ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-4— 2012

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 4

Термины и определения

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

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0–2004 «Стандартизации в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» и Федеральным государственным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации — «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 29 октября 2012 г. № 589-ст

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

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5)

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

4 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 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.ru)

© Стандартинформ, 2014

В Российской Федерации 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

Сведения о стандарте II
1 Область применения 1
2 Нормативные ссылки 2
3 Термины, определения и сокращения 3
3.1 Термины, относящиеся к безопасности 4
3.2 Оборудование и устройства 5
3.3 Системы: общие аспекты 8
3.4 Системы: аспекты, связанные с безопасностью 10
3.5 Функции безопасности и полнота безопасности 12
3.6 Сбой, отказ и ошибка 14
3.8 Подтверждение мер по обеспечению безопасности 20
Приложение А (справочное) Указатель терминов 24
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 27
Библиография 28

Введение

Системы, состоящие из электрических и/или электронных элементов, в течение многих лет используются для выполнения функций безопасности в большинстве областей применения. Компьютерные системы (обычно называемые «программируемые электронные системы»), применяемые во всех прикладных отраслях для выполнения функций, не связанных с безопасностью, во все более увеличивающихся количествах используются для выполнения функций обеспечения безопасности. Для эффективной и безопасной эксплуатации технологий, основанных на использовании компьютерных систем, чрезвычайно важно, чтобы лица, ответственные за принятие решений, имели в своем распоряжении руководства по вопросам безопасности, которые они могли бы использовать в своей работе.

Настоящий стандарт устанавливает общий подход к вопросам обеспечения безопасности для всего жизненного цикла систем, состоящих из электрических и/или электронных, и/или программируемых электронных (Э/Э/ПЭ) элементов, которые используются для выполнения функций обеспечения безопасности. Этот унифицированный подход был принят для разработки рациональной и последовательной технической политики для всех электрических систем обеспечения безопасности. При этом основной целью является содействие разработке стандартов для продукции и областей применения на основе стандартов серии МЭК 61508.

Примечание — Примерами стандартов для продукции и областей применения, разработанных на основе стандартов серии МЭК 61508, являются [1] — [3].

Обычно безопасность достигается за счет использования нескольких систем, в которых используются различные технологии (например, механические, гидравлические, пневматические, электрические, электронные, программируемые электронные). Любая стратегия безопасности должна, следовательно, учитывать не только все элементы, входящие в состав отдельных систем (например, датчики, управляющие устройства и исполнительные механизмы), но также и все подсистемы безопасности, входящие в состав общей системы обеспечения безопасности. Таким образом, хотя настоящий стандарт посвящен в основном Э/Э/ПЭ системам, связанным с безопасностью, он может также предоставлять общий подход, в рамках которого рассматриваются системы, связанные с безопасностью, базирующиеся на других технологиях.

Признанным фактом является существование огромного разнообразия использования Э/Э/ПЭ систем в различных областях применения, отличающихся различной степенью сложности, возможными рисками и опасностями. В каждом конкретном применении необходимые меры безопасности будут зависеть от многочисленных факторов, специфичных для конкретного применения. Настоящий стандарт, являясь базовым, позволит формулировать такие меры для областей применения будущих международных стандартов, а также для последующих редакций уже существующих стандартов.

Настоящий стандарт:

- рассматривает все соответствующие стадии жизненного цикла безопасности систем в целом, а также подсистем Э/Э/ПЭ системы и программного обеспечения (например, от первоначальной концепции, через проектирование, внедрение, эксплуатацию и техническое обеспечение до снятия с эксплуатации), в ходе которых Э/Э/ПЭ системы используются для выполнения функций безопасности;
- был задуман с учетом быстрого развития технологий; его основа является в значительной мере устойчивой и полной для будущих разработок;
- делает возможной разработку стандартов областей применения, в которых используются Э/Э/ПЭ системы, связанные с безопасностью; разработка стандартов для областей применения в рамках общей структуры, вводимой настоящим стандартом, должна привести к более высокому уровню согласованности (например, основных принципов, терминологии и т.д.) как для отдельных областей применения, так и для их совокупностей, что даст преимущества в плане безопасности и экономики;
- предоставляет метод разработки спецификации требований к безопасности, необходимых для достижения заданной функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью;
- использует для определения требований к уровням полноты безопасности подход, основанный на оценке рисков;
- вводит уровни полноты безопасности для определения целевого уровня полноты безопасности для функций безопасности, которые должны быть реализованы Э/Э/ПЭ системами, связанными с безопасностью.

Примечание — Настоящий стандарт не устанавливает требований к уровню полноты безопасности для любой функции безопасности и не определяет то, как устанавливается уровень полноты безопасности. Однако настоящий стандарт формирует основанный на риске концептуальный подход и приводит примеры методов;

- устанавливает целевые меры отказов для функций безопасности, реализуемых Э/Э/ПЭ системами, связанными с безопасностью, и связывает эти меры с уровнями полноты безопасности;

- устанавливает нижнюю границу для целевых мер отказов для функции безопасности, реализуемой одиночной Э/Э/ПЭ системой, связанной с безопасностью. Для Э/Э/ПЭ систем, связанных с безопасностью в режиме:

- низкой интенсивности запросов на обслуживание: нижняя граница для выполнения функции, для которой система предназначена, устанавливается в соответствии со средней вероятностью опасного отказа по запросу, равной 10^{-5},

- высокой интенсивности запросов на обслуживание или в непрерывном режиме: нижняя граница устанавливается в соответствии со средней частотой опасных отказов 10^{-9} в час.

Примечания

1 Одиночная Э/Э/ПЭ система, связанная с безопасностью, не обязательно предполагает одноканальную архитектуру.

2 В проектах систем, связанных с безопасностью и имеющих низкий уровень сложности, можно достигнуть более низких значений целевой полноты безопасности, но предполагается, что в настоящее время указанные предельные значения целевой полноты безопасности могут быть достигнуты для относительно сложных систем (например, программируемые электронные системы, связанные с безопасностью);

- устанавливает требования по предотвращению и управлению систематическими отказами, основанные на опыте и заключениях из практического опыта. Учитывая, что вероятность возникновения систематических отказов, в общем случае, не может быть определена количественно, настоящий стандарт позволяет утверждать для специфицируемой функции безопасности, что целевая мера отказов, связанных с этой функцией, может считаться достигнутой, если все требования стандарта были выполнены;

- вводит понятие «стойкость к систематическим отказам», применяемое к элементу, характеризующее уверенность в том, что полнота безопасности, касающаяся систематических отказов элемента, соответствует требованиям заданного уровня полноты безопасности;

- применяет широкий диапазон принципов, методов и средств для достижения функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, но не использует явно понятие «безопасный отказ». В то же время, понятия «безопасный отказ» и «безопасный в своей основе отказ» могут быть использованы, но для этого необходимо обеспечить соответствующие требования в конкретных разделах стандарта, которым эти понятия должны соответствовать.

Поправка к ГОСТ Р МЭК 61508-4—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

В каком месте	Напечатано	Должно быть
Сведения о стандарте. Пункт 4	ВВЕДЕН ВПЕРВЫЕ	ВЗАМЕН ГОСТ Р МЭК 61508-4—2007
Библиографические данные	13.110	25.040.40; 29.020

(ИУС № 4 2015 г.)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 4

Термины и определения

Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 4. Terms and definitions

Дата введения — 2013—08—01

1 Область применения

1.1 Настоящий стандарт содержит определения и объяснения терминов, которые используются в частях 1 — 7 МЭК 61508.

1.2 Определения сгруппированы в соответствии с общими заголовками так, чтобы близкие по смыслу термины могли быть поняты в пределах общего контекста. Однако заголовки не расширяют значения определений.

1.3 МЭК 61508-1, МЭК 61508-2, МЭК 61508-3 и МЭК 61508-4 являются базовыми стандартами по безопасности, хотя этот статус не применим в контексте Э/Э/ПЭ систем, связанных с безопасностью, имеющих низкую сложность (см. 3.4.3). В качестве базовых стандартов по безопасности, данные стандарты предназначены для использования техническими комитетами при подготовке стандартов в соответствии с принципами, изложенными в руководстве МЭК 104 и руководстве ИСО/МЭК 51. Следующие МЭК 61508-1, МЭК 61508-2, МЭК 61508-3 и МЭК 61508-4 предназначены для использования в качестве самостоятельных стандартов. Функция безопасности настоящего стандарта не применима к медицинскому оборудованию, соответствующему требованиям серии горизонтальных стандартов МЭК 60601 [4].

1.4 В круг обязанностей технического комитета входит использование (там, где это возможно) основополагающих стандартов по безопасности при подготовке собственных стандартов. В этом случае требования, методы проверки или условия проверки настоящего основополагающего стандарта по безопасности не применяют, если на них нет конкретной ссылки или они не включены в стандарты, подготовленные этими техническими комитетами.

1.5 Общая структура стандартов серии МЭК 61508 и роль, которую играет настоящий стандарт в достижении функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, показана на рисунке 1.

Издание официальное

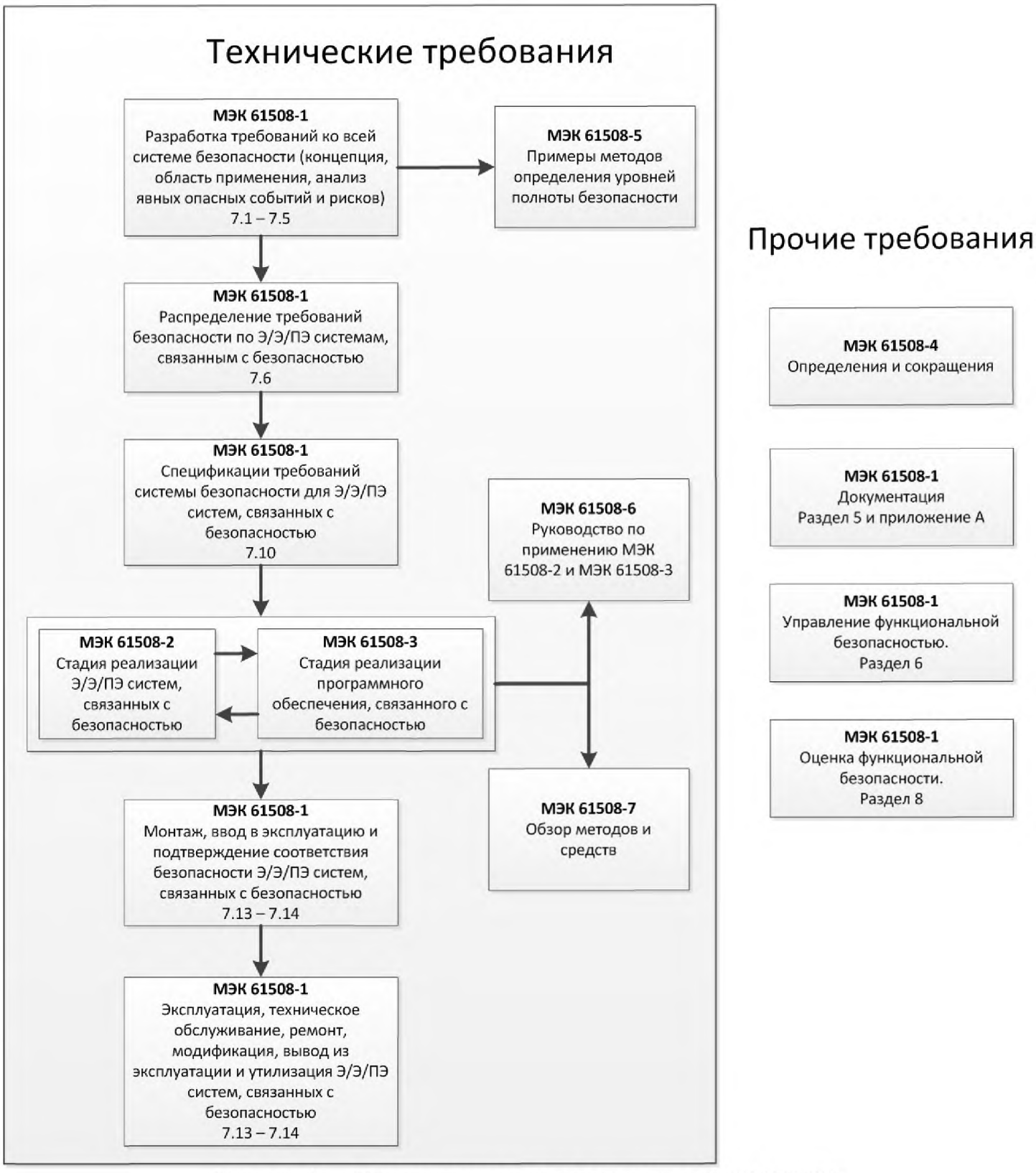


Рисунок 1 — Общая структура стандартов серии МЭК 61508

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

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)

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

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 (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)

3 Термины, определения и сокращения

В настоящем стандарте применимы термины, определения и сокращения в соответствии с таблицей 1, а также следующие термины с соответствующими определениями.

Таблица 1 — Сокращения, используемые в настоящем стандарте

Сокращение	Полное название	Пункт или раздел настоящего стандарта, в котором дано определение и/или объяснение термина
ALARP	Низкий, насколько это возможно	МЭК 61508-5, приложение С
ASIC	Специализированная интегральная схема	3.2.15
CCF	Отказ по общей причине	3.6.10
CPLD	Сложное программируемое логическое устройство	—
DC	Охват диагностикой	3.8.6
(E)EPLD	Электрически программируемое логическое устройство	—
E/E/PE	Электрическая/электронная/программиру-емая электроника	3.2.13, например: Э/Э/ПЭ система, связанная с безопасностью
E/E/PE система	Электрическая/электронная/программиру-емая электронная система	3.3.2
EEPROM	Перепрограммируемая постоянная память, стираемая электрически	—
EPROM	Перепрограммируемая постоянная память, стираемая ультрафиолетом	—
EUC	Управляемое оборудование	3.2.1
FPGA	Вентильная матрица, программируемая пользователем	—
GAL	Перепрограммируемая матричная логика	—
HFT	Отказоустойчивость аппаратных средств	МЭК 61508-2, 7.4.4
MooN	Канальная архитектура M из N (например, 1oo2 представляет собой канальную архитектуру 1 из 2)	МЭК 61508-6, приложение В
MooND	Канальная архитектура M из N с диагностикой	МЭК 61508-6, приложение В
MTBF	Среднее время между отказами	3.6.19, примечание 3

Окончание таблицы 1

Сокращение	Полное название	Пункт или раздел настоящего стандарта, в котором дано определение и/или объяснение термина
MTTR	Среднее время восстановления	3.6.21
MRT	Среднее время ремонта	3.6.22
PAL	Программируемая матричная логика	—
PE	Программируемая электроника	3.2.12
PE(system)	Программируемая электронная (система)	3.3.1
PFD	Вероятность опасных отказов по запросу	3.6.17
PFD_{avg}	Средняя вероятность опасных отказов по запросу	3.6.18
PFH	Средняя частота опасных отказов (в час)	3.6.19
PLA	Программируемая логическая матрица	—
PLC	Программируемый логический контроллер	МЭК 61508-6, приложение E
PLD	Программируемое логическое устройство	—
PLS	Программируемое логическое синхронизирующее устройство	—
PML	Программируемая макрологика	—
RAM	Запоминающее устройство с произвольным доступом	—
ROM	Постоянное запоминающее устройство	—
SFF	Доля безопасных отказов	3.6.15
SIL	Уровень полноты безопасности	3.5.8
VHDL	Язык описания технических средств на быстродействующих интегральных схемах	МЭК 61508-2, приложение F, примечание к перечислению f)

3.1 Термины, относящиеся к безопасности

3.1.1 **вред** (harm): Физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде.

[ИСО/МЭК Руководство 51:1999, определение 3.3].

3.1.2 **опасность** (hazard): Потенциальный источник причинения вреда

[ИСО/МЭК Руководство 51: 1999, определение 3.5].

Примечание — Термин включает в себя возможную опасность для людей в короткий промежуток времени (например, при пожаре и взрыве), а также опасность, имеющую долгосрочное воздействие на здоровье людей (например, при утечке токсического вещества).

3.1.3 **опасная ситуация** (hazardous situation): Обстоятельства, при которых люди, имущество или окружающая среда подвергаются одной или нескольким опасностям.

3.1.4 **опасное событие** (hazardous event): Событие, в результате которого может быть причинен вред.

Примечание — Причинение вреда в результате опасного события зависит от того, подвергаются ли люди, имущество или окружающая среда воздействию последствий опасного события, и, если причинение людям вреда возможно, то могут ли они избежать последствий события после того, как оно произошло.

3.1.5 **причиняющее вред событие** (harmful event): Событие, при котором в результате опасной ситуации либо опасного события причиняется вред.

Примечание — ИСО/МЭК Руководство 51: 1999, определение 3.4, адаптированное с учетом определения опасного события.

3.1.6 **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.

3.1.7 **допустимый риск** (tolerable risk): Риск, который приемлем при данных обстоятельствах на основании существующих в обществе ценностей.
[ИСО/МЭК Руководство 51:1999, определение 3.7].

Примечание — См. МЭК 61508-5, приложение В.

3.1.8 **остаточный риск** (residual risk): Риск, остающийся после принятия защитных мер.
[ИСО/МЭК Руководство 51:1999, определение 3.9].

3.1.9 **связанный с управляемым оборудованием риск** (EUC risk): Риск, обусловленный применением управляемого оборудования (УО) и его взаимодействием с системой управления УО.

Примечания

1 В данном случае риск связан с конкретным причиняющим вред событием, в котором для необходимого снижения риска используются Э/Э/ПЭ системы, связанные с безопасностью, и применяются другие меры по снижению риска (т.е. риск связан с функциональной безопасностью).

2 Риск УО показан на рисунке А.1 приложения А МЭК 61508-5. Основной целью определения, связанного с УО риска, является установление понятия «риск без учета Э/Э/ПЭ систем, связанных с безопасностью, и других средств по снижению риска».

3 Оценка этого риска включает в себя вопросы учета человеческого фактора.

3.1.10 **ожидаемый риск** (target risk): Значение риска, которое намереваются достигнуть (получить) для конкретной опасности с учетом риска, обусловленного применением управляемого оборудования совместно с Э/Э/ПЭ системами, связанными с безопасностью, и применением других мер по снижению риска.

3.1.11 **безопасность** (safety): Отсутствие неприемлемого риска.
[ИСО/МЭК Руководство 51:1999, определение 3.1].

3.1.12 **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.

3.1.13 **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.

3.1.14 **разумно предсказуемое неправильное использование** (reasonably foreseeable misuse): Использование изделия, процесса или услуги в условиях или с целью, не предусмотренными поставщиком, но которое может случиться в результате легко предсказуемого поведения человека.
[ИСО/МЭК Руководство 51:1999, определение 3.14].

3.2 Оборудование и устройства

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

Примечание — «Системы управления УО» представляют собой отдельное, отличное от УО понятие.

3.2.2 **окружение** (environment): Все параметры, которые могут повлиять на достижение функциональной безопасности в конкретном рассматриваемом применении и для любого этапа жизненного цикла его системы безопасности.

Примечание — Например, физическая, эксплуатационная, правовая среды и среда обслуживания.

3.2.3 **функциональный блок** (functional unit): Объект аппаратного или программного обеспечения (или обоих), способный к выполнению определенного назначения.

См. [5], определение 01-01-40.

Примечание — В Международном электротехническом словаре МЭС 191-01-01 вместо термина «функциональный блок» используется более общий термин «элемент». Элемент может иногда включать в себя людей.

3.2.4 **применение** (application): Задача, решаемая УО, а не Э/Э/ПЭ системой.

3.2.5 **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 [5] добавлением слова «данные».

3.2.6 **системное программное обеспечение** (system software): Часть программного обеспечения системы РЕ, которая обеспечивает функционирование и предоставляет сервисы для самого программируемого устройства, в отличие от прикладного программного обеспечения, которое по запрограммированным специфицированным функциям выполняет задачу безопасности УО.

Примечание — Примеры см. в [6].

3.2.7 **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.

3.2.8 **существующее ранее программное обеспечение** (pre-existing software): Компонент программного обеспечения, который уже существует, а не разработан специально для выполняемого проекта либо для системы, связанной с безопасностью.

Примечание — Программное обеспечение могло быть коммерчески доступным продуктом, или оно, возможно, было разработано некоторой организацией для ранее выпущенного изделия или системы. Существующее ранее программное обеспечение может быть (или не могло быть) разработано в соответствие с требованиями настоящего стандарта.

3.2.9 **данные** (data): Информация, представленная в виде, удобном для передачи, интерпретации либо обработки компьютером.

Примечания

1 Данные могут быть представлены в виде статической информации (например, совокупности заданных значений, либо представления географической информации) или команды для задания последовательности выполнения предварительно созданных функций.

2 Примеры см. в [6].

3.2.10 **средства поддержки программного обеспечения в режиме реального времени** (software on-line support tool): Программное средство, имеющее непосредственный доступ к системе, связанной с безопасностью, в процессе ее функционирования.

3.2.11 **средства поддержки программного обеспечения в автономном режиме** (software off-line support tool): Программное средство, поддерживающее этап разработки жизненного цикла программного обеспечения, которое не имеет непосредственного доступа к системе, связанной с безопасностью, в процессе ее функционирования. Средства поддержки программного обеспечения в автономном режиме можно разделить на следующие классы:

- класс Т1 – не генерирует программ, которые явно или неявно включаются в рабочую программу (включая данные) системы, связанной с безопасностью.

Примечание — Примерами класса Т1 являются: текстовый редактор или средства поддержки проектирования, написанные не на автокоде;

- класс Т2 — включает в себя средства тестирования 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.

Примечание — Примерами класса Т2 являются: генератор тестовых программ, средства измерения тестового охвата, средства статического анализа;

- класс Т3 — генерирует программы, которые явно или неявно включаются в рабочую программу системы, связанной с безопасностью.

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

3.2.12 **программируемая электроника**; ПЭ (programmable electronic, PE): Средство, основанное на использовании компьютерных технологий, и которое может включать в себя аппаратное и программное обеспечение, а также устройства ввода и/или вывода.

Примечание — Данный термин охватывает микроэлектронные устройства, основанные на одном или нескольких центральных процессорах (ЦП) и связанных с ними устройствах памяти и т.п.

Пример — К программируемым электронным устройствам относятся:
- микропроцессоры;
- микроконтроллеры;
- программируемые контроллеры;
- специализированные интегральные схемы;
- программируемые логические контроллеры;
- другие устройства на основе компьютерных технологий (например, микропроцессорные датчики, преобразователи, устройства привода).

3.2.13 **электрический/электронный/программируемый электронный** (electrical/electronic/programmable electronic); Э/Э/ПЭ: Основанный на электрической (Э) и/или электронной (Э) и/или программируемой электронной (ПЭ) технологии.

Примечание — Данный термин предназначен для того, чтобы охватить любое или все устройства или системы, действующие на основе электричества.

Пример — В число электрических/электронных/программируемых элек-тронных устройств входят:
- электромеханические устройства (электрические);
- твердотельные непрограммируемые электронные устройства (электронные);
- электронные устройства, основанные на компьютерных технологиях (программируемые электронные), см. 3.2.12.

3.2.14 **язык с ограниченной изменчивостью** (limited variability language): Язык программирования, текстовый или графический либо обладающий свойствами обоих, предназначенный для коммерческих и промышленных программируемых электронных контроллеров, диапазон возможностей которого ограничен применением этих устройств.

Пример — Ниже приведены примеры языков с ограниченной изменчивостью, взятые из [7] и других источников, которые используются для представления прикладных программ для систем на основе ПЛК:
- схемы электроавтоматики: графический язык, состоящий из набора входных символов (представляющих поведение, характерное для таких устройств, в которых контакты в нормальном состоянии замкнуты или разомкнуты), соединенных с помощью линий (определяющих направление тока) с выходными символами (представляющими поведение, свойственное реле);
- булева алгебра: низкоуровневый язык, основанный на булевых операторах, таких как И, ИЛИ и НЕ, с возможностью добавления некоторых мнемонических команд;
- функциональные блок диаграммы: в дополнение к булевым операторам допускают использование более сложных функций (таких как операции с файлами, операций чтения и записи) передаваемых блоков данных, команд для сдвиговых регистров и устройств, задающих последовательность;
- последовательностные функциональные схемы: графическое представление последовательностной программы, состоящей из взаимосвязанных шагов, действий и ориентированных связей с условиями перехода.

3.2.15 **специализированная заказная интегральная схема**; СИС (application specific integrated circuit, ASIC): Интегральная схема, разработанная и изготовленная для выполнения конкретной функции, которая определяется разработчиком изделия.

Примечание — СИС как отдельный термин относится ко всем типам перечисленных ниже интегральных схем:

- полностью заказная СИС — СИС, проектирование и производство которой, выполняется подобно стандартной интегральной схеме с функциональностью, определенной заказчиком изделия. Стандартная интегральная схема обычно производится в больших количествах и может использоваться для различных применений. Функциональность, подтверждение соответствия, изготовление и заводское испытание выполняются исключительно поставщиком полупроводникового прибора. Для того чтобы уменьшить используемую площадь кристалла, при размещении часто используют ручные процедуры и ручная оптимизация. Такие интегральные схемы не разрабатываются специально для систем, связанных с безопасностью. Частые изменения производственного процесса, технологии производства и компоновки не всегда экономически оправдывают их разработку. Процент выхода интегральных схем для конкретного производственного процесса или при смене маски не публикуется;
- СИС на основе стандартных ячеек — такая СИС строится на основе предварительно размещенных, спроектированных либо сгенерированных стандартных макроячеек, которые соединяются между собой с помощью дополнительной логики.

Примеры

1 Примерами предварительно размещенных макроячеек являются: стандартные микропроцессоры, периферийные компоненты, коммуникационные интерфейсы, аналоговые блоки, ячейки со специальными функциями ввода/ вывода.

2 Примерами предварительно спроектированных макроячеек как объектов интеллектуальной собственности являются: разнообразные компоненты, аналогичные упомянутым в примере 1, с той разницей, что проектные данные описаны на высокоуровневом языке описания технических средств (VHDL, Verilog), как это сделано для СИС на основе базовых ячеек.

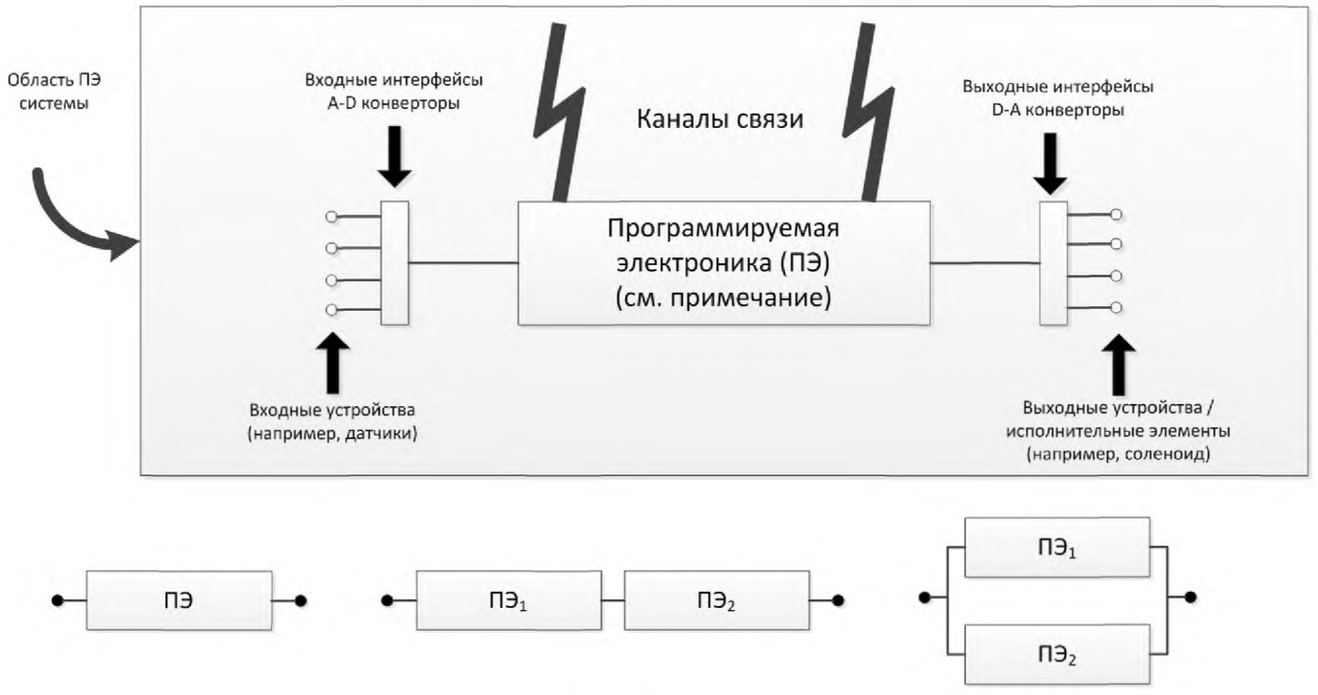
3 Примерами предварительно сгенерированных макроячеек являются: RAM, ROM, EEPROM либо FLASH память. Предполагается, что сгенерированные блоки разработаны корректно на основе правил проектирования. Предварительно размещенные либо спроектированные макроячейки ориентированы на конкретный технологический процесс, но могут быть реализованы и в других технологиях. В большинстве случаев макроячейки не идентичны ячейкам, разработанным на дискретных стандартных компонентах (другой процесс выполняется в другой организации);

- СИС на основе базовых ячеек — такая СИС строится на основе логических элементов (И, ИЛИ, триггер, триггер-защелка), взятых из библиотеки ячеек. Список элементов на уровне логических вентилей, содержащий описание логических элементов и соединений между ними, обычно синтезируется на высокоуровневом языке описания аппаратных средств (VHDL, HDL Verilog). Функциональные и временны́е характеристики логических элементов описаны в библиотеке ячеек; эти характеристики используются для управления средствами синтеза, а также для моделирования. Кроме того, используются инструментальные средства формирования топологии для размещения ячеек и трассировки соединений;
- вентильная матрица — предварительно изготовленные кремниевые базовые матричные кристаллы с фиксированным числом ячеек, которые затем используются для создания различных электронных компонентов. Функциональность матрицы определяется с помощью одного или нескольких уровней металлизированных соединений между предварительно изготовленными ячейками. Процесс проектирования практически аналогичен проектированию СИС на основе базовых ячеек, только этап размещения заменен этапом трассировки соединений для уже существующих ячеек;
- программируемая пользователем вентильная матрица FPGA — стандартная интегральная схема, использующая однократно программируемые или перепрограммируемые элементы для формирования соединений между функциональными блоками и конфигурирования их функций. Вследствие природы программируемого элемента полностью протестировать однократно программируемые FPGA в процессе производства невозможно;
- программируемое логическое устройство PLD — стандартные интегральные схемы с низким и средним уровнем интеграции, однократно программируемые с помощью электрически пережигаемых плавких элементов (перемычек) для формирования комбинаторной логики, обычно основанной на И или ИЛИ элементах и конфигурируемых элементов памяти. PLD обеспечивают предсказуемые параметры синхронизации и гарантируют в проектируемом устройстве максимальную рабочую частоту синхронизации вследствие регулярности структуры. Примеры программируемых логических устройств: PAL, GAL, PML, (E)EPLD, PLA, PLS;
- сложное программируемое логическое устройство CPLD — такая СИС представляет собой несколько блоков, подобных PLD, на одном чипе, соединенных между собой программируемой коммутационной матрицей (использующей перемычки). В большинстве случаев программируемый логический элемент является перепрограммируемым (EPROM или EEPROM).

3.3 Системы: общие аспекты

3.3.1 **программируемая электронная система**, ПЭС [programmable electronic system (PES)]: Система управления, защиты или мониторинга, основанная на использовании одного или нескольких программируемых электронных устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммуникационные магистрали, исполнительные устройства и другие устройства вывода (см. рисунок 2).

Примечание — Структура ПЭС показана на рисунке 2 a). Способ представления ПЭС, применяемый в настоящем стандарте, когда программируемая электроника показывается отдельно от датчиков, исполнительных устройств УО и их интерфейсов, но программируемая электроника может присутствовать в нескольких местах ПЭС, показан на рисунке 2 b). На рисунке 2 c) показана ПЭС с двумя отдельными блоками программируемой электроники. ПЭС с дублированием программируемой электроники (т.е. двухканальную), но с одним датчиком и одним исполнительным устройством показана на рисунке 2 d).



a) Структура базовой ПЭС

b) Одиночная ПЭС с одним программируемым электронным устройством (т.е. одна ПЭС включает один канал программируемой электроники)

c) Одиночная ПЭС с двумя программируемыми элек-тронными устройствами, соединенными последова-тельно (например, интеллек-туальный датчик и программируемый контроллер)

d) Одиночная ПЭС с двумя программируемыми электронными устройствами, но с общими датчиками и исполнительными элементами (т.е. одна ПЭС включает в себя два канала программируемой электроники)

Примечание — Программируемая электроника показана в центре, но она может быть в нескольких местах ПЭС.

Рисунок 2 — Структура программируемой электронной системы

3.3.2 **электрическая/электронная/программируемая электронная система**; Э/Э/ПЭ система (electrical/electronic/programmable electronic system): Система управления, защиты или мониторинга, основанная на использовании одного или нескольких Э/Э/ПЭ устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммуникационные магистрали, исполнительные устройства и другие устройства вывода (см. рисунок 3).



Примечание — Э/Э/ПЭ устройство показано в центре, но оно(и) могут присутствовать в нескольких местах Э/Э/ПЭ системы.

Рисунок 3 — Э/Э/ПЭ система: структура и терминология

3.3.3 **система управления управляемым оборудованием**; система управления УО (EUC control system): Система, реагирующая на входные сигналы, поступающие от процесса и/или от оператора, и генерирующая выходные сигналы, которые заставляют управляемое оборудование работать в необходимом режиме.

Примечание — Система управления УО включает в себя устройства ввода и исполнительные элементы.

3.3.4 **архитектура** (architecture): Конкретная конфигурация элементов аппаратного и программного обеспечения системы.

3.3.5 **программный модуль** (software module): Конструкция, состоящая из процедур и/или объявлений данных, которая может взаимодействовать с другими подобными конструкциями.

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

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

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

3.3.7 **разнообразие** (diversity): Признак, относящийся к средствам и характеризующий различие методов, применяемых для получения требуемой функции.

Пример — Разнообразие может достигаться использованием различных физических методов и различных проектных подходов.

3.4 Системы: аспекты, связанные с безопасностью

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

- реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния УО и
- 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) необходимого снижения риска для соответствия требованиям приемлемого риска (см. 3.1.7). См. также [8], приложение А.

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 могут быть 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) для ослабления последствий вредного события, снижая риск путем уменьшения последствий;

c) для достижения целей перечислений a) и b).

5 Человек может быть частью системы, связанной с безопасностью. 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 электрическую, электронную, программируемую электронную, гидравлическую и пневматическую технологии.

3.4.2 **другое средства снижения риска** (other risk reduction measure): Средство снижения и ослабления риска, отдельное и отличное от Э/Э/ПЭ систем, связанных с безопасностью, и не использующее Э/Э/ПЭ системы, связанные с безопасностью.

Пример — Предохранительный клапан является другим средством снижения риска.

3.4.3 **Э/Э/ПЭ система, связанная с безопасностью, низкой сложности** (low complexity Э/Э/ПЭ safety-related system): Э/Э/ПЭ система, связанная с безопасностью (3.2.13 и 3.4.1), в которой:

- режимы отказов каждого отдельного компонента хорошо определены;
- поведение системы в условиях сбоя может быть полностью определено.

Примечание — Поведение системы в условиях сбоя может быть определено аналитическими методами и/или методами тестирования.

Пример — Система, включающая в себя один или более концевых переключателей, работающих, возможно, через электромеханические реле, один или более контакторов, обесточивающих электродвигатель, является Э/Э/ПЭ системой, связанной с безопасностью, низкой сложности.

3.4.4 **подсистема** (subsystem): Объект высокоуровневого проектирования архитектуры системы, связанной с безопасностью, где опасный отказ согласно 3.6.7, перечисление a) подсистемы приводит к опасному отказу функции безопасности согласно 3.6.7, перечисление a).

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

Данное определение является модифицированным определением 3.2.6 из [2].

Примечания

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

2 Типичный элемент — датчик, программируемый контроллер или исполнительный элемент.

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

Данное определение основано на [9].

Пример — Дублирование функциональных компонентов, добавление битов четности.

Примечания

1 Избыточность используется прежде всего для улучшения отказоустойчивости (вероятность функционирования должным образом за установленный период времени) либо доступности (вероятность функционирования в данный момент). Избыточность может также использоваться для минимизации побочных воздействий через архитектуру, например, как 2oo3.

2 Определение 191-15-01 в Международном электротехническом словаре является менее полным.

3 Избыточность может быть «горячей» или «нагруженной» (все избыточные элементы работают одновременно), «холодной» или «ненагруженной» (только один из избыточных элементов работает в данный момент времени), «смешанной» (один или несколько элементов работают и один или несколько элементов находятся в резерве одновременно).

3.5 Функции безопасности и полнота безопасности

3.5.1 **функция безопасности** (safety function): Функция, реализуемая Э/Э/ПЭ системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния УО по отношению к конкретному опасному событию (см. 3.4.1 и 3.4.2).

Пример — Примерами функций безопасности являются:

- функции, которые должны быть выполнены как позитивные меры, чтобы снизить влияние опасной ситуации (например, выполняют выключение двигателя); и

- функции, которые осуществляют превентивные действия, не допускающие возникновения опасных ситуаций (например, предотвращают запуск двигателя).

3.5.2 **функция безопасности всей системы** (overall safety function): Средства достижения или поддержания безопасного состояния УО относительно определенного опасного события.

3.5.3 **функция безопасности элемента** (element safety function): Часть функции безопасности (см. 3.5.1), которая реализована элементом.

3.5.4 **полнота безопасности** (safety integrity): Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течении 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. 3.5.8).

3 При определении полноты безопасности должны учитываться 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. 3.5.7) и полноту безопасности по отношению к систематическим отказам (см. 3.5.6).

5 Данное определение основывается на определении безотказности (надежности) систем, связанных с безопасностью, при выполнении ими функций безопасности (определение надежности — см. 191-12-01 в Международном электротехническом словаре).

3.5.5 **полнота безопасности программного обеспечения** (software safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме и относящихся к программному обеспечению.

3.5.6 **полнота безопасности, касающаяся систематических отказов** (systematic safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме.

Примечание — Обычно полнота безопасности, касающаяся систематических отказов, не может быть охарактеризована количественно (в отличие от полноты безопасности аппаратного обеспечения, которой, как правило, может быть дана количественная оценка).

3.5.7 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, касающаяся случайных отказов аппаратуры, проявляющихся в опасном режиме.

Примечание — Данный термин относится к отказам, проявляющимся в опасном режиме, т. е. к тем отказам системы, связанной с безопасностью, которые могут ухудшить полноту ее безопасности. Данная ситуация характеризуется двумя параметрами: средней интенсивностью опасных отказов и вероятностью отказа при обработке запроса. Первый из этих параметров надежности используется при необходимости осуществлять не-

прерывный контроль над поддержанием безопасности, второй параметр применяется в контексте связанных с безопасностью систем защиты.

3.5.8 **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, сответствует наименьшей полноте безопасности.

Примечания

1 Меры целевых отказов (см. 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: система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до значения, равного n.

3.5.9 **стойкость к систематическим отказам** (systematic capability): Мера уверенности (выраженная в диапазоне ССО 1 — ССО 4) в том, что систематическая полнота безопасности элемента соответствует требованиям заданного значения УПБ для определенной функции безопасности элемента, если этот элемент применен в соответствии с указаниями, определенными для этого элемента в соответствующем руководстве по безопасности.

Примечания

1 Стойкость к систематическим отказам определяется с учетом требований по предотвращению систематических отказов и управлению ими (см. МЭК 61508-2 и МЭК 61508-3).

2 Механизм систематического отказа зависит от природы элемента. Например, для элемента, представляющего программное обеспечение, должны быть рассмотрены только механизмы ошибок в программах. Для элемента, включающего в себя аппаратное средство и программное обеспечение, должны быть рассмотрены механизмы систематических отказов как для аппаратных средств, так и для программного обеспечения.

3 Стойкость к систематическим отказам элемента ССО N при выполнении определенной функции безопасности означает, что элемент соответствует УПБ N для систематических отказов, если этот элемент применен в соответствии с указаниями, определенными для этого элемента в соответствующем руководстве по безопасности.

3.5.10 **уровень полноты безопасности программного обеспечения** (software safety integrity level): Стойкость к систематическим отказам элемента программного обеспечения, являющегося частью подсистемы или системы, связанной с безопасностью.

Примечание — УПБ характеризует функцию безопасности всей системы, но не любую из ее отдельных подсистем либо элементов, которые реализуют эту функцию безопасности. Поэтому программное обеспечение, как и любой его элемент, не имеет собственного УБП. Однако фраза «программное обеспечение с УПБ N» означает, что «обоснована уверенность (выраженная значениями от 1 до 4), и функция безопасности, реализуемая элементом (программным обеспечением), не будет приводить к сбою из-за соответствующих механизмов систематических отказов, если этот элемент (программное обеспечение) применяется в соответствии с указаниями, определенными в руководстве по безопасности, разработанном для такого элемента».

3.5.11 **спецификация требований к Э/Э/ПЭ системе безопасности** (Э/Э/ПЭ system safety requirements specification): Спецификация, содержащая требования к функциям безопасности и связанными с ними УПБ.

3.5.12 **спецификация требований к функциям безопасности Э/Э/ПЭ системы** (E/E/PE system safety functions requirements specification): Спецификация, содержащая требования к функциям безопасности, которые должны быть выполнены системами, связанными с безопасностью.

Примечания

1 Данная спецификация представляет собой часть (относящуюся к функциям безопасности) спецификации требований к безопасности Э/Э/ПЭ системы (см. МЭК 61508-1, подраздел 7.10 и подпункт 7.10.2.6) и содержит подробное и точное описание функций безопасности, которые должны выполняться системами, связанными с безопасностью.

2 Спецификации могут быть документированы с использованием текста, блок диаграмм, матриц, логических диаграмм и т.д., при условии, что функции безопасности четко определены.

3.5.13 **спецификация требований к полноте безопасности Э/Э/ПЭ системы** (E/E/PE system safety integrity requirements specification): Спецификация, содержащая требования к полноте безопасности для функций безопасности, которые должны выполняться системами, связанными с безопасностью.

Примечание — Данная спецификация представляет собой часть (относящуюся к полноте безопасности) спецификации требований к безопасности Э/Э/ПЭ системы (см. МЭК 61508-1, подраздел 7.10 и подпункт 7.10.2.7).

3.5.14 **спецификация требований к проекту Э/Э/ПЭ системы** (E/E/PE system design requirements specification): Спецификация, содержащая проектные требования к Э/Э/ПЭ системе, связанной с безопасностью, в терминах ее подсистем и элементов.

3.5.15 **программное обеспечение, связанное с безопасностью** (safety-related software): Программное обеспечение, которое используется для реализации функций безопасности в системах, связанных с безопасностью.

3.5.16 **режим работы** (mode of operation): Способ выполнения функции безопасности либо в режиме:

- с низкой частотой запросов, в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов не превышает одного в год или

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 отказывает так, что выполнение функции безопасности невозможно, то в этом случае УО может перейти в безопасное состояние (см. МЭК 61508-2, пункт 7.4.8);

- с высокой частотой запросов, в котором функция безопасности выполняется только по запросу и переводит УО в определенное безопасное состояние, а частота запросов превышает один в год, или

- непрерывном режиме, в котором функция безопасности поддерживает УО в безопасном состоянии, как и при нормальном функционировании.

3.5.17 **целевая величина отказов** (target failure measure): Заданная вероятность отказов в опасном режиме, которая должна быть достигнута в соответствии с требованиями к полноте безопасности, выраженная в виде:

- средней вероятности опасного отказа при выполнении функции безопасности по запросу (для режима работы с низкой частотой запросов) либо

- средней частоты возникновения опасных отказов в час (для режима с высокой частотой запросов или непрерывного режима работы).

Примечание — Числовые значения для целевых величин отказов приведены в МЭК 61508-1, таблицы 2 и 3.

3.5.18 **необходимое снижение риска** (necessary risk reduction): Снижение риска, которое должно быть достигнуто Э/Э/ПЭ системами, связанными с безопасностью, и/или другими средствами снижения риска, гарантирующее, что допустимый уровень риска не будет превышен.

3.6 Сбой, отказ и ошибка

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

См. [10], определение 14-01-10.

Примечание — Международный электротехнический словарь (191-05-01) определяет "сбой" как состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая неспособность, возникающую во время профилактических работ или других плановых мероприятий, либо в результате недостатка внешних ресурсов. Иллюстрация к этим двум точкам зрения показана на рисунке 4.

3.6.2 **предотвращение сбоя** (fault avoidance): Применение методов и процедур, предназначенных помочь избежать возникновения сбоев во время любой стадии жизненного цикла системы, связанной с безопасностью.

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

См. [10], определение 14-04-06.

Примечание — Определение 191-15-05, приведенное в Международном электротехничес-ком словаре, относится только к сбоям подкомпонентов. См. примечание к термину "сбой" в 3.6.1.

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

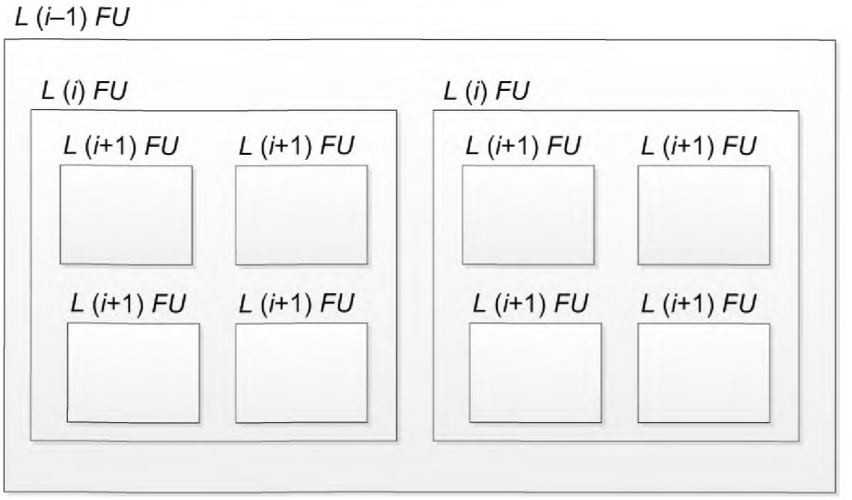
Примечания

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

2 Соотношение между сбоями и отказами в МЭК 61508 и [11] см. на рисунке 4.

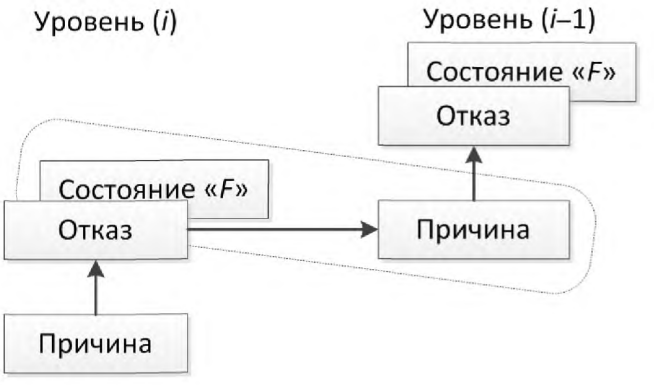
3 Характеристики требуемых функций неизбежно исключают определенные режимы работы, и некоторые функции могут быть определены путем описания режимов, которых следует избегать. Возникновение таких режимов представляет собой или отказ.

4 Отказы являются либо случайными (в аппаратных средствах), либо систематическими (в аппаратных средствах или в программном обеспечении), см. 3.6.5 и 3.6.6.

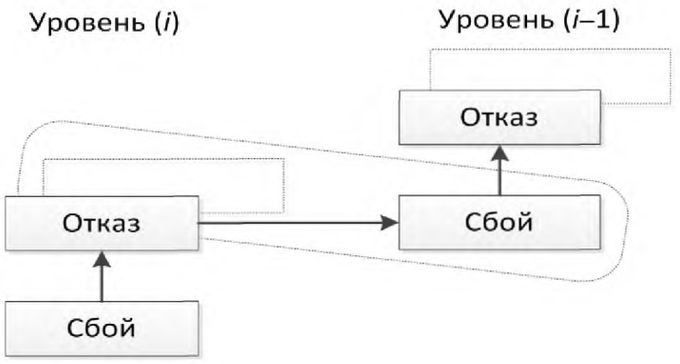


(*L* - уровень; *i* = 1, 2, 3 и т.д.; *FU* - функциональный блок)

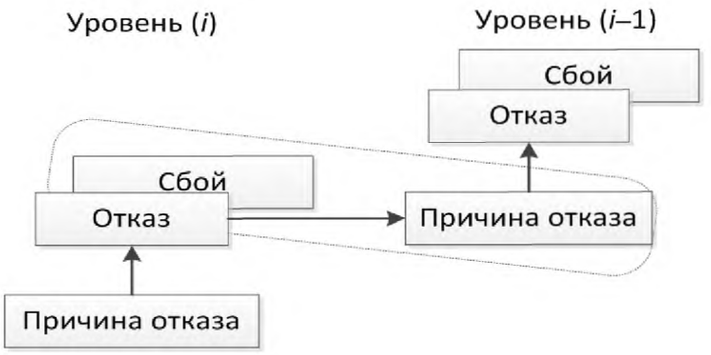
a) Конфигурация функционального блока



b) Обобщенный вид



c) С точки зрения МЭК 61508 и [10].



d) С точки зрения [11]

Примечания к рисунку 4

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 «функциональным блоком». 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 [10], в которой внимание акцентируется на причинном аспекте, как показано на рисунке c), и концепцию «отказа», представленную в [11], в которой основное внимание уделено аспекту состояния, как показано на рисунке d). В [11] состояние «F» называется «отказом», а в МЭК 61508 и [10] 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 4 — Модель отказа

3.6.5 **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.

3.6.6 **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.

[Международный электротехнический словарь, статья 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.

3.6.7 **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, или

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

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

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

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

3.6.9 **зависимый отказ** (dependent failure): Отказ, вероятность которого не может быть выражена в виде простого произведения безусловных вероятностей отдельных событий, являющихся причиной отказа.

Примечание — Пусть $P(z)$ вероятность события z. Два события A и B будут зависимы только в том случае, если: $P(A \text{ и } B) > P(A) \cdot P(B)$.

3.6.10 **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, ведущих к отказу системы.

3.6.11 **ошибка** (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и истинным, специфицированным или теоретически правильным значением или условием.

Данное определение является адаптированным определением [Международный электротехнический словарь, статья 191-05-24].

3.6.12 **исправимая ошибка** (soft-error): Ошибочные изменения в содержании данных, но не в самой физической схеме.

Примечания

1 После выявления исправимой ошибки и исправления данных схема восстанавливается в исходное состояние.

2 Исправимые ошибки могут происходить в памяти, цифровой логике, аналоговых схемах, линиях передачи и т.д. и являются доминирующими в полупроводниковой памяти, включая регистры и защелки. Данные по ним могут быть получены, например, от производителей.

3 Исправимые ошибки являются неустановившимися ошибками, их не следует путать с ошибками программирования в программном обеспечении.

3.6.13 **отказ невлияющего компонента** (no part failure): Отказ компонента, который не влияет на выполнение функции безопасности.

Примечание — Отказ невлияющего компонента не используется для вычислений ДБО.

3.6.14 **невлияющий отказ** (no effect failure): Отказ компонента, который участвует в реализации функции безопасности, но непосредственно не влияет на функцию безопасности.

Примечания

1 Невлияющий отказ по определению не влияет на функцию безопасности, поэтому он не вносит вклад в интенсивность отказов функции безопасности.

2 . Невлияющий отказ не используется при вычислениях ДБО.

3.6.15 **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. Данное отношение имеет вид

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

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

$$\text{ДБО} = (\sum\lambda_{S} + \sum\lambda_{Dd})/(\sum\lambda_{S} + \sum\lambda_{Dd} + \sum\lambda_{Du}).$$

3.6.16 **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 $\lambda avg(T) = \left(\int_0^T \lambda(\tau)d\tau\right)/T$, 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_{as}, 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.

3.6.17 **вероятность опасного отказа по запросу** (probability of dangerous failure on demand, PFD): Неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность (см. [11]),

т. е. выполнить указанную функцию безопасности, когда происходит запрос от УО или системы управления УО.

Примечания

1 [Мгновенная] неготовность (согласно [11]) является вероятностью ненахождения элемента в состоянии выполнения необходимой функции при данных условиях в данный момент времени, предполагается, 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.

3.6.18 **средняя вероятность опасного отказа по запросу** (probability of dangerous failure on demand, PFD_{avg}): Средняя неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность (см. [11]), т. е. выполнить указанную функцию безопасности, когда происходит запрос от УО или системы управления УО.

Примечания

1 Среднюю неготовность на заданном временном отрезке $[t_1, t_2]$ обозначают как $U(t_1, t_2)$.

2 PFD и PFDavg включают в себя два вида отказов: опасные необнаруженные отказы, произошедшие после последней контрольной проверки, и сами реальные отказы по запросу, вызванные запросами (от контрольных проверок и запросов на безопасность). Первый вид отказов зависит от времени и характеризуется интенсивностью опасных отказов $\lambda_{DU}(t)$, а второй зависит только от числа запросов и характеризуется вероятностью отказа по запросу (обозначается γ).

3 Так как реальные отказы по запросу не могут быть обнаружены тестами, то их необходимо идентифицировать и учитывать при вычислении целевых мер отказов.

3.6.19 **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 используется, 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 в [12]).

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. выше PFD). 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.

3.6.20 **время безопасности процесса** (process safety time): Промежуток времени между моментом появления отказа, имеющего возможность дать начало опасному событию в УО или системе управления УО, и моментом времени, к которому в УО должно быть завершено действие по предотвращению появления опасного события.

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

Примечание — MTTR включает в себя:

a)время выявления отказа; и

b)время, прошедшее до начала восстановления; и

c)время, фактически затраченное на ремонт; и

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).

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

Примечание — MRT охватывает времена MTTR, описанные в перечислениях b), c) и d) примечания к 3.6.21.

3.7 Процессы жизненного цикла

3.7.1 **жизненный цикл систем безопасности** (safety lifecycle): Необходимые процессы, относящиеся к реализации систем, связанных с безопасностью, проходящие в течение периода времени, начиная со стадии разработки концепции проекта и заканчивая стадией, когда все Э/Э/ПЭ системы, связанные с безопасностью, и другие средства снижения риска уже не используются.

Примечания

1 Термин «жизненный цикл систем функциональной безопасности» является более точным, однако прилагательное «функциональной» не является обязательным в данном случае в контексте настоящего стандарта.

2 Модели жизненного цикла систем безопасности, применяемые в настоящем стандарте, определены на рисунках 2, 3 и 4 МЭК 61508-1.

3.7.2 **жизненный цикл программного обеспечения (**software lifecycle): Процессы, происходящие в течение периода времени, который начинается с появления общей концепции программного обеспечения и заканчивается если программное обеспечение окончательно выведено из эксплуатации.

Примечания

1 Обычно жизненный цикл программного обеспечения включает в себя стадию разработки требований, стадии разработки, тестирования, интеграции, установки, а также стадию модификации.

2 Программное обеспечение не поддерживается, точнее говоря, его модифицируют.

3.7.3 **управление конфигурацией** (configuration management): Дисциплина идентификации компонентов примененных систем для осуществления контролируемых изменений этих компонентов и поддержания преемственности и прослеживания на протяжении всего жизненного цикла.

Примечание — Более подробное описание управления конфигурацией приведено в [6], С.5.24 приложения С.

3.7.4 **базовая конфигурация** (configuration baseline): Информация, которая позволяет проверяемым и систематическим путем воссоздать версию программного обеспечения, включая все исходные коды, данные, файлы времени выполнения, документацию, конфигурационные файлы и скрипты для установки, которые включают в себя версию программного обеспечения, информацию о компиляторах, операционных системах и средствах разработки, используемых для создания версии программного обеспечения.

3.7.5 **анализ влияния** (impact analysis): Определение влияния, которое окажет изменение в функции или в компоненте системы на другие функции или компоненты этой системы, а также других систем.

Примечание — В контексте программного обеспечения см. [6], С.5.23 приложения С.

3.8 Подтверждение мер по обеспечению безопасности

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

Данное определение является модификацией определения 2.17 [13].

Примечание — В контексте настоящего стандарта верификация представляет собой выполняемую для каждой стадии жизненного цикла соответствующей системы безопасности (общей, Э/Э/ПЭ системы и программного обеспечения) 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, что они работают в соответствии с их спецификациями;

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

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

Данное определение является модификацией определения 2.18 из [13].

Примечания

1 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 (см. рисунок 3 МЭК 61508-1);
- подтверждение соответствия программного обеспечения (см. рисунок 4 МЭК 61508-1).

2 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.

3.8.3 **оценка функциональной безопасности** (functional safety assessment): Исследование, основанное на фактах, предназначенное для оценки функциональной безопасности, достигаемой одной или несколькими Э/Э/ПЭ системами, связанными с безопасностью, и/или другими средствами снижения риска.

3.8.4 **аудит функциональной безопасности** (functional safety audit): Систематическое и независимое исследование, проводящееся с тем, чтобы определить, насколько эффективно реализованы процедуры, предназначенные для согласования требований к функциональной безопасности с запланированными мероприятиями и определения, насколько они пригодны для достижения поставленных целей.

Примечание — Аудит функциональной безопасности может выполняться как часть оценки функциональной безопасности.

3.8.5 **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 проверяться 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.

3.8.6 **охват диагностикой** (diagnostic coverage): 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.

3.8.7 **интервал диагностических проверок** (diagnostic test interval): Интервал между неавтономными проверками, предназначенными для обнаружения отказов в системах, связанных с безопасностью, с заданным охватом диагностикой.

3.8.8 **обнаруженный** (detected, revealed, overt): По отношению к аппаратным средствам, установленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физическим осмотром и ручной проверкой) либо в ходе нормальной работы.

Пример — Эти прилагательные используются для обнаруженных сбоев и обнаруженных отказов.

Примечание — Опасный отказ, выявленный диагностическими проверками, является обнаруженным отказом и может считаться безопасным отказом, только если применяются рекомендуемые эффективные автоматические меры.

3.8.9 **необнаруженный** (undetected, unrevealed, covert): По отношению к аппаратным средствам не выявленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физическим осмотром и ручной проверкой) либо в ходе нормальной работы.

Пример — Это прилагательное используется для необнаруженных сбоев и необнаруженных отказов.

3.8.10 **эксперт** (assessor): Конкретное лицо, группа лиц или организация, выполняющие оценку функциональной безопасности, для принятия решения по функциональной безопасности, достигаемой Э/Э/ПЭ системами, связанными с безопасностью, и другими мерами по снижению риска.

Примечание — См. также МЭК 61508-1, раздел 8.

3.8.11 **независимое лицо** (independent person): Лица, независимые и не связанные с процессами, происходящими на конкретной стадии жизненного цикла подсистем безопасности Э/Э/ПЭ системы в целом или программного обеспечения, которые выполняют оценку или подтверждение соответствия функциональной безопасности и не несут прямой ответственности за эти процессы.

3.8.12 **независимое подразделение** (independent department): Подразделение, независимое и не связанное с подразделениями, отвечающими за процессы, которые происходят в течение конкретной стадии жизненного цикла подсистем безопасности Э/Э/ПЭ системы в целом или программного обеспечения, которое проводит оценку или подтверждение соответствия функциональной безопасности.

3.8.13 **независимая организация** (independent organisation): Организация, отдельная и отличная в отношении управления и других ресурсов от организаций, отвечающих за процессы, происходящих в течение конкретной стадии жизненного цикла подсистем безопасности Э/Э/ПЭ системы в целом или программного обеспечения, которая выполняет оценку и подтверждение соответствия функциональной безопасности.

3.8.14 **анимация** (animation): Имитация работы программной системы (или существенной части этой системы), предназначенная для отображения существенных аспектов поведения системы: может быть применена, например, к спецификации требований в соответствующем формате или на достаточно высоком уровне представления проекта системы.

Примечание — Анимация может дать дополнительную уверенность в том, что система соответствует реальным требованиям, поскольку улучшает восприятие человеком конкретное поведение системы.

3.8.15 **динамическое тестирование** (dynamic testing): Работа программного обеспечения и/или аппаратного обеспечения, выполняемая под контролем и планомерно для демонстрации наличия требуемого поведения и отсутствия нежелательного поведения.

Примечание — Динамическое тестирование противоположно статическому анализу, при котором не требуется выполнения программ и функционирования технических средств.

3.8.16 **средство тестирования** (test harness): Средство, имитирующее (до некоторой полезной степени) среду, в которой будет работать разрабатываемое программное обеспечение или аппаратные средства, путем передачи тестовых данных в программу и регистрации ответа.

Примечание — Средство тестирования может также включать в себя генератор тестовых данных и средства верификации результатов проверки (с помощью автоматического сравнения с правильными значениями либо ручного анализа).

3.8.17 **руководство по безопасности для применяемых изделий** (safety manual for compliant items): Документ, предоставляющий всю информацию, связанную с функциональной безопасностью компонента, выполняющего указанные функции безопасности, гарантирующий, что система соответствует требованиям серии стандартов МЭК 61508.

3.8.18 **проверено в эксплуатации** (proven-in-use): Демонстрация, основанная на анализе опыта работы определенной конфигурации компонента того, что вероятность опасных систематических отказов компонента настолько низка, что каждая функция безопасности, которую реализует этот компонент, достигает требуемого для нее уровня полноты безопасности.

Приложение А
(справочное)

Указатель терминов

анализ влияния	3.7.5
анимация	3.8.14
архитектура	3.3.4
аудит функциональной безопасности	3.8.4
базовые данные конфигурации	3.7.4
безопасность	3.1.11
безопасный отказ	3.6.8
верификация	3.8.1
вероятность опасного отказа по запросу	3.6.17
вред	3.1.1
время безопасности процесса	3.6.20
данные	3.2.9
динамическое тестирование	3.8.15
доля безопасных отказов	3.6.15
другое средство снижения риска	3.4.2
жизненный цикл программного обеспечения	3.7.2
жизненный цикл систем безопасности	3.7.1
зависимый отказ	3.6.9
избыточность	3.4.6
интервал диагностических проверок	3.8.7
исправимая ошибка	3.6.12
канал	3.3.6
контрольная проверка	3.8.5
невлияющий отказ	3.6.14
независимая организация	3.8.13
независимое лицо	3.8.11
независимое подразделение	3.8.12
необнаруженный	3.8.9
необходимое снижение риска	3.5.18
обнаруженный	3.8.8
ожидаемый риск	3.1.10
окружение	3.2.2
опасная ситуация	3.1.3
опасное событие	3.1.4
опасность	3.1.2
опасный отказ	3.6.7
остаточный риск	3.1.8
отказ	3.6.4
отказ невлияющего компонента	3.6.13
отказ по общей причине	3.6.10
охват диагностикой	3.8.6

оценка функциональной безопасности	3.8.3
ошибка	3.6.11
подсистема	3.4.4
подтверждение соответствия	3.8.2
полнота безопасности	3.5.4
полнота безопасности аппаратного обеспечения	3.5.7
полнота безопасности, касающаяся систематических отказов	3.5.6
полнота безопасности программного обеспечения	3.5.5
предотвращение сбоя	3.6.2
приемлемый риск	3.1.7
прикладное программное обеспечение	3.2.7
применение	3.2.4
причиняющее вред событие	3.1.5
проверено в эксплуатации	3.8.18
программируемая электроника	3.2.12
программируемая электронная система	3.3.1
программное обеспечение	3.2.5
программное обеспечение, связанное с безопасностью	3.5.15
программный модуль	3.3.5
разнообразие	3.3.7
разумно предсказуемое неправильное использование	3.1.14
режим работы	3.5.16
риск	3.1.6
руководство по безопасности для применяемых изделий	3.8.17
сбой	3.6.1
связанный с УО риск	3.1.9
система	3.4.1
систематический отказ	3.6.6
система, связанная с безопасностью	3.4.1
система управления управляемым оборудованием	3.3.3
системное программное обеспечение	3.2.6
случайный отказ аппаратных средств	3.6.5
специализированная интегральная схема	3.2.15
спецификация требований к Э/Э/ПЭ системе безопасности	3.5.11
спецификация требований к полноте безопасности Э/Э/ПЭ системы	3.5.13
спецификация требований к проекту Э/Э/ПЭ системы	3.5.14
спецификация требований к функциям безопасности Э/Э/ПЭ системы	3.5.12
среднее время восстановления	3.6.21
средняя вероятность опасного отказа по запросу	3.6.18
средняя продолжительность ремонта	3.6.22
средняя частота опасного отказа в час	3.6.19
средства поддержки программного обеспечения в автономном режиме	3.2.11
средства поддержки программного обеспечения в режиме реального времени	3.2.10
средство тестирования	3.8.16
стойкость к систематическим отказам	3.5.9
существующее ранее программное обеспечение	3.2.8
управление конфигурацией	3.7.3

управляемое оборудование 3.2.1
уровень полноты безопасности 3.5.8
уровень полноты безопасности программного обеспечения 3.5.10
устойчивость к отказам 3.6.3
функциональная безопасность 3.1.12
функциональный блок 3.2.3
функция безопасности 3.5.1
функция безопасности всей системы 3.5.2
функция безопасности элемента 3.5.3
целевая величина отказов 3.5.17
эксперт 3.8.10
электрическая/электронная/программируемая электронная система 3.3.2
Э/Э/ПЭ системы, связанные с безопасностью, низкой сложности 3.4.3
электрический/электронный/программируемый электронный 3.2.13
элемент 3.4.5
язык с ограниченной изменчивостью 3.2.14

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК Руководство 104:1997	—	*
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»
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»

*Соответствующий национальный стандарт отсутствует. До его утверждения реко-мендуется 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 использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector

[2] IEC 62061:2005, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

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

[4] IEC 60601 (all parts), Medical electrical equipment

[5] ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms

[6] IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

[7] IEC 61131-3:2003, Programmable controllers — Part 3: Programming languages

[8] 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)

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

[10] ISO/IEC 2382-14:1997, Information technology — Vocabulary — Part 14: Reliability, maintainability and availability

[11] IEC 60050-191:1990, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service

[12] 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

[13] ISO 8402:1994, Quality management and quality assurance — Vocabulary

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

Ключевые слова: функциональная безопасность, жизненный цикл систем, электрические компоненты, электронные компоненты, программируемые электронные компоненты и системы, определения терминов, объяснения терминов, сокращения

Подписано в печать 02.10.2014. Формат 60х84⅛.
Усл. печ. л. 4,19. Тираж 53 экз. Зак. 4144
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»,
123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru