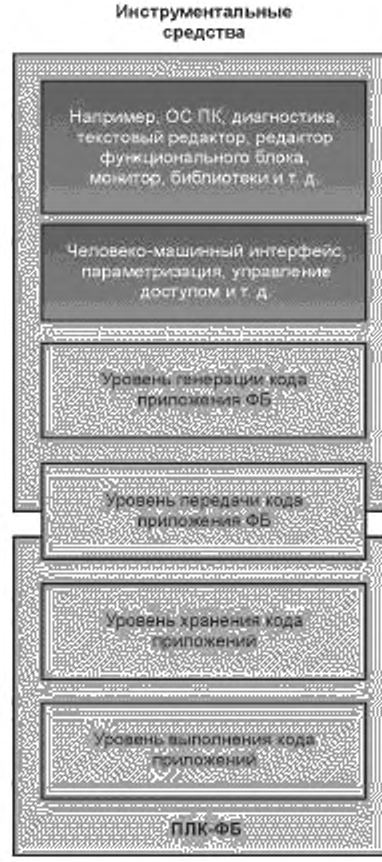


Рисунок 11 — Модель ПЛК-ФБ и уровни инструментальных средств

10.2 Требования

Все требования МЭК 61508-3 применяют к программному обеспечению ПЛК-ФБ и неавтономным средствам поддержки. Именно эти инструментальные программные средства могут непосредственно влиять на связанную с безопасностью систему в течение времени их работы.

10.3 Классификация инструментальных средств

Инструментальные средства ПЛК-ФБ необходимо разделить на следующие классы:

- Класс Т1. Не генерируют те программы, которые явно или неявно включаются в рабочую программу (включая данные) системы, связанной с безопасностью.

- Класс Т2. Включают в себя средства испытания или верификации проекта либо рабочей программы, причем такие, ошибки в которых могут привести к сбою при обнаружении ошибок в рабочей программе, но эти средства не могут создавать ошибки в самой рабочей программе.

- Класс Т3. Генерируют программы, которые явно или неявно включены в рабочую программу системы, связанной с безопасностью.

Примечания

1 Примерами класса Т1 являются: текстовый редактор, или требования, или средства поддержки разработки без автоматической генерации кода; средства управления конфигурацией.

2 Примерами класса Т2 являются: генератор тестовых программ, средства измерения тестового охвата, средства статического анализа.

3 Примерами класса Т3 являются: оптимизирующий компилятор, в котором связь между исходным кодом программы и сгенерированным объектным кодом не очевидна; компилятор, который включает исполнимый пакет программ в рабочую программу.

4 Данная классификация основана на МЭК 61508-4, п. 3.2.11.

В таблице 7 даны примеры разделения инструментальных средств ПЛК-ФБ на классы. Строгое разделение между встроенным программным обеспечением и инструментальными средствами зависит от выбранной архитектуры системы.

Таблица 7 — Примеры классификации инструментальных средств

Класс инструментальных средств[a)]	Класс	Объяснение
Инструментальные средства — ОС ПК, диагностика, текстовый редактор, редактор функционального блока, монитор, библиотеки и т.д.	Т1	Результаты работы инструментальных средств верифицируются, и выполняется подтверждение соответствия пользователем до использования в ПЛК-ФБ
Инструментальные средства — человеко-машинный интерфейс, параметризация, управление доступом и т.д.	Т1	Не генерирует те программы, которые могут явно или неявно включаться в рабочую программу (включая данные) системы, связанной с безопасностью
Инструментальные средства — уровень генерации кода приложения ФБ, человеко-машинный интерфейс, параметризация	Т3	Генерирует программы, которые могут явно или неявно включаться в рабочую программу ПЛК-ФБ
Инструментальные средства — уровень передачи кода приложения ФБ	Т3	Могут явно или неявно включаться в рабочую программу системы, связанной с безопасностью
ПЛК-ФБ — уровень хранения кода приложений	Не применяется	Встроенное микропрограммное обеспечение
ПЛК-ФБ — уровень выполнения кода приложений	Не применяется	Встроенное микропрограммное обеспечение
[a)] У инструментальных средств могут быть различные классификации в зависимости от их результатов работы или возможностей генерации кода.		

Как только такая классификация сформировалась, необходимо использовать применимые требования МЭК 61508-3.

10.4 Планирование подтверждения соответствия программного обеспечения

Примечания

1 Данную стадию жизненного цикла ПЛК-ФБ обычно выполняют параллельно с проектированием и разработкой требований программного обеспечения (см. 10.2).

2 См. 7.3.2.2 из МЭК 61508-3.

Планирование подтверждения соответствия программного обеспечения заключается в определении шагов, которые должны быть выполнены для демонстрации соответствия программного обеспечения ПЛК-ФБ спецификации требований функциональной безопасности (см. раздел 6).

План подтверждения соответствия функциональной безопасности должен включать процедуры, которые необходимо выполнить, описание среды испытаний и критерии «прошел»/«не прошел» компонент.

11 Подтверждение соответствия безопасности ПЛК-ФБ

Целью требований настоящего раздела является обеспечение соответствия системы ПЛК-ФБ во всех отношениях требованиям функциональной безопасности в терминах требуемых функций безопасности и полноты безопасности, определенных в разделе 6.

Производитель должен разработать и выполнить план подтверждения соответствия, используя информацию, определенную в разделах 6 и 12.

Отчет о подтверждении соответствия должен быть разработан и сохранен производителем ПЛК-ФБ. Данный отчет должен включать в себя отчеты по типовым испытаниям, которые должны охватить минимальное количество испытаний на уровне системы ПЛК-ФБ, определенных в разделе 12 и подразделах 13.1. и 13.2.

Производитель ПЛК-ФБ будет иметь ПЛК-ФБ, прошедший оценку безопасности, выполненную независимой организацией/подразделением для проекта с УПБ 3, как определено в разделе 14 (см. таблицу 5 МЭК 61508-1).

12 Типовые испытания ПЛК-ФБ

12.1 Общие положения

Типовые испытания системы ПЛК-ФБ должны быть выполнены, чтобы гарантировать, что система ПЛК-ФБ работает в соответствии со спецификацией и во внешних условиях, которые для нее предназначены.

Типовые испытания должны охватить минимальное количество испытаний на уровне системы ПЛК-ФБ, определенных в подразделах 12.2—12.5, и следовать плану подтверждения соответствия ПЛК-ФБ, рассмотренному в 9.3.

Отчет о типовом испытании должен быть написан и сохранен производителем ПЛК-ФБ.

12.2 Требования к типовым испытаниям

Важной частью работ по испытанию каждой системы ПЛК-ФБ является создание процедуры верификации надлежащего функционирования (PFVP — Proper Functioning Verification Procedure) и программы испытаний на основе PFVP. PFVP до максимально возможного уровня должна быть автоматизирована и интегрирована в программу испытаний, а использование в PFVP внешних инструментальных средств и ручных этапов испытаний должно быть сведено к минимуму. Если не указано иное, то данные требования должны быть проверены во время типовых испытаний: климатических, механических, на электромагнитную совместимость, отказоустойчивость и т. д.

PFVP и программу испытаний на ее основе должны использовать, чтобы проверить:

a) надлежащую установку испытуемого технического средства (EUT — equipment under test) ПЛК-ФБ,

b) надлежащее функционирование EUT ПЛК-ФБ до, во время и после типового испытания, как определено в таблице 8;

c) во время испытания, если не указано иное (см. в таблице 8 критерии выполнения функциональной безопасности), не должно быть:

- i) разрушения аппаратных средств,
- ii) непреднамеренной модификации операционной системы и программ испытаний и/или изменения их выполнения,
- iii) непреднамеренной модификации системных и прикладных данных, которые хранят или которыми обменивают,
- iv) ошибочного или непреднамеренного поведения EUT ПЛК-ФБ. Например:
  1) отклонение точности аналоговых входов/выходов от заданных пределов,
  2) отклонение времени отклика при передаче данных и минимальных интенсивностей ошибок от заданных пределов,
  3) отклонение времени сканирования системы и времени отклика системы от их вычисленных пределов для наихудшего случая,
  4) отклонение таймеров управляющей программы от заданных пределов,
  5) отказ в завершении сканирования,
  6) потеря корректности времени суток;

d) все различные режимы работы системы, важные для типичной реализации ПЛК-ФБ, такие как запуск и завершение работы, «холодный»/«теплый»/«горячий» перезапуск, «нормальное выполнение», «нормальная остановка», «запуск программы/контроль через внешний человеко-машинный интерфейс» и т.д.

e) условия инициализации и повторной установки всех компонентов системы во время управляемого запуска и завершения работы.

Следует иметь в виду ограничения инструментальных средств, которые не позволяют выполнить верификацию в реальном времени некоторых или всех этих элементов во время типового испытания. Например, при попытке проверить общеизвестные ограничения точности, когда аналоговые выходы замыкаются на аналоговые входы. В таких случаях установить ограничения на испытание при верификации системы максимально трудно. Другими примерами являются: рабочие режимы, условия инициализации и повторной установки и т. д.

PFVP, когда это применимо, должна выполнять испытание EUT ПЛК-ФБ таким способом, чтобы:

a) все соответствующие функции и части EUT ПЛК-ФБ срабатывали так, чтобы информационные связи к каждому или от каждого типа модуля/функции были реализованы и выполнялся контроль их корректного поведения;

b) было осуществлено функционирование необходимого и достаточного подмножества каналов ввода/вывода и коммуникационных каналов и их функций, определенных производителем, и был выполнен контроль их корректного поведения (см. 2.2 МЭК 61131-2);

c) было осуществлено функционирование всех соответствующих внешних и внутренних средств, информирующих о состоянии системы, таких как светодиодные индикаторы, аварийные сигналы, аварийные системы, и был выполнен контроль их корректного поведения.

Примечание — Ограничения инструментальных средств иногда не позволяют выполнять верификацию в реальном времени некоторых функций системы, например индикаторов передней панели при повышенном уровне тестирования;

d) программа испытаний, реализуемая PFVP, или просто PFVP, выполняла испытание EUT ПЛК-ФБ таким образом, чтобы отразить, насколько это возможно, условия наихудшего случая для времени отклика: быстро изменяющиеся входы и выходы, непрерывные внешние передачи данных, непрерывные одноуровневые коммуникации и т. д. Измерение времени отклика, когда это применимо, должно учитывать следующие действия системы, на выполнение которых может быть затрачено больше времени:

i) условные операторы печати,
ii) условные вычисления с плавающей точкой или работа с массивом,
iii) выполнение пакета событий, многократно одновременно изменяющиеся точки входа/выхода,
iv) выполнение пакета коммуникационных сообщений от внешних источников,
v) выполнение удаленного мониторинга точек входа/выхода во время пакета событий, приводящее к соответствующему внутри сгенерированному пакету сообщений,
vi) потеря связи в коммуникационном канале из-за разрыва, короткого замыкания или электромагнитных помех, приводящая к внутренним остановкам или неверным результатам,
vii) поведение во время выполнения приложения или в присутствии одиночного случайного сбоя аппаратного средства, приводящее к внутренним блокировкам по времени или неверным результатам;

e) во время выполнения типового испытания EUT ПЛК-ФБ должно функционировать с источниками питания, значения характеристик которых определены в МЭК 61131-2 (напряжение, частота и т. д.).

Во время выполнения типового испытания PFVP должна быть в состоянии проверить надлежащее выполнение в соответствии с перечисленными ниже критериями и при реализации требуемых в настоящем стандарте различных условий/ограничений.

Таблица 8 — Критерии оценки выполнения испытания

Критерии	Функционирование во время испытания	Функционирование после испытания
A	Система ПЛК-ФБ должна продолжать функционировать в соответствии с установленными требованиями, не допуская никаких функциональных неисправностей или отказов работоспособности	Система ПЛК-ФБ должна продолжать функционировать в соответствии с установленными требованиями

Критерий	Функционирование во время испытания	Функционирование после испытания
B	Допускаются следующие случаи ухудшения рабочих характеристик ПЛК-ФБ: 1) аналоговые значения не могут меняться более чем на ± значение в % от полной шкалы, заданной производителем; 2) возможны ложные аварийные сигналы системы ПЛК-ФБ без изменения его состояния: например, без перехода от состояния с резервированием к состоянию без резервирования; 3) преднамеренное изменение состояния, при котором не допускается следующее: - неумышленная потеря управления или изменение рабочего режима: например, потеря данных, потеря коммуникации, изменения состояния цифрового входа/выхода, переход от состояния с резервированием к состоянию без резервирования; - необратимая потеря хранившихся данных; - изменение наихудшего значения времени отклика системы ПЛК-ФБ (см. примечание 1)	Система ПЛК-ФБ должна продолжать функционировать в соответствии с установленными требованиями. Временное ухудшение рабочих характеристик должно устраняться автоматически
C	Допускаются функциональные сбои ПЛК-ФБ, но не допускается разрушение аппаратных средств или программного обеспечения (программ или данных)	Система ПЛК-ФБ должна продолжать функционировать в соответствии с установленными требованиями автоматически после ручной перезагрузки или после включения/выключения питания
Функциональная безопасность	Функции EUT ПЛК-ФБ, предназначенные для применения, связанного с безопасностью: 1) подчиняются требованиям критерия выполнения испытания A или 2) могут быть нарушены временно или постоянно, если EUT реагирует на нарушение так, что оно обнаруживается, а затем EUT поддерживает или достигает (за установленное время) заданного состояния или состояний ПЛК-ФБ. Функции применений, не связанные с безопасностью, могут быть нарушены временно или постоянно	Допустимо разрушение связанных с безопасностью компонент, если заданное состояние EUT ПЛК-ФБ поддерживается или достигается в течение установленного времени. Разрушение не связанных с безопасностью компонент допустимо

Примечания

1 Время отклика системы ПЛК-ФБ включает максимальную продолжительность от ступенчатого сигнала на любом входе системы ПЛК-ФБ до ступенчатого сигнала на любом выходе системы ПЛК-ФБ и от ступенчатого сигнала на любом входе системы ПЛК-ФБ до ступенчатого сигнала на любом выходе другой системы ПЛК-ФБ через канал связи, которым они непосредственно соединены.

2 См. 6.2 МЭК 61326-3-1 и 8.3.2 МЭК 61131-2.

12.3 Требования к климатическим испытаниям

О требованиях к климатическим испытаниям см. МЭК 61131-2.

До и после каждого климатического испытания EUT ПЛК-ФБ должно быть проверено на надлежащее функционирование с помощью PFVP. Кроме того, во время каждого такого типового испытания EUT ПЛК-ФБ должно быть проверено на надлежащее функционирование с помощью PFVP.

Специальные тесты для более серьезных климатических условий, чем приведенные в МЭК 61131-2, должны быть согласованы производителем и пользователем.

12.4 Требования к механическим испытаниям

О требованиях к механическим испытаниям см. МЭК 61131-2.

До и после каждого механического испытания EUT ПЛК-ФБ должно быть проверено на надлежащее функционирование с помощью PFVP. Кроме того, во время каждого такого типового испытания EUT ПЛК-ФБ должно быть проверено на надлежащее функционирование с помощью PFVP.

Специальные тесты для более серьезных механических условий, чем приведенные в МЭК 61131-2, должны быть согласованы производителем и пользователем.

12.5 Требования к испытаниям на электромагнитную совместимость (ЭМС)

12.5.1 Общие положения

О методологии достижения функциональной безопасности в случае электромагнитных явлений см. МЭК/ТС 61000-1-2. Однако фактические уровни электромагнитных испытаний там не указаны, поэтому должны использовать требования к испытаниям в 12.5.2 или 12.5.3.

Данные требования не применяют к не связанным с безопасностью функциям оборудования или систем.

До, во время и после каждого испытания на электромагнитную устойчивость тестируемая система ПЛК-ФБ должна быть проверена на надлежащее функционирование с помощью PFVP, в соответствии с критериями выполнения и таблицей 8. Требования по проведению испытаний воздействия излучений на ПЛК-ФБ идентичны тем, которые определены в МЭК 61131-2. Во время каждого испытания воздействия излучения тестируемая система ПЛК-ФБ должна выполняться, чтобы промоделировать типичную окружающую среду системы. Выполнение системы может быть реализовано при помощи автоматизированных средств PFVP.

12.5.2 Обычная электромагнитная среда

Настоящий пункт определяет требования к электромагнитной устойчивости для ПЛК-ФБ, предназначенного для использования в обычной электромагнитной среде, т.е. в среде, где отсутствуют ограничения или средства контроля, связанные с явлениями ЭМС.

Увеличенные уровни испытания на невосприимчивость в таблицах 9 и 10 связаны только с аспектами ФБ. Они не применимы для оценки надежности и готовности. Увеличенные уровни испытания на невосприимчивость применяют только к связанным с безопасностью функциям, имеющим конкретный критерий оценки результатов испытания (критерий оценки результатов испытания для ФБ). Увеличенные уровни испытания на невосприимчивость являются максимальными тестовыми значениями. Дальнейшее испытание с более высокими значениями для соответствия настоящему стандарту не требуется.

Таблицы 9 и 10 содержат все требования к электромагнитной устойчивости из МЭК 61131-2.

Таблица 9 — Уровни испытаний на устойчивость к электромагнитным помехам портов корпуса в обычной электромагнитной среде

Физическое явление	Ссылочный стандарт	Испытание	Уровень испытания	Критерий оценки
Электростатический разряд	МЭК 61000-4-2	Контактный разряд	±6 кВ[a)]	ФБ
		Воздушный разряд	±8 кВ[a)]	
Радиочастота Электромагнитное поле Амплитудная модуляция	МЭК 61000-4-3	2,0 — 2,7 Гц	3 В/м[b)]	ФБ
		1,4 — 2,0 Гц	10 В/м	
		80 — 1,0 Гц	20 В/м[b)]	
Магнитные поля промышленной частоты	МЭК 61000-4-8	50/60 Гц	30 А/м[c)] Увеличенный уровень испытаний не применяют	ФБ

[a)] Применяемые уровни должны соответствовать условиям окружающей среды, описанным в МЭК 61000-4-2, на компоненты, которые могут быть доступны лицам, не работающим в соответствии с определенными процедурами по управлению электростатическим разрядом и не работающим с оборудованием, доступ к которому ограничен только соответственно обученным персоналом.

[b)] Эти значения (более высокие, чем в МЭК 61131-2), как правило, должны применяться в частотных диапазонах, используемых для мобильных передатчиков, кроме тех случаев, когда поблизости реализованы надежные меры, предотвращающие влияние такого оборудования. Частоты промышленного, научного и медицинского диапазона ISM должны быть учтены отдельно.

[c)] Применим только к оборудованию, содержащему устройства, чувствительные к магнитным полям.

Таблица 10 — Уровни испытаний на устойчивость к электромагнитным помехам в обычной электромагнитной среде

	Физическое явление	Наносекундная импульсная помеха	Микросекундная импульсная помеха большой энергии (см. примечание)	Радиочастотные помехи	
	Ссылочный стандарт	МЭК 61000-4-4	МЭК 61000-4-5	МЭК 61000-4-6	
	Критерии оценки	ФБ	ФБ	ФБ	
Интерфейс/порт (обозначение)	Специальный интерфейс/порт	Уровень испытаний	Уровень испытаний[f]	Уровень испытаний	Значения, взятые из:
Питание оборудования F и питание входов-выходов J и выход вспомогательного источника питания K	Питание от источника переменного тока	3 кВ[a] (5/50 нс,5 кГц)	4 кВ CM 2 кВ DM	10 В[b] 15 кГц до 80 МГц	МЭК 61236-3-1, таблица 1b[b]
	Питание от источника постоянного тока[e]	3 кВ[a] (5/50 нс,5 кГц)	2 кВ CM[c] 1 кВ DM	10 В[b] 15 кГц до 80 МГц	МЭК 61236-3-1, таблица 1c[c]
Входы/выходы C и D	Обычный вход/выход	2 кВ[a],[d] (5/50 ns,5 кГц)	2 кВ CM	10 В[b] 15 кГц до 80 МГц	МЭК 61236-3-1, таблица 1d[d]
	Вход/выход, непосредственно соединенный к сетям источника питания	3 кВ[a] (5/50 нс,5 кГц)	4 кВ CM 2 кВ DM	10 В[b] 15 кГц до 80 МГц	МЭК 61236-3-1, таблица 1e[e]
Функциональное заземление H	—	2 кВ[a] (5/50 нс,5 кГц)	Нет теста	3 В	МЭК 61236-3-1, таблица 1f[f]

Примечание — Требуемый уровень невосприимчивости может быть достигнут с помощью внешних устройств защиты.

[a] Для оборудования, предназначенного для использования в применениях с УПБ 3, продолжительность испытания на максимальном уровне должна быть увеличена в 5 раз по сравнению с продолжительностью, заданной в базовом стандарте.

[b] Эти значения (более высокие, чем в МЭК 61131-2), как правило, должны применять в частотных диапазонах, используемых для мобильных передатчиков, кроме тех случаев, когда поблизости реализованы надежные меры, предотвращающие влияние такого оборудования. Частоты промышленного, научного и медицинского диапазона ISM должны быть учтены отдельно.

[c] Только для портов с длиной кабеля более 30 м внутри здания или за его пределами (включая кабели наружных установок).

[d] Испытания не проводят только для портов с требуемой длиной кабеля менее 3 м.

[e] Соединения по постоянному току между частями оборудования/системы, которые не соединены с распределительной сетью постоянного тока, рассматривают как порты входа/выхода сигнала/управления.

[f] DM — дифференциальный режим, CM — общий режим.

12.5.3 Задаваемая электромагнитная среда

В настоящем подразделе определены требования к электромагнитной устойчивости для ПЛК-ФБ, предназначенные для использования в электромагнитной среде, определенной производителем ПЛК-ФБ.

Требования к электромагнитной устойчивости, определенные в таблицах 11 и 12, включают требования МЭК 61131-2.

Описание среды промышленного применения в заданной электромагнитной обстановке обычно включает следующие характеристики:

- промышленная зона с ограниченным доступом;
- ограниченное использование мобильного передатчика;
- специально выделенные кабели для источника питания и управления, сигнальных линий или линий связи;
- разделение между кабелями источника питания и кабелями управления, сигнальными или коммуникационными;

- производственное здание, главным образом должно состоять из металлических конструкций;
- наличие защиты от повышения напряжения/молнии надлежащими мерами (например, использование металлических конструкций здания или устройств защиты);
- могут присутствовать системы водяного обогрева, управляемые основным источником питания переменного напряжения;
- рядом с чувствительными зонами не может быть расположена какая-либо высоковольтная подстанция;
- возможно присутствие ISM оборудования группы 2 CISPR 11, использующего частоты ISM, только низкой мощности;
- наличие компетентного штата;
- периодическое техническое обслуживание оборудования и систем;
- наличие инструкций по монтажу и установке для оборудования и систем.

Более подробное описание вышеупомянутых типичных характеристик дано в приложении В МЭК 61326-3-2.

Таблица 11 — Уровни испытаний на устойчивость к электромагнитным помехам портов корпуса в задаваемой электромагнитной среде

Физическое явление	Ссылочный стандарт	Испытание	Уровень испытания	Критерий оценки
Электростатический разряд	МЭК 61000-4-2	Контактный разряд	±6 кВ[a]	A
		Воздушный разряд	±8 кВ[a]	
Радиочастота Электромагнитное поле Амплитудная модуляция	МЭК 61000-4-3	2,0—2,7 Гц	3 В/м[b]	A
		1,4—2,0 Гц	10 В/м	
		80—1,0 Гц	10 В/м[b]	
Магнитные поля промышленной частоты	МЭК 61000-4-8	50/60 Гц	100 А/м[c]	A

[a] Применяемые уровни должны соответствовать условиям окружающей среды, описанным в МЭК 61000-4-2, на компоненты, которые могут быть доступны лицам, не работающим в соответствии с определенными процедурами по управлению электростатическим разрядом и не работающим с оборудованием, доступ к которому ограничен только соответственно обученным персоналом.

[b] За исключением полос частоты вещания ITU от 87 до 108 МГц, от 174 до 230 МГц и от 470 до 790 МГц, где уровень должен составить 3 В/м.

[c] Применим только к оборудованию, содержащему устройства, чувствительные к магнитным полям.

Таблица 12 — Уровни испытаний на устойчивость к электромагнитным помехам в задаваемой электромагнитной среде

	Физическое явление	Наносекундная импульсная помеха	Микросекундная импульсная помеха большой энергии (см. примечание)	Радиочастотные помехи	
	Ссылочный стандарт	МЭК 61000-4-4	МЭК 61000-4-5	МЭК 61000-4-6	
	Критерии оценки	A	A	A	
Интерфейс/порт (обозначение)	Специальный интерфейс/порт	Уровень испытания	Уровень испытания[f]	Уровень испытания	Значения, взятые из:
Питание оборудования F и питание входов-выходов J и выход вспомогательного источника питания K	Питание от источника переменного тока	2 кВ (5/50 нс,5 кГц)	2 кВ CM 1 кВ DM	10 В[a] 15 до 80 кГц	МЭК 61236-3-1, таблица 1b[b]
	Питание от источника постоянного токае	2 кВ (5/50 нс,5 кГц)	1 кВ CM 0,5 кВ DM	10 В[a] 15 до 80 кГц	МЭК 61236-3-1, таблица 1c[c]

Окончание таблицы 12

	Физическое явление	Наносекундная импульсная помеха	Микросекундная импульсная помеха большой энергии (см. примечание)	Радиочастотные помехи	
	Ссылочный стандарт	МЭК 61000-4-4	МЭК 61000-4-5	МЭК 61000-4-6	
	Критерии оценки	A	A	A	
Интерфейс/порт (обозначение)	Специальный интерфейс/порт	Уровень испытания	Уровень испытания[f]	Уровень испытания	Значения, взятые из:
Входы/выходы C и D	Обычный вход/выход	1 кВ[b] (5/50 нс,5 кГц)	1 кВ СМ[c] (см. примечание)	10 В[b],[d] 15 до 80 МГц	МЭК 61236-3-1, таблица 1d[d]
	Вход/выход, непосредственно соединенный к сетям источника питания	2 кВ[a] (5/50 нс,5 кГц)	2 кВ СМ 1 кВ DM	10 В[d] 10 до 80 МГц	МЭК 61236-3-1, таблица 1e[e]
Функциональное заземление H	—	2 kV[b] (5/50 нс,5 кГц)	1 kV СМ[c] (см. примечание)	10 В[d] 10 до 80 МГц	МЭК 61236-3-1, таблица 1f[f]

Примечание — Критерий оценки результатов испытания «ФБ» разрешен.

a) В частотном диапазоне от 10 до 150 кГц импеданс корпоративной сети обмена данными должен соответствовать требованиям асимметричного импеданса из МЭК 61000-4-6 при 150 кГц. Калибровка будет выполняться в соответствии с МЭК 61000-4-6. Может быть продемонстрирована достаточная развязка, если критерию импеданса соответствуют оба с короткозамкнутым и разомкнутым портом AE.

b) Испытания не проводят только для портов с требуемой длиной кабеля менее 3 м.

c) Только для портов с длиной кабеля более 30 м внутри здания, или за его пределами (включая кабели наружных установок).

d) В частотном диапазоне от 10 до 150 кГц импеданс корпоративной сети обмена данными должен соответствовать требованиям асимметричного импеданса МЭК 61000-4-6 при 150 кГц. Калибровка должна быть выполнена в соответствии с МЭК 61000-4-6. Может быть продемонстрирована достаточная развязка, если критерию импеданса соответствуют оба с короткозамкнутым и разомкнутым портом AE.

e) Соединения по постоянному току между частями оборудования/системы, которые не соединены с распределительной сетью постоянного тока, рассматривают как порты ввода/вывода сигнала/управления.

f) DM — дифференциальный режим, CM — общий режим.

13 Верификация ПЛК-ФБ

13.1 План верификации

План верификации ПЛК-ФБ должен быть выполнен и содержать, по крайней мере, следующие элементы:

- анализ спецификации требований;
- анализ процессов проектирования;
- анализ проекта аппаратных средств (пример: принципиальная схема, структура изделия);
- анализ проекта встроенного программного обеспечения;
- анализ пригодности инструментальных средств только для частей, связанных с функциональной безопасностью (см. рисунок 5);
- анализ спецификации испытания (испытания модуля, испытания интеграции);
- анализ спецификации испытания для системы и типового испытания;
- анализ видов и последствий отказов FMEA;
- анализ результатов испытаний (например, испытания модуля, испытания интеграции, испытания системы и типового испытания);
- испытание на отказ аппаратных средств, например, используя моделирование или выполняя на физическом устройстве;
- анализ критичности;
- испытание на отказ встроенного программного обеспечения, например, используя моделирование;

- анализ метода вычисления данных о надежности (например, анализ общей причины, моделирование Маркова, вычисление Маркова).

Выполнение перечисленных видов анализа должно быть независимым и документально оформлено.

13.2 Требования к испытанию с введением неисправности

Испытание с введением неисправности заключается в преднамеренном включении неисправности для определения ее влияния на работу ПЛК-ФБ.

Испытания с введением неисправности должны быть выполнены как часть проверочного испытания со следующими целями.

- проверить, что последствия отказа, предсказанные в аппаратных средствах с помощью FMEA, корректны, и, следовательно, интенсивность этих отказов правильно включена в классификацию отказов (см. 9.4.7);
- проверить, что реакция на диагностические проверки во время их выполнения соответствует предполагаемой в проекте реакции;
- проверить, что реакция на сбой ПЛК-ФБ соответствует предполагаемой в проекте реакции;
- проверить, что разрешенные процессы обслуживания в неавтономном режиме, например смена модуля, выполняют в соответствии с проектом.

Испытания с введением неисправности могут быть выполнены на уровне компонентов или на более высоком уровне: на уровне элемента или подсистемы.

Примеры испытания с введением неисправности на уровне компонентов:

- размыкание (обрыв) компонента;
- короткое замыкание компонента;
- действие, вызывающее выход цифровой ИС в некорректном состоянии.

Примеры испытания с введением неисправности в элементе или на уровне подсистемы:

a) удаление или включение модуля во время работы;

b) моделирование повышенного или пониженного напряжения на шине электропитания;

c) повреждение данных, передаваемых между элементами или подсистемами.

Таблица 13 представляет требуемую эффективность испытаний с введением неисправности в зависимости от целевого УПБ и требуемого ОД.

Таблица 13 — Требуемая эффективность испытания отказоустойчивости

Требуемая эффективность испытания с введением неисправности			
Требуемый охват диагностикой	УПБ 1	УПБ 2	УПБ 3
< 90 %	Низкая	Низкая	Средняя
≥ 90 %	Высокая	Высокая	Высокая

Для обеспечения низкой эффективности испытания должны быть выполнены, по крайней мере, на уровне элемента или подсистемы, включая передачу данных между модулями.

Для обеспечения средней и высокой эффективности испытания должны также быть выполнены на уровне компонентов с достаточной строгостью, чтобы проверить требуемый ОД. Испытания должны быть применены там, где:

- последствие отказа, предсказанное FMEA, не находится под четким контролем;
- велика интенсивность отказа при анализе его последствия;
- диагностические испытания во время выполнения предназначены для обнаружения неисправности.

Примечание — Необходимая строгость испытания с введением неисправности зависит от заявленного ОД, эффективности FMEA, архитектуры ПЛК-ФБ и т.д.

Для того чтобы проверить корректную работу ПЛК-ФБ, должны использовать процедуру PFVP:

- до выполнения испытания с введением неисправности;
- во время испытания с введением неисправности, если предназначенная реакция состоит в том, чтобы продолжить нормальное функционирование;
- после восстановления, которое следует за испытанием с введением неисправности.

До, во время и после каждого испытания с введением неисправности EUT ПЛК-ФБ должно быть проверено на надлежащее функционирование с помощью PFVP.

Метод применения испытаний с введением неисправности, конкретные применяемые испытания и требуемый результат каждого испытания должны быть установлены в плане проверочного испытания. Количество и строгость испытаний с введением неисправности должны быть согласованы производителем ПЛК-ФБ и экспертом, учитывая сложность ПЛК-ФБ, его предназначенное применение и его уровень полноты безопасности.

После выпуска изделия может возникнуть необходимость повторить некоторые испытания с введением неисправности, чтобы проверить модификацию изделия или его усовершенствование. Объем требуемого повторного испытания должен быть определен в результате анализа влияния изменения.

13.3 Проверенное изделие по сравнению с поставленным

Производитель должен принять меры, гарантирующие, что все изделия, поставляемые клиенту, должны действовать так же или лучше, чем модули, используемые во время типового испытания.

Примечание — Ниже перечислены примеры методов, которые могут использовать:

a) использование консервативных пределов рабочего режима во время типового испытания, например:

1) рабочая температура: на 10 °С больше верхнего и меньше нижнего значений, представленных в спецификации,

2) рабочая влажность: на 30 % больше максимального рабочего значения, но не более 95 % RH,

3) рабочая вибрация: на 30 % больше предельного значения *g*, представленного в спецификации,

4) электромагнитная устойчивость: на 50 % выше значения, представленного в спецификации,

b) использование дополнительных тестов во время типового испытания: резко ускоренное испытание жизненного цикла (HALT) и т.д.;

c) тестирование с дополнительными модулями во время типового испытания;

d) тестирование 100 % всех поставленных модулей или определение с помощью анализа критических характеристик системы и их 100 %-ное тестирование;

e) использование дополнительных тестов во время производства: ускоренное испытание в экстремальных условиях HAST и т.д.;

f) дополнительные проверки гарантии качества, оценки, анализ и т.д.;

g) запрет на любые изменения проекта, компонентов или материалов в изделии, для которого выполнены типовые испытания;

h) выполнение формального анализа влияния изменения.

14 Оценка функциональной безопасности

14.1 Цель

Цель требований настоящего раздела состоит в том, чтобы определить действия, необходимые для рассмотрения и достижения решения о соответствии ПЛК-ФБ требованиям функциональной безопасности, о соблюдении ПЛК-ФБ требований соответствующих подразделов настоящего стандарта, а также определить, было ли достигнуто соблюдение требований соответствующих подразделов настоящего стандарта.

Оценка функциональной безопасности ПЛК-ФБ должна быть выполнена для обеспечения гарантии достижения необходимого уровня безопасности. Ее результаты должны быть представлены в отчете оценки безопасности. Отчет должен содержать объяснения действий, выполненных экспертом по безопасности, чтобы определить, как система/подсистема/оборудование ПЛК-ФБ (аппаратные средства и программное обеспечение) были разработаны, чтобы удовлетворить заданным для них требованиям и определить некоторые дополнительные условия для работы системы/подсистемы/оборудования.

Эксперт или команда, выполняющие оценку, должны быть, по крайней мере, независимы от команды разработчиков ПЛК-ФБ.

14.2 Требования к оценке

14.2.1 Обоснование и документальное оформление оценки

Оценка должна представить доказательства, что все необходимые шаги по верификации и подтверждению соответствия выполнены, чтобы представить свидетельства о том, что:

a) меры по предотвращению отказов (действия по управлению функциональной безопасностью) подходят для требуемого УПБ;

b) меры по управлению отказами в аппаратных средствах и программном обеспечении подходят для требуемого УПБ.

Оценка функциональной безопасности должна основываться на оценке следующей документации:

- спецификация требований системы ПЛК-ФБ (или подсистемы/оборудования);
- определение системы/подсистемы/оборудования;
- план верификации и подтверждения соответствия (V&V);
- план обеспечения безопасности;
- отчет об управлении функциональной безопасностью в соответствии с МЭК 61508-1 и настоящим стандартом (доказательство управления безопасностью);
- отчет об аппаратных мерах в соответствии с МЭК 61508-2 и МЭК 61508-3 и этим стандартом; план(ы) и отчет(ы) тестирования;
- соответствие требованиям внешней среды и ЭМС;
- соответствие требованиям МЭК 61131-2.

14.2.2 Метод оценки

1) Для выполнения одной или более оценок функциональной безопасности необходимо назначить одно или более лиц, чтобы принять решение о соответствии:

a) функциональной безопасности, достигаемой ПЛК-ФБ в конкретной окружающей ее среде; положениям соответствующих подразделов настоящего стандарта;

b) выполнения в этом случае соответствующих положений настоящего стандарта элементами или подсистемами.

2) Лица, осуществляющие оценку функциональной безопасности, должны иметь доступ ко всем лицам, выполняющим любые действия на всех стадиях жизненного цикла системы безопасности на ПЛК-ФБ, а также ко всей информации и оборудованию (включая аппаратные средства и программное обеспечение).

3) Оценку функциональной безопасности следует применять ко всем стадиям на протяжении всего жизненного цикла, включая документацию, верификацию и управление функциональной безопасностью.

4) Лица, осуществляющие оценку функциональной безопасности, должны рассмотреть все выполняемые действия, а также все результаты, полученные в течение каждой стадии жизненного цикла всей системы безопасности, и дать заключение о том, была ли достигнута соответствующая функциональная безопасность на основе целей и требований настоящего стандарта.

5) Компетентность эксперта или команды, выполняющей оценку, должна соответствовать уровню разработки аппаратных средств и программного обеспечения ПЛК-ФБ, а также должна быть документально оформлена.

6) Все соответствующие заявления о соответствии, предоставленные поставщиками и другими сторонами, ответственными за достижение функциональной безопасности, должны быть включены в оценку функциональной безопасности.

7) Оценка функциональной безопасности может выполняться после каждой стадии жизненного цикла всей системы безопасности, включающей ПЛК-ФБ, или после нескольких стадий ее жизненного цикла.

8) Оценка функциональной безопасности должна включать в себя доказательство того, что аудит(ы) функциональной безопасности был(и) проведен(ы) (полностью или частично) в соответствии с его(их) областью применения.

9) При каждой оценке функциональной безопасности, если она выполняется шаг за шагом, необходимо учитывать, как минимум, следующее.

a) работы, выполненные со времени предыдущей оценки функциональной безопасности;

b) планы или стратегию реализации последующих оценок функциональной безопасности;

c) рекомендации предыдущих оценок функциональной безопасности и объем внесенных изменений, удовлетворяющих эти рекомендации.

10) Каждая оценка функциональной безопасности должна быть спланирована. План должен определять всю информацию, необходимую для проведения эффективной оценки, включая:

a) область применения оценки функциональной безопасности;

b) вовлеченные организации;

c) требуемые ресурсы;

d) о лицах, осуществляющих оценку функциональной безопасности, и об их компетентности,

e) об уровне независимости лиц, выполняющих оценку функциональной безопасности;

f) выходные материалы при каждой оценке функциональной безопасности;

g) как оценка функциональной безопасности соотносится и должна быть интегрирована с другими оценками функциональной безопасности;

h) в какой момент в течение жизненного цикла системы безопасности, включающей ПЛК-ФБ, будет(ут) выполняться оценка(ки).

11) Перед выполнением оценки функциональной безопасности ее план должен быть утвержден теми, кто будет выполнять эту оценку, и теми, кто несет ответственность за управление функциональной безопасностью.

12) В заключении об оценке функциональной безопасности лица, выполняющие оценку, должны документально оформить в соответствии с планами оценки и кругом полномочий:

- выполненные действия;
- полученные результаты;
- выводы;
- суждение о соответствии функциональной безопасности требованиям настоящего стандарта;
- рекомендации, вытекающие из оценки, в т.ч. рекомендации по принятию, условному принятию или отклонению.

13) Ответственным за любые действия на жизненном цикле всей системы безопасности на основе ПЛК-ФБ, включая конструкторов и экспертов ПЛК-ФБ, должны быть доступны соответствующие результаты оценки функциональной безопасности применяемого изделия.

14) Результат оценки функциональной безопасности применяемого изделия должен включать следующую информацию для облегчения повторного использования результатов оценки для более крупной системы:

a) точное определение применяемого изделия, включая версии аппаратного средства и программного обеспечения;

b) условия, предполагаемые в ходе оценки;

c) ссылку на документально оформленное доказательство, на котором основано заключение оценки;

d) процедуры, методы и инструменты, используемые для оценки стойкости к систематическим отказам, вместе с обоснованием их эффективности;

e) процедуры, методы и инструменты, используемые для оценки полноты безопасности аппаратного обеспечения, вместе с обоснованием используемого подхода и качества данных;

f) оценку результатов, полученных в соответствии с требованиями настоящего стандарта и спецификацией характеристик системы безопасности для применяемого изделия в соответствующем руководстве по безопасности.

15) Лица, осуществляющие оценку функциональной безопасности, должны быть компетентными в выполняемых действиях в соответствии с требованиями с 5.4.2.2.2 и 5.4.2.2.3.

14.3 Информация об оценке ПЛК-ФБ

Информацию, представленную в таблице 14, должен поддерживать производитель ПЛК-ФБ.

Таблица 14 — Информация об оценке функциональной безопасности

Стадия жизненного цикла ПЛК-ФБ	Информация
Концепция	Описание (концепция ПЛК-ФБ)
Определение области распространения ПЛК-ФБ	Описание (определение области распространения ПЛК-ФБ)
Требования функциональной безопасности к ПЛК-ФБ	Спецификация (требований функциональной безопасности к ПЛК-ФБ, включая требования к функциям безопасности и требования к полноте безопасности)
Распределение требований функциональной безопасности	Описание (распределение требований функциональной безопасности)
Планирование эксплуатации и технического обслуживания ПЛК-ФБ	План (эксплуатации и технического обслуживания ПЛК-ФБ)
Планирование верификации и подтверждения соответствия безопасности ПЛК-ФБ	План (верификации и подтверждения соответствия безопасности ПЛК-ФБ)

Окончание таблицы 14

Стадия жизненного цикла ПЛК-ФБ	Информация
Реализация	Документация по проектированию и разработке (см. МЭК 61508-2 и МЭК 61508-3)
Верификация и подтверждение соответствия безопасности ПЛК-ФБ	Отчет (о верификации и подтверждении соответствия безопасности ПЛК-ФБ)
Эксплуатация и техническое обслуживание ПЛК-ФБ	Процедуры эксплуатации и технического обслуживания ПЛК-ФБ
Модификация ПЛК-ФБ	Запрос (на модификацию ПЛК-ФБ); отчет (о модификации ПЛК-ФБ) и ведение анализа влияния записи (о модификации ПЛК-ФБ) в журнале модификаций
Для всех стадий	План (обеспечения безопасности); план (верификации); отчет (по верификации); план (оценки функциональной безопасности); отчет (об оценке функциональной безопасности)

14.4 Независимость

Минимальный уровень независимости, выполняющий оценку функциональной безопасности, должен соответствовать тому уровню, который указан в таблице 15. Таблицу 15 следует интерпретировать следующим образом:

X — уровень независимости, определенный в качестве минимального для заданного уровня полноты безопасности/стойкости к систематическим отказам. Если принят более низкий уровень независимости, то должно быть приведено подробное обоснование;

X1 и X2;

Y — уровень независимости, определенный как недостаточный для уровня полноты безопасности/стойкости к систематическим отказам.

В контексте таблицы 15 в качестве основы для определения уровня независимости должны использовать только X, X1, X2 или Y. Если выбраны X1 или X2, то применяют либо X1, либо X2 (но не оба вместе), в зависимости от ряда факторов, характерных для проекта ПЛК-ФБ. Обоснование выбора X1 или X2 должно быть подробным. Факторы, которые делают X2 более предпочтительным, чем X1, следующие:

- недостаток опыта в работе со схожими проектами;
- более высокая степень сложности;
- более высокая степень новизны разработки;
- более высокая степень новизны технологии.

Примечания

1 В зависимости от организационной структуры компании и опыта внутри компании требования к независимости лиц и подразделений в некоторых случаях могут быть выполнены путем использования услуг сторонней организации. В свою очередь, компании, которые имеют внутренние структуры с опытом оценки рисков и применения систем, связанных с безопасностью, и которые независимы и отделены (по управлению и используемым ресурсам) от тех, которые несут ответственность за основную разработку, в некоторых случаях могут оказаться способными использовать собственные ресурсы, чтобы удовлетворить требования по независимости организации.

2 См. 3.8.11, 3.8.12 и 3.8.13 МЭК 61508-4:2010 для определения терминов «независимое лицо», «независимое подразделение» и «независимая организация» соответственно.

3 Лица, осуществляющие оценку функциональной безопасности, должны быть осторожны в предоставлении консультаций по какому-либо вопросу, связанному с оценкой, поскольку это может ставить под угрозу их независимость. Зачастую принято давать советы по различным аспектам, что может повлечь за собой решение о недостаточности безопасности, такое как недостаточность доказательств, и обычно не принято давать советы или рекомендации для конкретных средств защиты от тех или иных проблем.

В контексте таблицы 15 минимальный уровень независимости должен основываться на наивысшей стойкости к систематическим отказам, на которую претендует ПЛК-ФБ и которая определена значением уровня полноты безопасности.

Таблица 15 — Минимальные уровни независимости, выполняющие оценку функциональной безопасности

Минимальный уровень независимости	Уровень полноты безопасности / стойкость к систематическим отказам			
	1	2	3	4
Независимое лицо	X	X1	Y	Y
Независимое подразделение	—	X2	X1	Y
Независимая организация	—	—	X2	X

15 Процедуры эксплуатации, технического обслуживания и модификации ПЛК-ФБ

15.1 Цель

Цель настоящего раздела состоит в том, чтобы гарантировать, что производитель ПЛК-ФБ обеспечивает процедуры эксплуатации, технического обслуживания и модификации системы ПЛК-ФБ, которые удовлетворяют во всех отношениях требованиям безопасности в терминах требуемых функций безопасности и полноты безопасности, определенных в разделе 6.

Информация для этих процедур эксплуатации, технического обслуживания и модификации определена в разделе 16.

15.2 Модификация ПЛК-ФБ

Производители, которые заявляют соответствие с настоящим стандартом, должны поддерживать систему управления изменениями, которая, например, в результате обнаружения дефектов, должна усовершенствовать процесс проектирования или производственный процесс либо улучшить функциональность. Эта система должна включать документацию: по деталям модификации, исследованию влияния модификации (включая необходимость в повторной верификации и повторном подтверждении соответствия), одобрению модификации, результатам повторного подтверждения соответствия/повторной верификации и любым связанным изменениям в эксплуатации или документации изделия. Более подробную информацию см. в 7.16 МЭК 61508-1 и 7.8 МЭК 61508-3.

Все модификации ПЛК-ФБ должны быть проанализированы, чтобы определить влияние, которое будет иметь изменение или улучшение модуля системы ПЛК-ФБ на другие модули той же системы, а также на другие части связанной с безопасностью системы.

Данный анализ должны выполнять до модификации или выполняемого улучшения.

После завершения анализа должно быть принято решение о необходимости повторной модификации системы ПЛК-ФБ. Это зависит от числа затронутых модулей, критичности затронутых модулей и природы изменения. Возможны следующие решения:

- только измененный модуль должен быть повторно проверен;
- все затронутые модули должны быть повторно проверены; или
- вся система ПЛК-ФБ должна быть повторно проверена.

Производитель ПЛК-ФБ должен сохранить историю этого анализа и принятые решения по всем изменениям, которые влияют на безопасность соответствующих частей ПЛК-ФБ.

16 Информация, предоставляемая пользователю производителем ПЛК-ФБ

16.1 Общие положения

Производитель должен предоставить пользователям информацию, необходимую для применения, установки, ввода в действие, эксплуатации и обслуживания ПЛК-ФБ. Кроме того, производитель может обеспечить обучение пользователей. Информация может быть предоставлена не только на бумажном, но и на других носителях.

16.2 Информация о соответствии настоящему стандарту

Производитель должен по запросу предоставлять информацию о проверке соответствия.

16.3 Информация о типе и содержании документации

Определены четыре типа документов:
- каталоги и спецификации;
- руководства пользователя;
- руководство по безопасности;
- техническая документация.

Примечание — О подготовке инструкций см. МЭК 62079 и МЭК 61506.

16.4 Информация каталогов и спецификаций

Документы данного типа должны содержать описание и спецификации ПЛК-ФБ и связанных с ним периферийных устройств. Кроме того, они должны содержать другую информацию, поясняющую сущность применения и использования данных изделий, включая функциональные характеристики, правила конфигурирования оборудования, нормальные условия эксплуатации, а также перечень соответствий стандартам и сертификатам.

16.5 Руководство по безопасности

16.5.1 Общие положения

Цель руководства по безопасности состоит в документальном оформлении информации, связанной с ПЛК-ФБ, которая необходима для обеспечения интеграции ПЛК-ФБ в связанную с безопасностью систему, чтобы она соответствовала требованиям серии МЭК 61508.

Примечание — Данный текст адаптирован из D.2.2 МЭК 61508-2:2010 и D.2.2 МЭК 61508-3:2010.

16.5.2 Содержание руководства по безопасности

16.5.2.1 Общие положения

Каждый ПЛК-ФБ должен иметь руководство по безопасности. В общем случае руководство по безопасности должно содержать:

a) функциональную спецификацию выполняемых функций;

b) идентификацию конфигурации аппаратных средств и/или программного обеспечения ПЛК-ФБ, чтобы обеспечить управление конфигурацией Э/Э/ПЭ системы, связанной с безопасностью, в соответствии с требованиями 6.2.1 МЭК 61508-1;

c) ограничения на использование ПЛК-ФБ и/или предположения, на которых основан анализ поведения или интенсивности отказов ПЛК-ФБ.

16.5.2.2 Содержание руководства по безопасности

Руководство по безопасности должно определить функции применяемого элемента. Они могут использоваться, чтобы поддерживать функцию безопасности связанной с безопасностью системы или функции в подсистеме или элементе. Спецификация должна ясно описать и функции, и интерфейсы ввода и вывода.

Для каждой функции руководство по безопасности должно содержать:

a) виды отказов применяемого элемента (в терминах поведения его выходов) из-за случайных отказов аппаратных средств, приводящих к отказу функции и не обнаруживаемых внутренней диагностикой ПЛК-ФБ;

b) оцененную интенсивность отказов для каждого вида отказов по перечислению a);

c) виды отказов применяемого изделия (в терминах поведения его выходов) из-за случайных отказов аппаратных средств, приводящих к отказу функции и обнаруживаемых внутренней диагностикой ПЛК-ФБ;

d) виды отказов внутренней диагностики ПЛК-ФБ (в терминах поведения его выходов) из-за случайных отказов аппаратных средств, приводящих к отказу диагностик для обнаружения отказов функции;

e) оцененную интенсивность отказов для каждого вида отказов по перечислениям c) и d);

f) диагностический испытательный интервал для каждого вида отказов по перечислению c), которые обнаруживаются внутренней диагностикой ПЛК-ФБ;

g) выходы применяемого изделия, инициируемые внутренними диагностиками для каждого вида отказов по перечислению c).

Примечание — Результаты внутренних диагностик инициируют применение дополнительных мер (аппаратных/процедурных) к Э/Э/ПЭ системе, связанной с безопасностью, подсистеме или элементу, чтобы обеспечить или поддержать безопасное состояние УО;

h) требования к любому периодическому испытанию и/или техническому обслуживанию;

i) для тех видов отказов указанной функции, которые обнаруживаются внешними диагностиками, должно быть предоставлено достаточное количество информации, чтобы облегчить разработку возможностей внешней диагностики. Такая информация должна включать в себя подробное описание видов отказа и их интенсивности;

j) отказоустойчивость аппаратных средств;

k) классификацию на тип А или тип В той части ПЛК-ФБ, которая обеспечивает выполнение функции.

Примечание — Виды отказов могут быть классифицированы как безопасные или опасные, только если известно, как ПЛК-ФБ применяется в опасных ситуациях УО. Например, если датчик будет применен так, что высокий уровень его выходного сигнала используется, чтобы сигнализировать об опасности УО (например, из-за высокого давления), то вид отказа, который предотвращает корректную индикацию опасности (например, выходной сигнал имеет постоянный низкий уровень), будет классифицирован как опасный, тогда как вид отказа, в результате которого выходной сигнал датчика имеет высокий уровень, будет классифицирован как безопасный. Это зависит от того, как сигнал датчика интерпретируется ПЛК-ФБ, и поэтому датчик не может быть специфицирован без ограничения способа его применения.

Кроме того, уровень ОД, требуемый для ПЛК-ФБ, может меняться от одного применения к другому в зависимости от объема любых диагностик для ПЛК-ФБ или обработки внешнего сигнала, к которым может добавляться любая внутренняя диагностика ПЛК-ФБ.

Из этого следует, что любая оценка отказоустойчивости аппаратных средств или доли безопасных отказов может быть выполнена, если только на применение ПЛК-ФБ накладывают ограничения. Эти ограничения не определены поставщиком ПЛК-ФБ. Поэтому в руководство по безопасности не должны включать требования к отказоустойчивости аппаратных средств, или к доле безопасных отказов, или к любым другим характеристикам функциональной безопасности, которые зависят от знания о безопасных и опасных видах отказов, если явно не определены основные предположения о соотношении безопасных и опасных видов отказов;

l) руководящие указания о том, как учитывать вклад ПЛК-ФБ во времени отклика функции безопасности или во времени безопасности процесса.

Для каждой функции ПЛК-ФБ, для которой возможны систематические отказы, руководство должно содержать:

1) стойкость к систематическим отказам ПЛК-ФБ или той части элемента, которая реализует функцию;

2) любые указания или ограничения, связанные с применением ПЛК-ФБ, реализующего рассматриваемую функцию, которые должны предотвратить систематические отказы ПЛК-ФБ.

Примечание — Систематическая полнота безопасности, определяемая стойкостью к систематическим отказам, может быть достигнута, только если указания и ограничения соблюдают. Там, где происходит их нарушение, требование к стойкости к систематическим отказам частично или полностью несостоятельно.

16.5.2.3 Содержание руководства по безопасности для инструментальных средств

Инструментальные средства должны быть определены, и все необходимые инструкции для их использования должны быть доступны интегратору и пользователю.

Примечание — Для инструментальных средств это демонстрируется явной идентификацией этого элемента и демонстрацией того, что его содержание неизменно.

Приложение А
(справочное)

Вычисление безотказности

А.1 Общие положения

В настоящем приложении рассмотрено несколько примеров методов вычисления вероятностей отказа для приборной системы безопасности, разработанной и введенной в действие в соответствии с МЭК 61511-1. Данная информация, по существу, имеет справочный характер, поэтому для вычисления вероятностей отказа вполне могут использовать и другие методы оценки.

Представленные методологии подробно рассмотрены в приложении В МЭК 61508-6:2010 и сериях МЭК 61078, МЭК 61025, МЭК 61165, ISA TR 84.00.02.

А.2 Метод блок-схем надежности

МЭК 61078 и приложение В МЭК 61508-6:2010 иллюстрируют метод блок-схем надежности для вычисления вероятностей отказа приборных функций безопасности, разработанных в соответствии с настоящим стандартом.

А.3 Метод анализа дерева отказов

МЭК 61025 и ISA TR 84.00.02-3 иллюстрируют метод анализа дерева отказов для вычисления вероятностей отказа приборных функций безопасности, разработанных в соответствии с настоящим стандартом.

А.4 Метод моделирования Маркова

МЭК 61165 и TR ISA 84.00.02-4 иллюстрируют метод моделирования Маркова для вычисления вероятностей отказа приборных функций безопасности, разработанных в соответствии с настоящим стандартом.

Приложение В
(справочное)

Типовые архитектуры ПЛК-ФБ

В.1 Примеры архитектур подсистем ПЛК-ФБ

Подсистемы ПЛК-ФБ могут иметь различные архитектуры. Дополнительная информация о примерах архитектур представлена в В.3.2.2 и В.3.3.2 МЭК 61508-6.

Архитектура *M* из *N* состоит из каналов *N*, каждый из которых может выполнять функцию безопасности ПЛК-ФБ. Требуется, чтобы, по крайней мере, *M* каналов выполняли функцию безопасности ПЛК-ФБ. Система выполняет функцию безопасности ПЛК-ФБ, если М каналов функционируют должным образом. Значение *N*-*M* определяет отказоустойчивость системы, где (*N* – *M* + 1) — число неисправных каналов, приводящих к отказу функции безопасности ПЛК-ФБ.

Примеры:

Архитектура 1oo1. Отказоустойчивость равна 0, и число каналов равно 1. Данная архитектура состоит из одного канала, и любой опасный отказ приводит к отказу функции безопасности при возникновении запроса на ее выполнение.

Архитектура 1oo2. Отказоустойчивость равна 1, и число каналов равно 2. Данная архитектура представляет собой два канала, соединенных параллельно, так что любой из каналов может выполнить функцию безопасности. Следовательно, для нарушения функции безопасности (при возникновении запроса на ее выполнение) опасные отказы должны возникнуть в обоих каналах. Предполагается, что любое диагностическое тестирование только сообщает о найденных сбоях и не может изменить ни выходные состояния каналов, ни результат голосования.

Архитектура 2oo2. Отказоустойчивость равна 0, и число каналов равно 2. Данная архитектура представляет собой два канала, соединенных параллельно, и для выполнения функции безопасности по запросу необходима работа обоих каналов. Предполагается, что любое диагностическое тестирование только сообщает о найденных неисправностях и не может изменить ни выходные состояния каналов, ни результат голосования

Архитектура 2oo3. Отказоустойчивость равна 1, и число каналов равно 3. Данная архитектура состоит из трех каналов, соединенных параллельно с мажорированием выходных сигналов так, что выходное состояние не меняется, если результат, выдаваемый одним из каналов, отличается от результата, выдаваемого двумя другими каналами. Предполагается, что любое диагностическое тестирование только фиксирует найденные сбои и не может изменить ни выходные состояния каналов, ни результат голосования.

Следующие реализации архитектуры типичны для ПЛК-ФБ.

В.2 Один ПЛК-ФБ с одним входом/выходом и внешним сторожевым таймером (1oo1D)

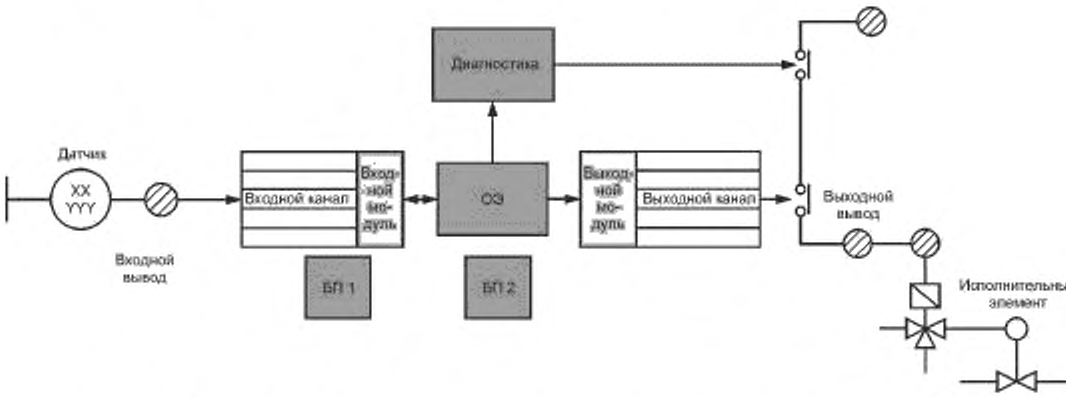


Рисунок В.1 — Один ПЛК-ФБ с одним входом/выходом и внешним сторожевым таймером (1oo1D)

Данная конфигурация не имеет избыточности. Она состоит из одного канала: один обрабатывающий элемент (ОЭ), входной канал (вх. канал) во входном модуле (вх. модуль), выходной канал (вых. канал) в выходном модуле (вых. модуль). Данная конфигурация может включать избыточные блоки питания (БП). Функция внешнего сторожевого таймера (диагностическая) обеспечивает дополнительное средство отключения выходов и переводит управляемый процесс в безопасное состояние. Эта внешняя сторожевая функция отключает дополнительный

выходной контакт, если обнаружен опасный сбой в обрабатывающем элементе (логическом решателе) или в связанном с ним выходном модуле. Выходы показаны как контакты, но могут быть реализованы как полупроводниковые переключатели или другие средства.

Все безопасные сбои приводят к ложному переводу управляемого процесса в безопасное состояние. Все опасные обнаруженные сбои также приводят к ложному переводу управляемого процесса в безопасное состояние, так как система должна быть отключена, чтобы заменить любой из неисправных модулей.

В.3 Два обрабатывающих элемента (ОЕ) с одним входом/выходом и внешними сторожевыми таймерами (1oo1D)

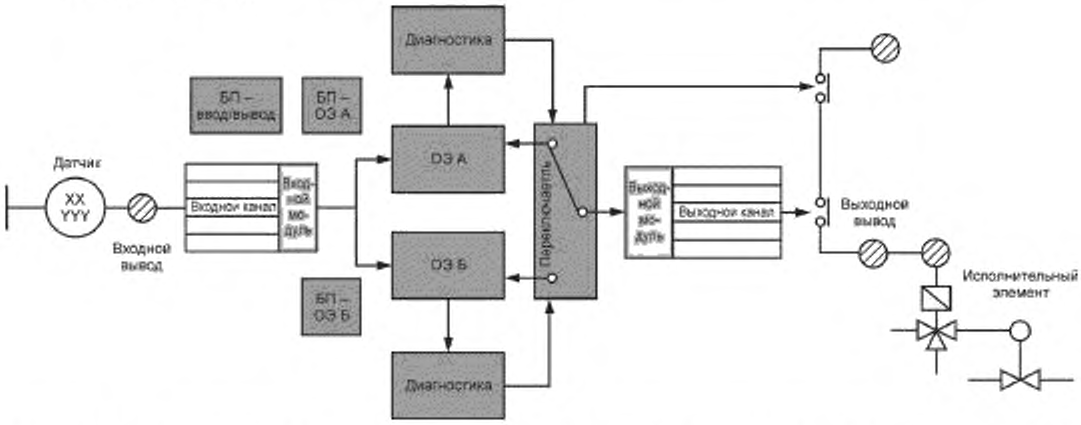


Рисунок В.2 — Два обрабатывающих элемента (ОЭ) с одним входом/выходом и двумя внешними сторожевыми таймерами (1oo1D)

Данная конфигурация имеет избыточные элементы обработки и внешние сторожевые таймеры. Представленным на рисунке переключателем управляют функции сторожевых таймеров, которые контролируют результаты диагностики обрабатывающих элементов. Дополнительные средства отключат питание выходных устройств, если на оба входа переключателя от диагностических устройств поступит сигнал об отключении. Переключатель периодически меняет свою позицию так, чтобы его функциональность и функциональность и диагностики каждого обрабатывающего элемента могли быть проверены в другой позиции. Результаты двух обрабатывающих элементов сравнивают, и если обнаружено несоответствие, то оба сторожевых таймера формируют команду отключить выходы. Следовательно, любое несоответствие между обрабатывающими элементами приведет к отключению выходов, чтобы перевести управляемый процесс в безопасное состояние. Обнаруженные сбои в любом из отдельных модулей входа/выхода также приведут к отключению выходов. Безопасные не обнаруживаемые сбои обрабатывающего элемента, а также ошибки упомянутого выше процесса сравнения приведут к ложному переводу управляемого процесса в безопасное состояние, другие обнаруживаемые безопасные и опасные сбои любого обрабатывающего элемента могут быть исправлены в неавтономном режиме.

Если опасный сбой процессора, управляющего выходами, будет не обнаружен, то система безопасности будет в состоянии отказа.

В.4 Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, без межпроцессорной связи и с логикой срабатывания 1oo2

Представленная на рисунке В.3 конфигурация имеет два независимых канала. Между обрабатывающими элементами нет никакой связи. Охват диагностикой определен охватом диагностикой, достигаемым в одноканальной системе. Выходы одного канала с его исполнительным элементом соединены последовательно с выходами другого канала, и, следовательно, каждый канал может разомкнуть выходную схему и перевести управляемый процесс в безопасное состояние. Каждый обрабатывающий элемент будет давать команду своему выходу о переходе к безопасному состоянию, если на какой-либо вход приходит сигнал, соответствующий опасному событию, или если обнаружен опасный сбой в любом из модулей в канале. У представленной конфигурации нет внешних сторожевых таймеров, так как выходы от каждого канала соединены последовательно.

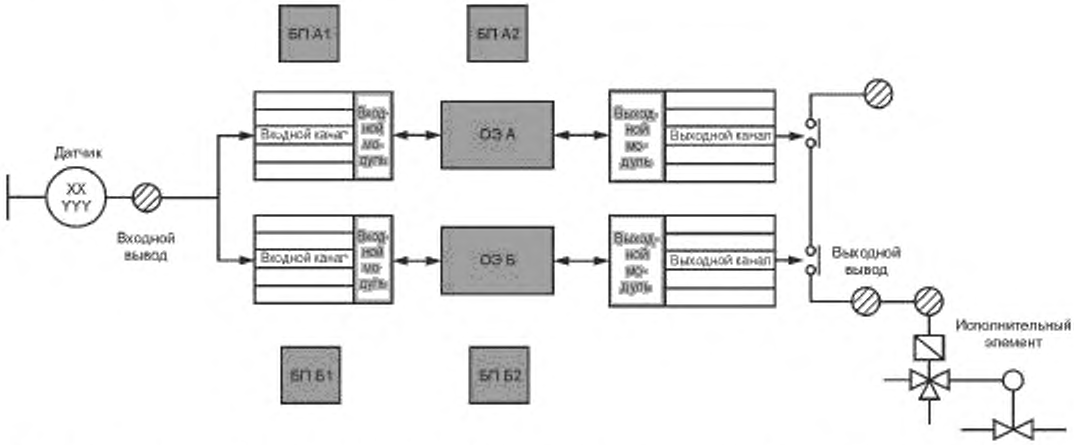


Рисунок В.3 — Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, без межпроцессорной связи и с логикой срабатывания 1oo2

Все безопасные сбои и опасные обнаруживаемые сбои в системе приводят к ложному переводу управляемого процесса в безопасное состояние.

В.5 Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, с межпроцессорной связью и логикой срабатывания 1oo2D

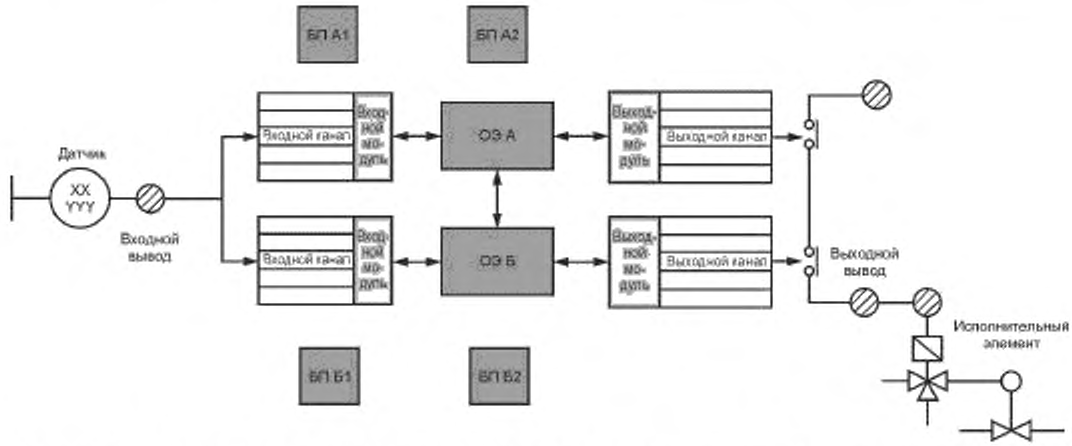


Рисунок В.4 — Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, с межпроцессорной связью и логикой срабатывания 1oo2D

Представленная на рисунке В.4 конфигурация также имеет два независимых канала. У нее есть связь между обрабатывающими элементами. Такая связь повышает общий охват диагностикой обрабатывающих элементов в результате сравнительного тестирования, которое может быть выполнено. Связь между процессорами также позволяет им сравнивать входные значения и продолжать работу с работоспособным входом, если обнаружен сбой на другом входе. Все другие безопасные сбои и все опасные обнаруживаемые сбои в системе приводят к ложному отключению управляемого процесса.

В.6 Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, без межпроцессорной связи, с внешними сторожевыми таймерами и логикой срабатывания 2oo2D

Данная конфигурации имеет два независимых 1oo1D канала. Между обрабатывающими элементами нет никакой связи. Выходы исполнительных элементов каждого канала соединены параллельно, чтобы сократить число ложных или случайных отключений. Следовательно, оба канала должны сформировать команду на отключение,

чтобы обесточить цепь исполнительного элемента. Такое соединение обеспечивает голосование выходов каждого канала по схеме 2oo2D. Для повышения уровня безопасности система в каждом канале имеет внешний сторожевой таймер. Эти сторожевые таймеры являются дополнительными средствами обесточивания выходной схемы канала, если обнаруживается опасный сбой в логическом решателе или выходном модуле.

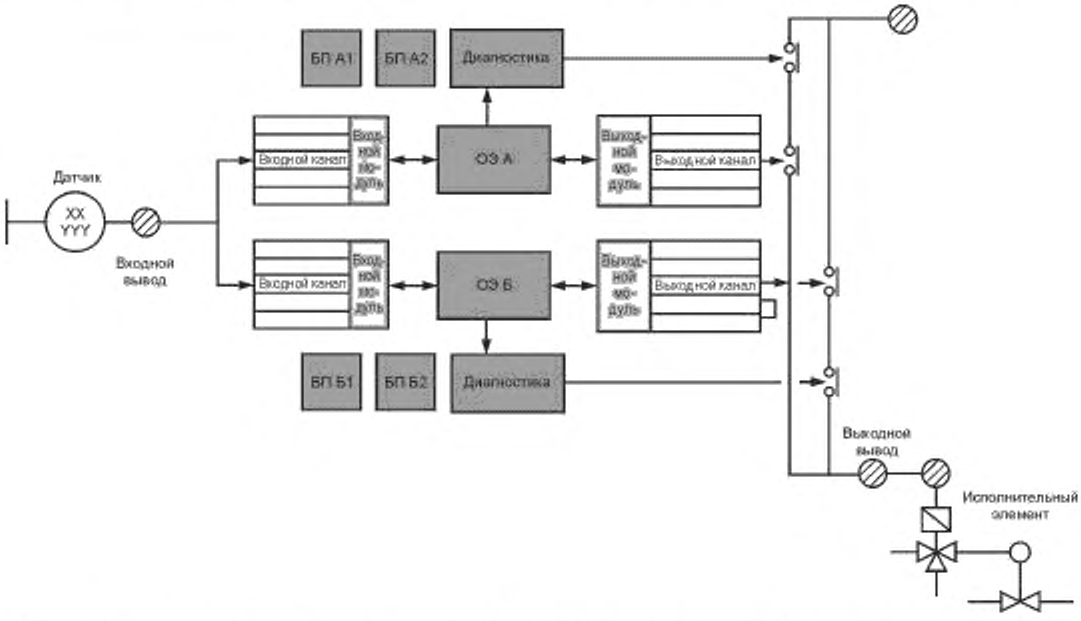


Рисунок В.5 — Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, без межпроцессорной связи, с внешними сторожевыми таймерами и логикой срабатывания 2oo2D.

Все опасные необнаруживаемые сбои в любом модуле любого канала системы переводят систему в состояние отказа.

В.7 Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, с межпроцессорной связью, с внешними сторожевыми таймерами и логикой срабатывания 2oo2D

Данная конфигурация с резервированием имеет два независимых канала. У системы есть связь между обрабатывающими элементами. Выходы исполнительных элементов каждого канала соединены параллельно, чтобы сократить число ложных или случайных отключений. Следовательно, оба канала должны сформировать команду на отключение, чтобы обесточить цепь исполнительного элемента. Для повышения уровня безопасности система в каждом канале или участке цепи имеет внешние сторожевые таймеры. Эти сторожевые таймеры являются дополнительными средствами обесточивания выходной схемы канала, если обнаруживается опасный сбой в логическом решателе. Межпроцессорная связь улучшает диагностическую способность, так как могут быть выполнены сравнения между состояниями выходов двух каналов.

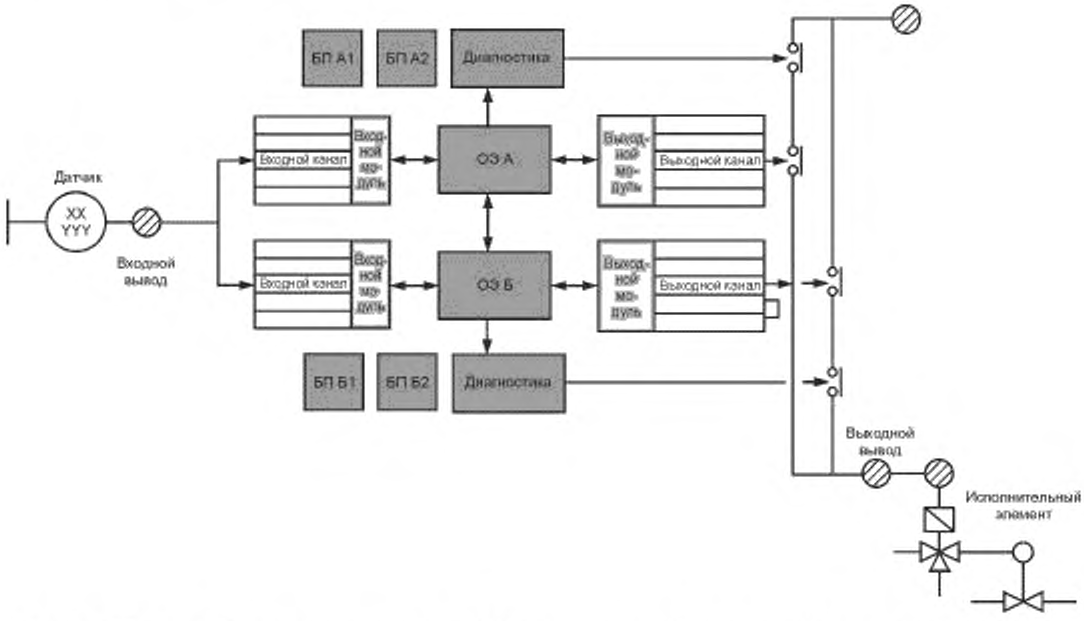


Рисунок В.6 — Два обрабатывающих элемента (ОЭ) с двумя входами/выходами, с межпроцессорной связью, с внешними сторожевыми таймерами и логикой срабатывания 2oo2D

Все обнаруживаемые сбои в этой системе, которые могут быть локализованы в канале, могут быть устранены в неавтономном режиме.

В.8 Три обрабатывающих элемента (ОЭ) с тремя входами/выходами, с межпроцессорной связью и логикой срабатывания 2oo3D

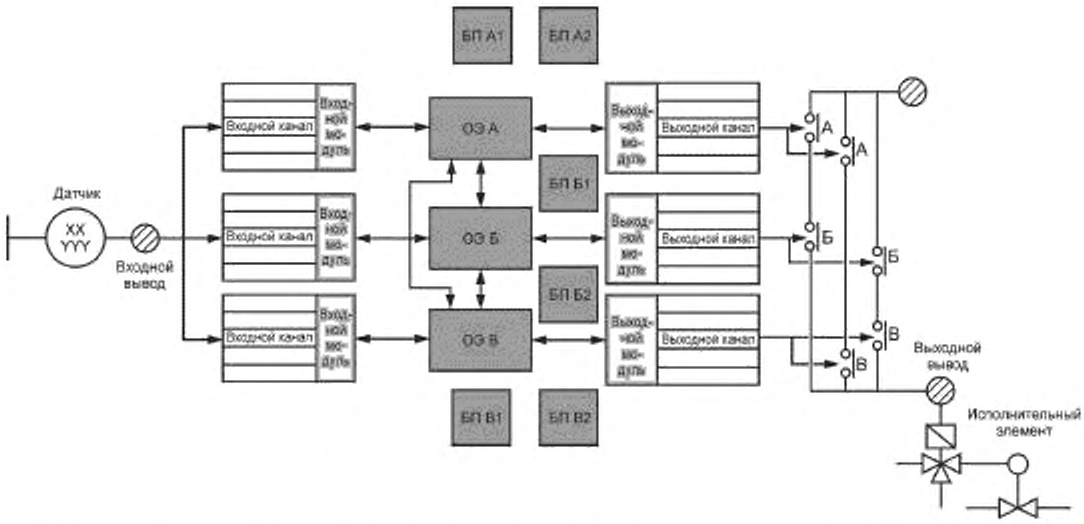


Рисунок В.7 — Три обрабатывающих элемента (ОЭ) с тремя входами/выходами, с межпроцессорной связью и логикой срабатывания 2oo3D

Данная конфигурация с резервированием имеет три канала с межпроцессорной связью. Каждый выход к исполнительному элементу использует отказоустойчивую схему голосования для шести выходов, которая выполняет

голосование по схеме 2oo3 D для трех входов. Используя межпроцессорную связь, процессоры могут выполнить голосование по схеме 2oo3 D значений датчика, считанных системой. На результаты голосования по схеме 2oo3 D не повлияет наличие одного сбоя в любом из этих трех голосующих участков или каналов. Любой обнаруженный безопасный или опасный сбой в системе с тройным резервированием может быть устранен в неавтономном режиме, не останавливая управляемый процесс.

Приложение С
(справочное)

ПЛК-ФБ в системах, реализующих срабатывание защиты при подаче питания

С.1 Общие положения

Результатом действия большинства функций безопасности по запросу является отключение подачи питания для срабатывания защиты. Другими словами, исполнительные устройства обесточиваются по запросу к функции безопасности.

Напротив, результатом действия ряда функций безопасности является подача питания для срабатывания защиты. То есть, при запросе к функции безопасности на исполнительные устройства подается питание.

Срабатывание защиты при подаче питания часто применяется при смягчении последствий опасного события, а не для его предотвращения. Типичными применениями являются противопожарная и газовая защита, например звуковой аварийный сигнал об эвакуации или включение противопожарного предохранительного клапана.

Запросы к ПЛК-ФБ, используемые в применениях, реализуемых срабатывание защиты при подаче питания, очень разнообразны и более серьезны. Если ПЛК-ФБ должен потенциально использоваться в применениях, реализуемых срабатывание защиты при подаче питания, то производитель должен рассмотреть это и обеспечить конкретные данные об отказах и инструкции использования таких применений.

С.2 Безопасное состояние и состояние запроса

Для применений, реализуемых срабатывание защиты при отключении питания, состояние при запросе функции безопасности является обычно таким же, как и заданное безопасное состояние — исполнительные устройства обесточены. Для применений, реализуемых срабатывание защиты при подаче питания, при запросе на выход(ы) подается питание, но в заданном безопасном состоянии обычно исполнительные устройства обесточены. Следовательно, действие, выполняемое при обнаружении сбоя, отличается от действия, выполняемого в случае запроса функции безопасности.

В конкретных применениях это необходимо, например неуправляемый выпуск огнегасящего средства из-за внутреннего сбоя, который сам может быть серьезной опасностью.

С.3 Дополнительная информация, необходимая для использования в применениях, реализуемых срабатывание защиты при подаче питания

Пользователю должна быть дополнительно предоставлена следующая информация:

- интенсивность случайных отказов аппаратных средств, реализующих срабатывание защиты при подаче питания. Модель надежности ПЛК-ФБ (см. 9.4.3), реализующего срабатывание защиты при подаче питания, вероятно, будет иной и, чтобы определить интенсивность отказов, возможно, должен быть выполнен отдельный FMEA. Необходимо отметить, что интенсивность отказов срабатывания защиты, вероятно, будет намного выше для срабатывания защиты при подаче питания;
- любое отличие для систематической полноты безопасности ПЛК-ФБ при работе в режиме срабатывания защиты при подаче питания;
- любые конкретные условия эксплуатации или рекомендуемые меры по смягчению сбоя, которые должны соблюдать при выполнении срабатывания защиты при подаче питания;
- различие между действием ПЛК-ФБ по запросу и действием по обнаружению неисправности должно быть выявлено.

С.4 Дополнительные соображения

Производитель и пользователь ПЛК-ФБ должны обратить особое внимание на следующее:

- ПЛК-ФБ особенно зависит от технического состояния источника питания в применениях, реализуемых срабатывание защиты при подаче питания. Отказ источника питания приведет к неспособности ПЛК-ФБ ответить на запрос. Кроме того, ПЛК-ФБ может быть не в состоянии указать на то, что он находится в состоянии отказа;
- рекомендуется использование независимых, избыточных источников питания. Отказы по общей причине в источниках питания или в системе электропитания должны быть тщательно рассмотрены;
- для противопожарной и газовой защиты необходимо рассмотреть соответствие с другими специфичными для области применения правилами и стандартами, например EN54 и NFPA72;
- сбои в схеме питания исполнительного устройства и устройств на объекте, вероятно, помешают исполнительному устройству выполнить защиту при подаче питания в случае работы по запросу. Для обнаружения таких отказов рекомендуется мониторинг (контроль) такой схемы, что обеспечит срабатывание защиты при подаче питания.

Приложение D
(справочное)

Доступные базы данных интенсивностей отказов

D.1 Базы данных

Представленный ниже список не является исчерпывающим, он не упорядочен и включает источники данных интенсивностей отказов для электронных и неэлектронных компонентов. Необходимо отметить, что перечисленные источники не всегда согласуются друг с другом, и поэтому необходимо быть внимательным при применении представленных в них данных.

IEC/TR 62380, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment. Union Technique de l'Electricité et de la Communication (gost.e-ecolog.ru al to RDF 2000/ Reliability Data Handbook, UTEC 80-810.

Siemens Standard SN 29500, Failure rates of components, (parts 1 to 14); Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.

Telcordia SR-332, Issue 01: May 2001, Reliability Prediction Procedure for Electronic Equipment, (telecom-info. telcordia.com), (Bellcore TR-332, Issue 06).

EPRD (RAC-STD-6100) — Electronic Parts Reliability Data, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).

NNPRD-95 (RAC-STD-6200) — Non-electronic Parts Reliability Data, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

HRD5, British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom

Chinese Military/Commercial Standard GJB/z 299B, Electronic Reliability Prediction, (http://gost.e-ecolog.ru china299b.html)

ISBN:0442318480, AT&T reliability manual — Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors, AT&T Reliability Manual, Van Nostrand Reinhold, 1990.

FIDES:January, 2004, Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA. FIDES is available on request at gost.e-ecolog.ru

IEEE Gold book — The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems provides data concerning equipment reliability used in industrial and commercial power distribution systems. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada), FAX: +1 732 981 9667 e-mail: customer. gost.e-ecolog.ru

IRPH ITALTEL, Reliability Prediction Handbook — The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy. This is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed.

PRISM (RAC / EPRD) — The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

D.2 Полезные стандарты, связанные с отказами компонентов

Следующие стандарты содержат информацию, связанную с отказами компонентов.

IEC 60300-3-2, Dependability management — Part 3-2: Application guide — Collection of dependability data from the field.

IEC 60300-3-5, Dependability management — Part 3-5: Application guide — Reliability test conditions and statistical test principles.

IEC 60319, Presentation and specification of reliability data for electronic components.

IEC 60706-3, Maintainability of equipment — Part 3: Verification and collection, analysis and presentation of data.

IEC 60721-1, Classification of environmental conditions — Part 1: Environmental parameters and their severities.

IEC 61709, Electronic components — Reliability — Reference conditions for failure rates and stress models for conversion.

IEC 62061:2005, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems.

Примечание — Дополнительная информация о видах отказов электрических/электронных компонентов представлена в приложении D.

Приложение Е
(справочное)

Методология оценки интенсивности отказов по общей причине в многоканальном ПЛК-ФБ

Е.1 Общие положения

Данное приложение представляет простой качественный подход для оценки интенсивности отказов по общей причине, который может быть применен при проектировании ПЛК-ФБ.

Оценка отказов по общей причине (ООП) также приведена в приложении D МЭК 61508-6.

Е.2 Методология

Должна быть выполнена оценка проекта многоканальной части канала или частей ПЛК-ФБ, чтобы установить эффективность мер, используемых для защиты от отказов по общей причине. Должны быть идентифицированы применимые мероприятия из таблицы Е.1 и определена общая оценка, которую используют, чтобы определить фактор отказов по общей причине из таблицы Е.2 как процентное значение.

Таблица Е.1 — Критерии оценки отказов по общей причине

Мероприятия	Оценка
Разделение/выделение	
Действительно ли все элементы канала физически отделены, например расположены на физически отдельных печатных платах?	5
Все элементы канала заключены в отдельные экранированные корпуса?	5
Действительно ли входы к каналам абсолютно отделены, например нет никакого общеиспользуемого резистора?	5
Являются ли используемые для каждого канала шины данных входа/выхода отдельными и независимыми?	5
Устранена ли, кроме передачи диагностической информации, перекрестная связь или передача данных между каналами?	5
Диверсификация/избыточность	
Независимы ли диагностические тесты одного канала от работы другого канала?	5
Используют ли каналы преднамеренные различия по времени при выполнении функций (временное разнообразие) для снижения риска совпадающих отказов?	10
Используется ли различное отдельно разработанное встроенное программное обеспечение в различных каналах?	10
Является ли интервал диагностических проверок каждого канала меньше 1 мин?	10
По крайней мере один канал использует существенно отличную технологию от другого(их) канала(ов), например, в одном канале реле электромагнитное, а в другом(их) оно электронное?	10
Проектирование	
Имеют ли шины данных входа-выхода эффективные средства обнаружения ошибок?	5
Имеется ли у разработчиков ПЛК-ФБ предыдущий опыт устранения отказов по общей причине?	5
Оценка/анализ	
Использовался ли анализ видов и последствий отказов аппаратных средств во время процесса проектирования для идентификации и устранения источников отказов по общей причине?	10
Был ли многоканальный проект детально рассмотрен компетентным персоналом, независимым от команды разработчиков?	10
Проверка влияния окружающей среды	
Существуют ли меры для обнаружения и реакции на повышенную температуру?	5
Выполнены ли тесты на ЭМС для более высоких, а не стандартных промышленных уровней?	10
Существует ли какая-либо существенная дополнительная защита от неблагоприятного воздействия окружающей среды?	5

Используя таблицу Е.1, выбирают те мероприятия, которые будут наиболее эффективно влиять на многоканальный проект. Затем значения оценок выбранных мероприятий складывают, чтобы получить общую оценку для проекта ПЛК-ФБ. Если для предотвращения отказов по общей причине в проекте ПЛК-ФБ использовались эквивалентные мероприятия, тогда соответствующая оценка может требоваться при условии, что эквивалентность мероприятий обоснована.

Полученную общую оценку с помощью таблицы Е.2 можно использовать для определения фактора отказов по общей причине β (β-фактор).

Таблица Е.2 — Оценка фактора отказов по общей причине

Общая оценка	Фактор отказов по общей причине β
Менее 45	5 % (0,05)
От 45 до 70	2 % (0,02)
Более 70	1 % (0,01)

Интенсивность отказов по общей причине для опасных необнаруживаемых отказов определяют умножением интенсивности опасных необнаруживаемых случайных отказов аппаратных средств для одного канала на фактор отказа по общей причине β.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60947-5-1:2003	MOD	ГОСТ 30011.5.1—2012 «Аппаратура распределения и управления низковольтная. Часть 5. Аппараты и коммутационные элементы цепей управления. Глава 1. Электромеханические аппараты для цепей управления»
МЭК/ТС 61000-1-2:2008	—	*
IEC 61000-4-2:2008	MOD	ГОСТ Р 51317.4.2—2010 «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний»
МЭК 61000-4-3:2006	—	*
МЭК 61000-4-4:2012	—	*
МЭК 61000-4-5:2005	—	*
МЭК 61000-4-6:2008	—	*
МЭК 61000-4-8:2009	—	*
МЭК 61131-1:2003	—	*
МЭК 61131-2:2007	—	*
МЭК 61131-4:2004	—	*
МЭК 61326-3-1:2008	—	*
МЭК 61326-3-2:2008	—	*
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/программируемым электронным, связанным с безопасностью»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-6:2010	IDT	ГОСТ Р МЭК 61508-6—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3»
МЭК 61784-3	—	*
МЭК 62443 (все части)	—	*
МЭК Руководство 104:1997	—	*

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898–2002 «Аспекты безопасности. Правила включения в стандарты»
ЕН 50205:2002	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

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

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

[1] IEC 60050-191:1990, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service

[2] IEC 60300-3-2:2004, Dependability management — Part 3-2: Application guide — Collection of dependability data from the field

[3] IEC 61000 (all parts), Electromagnetic compatibility (EMC)

[4] IEC 61025:2006, Fault tree analysis (FTA)

[5] IEC 61069-7:1999, Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Part 7: Assessment of system safety

[6] IEC 61078:2006, Analysis techniques for dependability — Reliability block diagram and boolean methods

[7] IEC 61131-3:2003, Programmable controllers — Part 3: Programming languages

[8] IEC 61165:2006, Application of Markov techniques

[9] IEC 61496-1:2008, Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests

[10] IEC 61496-3:2008, Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)

[11] IEC 61506:1997, Industrial-process measurement and control — Documentation of application software

[12] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

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

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

[15] IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

[16] IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector

[17] IEC 61511-1:2003, Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements

[18] IEC 61511-2:2003, Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1

[19] IEC 61511-3:2003, Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels electronic and programmable electronic control systems

[20] IEC 62079:2001, Preparation of instructions — Structuring, content and presentation

[21] IEC/TR 62380:2004, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment

[22] IEC Guide 104:2010, The preparation of safety publications and the use of basic safety publications and group safety publications

[23] CISPR 11:2009, Industrial, scientific and medical equipment — Radio-frequency disturbance characteristics — Limits and methods of measurement

[24] ISO/IEC 2382 (all parts), Information technology — Vocabulary

[25] ISO/IEC 2382-1, Information technology — Vocabulary — Part 1: Fundamental terms

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

[27] ISO/IEC 12207:2008, Systems and software engineering — Software life cycle processes

[28] ISO 8402:1994, Quality management and quality assurance — Vocabulary

[29] ISO 9000-3:1997, Quality management and quality assurance standards — Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software

[30] ISO 9001:2008, Quality management systems — Requirements

[31] ISO 13849-1:2006, Safety of Machinery — Safety-related parts of control systems — Part 1: General principles for design

[32] ISO 13849-2:2003, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

[33] ISO 14224:2006, Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment

[34] IEEE 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

[35] IEEE 828-2005, IEEE Standard for Software Configuration Management Plans

[36] IEEE 1042-1987, IEEE Guide to Software Configuration Management

[37] ISA TR 84.00.02:2002, Part-1, Safety Instrumented Function (SIF) — Safety Integrity Level

УДК 62-783:614.8:331.454:006.354

ОКС 25.040.40
35.240.50

Ключевые слова: функциональная безопасность; программируемый логический контроллер; логическая подсистема; стадии жизненного цикла системы безопасности; анализ системы безопасности; анализ уровня полноты безопасности; периферийные устройства

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

Сдано в набор 12.01.2016. Подписано в печать 08.02.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 9,77. Уч.-изд. л. 9,40. Тираж 33 экз. Зак. 224.

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

gost.e-ecolog.ru