ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-4— 2007

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

Часть 4

Термины и определения

IEC 61508-4:1998
Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations
(IDT)

Издание официальное

БЗ 3—2006/38

Москва
Стандартинформ
2008

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 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН обществом с ограниченной ответственностью «Корпоративные электронные системы» и Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением развития, информационного обеспечения и аккредитации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 582-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-4:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения» (IEC 61508-4:1998 «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 дополнительном приложении В

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2008

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

Содержание

1 Область применения 1
2 Нормативные ссылки 3
3 Термины и определения 3
Приложение А (справочное) Указатель терминов 17
Приложение В (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам 19
Библиография 20

Введение

Системы, состоящие из электрических и/или электронных компонентов, в течение многих лет используются для выполнения функций безопасности в большинстве областей применения. Компьютерные системы [обычно называемые программируемыми электронными системами (PES)], применяемые во всех областях для выполнения задач, не связанных с безопасностью, во все более увеличивающихся объемах используются для решения задач 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 компонентов [электрических/электронных/программируемых электронных систем (E/E/PES)], которые используются для выполнения функций безопасности. Этот унифицированный подход был принят для того, чтобы разработать рациональную и последовательную техническую концепцию для всех электрических систем, связанных с безопасностью. Основной целью при этом является содействие разработке стандартов.

В большинстве случаев безопасность достигается за счет использования нескольких систем защиты, в которых применяются 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, связанные с безопасностью, входящие в состав комбинированной системы, связанной с безопасностью. Таким образом, хотя данный стандарт посвящен в основном электрическим/электронным/программируемым электронным (E/E/PE) системам, связанным с безопасностью, он может также предоставлять общую структуру, в рамках которой рассматриваются системы, связанные с безопасностью, основанные на других технологиях.

Признанным фактом является существование огромного разнообразия использования E/E/PES в различных областях применения, отличающихся различной степенью сложности, опасностями и возможными рисками. В каждом конкретном случае необходимые меры безопасности будут зависеть от многочисленных факторов, которые являются специфичными для этого применения. Настоящий стандарт, являясь базовым стандартом, позволит формулировать такие меры в будущих стандартах.

Настоящий стандарт:

- рассматривает все соответствующие стадии жизненного цикла систем безопасности в целом, а также подсистем E/E/PES и программного обеспечения (например, начиная от исходной концепции, проектирование, разработку, эксплуатацию, техническое обслуживание и вывод из эксплуатации), в ходе которых подсистемы E/E/PES используются для выполнения задач обеспечения безопасности;

- был задуман с учетом быстрого развития технологий; его структура является достаточно устойчивой и полной для того, чтобы удовлетворять потребностям разработок, которые могут появиться в будущем;

- делает возможной разработку стандартов, предназначенных для прикладных отраслей и посвященных вопросам обеспечения безопасности на базе E/E/PES; разработка стандартов для прикладных отраслей в рамках общей структуры, вводимой настоящим стандартом, должна приводить к более высокому уровню согласованности (например, в отношении принципов, положенных в основу, терминологии и т. п.) как для отдельных прикладных отраслей, так и для их совокупности; это приносит преимущества как в плане безопасности, так и в плане экономики;

- предоставляет метод разработки спецификаций для требований безопасности, необходимых для достижения требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью;

- использует уровни полноты безопасности для задания планируемого уровня полноты безопасности для функций, которые должны быть реализованы E/E/PE системами, связанными с безопасностью;

- использует для определения уровней полноты безопасности подход, основанный на оценке рисков;

- устанавливает количественные величины отказов E/E/PE систем, связанных с безопасностью, которые связаны с уровнями полноты безопасности;

- устанавливает нижний предел для планируемой величины отказов в режиме опасных отказов, который может быть задан для отдельной E/E/PE системы, связанной с безопасностью; для E/E/PE систем, связанных с безопасностью, работающих:

- в режиме с низкой интенсивностью запросов нижний предел для выполнения планируемой функции по запросу устанавливается на средней вероятности отказов 10^{-5};

- в режиме с высокой интенсивностью запросов нижний предел устанавливается на вероятности опасных отказов 10^{-9} в час.

Примечание — Отдельная E/E/PE система, связанная с безопасностью, необязательно предполагает одноканальную архитектуру.

- применяет широкий набор принципов, методов и мер для достижения функциональной безопасности E/E/PE систем, связанных с безопасностью, но не использует концепцию безаварийности, которая может иметь важное значение, когда виды отказов хорошо определены, а уровень сложности является относительно невысоким. Концепция безаварийности признана неподходящей из-за широкого диапазона сложности E/E/PE систем, связанных с безопасностью, которые находятся в области применения настоящего стандарта.

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 — 2008—06—01

1 Область применения

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

1.2 Определения сгруппированы под общими заголовками, так что взаимосвязанные термины могут быть поняты в общем контексте. Следует, однако, отметить, что эти заголовки не добавляют нового значения определениям и в этом смысле могут быть оставлены без внимания.

1.3 МЭК 61508-1—МЭК 61508-4 представляют собой основополагающие стандарты по безопасности, хотя этот статус не применяется в контексте E/E/PE систем, связанных с безопасностью, имеющих небольшую сложность (МЭК 61508-4, пункт 3.4.4). Как основополагающие стандарты по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с МЭК Руководство 104 и ИСО/МЭК Руководство 51. МЭК 61508-1—МЭК 61508-4 предназначены, кроме того, для использования в качестве самостоятельных стандартов.

В круг обязанностей технического комитета входит использование, 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 будут применяться, если это не указано специально, или они будут включаться в стандарты, подготовленные этими техническими комитетами.

1.4 Рисунок 1 показывает общую структуру МЭК 61508-1—МЭК 61508-7 и указывает на роль, которую играет МЭК 61508-4 в достижении функциональной безопасности E/E/PE систем, связанных с безопасностью.

Примечание — В США и Канаде до тех пор, пока там не будет опубликована в качестве международного стандарта предлагаемая реализация МЭК 61508 для обрабатывающих отраслей (т. е. МЭК 61511), вместо МЭК 61508 в обрабатывающих отраслях допускается использовать национальный стандарт, базирующийся на МЭК 61508 (т. е. ANSI/ISA S 84.01—1996).

Издание официальное

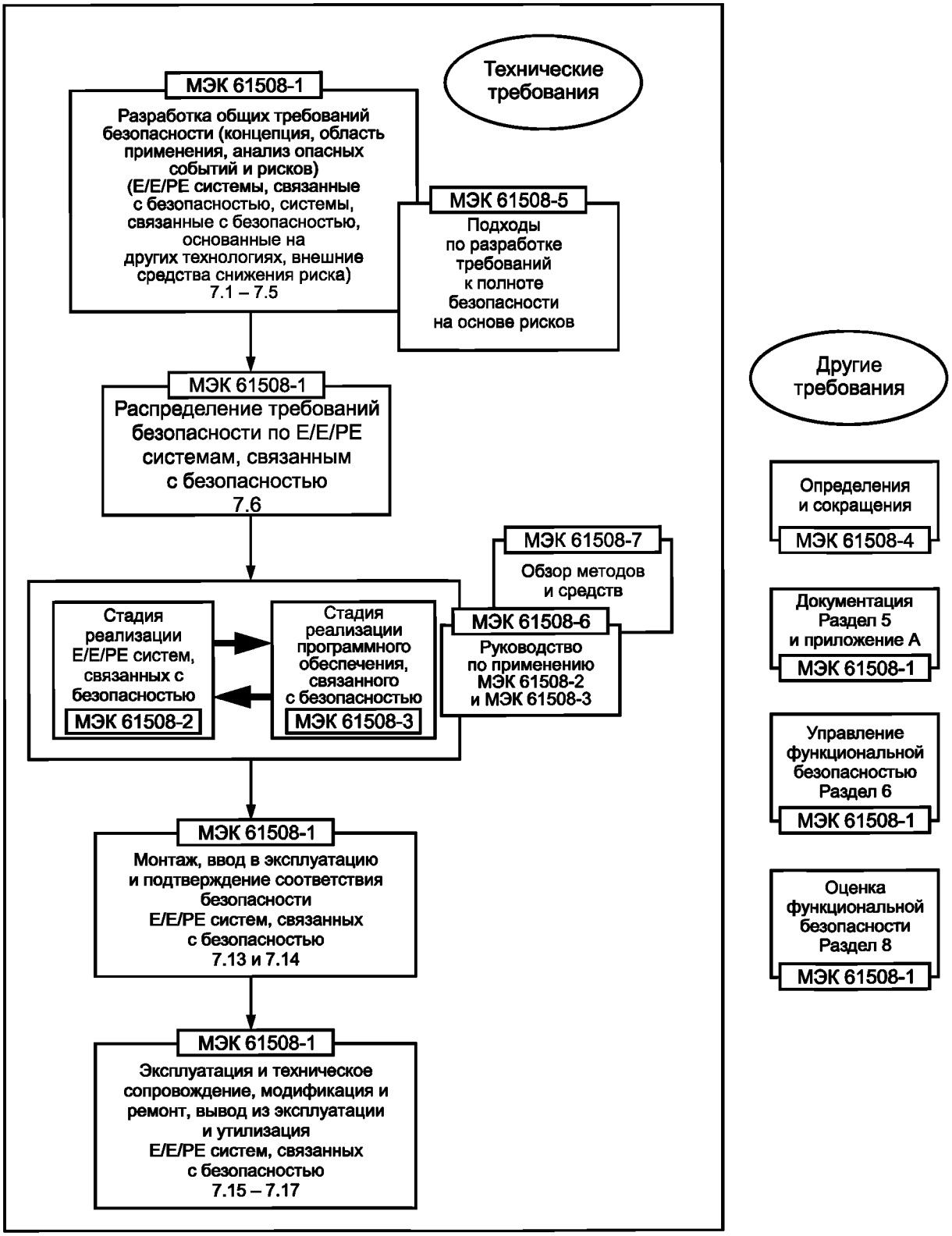


Рисунок 1 — Общая структура настоящего стандарта

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

МЭК 60050(191):1990 Международный электротехнический словарь. Глава 191. Надежность и качество услуг

МЭК 60050(351):1975 Международный электротехнический словарь. Глава 351. Автоматическое управление

МЭК 61508-1:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

МЭК 61508-2:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/ программируемым электронным, связанным с безопасностью

МЭК 61508-3:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

МЭК 61508-5:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты защиты

МЭК 61508-6:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2000 и МЭК 61508-3:1998

МЭК 61508-7:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Анализ методов и средств

МЭК Руководство 104:1997 Подготовка публикаций по безопасности и использование основополагающих публикаций и групповых публикаций по безопасности

ИСО/МЭК 2382-14:1998 Обработка данных. Словарь. Часть 14. Надежность, удобство сопровождения и работоспособность

ИСО/МЭК Руководство 51:1999 Аспекты безопасности. Руководящие указания по включению в стандарты

ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь

3 Термины и определения

В настоящем стандарте использованы сокращения, приведенные в таблице 1, и определения, приведенные ниже.

Таблица 1 — Сокращения, используемые в настоящем стандарте

Сокращение	Полное выражение	Определение и/или объяснение термина
MooN	Канальная архитектура M из N (например, 1oo2 представляет собой архитектуру один из двух, где каждый из двух каналов может выполнять функцию безопасности)	МЭК 61508-6 (приложение В)
MooND	Канальная архитектура M из N с диагностикой	МЭК 61508-6 (приложение В)
ALARP	Низкий, насколько это возможно	МЭК 61508-5 (приложение В)
E/E/PE	Электрическая/электронная/программируемая электронная	3.2.6
E/E/PES	Электрическая/электронная/программируемая электронная система	3.3.3
EUC	Управляемое оборудование	3.2.3
PES	Программируемая электронная система	3.3.2
PLC	Программируемый логический контроллер	МЭК 61508-6 (приложение Е)
SIL	Уровень полноты безопасности	3.5.6

3.1 Термины, относящиеся к безопасности

3.1.1 **ущерб** (harm): Физическое повреждение или вред здоровью человека, нанесенный как прямо, так и косвенно, в результате повреждения имущества или ухудшения окружающей среды [ИСО/МЭК Руководство 51].

Примечание — Это определение может потребоваться при проведении анализа опасностей и рисков (МЭК 61508-1, пункт 7.3). Если область применения должна быть расширена (например, с тем чтобы включить ухудшение окружающей среды, которое может не привести к травмам или причинению вреда здоровью), то это следует учесть на этапе «Полное определение области применения» жизненного цикла системы безопасности (МЭК 61508-1, пункт 7.3).

3.1.2 **опасность** (hazard): Потенциальный источник возникновения ущерба [ИСО/МЭК Руководство 51].

Примечание — Термин включает в себя опасности для людей, действующие в течение коротких промежутков времени (например, пожары и взрывы), а также опасности, имеющие долгосрочное влияние на здоровье людей (например, выделение токсических веществ).

3.1.3 **опасная ситуация** (hazardous situation): Обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности.

3.1.4 **опасное событие** (hazardous event): Опасная ситуация, результатом которой является ущерб.

3.1.5 **риск** (risk): Сочетание вероятности причинения ущерба и тяжести этого ущерба [ИСО/МЭК Руководство 51].

Примечание — Дальнейшее обсуждение этой концепции содержится в МЭК 61508-5 (приложение А).

3.1.6 **допустимый риск** (tolerable risk): Риск, который приемлем при данных обстоятельствах на основании существующих в текущий период времени ценностей в обществе.

Примечание — См. МЭК 61508-5 (приложение В).

3.1.7 **остаточный риск** (residual risk): Риск, остающийся после принятия мер защиты.

3.1.8 **безопасность** (safety): Отсутствие недопустимого риска.

3.1.9 **функциональная безопасность** (functional safety): Часть общей безопасности, которая относится к EUC и системам управления EUC и зависит от правильности функционирования E/E/PE систем, связанных с безопасностью, систем обеспечения безопасности, основанных на других технологиях, и внешних средств уменьшения риска.

3.1.10 **безопасное состояние** (safe state): Состояние EUC, в котором достигается безопасность.

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

3.1.11 **разумно предсказуемое неправильное использование** (reasonably foreseeable misuse): Использование продукта, процесса или услуги в условиях или с целью, не предусмотренных поставщиком, но которое может быть вызвано продуктом, процессом или услугой в сочетании с обычным поведением человека или в результате его.

3.2 Оборудование и устройства

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

Примечание — В МЭС 191-01-01 вместо функционального блока используется более общий термин «элемент». Элемент может иногда включать людей.

[ИСО/МЭК 2382-14-01-01]

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

Примечания

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

2 Данное определение без примечания 1 отличается от определения, приведенного в ИСО 2382-1, а полное определение отличается от определения, приведенного в ИСО 9000-3, добавлением слова данные.

3.2.3 **управляемое оборудование** (equipment under control (EUC)): Оборудование, машины, аппараты или установки, используемые для производства, обработки, транспортировки, в медицине или в иных процессах.

Примечание — Системы управления EUC представляют собой отдельное, отличное от EUC понятие.

3.2.4 **риск EUC** (EUC risk): Риск, связанный с EUC или с его взаимодействием с системой управления EUC.

Примечания

1 В этом контексте риск связан с конкретным опасным событием, в котором E/E/PE системы, связанные с безопасностью, системы обеспечения безопасности, основанные на иных технологиях, и внешние средства уменьшения риска используются для необходимого уменьшения риска (т.е. риск связан с функциональной безопасностью).

2 Риск EUC указан в МЭК 61508-5 (рисунок А.1, приложение А). Основная цель определения риска EUC состоит в том, чтобы установить понятие риска без учета E/E/PE систем, связанных с безопасностью, систем обеспечения безопасности, основанных на иных технологиях, и внешних средств уменьшения риска.

3 Оценка этого риска включает в себя факторы, связанные с человеком.

3.2.5 **программируемая электроника** (programmable electronic); PE: Основана на использовании компьютерных технологий и может включать в себя аппаратные средства 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 — Оборудование, перечисленное ниже, относится к программируемым электронным устройствам:

- ***микропроцессоры;***
- ***микроконтроллеры;***
- ***программируемые контроллеры;***
- ***специализированные интегральные схемы (ASIC);***
- ***программируемые логические контроллеры (ПЛК);***
- ***другие компьютеризованные устройства (например, интеллектуальные датчики, преобразователи, устройства привода).***

3.2.6 **электрический/электронный/программируемый электронный** (electrical/electronic/programmable electronic); E/E/PE: Основанный на электрической (E) и/или электронной (E), и/или программируемой электронной (PE) технологии.

Примечания

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

2 В число электрических/электронных/программируемых электронных устройств входят:

- электромеханические устройства (электрические);
- полупроводниковые непрограммируемые электронные устройства (электроника);
- электронные устройства, основанные на компьютерных технологиях (программируемые электронные); см. 3.2.5.

3.2.7 **язык с ограниченной варьируемостью** (limited variability language): Текстовый или графический язык программирования, предназначенный для коммерческих и промышленных программируемых электронных контроллеров, диапазон возможностей которого ограничен применением этих устройств.

ПРИМЕР — Ниже приведены примеры языков с ограниченной варьируемостью, взятые из МЭК 61131-3 и других источников, которые используются для представления прикладных программ для систем на основе ПЛК:

- ***многоступенчатые схемы: графический язык, состоящий из набора символов для входов (представляющих поведение, характерное для таких устройств, как нормально замкнутые или нормально разомкнутые контакты), соединенных с помощью линий (указывающих направление тока), с символами, обозначающими выходы (представляющими поведение, свойственное реле);***
- ***булева алгебра: язык низкого уровня, основанный на булевых операторах, таких как И, ИЛИ и НЕ с возможностью добавления некоторых мнемонических инструкций;***
- ***функциональные блоки диаграммы: в дополнение к булевым операторам допускается использование более сложных функций, таких как операции с файлами, чтение и запись блоков данных, команд для регистров сдвига и устройств, задающих последовательность;***

- последовательные функциональные схемы: графическое представление многостадийной программы, состоящее из взаимосвязанных шагов, действий и ориентированных связей с промежуточными состояниями.

3.3 Системы: общие аспекты

3.3.1 **система** (system): Набор элементов, которые взаимодействуют в соответствии с проектом, в котором элементом системы может быть другая система, называемая подсистемой; система может быть управляющей системой или управляемой системой и включать аппаратные средства, программное обеспечение и взаимодействие с человеком.

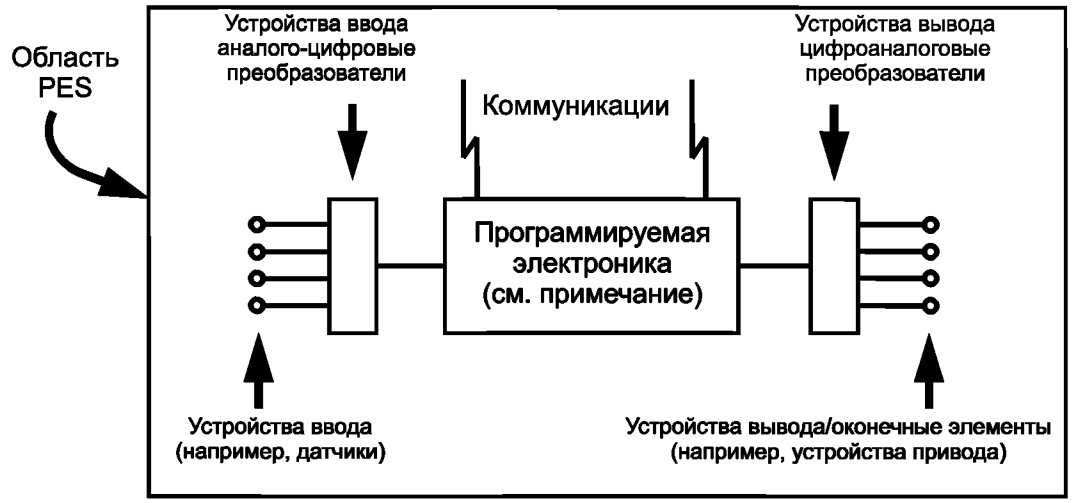
Примечания

1 Человек может быть частью системы, см. также 3.4.1, примечание 5.

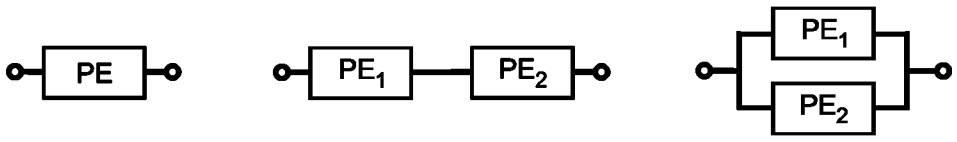
2 Это определение отличается от приведенного в МЭС 351-01-01.

3.3.2 **программируемая электронная система** (programmable electronic system); (PES): Система для 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 каналы связи, устройства привода и другие устройства вывода (см. рисунок 2).

Примечание — Структура PES показана на рисунке 2a). Рисунок 2b) демонстрирует способ представления PES, применяемый в настоящем стандарте, когда программируемая электроника показывается отдельно от датчиков и устройств привода EUC и их интерфейсов, но при этом программируемая электроника может присутствовать в нескольких местах PES. Рисунок 2c) показывает PES с двумя отдельными блоками программируемой электроники. Рисунок 2d) показывает PES с дублированием программируемой электроники (т. е. двухканальную), но с одним датчиком и одним устройством привода.



a) Структура базовой PES



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

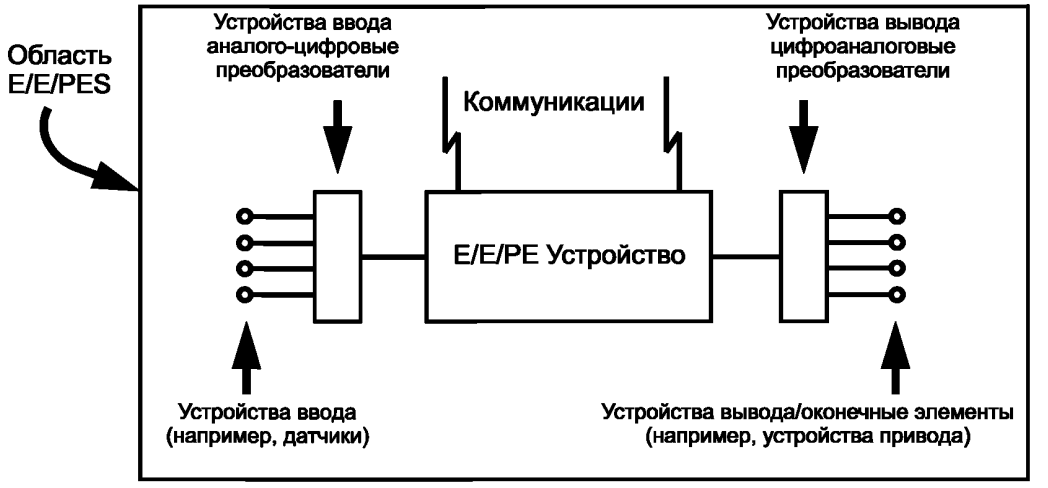
c) Одиночная PES с двумя программируемыми электронными устройствами, соединенными последовательно (например, интеллектуальный датчик и программируемый контроллер)

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

Примечание — Программируемая электроника показана в центре, но она может присутствовать в нескольких местах PES.

Рисунок 2 — Программируемая электронная система (PES): структура и терминология

3.3.3 **электрическая/электронная/программируемая электронная система** (electrical/electronic/programmable electronic system); E/E/PES: Система для управления, защиты или мониторинга, основанная на использовании одного или нескольких электрических/электронных/программируемых электронных (E/E/PE) устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммуникационные магистрали, устройства привода и другие устройства вывода (рисунок 3).



Примечание — E/E/PE устройство показано в центре, но оно(и) может присутствовать в нескольких местах E/E/PES.

Рисунок 3 — Электрическая/электронная/программируемая электронная система (E/E/PES): структура и терминология

3.3.4 **система управления EUC** (EUC control system): Система, которая реагирует на входные сигналы, поступающие от процесса и/или от оператора, и генерирует выходные сигналы, которые позволяют EUC работать в необходимом режиме.

Примечание — Система управления EUC включает в себя устройства ввода и оконечные элементы.

3.3.5 **архитектура** (architecture): Конкретная конфигурация элементов аппаратных средств и программного обеспечения системы.

3.3.6 **модуль** (module): Программа, дискретный компонент или функциональный набор инкапсулированных программ либо дискретных компонентов, объединенных между собой.

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

Примечание — E/E/PE устройство показано в центре, но такое устройство(а) может (могут) присутствовать в нескольких местах.

3.3.8 **канал** (channel): Элемент или группа элементов, которые независимо выполняют функцию.

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

Примечания

1 В число элементов канала могут входить модули ввода/вывода, логическая система (см. 3.4.5), датчики и оконечные элементы.

2 Термин допускается использовать для описания полных систем или частей системы (например, датчиков или оконечных элементов).

3.3.9 **разнообразие** (diversity): Различные средства для выполнения требуемой функции.

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

3.3.10 **избыточность** (redundancy): Существование средств в дополнение к средствам, которые могут быть достаточны функциональному блоку для выполнения требуемой операции, данным для представления информации.

ПРИМЕР — Примерами избыточности являются дублирование функциональных компонентов и добавление битов четности.

Примечания

1 Избыточность используется в первую очередь для повышения надежности или работоспособности.

2 Определение в МЭС 191-15-01 является менее полным [ИСО/МЭК 2382-14-01-12].

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 того, чтобы достигнуть и поддерживать безопасное состояние для EUC, и

- предназначена для достижения своими собственными средствами или в сочетании с другими E/E/PE системами, связанными с безопасностью, системами обеспечения безопасности, основанными на других технологиях, или внешними средствами уменьшения, необходимого уровня полноты безопасности для требуемых функций безопасности.

Примечания

1 Этот термин относится к системам, обозначающимся как системы, связанные с безопасностью, и предназначенным для достижения, совместно с внешними средствами уменьшения риска (см. 3.4.3), необходимого снижения риска для того, чтобы удовлетворять требованиям допустимого риска (см. 3.1.6). См. также МЭК 61508-5 (приложение А).

2 Системы, связанные с безопасностью, предназначены для того, чтобы предотвратить переход EUC в опасное состояние выполнением необходимых действий после получения команд. Отказ системы, связанной с безопасностью, может быть включен в события, ведущие к возникновению определенной опасности или опасностей. Хотя могут существовать и другие системы, имеющие функции безопасности, именно системы, связанные с безопасностью, предназначены для достижения требуемого допустимого риска. В широком смысле системы, связанные с безопасностью, могут быть разделены на две категории: управляющие и защитные; эти системы работают в двух режимах (см. 3.5.12).

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

4 Система, связанная с безопасностью, может:

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

b) быть предназначена для смягчения последствий опасного события, уменьшая риск уменьшением последствий;

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

5 Человек может быть частью системы, связанной с безопасностью (см. 3.3.1). Например, человек может получать информацию от программируемого электронного устройства и выполнять действие, связанное с безопасностью, основываясь на этой информации, либо выполнять действие с помощью программируемого электронного устройства.

6 Термин включает все аппаратные средства, программное обеспечение и дополнительные средства (например, источники питания), которые необходимы для выполнения указанных функций безопасности (датчики, другие устройства ввода, оконечные элементы (устройства привода) и другие устройства вывода включаются, следовательно, в системы, связанные с безопасностью).

7 Система, связанная с безопасностью, может основываться на широком диапазоне технологий, включая электрическую, электронную, программируемую электронную, гидравлическую и пневматическую.

3.4.2 **система обеспечения безопасности, основанная на других технологиях** (other technology safety-related system): Система, связанная с безопасностью, которая основана на технологиях иных, чем электрическая/ электронная/программируемая электронная.

ПРИМЕР — Примером системы обеспечения безопасности, основанной на других технологиях, является перепускной клапан.

3.4.3 **внешнее средство уменьшения риска** (external risk reduction facility): Мера, предназначенная для уменьшения или ослабления рисков, которая является отдельной и отличной и не использует E/E/PE системы, связанные с безопасностью, или системы обеспечения безопасности, основанные на других технологиях.

ПРИМЕР — Дренажная система, брандмауэр и плотина относятся к внешним средствам уменьшения риска.

3.4.4 **E/E/PE системы, связанные с безопасностью, имеющие низкую сложность** (lowcomplexity E/E/PE safety-related system): E/E/PE системы, связанные с безопасностью (см. 3.2.6 и 3.4.1), в которых:

- режимы отказа каждого из компонентов четко определены;
- поведение системы в условиях отказа может быть полностью определено.

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

ПРИМЕР — Система, включающая в себя один или несколько концевых выключателей, работающая, возможно, с использованием нескольких промежуточных электромеханических реле, один или несколько контакторов и предназначенная для отключения напряжения от электрического двигателя, представляет собой E/E/PE систему, связанную с безопасностью, низкой сложности.

3.4.5 **логическая система** (logic system): Часть системы, выполняющая логические функции, исключая датчики и оконечные элементы.

Примечание — В настоящем стандарте используют следующие логические системы:

- электрическую логическую систему для электромеханической технологии;
- электронную логическую систему для электронной технологии;
- программируемую электронную логическую систему для программируемых электронных систем.

3.5 Функции безопасности и полнота безопасности

3.5.1 **функция безопасности** (safety function): Функция, реализуемая E/E/PE системой, связанной с безопасностью, системой обеспечения безопасности, основанной на других технологиях, или внешними средствами снижения риска, которая предназначена для достижения или поддержания безопасного состояния EUC по отношению к конкретному опасному событию (см. 3.4.1).

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

Примечания

1 Чем выше уровень полноты безопасности системы, связанной с безопасностью, тем ниже вероятность того, что система, связанная с безопасностью, не сможет выполнить требуемые функции безопасности.

2 Имеется четыре уровня полноты безопасности для систем (см. 3.5.6).

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

4 Полнота безопасности включает полноту безопасности аппаратуры (см. 3.5.5) и полноту безопасности по отношению к систематическим отказам (см. 3.5.4).

5 Данное определение фокусируется на надежности систем, связанных с безопасностью, при выполнении функций безопасности (определение надежности см. в МЭС 191-12-01).

3.5.3 **полнота безопасности программного обеспечения** (software safety integrity): Количественная характеристика, которая означает вероятность того, что программное обеспечение программируемой электронной системы будет выполнять специфицированные функции обеспечения безопасности при всех установленных условиях в течение установленного периода времени.

3.5.4 **полнота безопасности по отношению к систематическим отказам** (systematic safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, по отношению к систематическим отказам (см. 3.5.2 (примечание 3)), проявляющаяся в опасном режиме.

Примечания

1 Обычно полнота безопасности по отношению к систематическим отказам не может быть охарактеризована количественно (в отличие от полноты безопасности аппаратных средств, которой, как правило, может быть дана количественная оценка).

2 См. 3.5.2, 3.5.5 и 3.6.6.

3.5.5 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью по отношению к случайным отказам аппаратуры, проявляющимся в опасном режиме.

Примечания

1 Данный термин относится к отказам, проявляющимся в опасном режиме, к тем отказам, которые могут ухудшить полноту безопасности. Данная ситуация характеризуется двумя параметрами: суммарной интенсивностью опасных отказов и вероятностью отказа в выполнении запроса. Первый из этих параметров надежности используется при необходимости осуществлять непрерывный контроль над поддержанием безопасности, второй параметр применяется в контексте связанных с безопасностью систем защиты.

2 См. 3.5.2, 3.5.4 и 3.6.5.

3.5.6 **уровень полноты безопасности** (safety integrity level (SIL)): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности для функций безопасности, который ставится в соответствие E/E/PE системам, связанным с безопасностью; уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности.

Примечание — Меры целевых отказов (см. 3.5.13) для четырех уровней полноты безопасности указаны в МЭК 61508-1 (таблицы 2 и 3).

3.5.7 **уровень полноты безопасности программного обеспечения** (software safety integrity level): Дискретный уровень (принимающий одно значение из четырех возможных), определяющий полноту безопасности программного обеспечения в системе, связанной с безопасностью.

Примечание — См. 3.5.3 и 3.5.6.

3.5.8 **спецификация требований к безопасности** (safety requirements specification): Спецификация, содержащая все требования к функциям безопасности, которые должны быть выполнены системами, связанными с безопасностью.

Примечание — Данная спецификация разделяется на:
- спецификацию требований к функциям безопасности (см. 3.5.9);
- спецификацию требований к полноте безопасности (см. 3.5.10).

3.5.9 **спецификация требований к функциям безопасности** (safety functions requirements specification): Спецификация, содержащая требования к функциям безопасности, которые должны выполняться системами, связанными с безопасностью.

Примечания

1 Данная спецификация является частью (относящейся к функциям безопасности) спецификации требований к безопасности (см. 3.5.8), содержащей 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.

3.5.10 **спецификация требований к полноте безопасности** (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 (см. 3.5.8).

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

3.5.12 **режим работы** (mode of operation): Способ предполагаемого использования системы, связанной с безопасностью, по отношению к частоте обращений к ней; может быть:

либо режимом с низкой частотой запросов, когда частота запросов на выполнение операции системы, связанной с безопасностью, не превышает одного в год или не превышает более чем в два раза частоту запроса, зарегистрированную во время контрольных испытаний,

либо режимом с высокой частотой запросов или режимом непрерывной работы, когда частота запросов на выполнение операции системы, связанной с безопасностью, превышает один в год или

превышает более чем в два раза частоту запроса, зарегистрированную во время контрольных испытаний.

Примечания

1 Режим высокой частоты запросов или непрерывной работы охватывает те системы, относящиеся к безопасности, которые реализуют непрерывный контроль над поддержанием функциональной безопасности.

2 Целевые меры отказов для систем, связанных с безопасностью, работающих в режиме низкой частоты запросов, а также в режиме высокой частоты запросов и в режиме непрерывной работы, определены в 3.5.13.

3.5.13 **целевая мера 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 отказа при выполнении запроектированной функции по запросу (для режима работы с низкой частотой запросов);
- либо в виде вероятности возникновения опасных отказов в течение часа (для режима с высокой частотой запросов или непрерывной работы).

Примечание — Числовые значения для целевых мер отказов даны в МЭК 61508-1 (таблицы 2 и 3).

3.5.14 **необходимое уменьшение риска** (necessary risk reduction): Уменьшение риска, которое должно быть достигнуто E/E/PE системой, связанной с безопасностью, системой обеспечения безопасности, основанной на других технологиях, и внешними средствами снижения риска для гарантии того, что не будет превышен допустимый уровень риска.

3.6 Сбой, отказ и ошибка

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

Примечание — МЭС 191-05-01 определяет «сбой» как состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая неспособности, возникающие во время профилактического ухода или других плановых мероприятий, либо в результате недостатка внешних ресурсов. Иллюстрация к этим двум точкам зрения показана на рисунке 4 [ИСО/МЭК 2382-14-01-10].

3.6.2 **предотвращение сбоя** (fault avoidance): Использование методов и процедур, предназначенных для предотвращения возникновения сбоев во время любой фазы жизненного цикла систем, связанных с безопасностью.

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

Примечание — Определение, приведенное в МЭС 191-15-05, относится только к отказам подкомпонентов. См. примечание к 3.6.1 [ИСО/МЭК 2382-14-04-06].

3.6.4 **отказ** (failure): Прекращение способности функционального блока выполнять необходимую функцию.

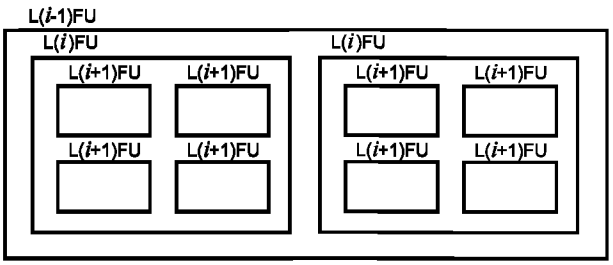
Примечания

1 Определение в МЭС 191-04-01 является идентичным, с дополнительными комментариями [ИСО/МЭК 2382-14-01-11].

2 Соотношение между сбоями и отказами в МЭК 61508 и МЭС 60050(191) см. на рисунке 4.

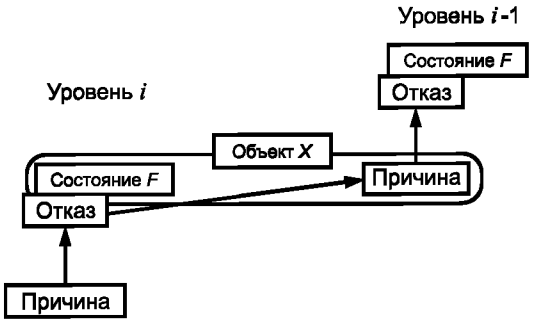
3 Характеристики требуемых функций неизбежно исключают определенные режимы работы, некоторые функции могут быть определены путем описания режимов, которых следует избегать. Возникновение таких режимов представляет собой отказ.

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

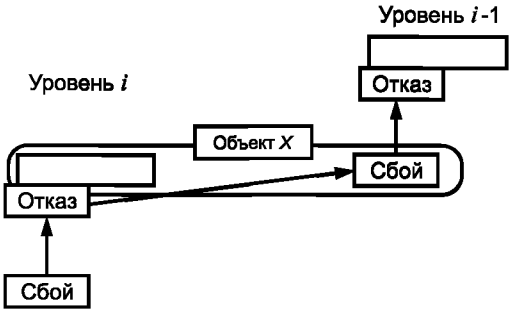


(L — уровень; i = 1, 2, 3, . . . ; FU — функциональный блок)

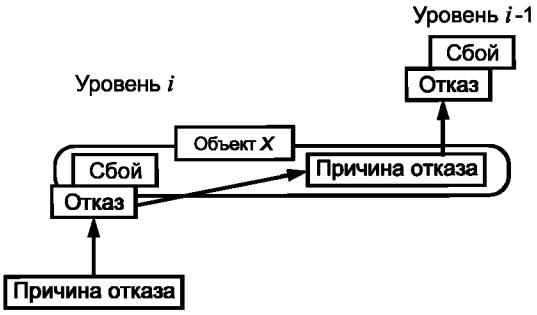
a) конфигурация функционального блока



b) обобщенный вид



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



d) с точки зрения МЭК 60050 (191)

Примечания

1 Как показано на рисунке 4a), функциональный блок может быть представлен в виде многоуровневой иерархической конструкции, 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 она не будет исправлена или нейтрализована, эта ошибка может привести к отказу данного функционального блока, который в результате перейдет в состояние F, в котором он более не может выполнять необходимую функцию (см. рисунок 4b)). 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 F функционального блока уровня i, в которое он попадает в результате отказа, а также как причина отказа функционального блока уровня i-1. Данный «объект X» объединяет концепцию «отказа» в МЭК 61508 и ИСО/МЭК 2382-14, в которой внимание акцентируется на причинном аспекте, как показано на рисунке 4c), и концепцию «отказа» из МЭС 60050(191), в которой основное внимание уделено аспекту состояния, как показано на рисунке 4d). В МЭС 60050(191) состояние F называется отказом, а в МЭК 61508 и ИСО/МЭК 2382-14 оно не определено.

3 В некоторых случаях отказ или ошибка могут быть вызваны внешним событием, таким 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 аппаратуры** (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик аппаратных средств.

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, отказы оборудования включают в себя много факторов, они происходят с предсказуемой частотой, но в непредсказуемые (т. е. случайные) моменты времени.

2 Основное различие между случайными отказами аппаратуры и систематическими отказами (см. 3.6.6) состоит в том, что интенсивность отказов системы (или другие подобные характеристики таких отказов), связанная со случайными отказами аппаратуры, может быть прогнозируема с достаточной степенью точности, но систематические отказы по своей природе не могут быть предсказаны точно. Это означает, что интенсивность отказов системы, связанных со случайными отказами аппаратуры, может быть охарактеризована количественно с достаточной степенью точности, тогда как отказы системы, связанные с систематическими отказами, не могут быть охарактеризованы статистически 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 некоторой причиной, который может быть исключен только путем модификации проекта, либо производственного процесса, операций, документации, либо других факторов.

Примечания

1 Корректирующее сопровождение без модификации обычно не устраняет причину отказа.

2 Систематический отказ может быть воспроизведен имитацией причины отказа [МЭС 191-04-19].

3 Примерами причин систематических отказов являются ошибки человека:

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

4 В настоящем стандарте отказы в системах, связанных с безопасностью, разделяются на случайные отказы аппаратуры и систематические отказы (см. 3.6.4 и 3.6.5).

3.6.7 **опасный отказ** (dangerous failure): Отказ, который может привести к тому, что система, связанная с безопасностью, перейдет в опасное состояние или в состояние ошибки при выполнении функции.

Примечание — Будут или не будут реализованы опасные последствия отказа, зависит от канальной архитектуры системы; в многоканальных системах опасные отказы с меньшей вероятностью ведут к итоговому опасному состоянию или состоянию отказа при выполнении функции.

3.6.8 **безопасный отказ** (safe failure): Отказ, который не переводит систему, связанную с безопасностью, в опасное состояние или в состояние отказа при выполнении функции.

Примечание — Будут или не будут реализованы опасные последствия отказа, зависит от канальной архитектуры системы; в системах с многоканальной архитектурой, предназначенных для повышения безопасности, безопасный отказ аппаратуры приведет к ошибочному отключению с меньшей вероятностью.

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 тогда, когда $P(A + B) > P(A) \times P(B)$.

3.6.10 **отказ с общей причиной** (common cause failure): Отказ, который является результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, ведущие к отказу системы.

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

Примечание — Адаптировано из МЭС 191-05-24 путем исключения примечаний.

3.6.12 **ошибка человека** (human error, mistake): Действие или бездействие человека, которое может привести к непредусмотренному результату [ИСО/МЭК 2382-14-01-09].

Примечание — Адаптировано из МЭС 191-05-25 путем добавления слов «или бездействие».

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, который начинается со стадии разработки концепции проекта и заканчивается, когда все E/E/PE системы, связанные с безопасностью, системы обеспечения безопасности, основанные на иных технологиях, и внешние средства уменьшения риска уже не используются.

Примечания

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

2 Модели жизненного цикла систем безопасности, использованные в настоящем стандарте, приведены в МЭК 61508-1 (рисунки 2—4).

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, когда программное обеспечение окончательно перестает эксплуатироваться.

Примечания

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

2 Программное обеспечение не может поддерживаться, точнее сказать, оно модифицируется.

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

Примечание — Более подробное описание управления конфигурацией приведено в МЭК 61508-7 (пункт С.5.24).

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

Примечание — В контексте программного обеспечения см. МЭК 61508-7 (пункт С.5.23).

3.8 Подтверждение мер безопасности

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

Примечания

1 Адаптировано из ИСО 8402 путем исключения примечаний.

2 В контексте настоящего стандарта верификация представляет собой выполняемую для каждой стадии жизненного цикла соответствующей системы безопасности (общей, E/E/PES систем и программного обеспечения) путем анализа и/или тестирования демонстрацию того, что для используемых входных данных компоненты удовлетворяют во всех отношениях набору задач и требований для соответствующей стадии.

ПРИМЕР — Процесс верификации включает в себя:

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

- просмотр проектов;

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

- проверка интеграции, реализуемая внешними тестами, для всех систем, образующихся покомпонентным добавлением к исходной системе, и необходимая для того, чтобы убедиться, что все компоненты работают вместе в соответствии со спецификацией.

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

Примечания

1 Адаптировано из ИСО 8402 путем исключения примечаний.

2 В настоящем стандарте имеется три фазы подтверждения соответствия:

- подтверждение соответствия общей системы безопасности (МЭК 61508-1 (рисунок 2));
- подтверждение соответствия E/E/PES системы (МЭК 61508-1 (рисунок 3));
- подтверждение соответствия программного обеспечения (МЭК 61508-1 (рисунок 4)).

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

3.8.3 **оценка функциональной безопасности** (functional safety assessment): Исследование, основанное на фактах, предназначенное для того, чтобы оценить функциональную безопасность, достигаемую одной или несколькими E/E/PE системами, связанными с безопасностью, системами обеспечения безопасности, основанными на других технологиях, или внешними 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 того, чтобы требования к функциональной безопасности согласовались с запланированными мероприятиями и 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, выполняемая для того, чтобы обнаружить 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.

Примечание — Эффективность контрольных проверок зависит от того, насколько близко к «исходному» состоянию восстанавливается система. Для того чтобы контрольная проверка была абсолютно эффективна, она должна быть в состоянии обнаруживать 100 % опасных отказов. Хотя на практике достигнуть 100 % не просто, если только это не E/E/PE система, связанная с безопасностью, имеющая низкую сложность, однако такая цель должна стоять. По крайней мере, все выполняемые функции безопасности должны проверяться в соответствии со спецификацией требований к безопасности E/E/PES системы. При использовании отдельных каналов эти проверки выполняются для каждого канала отдельно.

3.8.6 **диагностический охват** (diagnostic coverage): Частичное уменьшение вероятности опасных отказов аппаратуры, связанное с выполнением автоматических диагностических проверок.

Примечания

1 Определение может быть также представлено с помощью следующего уравнения, где *DC* представляет собой охват диагностический, λ_{DD} — вероятность обнаруженных опасных отказов, а λ_{total} — вероятность всех опасных отказов:

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

2 Охват диагностический может относиться ко всей системе, связанной с безопасностью, или к ее части. Например, охват диагностический может относиться к датчикам и/или к логической системе, и/или к концевым элементам.

3 Термины «охват безопасных отказов диагностикой» или «охват диагностический», включая безопасные отказы, используют соответственно для описания относительного уменьшения вероятности безопасных отказов или и опасных, и безопасных отказов в результате выполнения автоматических диагностических проверок.

3.8.7 **интервал диагностических проверок** (diagnostic test interval): Интервал между неавтономными проверками, предназначенными для того, чтобы обнаружить отказы в системах обеспечения безопасности с заданным охватом диагностикой.

3.8.8 **обнаруженный** (detected): По отношению к аппаратным средствам — выявленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физического осмотра и ручной проверки) либо в ходе нормальной работы.

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

3.8.9 **необнаруженный** (undetected): По отношению к аппаратному обеспечению — не выявленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физического осмотра и ручной проверки) либо в ходе нормальной работы.

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

3.8.10 **независимое лицо** (independent person): Лицо, независимое и не связанное с процессами, происходившими во время конкретной стадии жизненного цикла подсистем безопасности E/E/PES системы в целом или программного обеспечения, которое выполняет оценку или приемку функциональной безопасности и которое не несет прямой ответственности за эти процессы.

3.8.11 **независимое подразделение** (independent department): Подразделение, независимое и не связанное с подразделениями, отвечающими за процессы, которые имеют место в течение конкрет-

ной стадии жизненного цикла подсистем безопасности E/E/PES, системы в целом или программного обеспечения, которое выполняет оценку или приемку функциональной безопасности.

3.8.12 **независимая организация** (independent organisation): Организация, отдельная и отличная в отношении управления и других ресурсов, от организаций, отвечающих за процессы, которые имеют место в течение конкретной стадии жизненного цикла подсистем безопасности E/E/PES, системы в целом или программного обеспечения, которая выполняет оценку и приемку функциональной безопасности.

3.8.13 **анимация** (animation): Имитация работы программной системы (или существенной части этой системы) для отображения существенных аспектов поведения системы, применяемая, 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 удовлетворяет реальным требованиям, поскольку она улучшает восприятие человеком заданного поведения системы.

3.8.14 **динамическое тестирование** (dynamic testing): Работа программного обеспечения и/или работа аппаратных средств, выполняемая в режиме контроля и систематически для демонстрации наличия требуемого их поведения и отсутствия нежелательного поведения системы.

Примечание — Динамическое тестирование представляет собой противоположность статическому анализу, при котором не требуется выполнения программ.

3.8.15 **тестовая программа** (test harness): Программное средство, которое может имитировать (до некоторой степени) среду, в которой будет работать разрабатываемое программное обеспечение или аппаратные средства, путем подачи на вход программы тестовых данных и регистрации ответа на выходе.

Примечание — Тестовая программа может также включать в себя генератор тестовых данных и средства верификации результатов проверки (либо автоматической проверки на допустимые значения, либо с помощью ручного анализа).

Приложение А
(справочное)

Указатель терминов

анализ влияния	3.7.4
анимация	3.8.13
архитектура	3.3.5
аудит функциональной безопасности	3.8.4
безопасность	3.1.8
безопасность функциональная	3.1.9
блок функциональный	3.2.1
верификация	3.8.1
избыточность	3.3.10
интервал диагностических проверок	3.8.7
использование неправильное разумно предсказуемое	3.1.11
канал	3.3.8
лицо независимое	3.8.10
модуль	3.3.6
модуль программный	3.3.7
необнаруженный	3.8.9
обеспечение программное	3.2.2
обеспечение программное, связанное с безопасностью	3.5.11
обнаруженный	3.8.8
оборудование управляемое (EUC)	3.2.3
опасность	3.1.2
организация независимая	3.8.12
отказ	3.6.4
отказ аппаратуры случайный	3.6.5
отказ безопасный	3.6.8
отказ зависимый	3.6.9
отказ опасный	3.6.7
отказ систематический	3.6.6
отказ с общей причиной	3.6.10
охват диагностический	3.8.6
оценка функциональной безопасности	3.8.3
ошибка	3.6.11
ошибка человека	3.6.12
подразделение независимое	3.8.11
подтверждение соответствия	3.8.2
полнота безопасности	3.5.2
полнота безопасности аппаратных средств	3.5.5
полнота безопасности по отношению к систематическим отказам	3.5.4
полнота безопасности программного обеспечения	3.5.3
предотвращение сбоя	3.6.2
проверка контрольная	3.8.5
программа тестовая	3.8.15
разнообразие	3.3.9
режим работы	3.5.12
риск	3.1.5
риск EUC	3.2.4
риск допустимый	3.1.6
сбой	3.6.1
система	3.3.1
система логическая	3.4.5
система обеспечения безопасности, основанная на других технологиях	3.4.2
система программируемая электронная (PES)	3.3.2

система, связанная с безопасностью	3.4.1
система управления EUC	3.3.4
система электрическая/электронная/программируемая электронная (E/E/PES)	3.3.3
E/E/PE системы, связанные с безопасностью, имеющие низкую сложность	3.4.4
ситуация опасная	3.1.3
событие опасное	3.1.4
состояние безопасное	3.1.10
спецификация требований к безопасности	3.5.8
спецификация требований к полноте безопасности	3.5.10
спецификация требований к функциям безопасности	3.5.9
средство уменьшения риска внешнее	3.4.3
тестирование динамическое	3.8.14
уменьшение риска необходимое	3.5.14
управление конфигурацией	3.7.3
уровень полноты безопасности (SIL)	3.5.6
уровень полноты безопасности программного обеспечения	3.5.7
устойчивость к отказам	3.6.3
ущерб	3.11
функция безопасности	3.5.1
целевая мера отказов	3.5.13
цикл программного обеспечения жизненный	3.7.2
цикл систем безопасности жизненный	3.7.1
электрический/электронный/программируемый электронный (E/E/PE)	3.2.6
электроника программируемая (PE)	3.2.5
язык с ограниченной варьируемостью	3.2.7

Приложение В
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица В.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта Российской Федерации
МЭК 61508-1:1998	ГОСТ Р МЭК 61508-1—2007 (МЭК 61508-1—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
МЭК 61508-2:2000	*
МЭК 61508-3:1998	ГОСТ Р МЭК 61508-3—2007 (МЭК 61508-3 1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
МЭК 61508-5:1998	ГОСТ Р МЭК 61508-5—2007 (МЭК 61508-5—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
МЭК 61508-6:2000	*
МЭК 61508-7:2000	*
ИСО/МЭК Руководство 51:1999	ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты
МЭК Руководство 104:1997	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.	

Библиография

МЭК 61131-3:1993	Программируемые контроллеры. Часть 3. Языки программирования
МЭК 61151:1992	Инструменты для атомной промышленности. Усилители и предварительные усилители, используемые в детекторах ионизирующего излучения. Процедуры проверки
ИСО/МЭК 2382-1:1993	Информационные технологии. Словарь. Часть 1. Фундаментальные термины
ИСО/МЭК 90003:2004	Техника программного обеспечения. Рекомендации по применению ISO 9001:2000 к компьютерному программному обеспечению

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

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

Редактор *Р.Г. Говердовская*
Технический редактор *Л.А. Гусева*
Корректор *А.С. Черноусова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 23.04.2008. Подписано в печать 06.06.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 3,26. Уч.-изд. л. 2,70. Тираж 248 экз. Зак. 669.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru