ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-2— 2012

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

Часть 2

Требования к системам

IEC 61508-2:2010

Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

(IDT)

Издание официальное

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» и Федеральным бюджетным 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 от 29 октября 2012 г. № 587-ст

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

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 ДА

5 ВЗАМЕН ГОСТ Р МЭК 61508-2—2007

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 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 (gost.ru)

Содержание

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 программируемыми электронными системами), применяемые во всех прикладных отраслях для выполнения функций, не связанных с безопасностью, во все более увеличивающихся объемах 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 всех стадий 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 того, чтобы разработать рациональную и последовательную техническую политику для всех электрических систем обеспечения безопасности. Основной целью при этом 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].

В большинстве ситуаций 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 все подсистемы безопасности, входящие в состав общей системы обеспечения безопасности. Таким образом, хотя настоящий стандарт рассматривает электрические/электронные/программируемые (Э/Э/ПЭ) системы, связанные с безопасностью, предлагаемый в нем подход можно использовать также при рассмотрении систем, связанных с безопасностью, базирующихся на других технологиях.

Признанным фактом является существование огромного разнообразия приложений, использующих Э/Э/ПЭ системы в различных областях применений, отличающихся различной степенью сложности, возможными рисками и опасностями. В каждом конкретном применении необходимые меры безопасности будут зависеть от многочисленных факторов, которые являются специфичными для этого применения. Настоящий стандарт, являясь базовым, позволит сформулировать такие меры в будущих международных стандартах для изделий и областей применения, а также в следующих редакциях уже существующих стандартов.

Настоящий стандарт:

- рассматривает все соответствующие стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (например, от первоначальной концепции, через проектирование, реализацию, эксплуатацию, техническое обслуживание вплоть до снятия с эксплуатации), в ходе которых Э/Э/ПЭ системы используются для выполнения функций безопасности;
- был разработан с учетом быстрого развития технологий; его основа является в значительной мере устойчивой и полной для применения во время будущих разработок;
- делает возможной разработку стандартов для продукции и областей применения, в которых используются Э/Э/ПЭ системы, связанные с безопасностью; разработка стандартов для продукции и областей применения в рамках общей структуры, определенной 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 как в плане безопасности, так и в плане экономики;
- устанавливает метод разработки спецификации требований к безопасности, необходимых для достижения заданной функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью;
- применяет для определения требований к уровням полноты безопасности подход, основанный на оценке рисков;

- вводит уровни полноты безопасности при задании целевого уровня полноты безопасности для функций безопасности, которые должны быть реализованы Э/Э/ПЭ системами, связанными с безопасностью.

Примечание — Настоящий стандарт не устанавливает требования к уровню полноты безопасности для любой функции безопасности и не определяет того, как устанавливается уровень полноты безопасности. Однако настоящий стандарт формирует основанный на риске концептуальный подход и предлагает 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, работающих:

- 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};

- в режиме высокой интенсивности запросов на обслуживание или режиме с непрерывным запросом, нижняя граница устанавливается в соответствии с вероятностью 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 к 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 стойкость к систематическим отказам, применяемую к элементу, характеризующую 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» могут быть использованы, но для этого необходимо обеспечить подходящие требования в соответствующих разделах настоящего стандарта, которым эти понятия должны соответствовать.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Часть 2

Требования к системам

Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems

Дата введения — 2013—08—01

1 Область применения

1.1 Настоящий стандарт:

a) применяют только совместно с МЭК 61508-1, описывающим общий подход для достижения функциональной безопасности;

b) применяется (как определено в МЭК 61508-1) к любой системе, связанной с безопасностью, которая содержит хотя бы один электрический, электронный или программируемый электронный компонент;

c) применяется ко всем подсистемам и их компонентам внутри Э/Э/ПЭ систем, связанных с безопасностью (включая датчики, исполнительные устройства и интерфейс оператора);

d) определяет, как преобразовать спецификацию требований к Э/Э/ПЭ системе безопасности, разработанную в соответствии с МЭК 61508-1 (включающую в себя спецификацию требований к функциям безопасности Э/Э/ПЭ системы и спецификацию требований к полноте безопасности Э/Э/ПЭ системы), в спецификацию требований проектирования Э/Э/ПЭ системы;

e) устанавливает требования к действиям, которые должны быть реализованы на стадиях проектирования и изготовления Э/Э/ПЭ систем, связанных с безопасностью (то есть формирует модель жизненного цикла Э/Э/ПЭ системы безопасности), за исключением требований к программному обеспечению, которые рассмотрены в МЭК 61508-3 (см. рисунки 2—4). Эти требования включают в себя указания по применению, ранжированные по уровням полноты безопасности, методов и средств, для предотвращения ошибок и отказов и управления ошибками и отказами;

f) определяет информацию, необходимую для установки, ввода в эксплуатацию и заключительного подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью;

g) не определяет стадии эксплуатации и технического обслуживания Э/Э/ПЭ систем, связанных с безопасностью (см. МЭК 61508-1), но содержит требования для подготовки информации и процедур, необходимых пользователям для эксплуатации и технического обслуживания Э/Э/ПЭ систем, связанных с безопасностью;

h) определяет требования, предъявляемые к организациям, осуществляющим модификацию Э/Э/ПЭ систем, связанных с безопасностью.

Примечания

1 Настоящий стандарт главным образом предназначен для поставщиков и/или технических департаментов внутри компаний, отвечающих в том числе за формирование и реализацию требований по модификации Э/Э/ПЭ систем, связанных с безопасностью.

2 Взаимосвязь между настоящим стандартом и МЭК 61508-3 показана на рисунке 4;

i) не применяется для медицинского оборудования в соответствии с серией стандартов МЭК 60601 [4].

Издание официальное

1.2 МЭК 61508-1 — 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 (МЭК 61508-4, пункт 3.4.3). В качестве базовых стандартов по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с принципами, изложенными в руководстве МЭК 104 и руководстве ИСО/МЭК 51. 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].

1.3 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 на них нет конкретной ссылки, или они не включены в стандарты, подготовленные этими техническими комитетами.

Примечание — Функциональная безопасность Э/Э/ПЭ систем, связанных с безопасностью, может достигаться только в случае, если удовлетворены все установленные для них требования. Поэтому важно, чтобы все эти требования были тщательно проанализированы и обоснованы.

1.4 Рисунок 1 показывает общую структуру частей 1—7 МЭК 61508 и указывает на роль, которую играет настоящий стандарт в достижении функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью. МЭК 61508-6 (приложение А) содержит описание применения настоящего стандарта и МЭК 61508-3.

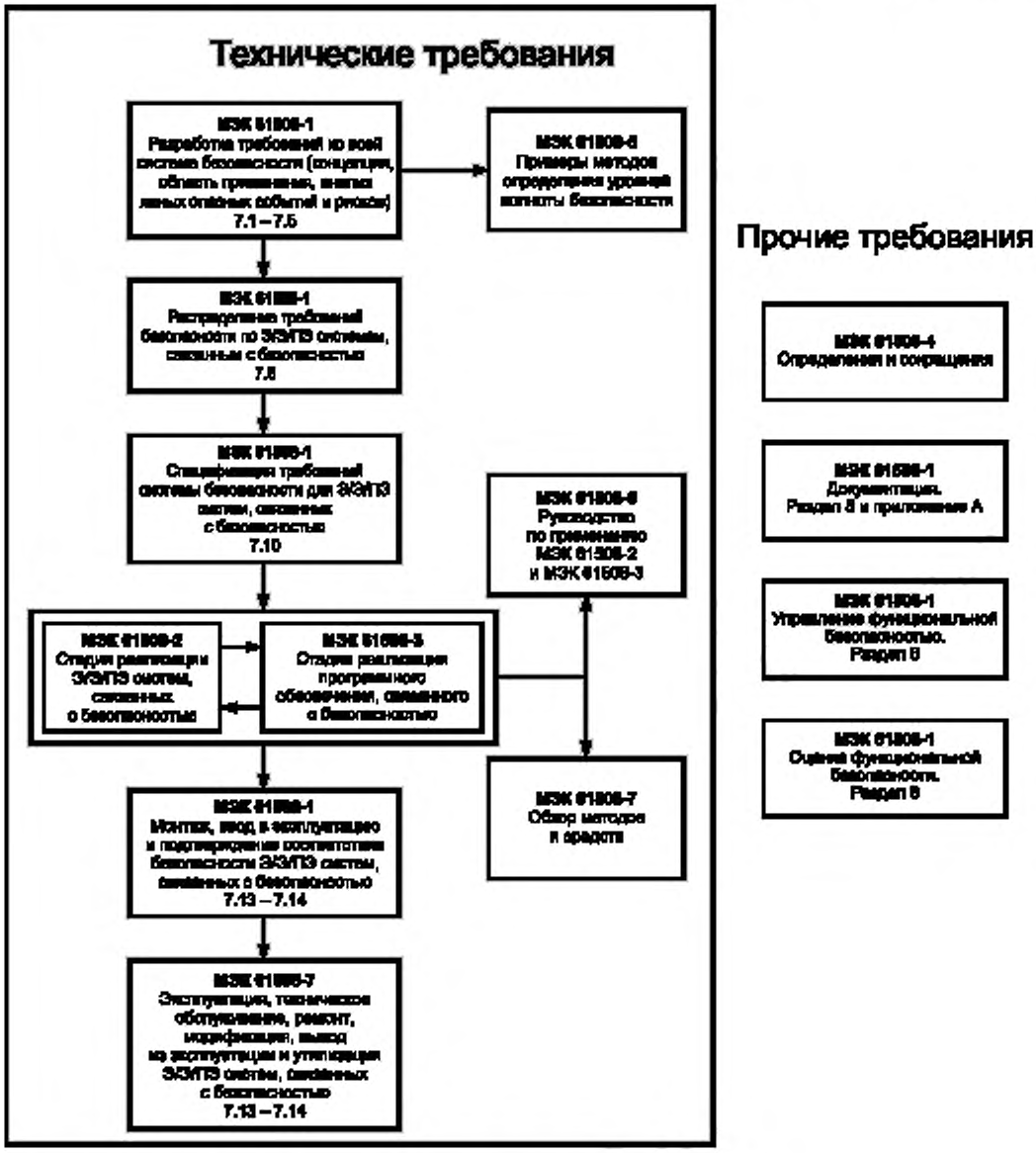


Рисунок 1 — Общая структура серии ГОСТ Р МЭК 61508

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

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)

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 60947-5-1 Низковольтная коммутационная аппаратура и механизм управления. Часть 5-1. Оборудование схемы управления и элементы переключения. Электромеханические устройства цепи управления (IEC 60947-5-1, Low-voltage switchgear and control gear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices)

МЭК/ТС 61000-1-2 Электромагнитная совместимость (ЭМС). Часть 1-2. Общая. Методология для достижения функциональной безопасности электрических и электронных систем, включая электромагнитное оборудование (IEC/TS 61000-1-2, Electromagnetic compatibility (EMC) — Part 1-2: General — Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena)

МЭК 61326-3-1 Электрооборудование для измерения, управления и лабораторного использования. Требования ЭМС. Часть 3-1. Требования устойчивости для систем, связанных с безопасностью, и оборудования для выполнения функций, связанных с безопасностью (функциональная безопасность). Общепромышленное применение (IEC 61326-3-1, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — General industrial applications)

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

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

МЭК 61508-5:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью Часть 5. Примеры методов определения уровней полноты безопасности (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)

МЭК 61508-6:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3 (IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3)

МЭК 61508-7:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью Часть 7. Методы и средства (IEC 61508-7: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures)

МЭК 61784-3 Промышленные сети связи. Профили. Часть 3. Функциональная безопасность коммуникационных сетей. Общие правила и определения профиля (IEC 61784-3, Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions)

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

МЭК 62280-2 Железные дороги. Системы связи, сигнализации и обработки данных. Часть 2. Экстренная связь в открытых системах передачи (IEC 62280-2, Railway applications — Communication, signalling and processing systems — Part 2: Safety-related communication in open transmission systems)

ЕН 50205 Реле с принудительно ведомыми (механически связанными) контактами (EN 50205, Relays with forcibly guided (mechanically linked) contacts)

3 Термины и определения

В настоящем стандарте применены термины, определения и сокращения по МЭК 61508-4.

4 Соответствие настоящему стандарту

Требования соответствия настоящему стандарту — по МЭК 61508-1, раздел 4.

5 Документация

Требования к документации — по МЭК 61508-1, раздел 5.

6 Управление функциональной безопасностью

Требования по управлению функциональной безопасностью — по МЭК 61508-1, раздел 6.

7 Требования к жизненному циклу Э/Э/ПЭ системы безопасности

7.1 Общие положения

7.1.1 Цели и требования. Общие положения

7.1.1.1 Настоящий подпункт устанавливает цели и требования для стадий жизненного цикла Э/Э/ПЭ системы безопасности.

Примечание — Цели и требования для полного жизненного цикла систем безопасности вместе с общим введением в структуру настоящего стандарта приведены в МЭК 61508-1.

7.1.1.2 Для каждой стадии жизненного цикла Э/Э/ПЭ системы безопасности (см. таблицу 1) указаны:

- цели, которые должны быть достигнуты;
- область применения конкретной стадии;
- ссылка на пункт, содержащий требования;
- входы стадии;
- выходы стадии.

7.1.2 Цели

7.1.2.1 Первая цель настоящего подраздела состоит в структурировании на систематической основе стадий жизненного цикла Э/Э/ПЭ системы безопасности, которые должны быть рассмотрены для достижения требуемой функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью.

7.1.2.2 Вторая цель настоящего подраздела заключается в документировании всей информации, относящейся к функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, на протяжении всего жизненного цикла Э/Э/ПЭ системы безопасности.

7.1.3 Требования

7.1.3.1 Структура жизненного цикла Э/Э/ПЭ системы безопасности, используемого в качестве требования соответствия настоящему стандарту, представлена на рисунке 2. Подробная V-модель жизненного цикла разработки специализированных интегральных схем (СИС) для их проектирования (см. пункт 3.2.15 МЭК 61508-4) представлена на рисунке 3. В случае использования другого жизненного цикла Э/Э/ПЭ системы безопасности или жизненного цикла разработки СИС, он должен быть определен как часть управления деятельностью по функциональной безопасности Э/Э/ПЭ систем (см. раздел 6 МЭК 61508-1), а также должны быть достигнуты все цели и требования каждого подраздела настоящего стандарта.

Примечания

1 Взаимосвязь и области применения настоящего стандарта и МЭК 61508-3 показаны на рисунке 4.

2 Существует много общего между процессами проектирования СИС и программного обеспечения. При разработке программного обеспечения, связанного с безопасностью, для предотвращения и управления систематическими отказами МЭК 61508-3 рекомендует использовать V-модель, которая требует, чтобы процесс проектирования был хорошо структурирован, а программное обеспечение обладало модульной структурой. Этой модели соответствует жизненный цикл разработки СИС, используемый для ее проектирования, который представлен на рисунке 3. Сначала из требований к системе формируют требования к спецификации СИС. Затем проектируют архитектуру, СИС и мо-

дуль. Результаты каждого шага левой части V-модели становятся входной информацией для следующего шага, а также, где необходима итерация, происходит возврат к предыдущему шагу, пока не создан окончательный программный код. Этот код верифицируется в обратном порядке к процессу проектирования, т. е. моделируются результаты размещения и трассировки, тестируется модуль, тестируется интеграция модулей и проверяется СИС полностью. Результаты любого шага могут потребовать изменений проекта на любом из предыдущих шагов. На последнем шаге, после того как СИС интегрирована в систему, связанную с безопасностью, для СИС выполняется подтверждение соответствия.

7.1.3.2 Процедуры управления функциональной безопасностью (см. раздел 6 МЭК 61508-1) должны осуществляться параллельно стадиям жизненного цикла Э/Э/ПЭ системы безопасности.

7.1.3.3 Каждую стадию жизненного цикла Э/Э/ПЭ системы безопасности подразделяют на элементарные действия с определением для каждой(го) из них области применения, входов и выходов (см. таблицу 1).

7.1.3.4 Выходы каждой стадии жизненного цикла Э/Э/ПЭ системы безопасности должны быть документально оформлены (см. раздел 5 МЭК 61508-1), если не будет обосновано, что они являются результатом деятельности по управлению функциональной безопасностью (см. раздел 6 МЭК 61508-1).

7.1.3.5 Результаты каждой стадии жизненного цикла Э/Э/ПЭ системы безопасности должны соответствовать определенным для этой стадии целям и требованиям (см. 7.2—7.9).

Примечания

1 См. раздел А.2, перечисление b) МЭК 61508-6.

2 На рисунке показаны только те стадии жизненного цикла Э/Э/ПЭ системы безопасности, которые составляют стадию реализации жизненного цикла всей системы безопасности. Полный жизненный цикл Э/Э/ПЭ системы безопасности также включает в себя блоки, определенные для Э/Э/ПЭ системы, связанной с безопасностью, последующих стадий жизненного цикла всей системы безопасности (см. рисунок 2 МЭК 61508-1, блоки 12—16).

Рисунок 2 — Структура жизненного цикла Э/Э/ПЭ системы безопасности (стадия реализации)

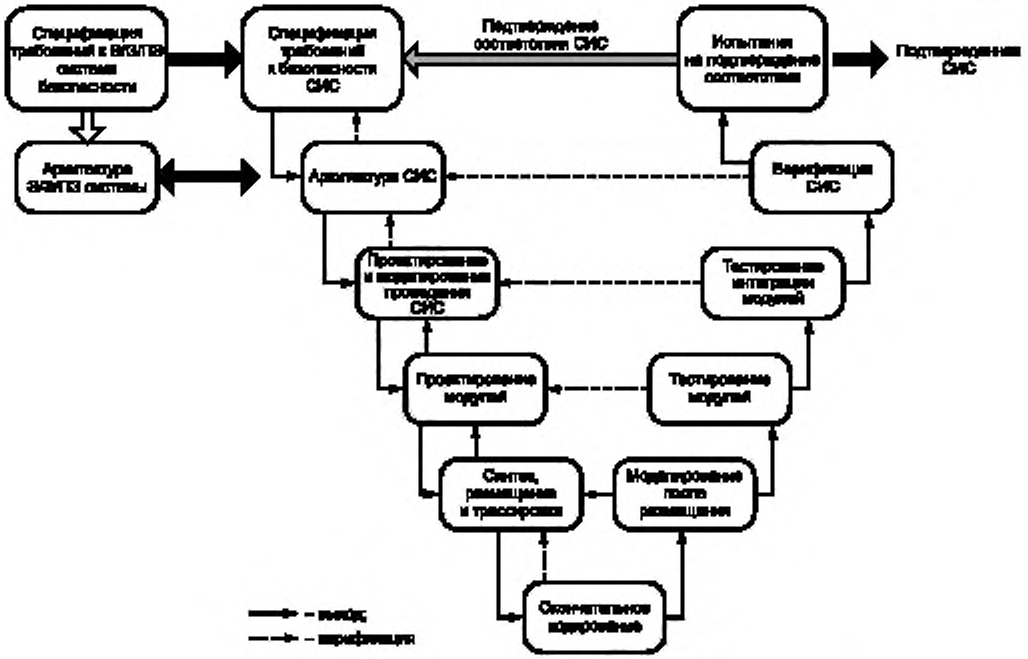


Рисунок 3 — Структура жизненного цикла разработки СИС (V-модель)

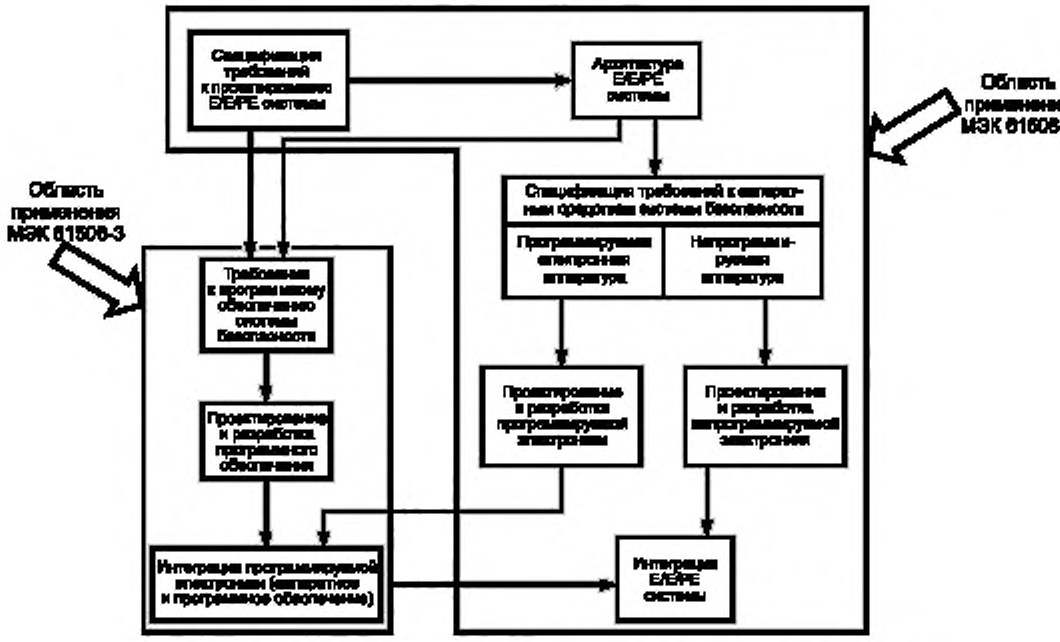


Рисунок 4 — Взаимосвязь и области применения МЭК 61508-2 и МЭК 61508-3

Таблица 1 — Обзор стадии реализации жизненного цикла Э/Э/ПЭ системы безопасности

Стадия и/или действие жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область применения	Пункт требований	Вход	Выход
10.1 Спецификация требований проектирования Э/Э/ПЭ системы	Определить требования проектирования для каждой Э/Э/ПЭ системы, связанной с безопасностью, в терминах подсистем и элементов (см. пункт 7.10.2 МЭК 61508-1)	Э/Э/ПЭ система, связанная с безопасностью	7.2.2	Спецификация требований к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1)	Спецификация требований проектирования Э/Э/ПЭ системы, описывающая оборудование и архитектуру для Э/Э/ПЭ системы
10.2 Планирование подтверждения соответствия безопасности Э/Э/ПЭ системы	Планировать подтверждение соответствия безопасности Э/Э/ПЭ системы, связанной с безопасностью	Э/Э/ПЭ система, связанная с безопасностью	7.3.2	Спецификация требований к Э/Э/ПЭ системе безопасности и спецификация требований проектирования Э/Э/ПЭ системы	План подтверждения соответствия безопасности Э/Э/ПЭ системы, связанной с безопасностью
10.3 Проектирование и создание Э/Э/ПЭ системы, включая СИС и программное обеспечение (см. рисунок 3 и МЭК 61508-3)	Спроектировать и создать Э/Э/ПЭ систему, связанную с безопасностью, (включая СИС, если необходимо), соответствующую спецификации требований проектирования [требования к функциям безопасности и требования к полноте безопасности (см. 7.2)]	Э/Э/ПЭ система, связанная с безопасностью	7.4.2—7.4.8	Спецификация требований проектирования Э/Э/ПЭ системы	Разработка Э/Э/ПЭ систем, связанных с безопасностью, в соответствии со спецификацией требований проектирования Э/Э/ПЭ системы. План тестирования интеграции Э/Э/ПЭ системы. Информация об архитектуре ПЭ системы как входная спецификация требований к программному обеспечению
10.4 Интеграция Э/Э/ПЭ системы	Интегрировать и тестировать Э/Э/ПЭ систему, связанную с безопасностью	Э/Э/ПЭ система, связанная с безопасностью	7.5.2	Разработка Э/Э/ПЭ системы. План тестирования интеграции Э/Э/ПЭ системы. Программируемая электроника и программное обеспечение	Полностью функционирующие Э/Э/ПЭ системы, связанные с безопасностью, в соответствии с проектом Э/Э/ПЭ системы. Результаты тестирования интеграции Э/Э/ПЭ системы
10.5 Процедуры установки, ввода в эксплуатацию, эксплуатации и технического обслуживания Э/Э/ПЭ системы	Разработать процедуры для гарантирования того, что требуемая функциональная безопасность Э/Э/ПЭ системы, связанной с безопасностью, поддерживается в период эксплуатации и технического обслуживания	Э/Э/ПЭ система, связанная с безопасностью. УО	7.6.2	Спецификация требований проектирования Э/Э/ПЭ системы. Проект Э/Э/ПЭ системы	Процедуры установки, ввода в эксплуатацию, эксплуатации и технического обслуживания для каждой отдельной Э/Э/ПЭ системы

Окончание таблицы 1

Стадия и/или действие жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область применения	Пункт требований	Вход	Выход
10.6 Подтверждение соответствия безопасности Э/Э/ПЭ системы	Подтвердить соответствие того, что Э/Э/ПЭ система, связанная с безопасностью, во всех отношениях отвечают требованиям к безопасности Э/Э/ПЭ системы в терминах требуемых функций безопасности и требований к полноте безопасности	Э/Э/ПЭ система, связанная с безопасностью	7.7.2	Спецификация требований к Э/Э/ПЭ системе безопасности и спецификация требований проектирования Э/Э/ПЭ системы. План подтверждения соответствия безопасности Э/Э/ПЭ системы, связанной с безопасностью	Э/Э/ПЭ системы, связанные с безопасностью, с полным подтверждением соответствия безопасности Э/Э/ПЭ системе. Результаты подтверждения соответствия безопасности Э/Э/ПЭ системы
Модификация Э/Э/ПЭ системы	Осуществлять коррекции, расширения или адаптации Э/Э/ПЭ системы, связанной с безопасностью, с гарантией того, что достигается и поддерживается требуемый уровень полноты безопасности	Э/Э/ПЭ система, связанная с безопасностью	7.8.2	Спецификация требований проектирования Э/Э/ПЭ системы	Результаты модификации Э/Э/ПЭ системы
Верификация Э/Э/ПЭ	Тестировать и оценивать выходные результаты конкретной стадии, чтобы гарантировать их правильность и соответствие требованиям разделов стандартов, предусмотренных для этой стадии	Э/Э/ПЭ система, связанная с безопасностью	7.9.2	Зависящие от стадии спецификации требований проектирования Э/Э/ПЭ системы. План верификации Э/Э/ПЭ систем, связанных с безопасностью, для каждой стадии	Зависящие от стадии результаты модификации Э/Э/ПЭ системы. Результаты верификации Э/Э/ПЭ систем, связанных с безопасностью, для каждой стадии
Оценка функциональной безопасности Э/Э/ПЭ системы	Провести исследование и получить заключение по функциональной безопасности, достигнутой с помощью Э/Э/ПЭ системы, связанной с безопасностью	Э/Э/ПЭ система, связанная с безопасностью	8	План оценки функциональной безопасности Э/Э/ПЭ системы	Результаты оценки функциональной безопасности Э/Э/ПЭ системы

7.2 Спецификация требований к проектированию Э/Э/ПЭ системы

Примечание — Эта стадия представлена на рисунке 2 (блок 10.1).

7.2.1 Цель

Цель настоящего подраздела состоит в задании требований проектирования для каждой Э/Э/ПЭ системы, связанной с безопасностью, в терминах подсистем и элементов.

Примечание — Обычно спецификация требований проектирования Э/Э/ПЭ системы формируется из спецификации требований к Э/Э/ПЭ системе безопасности с помощью декомпозиции функций безопасности и распределения частей функции безопасности между подсистемами (например, группами датчиков, логических решателей либо исполнительными устройствами). Требования для подсистем могут быть включены в спецификацию требований проектирования Э/Э/ПЭ системы или представлены в виде отдельного документа, или на них существует ссылка в спецификации требований проектирования Э/Э/ПЭ системы. Далее подсистемы могут быть декомпозированы на элементы и их совокупности, с тем чтобы соответствовать требованиям проектирования и разработки по 7.4. Требования для этих элементов могут быть включены в требования к декомпозируемым подсистемам или могут быть представлены в виде отдельного документа, на них существует ссылка в требованиях к подсистеме.

7.2.2 Общие требования

7.2.2.1 Спецификация требований проектирования Э/Э/ПЭ системы должна формироваться из требований к Э/Э/ПЭ системе безопасности, определенных в МЭК 61508-1 (подраздел 7.10).

Примечание — Не рекомендуется, чтобы одна и та же Э/Э/ПЭ система, связанная с безопасностью, выполняла функции безопасности и функции, не относящиеся к безопасности. Хотя это допускается настоящим стандартом, такое объединение приводит к большим сложностям при выполнении работ в процессе жизненного цикла Э/Э/ПЭ системы (например, при проектировании, подтверждении соответствия, оценке функциональной безопасности и техническом обслуживании). См. также 7.4.2.3.

7.2.2.2 Специфицируемые требования проектирования Э/Э/ПЭ системы должны быть выражены и структурированы, с тем чтобы они были:

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

b) оформлены в письменном виде для того, чтобы их лучше понимали те, кто использует эти требования на любой из стадий жизненного цикла Э/Э/ПЭ системы безопасности;

c) выводимыми из спецификации требований Э/Э/ПЭ системы безопасности.

7.2.3 Спецификация требований проектирования Э/Э/ПЭ системы

7.2.3.1 Спецификация требований Э/Э/ПЭ системы безопасности должна содержать требования проектирования, относящиеся к функциям безопасности (см. 7.2.3.2) и требования проектирования, относящиеся к полноте безопасности (см. 7.2.3.3).

7.2.3.2 Спецификация требований проектирования Э/Э/ПЭ системы должна содержать сведения обо всех аппаратных средствах и программном обеспечении, необходимых для осуществления требуемых функций безопасности, как указано в спецификации требований к функциям безопасности Э/Э/ПЭ системы (МЭК 61508-1,

7.10.2.6). Спецификация для каждой функции безопасности должна содержать:

a) требования к подсистемам и элементам их аппаратных средств и программного обеспечения (по мере необходимости);

b) требования к интеграции подсистем и их элементам аппаратных средств и программного обеспечения, соответствующие спецификации требований к функциям безопасности Э/Э/ПЭ системы;

c) характеристики производительности, соответствующие требованиям к времени реакции системы;

d) требования к точности и стабильности измерений и управления;

e) сведения об интерфейсах оператора Э/Э/ПЭ системы, связанной с безопасностью;

f) сведения об интерфейсах Э/Э/ПЭ систем, связанных с безопасностью, с любыми другими системами (внутренними, внешними, управляемым оборудованием);

g) описание всех режимов поведения Э/Э/ПЭ систем, связанных с безопасностью, в частности, их поведение при отказе и необходимая реакция на него (например, аварийные сигналы, автоматический останов и т. д.);

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

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

i) любые предельные и ограничивающие условия для Э/Э/ПЭ систем, связанных с безопасностью, и связанных с ними подсистем и элементов, например, ограничения синхронизации либо ограничения, связанные с возможностью отказов по общей причине;

j) любые специфические требования, относящиеся к процедурам запуска и повторного запуска Э/Э/ПЭ систем, связанных с безопасностью.

7.2.3.3 Спецификация требований проектирования Э/Э/ПЭ системы должна содержать сведения о том, как в проекте достигается уровень полноты безопасности и требуемая целевая мера отказов для функции безопасности, которые определены в спецификации требований к полноте безопасности Э/Э/ПЭ системы (см. подпункт 7.10.2.7 МЭК 61508-1), включая:

a) архитектуру каждой подсистемы, удовлетворяющую ограничениям на архитектуру, накладываемым полнотой безопасности на аппаратные средства (см. 7.4.4);

b) все соответствующие параметры моделирования отказоустойчивости, такие как требуемая частота контрольных испытаний элементов аппаратных средств, необходимая для достижения целевой меры отказов.

Примечание — Информация о конкретном применении не должна быть ограничена (см. подпункт 7.10.2.1 МЭК 61508-1). Это особенно важно для технического обслуживания, при котором интервал между контрольными испытаниями должен быть не менее предсказуемого интервала для конкретного применения. Например, интервалы между обслуживаниями, которые могут быть реально достигнуты для продукции массового производства, используемой населением, вероятно, будут больше, чем при более управляемых применениях;

c) действия, выполняемые в случае опасного отказа, выявленного диагностикой;

d) требования, ограничения, функции и доступность проведения контрольных испытаний аппаратных средств Э/Э/ПЭ системы;

e) возможности оборудования обычно соответствуют экстремальным значениям всех условий окружающей среды (например, значениям температуры, влажности, механических и электрических воздействий), которые определены как требования на всех этапах жизненного цикла Э/Э/ПЭ системы безопасности, включая изготовление, хранение, транспортирование, тестирование, установку, ввод в эксплуатацию, эксплуатацию и техническое обслуживание;

f) необходимые пределы электромагнитной устойчивости (см. МЭК/ТС 61000-1-2:2008).

Примечания

1 Пределы необходимой электромагнитной устойчивости могут отличаться для различных элементов системы, связанной с безопасностью, в зависимости от их физического местоположения и механизмов питания.

2 Руководящие указания также могут быть указаны в отдельных стандартах по электромагнитной совместимости на продукцию, но следует помнить, что для специфических условий размещения системы или если оборудование используется в более жестких электромагнитных условиях, могут потребоваться более высокие уровни электромагнитной устойчивости, чем заданы в таких стандартах;

g) обеспечение качества/меры контроля качества, необходимые для управления безопасностью (см. пункт 6.2.5 МЭК 61508-1).

7.2.3.4 Спецификация требований проектирования Э/Э/ПЭ системы должна постоянно уточняться при развитии проекта и по мере необходимости должна обновляться при его модификации.

7.2.3.5 Во избежание ошибок во время составления спецификации требований проектирования Э/Э/ПЭ системы необходимо использовать группу методов и средств в соответствии с таблицей В.1 (приложение В).

7.2.3.6 Должны быть рассмотрены последствия накладываемых на архитектуру требований проектирования Э/Э/ПЭ системы.

Примечание — Такое рассмотрение должно включать в себя анализ простоты реализации для достижения требуемого уровня полноты безопасности (включая анализ архитектуры и пропорциональное распределение функциональности, реализуемой за счет конфигурирования или встроенной системой).

7.3 Планирование подтверждения соответствия безопасности Э/Э/ПЭ системы

Примечание — Данная стадия представлена на рисунке 2 (см. блок 10.2). Она обычно выполняется параллельно с проектированием и разработкой Э/Э/ПЭ системы (см. 7.4).

7.3.1 Цель

Целью требований настоящего пункта является планирование подтверждения соответствия безопасности Э/Э/ПЭ системы, связанной с безопасностью.

7.3.2 Требования

7.3.2.1 Планирование для определения шагов (процедурных и технических) должно проводиться для демонстрации соответствия Э/Э/ПЭ системы, связанной с безопасностью, спецификации требований к Э/Э/ПЭ системе безопасности (см. 7.2) и спецификации требований к проектированию Э/Э/ПЭ системы.

7.3.2.2 При планировании подтверждения соответствия Э/Э/ПЭ системы, связанной с безопасностью, должны быть использованы:

a) требования, определенные в спецификации требований к Э/Э/ПЭ системе безопасности и в спецификации требований к проектированию Э/Э/ПЭ системы;

b) процедуры, применяемые для подтверждения соответствия тому, что каждая функция безопасности правильно выполняется по критериям «прошла испытания/не прошла испытания»;

c) процедуры, применяемые для подтверждения соответствия полноте безопасности каждой функции безопасности по критериям «прошла испытания/не прошла испытания»;

d) требуемые условия окружающей среды, при которых проводят испытания, включая необходимые инструменты и оборудование (в том числе план, в соответствии с которым эти инструменты и оборудование должны быть калиброваны);

e) процедуры оценочных испытаний (с обоснованиями);

f) процедуры испытаний и критерии, применяемые для подтверждения соответствия заданным в спецификации пределам электромагнитной устойчивости.

Примечание — Руководство по спецификации испытаний пределов электромагнитной устойчивости для элементов систем, связанных с безопасностью, представлено в МЭК/ТС 61000-1-2:2008;

g) стратегии по устранению подтвержденного отказа.

7.4 Проектирование и разработка Э/Э/ПЭ системы

Примечание — Данная стадия представлена на рисунке 2 (см. блок 10.3). Она обычно выполняется параллельно с планированием подтверждения соответствия Э/Э/ПЭ системы безопасности (см. 7.3).

7.4.1 Цель

Цель требований настоящего подраздела состоит в обеспечении соответствия проектирования и разработки Э/Э/ПЭ системы (включающей, при необходимости, СИС, см. пункт 3.2.15 МЭК 61508-4), связанной с безопасностью, спецификации требований к проектированию Э/Э/ПЭ системы [относительно требований функций безопасности и требований к полноте безопасности (см. 7.2)].

7.4.2 Общие требования

7.4.2.1 Проектирование Э/Э/ПЭ системы, связанной с безопасностью, должно быть проведено в соответствии со спецификацией требований проектирования Э/Э/ПЭ системы (см. 7.2.3) с учетом всех требований 7.2.3.

7.4.2.2 Проектирование Э/Э/ПЭ системы, связанной с безопасностью (включая архитектуру аппаратных средств и программного обеспечения всей системы, датчики, исполнительные устройства;, программируемую электронику, СИС, встроенное программное обеспечение, «зашитое» в ПЗУ, прикладное программное обеспечение и т. п.), должно соответствовать всем перечисленным ниже требованиям:

a) к полноте безопасности аппаратных средств, включая:

- требования к архитектурным ограничениям на полноту безопасности аппаратных средств (см. 7.4.4)
- требования к выполнению количественной оценки случайных отказов (см. 7.4.5);

b) специальной архитектуре для интегральных схем (ИС) с избыточностью схем на кристалле (см. приложение Е) в соответствующих случаях, если не может быть приведено обоснование того, что тот же самый уровень независимости между различными каналами достигается с помощью применения другого набора средств;

c) систематической полноте безопасности (стойкости к систематическим отказам), которая может быть обеспечена применением одного из следующих способов обеспечения соответствия:

- способ 1_S: соответствие с требованиями по предотвращению систематических отказов (см. 7.4.6 и МЭК 61508-3) и требованиями по управлению систематическими отказами (см. 7.4.7 и МЭК 61508-3), или
- способ 2_S: соответствие с требованиями с помощью доказательства того, что оборудование «проверено в эксплуатации» (см. 7.4.10), или
- способ 3_S: (только для ранее существующих элементов программного обеспечения): соответствие с требованиями подпункт 7.4.2.12 МЭК 61508-3.

Примечание — Индекс «S» в вышеупомянутых способах означает систематическую полноту безопасности в отличие от способа 1_H и способа 2_H (см. 7.4.4), для полноты безопасности аппаратных средств;

d) поведению системы при обнаружении отказов (см. 7.4.8);

e) процессам передачи данных (см. 7.4.11).

7.4.2.3 Если Э/Э/ПЭ система, связанная с безопасностью, осуществляет функции безопасности и функции, не относящиеся к безопасности, то все аппаратные средства и программное обеспечение должны рассматриваться как связанные с безопасностью до тех пор, пока не будет установлено, что эти

функции реализуются достаточно независимо (т. е. отказ какой-либо функции, не относящейся к безопасности, не станет причиной отказа функций, связанных с безопасностью).

Примечания

1 Достаточную независимость этих функций устанавливают демонстрацией того, что вероятность зависимого отказа между компонентами, не относящимися к безопасности и связанными с безопасностью, достаточно низка по сравнению с самым высоким уровнем полноты безопасности, связанным с используемыми функциями безопасности.

2 Следует предостеречь от совмещения функций безопасности и функций, не относящихся к безопасности, в одной и той же Э/Э/ПЭ системе, связанной с безопасностью. Такое объединение, допускаемое настоящим стандартом, может усложнить Э/Э/ПЭ систему и привести к трудностям при выполнении работ в процессе жизненного цикла Э/Э/ПЭ системы (например, при проектировании, подтверждении соответствия, оценке функциональной безопасности и техническом обслуживании).

7.4.2.4 Требования к аппаратным средствам и программному обеспечению должны определяться уровнем полноты безопасности функций безопасности, имеющих самый высокий уровень полноты безопасности, если не будет показано, что выполнение функций безопасности различных уровней полноты безопасности достаточно независимо.

Примечания

1 Достаточная независимость выполнения функций безопасности устанавливается демонстрацией вероятности зависимого отказа между компонентами, выполняемых функций безопасности различных уровней полноты безопасности, достаточно низкой по сравнению с самым высоким уровнем полноты безопасности, связанным с рассматриваемыми функциями безопасности.

2 Если в Э/Э/ПЭ системе, связанной с безопасностью, выполняется несколько функций безопасности, то необходимо рассмотреть возможность возникновения отказа в выполнении нескольких функций безопасности от единственной ошибки. В такой ситуации требования к аппаратным средствам и программному обеспечению допускается задавать на основе уровня полноты безопасности более высокого, чем связанный с любой из функций безопасности, в зависимости от риска, связанного с таким отказом.

7.4.2.5 Если требуется независимость функций безопасности (см. 7.4.2.3 и 7.4.2.4), то в процессе проектирования должны быть документально оформлены:

a) метод достижения независимости;

b) обоснование метода.

Пример — Для анализа предсказуемых видов отказа, которые могут нарушить независимость функций безопасности, и для определения интенсивности таких отказов используется метод анализа вида, последствий и критичности отказов (FMECA) или метод анализа зависимых отказов.

7.4.2.6 Требования к программному обеспечению, связанному с безопасностью (см. МЭК 61508-3), должны быть доступны разработчику Э/Э/ПЭ системы, связанной с безопасностью.

7.4.2.7 Разработчик Э/Э/ПЭ системы, связанной с безопасностью, должен провести анализ требований к связанным с безопасностью программному обеспечению и аппаратным средствам с тем, чтобы убедиться, что они корректно специфицированы. В частности, разработчик Э/Э/ПЭ системы должен рассмотреть:

a) функции безопасности;

b) требования к полноте безопасности Э/Э/ПЭ системы, связанной с безопасностью;

c) интерфейсы между оборудованием и обслуживающим персоналом.

7.4.2.8 Проектная документация на Э/Э/ПЭ систему, связанную с безопасностью, должна определять методы и средства, необходимые для достижения уровня полноты безопасности в течение стадий жизненного цикла Э/Э/ПЭ системы безопасности.

7.4.2.9 Проектная документация на Э/Э/ПЭ систему, связанную с безопасностью, должна обосновывать методы и средства, выбранные для ее интеграции, обеспечивающей требуемый уровень полноты безопасности.

Примечание — Принятие общего подхода, использующего независимое принятие Э/Э/ПЭ системы, связанной с безопасностью (включающей в себя датчики, исполнительные элементы и т. д.), ее технических средств и программного обеспечения, диагностических тестов и инструментов программирования и используемых (где это возможно) подходящих языков программирования, позволяет сократить сложность инженерного применения Э/Э/ПЭ системы.

7.4.2.10 В процессе проектирования и разработки все существенные (в соответствующих случаях) взаимодействия аппаратных средств и программного обеспечения должны быть идентифицированы, оценены и документально оформлены.

7.4.2.11 Проект должен быть основан на декомпозиции на подсистемы, каждая из которых имеет специфицированный проект и набор тестов интеграции (см. 7.5.2).

Примечания

1 Конкретная подсистема может состоять из единственного компонента или группы компонентов. См. определения в МЭК 61508-4. Полная Э/Э/ПЭ система, связанная с безопасностью, может состоять из множества идентифицируемых и отдельных подсистем, которые при их объединении обеспечивают выполнение рассмотренной функции безопасности. Подсистема может иметь более чем один канал (см. 7.4.9.3 и 7.4.9.4).

2. Везде, где это практически возможно, должны быть использованы существующие проверенные подсистемы. Это положение является в общем случае верным, только если существует почти стопроцентное совпадение функциональных возможностей, пропускной способности и производительности существующей подсистемы с новыми требованиями или верифицированная (проверенная) подсистема структурирована так, чтобы пользователь мог выбрать лишь требуемые функции, пропускную способность и производительность для специфического применения. Избыточные функциональные возможности, пропускная способность или производительность могут повредить безопасности системы, если существующие подсистемы чрезмерно усложнены или имеют неиспользуемые возможности и не обеспечена защита от непредусмотренных функций.

7.4.2.12 Когда завершается начальный проект Э/Э/ПЭ системы, связанной с безопасностью, необходимо провести анализ, чтобы определить, может ли какой-либо разумно предсказуемый отказ Э/Э/ПЭ системы, связанной с безопасностью, вызвать опасную ситуацию или сформировать запрос к какому-либо средству управления риском. Если происходит любой из таких разумно предсказуемых отказов, то первым по приоритету действием должно быть изменение проекта Э/Э/ПЭ системы, связанной с безопасностью, чтобы избежать таких видов отказов. Если это выполнить не удается, то должны быть приняты меры по сокращению вероятности таких видов отказов до уровня, соизмеримого с целевой мерой отказа. Эти меры должны соответствовать требованиям настоящего стандарта.

Примечание — Цель данного подпункта — выявить виды отказов Э/Э/ПЭ системы, связанной с безопасностью, формирующей запрос к какому либо средству управления риском. Возможны ситуации, когда интенсивность отказов для выявленных видов отказов не может быть снижена, в этом случае требуется сформировать новую функцию безопасности, либо УПБ других функций безопасности должны быть пересмотрены с учетом интенсивности отказов.

7.4.2.13 Для всех компонентов аппаратных средств должно быть учтено снижение параметров относительно предельных значений (см. МЭК 61508-7). Обоснование работы любых компонентов аппаратных средств при предельных значениях их параметров должно быть документально оформлено (см. раздел 5 МЭК 61508-1).

Примечание — При назначении снижения параметров коэффициент снижения обычно устанавливают приблизительно равным двум третям.

7.4.2.14 Если проект Э/Э/ПЭ системы, связанной с безопасностью, для реализации функции безопасности включает одну или более СИС, то должен применяться жизненный цикл разработки СИС (см. 7.1.3.1).

7.4.3 Синтез элементов для обеспечения требуемой стойкости к систематическим отказам

7.4.3.1 Для удовлетворения требований к систематической полноте безопасности создаваемая Э/Э/ПЭ система, связанная с безопасностью, при условиях, описанных в настоящем пункте, может быть разделена на элементы, обладающие различной стойкостью к систематическим отказам.

Примечания

1 Стойкость к систематическим отказам элемента определяется способностью функции безопасности противостоять отказу при отказе этого элемента. Концепция стойкости к систематическим отказам элемента применима к элементам как аппаратных средств, так и программного обеспечения.

2 В МЭК 61508-1 (подпункт 7.6.2.7) указывается на важность принципов независимости и разнообразия на этапе распределения функции безопасности по Э/Э/ПЭ системам, связанным с безопасностью, которые эту функцию безопасности могут выполнить. Эти понятия могут быть применены при более детальном проектировании, где некоторая структура элементов, реализующая функцию безопасности, возможно, может достичь лучшей стойкости к систематическим отказам, чем ее отдельные элементы.

7.4.3.2 Если систематический сбой элемента со стойкостью к систематическим отказам ССN (N = 1, 2, 3) не вызывает отказ указанной функции безопасности, но вызывает ее отказ только в сочетании со вторым систематическим отказом другого элемента со стойкостью к систематическим отказам ССN, то результирующая стойкость к систематическим отказам комбинации этих двух элементов может рассматриваться как СС(N+1) при условии, что эти два элемента достаточно независимы (см. 7.4.3.4).

Примечание — Независимость элементов может быть оценена, только если известны конкретные применения этих элементов для оговоренных функций безопасности.

7.4.3.3 Стойкость к систематическим отказам, которая может быть предъявлена к комбинации элементов со стойкостью к систематическим отказам каждого из них, равной СС*N*, в лучшем случае может быть равна СС(*N*+1). Элемент со стойкостью к систематическим отказам, равной СС*N*, может быть использован таким способом только один раз. Не допускается для получения СС(*N*+2) и выше последовательно строить комбинации из элементов с СС*N*.

7.4.3.4 Для обоснования достаточной независимости между элементами при проектировании и между элементами в их конкретном применении необходимо применять анализ отказов по общей причине, чтобы показать, что вероятность взаимодействия между элементами и между элементами и окружающей средой является незначительной по сравнению с уровнем полноты безопасности рассматриваемой функции безопасности.

Примечания

1 При определении стойкости к систематическим отказам в процессе проектирования, реализации, эксплуатации и технического обслуживания аппаратных средств возможно использование следующих подходов для достижения достаточной независимости:

- функциональное разнообразие: использование различных подходов для достижения тех же результатов;
- разнообразие технологий: использование различных типов оборудования для достижения тех же результатов;
- общие компоненты/процедуры обслуживания: обеспечение отсутствия общих компонентов или процедур обслуживания, или систем поддержки (например, электропитания), отказ которых может привести к опасному виду отказа всех систем;
- общие процедуры: обеспечение отсутствия общих процедур при эксплуатации, техническом обслуживании или тестировании.

2 Независимость применения означает, что элементы не повлияют друг на друга настолько неблагоприятно, что это может привести к опасному отказу.

3 Для обеспечения независимости элементов программного обеспечения см. подпункты 7.4.2.8 и 7.4.2.9 МЭК 62508-3.

7.4.4 Архитектурные ограничения полноты безопасности аппаратных средств

Примечания

1 Выражение, связывающее ограничения полноты безопасности аппаратных средств, определено в приложении С, а сами ограничения полноты безопасности представлены в таблицах 2 и 3.

2 Обзор необходимых шагов для достижения требуемой полноты безопасности технических средств приведен в МЭК 61508-6 (пункт А.2, приложение А) и там же показано, как данный пункт соотносится с другими требованиями настоящего стандарта.

Наиболее высокий уровень полноты безопасности аппаратных средств, который может потребоваться для функции безопасности, ограничен предельными значениями полноты безопасности аппаратных средств, которые достигаются одним из двух возможных способов (реализуемых на уровне системы или подсистемы):

- способ 1_H основан на концепции отказоустойчивости аппаратных средств и концепции составляющей безопасных отказов;
- способ 2_H основан на полученных данных о безотказности компонентов, об их использовании конечными пользователями, повышающих уровни доверия и отказоустойчивость аппаратных средств для указанных уровней полноты безопасности.

Стандарты для прикладных областей, основанные на стандартах серии МЭК 61508, могут содержать указание на предпочтительный способ (т. е. способ 1_H или способ 2_H).

Примечание — Индекс «Н» в вышеупомянутых способах означает полноту безопасности технических средств в отличие от способов 1_S, 2_S, и 3_S для систематической полноты безопасности.

7.4.4.1 Общие требования

7.4.4.1.1 Что касается требований к обеспечению отказоустойчивости аппаратных средств, необходимо учитывать, что:

a) отказоустойчивость аппаратных средств *N* означает, что *N*+1 является минимальным числом отказов, которые могут привести к потере функции безопасности (для дополнительных разъяснений см. примечание 1 и таблицы 2 и 3). В определении отказоустойчивости не должны учитываться средства, которые могли бы контролировать последствия ошибок, например, диагностика, и

b) если одна ошибка непосредственно приводит к одной или более последующим ошибкам, их рассматривают как одиночную ошибку;

c) при определении отказоустойчивости некоторые ошибки могут быть исключены при условии, что вероятность их возникновения очень мала по сравнению с требованиями полноты безопасности

подсистемы. Любые исключения ошибок должны быть обоснованы и документально оформлены (см. примечание 3).

Примечания

1 Для получения достаточно отказоустойчивой архитектуры с учетом уровня сложности элемента и подсистемы используют ограничения на полноту безопасности аппаратных средств (см. 7.4.4.1.1 и 7.4.4.1.2). Самым высоким допустимым уровнем полноты безопасности для функции безопасности, реализуемой Э/Э/ПЭ системой, связанной с безопасностью, полученным в результате применения требований настоящего подпункта, является максимальный уровень из заявленных для функции безопасности, хотя в некоторых случаях расчеты надежности показывают, что может быть достигнут более высокий уровень полноты безопасности. Следует также отметить, что даже если отказоустойчивость аппаратных средств достигнута для всех подсистем, необходимо выполнить расчет надежности, чтобы продемонстрировать, что заданная целевая мера отказов достигнута, так как для выполнения требований проекта может потребоваться, чтобы отказоустойчивость аппаратных средств была увеличена.

2 Требования отказоустойчивости аппаратных средств применяют к архитектуре подсистемы, которая используется при нормальных условиях эксплуатации. Требования отказоустойчивости к аппаратным средствам могут быть снижены, если Э/Э/ПЭ система, связанная с безопасностью, восстанавливается автономно. Однако ключевые параметры, связанные с любым снижениям требований, должны быть предварительно оценены (например, оценка среднего времени восстановления по отношению к вероятности запроса).

3 Некоторые ошибки могут быть исключены, так как если некоторый элемент системы имеет очень низкую вероятность отказа благодаря присущим ему свойствам и конструкции (например, механический соединитель привода), то нет необходимости рассматривать ограничение (связанное с отказоустойчивостью аппаратных средств) полноты безопасности любой функции безопасности, для реализации которой используется этот элемент.

4 Выбор дальнейших шагов зависит от области применения и для выбора способа необходимо учитывать:

- безопасный отказ одной функции может создать новую опасность или стать дополнительной причиной для существующей опасности;
- резервирование не может быть реализовано для всех функций;
- ремонт не всегда возможен или быстро осуществим (например, не представляется возможным его провести за период времени, который существенно меньше интервала времени между тестовыми испытаниями).

5 Специальные требования к архитектуре ИС с избыточностью схем на кристалле приведены в приложении Е.

7.4.4.1.2 Элемент может быть отнесен к типу А, если для его компонентов, необходимых для реализации функции безопасности, одновременно выполняются следующие условия:

a) виды отказов всех составляющих компонентов определены;

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

c) данные о претензиях по поводу интенсивности отказов для обнаруженных и необнаруженных опасных отказов недостаточно надежны (см. 7.4.9.3—7.4.9.5).

7.4.4.1.3 Элемент может быть отнесен к типу В, если для его компонентов, необходимых для реализации функции безопасности, выполняется хотя бы одно из следующих условий:

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

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

c) данные о претензиях по поводу интенсивности отказов для обнаруженных и необнаруженных опасных отказов недостаточно надежны (см. 7.4.9.3—7.4.9.5).

Примечание — Если по крайней мере один из компонентов конкретного элемента соответствует условиям для типа В, то такой элемент должен быть отнесен к типу В, а не к типу А.

7.4.4.1.4 При оценке доли безопасных отказов элемента, предназначенного для использования в подсистеме с отказоустойчивостью аппаратных средств равной нулю, которая выполняет функцию безопасности или часть функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами, доверие (предпочтение) должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и времени выполнения определенного действия для достижения или поддержания безопасного состояния было меньше времени безопасности процесса или
- при работе в режиме высокой частоты запросов отношение частоты диагностических испытаний к частоте запросов равно или превышает 100.

7.4.4.1.5 При оценке доли безопасных отказов элемента, который имеет отказоустойчивость аппаратных средств больше нуля и который выполняет функцию безопасности или часть функции безопасности, действуя в режиме высокой частоты запросов или с непрерывными запросами, или выполняет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов, доверие (предпочтение) должно быть отдано только диагностике, если суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа будет

меньше среднего времени восстановления (MTTR), используемого в вычислениях при определении достигаемой полноты безопасности для этой функции безопасности.

7.4.4.2 Способ 1_H

7.4.4.2.1 Для того чтобы определить максимальный уровень полноты безопасности, который может быть предъявлен к функции безопасности, необходимо выполнить следующие процедуры:

1) Определяют подсистемы, из которых состоит Э/Э/ПЭ система, связанная с безопасностью.

2) Для всех элементов каждой подсистемы отдельно определяют долю безопасных отказов (индивидуально для каждого элемента, имеющего отказоустойчивость аппаратных средств, равную нулю). Для конфигураций элементов с резервированием доля безопасных отказов может быть вычислена с учетом дополнительной диагностики, которая может быть доступна (например, сравнением резервированных элементов).

3) Для каждого элемента, используя полученное значение доли безопасных отказов и значение отказоустойчивости аппаратных средств, равное нулю, определяют максимальный уровень полноты безопасности из второй графы таблицы 2 (для элементов типа А) и второй графы таблицы 3 (для элементов типа В).

4) Используя метод, представленный в 7.4.4.2.3 и 7.4.4.2.4, определяют максимальный уровень полноты безопасности, который может быть предъявлен к подсистеме.

5) Максимальный уровень полноты безопасности, который может быть предъявлен к Э/Э/ПЭ системе, связанной с безопасностью, определяется подсистемой с самым низким уровнем полноты безопасности.

7.4.4.2.2 Для подсистем, включающих в себя элементы, отвечающие представленным ниже требованиям, в качестве альтернативы применению требований перечислений 2)—4) 7.4.4.2.1 применяют следующие процедуры определения максимального уровня полноты безопасности:

1) подсистема состоит из более чем одного элемента, и

2) элементы являются однотипными, и

3) все элементы имеют значения доли безопасных отказов, находящиеся в одном диапазоне (см. примечание), определенном в таблицах 2 или 3; в таком случае может быть выполнена следующая процедура:

a) определяют долю безопасных отказов для всех отдельных элементов. В случае конфигураций элементов с резервированием доля безопасных отказов может быть вычислена с учетом доступной дополнительной диагностики (например, сравнение резервированных элементов);

b) определяют отказоустойчивость аппаратных средств подсистемы;

c) определяют по таблице 2 максимальный уровень полноты безопасности, на который может претендовать подсистема, если ее элементы типа А;

d) определяют по таблице 3 максимальный уровень полноты безопасности, на который может претендовать подсистема, если ее элементы типа В.

Примечание — Упоминание о диапазоне в перечислении 3) означает, что в таблицах 2 и 3 значения доли безопасных отказов разделены на четыре диапазона (менее 60 %; от 60 % до менее 90 %; от 90 % до менее 99 % и более и равным 99 %). Все значения доли безопасных отказов должны быть в одном диапазоне (например, все в диапазоне от 90 % до менее 99 %).

Примеры

1 Для определения максимального допустимого уровня полноты безопасности, который для указанной функции безопасности может быть достигнут подсистемой, имеющей отказоустойчивость аппаратных средств 1, для которой функция безопасности элемента реализована с помощью параллельных элементов, может быть принят следующий подход при условии, что подсистема соответствует требованиям 7.4.4.2.2. В этом примере все элементы имеют тип В, а значения доли безопасных отказов элементов находятся в диапазоне от 90 % до менее 99 %.

Из таблицы 3 следует, что для отказоустойчивости аппаратных средств, равной 1, и для значений доли безопасных отказов элементов, находящихся в диапазоне от 90 % до менее 99 %, максимальный допустимый уровень полноты безопасности для указанной функции безопасности — УПБ 3.

2 Для определения необходимой отказоустойчивости аппаратных средств подсистемы для указанной функции безопасности, в которой функция безопасности элемента реализована с помощью параллельных элементов, может быть принят следующий подход, при условии что подсистема соответствует требованиям 7.4.4.2.2. В настоящем примере все элементы имеют тип А, а значения доли безопасных отказов элементов находятся в диапазоне от 60 % до менее 90 %. Уровень полноты безопасности функции безопасности — УБП 3.

Из таблицы 2 следует, что требованию УПБ 3 соответствует необходимая отказоустойчивость аппаратных средств, равная 1. Это означает, что необходимы два параллельных элемента.

Таблица 2 — Максимальный допустимый уровень полноты безопасности для функции безопасности, реализуемой элементом или подсистемой типа А, связанной с безопасностью

Доля безопасных отказов элемента	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
менее 60 %	УПБ 1	УПБ 2	УПБ 3
от 60 % до менее 90 %	УПБ 2	УПБ 3	УПБ 4
от 90 % до менее 99 %	УПБ 3	УПБ 4	УПБ 4
более и равно 99 %	УПБ 3	УПБ 4	УПБ 4

Примечания

1 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения максимального значения УПБ, который может быть предъявлен к подсистеме: задаются отказоустойчивость подсистемы и доля безопасных отказов используемых элементов:

i) для общего применения к любой подсистеме см. 7.4.4.2.1;

ii) для применения к подсистемам, включающим в себя элементы, отвечающие требованиям 7.4.4.2.2. Для того чтобы утверждать, что подсистема соответствует указанному УПБ непосредственно по данной таблице, необходимо чтобы для нее были выполнены все требования 7.4.4.2.2.

2 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения:

i) требований отказоустойчивости аппаратных средств подсистемы, задавая необходимый УПБ функции безопасности и долю безопасных отказов используемых элементов;

ii) требований к значению доли безопасных отказов элементов, задавая необходимый УПБ функции безопасности и отказоустойчивость аппаратных средств подсистемы.

3 Требования 7.4.4.2.3 и 7.4.4.2.4 основаны на данных, определенных в настоящей таблице и в таблице 2.

4 Расчет доли безопасных отказов см. в приложении С.

Таблица 3 — Максимальный допустимый уровень полноты безопасности для функции безопасности, реализуемой элементом или подсистемой типа В, связанной с безопасностью

Доля безопасных отказов элемента	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
менее 60 %	Не оговаривается	УПБ 1	УПБ 2
от 60 % до менее 90 %	УПБ 1	УПБ 2	УПБ 3
от 90 % до менее 99 %	УПБ 2	УПБ 3	УПБ 4
более и равно 99 %	УПБ 2	УПБ 4	УПБ 4

Примечания

1 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения максимального значения УПБ, который может быть предъявлен к подсистеме: задаются отказоустойчивость подсистемы и доля безопасных отказов используемых элементов:

i) для общего применения к любой подсистеме см. 7.4.4.2.1;

ii) для применения к подсистемам, включающим в себя элементы, отвечающие требованиям 7.4.4.2.2. Для того чтобы утверждать, что подсистема соответствует указанному УПБ непосредственно из данной таблицы, необходимо чтобы для нее были выполнены все требования 7.4.4.2.2.

2 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения:

i) требований отказоустойчивости аппаратных средств подсистемы, задавая необходимый УПБ функции безопасности и долю безопасных отказов используемых элементов;

ii) требований к значению доли безопасных отказов элементов, задавая необходимый УПБ функции безопасности и отказоустойчивость аппаратных средств подсистемы.

3 Требования 7.4.4.2.3 и 7.4.4.2.4 основаны на данных, определенных в настоящей таблице и в таблице 3.

4 Расчет доли безопасных отказов см. в приложении С.

5 Если используются требования 7.4.4.2.1 для комбинации элементов типа В, с отказоустойчивостью аппаратных средств, равной 1, в которой у обоих элементов доля безопасных отказов менее 60 %, то максимальным допустимым уровнем полноты безопасности для функции безопасности, выполняемой этой комбинацией, является УБП 1.

7.4.4.2.3 В Э/Э/ПЭ подсистеме, связанной с безопасностью, в которой некоторое число элементов функций безопасности реализуется с помощью последовательности элементов (как показано на рисунке 5), максимальный уровень полноты безопасности, который может быть предъявлен к функции безопасности, должен определяться элементом, который имеет самый низкий уровень полноты безопасности для достигнутой им доли безопасных отказов и отказоустойчивости аппаратных средств равной 0. Чтобы проиллюстрировать этот метод, примем архитектуру, как показано на рисунке 5, и рассмотрим далее пример.

Пример — Пусть архитектура (рисунок 5), где некоторое число элементов функций безопасности реализуется подсистемой, выполненной по одноканальной архитектуре, состоящей из элементов 1, 2 и 3, которые соответствуют требованиям таблиц 2 и 3 следующим образом:

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

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

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

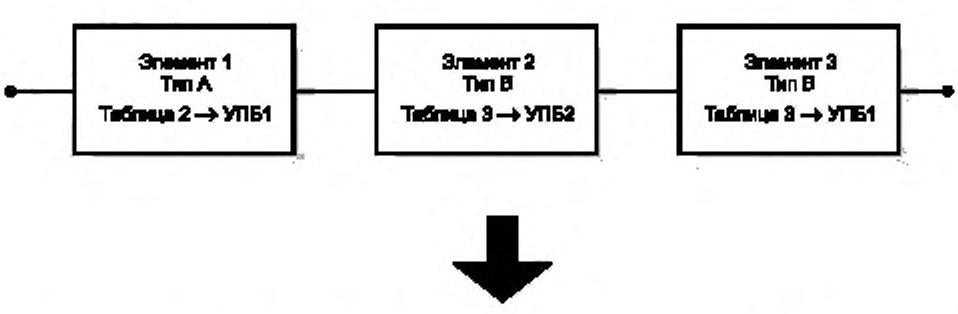


Рисунок 5 — Порядок определения максимального значения УПБ для заданной архитектуры (Э/Э/ПЭ подсистема, связанная с безопасностью, состоящая из последовательности элементов, см. 7.4.4.2.3)

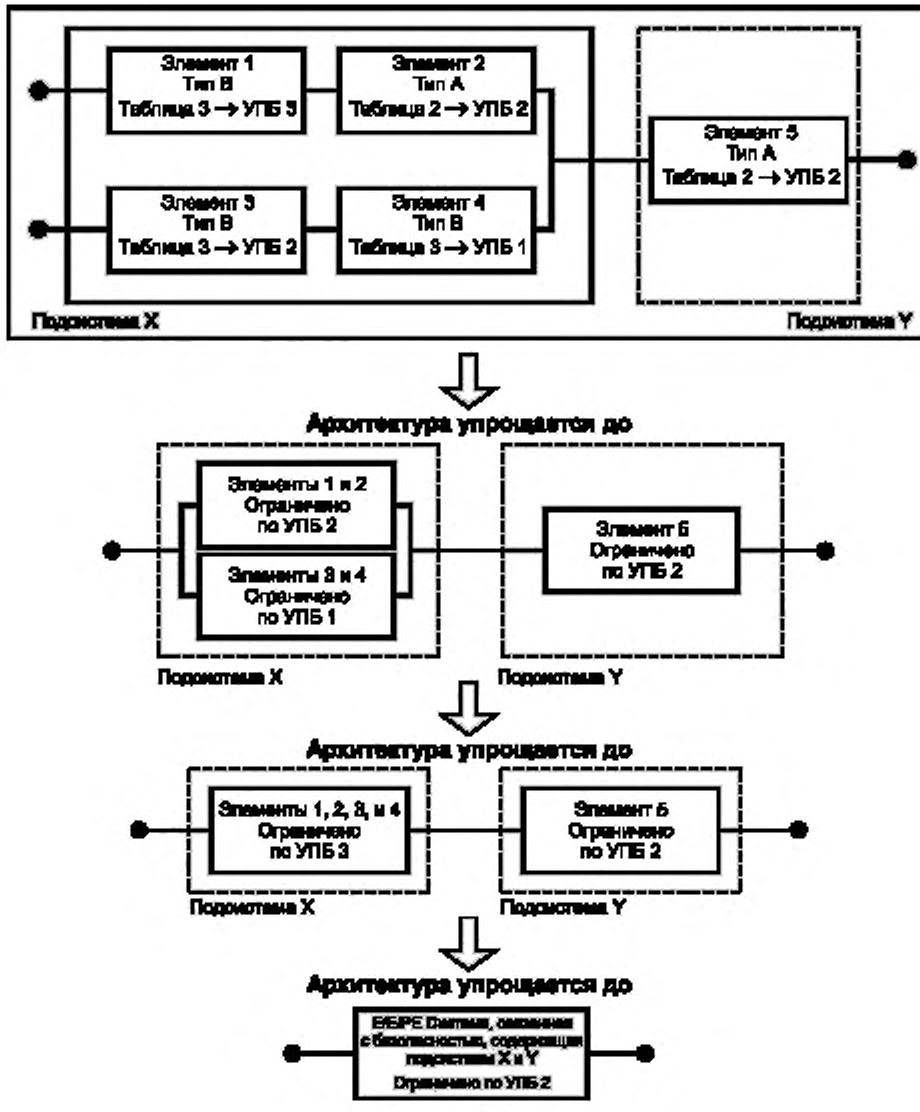
Оба элемента 1 и 3 ограничивают максимальный уровень полноты безопасности, который может потребоваться для соответствия отказоустойчивости аппаратных средств и доле безопасных отказов, до УПБ1.

7.4.4.2.4 В Э/Э/ПЭ подсистеме, связанной с безопасностью, в которой функция безопасности реализуется в многоканальной архитектуре (параллельное соединение элементов) с отказоустойчивостью аппаратных средств, равной *N*, максимальный уровень полноты безопасности, который может быть достигнут для рассматриваемой функции безопасности, должен быть определен:

a) группированием последовательно соединенных элементов для каждого канала и затем определением максимального уровня полноты безопасности, который может быть достигнут для рассматриваемой функции безопасности для каждого канала (см. 7.4.4.2.3), и

b) выбором канала с самым высоким уровнем полноты безопасности, который может быть достигнут для рассматриваемой функции безопасности и затем сложением уровней полноты безопасности *N* для определения максимальной полноты безопасности для полной подсистемы.

Для того чтобы проиллюстрировать этот метод, примем архитектуру, как показано на рисунке 6, и рассмотрим следующий пример.



Примечания

1 Элементы 1 и 2 реализуют требуемую часть функции безопасности подсистемы X независимо от элементов 3 и 4 и наоборот.

2 Подсистемы, выполняющие функцию безопасности, считают полной Э/Э/ПЭ системой, связанной с безопасностью, включая все элементы — от сенсоров до исполнительных устройств.

Рисунок 6 — Порядок определения максимального УПБ для заданной архитектуры (Э/Э/ПЭ подсистема, связанная с безопасностью, состоящая из двух подсистем X и Y, см. 7.4.4.2.4)

Примечания

1 *N* — отказоустойчивость аппаратных средств комбинации параллельных элементов (см. 7.4.4.1.1).

2 В примере рассматривается применение настоящего подпункта.

Пример — Группирование и анализ этих комбинаций могут быть проведены разными методами. Для иллюстрации одного из возможных методов принимают архитектуру, в которой конкретная функция безопасности реализована двумя подсистемами X и Y, где подсистема X состоит из элементов 1, 2, 3 и 4, а подсистема Y — из одного элемента 5, как показано на рисунке 6. Использование параллельных каналов в подсистеме X гарантирует, что элементы 1 и 2 реализуют требуемую часть функции безопасности подсистемы X независимо от элементов 3 и 4 и наоборот. Функцию безопасности считают выполненной:

- при событии отказа в элементе 1 или 2 (поскольку комбинация элементов 3 и 4 позволяет реализовать требуемую часть функции безопасности) или

- при событии отказа в элементе 3 или 4 (поскольку комбинация подсистем 1 и 2 позволяет реализовать требуемую часть функции безопасности).

Далее подробно рассматривают процедуру определения максимального уровня полноты безопасности, который может потребоваться для рассматриваемой функции безопасности:

В подсистеме X при заданной функции безопасности каждый элемент соответствует требованиям таблиц 2 и 3 следующим образом:

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

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

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

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

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

a) Объединение элементов 1 и 2. Отказоустойчивость аппаратных средств и доля безопасных отказов, обеспеченная комбинацией элементов 1 и 2 (каждая в отдельности соответствует требованиям для УПБ 3 и УПБ 2, соответственно), соответствует требованиям УПБ 2 (определенным элементом 2, см. 7.4.4.2.3).

b) Объединение элементов 3 и 4. Отказоустойчивость аппаратных средств и доля безопасных отказов, обеспеченная комбинацией элементов 3 и 4 (каждая в отдельности соответствует требованиям для УПБ 2 и УПБ 1, соответственно), соответствует требованиям УПБ 1 (определенным элементом 5, см. 7.4.4.2.3).

c) Дальнейшее объединение комбинации элементов 1 и 2 с комбинацией элементов 3 и 4. Максимальный уровень полноты безопасности аппаратных средств, который может быть достигнут для рассматриваемой функции безопасности, определяется выбором канала с самым высоким уровнем полноты безопасности, который был достигнут, и затем сложением уровней полноты безопасности N для определения максимального уровня полноты безопасности для всей комбинации элементов. В данном случае подсистема включает в себя два параллельных канала с отказоустойчивостью аппаратных средств, равной 1. Каналом с самым высоким уровнем полноты безопасности для рассматриваемой функции безопасности является канал, включающий в себя элементы 1 и 2 и соответствующий требованиям для УПБ 2. Поэтому максимальный уровень полноты безопасности для подсистемы при отказоустойчивости аппаратных средств, равной 1, будет УПБ 2 + 1 = УПБ 3 (см. 7.4.4.2.4).

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

Для полной Э/Э/ПЭ системы, связанной с безопасностью (включающей в себя две подсистемы X и Y, которые достигли требований для рассматриваемой функции безопасности УПБ 3 и УПБ 2 соответственно), максимальный уровень полноты безопасности, который может быть достигнут для Э/Э/ПЭ системы, связанной с безопасностью, определен подсистемой, которая достигла самого низкого уровня полноты безопасности (7.4.4.2.1, перечисление 5). Поэтому для настоящего примера максимальным уровнем полноты безопасности, который может быть достигнут для Э/Э/ПЭ системы, связанной с безопасностью, для рассматриваемой функции безопасности является УПБ 2.

7.4.4.3 Способ 2_H

7.4.4.3.1 Минимальное значение отказоустойчивости аппаратных средств для каждой подсистемы Э/Э/ПЭ системы, связанной с безопасностью, выполняющей функцию безопасности с заданным уровнем полноты безопасности, должно быть следующим:

Примечание — Для следующих перечислений, если не указано иное, считается, что функция безопасности может выполняться либо в режиме с низкой частотой запросов, либо в режиме с высокой частотой запросов или с непрерывным запросом.

a) значение отказоустойчивости аппаратных средств равно 2 для заданной функции безопасности с УПБ 4, если не применяются условия по 7.4.4.3.2;

b) значение отказоустойчивости аппаратных средств равно 1 для заданной функции безопасности с УПБ 3, если не применяются условия по 7.4.4.3.2;

c) значение отказоустойчивости аппаратных средств равно 1 для заданной функции безопасности с УПБ 2, если не применяются условия по 7.4.4.3.2;

d) значение отказоустойчивости аппаратных средств равно 0 для заданной функции безопасности с УПБ 2, работающей в режиме с низкой частотой запросов;

e) значение отказоустойчивости аппаратных средств равно 0 для заданной функции безопасности с УПБ 1.

7.4.4.3.2 Если установлено, только для элементов типа А, что, следуя требованиям отказоустойчивости аппаратных средств, определенным в 7.4.4.3.1, для конкретной ситуации требуется значение отказоустойчивости аппаратных средств больше 0, и это приводит к дополнительным отказам и уменьшению полной безопасности УО, то может быть реализована более безопасная альтернативная архитектура с уменьшенным значением отказоустойчивости аппаратных средств (*HFT)*. В таком случае решение должно быть обосновано и документально оформлено. Обоснование должно представить свидетельства о том, что:

a) соответствие с требованиями отказоустойчивости аппаратных средств, определенными в 7.4.4.3.1, приведет к дополнительным отказам, уменьшению полной безопасности УО и

b) если значение отказоустойчивости аппаратных средств уменьшено до нуля, то режимы отказа, идентифицированные в элементе, выполняющем функцию безопасности, могут не учитываться, потому что интенсивность(и) опасных отказов идентифицированного режима(ов) отказа очень низка по сравнению с целевой мерой отказов для рассматриваемой функции безопасности [(см. 7.4.4.1.1, перечисление c)]. То есть сумма интенсивностей опасных отказов всех последовательно соединенных элементов, для которых требуется исключение ошибки, не должна превышать 1 % целевой меры отказа. Более того, такое использование исключений ошибки должно быть обосновано с учетом возможности систематических ошибок.

Примечание — Отказоустойчивость — предпочтительный путь получить необходимую уверенность в том, что была достигнута робастная архитектура. Если применяют требования 7.4.4.3.2, то цель обоснования состоит в том, чтобы продемонстрировать, что предложенная альтернативная архитектура обеспечивает эквивалентное или лучшее решение. Реализация такого решения может зависеть от технической сферы и/или применения. Например, применяют: механизмы резервирования (аналитическая избыточность — замена выхода неисправного датчика, выполненная физическим вычислением выходных результатов других датчиков); использование более надежных положений той же самой технологии (при их наличии); изменения для увеличения надежности технологии; сокращение влияния отказов по общей причине при использовании разных технологий; расширение области проектирования; ограничение условий окружающей среды (например, для электронных компонентов); снижение неопределенности данных о надежности, накапливая данные в процессе эксплуатации или оценки экспертов.

7.4.4.3.3 Если выбран способ 2_H, то данные о надежности, используемые для определения количественного значения случайных отказов аппаратных средств (см. 7.4.5), должны быть:

a) основаны на данных об эксплуатации элементов в аналогичном применении и в подобных условиях окружающей среды и

b) основаны на данных, собранных в соответствии со стандартами (например, [5] или [6]), и

c) оценены в соответствии:

i) с количеством данных об эксплуатации и ii) результатами экспертной оценки, и, где необходимо,

iii) результатами проведенных специальных тестов,

чтобы оценить среднее значение и уровень неопределенности [например, 90%-ный доверительный интервал или распределение вероятности (см. примечание 2)] для каждого параметра надежности (например, интенсивность отказов) используемого в вычислениях.

Примечания

1 Конечные пользователи стимулируются для организации соответствующих наборов данных по надежности, как описано в [5] или [6].

2 90%-ный доверительный интервал интенсивности отказов λ — это интервал $[\lambda_{5\,\%}, \lambda_{95\,\%}]$, в котором ее фактические значения должны принадлежать с вероятностью 90 %. λ принимает значения с вероятностью 5 %, лучше чем $\lambda_{5\,\%}$ и хуже чем $\lambda_{95\,\%}$. Чисто статистически среднее значение интенсивности отказов может быть оценено при использовании «оценки максимальной вероятности», а доверительные границы $\lambda_{5\,\%}$ и $\lambda_{95\,\%}$ могут быть вычислены с помощью функции χ^2. Точность зависит от общего времени наблюдения и числа наблюдаемых отказов. Для обработки статистических наблюдений, экспертных оценок и конкретных результатов испытаний может ис-

пользоваться Байесовский подход. Эти данные могут использоваться для формирования соответствующих функций распределения вероятностей для дальнейшего использования в методе моделирования Монте Карло.

Если выбран способ 2_H, то необходимо учесть неопределенность данных о надежности при вычислении целевой меры отказов (то есть PFD_{avg} или PFH), и систему следует дорабатывать до тех пор, пока нет уверенности более чем на 90 % в том, что достигнута целевая мера отказов.

7.4.4.3.4 Если выбран способ 2_H, то все элементы типа B должны иметь, как минимум, охват диагностикой не менее 60 %.

7.4.5 Требования к количественной оценке случайных отказов аппаратных средств

Примечание — В разделе А.2 МЭК 61508-6 приведен краткий обзор необходимых шагов в достижении требуемой полноты безопасности аппаратных средств и показано, как настоящий пункт связан с другими требованиями настоящего стандарта.

7.4.5.1 Для каждой функции безопасности полнота безопасности, достигнутая Э/Э/ПЭ системой, связанной с безопасностью, из-за случайных отказов аппаратных средств (включая ошибки программ) и в коммуникационных процессах должна быть оценена по 7.4.5.2 и 7.4.11 и должна быть равна или менее целевой меры отказов, определенной в спецификации требований к безопасности Э/Э/ПЭ системы (см. подраздел 7.10 МЭК 61508-1).

Примечание — Для того чтобы показать, что это было достигнуто, необходимо выполнить прогнозирование надежности для рассматриваемой функции безопасности, используя соответствующие методы (см. 7.4.5.2), и сравнить результаты с целевой мерой отказов для этой функции безопасности (см. МЭК 61508-1).

7.4.5.2 При оценке достигнутой меры отказов каждой функции безопасности в соответствии с требованиями 7.4.5.1 следует учитывать:

a) архитектуру Э/Э/ПЭ системы, связанной с безопасностью в терминах ее подсистем, поскольку это касается каждой рассматриваемой функции безопасности.

Примечание — При этом приходится решать, какие виды отказов элементов подсистем находятся в последовательной связи (любой отказ вызывает отказ соответствующей функции безопасности, которая должна выполняться), а какие виды отказов находятся в параллельной связи (для сбоя соответствующей функции безопасности необходимы совпадающие отказы);

b) архитектуру каждой Э/Э/ПЭ подсистемы, связанной с безопасностью в терминах ее элементов, поскольку это касается каждой рассматриваемой функции безопасности;

c) оцененную интенсивность отказов каждой подсистемы и ее элементов в любых режимах, которые могли бы вызвать опасный отказ Э/Э/ПЭ системы, связанной с безопасностью, но которые обнаружены диагностической проверкой (см. 7.4.9.3 и 7.4.9.4). Должно быть приведено обоснование интенсивности отказов с учетом источника данных и его точности или допустимого отклонения. Обоснование может включать в себя рассмотрение и сравнение данных из многих источников, а также объяснение выбора интенсивностей отказов систем, наиболее близко напоминающих рассматриваемую. Интенсивность отказов, используемая для количественной оценки случайных отказов аппаратных средств и вычисления доли безопасных отказов или охвата диагностикой, должна учитывать указанные условия эксплуатации.

Примечание — Для выбора интенсивности отказов из баз данных обычно бывает необходимо учесть условия эксплуатации, связанные, например, с нагрузкой или температурой;

d) восприимчивость Э/Э/ПЭ системы, связанной с безопасностью, и ее подсистем к отказам по общей причине (см. примечания 1 и 2). Сделанные предположения должны быть обоснованы.

Примечания

1 Отказы из-за влияния общей причины могут быть результатом других влияний, отличных от реальных отказов компонентов аппаратных средств (например, электромагнитные помехи, ошибки декодирования и т. п.). Однако такие отказы рассматриваются в настоящем стандарте как оцениваемые количественно случайные отказы аппаратных средств. Тестирование в шахматном порядке приводит к уменьшению отказов по общей причине.

2 Если отказы по общей причине, идентифицируемые между Э/Э/ПЭ системами, связанными с безопасностью, формируют запрос к ним или к другим уровням защиты, то должно быть подтверждение в том, что отказы по общей причине были учтены при определении требований к уровню полноты безопасности и целевой мере отказов. О методах определения факторов общей причины см. приложение D МЭК 61508-6;

e) охват диагностическими тестами (по приложению С) и связанные с ним диагностический испытательный интервал и интенсивность не обнаруженных диагностикой опасных отказов для случайных

отказов аппаратных средств каждой подсистемы. В соответствующих случаях необходимо рассматривать только те диагностические тесты, которые соответствуют требованиям 7.4.5.3. В модели надежности необходимо учесть *MTTR* и *MRT* (см. пункты 3.6.21 и 3.6.22 МЭК 61508-4).

Примечание — При установлении времени диагностического испытательного интервала должны быть рассмотрены интервалы между всеми испытаниями, которые вносят вклад в охват диагностикой;

f) интервалы времени, на которых реализуются контрольные проверки для обнаружения опасных ошибок;

g) является ли контрольная проверка эффективной на 100 %.

Примечание — В результате выполнения несовершенной контрольной проверки функция безопасности может не восстановиться до состояния «как новая», и поэтому вероятность отказа увеличится. Для сделанных предположений должно быть дано обоснование, в частности, должны быть включены периоды возобновления работоспособности для элементов или некоторое снижение риска дальнейшего выполнения функции безопасности. Необходимо рассмотреть продолжительность испытания, если элемент будет проверяться автономно;

h) время ремонта для обнаруженных отказов.

Примечание — Среднее время ремонта *MRT* составляет часть среднего времени восстановления *MTTR* (см. пункты 3.6.22 и 3.6.21 МЭК 61508-4), включающего в себя также время обнаружения отказа и период времени, в течение которого ремонт невозможен (пример того, как *MTTR* и *MRT* используются для вычисления вероятности отказа, приведен в приложении В МЭК 61508-6). Можно полагать, что ремонт происходит мгновенно только тогда, когда УО выключено или находится в безопасном состоянии во время ремонта. Для ситуаций, когда ремонт может быть выполнен в течение конкретного периода времени, например, в то время как управляемое оборудование отключено или находится в надежном (закрытом) состоянии, особенно важно, чтобы при полном расчете был учтен период времени, когда ремонт не может быть произведен, особенно, когда этот период является относительно большим. Все соответствующие факторы, связанные с ремонтом, должны быть учтены;

i) влияние случайной ошибки человека, если человек обязан принимать меры для выполнения функции безопасности.

Примечание — Природу случайной ошибки человека необходимо рассмотреть в условиях, когда человек готов к опасному событию и обязан принимать данные меры, тогда вероятность ошибки человека должна быть включена в вычисление полной вероятности;

j) тот факт, что доступны многие методы моделирования и что самый подходящий метод выбирает аналитик, и этот выбор зависит от ряда обстоятельств. Доступные методы включают в себя: анализ последствий причин отказов (см. В.6.6.2 приложения В МЭК 61508-7), анализ дерева ошибки (см. В.6.6.5 приложения В МЭК 61508-7), модели Маркова (см. приложение В МЭК 61508-6 и В.6.6.6 приложения В МЭК 61508-7), блок-диаграммы надежности (см. приложение В МЭК 61508-6 и В.6.6.7 МЭК 61508-7) и сети Петри (см. приложение В МЭК 61508-6 и В.2.3.3 приложения В МЭК 61508-7);

Примечания

1 Упрощенный подход, который может быть использован для оценки средней вероятности опасного отказа по запросу функции безопасности из-за случайных отказов аппаратных средств для определения того, как аппаратура обеспечивает требуемую целевую меру отказов, описан в приложении В МЭК 61508-6.

2 Краткий обзор необходимых шагов для достижения аппаратными средствами полноты безопасности и соотношения с другими требованиями настоящего стандарта приведены в подразделе А.2 приложения А МЭК 61508-6.

3 Необходимо отдельно для каждой функции безопасности количественно определять надежность Э/Э/ПЭ систем, связанных с безопасностью, поскольку на нее будут оказывать влияние как разнообразие видов отказов компонентов, так и изменения архитектуры (при использовании избыточности) самих Э/Э/ПЭ систем, связанных с безопасностью.

7.4.5.3 При количественной оценке случайных отказов аппаратных средств подсистемы со значением отказоустойчивости аппаратных средств, равным нулю, которая осуществляет функцию безопасности или часть функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами, доверие (предпочтение) должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и время выполнения определенного действия для достижения или поддержания безопасного состояния меньше времени безопасности процесса; или
- при работе в режиме высокой частоты запросов отношение частоты диагностических испытаний к частоте запросов равно или более 100.

7.4.5.4 Диагностический испытательный интервал любой подсистемы, которая:

- имеет значение отказоустойчивости аппаратных средств больше нуля и которая осуществляет функцию безопасности или часть функции безопасности, действуя в режиме высокой частоты запросов или с непрерывными запросами, или

- осуществляет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов,

должен быть таким, чтобы суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа было меньше среднего времени восстановления *MTTR*, используемого в вычислении при определении достигаемой полноты безопасности для этой функции безопасности.

7.4.5.5 Если для конкретного проекта требование к полноте безопасности для выполняемой функции безопасности не достигается, то следует:

- определить элементы, подсистемы и/или параметры, вносящие наибольший вклад в формулу расчета интенсивности отказов;

- оценить влияние возможных мер усовершенствования на выявленные критические компоненты, подсистемы или параметры (например, более надежные компоненты, дополнительные меры защиты от отказов по общей причине, расширенный охват диагностикой, расширенная избыточность, уменьшение интервала контрольных испытаний, смещение проверок и т. п.);

- выбрать и осуществить подходящие меры усовершенствования;

- повторить необходимые шаги для вычисления нового значения вероятности случайных отказов аппаратных средств.

7.4.6 Требования по предотвращению систематических отказов

Примечание — Подробности применения требований данного пункта см. в 7.4.2.2, перечисление с).

7.4.6.1 Должна быть использована соответствующая группа методов и средств, предназначенных для предотвращения внесения ошибок во время разработки и создания аппаратных средств и программного обеспечения Э/Э/ПЭ системы, связанной с безопасностью (см. таблицу В.2 и МЭК 61508-3).

Примечание — Настоящий стандарт не содержит конкретных требований, касающихся предотвращения систематических ошибок во время проектирования серийно выпускаемых электронных интегральных схем, таких как стандартные микропроцессоры, так как вероятность ошибок в таких устройствах минимизирована строгими процедурами разработки, строгим тестированием и обширным опытом использования со значительной информацией от пользователей. Применение электронных интегральных схем, таких как новые устройства или СИС, не может быть таким образом обосновано. Поэтому к СИС, если они должны использоваться в Э/Э/ПЭ системе, связанной с безопасностью, будут применяться требования, представленные в 7.4.6.7 и приложении F. В случае сомнения (об обширном опыте использования со значительной информацией от пользователей) должны быть учтены требования для «опыта работы на месте» по таблице В.6 приложения В с эффективностью «низкий» для УПБ 1 и УПБ 2, эффективностью «средний» — для УПБ 3 и эффективностью «высокий» — для УПБ 4.

7.4.6.2 В соответствии с требуемым уровнем полноты безопасности выбранный метод проектирования должен обладать возможностями, способствующими:

a) прозрачности, модульности и другим характеристикам, которые управляют сложностью проекта;

b) ясности и точности представления:

- функциональных возможностей,
- интерфейсов между подсистемами и элементами,
- информации, устанавливающей последовательность и время,
- параллелизма и синхронизации;

c) ясности и точности документирования и передачи информации;

d) проверке и подтверждению соответствия.

7.4.6.3 Требования к техническому обслуживанию для гарантированного поддержания на необходимом уровне требуемой полноты безопасности Э/Э/ПЭ систем, связанных с безопасностью, должны быть формализованы на стадии проектирования.

7.4.6.4 Следует использовать (где применимо) автоматические средства измерения и интегрированные инструментальные средства разработки.

7.4.6.5 В период проектирования должны быть запланированы испытания интеграции Э/Э/ПЭ систем S. Документация по планированию испытаний должна включать в себя:

a) типы проводимых испытаний и сопровождающие их процедуры;

b) условия окружающей среды при испытаниях, испытательные средства, схему испытаний и программы испытаний;

c) критерии оценки «прошел испытание»/«не прошел испытание».

7.4.6.6 В период проектирования действия, выполняемые на рабочем месте проектировщика, должны отличаться от действий, которые должны быть доступными на рабочем месте пользователя.

7.4.6.7 В период проектирования и разработки СИС должна использоваться соответствующая группа методов и средств, предназначенных для предотвращения внесения ошибок.

Примечание — Методы и средства, которые поддерживают достижение соответствующих свойств, приведены в приложении F. Жизненный цикл разработки СИС представлен на рисунке 3.

7.4.7 Требования по управлению систематическими сбоями

Примечание — Подробности применения требований настоящего пункта см. в 7.4.2.2, перечисление c).

7.4.7.1 Для управления систематическими сбоями проектирование Э/Э/ПЭ системы должно обладать особенностями проектирования, которые делают Э/Э/ПЭ системы, связанные с безопасностью, устойчивыми:

a) к любым остаточным ошибкам проектирования аппаратных средств, если вероятность ошибок проектирования аппаратных средств не может быть исключена (см. таблицу А.15 приложения А);

b) внешним влияниям, включая электромагнитные воздействия (см. таблицу А.16 приложения А);

c) ошибкам оператора управляемого оборудования (см. таблицу А.17 приложения А);

d) любым остаточным ошибкам в программном обеспечении (см. МЭК 61508-3, пункт 7.4.3 и соответствующие таблицы);

e) любым ошибкам, возникающим в результате выполнения любого процесса передачи данных (см. 7.4.8).

7.4.7.2 Для облегчения реализации свойств ремонтопригодности и тестируемости в созданных Э/Э/ПЭ системах, связанных с безопасностью, эти свойства должны быть учтены в процессе проектирования и создания Э/Э/ПЭ систем.

7.4.7.3 При проектировании Э/Э/ПЭ систем, связанных с безопасностью, должны быть учтены способности и возможности человека, а созданные Э/Э/ПЭ системы должны быть удобны для работы персонала по эксплуатации и технической поддержке. Разработка всех интерфейсов должна следовать «положительному опыту» при учете человеческого фактора и учитывать возможный уровень подготовки или осведомленности операторов, например, для Э/Э/ПЭ систем массового производства, где оператором является специально не подготовленный человек.

Примечания

1 Цель проектирования должна состоять в том, чтобы предсказуемые критические ошибки, допущенные операторами или персоналом технической поддержки, предотвращались или устранялись проектом везде, где возможно, либо действия для их выполнения требовали повторного подтверждения.

2 Некоторые ошибки, допущенные операторами или персоналом технического обслуживания, могут быть не восстанавливаемыми Э/Э/ПЭ системами, связанными с безопасностью, например, если они являются не обнаруживаемыми или реально восстанавливаемыми исключительно при непосредственном доступе, например, некоторые механические отказы в управляемом оборудовании.

7.4.8 Требования к поведению системы при обнаружении отказов

Примечание — Требования настоящего пункта относятся к заданным функциям безопасности, выполняемым одиночной Э/Э/ПЭ системой, связанной с безопасностью, для которой полная функция безопасности не была распределена между другими средствами по снижению риска.

7.4.8.1 Обнаружение опасного отказа (с помощью диагностических тестов, контрольных испытаний или иным методом) в любой подсистеме с отказоустойчивостью аппаратных средств больше нуля должно завершаться:

a) конкретным действием для достижения или поддержания безопасного состояния (см. примечание), или

b) изоляцией дефектной части подсистемы для обеспечения возможности продолжения выполнения безопасного действия управляемым оборудованием, пока дефектная часть не будет отремонтирована. Если ремонт не завершен в пределах средней продолжительности ремонта (*MRT*) (см. пункт 3.6.22 МЭК 61508-4), принятого при вычислении вероятности случайных отказов аппаратных средств (см. 7.4.5.2), то для достижения и поддержания их безопасного состояния должно быть выполнено конкретное действие (см. примечание).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в требованиях безопасности Э/Э/ПЭ системы, необходимо выполнить конкретное действие (реакцию на от-

каз). Это действие может состоять, например, в безопасном отключении управляемого оборудования или той его части, функциональная безопасность которой реализуется в дефектной подсистеме.

7.4.8.2 Обнаружение опасного отказа (с помощью диагностических тестов, контрольных испытаний или иным способом) в любой подсистеме, с отказоустойчивостью аппаратных средств равной нулю, в случае если такая подсистема используется только функцией(ми) безопасности в режиме с низкой частотой запросов, должно завершаться:

a) конкретным действием для достижения и поддержания безопасного состояния либо

b) восстановлением дефектной подсистемы за период времени средней продолжительности ремонта (*MRT*), см. пункт 3.6.22 МЭК 61508-4, полученный при расчете вероятности случайных отказов аппаратных средств (см. 7.4.5.2). В течение этого времени безопасность управляемого оборудования должна обеспечиваться дополнительными мерами и ограничениями. Полнота безопасности, обеспеченная этими мерами и ограничениями, должна по крайней мере равняться полноте безопасности, обеспеченной Э/Э/ПЭ системой, связанной с безопасностью, в отсутствие любых отказов. В процедурах эксплуатации и технического обслуживания Э/Э/ПЭ системы должны быть определены дополнительные меры и ограничения (см. 7.6).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в спецификации требований безопасности Э/Э/ПЭ системы, необходимо выполнить конкретное действие (реакцию на отказ). Это действие может состоять, например, в безопасном отключении управляемого оборудования или той его части, функциональная безопасность которой реализуется в дефектной подсистеме.

7.4.8.3 Обнаружение опасного отказа (путем диагностического тестирования, контрольных испытаний или иным способом) в любой подсистеме, с отказоустойчивостью равной нулю, в случае подсистемы, выполняющей любую функцию(и) безопасности, действующей(их) в режиме с высокой частотой запросов или непрерывными запросами для достижения и поддержания безопасного состояния, должно завершаться конкретными действиями (см. примечание).

Примечание — Для достижения и поддержания безопасного состояния, которое должно быть определено в требованиях безопасности Э/Э/ПЭ системы, необходимо выполнить конкретное действие (реакцию на отказ). Это действие может состоять, например, в безопасном отключении управляемого оборудования или той его части, функциональная безопасность которой реализуется в дефектной подсистеме.

7.4.9 Требования к реализации Э/Э/ПЭ системы

7.4.9.1 Э/Э/ПЭ системы, связанные с безопасностью, должны быть изготовлены в соответствии со спецификацией требований проектирования Э/Э/ПЭ системы (см. 7.2.3).

7.4.9.2 Подсистемы и их элементы, используемые для одной или более функций безопасности, должны быть идентифицированы и документально оформлены как подсистемы и элементы, связанные с безопасностью.

7.4.9.3 Для каждой подсистемы, связанной с безопасностью, должна быть представлена следующая информация (см. также 7.4.9.4):

Примечание — Поставщик подсистемы или элемента, от которого требуется соответствие МЭК 61508, должен предоставить эту информацию разработчику системы, связанной с безопасностью (либо другой подсистемы или элемента), в виде соответствующего руководства по безопасности (см. приложение D).

a) функциональная спецификация подсистемы и ее элементов (по мере необходимости);

b) все инструкции или ограничения, касающиеся применения подсистемы и ее элементов, которые должны быть соблюдены для предотвращения систематических отказов подсистемы;

c) стойкость к систематическим отказам каждого элемента [см. перечисление c) 7.4.2.2];

d) определение конфигурации аппаратных средств и/или программного обеспечения элемента, позволяющее управлять конфигурацией Э/Э/ПЭ системы, связанной с безопасностью, в соответствии с пунктом 6.2.1 МЭК 61508-1;

e) документально оформленное доказательство того, что подсистема и ее элементы прошли проверку указанных для них функциональных требований и стойкости к систематическим отказам в соответствии со спецификацией требований проектирования Э/Э/ПЭ системы (см. 7.2.3).

7.4.9.4 Для каждого элемента, связанного с безопасностью, в котором возможны случайные отказы аппаратных средств, должна быть представлена следующая информация (см. также 7.4.9.3 и 7.4.9.5):

Примечание — Поставщик элемента, от которого требуется соответствие МЭК 61508, должен предоставить эту информацию разработчику системы, связанной с безопасностью, в виде руководства по безопасности для поставляемого элемента, см. приложение D.

a) виды отказа элемента (в виде описания поведения его выходов) из-за случайных отказов аппаратных средств, которые приводят к отказу функции безопасности и не выявляются внутренними для элемента диагностическими тестами или не обнаруживаются диагностикой, внешней к элементу (см. 7.4.9.5);

b) для каждого вида отказов, рассмотренного в перечислении a), оцененная интенсивность отказов для указанных условий эксплуатации;

c) виды отказов элемента (в виде описания поведения его выходов) из-за случайных отказов аппаратных средств, которые приводят к отказу функции безопасности и выявляются внутренними для элемента диагностическими тестами или обнаруживаются диагностикой, внешней к элементу (см. 7.4.9.5);

d) для каждого вида отказов, рассмотренного в перечислении c), оцененная интенсивность отказов для указанных условий эксплуатации;

e) все ограничения на окружающую среду элемента, которые должны быть соблюдены для обеспечения легитимности оценочных частот отказов из-за случайных отказов аппаратных средств;

f) любое ограничение срока жизни элемента, который не должен быть превышен для обеспечения легитимности оценочных частот отказов из-за случайных отказов аппаратных средств;

g) требования к любым контрольным испытаниям и/или техническому обслуживанию;

h) для каждого вида отказов, рассмотренного в перечислении c), выявленного внутренними для элемента диагностическими тестами, — охват диагностикой, полученный в соответствии с приложением C [см. примечание к перечислению i)];

i) для каждого вида отказов, рассмотренного в перечислении c), выявленного внутренними для элемента диагностическими тестами, междиагностический интервал (см. примечание).

Примечание — Охват диагностикой и междиагностический интервал необходимы, если требуется доверие к действиям по проведению диагностических тестов, выполняемых для элемента при моделировании полноты безопасности аппаратных средств Э/Э/ПЭ системы, связанной с безопасностью (см. 7.4.5.2, 7.4.5.3 и 7.4.5.4);

j) интенсивность отказов диагностики из-за случайных отказов аппаратных средств;

k) любая дополнительная информация (например, время ремонта), необходимая для обеспечения возможности получения среднего значения времени ремонта (*MRT*) (см. пункт 3.6.22 МЭК 61508-4) после обнаружения отказа с помощью диагностики;

l) вся информация, необходимая для обеспечения определения доли безопасных отказов (ДБО) элемента, как принято в Э/Э/ПЭ системе, связанной с безопасностью, определенной в соответствии с приложением C, включая классификацию элементов на тип A и тип B, в соответствии с 7.4.4;

m) отказоустойчивость элемента аппаратных средств.

7.4.9.5 Оценочные частоты отказов элемента из-за случайных отказов аппаратных средств [см. перечисления a) и c) 7.4.9.4] могут быть определены:

a) методом анализа видов и последствий отказов проекта с использованием данных по отказам элементов из признанного промышленного источника либо

b) из предыдущего опыта использования элемента в похожих условиях окружающей среды (см. 7.4.10).

Примечания

1 Уровень доверия любых используемых данных о частоте отказов должен быть по крайней мере равен 70 %. Статистическое определение уровня доверия приведено в [7]. Эквивалентный термин «уровень значимости» используется в [8].

2 Предпочтительно, чтобы место размещения данных об отказах было доступным. Если доступ к таким данным невозможен, то может потребоваться использование общих данных.

3 Хотя понятие «постоянная частота отказов» подсистемы принято большинством вероятностных оценочных методов, оно применимо лишь при условии, что не превышен срок жизни компонентов подсистемы. Вне их полезного срока жизни (так как вероятность отказов значительно увеличивается со временем) результаты большинства вероятностных расчетных методов бесполезны. Таким образом, любая вероятностная оценка должна включать в себя спецификацию полезного срока жизни компонентов. Полезный срок жизни компонентов подсистем очень зависит от самого компонента и от условий его эксплуатации, особенно температуры окружающей среды компонента (например, электролитические конденсаторы могут быть очень чувствительны к температуре). Опыт показывает, что полезный срок жизни компонентов часто находится в пределах 8—12 лет. Однако эти сроки могут быть значительно меньшими, если компоненты работают в условиях значений параметров эксплуатации близких к предельным.

7.4.9.6 Для каждого применяемого изделия, для которого требуется соответствие стандартам серии МЭК 61508, поставщики должны обеспечить руководство по безопасности в соответствии с приложением D.

7.4.9.7 Поставщик должен документально обосновать всю информацию, которая представлена в каждом руководстве по безопасности для применяемых изделий.

Примечания

1 Важно, чтобы требуемое безопасное исполнение конкретного элемента было обеспечено достаточными доказательствами. Требования, не обеспеченные достаточными доказательствами, не помогают установить корректность и полноту функции безопасности, в реализации которой участвует элемент.

2 Могут существовать коммерческие или юридические ограничения на доступность доказательств. Эти ограничения в настоящем стандарте не рассматриваются. Если такие ограничения не обеспечивают необходимого доступа к доказательствам оценки функциональной безопасности, то такой элемент в Э/Э/ПЭ системах, связанных с безопасностью, не используется.

7.4.10 Требования к проверенным в эксплуатации элементам

Примечание — Подробности применения требований настоящего пункта см. в перечислении c) 7.4.2.2.

7.4.10.1 Элемент должен рассматриваться как проверенный в эксплуатации, только если он имеет явно ограниченные и определенные функциональные возможности и при наличии соответствующего документально оформленного свидетельства, демонстрирующего, что вероятность любых опасных систематических сбоев существенно меньше требуемых уровней полноты безопасности функций безопасности, которые используют этот элемент. Доказательства должны быть основанными на анализе опыта работы конкретной конфигурации элемента, проведенном вместе с анализом пригодности и тестированием.

Примечание — Анализ пригодности и тестирование сосредотачиваются на демонстрации работы элемента в конкретном применении. Должны быть учтены результаты уже проведенного анализа и тестирования. Они включают в себя функциональное поведение, точность, поведение в случае сбоя, время отклика, реакцию на перегрузку, удобство и простоту использования (например, предотвращение ошибки человека) и ремонтопригодность.

7.4.10.2 Документально оформленное свидетельство в соответствии с 7.4.10.1 должно продемонстрировать, что:

a) предыдущие условия эксплуатации (см. примечание) конкретного элемента являются такими же или достаточно близкими к тем, в которых будет эксплуатироваться элемент в Э/Э/ПЭ системе, связанной с безопасностью.

Примечание — Условия эксплуатации (эксплуатационный профиль) включают в себя все факторы, которые могут вызвать систематические ошибки в элементе аппаратных средств и программного обеспечения, например, окружающую среду, виды использования, выполняемые функции, конфигурацию, связи с другими системами, операционную систему, тип транслятора, человеческий фактор. Точные условия обеспечения подобия эксплуатационного профиля можно найти в МЭК 61784-3;

b) интенсивность опасных отказов не выше, чем в предыдущем использовании.

Примечания

1 Руководство по использованию вероятностного подхода для определения полноты безопасности предварительно разработанного программного обеспечения, основанного на его эксплуатации, см. в приложении D МЭК 61508-7.

2 Для сбора доказательств для элементов, проверенных в эксплуатации, требуется эффективная система, сообщающая об отказах.

7.4.10.3 Если имеются различия между предыдущими условиями эксплуатации подсистемы и условиями, в которых будет эксплуатироваться Э/Э/ПЭ система, связанная с безопасностью, то такие различия должны быть идентифицированы и с помощью комбинации соответствующих аналитических методов и испытаний должно быть явно показано, что вероятность любой опасной систематической ошибки настолько низка, что требуемый уровень(и) полноты безопасности для функции(й) безопасности элемента достигается.

7.4.10.4 Обоснование безопасности проверенного в эксплуатации элемента должно быть документально оформлено, используя информацию, доступную в 7.4.10.2, о том, что элемент поддерживает требуемую функцию безопасности с необходимой систематической полнотой безопасности. Обоснование безопасности проверенного в эксплуатации элемента должно включать в себя:

a) анализ пригодности и тестирование элемента для предназначенного применения;

b) демонстрацию эквивалентности между намеченной эксплуатацией и предыдущим опытом эксплуатации, включая анализ влияния различий;

c) статистические данные.

7.4.10.5 При проверке выполнения или невыполнения требований 7.4.10.1—7 .4.10.4 с учетом охвата и степени детализации имеющейся информации (см. также подраздел 4.1 МЭК 61508-1) должны быть приняты во внимание следующие факторы:

a) сложность элемента;

b) стойкость к систематическим отказам, требуемая для элемента;

c) новизна проекта.

7.4.10.6 Должно быть убедительно доказано, что существующие функции элемента, для которых не было продемонстрировано, что они проверены в эксплуатации, не могут оказать негативного влияния на полноту безопасности выполняемых элементом функций.

Примечание — Данное требование может быть обеспечено путем гарантирования того, что функции физически или электрически отключены или что программное обеспечение, реализующее эти функции, исключено из эксплуатационной конфигурации, или другими видами аргументов и доказательств.

7.4.10.7 Любая будущая модификация проверенного в эксплуатации элемента должна соответствовать требованиям 7.8 и МЭК 61508-3.

7.4.11 Дополнительные требования к передаче данных

7.4.11.1 Если при реализации функции безопасности используются средства передачи данных, то должна быть оценена мера отказов (такая как коэффициент необнаруженных ошибок) коммуникационного процесса с учетом ошибок передачи, повторения, исключения, вставки, повторного упорядочивания, искажения, задержки и нелегального проникновения. Эта мера отказов должна быть учтена при оценке меры отказов функции безопасности из-за случайных отказов (см. 7.4.5).

Примечание — Термин «нелегальное проникновение» означает, что истинное содержание сообщения не идентифицировано правильно (например, сообщение от элемента, не связанного с безопасностью, идентифицировано как сообщение от элемента, связанного с безопасностью).

7.4.11.2 Методы и средства, гарантирующие необходимую меру отказов (такую как коэффициент необнаруженных ошибок) коммуникационного процесса (см. 7.4.11.1), должны быть реализованы в соответствии с требованиями настоящего стандарта и МЭК 61508-3. Допускается два возможных подхода:

- канал связи должен быть полностью разработан, реализован и для него проведена процедура подтверждения соответствия в соответствии со стандартами серий МЭК 61508 и МЭК 61784-3 или стандартами серии МЭК 62280. Это так называемый «белый канал» (см. рисунок 7a) или

- части канала связи не разработаны, или для них не проведена процедура подтверждения соответствия в соответствии со стандартами серии МЭК 61508. Это так называемый «черный канал» (см. рисунок 7b). В этом случае для того, чтобы гарантировать обработку отказа, коммуникационный процесс должен быть осуществлен с помощью Э/Э/ПЭ подсистем или элементов, связанных с безопасностью, которые взаимодействуют с каналом связи в соответствии с МЭК 61784-3 или стандартами серии МЭК 62280 (по мере необходимости).

Рисунок 7a — Белый канал

Рисунок 7b — Черный канал

Рисунок 7 — Архитектуры для передачи данных

7.5 Интеграция Э/Э/ПЭ системы

Примечание — Эта стадия показана как блок 10.4 на рисунке 2.

7.5.1 Цель

Целью настоящего подраздела является формирование требований к интеграции и испытанию Э/Э/ПЭ системы, связанной с безопасностью.

7.5.2 Требования

7.5.2.1 Э/Э/ПЭ система, связанная с безопасностью, должна быть интегрирована в соответствии с конкретным проектом Э/Э/ПЭ системы и испытана в соответствии с конкретными тестами интеграции для Э/Э/ПЭ системы (см. 7.4.2.11).

7.5.2.2 В соответствии с 7.4 на стадии интеграции всех модулей в Э/Э/ПЭ систему, связанную с безопасностью, должно быть проведено ее испытание. Такие испытания должны показать, что все модули взаимодействуют правильно, выполняют предназначенные для них функции и не выполняют не предназначенные для них функции.

Примечания

1. Испытание для всех входных комбинаций не проводится. Считается достаточным испытание для всех классов эквивалентности (см. пункт В.5.2 приложения В МЭК 61508-7). Статический анализ (см. пункт В.6.4 приложения В МЭК 61508-7), динамический анализ (см. пункт В.6.5 приложения В МЭК 61508-7) или анализ отказов (см. пункт В.6.6 приложения В МЭК 61508-7) могут сократить число испытаний до приемлемого уровня. Если разработка проводилась с использованием метода структурного проектирования (см. пункт В.3.2 приложения В МЭК 61508-7), или полуформальными методами (см. пункт В.2.3 приложения В МЭК 61508-7), то эти требования выполнить легче.

2 Если при разработке применены формальные методы (см. пункт В.2.2 приложения В МЭК 61508-7) либо формальные доказательства или программирование с проверкой условий (см. пункты С.5.12 и С.3.3 приложения С МЭК 61508-7), то объем таких испытаний может быть существенно сокращен.

3 Также могут быть использованы методы статистического тестирования (см. пункт В.5.3 приложения В МЭК 61508-7).

7.5.2.3 Интеграция программного обеспечения, связанного с безопасностью, в Э/Э/ПЭ систему, связанную с безопасностью, должна осуществляться в соответствии с требованиями подраздела 7.5 МЭК 61508-3.

7.5.2.4 Для испытания интеграции Э/Э/ПЭ систем, связанных с безопасностью, должна быть разработана соответствующая документация, устанавливающая результаты испытаний и определяющая, достигнуты ли цели и критерии, определенные на этапах проектирования и создания систем. В случае отказа причины и способы его устранения должны быть документально оформлены.

7.5.2.5 В период интеграции и испытаний любые модификации или изменения Э/Э/ПЭ системы, связанной с безопасностью, должны стать предметом анализа, при котором следует идентифицировать все подсистемы и элементы, на которые влияют эти модификации или изменения, и все необходимые действия по повторному подтверждению выполнения требований.

7.5.2.6 При испытаниях интеграции Э/Э/ПЭ системы должны быть документально оформлены:

a) используемая версия спецификации испытаний;

b) критерии принятия испытаний интеграции;

c) версия испытуемой Э/Э/ПЭ системы, связанной с безопасностью;

d) используемые средства испытаний и оборудование с датой поверки;

e) результаты каждого испытания;

f) любое несоответствие между ожидаемыми и фактическими результатами;

g) проведенный анализ и принятое решение о продолжении испытаний или выпуске запроса на изменение (при наличии несоответствия).

7.5.2.7 Для предотвращения ошибок во время интеграции Э/Э/ПЭ системы должна быть использована необходимая группа методов и средств в соответствии с таблицей В.3 приложения В.

7.6 Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы

Примечание — Эта стадия показана как блок 10.5 на рисунке 2.

7.6.1 Цель

Целью настоящего подраздела является разработка процедур, гарантирующих требуемую функциональную безопасность Э/Э/ПЭ системы, связанной с безопасностью, во время эксплуатации и технического обслуживания.

7.6.2 Требования

7.6.2.1 Должны быть предусмотрены следующие действия и процедуры по эксплуатации и техническому обслуживанию Э/Э/ПЭ системы:

a) обычные действия, которые должны быть выполнены для поддержания «спроектированной» функциональной безопасности Э/Э/ПЭ системы, связанной с безопасностью, включая обычную замену компонентов с предварительно заданными сроками жизни, например, вентиляторов, батарей и т. п.;

b) действия и ограничения, необходимые для предотвращения опасных отказов или уменьшения последствий опасных событий (например, во время установки, пуска в действие, обычного режима эксплуатации, типовых испытаний, обозримых неисправностей, отказов или ошибок, отключений);

c) оформление документации (которая должна поддерживаться) по отказам системы и частотам запросов Э/Э/ПЭ системы, связанной с безопасностью;

d) оформление документации (которая должна поддерживаться), хранящей результаты аудитов и испытаний Э/Э/ПЭ системы, связанной с безопасностью;

e) проведение процедур технического обслуживания, которым необходимо следовать в случае, если происходят отказы и ошибки в Э/Э/ПЭ системе, связанной с безопасностью, в том числе:

- диагностики отказов и восстановления (ремонта),
- повторного подтверждения соответствия,
- поддержания отчетности,
- повторного подтверждения соответствия, если компоненты оригинального оборудования больше не доступны или были заменены новыми версиями;

f) проведение процедур по поддержанию параметров отчетности, которые должны быть определены, в частности процедуры отчетности:

- по отказам,
- по анализу отказов;

g) применение инструментов, необходимых для технического обслуживания и повторного подтверждения соответствия, и выполнение процедур для поддержания инструментов и оборудования.

Примечания

1 По соображениям безопасности и экономичности может оказаться выгодным объединять процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы с полными процедурами эксплуатации и технического обслуживания управляемого оборудования.

2 В процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы должны быть включены процедуры модификации программного обеспечения (см. подраздел 7.8 МЭК 61508-3).

7.6.2.2 Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы, связанной с безопасностью, должны непрерывно совершенствоваться с учетом как результатов аудитов функциональной безопасности, так и результатов испытаний Э/Э/ПЭ системы, связанной с безопасностью.

7.6.2.3 Обычные действия по техническому обслуживанию, необходимые для поддержания требуемой (в соответствии с проектом) функциональной безопасности Э/Э/ПЭ системы, связанной с безопасностью, должны быть заданы на основе систематического подхода. Этот подход должен определять необнаруженные отказы всех элементов, связанных с безопасностью (от датчиков до исполнительных элементов), которые могли бы вызвать снижение достигнутой полноты безопасности. Подходящие методы этого подхода включают в себя:

- экспертизу деревьев отказов;
- анализ видов и последствий отказов.

Примечания

1 Рассмотрение человеческого фактора является ключевым моментом в определении требуемых действий и соответствующих интерфейсов с Э/Э/ПЭ системой, связанной с безопасностью.

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

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

- целевую меру отказов, связанных с уровнем полноты безопасности;
- архитектуру;
- охват диагностики диагностическими тестами и
- ожидаемую частоту запросов.

4 Частота контрольных проверок и интервал диагностических проверок, вероятно, должны иметь решающее влияние на достижение полноты безопасности аппаратных средств. Одна из основных причин проведения анализа надежности аппаратных средств (см. 7.4.5.2) состоит в гарантии соответствия частоты проведения этих двух типов испытаний целевой полноте безопасности аппаратных средств.

5 Следует придерживаться требований к техническому обслуживанию изготовителя и не ориентироваться только на надежность методов центра обслуживания, пока они не будут полностью обоснованы (например, анализом надежности, демонстрирующим, что целевые меры по отказу Э/Э/ПЭ системы, связанной с безопасностью, удовлетворены).

7.6.2.4 Процедуры эксплуатации и технической поддержки Э/Э/ПЭ системы должны быть оценены на возможность воздействия, которое они могут оказать на управляемое оборудование.

7.6.2.5 Для предотвращения отказов и ошибок во время процедур эксплуатации и технического обслуживания Э/Э/ПЭ системы используют группу средств и методов в соответствии с таблицей В.4 приложения В.

7.7 Подтверждение соответствия безопасности Э/Э/ПЭ системы

Примечание — Эта стадия показана как блок 10.6 на рисунке 2.

7.7.1 Цель

Целью настоящего подраздела является подтверждение соответствия того, что заданная Э/Э/ПЭ система, связанная с безопасностью, полностью соответствует требованиям безопасности системы в терминах требований к функциям безопасности и полноте безопасности (см. 7.2 настоящего стандарта и подраздел 7.10 МЭК 61508-1).

7.7.2 Требования

7.7.2.1 Подтверждение соответствия безопасности Э/Э/ПЭ системы должно проводиться в соответствии с подготовленным планом (см. также МЭК 61508-3, подраздел 7.7).

Примечания

1 Стадия подтверждения соответствия безопасности Э/Э/ПЭ системы на схеме жизненного цикла Э/Э/ПЭ системы безопасности, предшествует стадии установки, но в некоторых случаях не может быть выполнена до окончания установки (например, если разработка прикладного программного обеспечения еще не завершена до окончания установки).

2 Подтверждение соответствия программируемой электроники системы, связанной с безопасностью, включает в себя подтверждение соответствия аппаратных средств и программного обеспечения. Требования к подтверждению соответствия программного обеспечения содержатся в МЭК 61508-3.

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

7.7.2.3 Для адекватной реализации каждой функции безопасности, определенной в требованиях к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1), требований проектирования Э/Э/ПЭ системы (см. 7.2) и всех процедур эксплуатации и технического обслуживания Э/Э/ПЭ системы должно быть выполнено подтверждение соответствия тестированием и/или анализом. Если адекватную независимость или разделение между отдельными элементами или подсистемами нельзя показать аналитически, то должны быть испытаны связанные сочетания функционального поведения.

Примечание — Поскольку число необходимых тестовых комбинаций может быть очень большим, то может требоваться переструктурирование системы.

7.7.2.4 Должна быть подготовлена необходимая документация по проведению испытаний на подтверждение соответствия безопасности Э/Э/ПЭ системы, в которой для каждой функции безопасности должны быть указаны:

a) версия используемого плана проведения подтверждения соответствия безопасности Э/Э/ПЭ системы;

b) функция безопасности, подвергаемая испытаниям (или анализу), вместе с конкретной ссылкой на указанные в документации требования к планированию проведения подтверждения соответствия безопасности Э/Э/ПЭ системы;

c) испытательные средства и оборудование, вместе с данными об их калибровке;

d) результаты каждого испытания;

e) несоответствие между ожидаемыми и фактическими результатами.

Примечание — Для каждой функции безопасности отдельная документация не требуется, но каждая функция безопасности и каждое отклонение от функции безопасности должны быть отражены в информации по перечислениям a)—e).

7.7.2.5 Если фактические результаты отличаются от ожидаемых результатов более, чем это установлено допусками, результаты испытаний на подтверждение соответствия безопасности Э/Э/ПЭ системы должны быть документально оформлены, включая:

a) описание проведенного анализа и

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

7.7.2.6 Поставщик или производитель должны сделать доступными результаты испытаний подтверждения соответствия безопасности Э/Э/ПЭ системы производителю управляемого оборудования и систем управления управляемого оборудования, с тем чтобы позволить им обеспечить выполнение требований подтверждения соответствия всей системы безопасности в соответствии с МЭК 61508-1.

7.7.2.7 Для предотвращения отказов при проведении подтверждения соответствия безопасности Э/Э/ПЭ системы используют группу методов и средств в соответствии с таблицей В.5 приложения В.

7.8 Модификация Э/Э/ПЭ системы

7.8.1 Цель

Целью требований настоящего подраздела является гарантирование требуемой полноты безопасности, ее достижение и поддержание после изменения, расширения или адаптации Э/Э/ПЭ системы, связанной с безопасностью.

7.8.2 Требования

7.8.2.1 Должна быть изготовлена и обеспечена поддержка документации по каждому действию по модификации Э/Э/ПЭ системы. Документация должна включать в себя:

a) детальную спецификацию модификации или изменений;

b) анализ влияния действий по модификации на всю систему, включая аппаратные средства и программное обеспечение (см. МЭК 61508-3), взаимодействие с человеком, окружение и возможные взаимодействия;

c) утвержденные изменения;

d) порядок проведения изменений;

e) испытания подсистем и элементов, включая данные повторного подтверждения соответствия;

f) предысторию управления конфигурацией Э/Э/ПЭ системы;

g) отклонения от нормальных действий и условий;

h) необходимые изменения системных процедур;

i) необходимые изменения документации.

7.8.2.2 Производители или поставщики систем, требующие подтверждения соответствия всем (или части) требованиям настоящего стандарта, должны осуществлять техническую поддержку системы при инициировании изменений в результате обнаруживаемых в аппаратных средствах или программном обеспечении дефектов и сообщать пользователям о необходимости модификации в случае обнаружения дефекта, затрагивающего безопасность.

7.8.2.3 Модификация должна проводиться, по крайней мере, с тем же уровнем компетентности специалистов, автоматизированных средств (см. МЭК 61508-3, подпункт 7.4.4.2), планирования и управления, что и при разработке Э/Э/ПЭ систем, связанных с безопасностью.

7.8.2.4 После модификации Э/Э/ПЭ системы, связанные с безопасностью, должны быть повторно проверены и должно быть повторно подтверждено их соответствие.

Примечание — См. также подпункт 7.16.2.6 МЭК 61508-1.

7.9 Верификация Э/Э/ПЭ системы

7.9.1 Цель

Цель требований настоящего подраздела состоит в проверке и оценке выходных результатов конкретной стадии для гарантирования их правильности и соответствия требованиям разделов стандартов, предусмотренных для этой стадии.

Примечание — Для удобства все требования к действиям по верификации объединены в 7.9, но фактически они выполняются на всех стадиях жизненного цикла Э/Э/ПЭ системы безопасности.

7.9.2 Требования

7.9.2.1 Верификация Э/Э/ПЭ систем, связанных с безопасностью, должна быть запланирована одновременно с их разработкой (см. 7.4) для каждой стадии жизненного цикла Э/Э/ПЭ системы безопасности и документально оформлена.

7.9.2.2 Планирование верификации Э/Э/ПЭ системы должно относиться ко всем критериям, методам и средствам, используемым для верификации на проверяемой стадии.

7.9.2.3 Планирование верификации Э/Э/ПЭ системы должно определять на каждой стадии выполнение обязательных действий для гарантии правильности выходных результатов и соответствия требованиям разделов стандартов, предусмотренных для этой стадии.

7.9.2.4 Планирование верификации Э/Э/ПЭ системы должно предусматривать:

a) выбор стратегии и методов верификации;

b) выбор и использование испытательного оборудования;

c) выбор и документальное оформление действий в ходе верификации;

d) оценку результатов верификации, полученных непосредственно из верифицирующего оборудования и испытаний.

7.9.2.5 На каждой стадии проектирования и разработки должно быть показано, что требования функциональной безопасности и полноты безопасности выполняются.

7.9.2.6 Результат каждого действия по верификации должен быть документально оформлен с указанием, прошли ли Э/Э/ПЭ системы, связанные с безопасностью, проверку, или причины отказов. Должны быть описаны устройства, не соответствующие одному или более из следующих требований:

a) жизненный цикл Э/Э/ПЭ системы безопасности (см. 7.2);

b) стандарты проектирования (см. 7.4);

c) управление функциональной безопасностью (см. раздел 6).

7.9.2.7 Для верификации требований проектирования Э/Э/ПЭ системы, после того как были установлены требования проектирования Э/Э/ПЭ системы (см. 7.2) и перед началом следующей стадии (проектирования и разработки), проверка должна:

a) определить, адекватно ли требования проектирования Э/Э/ПЭ системы удовлетворяют спецификациям требований к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1): по безопасности, функциональным возможностям и другим заданным при планировании безопасности, и

b) проверить, существуют ли несоответствия между:

- требованиями к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1),
- требованиями проектирования Э/Э/ПЭ системы (см. 7.2),
- тестами Э/Э/ПЭ системы (см. 7.4) и
- документацией пользователя вместе с остальной документацией на систему.

7.9.2.8 Для верификации стадии проектирования и разработки Э/Э/ПЭ системы после завершения проектирования и разработки Э/Э/ПЭ системы (см. 7.4) и до начала следующей стадии (интеграции) проверка должна:

a) определить, адекватны ли тесты Э/Э/ПЭ системы для стадии проектирования и разработки Э/Э/ПЭ системы;

b) определить согласованность и полноту (до уровня модулей включительно) стадии проектирования и разработки Э/Э/ПЭ системы (см. 7.4) в соответствии с требованиями к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1) и

c) проверить, существуют ли несоответствия между:

- требованиями к Э/Э/ПЭ системе безопасности (см. подраздел 7.10 МЭК 61508-1),
- требованиями проектирования Э/Э/ПЭ системы (см. 7.2),
- результатами проектирования и разработки Э/Э/ПЭ системы (см. 7.4) и
- тестами Э/Э/ПЭ системы (см. 7.4).

Примечания

1 Методы подтверждения соответствия системе безопасности, анализ отказов и тестирование, рекомендуемые в таблице В.5 (приложение В), также могут быть использованы для верификации.

2 При верификации достижения необходимого охвата диагностикой в таблице А.1 (приложение А) следует учесть отказы и ошибки, которые должны быть обнаружены.

7.9.2.9 Для верификации интеграции Э/Э/ПЭ системы должна быть проверена интеграция Э/Э/ПЭ системы, связанной с безопасностью, с тем чтобы установить выполнение требований 7.5.

7.9.2.10 Проверки и их результаты должны быть документально оформлены.

8 Оценка функциональной безопасности

Требования к оценке функциональной безопасности — в соответствии с разделом 8 МЭК 61508-1.

Приложение А
(обязательное)

Методы и средства для Э/Э/ПЭ систем, связанных с безопасностью. Управление отказами в процессе эксплуатации

А.1 Общие положения

Настоящее приложение должно использоваться совместно с 7.4 и ограничивает максимальный охват диагностикой, что может потребоваться для выбора методов и средств управления отказами в процессе эксплуатации. Для каждого уровня полноты безопасности в настоящем приложении рекомендованы методы и средства управления случайными, систематическими, эксплуатационными отказами и отказами, относящимися к окружающей среде. Более подробную информацию об архитектурах и методах см. в МЭК 61508-6 (приложение В) и МЭК 61508-7 (приложение А).

Перечислить каждую индивидуальную физическую причину отказов в сложных аппаратных средствах не представляется возможным по следующим основным причинам:

- причинно-следственные отношения между ошибками и отказами часто трудно определить;
- при использовании сложных аппаратных средств и программного обеспечения характер отказов изменяется в диапазоне от случайных до систематических.

Категории отказов в Э/Э/ПЭ системах, связанных с безопасностью, могут быть установлены в зависимости от времени их возникновения как:

- отказы из-за ошибок, возникающих до установки или в период установки системы (например, вследствие ошибок программного обеспечения, включая спецификацию и ошибки программы; вследствие ошибок в аппаратных средствах, включая производственные ошибки и неправильный выбор элементов);
- отказы из-за технических ошибок или ошибок человека, возникающих после установки системы (например, случайные отказы аппаратных средств или отказы, вызванные неправильным использованием).

Для предотвращения таких отказов или управления ими (если они происходят) обычно требуется применение большого числа средств. Структура требований, приведенных в приложениях А и В, является следствием разделения средств на средства, используемые для предотвращения отказов на различных стадиях жизненного цикла Э/Э/ПЭ системы безопасности (см. приложение В), и средства, используемые для управления отказами в период эксплуатации (см. настоящее приложение). Средства по управлению отказами — это собственные встроенные составляющие Э/Э/ПЭ систем, связанных с безопасностью.

Охват диагностикой и долю безопасных отказов определяют в соответствии с таблицей А.1 и процедурами, описанными в приложении С. Таблицы А.2—А.14 поддерживают требования таблицы А.1 методами и средствами диагностического тестирования и требованиями максимальных уровней охвата диагностикой, которые могут быть достигнуты при их использовании. Требования, приведенные в этих таблицах, не отменяют требований, приведенных в приложении С. Требования таблиц А.2—А.14 не являются исчерпывающими. Могут быть использованы другие методы и средства диагностического тестирования, если приведены свидетельства о поддержке ими требующегося охвата диагностикой. Если требуется высокий уровень охвата диагностикой, то в каждой из таблиц А.2—А.14 должно быть выбрано и применено, как минимум, одно средство с высоким уровнем охвата диагностикой.

Таблицы А.15—А.17 содержат рекомендуемые меры и средства управления систематическими отказами для каждого уровня полноты безопасности. Таблица А.15 относится к общим мерам, рекомендуемым для управления систематическими отказами (см. также МЭК 61508-3). Таблица А.16 относится к рекомендуемым мерам по управлению отказами из-за влияния окружающей среды. Таблица А.17 относится к рекомендуемым мерам по управлению ошибками при эксплуатации. Большинство этих мер по управлению отказами может быть разделено по эффективности их применения в соответствии с таблицей А.18.

Методы и средства, приведенные в этих таблицах, описаны в приложении А МЭК 61508-7. Методы и средства, требуемые для каждого уровня полноты безопасности программного обеспечения, приведены в МЭК 61508-3. Руководящие указания по определению архитектуры Э/Э/ПЭ системы, связанной с безопасностью, приведены в МЭК 61508-6.

Руководящие указания, представленные в настоящем приложении, сами по себе не гарантируют требуемой полноты безопасности. Важно учитывать:

- последовательность выбранных методов, средств и то, как они будут дополнять друг друга;
- какие методы и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой Э/Э/ПЭ системы, связанной с безопасностью.

А.2 Полнота безопасности аппаратных средств

Требования к ошибкам или отказам, которые должны быть обнаружены с помощью методов и средств управления отказами аппаратных средств для достижения соответствующего уровня охвата диагностикой, представлены в таблице А.1 (см. также приложение С). Требования, представленные в таблицах А.2—А.14, поддерживают требования, приведенные в таблице А.1, методами и средствами для диагностического тестирования и требовани-

ями максимальных уровней охвата диагностикой, которые могут быть достигнуты при их использовании. Данные диагностические тесты могут проводиться непрерывно или периодически. Таблицы А.2—А.14 не заменяют требований подраздела 7.4. Методы и средства, представленные в таблицах А.2—А.14, не являются исчерпывающими. Могут быть использованы другие методы и средства, если представлены свидетельства, что они поддерживают необходимый охват диагностикой.

Примечания

1 Краткий обзор методов и средств, упомянутых в таблицах А.2—А.14, приведен в МЭК 61508-7 (приложение А). Во вторых колонках таблиц А.2—А.14 приведены соответствующие ссылки.

2 Указания «низкий», «средний» и «высокий» охват диагностикой количественно определены как 60 %, 90 % и 99 % соответственно.

Таблица А.1 — Ошибки и отказы, которые подлежат рассмотрению при количественной оценке случайных отказов аппаратных средств или учитываются при определении доли безопасных отказов

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Электромеханические устройства	А.2	Не включение или не отключение. Приваренные контакты	Не включение или не отключение. Отдельные приваренные контакты	Не включение или не отключение. Отдельные приваренные контакты. Отсутствует принудительное управление контактами (для реле этот отказ не предполагается, если они изготовлены и испытаны в соответствии с EN 50205). Отсутствует принудительное включение (для положений переключателей этот отказ не рассматривается, если они изготовлены и испытаны в соответствии с МЭК 60947-5-1 или эквивалентными нормами)
Дискретные аппаратные средства: - цифровой вх./вых. - аналоговый вх./вых. - источник питания	А.3, А.7, А.9	 Константный отказ (см. примечание 1) Константный отказ Константный отказ	 Неисправности при постоянном токе (см. примечание 2) Отказы типа отклонений и колебаний при постоянном токе Отказы типа отклонений и колебаний при постоянном токе	 Отказы типа отклонений и колебаний при постоянном токе Отказы типа отклонений и колебаний при постоянном токе Отказы типа отклонений и колебаний при постоянном токе

Продолжение таблицы А.1

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Шина: - общая шина	A.3 A.7	Константный отказ адресов	Временная потеря работоспособности	Временная потеря работоспособности
- диспетчер памяти	A.8	Константный отказ данных или адресов	Неверное декодирование адреса. Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти (см. примечания 3 и 4).	Неверное декодирование адреса. Изменение адресов, вызванное кратковременными ошибками в регистрах диспетчера памяти
- прямой доступ к памяти		Нет доступа или непрерывный доступ	Неисправности данных и адресов при постоянном токе Изменение информации, вызванное кратковременными ошибками в регистрах памяти прямого доступа. Неверное время доступа	Все отказы, влияющие на данные в памяти Неверное время доступа
- управление доступом к шине (см. примечание 5)		Константный отказ сигналов управления доступом к шине	Отсутствует или непрерывный доступ к шине	Отсутствует или непрерывный, или неправильный доступ к шине
Процессор: - регистр, внутреннее ОЗУ	A.4, A.10	Константный отказ данных или адресов	Неисправности данных и адресов при постоянном токе. Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе. Перекрестные помехи в ячейках памяти. Изменение информации, вызванное исправимыми ошибками. Отсутствует, неверная или множественная адресация
- устройство кодирования и выполнения, включая регистр признаков		Неверное кодирование или невыполнение	Неверное кодирование или неверное выполнение	Отсутствует определение предполагаемого отказ.
- устройство вычисления адреса		Константный отказ	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками	Отсутствует определение предполагаемого отказа
- счетчик команд, указатель стека		Константный отказ	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками	Неисправности при постоянном токе. Изменение адресов, вызванное исправимыми ошибками

Продолжение таблицы А.1

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Устройство обработки прерываний: устройство прерывания схема возврата	А.4	Отсутствуют или непрерывные прерывания (см. примечание 6) Константный отказ. Отдельные компоненты не инициализируют состояние возврата	Отсутствуют или непрерывные прерывания. Пересечение прерываний Неисправности при постоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата	Отсутствуют или непрерывные прерывания. Пересечение прерываний. Неисправности при постоянном токе. Отказы типа отклонений и колебаний. Отдельные компоненты не инициализируют состояние возврата
Постоянная память	А.5	Константный отказ данных или адресов	Неисправности данных и адресов при постоянном токе	Все отказы, влияющие на данные в памяти
Память с произвольным доступом	А.6	Константный отказ данных или адресов	Неисправности данных и адресов при постоянном токе. Изменение информации, вызванное исправимыми ошибками	Неисправности данных и адресов при постоянном токе. Перекрестные помехи в ячейках памяти. Изменение информации, вызванное исправимыми ошибками. Отсутствует, неверная или множественная адресация
Устройство синхронизации (кварцевое)	А.11	Нижняя или верхняя гармоника	Неверная частота. Неустойчивость периода синхронизции	Неверная частота. Неустойчивость периода синхронизции
Устройство связи и запоминающее устройство большой емкости	А.12	Неверные данные или адреса. Отсутствует передача данных	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверна последовательность передачи	Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверна последовательность передачи
Датчики	А.13	Константный отказ	Неисправности при постоянном токе. Дрейф и колебания	Неисправности при постоянном токе. Дрейф и колебания
Исполнительные элементы	А.14	Константный отказ	Неисправности при постоянном токе. Дрейф и колебания	Неисправности при постоянном токе. Дрейф и колебания

Окончание таблицы А.1

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)

Примечания

1 «Непрерывный» — это вид отказа, который может быть описан всеми нулями («0») или единицами («1») на выводах элемента.

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

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

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

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

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

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

7 Для СИС данные настоящей таблицы и таблиц А.2—А.18 применяются в соответствующих случаях.

Таблица А.2 — Электрические компоненты

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывными запросами)	Зависит от охвата диагностикой обнаружения отказов
Мониторинг контактов реле	А.1.2	Высокий	Необходимо учесть скорость переключения реле при количественной оценке случайных отказов
Компаратор	А.1.3	Высокий	Высокий, если режимы отказов в основном безопасно диагностируются
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования

Примечания

1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.

2 Для определения охвата диагностикой применяют требования приложения С.

3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.3 — Электронные компоненты

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Компаратор	А.1.3	Высокий	Высокий, если режимы отказов в основном безопасно диагностируются
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования
Тестирование избыточным оборудованием	А.2.1	Средний	Зависит от охвата диагностикой обнаружения отказов
Принципы динамического управления	А.2.2	Средний	Зависит от охвата диагностикой обнаружения отказов
Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Высокий	Зависит от охвата диагностикой обнаружения отказов
Избыточный контроль	А.2.5	Высокий	Зависит от степени избыточности и текущего контроля
Электрические/электронные средства с автоматической проверкой	А.2.6	Высокий	Зависит от охвата диагностикой тестов
Текущий контроль аналоговых сигналов	А.2.7	Низкий	

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.
2 Для определения охвата диагностикой применяют требования приложения С.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.4 — Устройства обработки

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Компаратор	А.1.3	Высокий	Зависит от качества сравнения
Схема голосования по мажоритарному принципу	А.1.4	Высокий	Зависит от качества устройства голосования
Программное самотестирование: предельное количество комбинаций (одноканальное)	А.3.1	Низкий	—
Программное самотестирование: блуждающий бит (одноканальное)	А.3.2	Средний	—
Самотестирование, обеспечиваемое оборудованием (одноканальное)	А.3.3	Средний	—
Запрограммированная обработка (одноканальное)	А.3.4	Высокий	—

Окончание таблицы А.4

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Программное обнаружение несовпадений	А.3.5	Высокий	Зависит от качества сравнения

Примечания

1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.

2 Для определения охвата диагностикой применяют требования приложения С.

3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

4 Поскольку много отказов процессора приводят к изменению потока управления, то могут быть также рассмотрены диагностические методы и средства, перечисленные в таблице А.10. Эти диагностические методы и средства охватывают только поток управления, но не поток данных.

Таблица А.5 — Постоянная память

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Защита слов многобитовой избыточностью	А.4.1	Средний	Эффективность многобитовой избыточности защиты слов зависит от включения адреса слова в многоразрядную избыточность. Многобитовая избыточность защиты слов использует соответствующее средство для обнаружения многобитовых отказов по общей причине, например, множественная адресация (многократный выбор строки), проблемы источника питания (например, дефекты генератора подкачки заряда), перестановка при формировании строк и столбцов (это позволяет скрыть ошибки формирования) и т. д.
Модифицируемая контрольная сумма	А.4.2	Низкий	—
Сигнатура из одного слова (8 бит)	А.4.3	Средний	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации
Сигнатура из двух слов (16 бит)	А.4.4	Высокий	Эффективность сигнатуры зависит от ее длины по отношению к длине блока защищаемой информации
Дублирование блока	А.4.5	Высокий	—

Примечания

1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.

2 Для определения охвата диагностикой применяют требования приложения С.

3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.6 — Память с произвольным доступом (ОЗУ)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Тест ОЗУ «шахматная доска» или «марш»	А.5.1	Низкий	—
Тест ОЗУ «блуждающая траектория»	А.5.2	Средний	—

Окончание таблицы А.6

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Тест ОЗУ «GALPAT» — попарная запись — считывание с помощью бегущего кода или «Прозрачный GALPAT»	А.5.3	Высокий	—
Тест ОЗУ «Абраам»	А.5.4	Высокий	—
Бит четности для ОЗУ	А.5.5	Низкий	—
Контроль ОЗУ с помощью модифицированного кода Хэмминга или обнаружение сбоев данных с помощью кодов обнаружения и коррекции ошибок (EDC)	А.5.6	Высокий	Эффективность контроля ОЗУ с помощью модифицированного кода Хэмминга или обнаружение сбоев данных с помощью кодов обнаружения и коррекции ошибок (EDC) зависит от включения адреса в код Хемминга и основана на выполнении соответствующих средств для обнаружения многобитовых отказов по общей причине, например, множественная адресация (многократный выбор строки), перестановка при формировании строк и столбцов (это позволяет скрыть ошибки формирования) и т. д.
Дублирование со сравнением ОЗУ с аппаратными или программными средствами и тестирование чтением/записью	А.5.7	Высокий	—

Примечания

1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.

2 Для определения охвата диагностикой применяют требования приложения С.

3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

4 Для ОЗУ, в котором запись/считывание происходят не часто (например, во время конфигурирования), эффективны методы по МЭК 61508-7, пункты А.4.1—А.4.4 приложения А, если они осуществляются после каждой операции записи/считывания.

Таблица А.7 — Устройства ввода/вывода и интерфейс (внешний обмен)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Тестирующая комбинация	А.6.1	Высокий	—
Кодовая защита	А.6.2	Высокий	—
Многоканальное параллельное выходное устройство	А.6.3	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Средство контроля выходов	А.6.4	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	А.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала

Окончание таблицы А.7

Диагностический метод/средство	См МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Передача неэквивалентных сигналов	А.11.4	Высокий	Например, передача инвертированных сигналов
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Таблица А.8 — Информационные каналы (внутренний обмен)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Однобитовая аппаратная избыточность	А.7.1	Низкий	Данную эффективность для различных типов сетевых коммутаторов каналов передачи данных можно предположить, только если адресные и управляющие шины обеспечены средствами безопасности
Многобитовая аппаратная избыточность	А.7.2	Средний	Данную эффективность для различных типов сетевых коммутаторов каналов передачи данных можно предположить, только если адресные и управляющие шины обеспечены средствами безопасности
Полная аппаратная избыточность	А.7.3	Высокий	—
Анализ с использованием тестирующих комбинаций	А.7.4	Высокий	—
Избыточность при передаче	А.7.5	Высокий	Эффективно только для неустойчивых сбоев
Информационная избыточность	А.7.6	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Таблица А.9 — Источник питания

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Защита от броска напряжения с защитой от короткого замыкания или отключением/подключением ко второму источнику питания	А.8.1	Низкий	—
Контроль напряжения (вторичный) с безопасным отключением/подключением ко второму источнику питания	А.8.2	Высокий	—
Отключение системы безопасности при снижении питания или подключение ко второму источнику питания	А.8.3	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Таблица А.10 — Последовательность выполнения программ (контрольный датчик времени)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Контрольный датчик времени с отдельной временной базой без временного окна	А.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	А.9.2	Средний	—
Логический контроль последовательности выполнения программ	А.9.3	Средний	Зависит от качества контроля
Комбинация временного и логического контроля последовательности выполнения программ	А.9.4	Высокий	—
Первоначальный тест при включении	А.9.5	Средний	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.
2 Для определения охвата диагностикой применяют требования приложения С.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.11 — Генератор тактовой частоты

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Контрольный датчик времени с отдельной временной базой без временного окна	А.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	А.9.2	Средний	Зависит от временных ограничений для временного окна
Логический контроль последовательности выполнения программ	А.9.3	Средний	Эффективно только при отказе часов, если внешние временные события влияют на процесс выполнения программы
Комбинация временного и логического контроля последовательности выполнения программ	А.9.4	Высокий	—
Первоначальный тест при включении	А.9.5	Средний	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.
2 Для определения охвата диагностикой применяют требования приложения С.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

Таблица А.12 — Устройство связи и запоминающее устройство большой емкости

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обмен информацией между Э/Э/ПЭ системой, связанной с безопасностью, и процессом	А.6	См. таблицу А.7	См. устройства вх./вых. и интерфейс
Обмен информацией между Э/Э/ПЭ системами, связанными с безопасностью	А.7	См. таблицу А.8	См. каналы/шины передачи данных
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Таблица А.13 — Датчики

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Текущий контроль аналоговых сигналов	А.2.7	Низкий	—
Тестирующая комбинация	А.6.1	Высокий	—
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	А.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Эталонный датчик	А.12.1	Высокий	Зависит от охвата диагностикой обнаружения отказов
Положительно—управляемый переключатель	А.12.2	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Таблица А.14 — Исполнительные элементы (приводы)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечание
Обнаружение отказов путем мониторинга в режиме онлайн	А.1.1	Низкий (режим с низкой частотой запросов). Средний (режим с высокой частотой запросов или с непрерывным запросом)	Зависит от охвата диагностикой обнаружения отказов
Мониторинг контактов реле	А.1.2	Высокий	Необходимо учесть скорость переключения реле при количественной оценке случайных отказов

Окончание таблицы А.14

Тестирующая комбинация	А.6.1	Высокий	—
Мониторинг	А.13.1	Высокий	Зависит от охвата диагностикой обнаружения отказов
Перекрестный контроль групповых приводов	А.13.2	Высокий	—

Примечания
1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С.
2 Для определения охвата диагностикой применяют требования приложения С.
3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.

А.3 Систематическая полнота безопасности

Таблицы А.15—А.17 содержат рекомендации для применения методов и средств с целью:
- управления отказами, связанными с проектированием аппаратных средств (см. таблицу А.15);
- управления отказами, вызванными внешними нагрузками или влияниями (см. таблицу А.16), и
- управления отказами на стадии эксплуатации (см. таблицу А.17).

Рекомендации, приведенные в таблицах А.15—А.17, сформированы для уровней полноты безопасности, с указанием, во-первых, уровня важности метода или средства и, во-вторых, эффективности его использования. Уровень важности метода или средства обозначают:

M — данные методы или средства требуются обязательно (О) для данного уровня полноты безопасности;

HR — методы или средства крайне рекомендованы (КР) для данного уровня полноты безопасности. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их неиспользования;

R — методы или средства рекомендованы (Р) для данного уровня полноты безопасности;

— — методы или средства, не имеющие рекомендаций за и против применения;

NR — методы или средства явно не рекомендованы для данного уровня полноты безопасности. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемую эффективность методов и средств обозначают:
- «низкая (Low)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;
- «средняя (Medium)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;
- «высокая (High)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

Руководство по уровням эффективности для большинства методов и средств приведено в таблице А.18.

Если мера не является обязательной, то она может быть заменена другими мерами (отдельно или в комбинации с другими).

Все приведенные в таблицах А.15—А.17 методы и средства являются встроенными компонентами Э/Э/ПЭ систем, связанных с безопасностью, которые могут помочь управлять отказами в неавтономном режиме. Процедурные и организационные методы и средства необходимы на протяжении всего жизненного цикла Э/Э/ПЭ системы безопасности для предотвращения введения в них ошибок. Методы оценки соответствия для проверки действия Э/Э/ПЭ систем, связанных с безопасностью, по противостоянию ожидаемым внешним влияниям необходимы для демонстрации того, что встроенные особенности соответствуют заявленным требованиям (см. приложение В).

Информация по отказам по общей причине приведена в МЭК 61508-6 (приложение D).

Примечание — Большинство методов, приведенных в таблицах А.15—А.17, может быть использовано с разной эффективностью в соответствии с таблицей А.18, в которой приведены описания их применения для обеспечения низкой и высокой эффективности. Усилия, требуемые для получения средней эффективности, находятся в пределах усилий, необходимых для получения низкой и высокой эффективности.

Таблица А.15 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, источниками которых являются этапы разработки аппаратных средств

Методы/средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1) Мониторинг последовательности выполнения программ	А.9	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
2) Обнаружение отказов путем мониторинга в режиме он-лайн (см. примечание 5)	А.1.1	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий

Окончание таблицы А.15

Методы/средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
3) Тестирование избыточными аппаратными средствами	А.2.1	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
4) Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
5) Кодовая защита	А.6.2	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
6) Разнообразие аппаратных средств	В.1.4	низкий	низкий	Р (R) средний	Р (R) высокий

Примечания

1 Требуется выполнение, по крайней мере, одного из методов/средств 2—6 или одного из методов, определенных в таблице А.3 МЭК 61508-3.

2 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем настоящей таблице.

3 Методы/средства могут быть использованы для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры для низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в приложениях А, В и С МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

5 Для Э/Э/ПЭ систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в неавтономном режиме, обычно является низкой или этот метод не применяется.

Таблица А.16 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, вызванными внешними нагрузками или влияниями

Методы/средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения и других явлений, таких как изменение частоты переменного тока электропитания, которое может привести к опасному отказу	А.8	О (М) низкий	О (М) средний	О (М) средний	О (М) высокий
2 Разделение линий электрического питания и линий передачи информации (см. примечание 5)	А.11.1	О (М)	О (М)	О (М)	О (М)
3 Повышение устойчивости к электромагнитным воздействиям	А.11.3	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
4 Средства против физического воздействия окружающей среды (например, температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	А.14	О (М) низкий	О (М) высокий	О (М) высокий	О (М) высокий
5 Мониторинг последовательности выполнения программ	А.9	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
6 Меры против повышения температуры	А.10	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
7 Пространственное разделение групповых линий	А.11.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
8 Принцип реактивного тока (нет необходимости в непрерывном контроле для достижения или поддержки безопасного состояния УО)	А.1.5	Р (R)	Р (R)	Р (R)	Р (R)

Окончание таблицы А.16

Методы/средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
9 Средства обнаружения обрывов и коротких замыканий в линиях передачи сигналов		P (R)	P (R)	P (R)	P (R)
10 Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание 6)	А.1.1	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
11 Тестирование избыточными аппаратными средствами	А.2.1	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
12 Кодовая защита	А.6.2	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
13 Передача неэквивалентных сигналов	А.11.4	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
14) Разнообразие аппаратных средств (см. примечание 7)	В.1.4	низкий	низкий	средний	P (R) высокий
15) Архитектура программного обеспечения	МЭК 61508-3, пункт 7.4.3	См. МЭК 61508-3, таблицы А.2 и С.2			

Примечания

1 Все методы с уровнем важности P (R) разделены на две группы: одна группа — методы 8 и 9, другая группа — методы 10—15. Методы в каждой из этих групп взаимозаменяемы. Но требуется выполнение по крайней мере одного из методов из первой группы и одного метода из второй группы.

2 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице А.15.

3 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в приложениях А и В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

5 Отделение линий электропитания от линий передачи информации не является необходимым, в случае если информация предается по оптоволокну, а также для низковольтных линий, спроектированных для питания элементов Э/Э/ПЭ системы и передачи информации к ним или от них.

6 Для Э/Э/ПЭ систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в режиме он-лайн, обычно является низкой или этот метод не применяется.

7 Разнообразие аппаратных средств не требуется, если путем подтверждения соответствия или большим опытом эксплуатации может быть продемонстрировано, что аппаратные средства в достаточной степени свободны от ошибок на стадии проектирования и в достаточной степени защищены от отказов по общей причине для достижения целевых мер отказов.

Таблица А.17 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами при эксплуатации

Методы/средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Защита от модификаций	B.4.8	O (M) низкий	O (M) средний	O (M) высокий	O (M) высокий
2 Обнаружение отказов путем мониторинга в режиме он-лайн (см. примечание 5)	A.1.1	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
3 Подтверждение ввода	B.4.9	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
4 Программирование с проверкой ошибок	C.3.3	См. таблицы A.2 и C.2 МЭК 61508-3			

Примечания

1 Требуется выполнение по крайней мере одного из методов 2—4.

2 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице А.15.

3 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.18, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в приложениях А, В и С МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

5 Для Э/Э/ПЭ систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например, для систем аварийного отключения), эффективность охвата диагностикой, осуществляемого путем обнаружения отказа с помощью мониторинга в режиме он-лайн, обычно является низкой или этот метод не применяется.

Таблица А.18 — Эффективность методов и средств управления систематическими отказами

Методы / средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Обнаружение отказов путем мониторинга в режиме онлайн (см. примечание)	A.1.1	Запускающие сигналы от управляемого оборудования и его системы управления используются для подтверждения надлежащего действия Э/Э/ПЭ систем, связанных с безопасностью (только характер изменения во времени и когда система не используется)	Э/Э/ПЭ системы, связанные с безопасностью, перезапускаются временны́ми и логическими сигналами от управляемого оборудования и его системы управления (временно́е окно для временно́й функции контрольного датчика времени)
Тестирование избыточными аппаратными средствами (см. примечание)	A.2.1	Дополнительные аппаратные средства проверяют сигналы запускающие Э/Э/ПЭ системы, связанные с безопасностью (только характер изменения во времени и если система не используется). Эти средства включают в себя вспомогательный исполнительный элемент	Дополнительные аппаратные средства повторно перезапускаются временны́ми и логическими сигналами Э/Э/ПЭ систем, связанных с безопасностью (временно́е окно для контрольного датчика времени); голосование между несколькими каналами
Стандартный тестовый порт доступа и архитектура граничного сканирования	A.2.3	Твердотельная логика проверяется с помощью граничных тестовых испытаний в период контрольных испытаний	Диагностический контроль твердотельной логики на соответствие спецификации функций безопасности Э/Э/ПЭ систем, связанных с безопасностью. Проверяют все функции для всех интегральных схем
Кодовая защита	A.6.2	Обнаружение ошибок с помощью временно́й избыточности передачи сигналов	Обнаружение ошибок с помощью временно́й и информационной избыточности передачи сигналов

Окончание таблицы А.18

Методы / средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения	А.8	Защита от перенапряжения с безопасным отключением или переключением ко второму блоку питания	Регулировка напряжения (повторная) с безопасным отключением или переключением ко второму блоку питания; или выключение питания с безопасным отключением или переключением ко второму блоку питания
Мониторинг последовательности выполнения программ	А.9	Временно́й или логический мониторинг последовательности выполнения программ	Временно́й и логический мониторинг последовательности выполнения программ с большим количеством контрольных точек в программе
Средства против повышения температуры	А.10	Температурный датчик, определяющий превышение температуры	Применение безопасного выключателя с использованием плавкого предохранителя, или измерение нескольких уровней превышения температуры с подачей аварийных сигналов, или применение принудительного воздушного охлаждения с индикацией состояния
Повышение устойчивости к электромагнитным воздействиям (см. примечание)	А.11.3	Помехозащищающий фильтр в источнике питания и на критических входах и выходах; экранирование (при необходимости)	Фильтр против электромагнитных воздействий, которые обычно не ожидаются; экранирование
Средства против физического воздействия окружающей среды	А.14	Общепринятая практика, соответствующая прикладному применению	Методы, упомянутые в стандартах для специфического применения
Разнообразие аппаратных средств	В.1.4	Два или более устройств, спроектированные по-разному, но выполняют одну и ту же функцию	Два или более устройств, выполняют различные функции
Защита от модификаций	В.4.8	Модификация требует использования специальных средств	Модификация требует использования блокирующего ключа или специального инструмента с паролем
Подтверждение ввода	В.4.9	Отображение входных действий для оператора	Проверка по строгим правилам входных данных, вводимых оператором, с отклонением неправильных входных данных
Примечание — В случаях, когда методы и средства по А.1.1, А.2.1, А.11.3 и А.14 используются в качестве высокоэффективных методов и средств, предполагается, что методы и средства с низким уровнем эффективности также будут использованы.			

Приложение В
(обязательное)

Методы и средства для Э/Э/ПЭ систем, связанных с безопасностью. Предотвращение систематических отказов в течение различных стадий жизненного цикла

Для каждого уровня безопасности рекомендуемые методы, меры и средства предотвращения отказов в Э/Э/ПЭ системах, связанных с безопасностью, приведены в таблицах В.1—В.5. Более подробную информацию см. в приложении В МЭК 61508-7. Требования к методам по управлению отказами в период эксплуатации приведены в приложении А, а сами методы описаны в приложении А МЭК 61508-7.

Перечислить каждую причину систематических отказов, источники которых возникают на протяжении всех стадий жизненного цикла, и каждое средство защиты не представляется возможным по следующим причинам:

1) влияние систематических ошибок зависит от стадии жизненного цикла, на которой они вносятся, и

2) эффективность любой конкретной меры или средства по предотвращению отказов зависит от их применения.

Поэтому количественный анализ для предотвращения систематических отказов невозможен.

Категории отказов в Э/Э/ПЭ системах, связанных с безопасностью, могут быть установлены в соответствии со следующими стадиями жизненного цикла, которые явились источником внесения соответствующих ошибок:

- отказы, вызванные ошибками, возникающими до установки или в период установки системы (например, ошибки программного обеспечения включают в себя ошибки спецификации и ошибки программ; ошибки в аппаратных средствах включают в себя ошибки на этапе изготовления и неправильный выбор компонентов) и
- отказы, вызванные ошибками, возникающими после установки системы (например случайные отказы аппаратных средств или отказы, вызванные неправильным использованием оборудования).

Для предотвращения таких отказов или управления ими (если они происходят) обычно требуется применение большого числа средств. Структура требований, приведенных в приложениях А и В, является следствием разделения средств и мер на средства и меры, используемые для предотвращения отказов на различных стадий жизненного цикла Э/Э/ПЭ системы безопасности (см. настоящее приложение) и средства и меры, используемые для управления отказами в период эксплуатации (см. приложение А). Средства по управлению отказами — это собственные встроенные составляющие Э/Э/ПЭ систем, связанных с безопасностью, а средства и меры для предотвращения отказов — используемые в течение жизненного цикла системы безопасности.

Рекомендации, приведенные в таблицах В.1—В.5, сформированы для уровней полноты безопасности и устанавливают, во-первых, важность метода, меры или средства и, во-вторых, эффективность их использования. Уровень важности метода или средства обозначают:

M — данные методы или средства требуются обязательно (О) для данного уровня полноты безопасности;

HR — методы или средства крайне рекомендованы (КР) для данного уровня полноты безопасности. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их неиспользования;

R — методы или средства рекомендованы (Р) для данного уровня полноты безопасности;

— — методы или средства, не имеющие рекомендаций за и против применения;

NR — методы или средства явно (положительно) не рекомендованы для данного уровня полноты безопасности. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемую эффективность методов и средств обозначают:

- «низкая (Low)» — данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;
- «средняя (Medium)» — данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;
- «высокая (High)» — данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

Примечание — Большинство методов, приведенных в таблицах В.1—В.5, может использоваться с разной эффективностью в соответствии с таблицей В.6, в которой приведены описания их применения для обеспечения низкой и высокой эффективности. Усилия, требуемые для получения средней эффективности, находятся в пределах усилий, необходимых для получения низкой и высокой эффективности.

Если мера не является обязательной, то она может быть заменена другими мерами (одной или в комбинации с другими).

Руководящие указания, представленные в настоящем приложении, сами по себе не гарантируют требуемой полноты безопасности. Важно учитывать:

- последовательность выбранных методов и средств и то, как они будут дополнять друг друга;
- какие из методов и средств предназначены для каждой стадии жизненного цикла;
- какие методы и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой Э/Э/ПЭ системы, связанной с безопасностью.

Таблица В.1 — Рекомендации по предотвращению ошибок во время формирования спецификации требований проектирования Э/Э/ПЭ системы (см. 7.2)

Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Управление проектами	В.1.1	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
2 Документация	В.1.2	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
3 Разделение Э/Э/ПЭ систем, связанных с безопасностью, и систем, не связанных с безопасностью	В.1.3	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
4 Структурирование спецификации	В.2.1	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
5 Экспертиза спецификации	В.2.6	низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
6 Полуформальные методы	В.2.3, см. также таблицу В.7 МЭК 61508-3	Р (R) низкий	Р (R) низкий	КР (HR) средний	КР (HR) высокий
7 Таблица контрольных проверок	В.2.5	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
8 Автоматизированные средства разработки спецификаций	В.2.4	низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
9 Формальные методы	В.2.2	низкий	низкий	Р (R) средний	Р (R) высокий

Примечания

1 Методы 5—9, имеющие уровень важности Р (R), являются взаимозаменяемыми, но обязательно применение хотя бы одного из них.

2 Для верификации данной стадии жизненного цикла безопасности требуется выполнение по крайней мере одного из методов 5—9 или перечисленных в таблице В.5.

3 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем настоящей таблице.

4 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей В.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, требуемые для среднего уровня эффективности, находятся между усилиями, требуемыми для низкого и высокого уровней эффективности.

5 Краткий обзор методов, мер и средств, представленных в настоящей таблице, приведен в приложении В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

Таблица В.2 — Рекомендации по предупреждению внесения ошибок во время проектирования и разработки Э/Э/ПЭ системы (см. 7.4)

Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Соблюдение руководящих материалов и стандартов	В.3.1	О (М) высокий	О (М) высокий	О (М) высокий	О (М) высокий
2 Управление проектами	В.1.1	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
3 Документация	В.1.2	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
4 Структурное проектирование	В.3.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
5 Модульное проектирование	В.3.4	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
6 Использование достоверно испытанных компонент	В.3.3	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
7 Полуформальные методы	В.2.3, см. также МЭК 61508-3, пункт В.7	Р (R) низкий	Р (R) низкий	КР (HR) средний	КР (HR) высокий
8 Таблица контрольных проверок	В.2.5	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
9 Средства автоматизированного проектирования	В.3.5	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
10 Моделирование	В.3.6	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
11 Сквозной анализ или поверка аппаратных средств	В.3.7 В.3.8	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
12 Формальные методы	В.2.2	— низкий	низкий	Р (R) средний	Р (R) высокий

Примечания

1 Методы 6—12, имеющие уровень важности Р (R), являются взаимозаменяемыми, но обязательно применение хотя бы одного из них.

2 Для верификации данной стадии жизненного цикла безопасности требуется выполнение по крайней мере одного из методов 6—12 или перечисленных в таблице В.5.

3 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице В.1.

4 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей В.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

5 Краткий обзор методов, мер и средств, представленных в настоящей таблице, приведен в приложении В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

Таблица В.3 — Рекомендации для предотвращения ошибок на стадии интеграции Э/Э/ПЭ системы (см. 7.5)

Методы/меры	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Функциональное тестирование	В.5.1	О (М) высокий	О (М) высокий	О (М) высокий	О (М) высокий
2 Управление проектами	В.1.1	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
3 Документация	В.1.2	О (М) низкий	О (М) низкий	О (М) средний	О (М) высокий
4 Тестирование методом «черного ящика»	В.5.2	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий

Окончание таблицы В.3

Методы/меры	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
5 Полевые испытания	В.5.4	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
6 Статистическое тестирование	В.5.3	— низкий	— низкий	Р (R) средний	Р (R) высокий

Примечания

1 Методы 4—6, имеющие уровень важности Р (R), являются взаимозаменяемыми, но обязательно применение хотя бы одного из них.

2 Для верификации данной стадии жизненного цикла безопасности требуется выполнение по крайней мере одного из методов 4—6 или перечисленных в таблице В.5.

3 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице В.1.

4 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей В.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

5 Краткий обзор методов, мер и средств, представленных в настоящей таблице, приведен в приложении В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

Таблица В.4 — Рекомендации по предотвращению ошибок и отказов в период эксплуатации и технического обслуживания Э/Э/ПЭ системы (см. 7.6)

Методы/меры	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Инструкции по эксплуатации и техническому обслуживанию	В.4.1	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
2 Удобство общения с пользователем	В.4.2	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
3 Удобство общения с обслуживающим персоналом	В.4.3	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
4 Управление проектами	В.1.1	О (M) низкий	О (M) низкий	О (M) средний	О (M) высокий
5 Документация	В.1.2	О (M) низкий	О (M) низкий	О (M) средний	О (M) высокий
6 Сокращение работ на стадии эксплуатации	В.4.4	— низкий	Р (R) низкий	КР (HR) средний	КР (HR) высокий
7 Защита от ошибок оператора	В.4.6	— низкий	Р (R) низкий	КР (HR) средний	КР (HR) высокий
8 Эксплуатация только квалифицированным оператором	В.4.5	— низкий	Р (R) низкий	Р (R) средний	КР (HR) высокий

Примечания

1 Методы 6—8, имеющие уровень важности Р (R), являются взаимозаменяемыми, но обязательно применение хотя бы одного из них.

2 Для верификации данной стадии жизненного цикла безопасности требуется выполнение метода, основанного на таблице контрольных проверок (см. подраздел В.2.5 приложения В МЭК 61508-7), или метода, основанного на экспертизе спецификации (см. подраздел В.2.6 приложения В МЭК 61508-7).

3 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице В.1.

4 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей В.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

5 Краткий обзор методов, мер и средств, представленных в настоящей таблице, приведен в приложении В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

Таблица В.5 — Рекомендации по предотвращению ошибок при подтверждении соответствия безопасности Э/Э/ПЭ системы (см. 7.7)

Методы/меры	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Функциональное тестирование	В.5.1	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
2 Функциональные испытания в условиях окружающей среды	В.6.1	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
3 Испытания на устойчивость к пиковым выбросам внешних воздействий	В.6.2	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
4 Испытание с введением неисправностей (при требуемом охвате диагностикой ≥ 90 %)	В.6.10	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий
5 Управление проектами	В.1.1	О (M) низкий	О (M) низкий	О (M) средний	О (M) высокий
6 Документация	В.1.2	О (M) низкий	О (M) низкий	О (M) средний	О (M) высокий
7 Статический анализ, динамический анализ, анализ отказов	В.6.4, В.6.5, В.6.6	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
8 Моделирование и анализ отказов	В.3.6, В.6.6	— низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
9 Анализ наихудшего случая, динамический анализ и анализ отказов	В.6.7, В.6.5, В.6.6	— низкий	средний	Р (R) средний	Р (R) высокий
10 Статический анализ и анализ отказов (см. примечание 5)	В.6.4, В.6.6	Р (R) низкий	Р (R) низкий	НР (NR) не рекомендуемый	НР (NR) не рекомендуемый
11 Расширенное функциональное тестирование	В.6.8	— низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
12 Тестирование методом «черного ящика»	В.5.2	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
13 Испытание с введением неисправностей (при требуемом охвате диагностикой ≥ 90 %)	В.6.10	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
1 Статистическое тестирование	В.5.3	— низкий	— низкий	Р (R) средний	Р (R) высокий
15 Испытания в наихудших случаях	В.6.9	— низкий	— низкий	Р (R) средний	Р (R) высокий
16 Полевые испытания	В.5.4	Р (R) низкий	Р (R) низкий	Р (R) средний	НР (NR) не рекомендуемый

Примечания

1 Все методы 7—16, имеющие уровень важности Р (R), являются взаимозаменяемыми, но обязательно применение хотя бы одного из методов 7—10 (аналитические методы) и одного из методов 11—16 (средства испытаний).

2 Значения обозначений под каждым уровнем полноты безопасности (УПБ) см. в тексте, непосредственно предшествующем таблице В.1.

3 Методы, приведенные в настоящей таблице, могут быть использованы для различных уровней эффективности в соответствии с таблицей В.6, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, необходимые для среднего уровня эффективности, находятся между усилиями, которые определены для низкого и высокого уровней эффективности.

4 Краткий обзор методов, мер и средств, представленных в настоящей таблице, приведен в приложении В МЭК 61508-7. Ссылки на соответствующие подпункты указаны во второй графе.

5 Статистический анализ и анализ отказов не рекомендуются для УПБ 3 и УПБ 4, так как эти методы недостаточны, если не используются вместе с динамическим анализом.

Таблица В.6 — Эффективность методов и средств для предотвращения систематических ошибок

Методы/меры, средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Управление проектами (см. примечание)	В.1.1	Определение действий и обязанностей, планирование и распределение ресурсов, обучение соответствующего персонала, последовательность проверок после модификаций	Подтверждение соответствия, независимое от проекта; регулярный контроль проекта; стандартизованная процедура подтверждения соответствия; управление конфигурацией; статистики отказов; автоматизированные расчеты; автоматизированная разработка программного обеспечения
Документация (см. примечание)	В.1.2	Графические и естественные языки, например, блок-схемы, потоковые диаграммы	Правила, описывающие порядок прохождения и размещения документации в организации; содержимое таблиц контрольных проверок; автоматизированное управление документацией; формальный контроль изменений
Разделение функций безопасности Э/Э/ПЭ системы и функций, не связанных с безопасностью	В.1.3	Хорошо определенные интерфейсы между Э/Э/ПЭ системами, связанными с безопасностью, и системами, не связанными с безопасностью	Полное отделение Э/Э/ПЭ систем, связанных с безопасностью, от систем, не связанных с безопасностью, т. е. отсутствие доступа по записи систем, не связанных с безопасностью, к Э/Э/ПЭ системам, связанным с безопасностью, и физическое разделение в пространстве во избежание влияний общей причины
Структурирование спецификации	В.2.1	Иерархическое разделение вручную требований на подтребования, описание интерфейсов	Формирование иерархического разделения с использованием средств автоматизированного расчета, автоматический контроль последовательности, уточнение на более низком функциональном уровне
Формальные методы	В.2.2	Используемые персоналом, имеющим опыт в применении формальных методов	Используемые персоналом, имеющим опыт в применении формальных методов в аналогичных областях, с применением автоматизированных средств поддержки
Полуформальные методы	В.2.3	Использование полуформальных методов для описания некоторых критических частей	Полное описание Э/Э/ПЭ систем, связанных с безопасностью, различными полуформальными методами для демонстрации различных аспектов; проверка согласованности между методами
Автоматизированные средства разработки спецификации	В.2.4	Средства без предпочтения конкретному методу проектирования	Моделеориентированные процедуры с иерархической структурой, описание всех объектов и их отношений, общая база данных, автоматический контроль непротиворечивости
Таблицы контрольных проверок	В.2.5	Подготовленные таблицы контрольных проверок для всех стадий жизненного цикла системы безопасности, концентрация на главных проблемах безопасности	Подготовленные подробные таблицы контрольных проверок для всех стадий жизненного цикла системы безопасности
Экспертиза спецификации	В.2.6	Экспертиза спецификации требований безопасности независимым лицом	Экспертиза и повторная экспертиза независимой организацией, использующей формальную процедуру с исправлением всех обнаруженных ошибок
Структурное проектирование	В.3.2	Проектирование иерархических схем, выполненное вручную	Повторный контроль компонент схемы; отслеживание взаимосвязи между спецификацией, проектом, принципиальными схемами и перечнем компонент системы; автоматизация; использование определенных методов (см. также 7.4.6)

Продолжение таблицы В.6

Методы/меры, средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Использование достоверно испытанных компонентов (см. примечание)	В.3.3	Достаточно перепроверки; конструктивные характеристики	Проверено в эксплуатации (см. 7.4.10)
Модульное проектирование (см. примечание)	В.3.4	Модули ограниченных размеров; каждый модуль функционально изолирован	Повторное использование хорошо проверенных модулей; модулей с ясными свойствами; модулей, имеющих максимум один вход, один выход и один отказавший выход
Средства автоматизированного проектирования	В.3.5	Автоматизированная поддержка сложных стадий жизненного цикла безопасности	Использование средств, хорошо проверенных в эксплуатации (см. 7.4.10), или средств с подтвержденным соответствием; полная автоматизация создания системы для всех стадий жизненного цикла безопасности
Моделирование	В.3.6	Моделирование на модульном уровне, используя входные — выходные данные внешних устройств	Моделирование на уровне компонентов, используя входные/выходные данные
Поверка аппаратных средств	В.3.7	Проверка проводится лицом, не связанным с проектированием	Проверка и повторная проверка проводится независимой организацией, использующей формальные процедуры с исправлением всех обнаруженных ошибок
Сквозной контроль аппаратных средств	В.3.8	Сквозной контроль аппаратных средств проводится лицом, независимым от проектирования	Сквозной контроль аппаратных средств проводится независимой организацией, действующей по формальной процедуре с исправлением всех обнаруженных ошибок
Ограничение эксплуатационных возможностей (см. примечание)	В.4.4	Применение ключа или пароля для управления режимом работы	Определенная жесткая процедура для разрешенных действий
Эксплуатация исключительно квалифицированными операторами	В.4.5	Базовое обучение по используемому типу систем безопасности плюс два года соответствующего опыта работы	Ежегодное обучение всех операторов; опыт работы каждого оператора не менее пяти лет с устройствами, связанными с безопасностью, более низкого уровня полноты безопасности
Защита от ошибок оператора (см. примечание)	В.4.6	Подтверждение входного сообщения	Подтверждение и проверка согласованности каждой входной команды
Тестирование методом «черного ящика» (см. примечание)	В.5.2	Классы эквивалентности и тестирование по отдельным диапазонам входных сигналов, тестирование по граничным значениям, использование предписанных условий испытаний	Условия испытаний по диаграммам последствий причин (отказов) в комбинации с критическими случаями в экстремальных диапазонах работы
Статистическое тестирование (см. примечание)	В.5.3	Статистическое распределение для всех входных данных	Получение результатов испытаний автоматическими средствами, большое число тестовых испытаний, распределение входных данных в соответствии с условиями реального применения и принятыми моделями отказов

Окончание таблицы В.6

Методы/меры, средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Полевые испытания (см. примечание)	В.5.4	10000 часов эксплуатации; по крайней мере, один год эксплуатации и не менее десяти устройств в различных применениях; статистическая точность 95 %; отсутствие каких-либо критических отказов безопасности	10 млн. часов эксплуатации; по крайней мере два года эксплуатации и не менее 10 устройств в различных применениях; статистическая точность 99,9 %; подробная документация всех изменений (включая мельчайшие) в период прошлой эксплуатации
Испытания на устойчивость к пиковым выбросам внешних воздействий	В.6.2	—	Должна быть продемонстрирована устойчивость бóльшая, чем для граничных значений реальных режимов эксплуатации
Статический анализ	В.6.4	Применение блок-схем; выявление слабых мест; определение тестовых примеров	Применение подробных схем; предсказание ожидаемого поведения в случаях испытаний; применение инструментов испытаний
Динамический анализ и тестирование	В.6.5	Применение блок-схем; выявление слабых мест; определение тестовых примеров	Применение подробных схем; предсказание ожидаемого поведения в случаях испытаний; применение инструментов испытаний
Анализ отказов	В.6.6	На уровне модулей, используя входные/выходные данные периферийных устройств	На уровне компонентов, используя входные/выходные данные
Анализ наихудшего случая	В.6.7	Выполняется для функций безопасности, проводится с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации	Выполняется для функций, не относящихся к безопасности; проводится с использованием комбинаций граничных значений, соответствующих реальным условиям эксплуатации
Расширенное функциональное тестирование	В.6.8	Испытания, при которых все функции безопасности проверяют при таких же статических входных состояниях, что и в случаях, вызванных процессами отказов или условиями эксплуатации	Испытания, при которых все функции безопасности проверяют при таких же статических входных состояниях и/или необычных входных изменениях, что и в случаях, вызванных процессами отказов или условиями эксплуатации (включая те, которые могут возникать очень редко)
Испытания в наихудших случаях	В.6.9	Испытания, при которых функции безопасности проверяют для таких комбинаций граничных значений, которые встречаются в реальных условиях эксплуатации	Испытания, при которых функции, не относящиеся к безопасности, проверяются для таких комбинаций граничных значений, которые встречаются в реальных условиях эксплуатации
Испытания с введением неисправностей	В.6.10	На уровне блоков устройств, используя входные/выходные данные периферийных устройств	На уровне компонентов, используя их входные/выходные данные
Примечание — В случаях, когда методы и средства по В.1.1, В.1.2, В.3.3, В.3.4, В.4.4, В.4.6, В.5.2, В.5.3, В.5.4, В.6.7 и В.6.9 используются в качестве высокоэффективных методов и средств, предполагается, что методы и средства с низким уровнем эффективности будут также использованы.			

Приложение С
(обязательное)

Охват диагностикой и доля безопасных отказов

С.1 Расчет охвата диагностикой и доли безопасных отказов элемента аппаратного средства

Охват диагностикой и доля безопасных отказов элемента (см. МЭК 61508-4, пункты 3.8.6 и 3.6.15) рассчитываются следующим образом:

a) проводят анализ видов отказов и их влияния для определения влияния каждого вида отказов каждого компонента или группы компонентов в элементе на поведение Э/Э/ПЭ систем, связанных с безопасностью, в отсутствие диагностических проверок. В наличии должна быть информация (см. примечания), достаточная для того, чтобы убедиться в том, что влияние видов отказов и результаты анализа этого влияния с достаточной степенью достоверности соизмеримы с требованиями полноты безопасности.

Примечания

1 Для проведения такого анализа необходимы:

- подробная блок-схема Э/Э/ПЭ системы, связанной с безопасностью, описывающая элемент вместе со взаимосвязями для той части Э/Э/ПЭ системы, связанной с безопасностью, которая затрагивает рассматриваемую(ые) функцию(ии) безопасности;
- схемные решения элемента аппаратного средства, описывающие каждый компонент или группу компонентов и взаимосвязи между компонентами;
- виды отказов и частоты (интенсивности) отказов для каждого компонента или группы компонентов и связанные соотношения безопасных и опасных отказов к полной средней частоте (интенсивности) отказов в процентах.

2 Требуемая точность этого анализа зависит от ряда факторов (см. подраздел 4.1 МЭК 61508-1). В частности, должен быть принят во внимание уровень полноты безопасности рассматриваемых функций безопасности. Для более высоких уровней полноты безопасности ожидается, что виды отказов и анализ влияний будут специфичными в соответствии с конкретными типами компонентов и существующими условиями окружающей среды. Также очень важен полный и подробный анализ для элемента, используемого в архитектуре аппаратного средства, имеющего нулевую устойчивость к отказам аппаратного средства;

b) все виды отказов делят на категории по признаку, является ли он (в отсутствие диагностических испытаний):

- безопасным отказом или
- опасным отказом;

c) отказы компонентов, не принадлежащих Э/Э/ПЭ системе, связанной с безопасностью, а также отказы, не влияющие на поведение Э/Э/ПЭ системы, связанной с безопасностью, не должны учитываться при вычислении охвата диагностикой (ОД) или доли безопасных отказов (ДБО);

d) оценив частоты отказов каждого компонента или группы компонентов λ [см. примечание 1 перечисления h)] и с учетом видов отказов и результатов анализа последствий каждого вида отказа каждого компонента или группы компонентов, вычисляют частоту безопасных отказов λ_S и частоту опасных отказов λ_D. Если одна из этих интенсивностей отказов не будет иметь постоянного значения, то необходимо оценить ее среднее число за конкретный период времени и использовать для вычислений ОД и ДБО.

Примечание — Частота отказов каждого компонента или группы компонентов может быть оценена с использованием данных из признанного промышленного источника с учетом окружающей среды применения. Однако применение специфических данных предпочтительнее, особенно в случаях, если элемент состоит из небольшого числа компонентов и если любая ошибка в оценке вероятности безопасных и опасных отказов конкретного компонента может оказать существенное влияние на оценку доли безопасных отказов;

e) оценивают для каждого компонента или группы компонентов доли опасных отказов, которые могут быть обнаружены диагностическими тестами (см. приложение С.2), и, следовательно, частоты опасных отказов, обнаруженных диагностическими тестами λ_{Dd};

f) вычисляют полные частоты опасных отказов $\sum\lambda_D$, полные частоты опасных отказов, обнаруженных диагностическими тестами $\sum\lambda_{Dd}$, и полные частоты безопасных отказов $\sum\lambda_S$;

g) вычисляют охват диагностикой элемента, как $\sum\lambda_{Dd} / \sum\lambda_D$;

h) вычисляют долю безопасных отказов элемента, как $\text{ДБО} = \left(\sum\lambda_S + \sum\lambda_{Dd}\right) / \left(\sum\lambda_S + \sum\lambda_{Dd} + \sum\lambda_{Du}\right)$.

Примечания

1 Вышеупомянутое уравнение применимо, если значения интенсивностей отказов постоянны (см. определение формулы в пункте 3.6.15 МЭК 61508-4).

2 Охват диагностикой каждого элемента в Э/Э/ПЭ системе, связанной с безопасностью, должен учитываться при оценке достигаемой меры отказов для функции безопасности (см. 7.4.5.2). Доля безопасных отказов должна учитываться при определении архитектурных ограничений на полноту безопасности аппаратных средств (см. 7.4.4).

Анализ, выполняемый для определения охвата диагностикой и доли безопасных отказов, должен охватывать все компоненты, в том числе электрические, электронные, электромеханические, механические и т. п., необходимые элементу для выполнения функции(й) безопасности, которые требуются Э/Э/ПЭ системе, связанной с безопасностью. Для каждого из компонентов должны быть рассмотрены все возможные виды опасных отказов, которые приводят к опасному состоянию, препятствуют реакции безопасности, если такая реакция определена, или так или иначе ставят под угрозу полноту безопасности Э/Э/ПЭ систем, связанных с безопасностью.

Ошибки и отказы, которые должны быть обнаружены в период эксплуатации или проанализированы при определении доли безопасных отказов, приведены в таблице А.1.

Если для анализа видов отказов и их влияния используются эксплуатационные данные, то достаточно обеспечить требования полноты безопасности. При этом требуемый нижний предел статистической односторонней достоверности должен быть не менее 70 %.

Примечания

1 Пример вычисления охвата диагностикой и безопасной составляющей отказа представлен в приложении С МЭК 61508-6.

2 Для вычисления степени охвата диагностикой допускается использовать альтернативные методы, например моделирование ошибок с помощью более точных компьютерных моделей как для схем Э/Э/ПЭ систем, связанных с безопасностью, так и для используемых при их разработке электронных компонентов, например, использование моделей транзисторов для моделирования интегральной схемы.

С.2 Определение факторов охвата диагностикой

При вычислении охвата диагностикой для элемента (см. приложение С.1) для каждого компонента или группы компонентов необходимо оценить долю опасных отказов, обнаруживаемых диагностическими тестами. Диагностические тесты, которые могут внести вклад в охват диагностикой, включают в себя (но не ограничиваются) такие меры как:

- сравнительные проверки, например контроль и сравнение избыточных (резервных) сигналов;
- дополнительные встроенные тестовые программы, например вычисление контрольных сумм в устройстве памяти;
- контроль с помощью внешних воздействий, например пропусканием импульсного сигнала через контролируемые тракты;
- непрерывный контроль аналогового сигнала, например для обнаружения выхода из диапазона уровней показаний при отказе сенсора.

Для вычисления охвата диагностикой необходимо определить те виды отказов, которые обнаруживаются диагностическими тестами. Возможно, что отказы, связанные с разомкнутыми или короткозамкнутыми цепями для простых компонентов (резисторов, конденсаторов, транзисторов), могут быть обнаружены методом стопроцентного охвата диагностикой. Однако для более сложных элементов типа В (см. 7.4.4.1.3) должны быть учтены ограничения охвата диагностикой для различных компонентов, представленных в таблице А.1. Этот анализ должен быть проведен для каждого компонента или группы компонентов каждого элемента и каждой Э/Э/ПЭ системы, связанной с безопасностью.

Примечания

1 Рекомендуемые методы и средства диагностического тестирования (испытания) и рекомендуемые максимальные диагностические охваты, которые могут потребоваться, приведены в таблицах А.2—А.14. Эти тесты проводят непрерывно или периодически (в зависимости от интервала диагностического тестирования). Требования таблиц А.2—А.14 не заменяют требований настоящего приложения.

2 Диагностические тесты могут обеспечить значительные преимущества в достижении функциональной безопасности Э/Э/ПЭ системы, связанной с безопасностью. Однако следует позаботиться о том, чтобы излишне не усложнять тестирование, что может привести к увеличению трудностей при проведении действий по проверке, подтверждению соответствия, оценке функциональной безопасности, технической поддержке и модификации. Усложнение тестирования может также затруднить длительное поддержание функциональной безопасности Э/Э/ПЭ системы, связанной с безопасностью.

При расчетах охвата диагностикой и путей его использования предполагается, что УО успешно работают в присутствии другого опасного повреждения, обнаруженного диагностическими тестами. Если это предположение не верно, то Э/Э/ПЭ систему, связанную с безопасностью, следует рассматривать как систему, действующую в режиме с высокой частотой запросов или с непрерывным запросом (см. 7.4.8.3, 7.4.5.3 и 7.4.5.4).

Примечания

1 Определение охвата диагностикой приведено в 3.8.6 МЭК 61508-4. Важно отметить, что существуют альтернативные определения, но в настоящем стандарте они не применяются.

2 Диагностическое тестирование, используемое для обнаружения опасных отказов внутри элемента, может быть проведено другим элементом внутри Э/Э/ПЭ системы, связанной с безопасностью.

3 Диагностические тесты могут проводиться непрерывно или периодически, в зависимости от диагностического испытательного интервала. Могут существовать ситуации или интервалы времени, когда запуск диагностического испытания невозможен из-за того, что тестируемая система находится в неблагоприятном состоянии. В этом случае преимущества вычислений не могут помочь при диагностических испытаниях.

Приложение D
(обязательное)

Руководство по безопасности для применяемых изделий

D.1 Основные положения

Цель руководства по безопасности для применяемых изделий состоит в документальном оформлении информации, связанной с применяемым изделием, которая необходима для обеспечения интеграции применяемого изделия в связанную с безопасностью систему, или подсистему, или элемент в соответствии с требованиями настоящего стандарта.

D.2 Содержание

D.2.1 Руководство по безопасности должно определить функции применяемого изделия. Эти функции могут использоваться для того, чтобы поддержать функцию безопасности системы, связанной с безопасностью, или функции в подсистеме или элементе. Спецификация должна ясно описать и функции и интерфейсы входа и выхода.

Для каждого применяемого изделия руководство по безопасности должно содержать:

a) функциональную спецификацию выполняемых функций;

b) идентификацию конфигурации аппаратных средств и/или программного обеспечения применяемого изделия, чтобы обеспечить управление конфигурацией Э/Э/ПЭ системы, связанной с безопасностью, в соответствии с пунктом 6.2.1 МЭК 61508-1.

c) ограничения на использование применяемого изделия и/или предположения, на которых основан анализ поведения или интенсивности отказов применяемого изделия.

D.2.2 Для каждой функции руководство по безопасности должно содержать:

a) виды отказов применяемого изделия (в зависимости от поведения его выхода) из-за случайных отказов аппаратных средств, приводящих к отказу функции и не обнаруженных диагностикой, внутренней для применяемого изделия;

b) предполагаемую интенсивность отказов для каждого вида отказов по перечислению a);

c) виды отказов применяемого изделия (в зависимости от поведения его выходов) из-за случайных отказов аппаратных средств, приводящих к отказу функции и обнаруженных диагностикой, внутренней для применяемого изделия;

d) виды отказов диагностик, внутренних для применяемого изделия (в зависимости от поведения его выхода), из-за случайных отказов аппаратных средств, приводящих к отказу диагностик для обнаружения отказов функции;

e) предполагаемую интенсивность отказов для каждого вида отказов по перечислениям c) и d);

f) диагностический испытательный интервал для каждого вида отказов по перечислению c), которые обнаружены диагностикой, внутренней для применяемого изделия;

g) выходы применяемого изделия, инициируемые внешними диагностиками для каждого вида отказов по перечислению c).

Примечание — Результаты внутренней диагностики могут быть использованы, чтобы применить дополнительные меры (технические/процедурные) к Э/Э/ПЭ системе, связанной с безопасностью, подсистеме или элементу, чтобы обеспечить или поддержать безопасное состояние УО;

h) требования к любому периодическому испытанию и/или техническому обслуживанию;

i) для тех видов отказа указанной функции, которые обнаруживаются внешней диагностикой, должно быть предоставлено достаточное количество информации, чтобы облегчить разработку возможностей внешней диагностики. Информация должна включать в себя подробное описание видов отказа и их интенсивности;

j) отказоустойчивость аппаратных средств;

k) классификацию типа A или B той части применяемого изделия, которая обеспечивает выполнение функции (см. 7.4.4.1.2 и 7.4.4.1.3);

Примечание — Виды отказов могут быть классифицированы на безопасные или опасные, только если известно, как применяемое изделие применяется в опасных ситуациях УО. Например, если датчик будет применен так, что высокий уровень его выходного сигнала используется, чтобы сигнализировать об опасности УО (например, из-за высокого давления), то вид отказа, который предотвращает корректную индикацию опасности (например, выходной сигнал имеет постоянный низкий уровень), будет классифицирован как опасный, тогда как вид отказа, в результате которого выходной сигнал датчика имеет высокий уровень, будет классифицирован как безопасный. Это зависит от того, как сигнал датчика интерпретируется логикой системы, связанной с безопасностью, и поэтому датчик не может быть специфицирован без ограничения способа его применения.

Кроме того, уровень охвата диагностикой, требуемый для применяемого изделия, может меняться от одного применения к другому в зависимости от степени влияния любых диагностик на логику системы или обработку внешнего сигнала, к которым может добавляться любая внутренняя диагностика применяемого изделия.

Из этого следует, что любая оценка отказоустойчивости аппаратных средств или доли безопасных отказов, может быть выполнена, если только на применение применяемого изделия накладываются ограничения. Эти ограничения не определяются поставщиком применяемого изделия. Поэтому в руководство по безопасности не должны включаться требования к отказоустойчивости аппаратных средств или к доле безопасных отказов, или к любым другим характеристикам функциональной безопасности, которые зависят от знания о безопасных и опасных видах отказов, если ясно не определены основные предположения о соотношении безопасных и опасных видов отказов.

D.2.3 Для каждой функции применяемого изделия, для которой возможны систематические отказы, руководство должно содержать:

a) стойкость к систематическим отказам применяемого изделия или той части элемента, которая реализует функцию;

b) любые указания или ограничения, связанные с применением применяемого изделия, реализующего рассматриваемую функцию, которые должны предотвратить систематические отказы применяемого изделия.

Примечание — Систематическая полнота безопасности, определяемая стойкостью к систематическим отказам, может быть достигнута, только если указания и ограничения соблюдаются. Там, где происходит их нарушение, требование к систематической способности частично или полностью недействительно.

D.2.4 Дополнительные требования к программному обеспечению применяемого изделия представлены в подпункте 7.4.2.12 и приложении D МЭК 61508-3.

Приложение Е
(обязательное)

Специальные требования к архитектуре интегральных схем (ИС) с избыточностью схем на кристалле

Е.1 Основные положения

На данное приложение ссылается перечисление b) 7.4.2.2.

Ниже приведен ряд требований к использованию избыточности на кристалле для интегральных схем (ИС) на одной общей полупроводниковой подложке. Из соображений безопасности этот подход имеет консервативный характер, например, его применение ограничено до УПБ 3 и для него был определен ряд ограничительных требований. Последующие требования связаны только с цифровыми ИС. В настоящее время для аналого-цифровых и аналоговых ИС не существует общих требований. Анализ отказов по общей причине (см. подпункт 7.6.2.7 МЭК 61508-1) может исключить использование избыточности схем на кристалле для отдельного применения. В настоящем стандарте понятие избыточности (схем) на кристалле означает дублирование (или утроение и т. д.) функциональных единиц с целью установления значения отказоустойчивости аппаратных средств выше нуля. Согласно перечислению а) 7.4.4.1.1 в определении отказоустойчивости аппаратных средств не уделяется внимание средствам, которые могут управлять последствиями неисправностей, таким как диагностика.

Подсистема с отказоустойчивостью аппаратных средств больше нуля может быть реализована с использованием одной ИС на полупроводниковой подложке (с избыточностью на кристалле). В этом случае должны быть выполнены все следующие требования перечислений a)—q), а проектирование Э/Э/ПЭ системы и ИС должно выполняться в соответствии с этими требованиями. У ИС с избыточностью на кристалле должно быть собственное руководство по безопасности применяемого изделия (см. приложение D):

a) Самый высокий уровень полноты безопасности, на который может претендовать функция безопасности при использовании ИС, как определено выше, ограничен УПБ 3.

Примечание — Современное состояние дел, знаний и опыта не позволяют рассмотреть и принять меры для предотвращения всех несоответствий, связанных с указанным элементом (отдельной ИС), чтобы добиться достаточного доверия для УПБ 4.

b) Стойкость к систематическим отказам не должна увеличиваться за счет комбинации элементов (см.7.4.3.2).

c) Для того чтобы предотвратить отказ(ы) по общей причине, например из-за случайной ошибки(ок) аппаратных средств, необходимо рассмотреть влияние увеличения температуры на такие ошибки. Необходимо применить по крайней мере один из методов 6, перечисленных в таблице Е.2. В проекте, где локальная ошибка может вызвать критическое для безопасности увеличение температуры, должны быть приняты соответствующие меры.

Примечание — В то время как в крупном проекте локальная ошибка может вызвать значительное увеличение температуры, влияние локального короткого замыкания в логической схеме может быть незначительным. Например, в цифровых схемах — это область контактной площадки устройства и регуляторы напряжения.

d) Для каждого канала и каждого элемента контроля, такого как контрольный датчик времени, на подложке ИС должен быть предусмотрен отдельный физический блок. Эти блоки должны иметь соединительные проводники и выводы. У каждого канала должны быть свои собственные отделенные входы и выходы, которые не должны пересекаться с другими каналами/блоками.

Примечания

1 Это требование не исключает наличия внутренних соединений между блоками ИС: проводников между выходными и входными ячейками различных блоков (см. также методы 3a и 3b таблицы Е.1).

2 На входах и выходах блоков могут быть (но не только):

- сигналы для обеспечения контролепригодности (например, методом сканирования цепей);
- сигналы синхронизации и сигналы управления синхронизацией;
- электропитание;
- сигналы перезагрузки;
- сигналы конфигурирования и выбора его способа;
- сигналы выполнения отладки и записи ее результатов.

e) Для предотвращения опасных отказов, вызванных сбоями электропитания, включая отказы по общей причине, должны быть приняты соответствующие меры.

Примечания

1 Ошибки электропитания включают в себя (но этим не ограничиваются):

- шум;
- распространение помех по линиям электропитания;

- неодновременное включение электропитания, что может привести к срабатываниям защелок или к большим токам включения;
- превышение потребляемого тока в результате короткого замыкания.

2 Это требование может быть выполнено, если применять следующие методы:

- обеспечить каждый блок электропитанием через его собственный вывод питания, так чтобы на блок электропитание не подавалось через другой блок (например, через внутренние связи), а также через соединительные каналы связанных между собой отдельных физических блоков в ИС (см. также метод 3 таблицы Е.2);
- использовать внешние меры для предотвращения опасных отказов, которые могут быть вызваны различными напряжениями в соединительных каналах;
- выявлять ошибки электропитания с помощью мониторинга напряжения;
- использовать несколько увеличенный допуск по напряжению;
- анализировать проблемы понижения внутреннего сопротивления при проектировании шин электропитания.

f) Минимальное расстояние между границами отдельных физических блоков должно быть достаточным для предотвращения короткого замыкания и перекрестных наводок между этими блоками.

Примечания

1 Короткие замыкания, как правило, могут быть вызваны смещением при гальванических процессах, смещением сквозных отверстий, смещением контактных площадок, разрушением оксида вентиля из-за локального дефекта, эффекта защелкивания и т. д.

2 Перекрестные наводки, как правило, могут быть вызваны токами в подложке, емкостными связями и т. д.

3 Минимальное расстояние должно, как правило, выбираться согласно соответствующим правилам проектирования с коэффициентом запаса между 10 и 50.

4 Потенциальные кольца в соответствии с таблицей Е.2 не рассматриваются как часть блока при оценке расстояния между отдельными физическими блоками.

g) Короткое замыкание и/или перекрестные наводки между смежными проводниками отдельных физических блоков не должны приводить к невыполнению функции безопасности или к необнаруженной ошибке функции мониторинга (см. метод 5 таблицы Е.2).

h) Подложка должна быть заземлена, независимо от того, какой использовался процесс создания ИС (*n*-диффузия или *p*-диффузия).

Примечание — Для *p*-диффузии это означает использование отрицательного источника питания. Необходимо избегать отрицательной логики, так как ее использование может сделать проект чувствительным к ошибкам.

i) Чувствительность ИС с избыточностью на кристалле к отказам по общей причине должна оцениваться определением β-фактора согласно Е.3. Этот β-фактор, названный β_{IC}, должен использоваться при оценке достигнутой полноты безопасности Э/Э/ПЭ системы, связанной с безопасностью, согласно 7.4.5.1 и будет использоваться для ИС вместо β-фактора, определенного, например, в приложении D МЭК 61508-6.

j) Обнаружение отказа (диагностическими тестами, контрольными проверками или любыми другими средствами) в ИС с избыточностью на кристалле должно привести к конкретному действию для достижения или поддержки безопасного состояния.

Примечание — Это требование не применяется, если результатами отказа можно управлять, например с помощью обесточивания блока.

k) Минимальный охват диагностикой каждого канала должен составить по крайней мере 60 %. При однократной реализации элемента мониторинга минимальный охват диагностикой этого элемента должен также составить по крайней мере 60 %.

l) Если возникнет необходимость реализовать контрольный датчик времени, например для контроля последовательности программы и/или для того, чтобы гарантировать необходимый охват диагностикой или долю безопасных отказов, то один канал не должен использоваться в качестве контрольного датчика времени для другого канала, кроме тех случаев, когда используются функционально разные каналы.

m) При тестировании на электромагнитную совместимость без дополнительного запаса по безопасности функция, выполняемая ИС, не должна создавать помехи (например, соответствовать критерию А, как описано в стандартах по определению пределов электромагнитной устойчивости для достижения ЭМС, см. например [9] или МЭК 61326-3-1).

n) При тестировании на электромагнитную совместимость с дополнительным запасом по безопасности функция безопасности (включая ИС) должна соответствовать критерию «FS», как определено в МЭК 61326-3-1.

o) Должны быть предприняты соответствующие меры для предотвращения опасных ошибок, вызванных колебаниями в цифровых входных портах, подключенных к внешним асинхронным цифровым сигналам, например, введением соответствующей синхронизации со сложной структурой.

p) Должны быть проанализированы возможные общие причины отказов общих ресурсов, таких как схемы сканирования периферии и наборы регистров со специальными функциями.

q) В перечислениях a)—p) представлен перечень источников общих причин, характерных для ИС с избыточностью на кристалле. В настоящем стандарте будут рассмотрены другие соответствующие источники общих причин.

Примечание — В целом вышеупомянутые требования ограничивают использование избыточности на кристалле для ИС, разработанных для полностью или неполностью специализированных ИС, таких как СИС, микроконтроллеров или других специализированных систем на кристалле. Другие разработки, такие как вентильная матрица, вентильная матрица, программируемая заказчиком (FPGA) и т. д., могут не соответствовать всем требованиям.

Использование ИС с избыточностью на кристалле, как описано выше, должно быть разрешено, если только был проведен полный анализ общих причин (АОП). Этот анализ должен охватывать полный спектр возможных отказов по общей причине, появляющихся в результате проектирования, производства, сборки, а также процедурных факторов и условий окружающей среды. В частности, необходимо специально исследовать проблему нарушения физического разделения между каналами из-за использования ИС с избыточностью на кристалле. Окончательное значение УПБ, назначаемое Э/Э/ПЭ системе, связанной с безопасностью, должно зависеть от результатов этого АОП.

Примечания

1 Использование физического разделения (т. е. сегрегации) «каналов» может обеспечить защиту от широкого диапазона отказов по общей причине в избыточных системах.

2 Предложенная методология АОП состоит из следующих этапов:

1) идентификация возможных источников общей причины (ИОП). Рассмотрение влияния перечисленных в данном приложении и других предвидимых заранее физических ИОП и логических ИОП (совместно используемых ресурсов и сигналов);

2) идентификация избыточных блоков в ИС, которые пострадают от ИОП;

3) формирование списка мер и их качественная оценка для обеспечения безопасности для каждого ИОП, выявленного на этапе 1, для каждой пары избыточных блоков, выявленных на этапе 2;

4) получение количественных значений по таблицам Е.1 и Е.2 для каждой пары избыточных блоков, выявленных на этапе 2, и формирование оценки конкретного значения β-фактора;

5) использование определенного β-фактора в вероятностном моделировании.

Е.2 Дополнительные требования к ИС с избыточностью на кристалле для УПБ 3

ИС с избыточностью на кристалле с УПБ 3 должна соответствовать кроме перечисленных в Е.1 следующим требованиям:

a) наличие документально оформленных доказательств о том, что все конкретные условия окружающей среды были обеспечены в соответствии с принятыми для процессов спецификации, анализа, проверки и подтверждения соответствия;

b) определение внешних мер, которые могут обеспечить или поддержать безопасное состояние Э/Э/ПЭ системы. Эти меры должны достигать, как минимум, средней эффективности (см. также А.3 приложения А). Все средства, реализованные в самих ИС для контроля влияния систематических отказов и/или отказов по общей причине, должны использовать эти внешние меры, чтобы обеспечить или поддержать безопасное состояние Э/Э/ПЭ системы.

Е.3 β-фактор

Чувствительность ИС с избыточностью на кристалле к отказам по общей причине должна оцениваться определением специального для ИС с избыточностью на кристалле β-фактора $\beta_{ИС}$ [см. также Е.1, перечисление i)]. Его оценка должна проводиться следующим образом:

a) базовый β-фактор, обозначенный $\beta_{В\text{-}ИС}$, составляет 33 %;

b) увеличение базового β-фактора $\beta_{В\text{-}ИС}$ при проектировании выполняется в соответствии с таблицей Е.1 и

c) уменьшение базового β-фактора $\beta_{В\text{-}ИС}$ при проектировании выполняется в соответствии с таблицей Е.2.

$\beta_{ИС}$ вычисляют сложением значения $\beta_{В\text{-}ИС}$ со всеми значениями оценок по таблице Е.1 и далее вычитанием всех значений оценок по таблице Е.2. Результирующее значение $\beta_{ИС}$ не должно превышать 25 %.

Примечания

1 β-фактор, названный $\beta_{ИС}$, будет использоваться при оценке достигаемой полноты безопасности Э/Э/ПЭ системы, связанной с безопасностью, согласно 7.4.5.1 и применяться для ИС вместо β-фактора, определенного, например, согласно приложению D МЭК 61508-6.

2 Для того чтобы обосновать, что выбранный β-фактор консервативен, необходимо для используемой методологии проектирования ИС провести анализ доступных данных по отказам. Необходимо использовать только проверенные временем процессы разработки и реализации ИС.

Таблица Е.1 — Методы и средства, увеличивающие $\beta_{В-ИС}$

Методы / средства	Дополнение β -фактора, в %	Примечание
1 Контрольный датчик времени на кристалле, используемый в качестве элемента контроля	5	Элементы контроля, использующие функцию контрольного датчика времени и необходимые, чтобы гарантировать требуемый ОД или ДБО, должны быть реализованы вне ИС в основном из-за отказов по общей причине. Реализация контрольного(ых) датчика(ов) времени на кристалле может привести к более высокому ОД или ДБО по сравнению с внешней реализацией. См. также Е.2, перечисление b)
2 Элементы контроля на кристалле, отличные от контрольного датчика времени, например контроль синхронизации	5	Элементы контроля, используемые, например, для контроля синхронизации и необходимые, чтобы гарантировать требуемый ОД или ДБО, должны быть реализованы вне ИС в основном из-за отказов по общей причине. Реализация элемента(ов) контроля на кристалле может привести к более высокому ОД или ДБО по сравнению с внешней реализацией
3a Внутренние соединения между блоками с помощью проводников между выходными и входными ячейками отдельных физических блоков без пересечений на различных уровнях металлизации	2	Выполнение сравнения условий и результатов соединений между отдельными физическими блоками по возможности должно быть реализовано вне ИС. Требуется анализ возможных отказов по общей причине, включая FMEA константных отказов внутренних соединений. В частности, должно быть учтено влияние увеличения температуры из-за отказов. При анализе окончательного размещения должна быть выполнена его проверка, например, с использованием инструментальных средств
3b Внутренние соединения между блоками с помощью проводников между выходными и входными ячейками отдельных физических блоков с пересечениями	4	Выполнение сравнения условий и результатов соединений между отдельными физическими блоками по возможности должно быть реализовано вне ИС. Требуется анализ возможных отказов по общей причине, включая FMEA константных отказов и короткого замыкания внутренних соединений. В частности, должно быть учтено влияние увеличения температуры из-за отказов.

Примечание — Буквой после числа обозначены альтернативные методы / средства. Может быть выбран только один из них.

Методы и средства, перечисленные в настоящей таблице, не являются исчерпывающими. Могут использоваться другие методы и средства, если представлены доказательства, что они обеспечивают требуемое значение дополнения β-фактора.

Если могут быть представлены доказательства, что были приняты меры по ослаблению влияния отказов по общей причине, то могут использоваться другие значения дополнения β-фактора. В таких случаях должны быть рассмотрены общие рекомендации по приложению D МЭК 61508-6.

Соединения интерфейсных сигналов между избыточными блоками обычно выполняются с использованием нескольких уровней металлизации. Независимо от пути, по которому проходит это соединение, расположен ли он исключительно только на одном уровне металлизации или он использует несколько уровней металлизации, полное соединение интерфейсного сигнала рассматривают как один проводник. Для того, чтобы минимизировать возможные взаимные помехи двух каналов одним отказом, ни одно из соединений интерфейсного сигнала не должно пересекаться с другими соединениями интерфейсных сигналов.

Таблица Е.2 — Методы и средства, сокращающие $\beta_{В-ИС}$

Методы/средства	Дополнение β -фактора, %	Примечание
1a Разнообразные меры для управления отказами в различных каналах	4	—
1b Разнообразные функции и средства для управления отказами в различных каналах	6	—
2 Тестирование Э/Э/ПЭ системы на электромагнитную совместимость с дополнительным запасом безопасности без влияния на функции Э/Э/ПЭ системы (например, при выполнении критерия А)	5	Критерий выполнения А описан в стандартах по определению пределов электромагнитной устойчивости для достижения ЭМС, см. например [9] или МЭК 61326-3-1
3 Обеспечить каждый блок его собственным выводом питания так, чтобы никакой блок не получал питание от источника питания другого блока (например через внутренние соединения), а также через соединительные каналы связанных между собой отдельных физических блоков в ИС	6	Должны быть использованы внешние меры для предотвращения опасных отказов, которые могут быть вызваны разницей напряжений в каналах
4 Структуры, которые изолируют и разделяют физические размещения	2—4	Полезно разделять отдельные физические блоки
5 Заземленный вывод между выходными выводами отдельных физических блоков	2	Если не выполнено, то должно происходить короткое замыкание между соседними линиями отдельных физических блоков при проверке влияния разрыва проводников [см. также Е.1, перечисление g)]. В этом случае β-фактор не будет уменьшен
6a Высокий охват диагностикой (ОД ≥ 99 %) каждого канала, обнаружение отказа техническими средствами и достижение безопасного состояния за соответствующий короткий промежуток времени	7	Может быть целесообразным лишь в исключительном случае
6b Температурные датчики между блоками постоянно отключаемые (внутренне или внешне) в безопасном состоянии за соответствующий короткий промежуток времени; без диагностики эффективность низкая	2	См. также таблицу А.18, меры по предотвращению повышения температуры
6c Температурные датчики между блоками постоянно отключаемые (внутренне или внешне) в безопасном состоянии за соответствующий короткий промежуток времени; с диагностикой эффективность высокая	9	См. также таблицу А.18, меры по предотвращению повышения температуры
6d Анализ/тестирование влияния отказов (например, при повышении температуры). В зависимости от результата анализа/тестирования может потребоваться сравнение между каналами, включая обнаружение неисправностей и достижение безопасного состояния за соответствующий короткий промежуток времени	9	—
6e Проектирование функционала контролирующей схемы при повышенной температуре	7	Проект функции контроля (например, контрольного датчика времени) должен выполнять функцию безопасности при наихудших значениях температуры

Примечание — Буквой после числа обозначены альтернативные методы/средства. Может быть выбран только один из них.

Методы и средства, перечисленные в настоящей таблице, не являются исчерпывающими. Могут использоваться другие методы и средства, если представлены доказательства, что они обеспечивают требуемое значение дополнения β-фактора.

Методы и средства 6a—6e предназначены для управления результатами повышения температуры из-за отказа.

Приложение F
(справочное)

Методы и средства, предотвращающие систематические отказы в СИС

F.1 Основные положения

Для предотвращения отказов во время разработки специализированных интегральных схем (СИС) должны быть применены следующие методы и средства:

Примечания

1 На настоящее приложение ссылается 7.4.6.7.

2 Следующие методы и средства связаны только с цифровыми СИС и ИС, программируемыми пользователями. Для аналого-цифровых и аналоговых СИС в настоящее время не могут быть предложены никакие общие методы и средства.

a) Все действия по выполнению проекта, схемы тестирования, инструменты, используемые для функционального моделирования, и его результаты должны быть документально оформлены.

b) Все инструменты, библиотеки и производственные процедуры должны быть проверены в эксплуатации. Они включают в себя:

- применение конкретного инструмента (включая различные версии с эквивалентными функциями) в течение достаточно длительного промежутка времени в подобных проектах или более сложных.

Примечание — Достаточно длительный промежуток времени мог в этом случае быть 2 года;

- применение общих или широко используемых инструментов, гарантирующих, что информация о возможных ошибках и ограничениях известна для данного инструмента и/или данной его версии, которую необходимо рассмотреть во время использования. Для того чтобы отследить существующие отказы, производителями должны быть выполнены управление и контроль версии;
- проверки внутренней непротиворечивости и правдоподобия для предотвращения отказов в различных базах данных, создаваемых различными инструментами.

Примечание — Обучение пользователей является очень важным из-за быстрых изменений и прогресса в данной области.

c) Все действия и их результаты должны быть проверены, например, моделированием, проверками эквивалентности, временным анализом или проверкой технологических ограничений.

d) Должны использоваться средства воспроизводимости и автоматизации процесса реализации проекта (сценарий должен быть обоснован, выполняемые работы автоматизированы и последовательность выполнения проекта спланирована).

e) Из «мягких» (специфицированных на языке описания аппаратных средств VHDL или Verilog) и «твердых» [специфицированных на физическом (топологическом) уровне реализации СИС] макроблоков, поставляемых третьей стороной, должны использоваться только те макроблоки, для которых выполнено подтверждение соответствия и которые должны соответствовать всем ограничениям и указаниям, определенным для макроблоков поставщиком, если это возможно. Если для макроблока отсутствуют доказательства его проверки в эксплуатации, то каждый такой макроблок должен рассматриваться как блок с вновь написанным кодом, поэтому для него должно быть полностью выполнено подтверждение соответствия.

f) При проектировании должны использоваться проблемно-ориентированные с высоким уровнем абстракции методология проектирования и язык описания проекта.

Примечание — Для описания проекта должен использоваться язык описания аппаратных средств, такой, например, как язык описания технических средств на быстродействующих интегральных схемах VHDL или Verilog. Это наиболее распространенная методология описания аппаратных средств, используемая в настоящее время при проектировании СИС. Оба языка определены в стандартах IEEE и, как предполагается, удовлетворяют рекомендациям для высокоуровневых языков программирования. Язык описания аппаратных средств может использоваться для описания проекта и функциональных моделей или испытательных стендов. Для описания проекта допускается использовать только то подмножество языка описания аппаратных средств, которое позволят синтезировать аппаратные средства на уровне межрегистровых передач. Часть языка описания аппаратных средств (не способная к синтезу кода), достаточная для описания функциональных моделей и испытательных стендов, названа «языком моделирования поведения аппаратных средств».

g) Должен быть достигнут соответствующий уровень тестируемости (для тестирования полностью и неполностью специализированных СИС в процессе производства).

h) Необходимо учитывать задержки в логических элементах и межсоединениях (проводников) во время тестирования и выполнения проверки СИС.

i) Следует избегать применения логических элементов с тремя состояниями на выходе. Если они используются, то их выходы должны быть снабжены устройствами повышения или понижения выходного уровня или блокировки доступа к шине.

j) Перед изготовлением должна быть проведена соответствующая проверка всей СИС (включая все проверки, выполненные во время разработки и реализации, чтобы гарантировать корректность функциональности модуля и микросхемы).

Примечание — Адекватность проверки СИС зависит от сложности теста элемента и необходимого уровня полноты безопасности.

F.2 Методы и средства. Руководящие принципы

Необходимо использовать соответствующую группу методов и средств, которые важны в процессе проектирования и разработки СИС для предотвращения появления отказов. В зависимости от технической реализации необходимо разделение между полностью и неполностью специализированными цифровыми СИС и ИС, программируемыми пользователем (FPGA/PLD/CPLD). Методы и средства, которые поддерживают обеспечение получения соответствующих свойств для полностью и неполностью специализированных СИС, определены в таблице F.1, а для ИС, программируемых пользователем, — в таблице F.2. Жизненный цикл разработки СИС показан на рисунке 3.

Рекомендации, приведенные в таблицах F.1 и F.2, сформированы для уровней полноты безопасности и устанавливают, во-первых, уровень важности метода или средства и, во-вторых, эффективность его использования.

Уровень важности метода или средства обозначают:

HR* — методы или средства крайне рекомендованы (КР*) для данного уровня полноты безопасности. Проект обязательно должен использовать этот метод или средство;

HR — методы или средства крайне рекомендованы (КР) для данного уровня полноты безопасности. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их неиспользования;

R — методы или средства рекомендованы (Р) для данного уровня полноты безопасности. Если эти методы или средства не используются или не используется ни одна из возможных альтернатив, то должно быть приведено подробное обоснование их неиспользования;

— — методы или средства, не имеющие рекомендаций за и против применения;

NR — методы или средства явно (положительно) не рекомендованы (НР) для данного уровня полноты безопасности. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемую эффективность методов и средств обозначают:

- «низкая (Low)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;
- «средняя (Medium)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;
- «высокая (High)» — данные методы или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

Руководящие указания, представленные в настоящем приложении, не гарантируют сами по себе требуемой полноты безопасности. Важно учитывать:

- последовательность выбранных методов, мер и средств и то, как они будут дополнять друг друга;
- какие из методов, мер и средств предназначены для каждой стадии жизненного цикла разработки;
- какие методы, меры и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой отдельной Э/Э/ПЭ системы, связанной с безопасностью.

Таблица F.1 — Методы и средства, предотвращающие появление отказов в процессе проектирования и разработки полностью и неполностью специализированных цифровых СИС (см. 7.4.6.7)

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Начало проектирования	1 Структурное описание	E.3	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	2 Описание проекта на (V)HDL (см. примечание)	E.1	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	3 Ввод описаний схем	E.2	НР (NR)	НР (NR)	НР (NR)	НР (NR)
	4 Моделирование на (V)HDL (см. примечание)	E.5	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	5 Применение средств моделирования на (V)HDL, проверенных в эксплуатации (см. примечание)	E.4	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	6 Функциональное тестирование на уровне модулей (используя, например (V)HDL описания испытательных стендов) (см. примечание)	E.6	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	7 Высокоуровневое функциональное тестирование	E.7	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	8 Функциональное тестирование во внешней системной среде	E.8	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	9 Ограниченное использование асинхронных конструкций	E.9	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	10 Синхронизация основных входов и управление метастабильностью	E.10	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	11 Проектирование тестируемости (в зависимости от охвата тестами, %)	E.11	Р (R) > 95 %	Р (R) > 98 %	Р (R) > 99 %	Р (R) > 99 %
	12 Разбиение на модули	E.12	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	13 Охват сценариями верификации	E.13	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	14 Соблюдение руководств по кодированию	E.14	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	15 Применение средства проверки кода	E.15	Р (R)	Р (R)	Р (R)	Р (R)
	16 Программирование с защитой	E.16	Р (R) низкий	Р (R) средний	КР (HR) высокий	КР* (HR*) высокий
	17 Документальное оформление результатов моделирования	E.17	КР (HR) низкий	КР (HR) средний	КР (HR) высокий	КР* (HR*) высокий
	18a Проверка кода	E.18	Р (R) средний	Р (R) высокий	КР (HR) высокий	КР* (HR*) высокий
	18b Сквозной контроль	E.19	Р (R) средний	Р (R) высокий	КР (HR) высокий	КР* (HR*) высокий
	19a Применение прошедших подтверждение соответствия программных блоков, специфицированных на языке описания аппаратных средств, для проектирования микросхем	E.20	Р (R) средний	Р (R) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	19b Подтверждение соответствия программных блоков, специфицированных на языке описания аппаратных средств, для проектирования микросхем	E.21	Р (R) средний	Р (R) высокий	КР* (HR*) высокий	КР* (HR*) высокий

Продолжение таблицы F.1

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Синтез	20a Моделирование логической схемы на основе списка соединений для проверки ограничений синхронизации	E.22	P (R) средний	P (R) средний	P (R) высокий	P (R) высокий
	20b Статический анализ задержки распространения сигнала (STA)	E.23	P (R) средний	P (R) средний	P (R) высокий	P (R) высокий
	21a Проверочное сравнение списка соединений логических элементов с эталонной моделью средствами моделирования	E.24	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
	21b Сравнение списка соединений логических элементов с эталонной моделью (формальный тест на эквивалентность)	E.25	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
	22 Проверка требований и ограничений поставщика СИС	E.26	KP (HR) высокий	KP (HR) высокий	KP* (HR*) высокий	KP* (HR*) высокий
	23 Документальное оформление ограничений, результатов и средств синтеза	E.27	KP (HR) высокий	KP (HR) высокий	KP* (HR*) высокий	KP* (HR*) высокий
	24 Применение проверенных в эксплуатации средств синтеза	E.28	KP* (HR*) высокий	KP* (HR*) высокий	KP* (HR*) высокий	KP* (HR*) высокий
	25 Применение проверенной в эксплуатации целевой библиотеки	E.29	KP* (HR*) высокий	KP* (HR*) высокий	KP* (HR*) высокий	KP* (HR*) высокий
	26 Процедуры, основанные на сценарии	E.30	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
Ввод теста и генерация тестового шаблона	27 Реализация тестовых структур	E.31	P (R) > 95 %	P (R) > 98 %	P (R) > 99 %	P (R) > 99 %
	28a Оценка тестового охвата моделированием (основанная на достигнутом тестовом охвате, %)	E.32	P (R) > 95 %	P (R) > 98 %	P (R) > 99 %	P (R) > 99 %
	28b Оценка тестового охвата применением средств ATPG (основанная на достигнутом тестовом охвате, %)	E.33	P (R) > 95 %	P (R) > 98 %	P (R) > 99 %	P (R) > 99 %
	29a Моделирование логической схемы на основе списка соединений для проверки ограничений синхронизации	E.22	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
	29b Статический анализ задержки распространения сигнала (STA)	E.23	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
	30a Проверочное сравнение списка соединений логических элементов с эталонной моделью средствами моделирования	E.24	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий
	30b Сравнение списка соединений логических элементов с эталонной моделью (формальный тест на эквивалентность)	E.25	P (R) средний	P (R) средний	KP (HR) высокий	KP (HR) высокий

Продолжение таблицы F.1

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Размещение, трассировка, генерация топологии	31a Обоснование проверкой в эксплуатации применение блоков СИС на физическом уровне реализации	E.34	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	31b Применение блоков СИС, прошедших подтверждение соответствия	E.35	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	31c Тестирование блоков СИС в неавтономном режиме	E.36	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	32a Моделирование логической схемы на основе списка соединений для проверки ограничений синхронизации	E.22	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	32b Статический анализ задержки распространения сигнала (STA)	E.23	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	33a Проверочное сравнение списка соединений логических элементов с эталонной моделью средствами моделирования	E.24	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	33b Сравнение списка соединений логических элементов с эталонной моделью (формальный тест на эквивалентность)	E.25	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
Размещение, трассировка, генерация топологии	34 Проверка правил проектирования DRC	E.37	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	35 Проверка соответствия топологии схе-ме LVS	E.38	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	36 Применение проверенных в эксплуатации условий среды проектирования. Применение проверенных в эксплуатации библиотек ячеек	E.4	КР* (HR*) высокий	КР* (HR*) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	37 Дополнительный резерв времени (> 20 %) для технологических процессов, реализующихся меньше 3 лет	E.39	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий

Окончание таблицы F.1

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Изготовление микросхемы	38 Применение проверенной в эксплуатации технологии процесса	—	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	39 Проверенный в эксплуатации процесс производства	E.42	КР (HR) низкий	КР (HR) средний	КР (HR) высокий	КР* (HR*) высокий
	40 Обеспечение качества для технологии процесса	—	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	41 Контроль качества производственного процесса	E.43	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	42 Передача качественно изготовленного устройства	E.44	Р (R) низкий	Р (R) средний	КР (HR) высокий	КР* (HR*) высокий
	43 Передача качественно функционирующего устройства	E.45	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	44 Охват тестированием проверки производства	—	> 95 %	> 98 %	> 99 %	> 99 %
	45 Стандарты качества	E.46	КР (HR) низкий	КР (HR) средний	КР (HR) высокий	КР* (HR*) высокий
	46 Менеджмент качества, например, в соответствии с ИСО9000	—	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	47 Отбраковочное испытание	E.40	Р (R) низкий	Р (R) средний	КР (HR) высокий	КР* (HR*) высокий

Примечание — Согласно уровню полноты безопасности должны быть выбраны соответствующие методы/средства. Альтернативные или эквивалентные методы/средства обозначены буквой после числа. По крайней мере, один из альтернативных или эквивалентных методов/средств должен быть применен.

Термин (V)HDL обозначает или язык описания аппаратных средств на сверхбыстродействующих интегральных схемах VHDL, или язык описания аппаратных средств Verilog.

Таблица F.2 — Методы и средства, предотвращающие появление отказов в процессе проектирования и разработки СИС, для программируемых пользователем ИС (FPGA/PLD/CPLD) (см. 7.4.6.7)

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Начало проектирования	1 Структурное описание	E.3	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	2 Описание проекта на (V)HDL (см. примечание)	E.1	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	3 Ввод описаний схем	E.2	— высокий	— высокий	НР (NR)	НР (NR)
	4 Описание проекта, используя булевы уравнения	—	Р (R) высокий	Р (R) высокий	НР (NR)	НР (NR)
	5a Для описаний схем, использующих булевы уравнения: ручной контроль в проектах с ограниченной (низкой) сложностью	—	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	5b Для описаний схем, использующих булевы уравнения: моделирование изменений состояний в проектах с более высокой сложностью	—	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	6 Применение проверенных в эксплуатации условий среды проектирования	E.4	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	7 Применение средств моделирования на (V)HDL, проверенных в эксплуатации (см. примечание)	E.5	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	8 Функциональное тестирование на уровне модулей (используя, например (V)HDL описания испытательных стендов) (см. примечание)	E.6	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	9 Ограниченное использование асинхронных конструкций	E.9	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	10 Проектирование тестируемости (в зависимости от охвата тестами, %)	E.11	Р (R) > 95 %	Р (R) > 98 %	Р (R) > 99 %	Р (R) > 99 %
	11 Разбиение на модули	E.12	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	12 Охват сценариями проверки (испытательные стенды)	E.13	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	13 Соблюдение руководств по кодированию	E.14	КР (HR) высокий	КР (HR) высокий	КР* HR*) высокий	КР* HR*) высокий
	14 Документальное оформление результатов моделирования	E.17	КР (HR) низкий	КР (HR) средний	КР (HR) высокий	КР* HR*) высокий
	15a Проверка кода	E.18	Р (R) средний	Р (R) высокий	КР (HR) высокий	КР* HR*) высокий
	15b Сквозной контроль	E.19	Р (R) средний	Р (R) высокий	КР (HR) высокий	КР* HR*) высокий
	16a Применение «мягких» макроблоков, прошедших подтверждение соответствия	E.20	Р (R) средний	Р (R) высокий	КР (HR) высокий	КР* HR*) высокий
	16b Подтверждение соответствия «мягких» макроблоков	E.21	Р (R) средний	Р (R) высокий	КР* HR*) высокий	КР* HR*) высокий

Продолжение таблицы F.2

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Синтез	17 Внутренние проверки согласованности (см., например, E.4 приложения E МЭК 61508-7)	—	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	18a Моделирование логической схемы на основе списка соединений для проверки ограничений синхронизации	E.22	Р (R) средний	Р (R) средний	Р (R) высокий	Р (R) высокий
	18b Статический анализ задержки распространения сигнала STA	E.23	Р (R) средний	Р (R) средний	Р (R) высокий	Р (R) высокий
	19a Проверочное сравнение списка соединений логических элементов с эталонной моделью средствами моделирования	E.24	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	19b Сравнение списка соединений логических элементов с эталонной моделью (формальный тест на эквивалентность)	E.25	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	20 Для PLD/CPLD в сложных проектах: проверка проекта моделированием	—	Р (R) средний	Р (R) средний	КР (HR) высокий	КР (HR) высокий
	21 Проверка требований и ограничений поставщика СИС	E.26	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	22 Документальное оформление ограничений, результатов и средств синтеза	E.27	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	23 Применение проверенных в эксплуатации средств синтеза	E.28	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	24 Применение проверенной в эксплуатации целевой библиотеки	E.29	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	25 Процедуры, основанные на сценарии	E.30	Р (R) высокий	Р (R) высокий	КР (HR) высокий	КР* (HR*) высокий

Продолжение таблицы F.2

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Размещение, трассировка, генерация топологии	26a Обоснование проверенных в эксплу-атации примененных «жестких» макробло-ков	E.34	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	26b Применение «жестких» макроблоков, прошедших подтверждение соответствия	E.35	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	26c Тестирование «жестких» макроблоков в неавтономном режиме	E.36	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	27a Моделирование логической схемы на основе списка соединений для провер-ки ограничений синхронизации	E.22	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	27b Статический анализ задержки рас-пространения сигнала STA	E.23	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	28a Проверочное сравнение списка сое-динений логических элементов с эталон-ной моделью средствами моделирования	E.24	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	28b Сравнение списка соединений логи-ческих элементов с эталонной моделью (формальный тест на эквивалентность)	E.25	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	29 Проверки правил проектирования (DRC)	E.37	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	30 Применение проверенных в эксплу-атации условий среды проектирования. Применение проверенных в эксплуатации библиотек ячеек	E.4	КР* (HR*) высокий	КР* (HR*) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	31 Дополнительный резерв времени (более 20 %) для технологических про-цессов, реализуемых менее 3 лет	E.39	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий

Окончание таблицы F.2

Стадия проектирования	Методы/меры, средства	См. МЭК 61508-7	УПБ 1	УПБ 2	УПБ 3	УПБ 4
Изготовление микросхемы	32 Применение проверенной в эксплуатации технологии процесса	—	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	33 Применение серийных приборов, проверенных в эксплуатации	E.41	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	34 Проверенный в эксплуатации процесс производства	E.42	КР (HR) низкий	КР (HR) средний	КР (HR) высокий	КР* (HR*) высокий
	35 Контроль качества производственного процесса	E.43	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	36 Передача качественно изготовленного устройства	E.44	Р (R) низкий	Р (R) средний	КР (HR) высокий	КР* (HR*) высокий
	37 Передача функционально качественного устройства	E.45	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	38 Стандарты качества	E.46	КР (HR) низкий	Р (R) средний	КР (HR) высокий	КР* (HR*) высокий
	39 Управление качеством, например в соответствии с ИСО—9000	—	КР (HR) высокий	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий
	40 Окончательная проверка и подтверждение соответствия прототипа FPGA/PLD в системе	—	КР (HR) высокий	КР (HR) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	41 Окончательная проверка и подтверждение соответствия при массовом произ-водстве, поэкземплярная проверка	—	Р (R) высокий	Р (R) высокий	КР* (HR*) высокий	КР* (HR*) высокий
	42 Отбраковочное испытание	E.40	Р (R) низкий	Р (R) средний	Р (R) высокий	КР* (HR*) высокий

Примечание — Согласно уровню полноты безопасности должны быть выбраны соответствующие методы/средства. Альтернативные или эквивалентные методы/средства обозначены буквой после числа. По крайней мере один из альтернативных или эквивалентных методов/средств должен быть применен.

Термин (V)HDL обозначает или язык описания аппаратных средств на сверхбыстродействующих интегральных схемах VHDL, или язык описания аппаратных средств Verilog.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных и европейского регионального стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного, европейского регионального 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 60947-5-1:2003	—	*
МЭК/ТС 61000-1-2:2008	—	*
МЭК 61326-3-1:2008	—	*
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
МЭК 61508-5:2010	IDT	ГОСТ Р МЭК 61508-5— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов опреде-ления уровней полноты безопасности»
МЭК 61508-6:2010	IDT	ГОСТ Р МЭК 61508-6— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3»
МЭК 61508-7:2010	IDT	ГОСТ Р МЭК 61508-7— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
МЭК 61784—3:2010	—	*
МЭК 62280—1:2002	—	*
МЭК 62280—2:2002	—	*
ЕН 50205	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного (европейского регионального) 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	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]	IEC 60300-3-2	Dependability management — Part 3-2: Application guide — Collection of dependability data from the field
[6]	ISO 14224	Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment
[7]	IEC 61164	Reliability growth — Statistical test and estimation methods
[8]	IEC 62308	Equipment reliability — Reliability assessment methods
[9]	IEC 61000-6-2	Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments

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

Ключевые слова: функциональная безопасность; жизненный цикл систем; электрические компоненты; электронные компоненты; программируемые электронные компоненты и системы; системы, связанные с безопасностью; управление функциональной безопасностью; требования к жизненному циклу безопасности; оценка функциональной безопасности

Редактор *П.М. Смирнов*
Технический редактор *А.И. Белов*
Корректор *И.А. Белова*
Компьютерная верстка *А.С. Шаповаловой*

Сдано в набор 15.12.2013. Подписано в печать 20.03.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 9,77. Уч.-изд. л. 7,62. Тираж 81 экз. Зак. 2056.

Набрано в Издательском доме «Вебстер»
www.idvebster.ru project@idvebster.ru

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