ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-2— 2007

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

Часть 2

Требования к системам

IEC 61508-2:2000
Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
(IDT)

Издание официальное

БЗ 4—2007/63

Москва
Стандартинформ
2008

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 27 декабря 2007 г. № 581-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-2:2000 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам» (IEC 61508-2:2000 «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 D

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2008

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 3
3 Термины и определения . . . 3
4 Соответствие настоящему стандарту . . . 3
5 Документация . . . 3
6 Управление функциональной безопасностью . . . 4
7 Требования к жизненному циклу безопасности E/E/PES . . . 4
8 Оценка функциональной безопасности . . . 30
Приложение A (обязательное) Методы и средства для E/E/PE систем, связанных с безопасностью: управление отказами в процессе эксплуатации . . . 31
Приложение B (обязательное) Методы и средства для E/E/PE систем, связанных с безопасностью: предотвращение систематических отказов в течение различных стадий жизненного цикла . . . 45
Приложение C (обязательное) Диагностический охват и доля безопасных отказов . . . 54
Приложение D (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 56
Библиография . . . 57

Введение

Системы, состоящие из электрических и/или электронных компонентов, в течение многих лет используются для выполнения функций безопасности в большинстве областей применения. Компьютерные системы [обычно называемые программируемыми электронными системами (PES)], использующиеся во всех областях применения для выполнения задач, не связанных с безопасностью, во все возрастающих масштабах используются для решения задач обеспечения безопасности. Для эффективной и безопасной эксплуатации технологий, основанных на использовании компьютерных систем, чрезвычайно важно, чтобы лица, ответственные за принятие решений, имели в своем распоряжении руководство по вопросам безопасности, которое они могли бы использовать в своей работе.

Настоящий стандарт устанавливает общий подход к вопросам обеспечения безопасности всего жизненного цикла систем, состоящих из электрических и/или электронных, и/или программируемых электронных компонентов [электрических/электронных/программируемых электронных систем (E/E/PES)], которые используются для выполнения функций безопасности. Этот общий подход был принят для того, чтобы разработать рациональную и последовательную техническую концепцию для всех электрических систем, связанных с безопасностью. Основной целью настоящего стандарта является содействие разработке стандартов для их применения в различных предметных областях.

Обычно безопасность систем достигается за счет использования в них нескольких систем защиты, в которых используются различные технологии (например механические, гидравлические, пневматические, электрические, электронные, программируемые электронные). Следовательно, любая стратегия безопасности должна учитывать не только все элементы, входящие в состав отдельных систем (например, датчики, управляющие устройства и исполнительные механизмы), но также и все подсистемы, связанные с безопасностью, входящие в состав комбинированной системы, связанной с безопасностью. Таким образом, хотя настоящий стандарт в основном распространяется на электрические/электронные/программируемые электронные (E/E/PE) системы, связанные с безопасностью, он может также дать представление об общей структуре, в рамках которой рассматриваются системы, связанные с безопасностью, основанные на других технологиях.

Признанным фактом является существование огромного разнообразия применений E/E/PES в различных предметных областях, отличающихся разной степенью сложности, опасностями и возможными рисками. В каждом конкретном применении использование необходимых мер безопасности будет зависеть от многочисленных факторов, специфичных для этого конкретного применения. Настоящий стандарт, являясь базовым, позволяет формулировать такие меры для вновь разрабатываемых международных стандартов для различных предметных областей.

Настоящий стандарт:

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

- разработан с учетом быстрого развития технологий; его структура является достаточно устойчивой и полной для удовлетворения потребностей разработок, которые могут появиться в будущем;

- делает возможной разработку стандартов областей применения, в которых используются системы E/E/PES; разработка стандартов для областей применения в рамках общей структуры, вводимой настоящим стандартом, должна приводить к более высокому уровню согласованности (например основные принципы, терминология и т.п.) как для отдельных областей применения, так и для их совокупности; это дает преимущества как для безопасности, так и в сфере экономики;

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

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

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

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

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

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

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

Примечание — Конкретная E/E/PE система, связанная с безопасностью, не обязательно предполагает одноканальную архитектуру;

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

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 — 2008—09—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 E/E/PE систем, связанных с безопасностью (включая сенсоры, исполнительные устройства и интерфейс человек — машина);

d) определяет способ использования информации, полученной в соответствии с МЭК 61508-1, описывающей полные требования к безопасности и их распределение по E/E/PE системам, связанным с безопасностью, а также определяет, как полные требования к безопасности преобразуются в требования к функциям безопасности E/E/PES и в требования к полноте безопасности E/E/PES;

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

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

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

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

Примечания

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

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

1.2 МЭК 61508-1 — МЭК 61508-4 являются основополагающими стандартами по безопасности, хотя это не применяется в контексте E/E/PE систем, связанных безопасностью, имеющих небольшую сложность (см. МЭК 61508-4, пункт 3.4.4). В качестве основополагающих стандартов по безопасности данные стандарты предназначены для использования техническими комитетами при подготовке стандартов в соответствии с Руководствами МЭК 104:1997 и ИСО/МЭК Руководство 51:1999. Стандарты серии МЭК 61508 предназначены также для использования в качестве самостоятельных стандартов.

Издание официальное

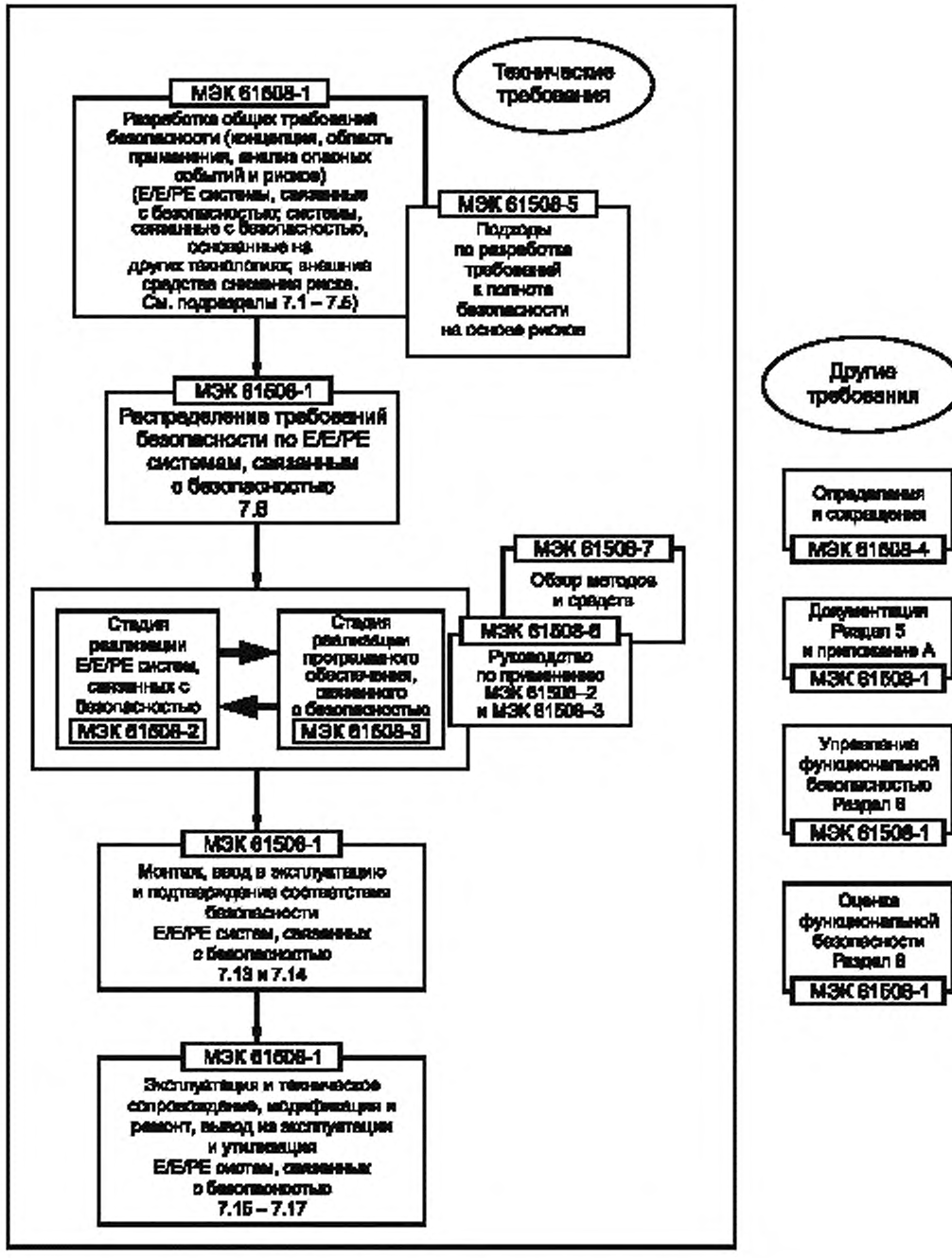


Рисунок 1 — Общая структура настоящего стандарта

В обязанности технического комитета входит использование (где возможно) базовых стандартов по безопасности при подготовке собственных стандартов. В этом случае требования, методы или условия проверки настоящего базового стандарта по безопасности не будут применяться, если это не указано специально, или будут включаться в стандарты, подготовленные этими техническими комитетами.

Примечания

1 Функциональная безопасность систем E/E/PE, 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.

2 В США и Канаде до тех пор, пока стандарты для конкретного сектора применения стандартов МЭК 61508 (например МЭК 61511 [1]) не будут опубликованы в качестве международных стандартов США и Канады, существующие там национальные стандарты по безопасности в обрабатывающих секторах, основанные на МЭК 61508, могут быть применены вместо МЭК 61508.

1.3 Структура серии стандартов МЭК 61508-1 — МЭК 61508-7 показана на рисунке 1, а также указана роль МЭК 61508-2 в достижении функциональной безопасности E/E/PE систем, связанных с безопасностью. МЭК 61508-6 (приложение А) содержит описание применения МЭК 61508-2 и МЭК 61508-3.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

МЭК 60050-371:1984 Международный электротехнический словарь. Глава 371. Телеуправление

МЭК 60300-3-2:2004 Управление общей надежностью. Часть 3. Руководство по применению. Полевой сбор данных по общей надежности

МЭК 61000-1-1:1992 Электромагнитная совместимость (ЭМС). Часть 1. Общие положения — Раздел 1: Применение и интерпретация фундаментальных определений и терминов

МЭК 61000-2-5:1995 Электромагнитная совместимость (ЭМС). Часть 2. Окружение. Раздел 5. Классификация электромагнитного окружения

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

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

МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

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

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

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

ИСО/МЭК 51:1999 Руководство по включению в стандарты аспектов, связанных с безопасностью

МЭК Руководство 104:1997 Руководство по подготовке стандартов, связанных с безопасностью, и по роли комитетов с функциями определения направлений и разработки стандартов в области безопасности

IEEE 352:1987 Руководство IEEE по основным принципам анализа надежности систем безопасности атомных энергетических станций

3 Термины и определения

В настоящем стандарте применены термины по МЭК 61508-4.

4 Соответствие настоящему стандарту

Требования соответствия настоящему стандарту — по МЭК 61508-1 (см. раздел 4).

5 Документация

Требования к документации — по МЭК 61508-1 (см. раздел 5).

6 Управление функциональной безопасностью

Требования по управлению функциональной безопасностью по МЭК 61508-1 (см. раздел 6).

7 Требования к жизненному циклу безопасности E/E/PES

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 безопасности E/E/PES.

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

7.1.1.2 Для каждой стадии жизненного цикла безопасности E/E/PES (см. таблицу 1) указаны:
- цели, которые должны быть достигнуты;
- область применения стадии;
- ссылка на пункт, содержащий требования;
- входы стадии;
- выходы стадии.

Таблица 1 — Обзор стадии реализации жизненного цикла безопасности E/E/PES

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область применения	Пункт требований	Вход	Выход
9.1 Спецификация требований безопасности E/E/PES	Определение требований для каждой E/E/PE системы, связанной с безопасностью, в терминах требований к функциям безопасности и требований к полноте безопасности для достижения требуемой функциональной безопасности	E/E/PE системы, связанные с безопасностью	7.2.2	Описание распределения требований безопасности (см. МЭК 61508-1, подраздел 7.6)	Требования безопасности E/E/PES. Требования безопасности программного обеспечения как входная спецификация требований к безопасности программного обеспечения
9.2 Планирование подтверждения соответствия безопасности E/E/PES	Планирование подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью	E/E/PE системы, связанные с безопасностью	7.2.3	Требования безопасности E/E/PES	План подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью
9.3 Разработка и создание E/E/PES	Создание E/E/PE систем, связанных с безопасностью, отвечающих требованиям к функциям безопасности и полноте безопасности	E/E/PE системы, связанные с безопасностью	7.4.2 — 7.4.8	Требования безопасности E/E/PES	Разработка E/E/PE систем, связанных с безопасностью, в соответствии с требованиями безопасности E/E/PES. План тестирования интеграции E/E/PES. Информация об архитектуре E/E/PES как входная спецификация требований к программному обеспечению

Продолжение таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область применения	Пункт требований	Вход	Выход
9.4 Интеграция E/E/PES	Интеграция и тестирование E/E/PE систем, связанных с безопасностью	E/E/PE системы, связанные с безопасностью	7.5.2	Разработка E/E/PES. План интеграции E/E/PES. Программируемая электроника и программное обеспечение	Полностью функционирующие E/E/PE системы, связанные с безопасностью, в соответствии с разработанной E/E/PES. Результаты тестирования интеграции E/E/PES
9.5 Процедуры установки E/E/PES, ввода в эксплуатацию, эксплуатации и технической поддержки	Разработка процедур для гарантирования того, что функциональная безопасность E/E/PE систем, связанных с безопасностью, поддерживается в период эксплуатации и технического обслуживания	E/E/PE системы, связанные с безопасностью управляемого оборудования	7.6.2	Требования безопасности E/E/PES. Разработка E/E/PES	Установка E/E/PES, ввод в эксплуатацию, эксплуатация и процедуры технического обслуживания для каждой отдельной E/E/PES
9.6 Подтверждение соответствия безопасности E/E/PES	Подтверждение соответствия того, что E/E/PE системы, связанные с безопасностью, во всех отношениях отвечают требованиям безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	E/E/PE системы, связанные с безопасностью	7.7.2	Требования безопасности E/E/PES. План подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью	E/E/PE системы, связанные с безопасностью с полным подтверждением соответствия безопасности. Результаты подтверждения соответствия безопасности E/E/PES
Модификация E/E/PES	Осуществление коррекции, расширения или адаптации E/E/PE систем, связанных с безопасностью, с гарантией того, что достигается и поддерживается требуемый уровень полноты безопасности	E/E/PE системы, связанные с безопасностью	7.8.2	Требования безопасности E/E/PES	Результаты модификации E/E/PES
Верификация E/E/PES	Тестирование и оценка выходной информации данной стадии, чтобы гарантировать правильность и соответствие в отношении продукции и стандартов, используемых в качестве входов к этой стадии	E/E/PE системы, связанные с безопасностью	7.9.2	Зависящие от стадии требования безопасности E/E/PES. План верификации E/E/PE систем, связанных с безопасностью, для каждой стадии	Результаты верификации E/E/PE систем, связанных с безопасностью, для каждой стадии

Окончание таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область применения	Пункт требований	Вход	Выход
Оценка функциональной безопасности E/E/PES	Исследование и получение заключения по функциональной безопасности, достигнутой с помощью E/E/PE систем, связанных с безопасностью	E/E/PE системы, связанные с безопасностью	8	План оценки функциональной безопасности E/E/PES	Результаты оценки функциональной безопасности E/E/PES

7.1.2 Цели

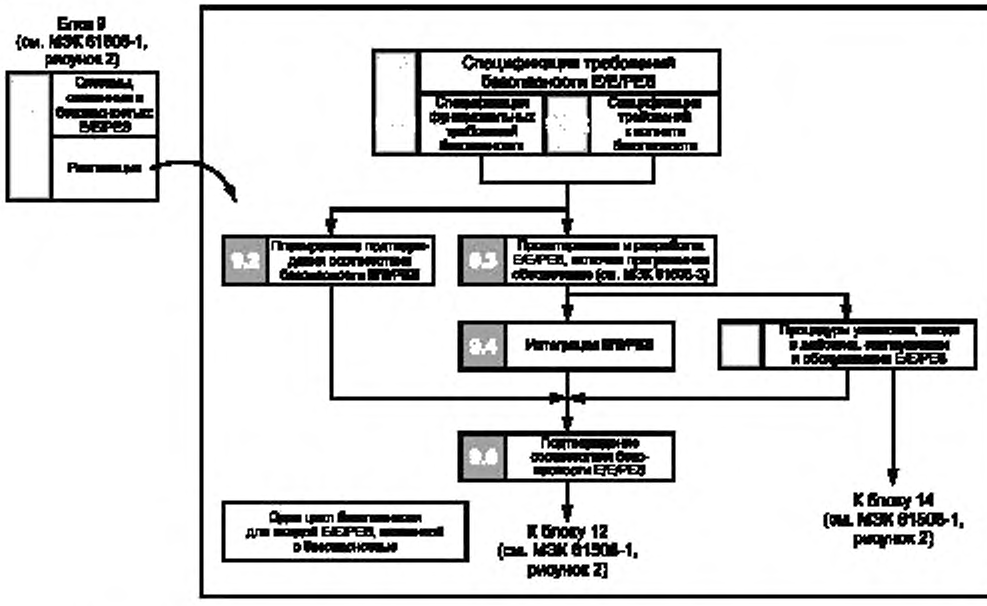
7.1.2.1 Первая цель настоящего подраздела состоит в структурировании на систематической основе стадий полного жизненного цикла безопасности E/E/PES, которые должны быть рассмотрены для достижения требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью.

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

7.1.3 Требования

7.1.3.1 Жизненный цикл безопасности E/E/PES, используемый в качестве требования соответствия настоящему стандарту, представлен на рисунке 2. В случае использования другого жизненного цикла E/E/PES он должен быть определен на этапе планирования функциональной безопасности E/E/PES (см. МЭК 61508-1, раздел 6), а также должны быть достигнуты все цели и требования каждого подраздела настоящего стандарта.

Примечание — Взаимосвязь и области применения настоящего стандарта и МЭК 61508-3 показаны на рисунке 3.



Примечание — См. также МЭК 61508-6, раздел А.2, перечисление b).

Рисунок 2 — Жизненный цикл безопасности E/E/PES (стадия реализации)

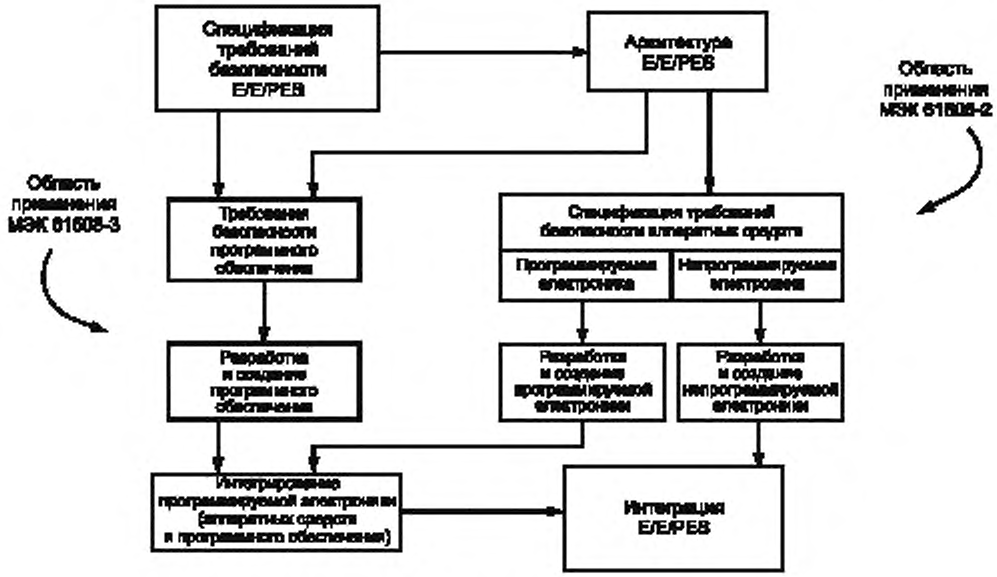


Рисунок 3 — Взаимосвязь и области применения МЭК 61508-2 и МЭК 61508-3

7.1.3.2 Процедуры управления функциональной безопасностью (см. МЭК 61508-1, раздел 6) должны осуществляться параллельно стадиям жизненного цикла безопасности E/E/PES.

7.1.3.3 Каждую стадию жизненного цикла безопасности E/E/PES подразделяют на элементарные действия с определением для каждой стадии области применения, входов и выходов (см. таблицу 1).

7.1.3.4 Выходы каждой стадии жизненного цикла E/E/PES должны быть документированы (если иное не будет обосновано на стадии планирования функциональной безопасности, см. МЭК 61508-1, раздел 5).

7.1.3.5 Выходы каждой стадии жизненного цикла E/E/PES должны отвечать определенным для этой стадии целям и требованиям (см. 7.2 — 7.9).

7.2 Спецификация требований безопасности E/E/PES

Примечание — Эта стадия представлена на рисунке 2 (блок 9.1).

7.2.1 Цель

Цель настоящего пункта состоит в задании требований к каждой E/E/PE системе, связанной с безопасностью, в терминах требований к функциям безопасности и к полноте безопасности для достижения требуемой функциональной безопасности.

Примечание — Например, для функций безопасности может потребоваться приведение управляемого оборудования в безопасное состояние или в состояние технического обслуживания.

7.2.2 Общие требования

7.2.2.1 Спецификация требований безопасности E/E/PES должна формироваться исходя из распределения требований безопасности, как определено в МЭК 61508-1 (подраздел 7.6), а также учитывать требования, определенные в ходе планирования функциональной безопасности (см. МЭК 61508-1, раздел 6). Эта информации должна быть доступна разработчику E/E/PES.

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

7.2.2.2 Требования к функциональной безопасности E/E/PES должны быть выражены и структурированы, 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 безопасности E/E/PES.

7.2.2.3 Спецификация требований безопасности E/E/PES должна содержать требования к функциям безопасности E/E/PES (см. 7.2.3.1) и требования к полноте безопасности E/E/PES (см. 7.2.3.2).

7.2.3 Требования к безопасности E/E/PES

7.2.3.1 Спецификация требований к функциям безопасности должна содержать:

a) описание всех функций безопасности, необходимых для достижения функциональной безопасности, которое для каждой функции безопасности должно:

- обеспечивать всесторонние подробные требования, достаточные для проектирования и разработки E/E/PE систем, связанных с безопасностью,
- включать в себя методы, с помощью которых E/E/PE системы, связанные с безопасностью, достигают или поддерживают безопасное состояние управляемого оборудования,
- определять, требуется ли непрерывное управление, и что приводит к достижению или поддержанию безопасного состояния управляемого оборудования,
- определять, к какому режиму применима функция безопасности E/E/PE системы, связанной с безопасностью, — к режиму с низкой частотой обращения или к режиму с высокой частотой обращения, или к режиму с непрерывным обращением;

b) характеристики производительности и времени реакции системы;

c) сведения об интерфейсах E/E/PE системы, связанной с безопасностью, с обслуживающим персоналом, необходимые для достижения требуемой функциональной безопасности;

d) информацию, относящуюся к функциональной безопасности, которая может повлиять на проектирование E/E/PE системы, связанной с безопасностью;

e) сведения об интерфейсах E/E/PE систем, связанных с безопасностью с любыми другими системами (внутренними, внешними, управляемым оборудованием);

f) описание всех используемых режимов работы управляемого оборудования, в том числе:

- подготовки к эксплуатации, включая монтаж и наладку;
- запуска в эксплуатацию, обучения, автоматический, ручной, полуавтоматический, стационарный рабочий режимы работы;
- стационарного нерабочего режима работы, переустановки, останова, технического обслуживания,
- режима работы при разумно предсказуемых ненормальных условиях.

Примечания

1 Разумно предсказуемые ненормальные условия работы управляемого оборудования являются разумно предсказуемыми для разработчиков или пользователей.

2 Для конкретных режимов работы управляемого оборудования могут потребоваться дополнительные функции безопасности (например монтаж, настройка или техническое обслуживание), чтобы безопасно выполнить эти работы;

g) подробное описание всех требуемых режимов поведения E/E/PE 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 (при необходимости); любые необходимые ограничения между аппаратными средствами и программным обеспечением должны быть идентифицированы и документированы.

Примечание — Если эти взаимодействия не известны до завершения разработки, устанавливают только общие ограничения;

i) предельные и ограничивающие условия для E/E/PE систем, связанных с безопасностью, и связанных с ними подсистем, например временные ограничения;

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

7.2.3.2 Спецификация требований к полноте безопасности должна включать в себя:

a) уровень полноты безопасности для каждой функции безопасности и, при необходимости (см. примечание 2), требуемую целевую меру отказов функции безопасности.

Примечания

1 Уровень полноты безопасности функции безопасности задает целевую меру отказов в соответствии с МЭК 61508-1 (см. таблицы 2 и 3).

2 Целевую меру отказов функции безопасности определяют, если требуемое снижение риска для функции безопасности получено с использованием количественного метода (см. МЭК 61508-1, подпункт 7.5.2.2);

b) режим работы (с низкой частотой запросов или с высокой частотой запросов/с непрерывными запросами) каждой функции безопасности;

c) требования, ограничения, функции и доступность проведения контрольных испытаний E/E/PE систем, связанных с безопасностью;

d) экстремальные значения всех условий окружающей среды в течение жизненного цикла безопасности E/E/PES, включая производство, хранение, транспортировку, испытание, установку, ввод в эксплуатацию, эксплуатацию и техническое обслуживание;

e) пределы электромагнитной устойчивости (см. МЭК 61000-1-1), необходимые для достижения электромагнитной совместимости; пределы электромагнитной устойчивости формируются с учетом как электромагнитной окружающей обстановки (см. МЭК 61000-2-5), так и уровней требуемой полноты безопасности.

Примечания

1 Важно отметить, что уровень полноты безопасности учитывается при определении пределов электромагнитной устойчивости, тем более, что электромагнитные возмущения в окружающей среде распределяются случайно. На практике невозможно определить абсолютный уровень электромагнитного возмущения, а определяют только уровень, который предположительно не будет превышен (уровень электромагнитной совместимости). К сожалению, на практике вероятность, связанную с этим предположением, очень трудно определить. Поэтому предел электромагнитной устойчивости не гарантирует, что E/E/PE система, связанная с безопасностью, не откажет из-за электромагнитного возмущения; он гарантирует лишь некоторый уровень доверия того, что такой отказ не произойдет. Фактический уровень доверия — это функция предела электромагнитной устойчивости по отношению к статистическому распределению уровней электромагнитного возмущения в окружающей среде. Для более высоких уровней полноты безопасности может оказаться необходимым более высокий уровень доверия, что означает, что его нижняя граница, из-за которой предел электромагнитной устойчивости выходит за пределы уровня электромагнитной совместимости, должна быть выше для более высоких уровней полноты безопасности.

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.

3 При разработке спецификации на требования безопасности E/E/PES должны быть учтены условия использования E/E/PE систем, связанных с безопасностью. 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 интервалов для контролируемых применений.

7.2.3.3 Во избежание ошибок во время составления спецификации требований безопасности E/E/PES используют группу методов и средств в соответствии с таблицей В.1 (приложение В).

7.3 Планирование подтверждения соответствия безопасности E/E/PES

Примечание — Данная стадия представлена на рисунке 2 (см. блок 9.2). Она обычно выполняется параллельно с проектированием и разработкой E/E/PES (см. 7.4).

7.3.1 Цель

Целью настоящего пункта является планирование подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью.

7.3.2 Требования

7.3.2.1 Планирование для определения шагов (процедурных и технических) должно осуществляться для демонстрации соответствия E/E/PE систем, связанных с безопасностью, спецификациям требований к безопасности E/E/PES (см. 7.2).

Примечание — Планирование подтверждения соответствия программного обеспечения — в соответствии с МЭК 61508-3.

7.3.2.2 При планировании подтверждения соответствия E/E/PE систем, связанных с безопасностью, должны быть использованы:

a) требования, определенные в спецификации требований безопасности E/E/PES;

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

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

d) 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 заданных в спецификации пределов электромагнитной устойчивости.

Примечание — Руководство по спецификации испытаний пределов электромагнитной устойчивости в соответствии с МЭК 61000-2-5 и МЭК 61000-4 [2].

g) стратегии по устранению подтвержденного отказа.

7.4 Проектирование и разработка E/E/PES

Примечание — Данная стадия представлена на рисунке 2 (см. блок 9.3). Она обычно выполняется параллельно с планированием подтверждения соответствия безопасности E/E/PES (см. 7.3).

7.4.1 Цель

Цель требований настоящего подраздела состоит в гарантировании соответствия проектирования и разработки E/E/PE систем, связанных с безопасностью, заданным требованиям функций безопасности и требованиям полноты безопасности (см. 7.2).

7.4.2 Общие требования

7.4.2.1 Проектирование E/E/PE систем, связанных с безопасностью, должно быть выполнено в соответствии со спецификацией требований безопасности (см. 7.2) с учетом требований настоящего подраздела.

7.4.2.2 Проектирование E/E/PE систем (см. рисунок 4), связанных с безопасностью (включая полную архитектуру аппаратных средств и программного обеспечения; сенсоры; исполнительные устройства; программируемую электронику; встроенное программное обеспечение, «зашитое» в ПЗУ; прикладное программное обеспечение и т.п.), должно быть таким, чтобы отвечать перечисленным ниже требованиям к:

a) полноте безопасности аппаратных средств:

- требования к архитектурным ограничениям на полноту безопасности аппаратных средств (см. 7.4.3.1) и

- требования к вероятности опасных случайных отказов аппаратных средств (см. 7.4.3.2);

b) систематической полноте безопасности:

- требования по предотвращению отказов (см. 7.4.4) и требования по управлению систематическими отказами (см. 7.4.5) или

- требования к подтверждению того, что оборудование «проверено в эксплуатации» (см. 7.4.7.6 — 7.4.7.12);

c) поведению системы при обнаружении ошибок (см. 7.4.6).

Примечания

1 Общий подход к полноте безопасности E/E/PES основан на общем методе выбора проектного подхода, обеспечивающего достижение уровня полноты безопасности (как для полноты безопасности аппаратных средств, так и для систематической полноты безопасности) в E/E/PE системах, связанных с безопасностью, в ходе которого:

- определяют требуемый уровень полноты безопасности функций безопасности (см. МЭК 61508-1);

- устанавливают, что полнота безопасности аппаратных средств равна систематической полноте безопасности и равна уровню полноты безопасности (см. 7.4.3.2.1);

- для полноты безопасности аппаратных средств определяют архитектуру, соответствующую ограничениям на нее (см. 7.4.3.1), и демонстрируют соответствие вероятности отказа функций безопасности из-за случайных отказов аппаратных средств требуемым целевым значениям (см. 7.4.3.2);

- для систематической полноты безопасности выделяют особенности проектирования, которые приводят к систематическим сбоям в реальной работе (см. 7.4.5) или подтверждают соответствие требованиям «проверено при эксплуатации» (см. 7.4.7.6 — 7.4.7.12) и

- для систематической полноты безопасности выделяют методы и средства, исключающие (не допускающие) систематические сбои в процессе проектирования и разработки (см. 7.4.4) или подтверждают соответствие требованиям «проверено при эксплуатации» (см. 7.4.7.6 — 7.4.7.12).

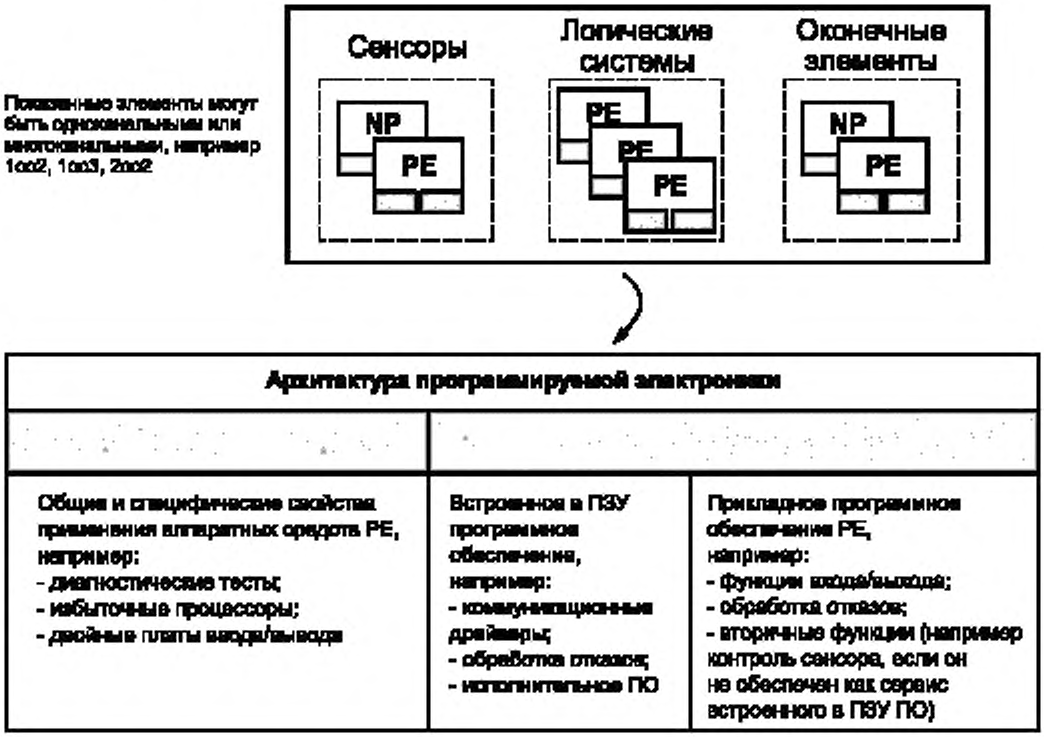
2 МЭК 61508-3 содержит:

- требования к архитектуре программного обеспечения (см. 7.4.2.2),

- требования к производству программируемой электроники и спецификации тестирования интеграции программного обеспечения (см. 7.5) и

- требования к интеграции программируемой электроники и программного обеспечения в соответствии со спецификацией тестирования интеграции программного обеспечения (см. 7.5).

Во всех случаях требуется тесная кооперация между производителем E/E/PE систем, связанных с безопасностью, и производителем программного обеспечения.



PE — программируемая электроника; NP — непрограммируемые устройства; АС — аппаратные средства; ПО — программное обеспечение, ПЗУ — программируемое запоминающее устройство, MooN — M из N (например 1oo2 означает один из двух)

Рисунок 4 — Соотношение между архитектурами аппаратных средств и программного обеспечения программируемой электроники

7.4.2.3 Когда E/E/PE система, связанная с безопасностью, осуществляет функции безопасности и функции, не относящиеся к безопасности, 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). Функции, связанные с безопасностью, везде, где практически возможно, должны быть отделены от функций, не относящихся к безопасности.

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 E/E/PE системе, связанной с безопасностью. Такое объединение, допускаемое настоящим стандартом, может привести к большим сложностям при выполнении работ в процессе жизненного цикла E/E/PE 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 доказано, 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 E/E/PE 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 задокументированы:

a) метод достижения независимости;

b) обоснование метода.

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

7.4.2.7 Разработчик E/E/PE системы, связанной с безопасностью, должен еще раз пересмотреть требования к программному обеспечению и аппаратным средствам с тем, чтобы убедиться, что они корректно специфицированы. В частности, разработчик E/E/PES должен рассмотреть:

a) функции безопасности,

b) требования к полноте безопасности E/E/PE системы, связанной с безопасностью;

c) интерфейсы между оборудованием и обслуживающим персоналом.

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

7.4.2.9 Проектная документация на E/E/PE систему, связанную с безопасностью, должна обосновывать методы и средства, выбранные для формирования их интегрированного набора, обеспечивающего требуемый уровень полноты безопасности.

Примечание — Выбор общего подхода, использующего независимое письменное одобрение E/E/PES, связанных с безопасностью (включая сенсоры, датчики и т.д.), для технических средств и программного обеспечения, диагностических тестов и инструментов программирования и использование (где это возможно) подходящих языков программирования позволяет сократить сложность инженерного применения E/E/PES.

7.4.2.10 В процессе проектирования и разработки E/E/PE системы, связанной с безопасностью, все значимые (допустимые) взаимодействия аппаратных средств и программного обеспечения должны быть идентифицированы, оценены и документированы.

7.4.2.11 Проект E/E/PE системы, связанной с безопасностью, должен быть основан на декомпозиции на подсистемы, каждая из которых имеет специфицированный проект и набор тестов интеграции (см. 7.4.7).

Примечания

1 Конкретная подсистема может состоять из единственного компонента или группы компонентов. Полная E/E/PE 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. 7.4.7.3).

2 Везде, где это практически возможно, должны быть использованы существующие проверенные подсистемы. Это положение является в общем случае верным, только если существует почти 100 %-ное совпадение функциональных возможностей, пропускной способности и производительности существующей подсистемы с новыми требованиями или верифицированная (проверенная) подсистема структурирована таким образом, что пользователь может выбрать лишь требуемые функции, пропускную способность и производительность для специфического применения. Избыточные функциональные возможности, пропускная способность или производительность могут быть вредными для безопасности системы, если существующие подсистемы чрезмерно усложнены или имеют неиспользуемые возможности и если не может быть обеспечена защита от непреднамеренных функций.

7.4.2.12 Если подсистема имеет многоканальный выход, необходимо определить наличие какой-либо комбинации выходных состояний, которые могут быть вызваны отказом самой E/E/PE систе-

мы, связанной с безопасностью, способной непосредственно вызвать событие опасного отказа (см. анализ опасностей и рисков в МЭК 61508-1, подпункт 7.4.2.10). Если это определено, то предотвращение такой комбинации выходных состояний должно быть расценено как функция безопасности, работающая в режиме с высокой частотой обращения или с непрерывными обращениями (см. 7.4.6.3 и 7.4.3.2.5).

7.4.2.13 Для любых компонентов E/E/PE системы, связанной с безопасностью, в максимальной степени должно использоваться ограничение допустимых значений (см. МЭК 61508-7, подраздел 2.8). Обоснование работы на пределах любых компонентов должно быть документировано (см. МЭК 61508-1, раздел 5).

Примечание — При ограничении допустимых значений должен использоваться коэффициент ограничения, равный 0,67.

7.4.3 Требования к полноте безопасности аппаратных средств

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

7.4.3.1 Архитектурные ограничения полноты безопасности аппаратных средств

7.4.3.1.1 В контексте полноты безопасности аппаратных средств наиболее высокий уровень полноты безопасности, который может потребоваться для функции безопасности, ограничивается отказоустойчивостью аппаратных средств и составляющей безопасных отказов подсистем, которые выполняют эту функцию безопасности (см. приложение С). Наибольший уровень полноты безопасности, который может потребоваться для функции безопасности, использующей подсистему, с учетом отказоустойчивости аппаратных средств и составляющей безопасных отказов этой подсистемы представлен в таблицах 2 и 3 (см. также приложение С). Требования таблиц 2 и 3 должны применяться к каждой подсистеме, выполняющей функцию безопасности, и, следовательно, к каждой части E/E/PE системы, связанной с безопасностью. Подпункты 7.4.3.1.2 — 7.4.3.1.4 определяют, какая из таблиц 2 или 3 применяется к конкретной подсистеме. Подпункты 7.4.3.1.5 и 7.4.3.1.6 определяют самый высокий уровень полноты безопасности, который может быть применен к функции безопасности по запросу. В соответствии с этими требованиями:

a) отказоустойчивость аппаратных средств *N* означает, что отказ *N* + 1 может привести к потере функции безопасности. В определении отказоустойчивости не должны учитываться средства, которые могли бы управлять влиянием ошибок, например диагностика, и

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

c) в определении отказоустойчивости некоторые ошибки могут быть исключены при условии, что вероятность их возникновения очень мала по отношению к требованиям полноты безопасности подсистемы. Любые исключения ошибок должны быть обоснованы и документированы (см. примечание 3);

d) долю безопасных отказов подсистемы определяют как отношение суммы средних частот безопасных отказов и опасных отказов, обнаруженных тестами, к полной средней частоте отказов подсистемы (см. приложение С).

Примечания

1 Для получения достаточно отказоустойчивой архитектуры с учетом уровня сложности подсистемы используются архитектурные ограничения. Уровень полноты безопасности E/E/PE системы, связанной с безопасностью, полученный в результате применения требований настоящего подпункта, является максимальным из заявленных, хотя в некоторых случаях математически может быть определен более высокий уровень полноты безопасности, если для E/E/PE системы, связанной с безопасностью, принять исключительно математический подход.

2 Архитектура и подсистема, сформированные для соответствия требованиям отказоустойчивости аппаратных средств, должны быть такими, какие обычно используются в режиме эксплуатации. Требования отказоустойчивости могут быть снижены, если E/E/PE система, связанная с безопасностью, восстанавливается, находясь под управлением основного оборудования (on-line). Однако ключевые параметры, связанные с любым ослаблением, должны быть предварительно оценены (например среднее время восстановления по сравнению с вероятностью запроса).

3 Если некоторый компонент системы имеет очень низкую вероятность отказа благодаря присущим ему свойствам (например механический соединитель привода), то рассматривать ограничение (на основе отказоустойчивости аппаратных средств) полноты безопасности любой функции безопасности, для реализации которой используется этот компонент, нет необходимости.

7.4.3.1.2 Конкретная подсистема (см. 7.4.2.11, примечание 1) может быть отнесена к типу А, если для ее компонентов, необходимых для реализации функции безопасности:

a) виды отказов всех составляющих компонентов определены, и

b) поведение системы в условиях отказа может быть полностью определено, и

c) имеются достоверные эксплуатационные данные, показывающие, что частоты, требуемые для обнаруженных отказов и необнаруженных опасных отказов, реализованы (см. 7.4.7.3 и 7.4.7.4).

7.4.3.1.3 Конкретная подсистема (см. 7.4.2.11, примечание 1) должна быть отнесена к типу B, если для ее компонентов, необходимых для реализации функции безопасности:

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

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

c) нет достоверных эксплуатационных данных по подтверждению требований для частот обнаруженных отказов и необнаруженных опасных отказов (см. 7.4.7.3 и 7.4.7.4).

Примечание — Если, по крайней мере, один из компонентов конкретной подсистемы соответствует условиям для типа B, то такая подсистема должна быть отнесена к типу B, а не к типу A (см. также 7.4.2.11, примечание 1).

7.4.3.1.4 Архитектурные ограничения по таблице 2 или таблице 3 должны применяться к каждой подсистеме, выполняющей функцию безопасности так, чтобы:

a) требования отказоустойчивости аппаратных средств достигались для полной E/E/PE системы, связанной с безопасностью;

b) требования таблицы 2 применялись для любой подсистемы типа A, составляющей часть E/E/PE системы, связанной с безопасностью.

Примечание — Если E/E/PE система, связанная с безопасностью, содержит только подсистемы типа A, то требования, приведенные в таблице 2, следует применять к полной E/E/PE системе, связанной с безопасностью;

c) требования таблицы 3 применялись для любой подсистемы типа B, составляющей часть полной E/E/PE системы, связанной с безопасностью.

Примечание — Если E/E/PE система, связанная с безопасностью, содержит только подсистемы типа B, то требования, приведенные в таблице 3, будут применяться для полной системы, связанной с безопасностью;

d) требования таблиц 2 и 3 применялись к E/E/PE системам, связанным с безопасностью, содержащим оба типа подсистем A и B, поскольку требования таблицы 2 должны применяться к подсистемам типа A, а требования таблицы 3 — к подсистемам типа B.

Таблица 2 — Полнота безопасности аппаратных средств: архитектурные ограничения подсистем, связанных с безопасностью, типа A

Доля безопасных отказов	Отказоустойчивость аппаратных средств (см. примечание 2)		
	$N = 0$	$N = 1$	$N = 2$
< 60 %	SIL1	SIL2	SIL3
60 % — 90 %	SIL2	SIL3	SIL4
90 % — 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Примечания

1 Для детальной интерпретации этой таблицы см. 7.4.3.1.1 — 7.4.3.1.4.

2 Отказоустойчивость аппаратных средств N означает, что $N + 1$ отказ приведет к потере функции безопасности.

3 Расчет доли безопасных отказов см. в приложении C.

4 SIL — уровень полноты безопасности (см. МЭК 61508-1, подпункт 7.6.2.9, таблицы 2 и 3).

Таблица 3 — Полнота безопасности аппаратных средств: архитектурные ограничения подсистем, связанных с безопасностью, типа В

Доля безопасных отказов	Отказоустойчивость аппаратных средств (см. примечание 2)		
	$N = 0$	$N = 1$	$N = 2$
< 60 %	Не оговаривается	SIL1	SIL2
60 % — 90 %	SIL1	SIL2	SIL3
90 % — 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL2	SIL4	SIL4

Примечания

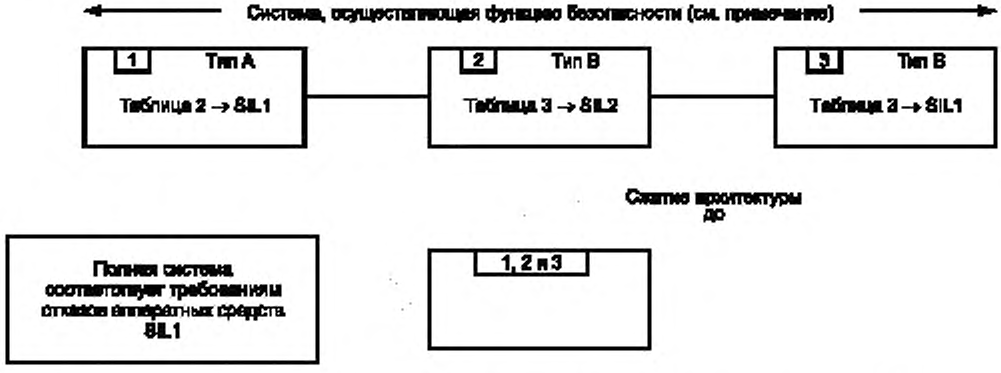
1 Для детальной интерпретации этой таблицы см. 7.4.3.1.1 — 7.4.3.1.4.

2 Отказоустойчивость аппаратных средств N означает, что $N + 1$ отказ приведет к потере функции безопасности.

3 Расчет доли безопасных отказов см. в приложении С.

4 SIL — уровень полноты безопасности (см. МЭК 61508-1, подпункт 7.6.2.9, таблицы 2 и 3).

7.4.3.1.5 BE/E/PE системах, связанных с безопасностью, в которых функция безопасности реализуется в одноканальной архитектуре (см. рисунок 5), максимальный уровень полноты безопасности аппаратных средств, который может быть достигнут для функции безопасности, определяется подсистемой аппаратных средств, отвечающей наименьшим требованиям полноты безопасности аппаратных средств (определяют по таблицам 2 и 3).



Примечание — Подсистемы, выполняющие функцию безопасности, считают полной E/E/PE системой, связанной с безопасностью, включая все элементы — от сенсоров до исполнительных устройств.

Рисунок 5 — Пример ограничения полноты безопасности аппаратных средств для одноканальной функции безопасности

Пример — Пусть система, в которой реализована конкретная функция безопасности, выполнена по одноканальной архитектуре, состоящей из подсистем 1, 2 и 3, типы которых указаны на рисунке 5, и эти подсистемы соответствуют требованиям таблиц 2 и 3 следующим образом:

- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL1;

- для подсистемы 2 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL2;

- для подсистемы 3 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL1.

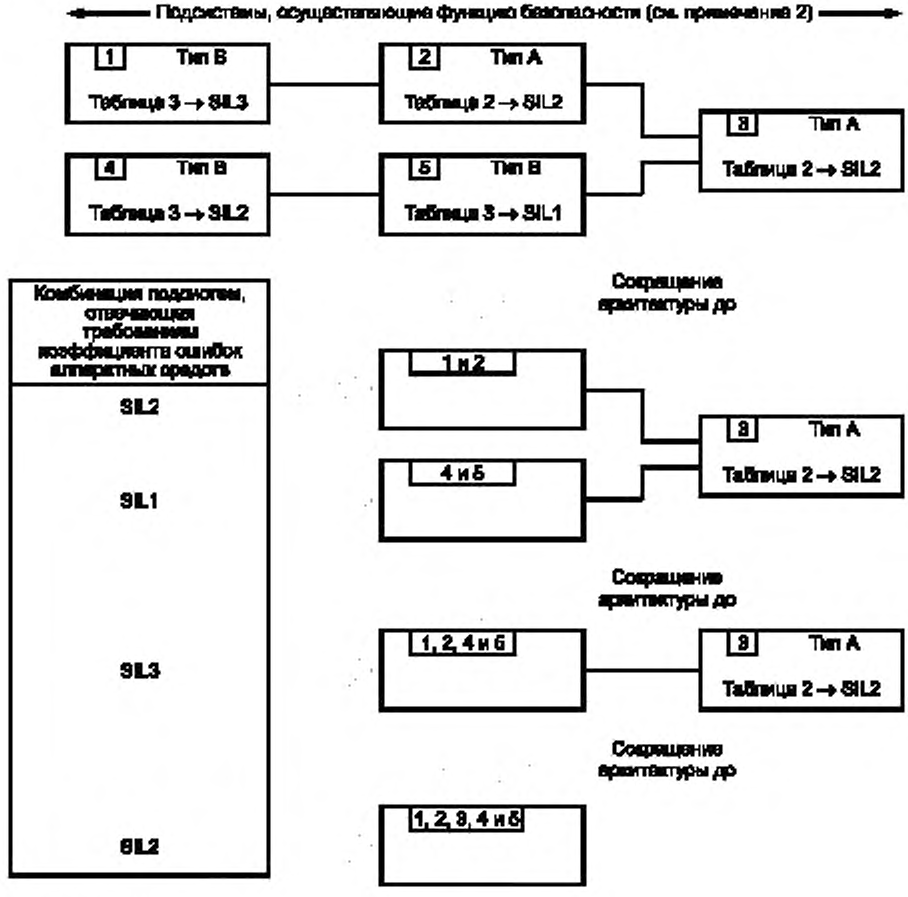
Для этой архитектуры каждая из подсистем 1 и 3 имеет уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равный SIL1, в то время как подсистема 2 имеет уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств, равный SIL2. Поэтому обе подсистемы 1 и 3 ограничивают уровень полноты безопасности, который может потребоваться для соблюдения отказоустойчивости аппаратных средств для рассматриваемой функции безопасности, до значения SIL1.

7.4.3.1.6 В E/E/PE системах, связанных с безопасностью, в которых функция безопасности реализуется в многоканальной архитектуре (см. рисунок 6), максимальный уровень полноты безопасности, который может быть достигнут для рассматриваемой функции безопасности, должен быть определен путем:

a) оценивания каждой подсистемы в соответствии с требованиями, представленными в таблицах 2 и 3 (см. 7.4.3.1.2 и 7.4.3.1.4);

b) группирования подсистем в комбинации и

c) анализа этих комбинаций для определения полного уровня полноты безопасности аппаратных средств.



Примечания

1 Подсистемы 1, 2 и подсистемы 4, 5 имеют одинаковые функциональные возможности в отношении функции безопасности и обеспечивают раздельные входы в подсистему 3.

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

Рисунок 6 — Пример ограничения полноты безопасности для многоканальной функции безопасности

Пример — Группирование и анализ этих комбинаций могут быть выполнены разными способами. Для иллюстрации одного из возможных методов примем архитектуру, в которой конкретная функция безопасности реализована либо комбинацией подсистем 1, 2 и 3, либо комбинацией подсистем 4, 5 и 3, как показано на рисунке 6. В этом случае комбинация подсистем 1 и 2 и комбинация подсистем 4 и 5 имеют одинаковые функциональные возможности в отношении функции безопасности и имеют раздельные входы в систему 3. В этом примере комбинация параллельных подсистем основывается на каждой подсистеме, реализующей требуемую часть функции безопасности, независимо от другой (параллельной) подсистемы. Функцию безопасности считают выполненной:

- при событии отказа в подсистеме 1 или подсистеме 2 (поскольку комбинация подсистем 4 и 5 позволяет реализовать функцию безопасности) или

- при событии отказа в подсистеме 4 или подсистеме 5 (поскольку комбинация подсистем 1 и 2 позволяет реализовать функцию безопасности).

Каждая подсистема удовлетворяет требованиям таблиц 2 и 3 следующим образом:

- для подсистемы 1 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL3;

- для подсистемы 2 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL2;

- для подсистемы 3 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL2;

- для подсистемы 4 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL2;

- для подсистемы 5 уровень полноты безопасности, соответствующий требованиям отказоустойчивости аппаратных средств и доле безопасных отказов, равен SIL1.

Далее более подробно рассмотрим процедуру определения максимального уровня полноты безопасности аппаратных средств, который может потребоваться для рассматриваемой функции безопасности:

a) Объединение подсистем 1 и 2

Отказоустойчивость и доля безопасных отказов, обеспеченная комбинацией подсистем 1 и 2 (каждая в отдельности соответствует требованиям для SIL3 и SIL2), соответствуют требованиям SIL2 (определенным подсистемой 2).

b) Объединение подсистем 4 и 5

Отказоустойчивость и доля безопасных отказов, обеспеченная комбинацией подсистем 4 и 5 (каждая в отдельности соответствует требованиям для SIL2 и SIL1), соответствуют требованиям SIL1 (определенным подсистемой 5).

c) Дальнейшее объединение комбинации подсистем 1 и 2 с комбинацией подсистем 4 и 5

Уровень полноты безопасности аппаратных средств в отношении отказоустойчивости аппаратных средств комбинации подсистем 1, 2, 4 и 5 определяется:

- решением, какая из комбинаций подсистем (т.е. комбинация подсистем 1 и 2 или 4 и 5) достигла самого высокого возможного уровня полноты безопасности аппаратных средств (в показателях соответствия требованиям отказоустойчивости), и

- анализом влияния другой комбинации подсистем на отказоустойчивость для комбинаций подсистем 1, 2, 4 и 5.

В данном примере комбинация подсистем 1 и 2 имеет максимально допустимое требование SIL2 (см. перечисление a)), в то время как комбинация подсистем 4 и 5 имеет максимально допустимое требование SIL1 (см. перечисление b)). Однако в случае отказа, встречающегося в комбинации подсистем 1 и 2, функция безопасности могла бы быть выполнена комбинацией подсистем 4 и 5. С учетом этого отказоустойчивость аппаратных средств, достигнутая комбинацией подсистем 1 и 2, увеличивается на единицу. Увеличение отказоустойчивости аппаратных средств на единицу приводит к увеличению на единицу уровня полноты безопасности аппаратных средств, которое может потребоваться (см. таблицы 2 и 3). Поэтому комбинация подсистем 1, 2, 4 и 5 имеет максимально допустимый уровень полноты безопасности в отношении отказоустойчивости и доли безопасных отказов, равный SIL3 (т.е. уровень полноты безопасности аппаратных средств, достигнутый комбинацией подсистем 1 и 2, SIL2 плюс единица).

d) Полная E/E/PE система, связанная с безопасностью

Уровень полноты безопасности аппаратных средств в отношении отказоустойчивости, который может потребоваться для рассматриваемой функции безопасности, определяют анализом комбинации подсистем 1, 2, 4 и 5 (которая достигает уровня отказоустойчивости, равного SIL3 (см. перечисление c)) и подсистемы 3 (которая достигает уровня отказоустойчивости, равного SIL2). Подсистема, достигшая самого низкого уровня полноты безопасности аппаратных средств (в данном случае подсистема 3), определяет максимальный уровень полноты безопасности всей E/E/PE системы,

связанной с безопасностью. Поэтому максимальный уровень полноты безопасности аппаратных средств в отношении отказоустойчивости аппаратных средств, который может быть достигнут для функции безопасности в данном примере, — SIL 2.

7.4.3.2 Требования к оценке вероятности отказа функций безопасности из-за случайных отказов аппаратных средств

7.4.3.2.1 Вероятность отказа каждой функции безопасности из-за случайных отказов аппаратных средств по 7.4.3.2.2 и 7.4.3.2.3 будет равна или менее целевой меры отказов, определенной в спецификации требований безопасности (см. 7.2.3.2).

Примечания

1 Для функции безопасности, выполняемой в режиме с низкой частотой запросов, целевая мера отказов будет выражена в терминах средней вероятности отказа выполнения по запросу предусмотренной функции безопасности, как определено уровнем полноты безопасности (см. МЭК 61508-1, таблица 2), пока требования в спецификации требований к полноте безопасности для функции безопасности E/E/PES (см. 7.2.3.2) не достигнут определенной целевой меры отказов, иной, чем конкретный SIL. Например, если целевая мера отказов равна $1,5 \times 10^{-6}$ (вероятность отказа по запросу), то есть заданному значению для удовлетворения требуемого снижения риска, то вероятность отказа по запросу функции безопасности, вызванного случайными отказами аппаратных средств должна быть равна или менее $1,5 \times 10^{-6}$.

2 Для функции безопасности, выполняемой в режиме с высокой частотой запросов или с непрерывными запросами, целевая мера отказов будет выражена в терминах средней вероятности опасного отказа в час, как определено уровнем полноты безопасности функции безопасности (см. МЭК 61508-1, таблица 3), пока требования в спецификации требований к полноте безопасности (см. 7.2.3.2) для функции безопасности E/E/PES не достигнут определенной целевой меры отказов, иной, чем конкретный SIL. Например, если целевая мера отказов равна $1,5 \times 10^{-6}$ (вероятность опасного отказа в час) и задана для выполнения требований по снижению риска, то вероятность отказа функции безопасности, вызванного случайными отказами аппаратных средств, должна быть равна или менее $1,5 \times 10^{-6}$.

3 Для демонстрации выполнения данного требования необходимо осуществить предсказание надежности для уместной функции безопасности, используя соответствующие средства (см. 7.4.3.2.2), и сравнить полученный результат с целевой мерой отказов конкретной полноты безопасности для уместной функции безопасности (см. МЭК 61508-1, таблицы 2 и 3).

7.4.3.2.2 Вероятность отказа каждой функции безопасности из-за случайных отказов аппаратных средств может быть оценена с учетом:

a) архитектуры E/E/PE системы, связанной с безопасностью, поскольку это касается каждой функции безопасности.

Примечание — При этом приходится решать, какие виды отказов 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) оцененной частоты (коэффициента) отказов каждой подсистемы в любых режимах, которые могли бы вызвать опасный отказ E/E/PE системы, связанной с безопасностью, но обнаружены диагностической проверкой (см. 7.4.7.3 и 7.4.7.4);

d) восприимчивости E/E/PE системы, связанной с безопасностью, к отказам по общей причине (см. примечание к настоящему перечислению и примечание 6 к перечислению h)).

Примечание — Например, см. МЭК 61508-6, приложение D;

e) охвата диагностическими тестами (по приложению C) и связанного с ним диагностического испытательного интервала.

Примечания

1 Время диагностического испытательного интервала вместе с последующим временем ремонта составляют среднее время восстановления, которое должно быть рассмотрено в модели надежности. Кроме того, для работы E/E/PE системы, связанной с безопасностью, в режиме высокой частоты запросов или с непрерывными запросами, где любые опасные отказы каналов приводят к опасным отказам E/E/PE системы, связанной с безопасностью, время диагностического испытательного интервала должно быть рассмотрено непосредственно (то есть дополнительно к среднему времени восстановления) в модели надежности, если его величина не является значительно меньшей, чем ожидаемая частота запросов (см 7.4.3.2.5).

2 При установлении времени диагностического испытательного интервала должны быть рассмотрены интервалы между всеми испытаниями, которые вносят вклад в диагностический охват.

f) интервалов времени, на которых реализуются испытательные (контрольные) интервалы для обнаружения опасных ошибок, не обнаруживаемых диагностическими тестами;

g) времени ремонта для обнаруженных отказов.

Примечание — Время ремонта составляет часть среднего времени восстановления (см. МЭС 191-13-08 [3]), включающего в себя также время обнаружения отказа и период времени, в течение которого ремонт невозможен (пример использования среднего времени восстановления для вычисления вероятности отказа приведен в МЭК 61508-6 (приложение В)). 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.

h) вероятности необнаруженного отказа любого процесса передачи данных (см. примечание 6 и подпункт 7.4.8.1).

Примечания

1 Упрощенный подход, который может быть использован для оценки вероятности опасного отказа функции безопасности из-за случайных отказов аппаратных средств для определения того, что аппаратура обеспечивает требуемую целевую меру отказов, представлен в МЭК 61508-6, приложение В.

2 Краткий обзор шагов по достижению аппаратными средствами полноты безопасности и соотношения с другими требованиями настоящего стандарта приведены в МЭК 61508-6, подраздел А.2.

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

4 Среди множества возможных методов моделирования наиболее подходящий метод выбирает аналитик. Возможные методы моделирования включают в себя:

- анализ последствий причин отказа (см. МЭК 61508-7, пункт В.6.6.2, приложение В);
- анализ дерева ошибок (см. МЭК 61508-7, пункт С.6.6.5, приложение С);
- марковские модели (см. МЭК 61508-7, подраздел С.6.4, приложение С);
- блок-диаграммы надежности (см. МЭК 61508-7, раздел С.5, приложение С).

5 Среднее время восстановления (см. МЭС 191-13-08 [3]), рассматриваемое в модели надежности, нуждается в учете времени диагностического испытательного интервала, времени восстановления и любых других задержек до (момента) восстановления.

6 Отказы из-за влияния общей причины и процессов передачи данных могут быть результатом других влияний, отличных от реальных отказов компонентов аппаратных средств (например электромагнитной интерференции, ошибок декодирования и т.п.). Однако такие отказы рассматривают в настоящем стандарте как случайные отказы аппаратных средств.

7.4.3.2.3 Диагностический испытательный интервал любой подсистемы, обладающей величиной отказоустойчивости аппаратных средств, большей нуля, должен быть таким, чтобы обеспечить возможность E/E/PE системе, связанной с безопасностью, удовлетворить требования по вероятности случайных отказов аппаратных средств (см. 7.4.3.2.1).

7.4.3.2.4 Диагностический испытательный интервал любой подсистемы с величиной отказоустойчивости аппаратных средств, равной нулю, от которой полностью зависит функция безопасности (см. примечание 1) и которая является лишь средством реализации функции(й) безопасности, действующей(их) в режиме с низкой интенсивностью запросов, должен быть таким, чтобы обеспечить возможность E/E/PE системе, связанной с безопасностью, удовлетворить требования по вероятности случайных отказов аппаратных средств (см. 7.4.3.2.1).

Примечания

1 Считают, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы вызывает отказ этой функции безопасности E/E/PE системы, связанной с безопасностью, и эта функция безопасности не относится к другой системе, связанной с безопасностью (см. МЭК 61508-1, подраздел 7.6).

2 Если существует вероятность, что некоторые комбинации выходных состояний подсистем могут непосредственно привести к опасному событию (см. анализ опасностей и рисков в МЭК 61508-1, подпункт 7.4.2.10), и если комбинация выходных состояний в присутствии ошибки в подсистеме не может быть определена (например в подсистеме типа В), тогда необходимо рассматривать обнаружение опасных отказов в подсистеме как функцию безопасности, действующую в режиме с высокой частотой запросов или с непрерывными запросами, и применять требования 7.4.6.3 и 7.4.3.2.5.

7.4.3.2.5 Диагностический испытательный интервал любой подсистемы (со значением величины отказоустойчивости аппаратных средств, равным нулю), от которой полностью зависит функция безо-

пасности (см. примечание 1) и которая является лишь средством реализации функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами (см. примечание 2), должен быть таким, чтобы суммарное время диагностического испытательного интервала и время выполнения определенного действия (реакции на отказ) для достижения или поддержания безопасного состояния (см. 7.3.3.1, перечисление g)) было меньше времени безопасности процесса. Время безопасности процесса определяется как период времени между отказом, возникающим в управляемом оборудовании или в системе управления управляемого оборудования (с потенциальной возможностью вызвать опасное событие) и возникновением опасного события, если функция безопасности не выполнена.

Примечания

1 Считают, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы вызывает отказ этой функции безопасности E/E/PE системы, связанной с безопасностью, и эта функция безопасности не относится к другой системе, связанной с безопасностью (см. МЭК 61508-1, подраздел 7.6).

2 Подсистему, осуществляющую конкретную функцию безопасности, для которой отношение частоты диагностических испытаний к частоте запросов превышает 100, допускается рассматривать, как если бы она осуществляла функцию безопасности в режиме с низкой частотой запросов (см. 7.4.3.2.4) при условии, что функция безопасности не предотвращает комбинацию состояний выходов, которые могли бы привести к опасному событию (см. примечание 3).

3 Если функция безопасности служит для предотвращения специфической комбинации состояний выходов, которые могут непосредственно вызвать опасное событие, то необходимо расценивать такую функцию безопасности как функцию, действующую в режиме с высокой частотой запросов или непрерывными запросами (см. 7.4.2.12).

7.4.3.2.6 Если для конкретного проекта целевая мера отказов требования полноты безопасности для выполняемой функции безопасности не достигается, то следует:

- определить критические компоненты, подсистемы и/или параметры;
- оценить эффект возможных мер усовершенствования критических компонентов, подсистем или параметров (например более надежные компоненты, дополнительные меры защиты от отказов по общей причине, расширенный охват диагностикой, расширенная избыточность, уменьшение интервала контрольных испытаний и т.п.);
- выбрать и осуществить подходящие меры усовершенствования;
- повторить вычисление нового значения вероятности отказов аппаратных средств.

7.4.4 Требования по предотвращению отказов

Примечание — Для подсистемы, отвечающей требованиям, позволяющим рассматривать ее как «проверенную в эксплуатации» (см. 7.4.7.6 — 7.4.7.12), требования 7.4.4.1 — 7.4.4.6 не применяют

7.4.4.1 Должна быть использована соответствующая группа методов и средств, предназначенных для предотвращения внесения ошибок во время разработки и создания аппаратных средств E/E/PE системы, связанной с безопасностью (см. таблицу В.2).

7.4.4.2 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,
- информации, устанавливающей последовательность и время,
- параллелизма и синхронизации;

c) ясности и точности документирования и передачи информации;

d) проверке и подтверждению соответствия.

7.4.4.3 Требования к техническому обслуживанию для гарантированного поддержания требуемой полноты безопасности E/E/PE системы, связанной с безопасностью, на необходимом уровне должны быть формализованы на стадии проектирования.

7.4.4.4 Следует использовать (если применимо) автоматические средства измерения и интегрированные инструментальные средства разработки.

7.4.4.5 В период проектирования должны быть запланированы испытания интеграции E/E/PES. 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 «выдержал»/«не выдержал» испытание.

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

7.4.5 Требования по управлению систематическими сбоями

Примечание — Для подсистемы, отвечающей требованиям, которые расцениваются как «проверено в эксплуатации» (см. 7.4.7.6 — 7.4.7.12), требования 7.4.5.1 — 7.4.5.3 не применяют.

7.4.5.1 Для управления систематическими сбоями проектирование E/E/PES должно обладать особенностями проектирования, которые делают E/E/PE системы, связанные с безопасностью, устойчивыми к:

a) любым остаточным ошибкам проектирования аппаратных средств, если вероятность ошибок проектирования не может быть исключена (см. таблицу А.16);

b) внешним влияниям, включая электромагнитные воздействия (см. таблицу А.17);

c) ошибкам оператора управляемого оборудования (см. таблицу А.18);

d) любым остаточным ошибкам в программном обеспечении (см. МЭК 61508-3, пункт 7.4.3, таблицы А.2 и В.7);

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

7.4.5.2 Для облегчения реализации свойств ремонтопригодности и тестируемости в созданных E/E/PE системах, связанных с безопасностью, эти свойства должны быть учтены в процессе проектирования и создания E/E/PES.

7.4.5.3 При проектировании E/E/PE систем, связанных с безопасностью, должны быть учтены способности и возможности человека, а созданные E/E/PES 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 E/E/PE 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 E/E/PE системой, связанной с безопасностью, например, если они являются необнаруживаемыми или реально восстанавливаемыми исключительно при непосредственном доступе, например некоторые механические отказы в управляемом оборудовании.

7.4.6 Требования к поведению системы при обнаружении отказов

7.4.6.1 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 к перечислению b)) 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 среднего времени восстановления (MTTR), принятого при вычислении вероятности случайных отказов аппаратных средств (см. 7.4.3.2.2), то для достижения и поддержания их безопасного состояния должно быть выполнено конкретное действие.

Примечание — Конкретное действие (реакция на отказ), которое требуется для достижения или поддержания безопасного состояния E/E/PES, должно быть определено в требованиях безопасности E/E/PES (см. 7.2.3.1). Оно может состоять, например, в отключении управляемого оборудования на дефектной подсистеме или его части, относящейся к снижению риска.

7.4.6.2 Обнаружение опасного отказа (с помощью диагностических тестов, контрольных испытаний или иным способом) в любой подсистеме с отказоустойчивостью аппаратных средств, равной нулю, функция безопасности которой является полностью зависимой (см. примечание 1) в случае, если такая подсистема используется только функцией(ями) безопасности в режиме с низкой частотой запросов, должно завершаться:

a) конкретным действием для достижения и поддержания безопасного состояния либо

b) восстановлением дефектной подсистемы в пределах периода среднего времени восстановления (MTTR), полученного при расчете вероятности случайных отказов аппаратных средств (см. 7.4.3.2.2). В течение этого времени безопасность управляемого оборудования должна обеспечиваться дополнительными мерами и ограничениями. Снижение риска, обеспеченное этими мерами и ограничениями, должно, по крайней мере, равняться сокращению риска, обеспеченному E/E/PE системой, связанной с безопасностью, в отсутствие любых отказов. Дополнительные меры и ограничения должны быть определены в процедурах эксплуатации и технического обслуживания E/E/PES (см. 7.6). Если восстановление не предпринято в пределах заданного среднего времени восстановления (MTTR), то для достижения и поддержания безопасного состояния должны быть предприняты конкретные действия (см. примечание 2).

Примечания

1 Предполагается, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы приводит к отказу функции безопасности рассматриваемой E/E/PE системы, связанной с безопасностью, и функция безопасности не предназначена для другой системы, связанной с безопасностью (см. МЭК 61508-1, подраздел 7.6).

2 Конкретное действие (реакция на отказ) требуется для достижения и поддержания безопасного состояния, которое должно быть определено в требованиях безопасности E/E/PES (см. 7.2.3.1). Это действие может состоять, например, в безопасном отключении управляемого оборудования в дефектной подсистеме или его части, предназначенной для снижения риска.

7.4.6.3 Обнаружение опасного отказа (путем диагностического тестирования, контрольных испытаний или иным способом) в любой подсистеме с отказоустойчивостью, равной нулю, в которой функция безопасности является зависимой (см. примечание 1) в случае подсистемы, выполняющей любую функцию(ии) безопасности, действующей(их) в режиме с высокой частотой запросов или непрерывными запросами (см. примечания 2 и 3), для достижения и поддержания безопасного состояния должно завершаться конкретными действиями (см. примечание 3).

Примечания

1 Считается, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы служит причиной отказа функции безопасности рассматриваемой E/E/PE системы, связанной с безопасностью, а также функция безопасности не принадлежит другой системе, связанной с безопасностью (см. МЭК 61508-1, подраздел 7.6).

2 Если существует вероятность, что некоторая комбинация состояний выходов подсистемы может стать непосредственной причиной опасного события (см. анализ опасностей и рисков 7.4.2.12), и если комбинацию выходных состояний в случае отказа в подсистеме невозможно определить (например для подсистемы типа B), то детектирование опасных событий в подсистеме следует расценивать как для функции безопасности, действующей в режиме с высокой частотой запросов или непрерывными запросами, и применять требования 7.4.6.3 и 7.4.2.5.

3 Для достижения и поддержания состояния безопасности, которое должно быть определено в требованиях безопасности E/E/PES, необходимо выполнить конкретное действие (реакцию на отказ). Это действие может состоять, например, в безопасном отключении в дефектной подсистеме управляемого оборудования или его части, предназначенной для сокращения риска.

7.4.7 Требования к развитию E/E/PES

7.4.7.1 E/E/PE системы, связанные с безопасностью, должны быть изготовлены в соответствии с проектом.

7.4.7.2 Подсистемы, используемые для одной или более функций безопасности, должны быть идентифицированы и документированы как подсистемы, связанные с безопасностью.

7.4.7.3 Для каждой подсистемы, связанной с безопасностью, должна быть представлена следующая информация (см. также 7.4.7.4):

a) функциональная спецификация тех функций и интерфейсов подсистемы, которые могут быть использованы функциями безопасности;

b) оценочные частоты отказов (из-за случайных отказов аппаратных средств) в любых режимах, которые могли бы привести к отказу E/E/PE системы, связанной с безопасностью, обнаруживаемые диагностическими тестами (см. 7.4.7.4);

c) оценочные частоты отказов (из-за случайных отказов аппаратных средств), которые могли бы привести к отказу E/E/PE системы, связанной с безопасностью, не обнаруживаемые диагностическими тестами (см. 7.4.7.4),

d) любые ограничения на окружающую среду подсистемы, которые должны быть соблюдены для обеспечения легитимности оценочных частот отказов из-за случайных отказов аппаратных средств;

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

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

h) диагностический охват в соответствии с приложением С (при необходимости).

Примечание — Испытания по перечислениям g) и h) относятся к диагностическим испытаниям, которые являются внутренними для подсистемы. Эта информация необходима, если требуется доверие к действиям по проведению диагностических тестов в подсистемах в модели надежности E/E/PE систем, связанных с безопасностью (см. 7.4.3.2.2).

i) любая дополнительная информация (например время восстановления), необходимая для обеспечения возможности получения среднего времени восстановления (MTTR), после обнаружения отказа с помощью диагностики.

Примечания

1 Испытания по требованиям перечислений b) и i) необходимы для оценки функции безопасности вероятности отказов по запросу или вероятности отказов в час (см. 7.4.3.2.2).

2 Требования перечислений b), c), g), h) и i) нужны лишь для оценки отдельных параметров подсистем, таких как сенсорные устройства и приводы, которые могут быть объединены в избыточные архитектуры для улучшения полноты безопасности аппаратных средств. Для логических решающих устройств, которые сами не объединяются в избыточные архитектуры в E/E/PE системе, связанной с безопасностью, с учетом требований перечислений b), c), g), h) и i) допускается определять характеристики в терминах вероятности отказов по запросам или вероятности отказов в час. Для таких устройств необходимо также устанавливать интервал контрольных испытаний для необнаруженных отказов;

j) информация, необходимая для обеспечения выделения составляющей безопасных отказов (SFF) подсистемы, как принято в E/E/PE системе, связанной с безопасностью, в соответствии с приложением С;

k) отказоустойчивость подсистемы.

Примечание — Требования перечислений j) и k) необходимы для определения самого высокого уровня полноты безопасности, который может потребоваться для функции безопасности в соответствии с архитектурными ограничениями (см. 7.4.3.1).

l) любые ограничения по применению подсистемы, которые должны быть рассмотрены во избежание систематических отказов;

m) самый высокий уровень полноты безопасности, который может потребоваться для функции безопасности в подсистеме, на основе:

- методов и средств, используемых для предотвращения систематических ошибок, которые вносятся в период проектирования и изготовления аппаратных средств и программного обеспечения (см. МЭК 61508, подпункт 7.4.4.1 и подраздел 7.4),

- особенностей проекта, которые делают подсистему устойчивой к систематическим отказам (см. 7.4.5.1).

Примечание — Не требуется в случаях, если эти подсистемы расцениваются как «проверенные в эксплуатации» (см. 7.4.7.5).

n) любая информация, необходимая для идентификации конфигурации аппаратных средств и программного обеспечения подсистемы для обеспечения возможности управления конфигурацией E/E/PE системы, связанной с безопасностью, в соответствии с МЭК 61508-1, пункт 6.2.1.

7.4.7.4 Оценочные частоты отказов подсистем из-за случайных отказов аппаратных средств (см. 7.4.7.3, перечисления b) и c)) могут быть определены:

a) методом отказов и анализом влияния проекта с использованием данных по отказам компонентов из признанного промышленного источника.

Примечания

1 Уровень доверия любых используемых данных о частоте отказов должен быть, по крайней мере, равен 70 %. Статистическое определение уровня доверия приведено в IEEE 352. Эквивалентный термин «уровень значимости» используется в МЭК 61164 [4].

2 Предпочтительно, чтобы место размещения данных об отказах было доступным. Если это требование не выполняется, может потребоваться использование исходных 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 в значительной степени зависит от самого компонента и условий его эксплуатации, особенно температуры окружа-

ющей среды компонента (например, могут быть очень чувствительны к температуре электролитические конденсаторы). 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 заданных пределах их использования. Компоненты с более длительным полезным сроком жизни стоят значительно дороже;

b) либо из предыдущего опыта использования подсистемы в похожих условиях окружающей среды (см. 7.4.7.9).

7.4.7.5 Для подсистем, проверенных в эксплуатации (см. 7.4.7.6), информация о методах и средствах предотвращения и управления систематическими ошибками (см. 7.4.7.3, перечисление m)) не требуется.

7.4.7.6 Ранее разработанная подсистема должна рассматриваться только как проверенная в эксплуатации, если она имеет явно ограниченные функциональные возможности и имеется соответствующее документальное свидетельство, основанное на предыдущей эксплуатации конкретной конфигурации этой подсистемы (в течение которого все отказы были формально зарегистрированы (см. 7.4.7.10)) и учитывающее любые требующиеся (см. 4.4.7.8) дополнительные анализы и тесты. Документальное подтверждение должно продемонстрировать, что вероятность любого отказа подсистемы (из-за случайных и систематических отказов аппаратных средств) в E/E/PE системе, связанной с безопасностью, настолько низка, что достигается(ются) требуемый(ые) уровень(ни) полноты безопасности функции(ий) безопасности.

7.4.7.7 Документальное свидетельство в соответствии с 7.4.7.6 должно продемонстрировать, что предыдущие условия эксплуатации конкретной подсистемы являются такими же или достаточно близкими к тем, в которых будет эксплуатироваться подсистема в E/E/PE системе, связанной с безопасностью, и установить, что вероятность любых необнаруженных систематических отказов настолько низка, что достигается требуемый уровень(ни) полноты безопасности функции(ий) безопасности для подсистемы.

Примечание — Условия эксплуатации (эксплуатационный профиль) включают в себя все факторы, которые могут повлиять на вероятность систематических ошибок аппаратных средств и программного обеспечения подсистемы (например окружающую среду, виды использования, выполняемые функции, конфигурацию, связи с другими системами, операционную систему, тип транслятора, человеческий фактор).

7.4.7.8 Если имеются различия между предыдущими условиями эксплуатации подсистемы и условиями, в которых будет эксплуатироваться E/E/PE 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 необнаруженной систематической ошибки настолько низка, что достигается требуемый уровень(ни) полноты безопасности для функции(ий) безопасности подсистемы.

7.4.7.9 Документальное свидетельство по 7.4.7.6 должно установить, что мера предыдущего использования конкретной конфигурации подсистемы (в часах эксплуатации) является достаточной, чтобы статистически рассматривать заявленные частоты отказов. Как минимум, требуется достаточное время эксплуатации для установления данных заявленной частоты отказов в одностороннем нижнем пределе доверия, по крайней мере, 70 % (см. МЭК 61508-7, приложение D, а также IEEE 352). В статистическом анализе время эксплуатации любой индивидуальной подсистемы меньше одного года не рассматривается как часть полного времени эксплуатации.

Примечание — Требуемое время часов эксплуатации для установления заявляемой частоты отказов может быть получено по результатам эксплуатации нескольких идентичных подсистем при условии, что отказы всех подсистем были эффективно обнаружены и документированы (см. 7.4.7.10). Например, если имеется 100 подсистем, каждая из которых проработала без отказов 10000 ч, то полное время эксплуатации без отказов можно считать равным 1000000 ч. В этом случае каждая подсистема должна эксплуатироваться более одного года, и действия при расчетах относят к полученному выше полному числу часов эксплуатации.

7.4.7.10 При проверке выполнения требований по 7.4.7.6 и 7.4.6.9 принимают во внимание только предыдущую эксплуатацию, при которой все отказы подсистем были эффективно обнаружены и документированы (например, если информация об отказах была собрана в соответствии с рекомендациями МЭК 60300-3-2).

7.4.7.11 При проверке выполнения или невыполнения требований по 7.4.7.6 и 7.4.6.9 учитывают как охват, так и уровень детализации имеющейся информации (см. также МЭК 61508-1, подраздел 4.1) для следующих факторов:

a) сложности подсистемы;

b) вклада, внесенного конкретной подсистемой в сокращение риска;

c) последствий, связанных с отказом системы;

d) новизну проекта.

7.4.7.12 Термин «проверено в эксплуатации» применяют к подсистеме, связанной с безопасностью, в E/E/PE системе, связанной с безопасностью, и ограничивают его рассмотрение функциями и интерфейсами подсистемы, соответствующими требованиям по 7.4.7.6 и 7.4.7.10.

Примечание — Требования 7.4.7.4 — 7.4.7.12 также применимы для подсистем, содержащих программное обеспечение. В этом случае должна быть уверенность в том, что конкретная подсистема выполняет в системе, связанной с безопасностью, только те функции, для которых задана требуемая полнота безопасности (см. также МЭК 61508-3, подпункт 7.4.2.11).

7.4.8 Требования к передаче данных

7.4.8.1 При любой форме передачи данных, используемой при выполнении функции безопасности, оценивается вероятность необнаруженного отказа процесса связи с учетом ошибок передачи, повторов, удалений, вставок, повторного упорядочения, искажения, задержки и ошибок идентификации (см. 7.4.8.2). Эта вероятность должна быть принята во внимание при оценке вероятности опасного отказа функции безопасности из-за случайных отказов аппаратных средств (см. 7.4.3.2.2).

Примечание — Ошибка идентификации означает, что истинное содержание сообщения не идентифицировано правильно (например сообщение от компонента, не связанного с безопасностью, идентифицировано как сообщение от компонента, связанного с безопасностью).

7.4.8.2 При оценке вероятности отказа функции безопасности из-за процесса передачи данных, в частности, должны быть учтены:

a) остаточный коэффициент ошибок (см. МЭК 60050-371);

b) остаточный коэффициент потери информации (см. МЭК 60050-371);

c) пределы и непостоянство скорости передачи информации (битовая скорость);

d) пределы и непостоянство задержки распространения информации.

Примечания

1 Можно показать, что вероятность опасного отказа в час равна частному от деления вероятности остаточных ошибок на длину сообщения (в битах) и умноженному на скорость передачи в шине сообщений, относящихся к безопасности, и на коэффициент 3600.

2 Более подробную информацию см. в МЭК 60870-5-1 [5], EH 50159-1 [7] и EH 50159-2 [8].

7.5 Интеграция E/E/PES

Примечание — Эта стадия показана как блок 9.4 на рисунке 2.

7.5.1 Цель

Целью настоящего подраздела является формирование требований к интеграции и испытанию E/E/PE систем, связанных с безопасностью.

7.5.2 Требования

7.5.2.1 E/E/PE системы, связанные с безопасностью, должны быть интегрированы в соответствии с конкретным проектом E/E/PES и испытаны в соответствии с конкретными тестами интеграции для E/E/PES (см. 7.4.2.11).

7.5.2.2 Как часть интеграции всех модулей в E/E/PE систему, связанную с безопасностью, E/E/PE системы, связанные с безопасностью, должны быть испытаны в соответствии с 7.4. Эти испытания должны показать, что все модули взаимодействуют правильно и не выполняют непредназначенные для них функции.

Примечания

1 Испытание всех входных комбинаций не проводится. Считается достаточным испытание всех классов эквивалентности (см. МЭК 61508-7, пункт B.5.2, приложение B). Статический анализ (см. МЭК 61508-7, пункт B.6.4, приложение B), динамический анализ (см. МЭК 61508-7, пункт B.6.5, приложение B) или анализ отказов (см. МЭК 61508-7, пункт B.6.6, приложение B) могут сократить число испытаний до приемлемого уровня. В случае разработки, проводимой в соответствии с правилами, приводящими к структурному проектированию (см. МЭК 61508-7, пункт B.3.2, приложение B), или полуформальными методами (см. МЭК 61508-7, пункт B.2.3, приложение B) эти требования выполнить легче.

2 Если при разработке используются формальные методы (см. МЭК 61508-7, пункт B.2.2, приложение B) или формальные доказательства и утверждения, то возможности таких испытаний могут быть ограничены.

3 Также могут быть использованы статистические методы (см. МЭК 61508-7, пункт B.5.3, приложение B).

7.5.2.3 Интеграция программного обеспечения, связанного с безопасностью, в программируемой электронной системе должна осуществляться в соответствии с МЭК 61508-3, подраздел 7.5.

7.5.2.4 Для испытания интеграции E/E/PE 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 должны быть документированы причины и способы его устранения.

7.5.2.5 В период интеграции и испытаний любые модификации или изменения E/E/PE систем, связанных с безопасностью, должны стать предметом анализа, при котором следует идентифицировать все компоненты, на которые влияют эти модификации или изменения, и все необходимые действия по повторному подтверждению выполнения требований.

7.5.2.6 При испытаниях интеграции E/E/PES должна быть документирована следующая информация:

a) версия спецификации испытаний;

b) критерии принятия испытаний интеграции;

c) версия испытуемой E/E/PE 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 E/E/PES должна быть использована соответствующая группа методов и средств в соответствии с таблицей В.3, приложение В.

7.6 Процедуры эксплуатации и технического обслуживания E/E/PES

7.6.1 Цель

Целью настоящего подраздела является разработка процедур, гарантирующих требуемую функциональную безопасность E/E/PE систем, связанных с безопасностью, во время эксплуатации и технического обслуживания.

7.6.2 Требования

7.6.2.1 Должны быть предусмотрены следующие действия, процедуры и документация по эксплуатации и техническому обслуживанию E/E/PES:

a) обычные действия, которые должны быть выполнены для поддержания «спроектированной» функциональной безопасности E/E/PE систем, связанных 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) документация (которая должна поддерживаться) по отказам системы и частотам запросов E/E/PE систем, связанных с безопасностью;

d) документация (которая должна поддерживаться), хранящая результаты аудитов и испытаний E/E/PE систем, связанных с безопасностью;

e) процедуры технического обслуживания, которым необходимо следовать в случае, если происходят отказы и ошибки в E/E/PE системах, связанных с безопасностью, в том числе:

- процедуры диагностики отказов и восстановления (ремонта),
- процедуры повторного подтверждения соответствия (вновь придания юридической силы),
- требования поддержания отчетности;

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

- по отказам,
- по анализу отказов;

g) инструменты, необходимые для технического обслуживания и подтверждения соответствия, и процедуры для поддержания инструментов и оборудования.

Примечания

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

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

7.6.2.2 Процедуры эксплуатации и технического обслуживания E/E/PE систем, связанных с безопасностью, должны непрерывно совершенствоваться с учетом как результатов проверок функциональной безопасности, так и результатов испытаний E/E/PE систем, связанных с безопасностью.

7.6.2.3 Обычные действия по техническому обслуживанию, необходимые для поддержания функциональной безопасности (в соответствии с проектом) E/E/PE систем, связанных с безопасностью, должны быть заданы на основе систематического подхода. Этот подход должен определять необнаруженные отказы всех компонентов, связанных с безопасностью (от сенсорных устройств до оконечных элементов), которые могли бы вызвать сокращение достигнутой полноты безопасности. Подходящие методы этого подхода включают в себя:

- экспертизу деревьев отказов;
- анализ видов отказов и анализ влияния;
- поддержание надежности тщательного технического обслуживания.

Примечания

1 Рассмотрение человеческого фактора является ключевым моментом в определении требуемых действий и соответствующих интерфейсов с E/E/PE системами, связанными с безопасностью.

2 Необходимо, чтобы частота проведения типовых испытаний была такой, чтобы была достигнута целевая мера отказов.

3 Частота типовых испытаний, интервал диагностического тестирования и время для последующего ремонта зависят от нескольких факторов (см. МЭК 61508-6, приложение В), включая:

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

4 Частота типовых испытаний и диагностический интервал тестирования, вероятно, должны иметь решающее влияние на достижение полноты безопасности аппаратных средств. Одна из основных причин проведения анализа надежности аппаратных средств (см. 7.4.3.2.2) состоит в гарантии того, что частоты проведения этих двух типов испытаний соответствуют целевой полноте безопасности аппаратных средств.

7.6.2.4 Процедуры эксплуатации и технической поддержки E/E/PES 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 E/E/PES используют группу средств и методов в соответствии с таблицей В.4, приложение В.

7.7 Подтверждение соответствия требованиям безопасности E/E/PES

Примечание — Эта стадия показана как блок 9.6 на рисунке 2.

7.7.1 Цель

Целью настоящего подраздела является подтверждение того, что заданная E/E/PE система, связанная с безопасностью, полностью соответствует требованиям безопасности в терминах требований к функциям безопасности и к полноте безопасности (см. 7.2).

7.7.2 Требования

7.7.2.1 Подтверждение соответствия E/E/PES требованиям безопасности должно выполняться в соответствии с подготовленным планом (см. также МЭК 61508-3, подраздел 7.7).

Примечания

1 Подтверждение соответствия E/E/PES требованиям безопасности демонстрируется жизненным циклом безопасности E/E/PES, предшествующим установке, но в некоторых случаях не может быть осуществлено до окончания установки (например, если разработка прикладного программного обеспечения еще не завершена до окончания установки).

2 Подтверждение соответствия программируемой электроники, 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, относящимся, по возможности, к национальному стандарту, или с общепризнанной процедурой. Все испытательное оборудование должно быть проверено на корректность функционирования.

7.7.2.3 Подтверждение соответствия каждой функции безопасности, указанной в требованиях безопасности E/E/PES (см. 7.2), и процедур эксплуатации и технического обслуживания должно осуществляться проведением испытаний и/или анализа.

7.7.2.4 Должна быть подготовлена необходимая документация по проведению испытаний на подтверждение соответствия E/E/PES требованиям безопасности, в которой для каждой функции безопасности должны быть указаны:

a) версия используемого плана проведения подтверждения соответствия E/E/PES;

b) функция безопасности, подвергаемая испытаниям (или анализу), вместе с конкретной ссылкой на указанные в документации требования на планирование проведения подтверждения соответствия E/E/PES требованиям безопасности;

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

d) результаты 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 E/E/PES требованиям безопасности должны быть документированы, включая:

a) описание проведенного анализа и

b) принятое решение либо 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 E/E/PES требованиям безопасности производителю управляемого оборудования и систем управления управляемого оборудования с тем, чтобы позволить им обеспечить выполнение требований полного подтверждения соответствия требованиям безопасности в соответствии с МЭК 61508-1.

7.7.2.7 Для предотвращения отказов при проведении подтверждения соответствия E/E/PES требованиям безопасности используют группу методов и средств в соответствии с таблицей B.5, приложение B.

7.8 Модификация E/E/PES

7.8.1 Цель

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

7.8.1 Требования

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

a) детальную спецификацию модификации или изменений;

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

c) утвержденные изменения;

d) порядок проведения изменений;

e) испытания компонентов, включая данные повторного подтверждения соответствия;

f) предысторию управления конфигурацией E/E/PES;

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 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 экспертизы, автоматизированных средств (см. МЭК 61508-3, подпункт 7.4.4.2), планирования и управления, что и при разработке E/E/PE систем, связанных с безопасностью.

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

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

7.9 Верификация

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. Требования см. в 7.2.2, 7.4.2—7.4.8, 7.5.2, 7.6.2, 7.7.2, 7.8.2 настоящего стандарта, а также в МЭК 61508-1, пункты 7.2.2, 7.3.2, 7.4.2, 7.5.2, 7.6.2, 7.11.2, 7.12.2.

Примечание — Все требования к действиям по верификации объединены в подразделе 7.9, но фактически они выполняются на всех стадиях жизненного цикла безопасности E/E/PES.

7.9.2 Требования

7.9.2.1 Верификация E/E/PE систем, связанных с безопасностью, должна быть запланирована одновременно с их разработкой (см. 7.4) для каждой стадии жизненного цикла безопасности E/E/PES и документирована.

7.9.2.2 Планирование верификации E/E/PES должно относиться к критериям, методам и средствам, используемым для верификации на проверяемой стадии.

7.9.2.3 Планирование верификации E/E/PES должно определять на каждой стадии выполнение обязательных действий для гарантии правильности выходных результатов и соответствия требованиям разделов стандартов, предусмотренных для этой стадии. Требования см. в пункте 7.3.2, а также в МЭК 61508-1, пункты 7.7.2, 7.8.2, 7.9.2.

7.9.2.4 Планирование верификации E/E/PES должно предусматривать:

a) выбор стратегии и методов;

b) выбор и использование испытательного оборудования;

c) выбор и документирование действий в ходе верификации;

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

7.9.2.5 При проектировании и разработке каждой стадии должно быть показано, что требования функциональной безопасности и полноты безопасности выполняются.

7.9.2.6 Результат каждого действия по верификации должен быть документирован. В документе должно быть указано, прошли ли E/E/PES проверку, причины отказов (при их наличии). В случае несоответствия E/E/PES требованиям одного или более пунктов:

a) жизненного цикла безопасности E/E/PES (см. 7.2);

b) стандартов проектирования (см. 7.4.2—7.4.8);

c) управления функциональной безопасностью (см. раздел 6)

в документе должны быть указаны пункты несоответствия.

7.9.2.7 Для верификации требований безопасности E/E/PE систем, связанных с безопасностью, после того как эти требования были установлены (см. 7.2), и перед началом следующей стадии (проектирования или разработки) проверка должна:

a) определить, адекватны ли по безопасности и функциональным возможностям требования безопасности E/E/PES требованиям, установленным в требованиях к распределению безопасности E/E/PES (см. МЭК 61508-1, пункт 7.6.2), и другим требованиям, заданным при планировании безопасности (см. МЭК 61508-1, пункты 7.7.2, 7.8.2, 7.9.2), и

b) проверить на несовместимость:

- требования безопасности E/E/PES (см. 7.2),
- распределение требований безопасности (см. МЭК 61508-1),
- испытания E/E/PES (см. 7.4) и
- документацию пользователя вместе с остальной документацией на систему.

7.9.2.8 Для верификации стадии проектирования и разработки E/E/PES после ее завершения (см. 7.4) и до начала следующей стадии (интеграции) проверка должна:

a) определить, адекватны ли тесты для стадии проектирования и разработки E/E/PES (см. 7.4);

b) определить связанность и завершенность (до уровня модулей, включительно) стадии проектирования и разработки E/E/PES (см. 7.4) в отношении требований безопасности (см. 7.2) и

c) проверить на несовместимость:

- требования безопасности E/E/PES (см. 7.2),
- результат проектирования и разработки E/E/PES (см. 7.4) и
- испытания E/E/PES (см. 7.4).

Примечания

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

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

7.9.2.9 Для проверки интеграции E/E/PES должна быть проверена интеграция E/E/PE систем, связанных с безопасностью, с тем чтобы установить выполнение требований 7.5.

7.9.2.10 Проверки и их результаты должны быть задокументированы.

8 Оценка функциональной безопасности

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

Приложение А
(обязательное)

Методы и средства для E/E/PE систем, связанных с безопасностью: управление отказами в процессе эксплуатации

А.1 Общие положения

Настоящее приложение должно использоваться совместно с 7.4 и ограничивает максимальный диагностический охват, 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 E/E/PE 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 компонентов);
- 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 E/E/PES (см. приложение В), и средства, используемые для управления отказами в период эксплуатации (см. настоящее приложение). Средства по управлению отказами — это собственные встроенные составляющие E/E/PE систем, связанных с безопасностью.

Охват диагностикой и доля безопасных отказов определяются в соответствии с таблицей А.1 и процедурами, описанными в приложении С. Таблицы А.2 — А.15 поддерживают требования таблицы А.1 методами и средствами для диагностического тестирования и требованиями максимальных уровней диагностического охвата, которые могут быть достигнуты при их использовании. Требования, приведенные в данных таблицах, не отменяют требований, приведенных в приложении С. Требования таблиц А.2 — А.15 не являются исчерпывающими. Могут быть использованы другие методы и средства диагностического тестирования, если приведены свидетельства о поддержании ими требующегося диагностического охвата. Если требуется высокий уровень диагностического охвата, то из каждой из таблиц А.2 — А.15 должно быть применено, как минимум, одно средство с высоким уровнем диагностического охвата.

Таблицы А.16 — А.18 содержат рекомендуемые меры и средства управления систематическими отказами для каждого уровня полноты безопасности. Таблица А.16 относится к общим мерам, рекомендуемым для управления систематическими отказами (см. также МЭК 61508-3). Таблица А.17 относится к рекомендуемым мерам по управлению отказами из-за влияния окружающей среды. Таблица А.18 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.19.

Методы, средства и меры, приведенные в таблицах А.2 — А.15, описаны в МЭК 61508-7, приложение А. Методы, средства и меры, требуемые для каждого уровня полноты безопасности программного обеспечения, приведены в МЭК 61508-3. Руководящие указания по определению архитектуры E/E/PE системы, связанной с безопасностью, приведены в МЭК 61508-6.

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

- последовательность выбранных методов и средств и то, как они будут дополнять друг друга;
- какие методы, средства и меры в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой E/E/PE 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 диагностического охвата, представлены в таблице А.1 (см. также приложение С). Требования, представленные в таблицах А.2 — А.15, поддерживают требования, приведенные в таблице А.1, методами и средствами для диагностического тестирова-

ния и требованиями максимальных уровней диагностического охвата, которые могут быть достигнуты при их использовании. Данные диагностические тесты могут проводиться непрерывно или периодически. Таблицы А.2 — А.15 не заменяют требований подраздела 7.4. Методы, средства и меры, представленные в таблицах А.2 — А.15, не являются исчерпывающими. Могут быть использованы другие методы, средства и меры, если представлены свидетельства, что они поддерживают необходимый диагностический охват.

Примечания

1 Краткий обзор методов и средств, упомянутых в таблицах А.2 — А.15, приведен в МЭК 61508-7 (приложение А). Во вторых колонках таблиц А.2 — А.15 приведены соответствующие ссылки.

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

Таблица А.1 — Ошибки и отказы, которые должны быть обнаружены в период эксплуатации или проанализированы 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	Невключение или неотключение. Приваренные контакты	Невключение или неотключение. Отдельные приваренные контакты	Невключение или неотключение. Отдельные приваренные контакты. Отсутствуют определенные руководства (для реле этот отказ не предполагается, если они изготовлены и испытаны в соответствии с ЕН 50205 [8]). Отсутствуют конкретные ссылки (для положений переключателей этот отказ не рассматривается, если они изготовлены и испытаны в соответствии с ЕН 60947-5-1 [10] или эквивалентными нормами)
Дискретные аппаратные средства: - цифровой вх./вых. - аналоговый вх./вых. - источник питания	А.3, А.7, А.9, А.11	 Непрерывный отказ То же »	 Модель отказов при постоянном токе Модель отказов из-за отклонений и колебаний постоянного тока То же	 Модель отказов из-за отклонений и колебаний постоянного тока То же »
Шина: - общая шина - элемент управления памятью - прямой доступ к памяти	А.3, А.7, А.8	 Непрерывный отказ адресов Непрерывный отказ данных или адресов. Нет доступа или непрерывный доступ.	 Блокировка по времени Неверное декодирование адреса Модель отказов по постоянному току для данных и адресов. Неверное время доступа	 Блокировка по времени Неверное декодирование адреса Все отказы, влияющие на данные в памяти. Неверные данные или адреса. Неверное время доступа

Продолжение таблицы А.1

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
- управление доступом к шине (см. примечание 1)	А.3, А.7, А.8	Непрерывный отказ сигналов управления доступом к шине	Отсутствует или непрерывное управление доступом к шине	Отсутствует, непрерывное или неправильное управление доступом к шине
Процессор:	А.4, А.10			
- регистр, внутреннее ОЗУ		Непрерывный отказ данных или адресов	Модель отказов по постоянному току для данных и адресов	Модель отказов по постоянному току для данных и адресов. Динамическое пересечение запоминающих элементов. Отсутствует, неверная или множественная адресация
- устройство кодирования и выполнения, включая регистр признаков		Неверное кодирование или невыполнение	Неверное кодирование или неверное выполнение	Отсутствует определение предполагаемого отказа
- устройство вычисления адреса		Непрерывный отказ	Модель отказов при постоянном токе	Отсутствует определение предполагаемого отказа
- счетчик команд, указатель стека		Непрерывный отказ	Модель отказов при постоянном токе	Модель отказов при постоянном токе
Устройство обработки прерываний	А.4	Отсутствуют или непрерывные прерывания	Отсутствуют или непрерывные прерывания. Пересечение прерываний	Отсутствуют или непрерывные прерывания. Пересечение прерываний
Постоянная память	А.5	Непрерывный отказ данных или адресов	Модель отказов по постоянному току для данных и адресов	Все отказы, влияющие на данные в памяти
Память с произвольным доступом	А.6	Непрерывный отказ данных или адресов	Модель отказов по постоянному току для данных и адресов. Изменение информации, вызванное ошибками программного обеспечения для удвоенного ОЗУ с объемом не менее 1 Мбит	Модель отказов по постоянному току для данных и адресов. Динамическое пересечение запоминающих элементов. Отсутствует, неверная или множественная адресация Изменение информации, вызванное ошибками программного обеспечения для удвоенного ОЗУ с объемом не менее 1 Мбит
Устройство синхронизации (кварцевое)	А.12	Нижняя или верхняя гармоника	Нижняя или верхняя гармоника	Нижняя или верхняя гармоника

Окончание таблицы А.1

Компонент	См. таблицу	Требования к охвату диагностикой или к заданной доле безопасных отказов		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Устройство связи и запоминающее устройство большей емкости	А.13	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 ошибки, влияющие на данные в памяти. Неверные данные или адреса. Неверное время передачи. Неверна последовательность передачи
Сенсоры	А.14	Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока
Оконечные элементы	А.15	Непрерывный отказ	Модель отказов из-за отклонений и колебаний постоянного тока	Модель отказов из-за отклонений и колебаний постоянного тока

Примечания

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

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

3 «Модель отказов при постоянном токе» включает следующие модели отказов: непрерывные отказы, открытые непрерывные, открытые выходы или выходы с высоким сопротивлением, а также короткие замыкания между линиями связи.

Таблица А.2 — Электрические подсистемы

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
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 диагностического охвата обнаружения отказов
Мониторинг контактов реле	А.1.2	Высокий	—
Компаратор	А.1.3	Высокий	Высокий, если режимы отказов в основном безопасно диагностируются
Мажоритарная схема голосования	А.1.4	Высокий	Зависит от качества устройства голосования
Принцип реактивного тока	А.1.5	Низкий	Только для E/E/PE систем, связанных с безопасностью, где не требуется непрерывное управление для достижения и поддержания безопасного состояния управляемого оборудования

Примечания

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

2 Для определения диагностического охвата применяются требования приложения С.

Таблица А.3 — Электронные подсистемы

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
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 диагностического охвата обнаружения отказов
Компаратор	А.1.3	Высокий	Высокий, если режимы отказов в основном безопасно диагностируются
Мажоритарная схема голосования	А.1.4	Высокий	Зависит от качества устройства голосования
Тестирование с помощью избыточных аппаратных средств	А.2.1	Средний	Зависит от диагностического охвата обнаружения отказов
Динамические принципы	А.2.2	Средний	Зависит от диагностического охвата обнаружения отказов
Стандартный тестовый порт доступа и архитектура граничного сканирования	А.2.3	Высокий	Зависит от диагностического охвата обнаружения отказов
Контролируемая избыточность	А.2.5	Высокий	Зависит от степени избыточности и текущего контроля
Аппаратные средства с автоматической проверкой	А.2.6	Высокий	Зависит от диагностического охвата тестов
Текущий контроль аналоговых сигналов	А.2.7	Низкий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

Таблица А.4 — Устройства обработки

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Компаратор	А.1.3	Высокий	Зависит от качества сравнения
Мажоритарная схема голосования	А.1.4	Высокий	Зависит от качества устройства голосования
Самотестирование с помощью программного обеспечения: ограниченное число отказов (один канал)	А.3.1	Низкий	—
Самотестирование с помощью программного обеспечения: «блуждающий бит» (один канал)	А.3.2	Средний	—
Самотестирование с помощью аппаратных средств (один канал)	А.3.3	Средний	—
Запрограммированная обработка (один канал)	А.3.4	Высокий	—
Взаимное сравнение с помощью программного обеспечения	А.3.5	Высокий	Зависит от качества сравнения
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С			

Таблица А.5 — Постоянная память

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Мультибитовая избыточность защиты слов	А.4.1	Средний	—
Модифицированная 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 диагностического охвата применяются требования приложения С.			

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

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Тест ОЗУ «поклеточная разбивка» или «марш»	А.5.1	Низкий	—
Тест ОЗУ «блуждающая траектория»	А.5.2	Средний	—
Тест ОЗУ «GALPAT» — попарная запись — считывание с помощью бегущего кода или «Прозрачный GALPAT»	А.5.3	Высокий	—
Тест ОЗУ «Авраам»	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	—
Задублированное ОЗУ с аппаратным или программным сравнением и контролем чтения/записи	А.5.7	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С. 3 Для ОЗУ, в котором запись/считывание происходят не часто (например во время конфигурирования), эффективны методы по МЭК 6108-7, пункты А.4.1 — А.4.4, приложение А, если они осуществляются после каждой записи/считывания.			

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

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
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 диагностического охвата обнаружения отказов
Тестирующая комбинация	А.6.1	Высокий	—
Кодовая защита	А.6.2	Высокий	—
Многоканальный параллельный вывод	А.6.3	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Контролируемый вывод	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
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С			

Таблица А.8 — Маршруты данных (внутренний обмен)

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Однобитовая аппаратная избыточность	А.7.1	Низкий	—
Многобитовая аппаратная избыточность	А.7.2	Средний	—
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 диагностического охвата применяются требования приложения С.			

Таблица А.9 — Источник питания

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Защита от перенапряжения с защитой от короткого замыкания или отключением/подключением ко второму источнику питания	А.8.1	Низкий	Рекомендуется использовать всегда в дополнение к другим методам в настоящей таблице
Контроль напряжения (вторичный) с безопасным отключением/подключением ко второму источнику питания	А.8.2	Высокий	—
Отключение питания с защитой от короткого замыкания и отключение/подключение ко второму источнику питания.	А.8.3	Высокий	Рекомендуется использовать всегда в дополнение к другим методам в настоящей таблице
Принцип реактивного тока	А.1.5	Низкий	Полезен только против отключения питания
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

Таблица А.10 — Последовательность выполнения программ (дежурный таймер)

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Дежурный таймер с отдельным временным периодом без временного окна	А.9.1	Низкий	—
Дежурный таймер с отдельной временной базой и временным окном	А.9.2	Средний	—
Логический мониторинг последовательности выполнения программ	А.9.3	Средний	Зависит от качества мониторинга
Комбинация временного и логического мониторинга 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 диагностического охвата применяются требования приложения С.			

Таблица А.11 — Система вентиляции и подогрева (при необходимости)

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Датчик температуры	А.10.1	Средний	—
Управление вентиляцией	А.10.2	Средний	—
Безопасное выключение с использованием плавкого предохранителя	А.10.3	Высокий	—
Пороговые сообщения от термодатчиков и условная тревога	А.10.4	Высокий	—
Соединение устройства принудительного охлаждения воздуха и индикатора состояния	А.10.5	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

Таблица А.12 — Генератор тактовой частоты

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Дежурный таймер с отдельным временным периодом без временного окна	А.9.1	Низкий	—
Дежурный таймер с отдельной временной базой и временным окном	А.9.2	Средний	Зависит от временных ограничений для временного окна
Логический мониторинг 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 мониторинга 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 диагностического охвата применяются требования приложения С.			

Таблица А.13 — Устройство связи и запоминающее устройство большой емкости

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обмен информацией между E/E/PE системой, связанной с безопасностью, и процессом ее обработки	А.6	См. таблицу А.7	См. устройства вх./вых. и интерфейс
Обмен информацией между E/E/PE системами, связанными с безопасностью	А.7	См. таблицу А.8	См. цепи/шины данных
Разделение линий электрического питания и линий передачи информации	А.11.1	Высокий	Рекомендуется использовать всегда в дополнение к другим методам в этой таблице
Пространственное разделение групповых линий	А.11.2	Высокий	—
Увеличение устойчивости к электромагнитным воздействиям	А.11.3	Высокий	—
Передача сигнала без наводок	А.11.4	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

Таблица А.14 — Датчики

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
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 диагностического охвата обнаружения отказов
Принцип реактивного тока	А.1.5	Низкий	Только для E/E/PE систем, связанных с безопасностью, где не требуется непрерывное управление для достижения и поддержания безопасного состояния управляемого оборудования
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 диагностического охвата обнаружения отказов
Положительно активизированный переключатель	А.12.2	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

Таблица А.15 — Оконечные элементы (приводы)

Диагностические методы/средства	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
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 диагностического охвата обнаружения отказов
Мониторинг контактов реле	А.1.2	Высокий	—
Принцип реактивного тока	А.1.5	Низкий	Только для E/E/PE систем, связанных с безопасностью, где не требуется непрерывное управление для достижения и поддержания безопасного состояния управляемого оборудования
Тестирующая комбинация	А.6.1	Высокий	—
Мониторинг	А.13.1	Высокий	Зависит от диагностического охвата обнаружения отказов
Перекрестный контроль сложных приводов	А.13.2	Высокий	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения диагностического охвата применяются требования приложения С.			

А.3 Систематическая полнота безопасности

Таблицы А.16 — А.18 содержат рекомендации для применения методов и средств с целью:

- управления отказами, связанными с проектированием аппаратных средств и программного обеспечения (см. таблицу А.16);
- управления отказами, вызванными внешними нагрузками или влияниями (см. таблицу А.17);
- управления отказами на стадии эксплуатации (см. таблицу А.18).

Рекомендации в таблицах А.16 — А.18 приведены на основе уровня полноты безопасности, устанавливая, 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. 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 для 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:

- «обязательная (Mandatory)» — данные методы или средства требуются для всех уровней полноты безопасности и должны быть использованы настолько эффективно, насколько возможно (т. е. с наивысшей эффективностью);
- «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.19.

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

Все приведенные в таблицах А.16 — А.18 методы и средства являются встроенными компонентами E/E/PE систем, связанных с безопасностью, которые могут помочь управлять отказами в режиме «онлайн». Процедурные и организационные методы и средства необходимы на протяжении всего жизненного цикла безопасности E/E/PES для предотвращения введения в них ошибок. Методы оценки соответствия для проверки действия E/E/PE 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.16 — А.18, может использоваться с разной эффективностью в соответствии с таблицей А.19, 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.16 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, источниками которых являются этапы разработки аппаратных средств и программного обеспечения

Методы/средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
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 «онлайн» (см. примечание 4)	А.1.1	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
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

Окончание таблицы А.16

Методы/средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
7 Обнаружение и диагностика ошибок	С.3.1	См. МЭК 61508-3, таблица А.2			
8 Обнаружение и исправление ошибок	С.3.2				
9 Программирование с проверкой ошибок	С.3.3				
10 Методы «подушки безопасности»	С.3.4				
11 Многовариантное программирование	С.3.5				
12 Блоки восстановления	С.3.6				
13 Восстановление предыдущего состояния	С.3.7				
14 Прямое восстановление	С.3.8				
15 Повторный запуск механизмов восстановления после ошибок	С.3.9				
16 Сохранение достигнутых состояний	С.3.10				
17 Постепенное отключение функций	С.3.11				
18 Исправление ошибок методами искусственного интеллекта	С.3.12				
19 Динамическое реконфигурирование	С.3.13				

Примечания

1 Требуется выполнение, по крайней мере, одного из методов 2—19.

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

3 Методы и средства 1—6 могут быть использованы для различных уровней эффективности в соответствии с таблицей А.19, в которой приведены примеры для низкого и высокого уровней эффективности. Усилия, требуемые для среднего уровня эффективности, находятся между усилиями, требуемыми для низкого и высокого уровней эффективности.

4 Краткий обзор методов и средств, представленных в настоящей таблице, приведен в МЭК 61508-7, приложения A, B и C. Ссылки на соответствующие подпункты указаны во второй колонке.

5 Для E/E/PE систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например для систем аварийного отключения), диагностический охват, осуществляемый путем обнаружения отказа с помощью мониторинга в режиме «онлайн», обычно является низким или отсутствует.

Таблица А.17 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами, вызванными внешними нагрузками или влияниями

Методы/меры, средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения	А.8	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
2 Разделение линий электрического питания и линий передачи информации (см. примечание 5)	А.11.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
3 Увеличение устойчивости к электромагнитным воздействиям	А.11.3	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
4 Средства против физического воздействия окружающей среды (например температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	А.14	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
5 Мониторинг последовательности выполнения программ	А.9	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий

Окончание таблицы А.17

Методы/меры, средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
6 Меры против повышения температуры	А.10	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
7 Пространственное разделение групповых линий	А.11.2	KP (HR) низкий	KP (HR) низкий	KP (HR) средний	KP (HR) высокий
8 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
9 Тестирование избыточными аппаратными средствами	А.2.1	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
10 Кодовая защита	А.6.2	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
11 Передача неэквивалентных сигналов	А.11.4	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
12 Разнообразие аппаратных средств (см. примечание 7)	В.1.4	— низкий	— низкий	— средний	P (R) высокий
13 Архитектура программного обеспечения	МЭК 61508-3, пункт 7.4.3	См. МЭК 61508-3, таблица А.2			

Примечания

1 Требуется выполнение, по крайней мере, одного из методов 8—13.

2 Значения обозначений под каждым уровнем полноты безопасности (SIL) см. в тексте, непосредственно предшествующем таблице А.16.

3 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.19, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, требуемые 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 МЭК 61508-7, приложения А и В. Ссылки на соответствующие подпункты указаны во второй колонке.

5 Отделение линий электропитания от линий передачи информации не является необходимым, в случае если информация передается по оптоволокну, а также для низковольтных линий, спроектированных для питания компонентов E/E/PES и для передачи информации к компонентам E/E/PES или от них.

6 Для E/E/PE систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например для систем аварийного отключения), диагностический охват, осуществляемый путем обнаружения отказа с помощью мониторинга в режиме «онлайн», обычно является низким или отсутствует.

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.18 — Уровни важности и требуемые эффективности методов и средств управления систематическими отказами при эксплуатации

Методы/средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Защита от модификаций	В.4.8	KP (HR) обязательно	KP (HR) обязательно	KP (HR) обязательно	KP (HR) обязательно
2 Обнаружение отказов путем мониторинга в режиме «онлайн» (см. примечание 5)	А.1.1	P (R) низкий	P (R) низкий	P (R) средний	P (R) высокий
3 Подтверждение ввода	В.4.9	P (R) низкий	P (R) низкий	P (R) средний	P(R) высокий
4 Программирование с проверкой ошибок	С.3.3	См. МЭК 61508-3, таблица А.2			

Окончание таблицы А.18

Примечания

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

2 Значения обозначений под каждым уровнем полноты безопасности (SIL) см. в тексте, непосредственно предшествующем таблице А.16.

3 Большинство средств, перечисленных в настоящей таблице, может быть использовано для различных уровней эффективности в соответствии с таблицей А.19, в которой приведены примеры низкого и высокого уровней эффективности. Усилия, требуемые 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 МЭК 61508-7, приложения A, B и C. Ссылки на соответствующие подпункты указаны во второй колонке.

5 Для E/E/PE систем, связанных с безопасностью, действующих в режиме с низкой частотой запросов (например для систем аварийного отключения), диагностический охват, осуществляемой путем обнаружения отказа с помощью мониторинга в режиме «онлайн», обычно является низким или отсутствует.

Таблица А.19 — Эффективность методов, мер 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 E/E/PE систем, связанных с безопасностью (только характер изменения во времени и когда система не используется)	E/E/PE системы, связанные с безопасностью, перезапускаются временными и логическими сигналами от управляемого оборудования и его системы управления (временное окно для временной функции дежурного таймера)
Тестирование избыточными аппаратными средствами (см. примечание)	A.2.1	Дополнительные аппаратные средства проверяют сигналы, запускающие E/E/PE системы, связанные с безопасностью (только характер изменения во времени и когда система не используется). Эти средства включают вспомогательный оконечный элемент	Дополнительные аппаратные средства повторно перезапускаются временными и логическими сигналами E/E/PE систем, связанных с безопасностью (временное окно для временного дежурного таймера); 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 E/E/PE систем, связанных с безопасностью. Проверяются все функции для всех интегральных микросхем
Кодовая защита	A.6.2	Обнаружение ошибок с помощью временной избыточности передачи сигналов	Обнаружение ошибок с помощью временной и информационной избыточности передачи сигналов
Мониторинг последовательности выполнения программ	A.9	Временной или логический мониторинг последовательности выполнения программ	Временной и логический мониторинг последовательности выполнения программ с большим количеством контрольных точек в программе
Средства против повышения температуры	A.10	Температурный датчик, определяющий превышение температуры	Применение безопасного выключателя с использованием плавкого предохранителя

Окончание таблицы А.19

Методы/средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Повышение устойчивости к электромагнитным воздействиям (см. примечание)	А.11.3	Помехозащитный 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, выполняют одну и ту же функцию	Два или более устройств, выполняют различные функции
Подтверждение ввода	В.4.9	Отображение входных действий оператору	Проверка по строгим правилам входных данных, вводимых оператором, с отклонением неправильных входных данных
Примечание — В случаях, когда методы и средства 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 будут также использованы.			

Приложение В
(обязательное)

Методы и средства для E/E/PE систем, связанных с безопасностью: предотвращение систематических отказов в течение различных стадий жизненного цикла

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

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

- влияние систематических ошибок зависит от стадии жизненного цикла, на которой они вносятся, и
- эффективность любого одиночной меры или средства по предотвращению отказов зависит от их применения.

Поэтому количественный анализ для предотвращения систематических отказов невозможен.

Категории отказов в E/E/PE системах, связанных с безопасностью, могут быть установлены в соответствии со 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 производственные ошибки и неправильный выбор компонентов), и
- отказы, вызванные ошибками, возникающими после установки системы (например случайные отказы аппаратных средств, 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 стадиях жизненного цикла E/E/PES (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 E/E/PE систем, связанных с безопасностью, а средства и меры для предотвращения отказов — используемые в течение жизненного цикла безопасности.

Рекомендации, приведенные в таблицах В.1 — В.5, приведены на основе уровня полноты безопасности и устанавливают, во-первых, важность метода, меры или средства и, во-вторых, эффективность его использования.

Уровень важности метода, меры или средства обозначают:

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

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

- методы, меры или средства, не имеющие рекомендаций для и против применения;

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

Требуемую эффективность методов, мер и средств обозначают:

- «обязательная (Mandatory)» — данные методы, меры или средства требуются для всех уровней полноты безопасности и должны быть использованы настолько эффективно, насколько возможно (т. е. с наивысшей эффективностью);
- «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, 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;
- какие методы, меры и средства в наибольшей степени подходят для решения конкретных проблем, с которыми сталкиваются специалисты во время создания каждой E/E/PE системы, связанной с безопасностью.

Таблица В.1 — Рекомендации по предотвращению ошибок во время задания спецификации требований к E/E/PES (см. 7.2)

Методы/меры, средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Управление проектами	В.1.1	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
2 Документация	В.1.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
3 Разделение E/E/PE 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 МЭК 61508-3, таблица В.7	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

Окончание таблицы В.1

Методы/меры, средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
8 Компьютерные 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, обозначенные «Р (R)», являются заменяемыми, 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 (SIL) 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 для 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 МЭК 61508-7, приложение В. Ссылки на соответствующие подпункты указаны во второй колонке.

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

Методы/меры, средства	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Соблюдение руководящих материалов и стандартов	В.3.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
2 Управление проектами	В.2.1	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
3 Документация	В.1.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
4 Структурированное 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 Поверка аппаратных средств или сквозной анализ	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

Окончание таблицы В.2

Примечания

1 Методы 6—12, обозначенные «Р (R)», являются заменяемыми, 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 (SIL) 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 для 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 МЭК 61508-7, приложение В. Ссылки на соответствующие подпункты указаны во второй колонке.

Таблица В.3 — Рекомендации для предотвращения ошибок в период интеграции E/E/PES (см. 7.5)

Методы/меры	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Функциональное тестирование	В.5.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
2 Управление проектами	В.1.1	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
3 Документация	В.1.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
4 Тестирование методом «черного ящика»	В.5.2	Р (R) низкий	Р (R) низкий	Р (R) средний	Р (R) высокий
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, обозначенные «Р (R)», являются заменяемыми, 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 (SIL) 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 для 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 МЭК 61508-7, приложение В. Ссылки на соответствующие подпункты указаны во второй колонке.

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

Методы/меры	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Инструкции по эксплуатации и техническому обслуживанию	В.4.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
2 Удобство общения с пользователем	В.4.2	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно

Окончание таблицы В.4

Методы/меры	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
3 Удобство общения с обслуживающим персоналом	В.4.3	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
4 Управление проектами	В.1.1	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) высокий
5 Документация	В.1.2	КР (HR) низкий	КР (HR) низкий	КР (HR) средний	КР (HR) 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, обозначенные «Р (R)», являются заменяемыми, 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. МЭК 61508-7, подраздел В.2.5), или метода, основанного на экспертизе спецификации (см. МЭК 61508-7, подраздел В.2.6).

3 Значения обозначений под каждым уровнем полноты безопасности (SIL) 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 для 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 МЭК 61508-7, приложение В. Ссылки на соответствующие подпункты указаны во второй колонке.

Таблица В.5 — Рекомендации по предотвращению ошибок при подтверждении соответствия E/E/PES (см. 7.7)

Методы/меры	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
1 Функциональное тестирование	В.5.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
2 Функциональные испытания в условиях окружающей среды	В.6.1	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
3 Испытания на устойчивость к пиковым выбросам внешних воздействий	В.6.2	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
4 Испытание с введением неисправностей (при требуемом диагностическом охвате $\geq$ 90 %)	В.6.10	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно	КР (HR) обязательно
5 Управление проектами	В.1.1	КР (HR) низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
6 Документация	В.1.2	КР(HR) низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
7 Статический анализ, динамический анализ, анализ отказов	В.6.4, В.6.5, В.6.6	— низкий	Р (R) средний	Р (R) средний	Р (R) высокий
8 Моделирование и анализ отказов	В.3.6, В 6.6	— низкий	Р (R) средний	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

Окончание таблицы В.5

Методы/меры	См. МЭК 61508-7	SIL1	SIL2	SIL3	SIL4
10 Статический анализ и анализ отказов (см. примечание 5)	В.6.4, В.6.6	Р (R) низкий	Р (R) средний	НР (NR) не рекомендуемый	НР (NR) не рекомендуемый
11 Расширенное функциональное тестирование	В.6.8	— низкий	КР (HR) средний	КР (HR) средний	КР (HR) высокий
12 Тестирование методом «черного ящика»	В.5.2	Р (R) низкий	Р (R) средний	Р (R) средний	Р (R) высокий
13 Испытания с введением неисправностей (при требуемом диагностическом охвате < 90 %)	В.6.10	Р (R) низкий	Р (R) средний	Р (R) средний	Р (R) высокий
14 Статистическое тестирование	В.5.3	— низкий	— средний	Р (R) средний	Р (R) высокий
15 Испытания в наихудших случаях	В.6.9	— низкий	— средний	Р (R) средний	Р (R) высокий
16 Полевые испытания	В.5.4	Р (R) низкий	Р (R) средний	Р (R) средний	НР (NR) не рекомендуемый

Примечания

1 Методы 7— 16, обозначенные «Р (R)», являются заменяемыми, 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 (SIL) 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 для низкого и высокого уровней эффективности. Усилия, требуемые для среднего уровня эффективности, находятся между усилиями, требуемыми для низкого и высокого уровней эффективности.

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

5 Статистический анализ и анализ отказов не рекомендуются для SIL3 и SIL4, т.к. 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	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

Продолжение таблицы В.6

Методы/меры, средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
Разделение E/E/PE систем, связанных с безопасностью, и систем, не связанных с безопасностью	В.1.3	Хорошо определенные интерфейсы между E/E/PE системами, связанными с безопасностью, и системами, не связанными с безопасностью	Полное отделение E/E/PE систем, связанных с безопасностью, от систем, не связанных с безопасностью, т.е. отсутствие доступа по проводам систем, не связанных с безопасностью к E/E/PE системам, связанным с безопасностью, физическое разделение в пространстве во избежание влияний по общей причине
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 нижнем 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 E/E/PE 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 одному специфическому 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 безопасности, концентрация на главных проблемах безопасности	Подготовленные подробные таблицы контрольных проверок для всех стадий жизненного цикла 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 компонентов схемы; отслеживание взаимосвязи между спецификацией, проектом, принципиальными схемами и перечнем компонентов системы; автоматизация; использование определенных методов (см. также 7.4.4)
Использование достоверно испытанных компонентов (см. примечание)	В.3.3	Достаточная перепроверка характеристик конструкции	Проверка на практике (см. 7.4.7.6)

Продолжение таблицы В.6

Методы/меры, средства	См. МЭК 61508-7	Низкая эффективность	Высокая эффективность
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 выход отказа
Средства автоматизированного проектирования	В.3.5	Автоматизированная поддержка сложных стадий жизненного цикла безопасности	Использование средств, хорошо проверенных на практике (см. 7.4.7.6), или средств с подтвержденным соответствием; полная автоматизация создания системы для всех стадий жизненного цикла безопасности
Моделирование	В.3.6	Моделирование на модульном уровне, включая предельные данные внешних устройств	Моделирование на уровне компонентов, включая предельные 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, не зависимым 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 ч эксплуатации; по крайней мере, один год эксплуатации как минимум десяти устройств в различных применениях; статистическая точность 95 %; отсутствие каких-либо критических отказов безопасности	10 млн часов эксплуатации; по крайней мере, два года эксплуатации как минимум 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 большая, чем для граничных значений реальных режимов эксплуатации
Статический анализ	В.6.4	Основанный на блок-схемах; выявление слабых точек, задание условий испытаний	Основанное на подробных схемах, предсказание ожидаемого поведения в случаях испытаний, применение инструментов испытаний
Динамический анализ	В.6.5	Основанный на блок-схемах; выявление слабых точек, задание условий испытаний	Основанное на подробных схемах, предсказание ожидаемого поведения в случаях испытаний, применение инструментов испытаний
Анализ отказов	В.6.6	На уровне модулей, включая граничные данные периферийных устройств	На уровне компонентов, включая граничные данные
Анализ на наихудший случай	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 проверяются при таких статических входных состояниях, как и в случаях, вызванных процессами отказов, или условиями эксплуатации	Испытания, при которых все функции безопасности проверяются при таких статических входных состояниях и/или необычных входных изменениях, как 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 проверяются 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 составляющих устройств, включая граничные данные периферийных устройств	На уровне компонентов, включая граничные данные
Примечание — В случаях, когда методы и средства В.1.1, В.1.2, В.3.3, В.3.4, В.4.4, В.4.6, В.5.2, В.5.3 и В.5.4 используются в качестве высокоэффективных методов и средств, предполагается, что будут также использованы методы и средства с низким уровнем эффективности.			

Приложение С
(обязательное)

Диагностический охват и доля безопасных отказов

С.1 Расчет диагностического охвата и доли безопасных отказов

Диагностический охват и доли безопасных отказов рассчитываются следующим образом:

a) проводят анализ видов отказов и их влияния для определения влияния каждого вида отказов каждого компонента или группы компонентов в подсистеме на поведение E/E/PE 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 требуются:

- подробная блок-схема E/E/PE системы, связанной с безопасностью, описывающая подсистему вместе со взаимосвязями для той части E/E/PE системы, связанной с безопасностью, которая затрагивает рассматриваемую(ые) функцию(ии) безопасности,
- схемные решения подсистемы аппаратных средств, 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. МЭК 61508-1, подраздел 4.1). 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 специфичны в соответствии с конкретными типами компонентов и существующей окружающей средой. Также очень важен полный и подробный анализ для подсистемы, используемой в архитектуре аппаратных средств, имеющей нулевую устойчивость к отказам аппаратных средств.

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

- безопасным отказом (т.е. не приводящим к снижению полноты безопасности E/E/PE системы, связанной с безопасностью, например, приводящим к безопасному отключению, или не влияющим на полноту безопасности E/E/PE системы, связанной с безопасностью), или
- опасным отказом (т.е. приводящим к отказу выполнения функции безопасности E/E/PE системой, связанной с безопасностью, или ее частью, либо к невыполнению полноты безопасности E/E/PE системы, связанной с безопасностью),

c) оценив частоты отказов каждого компонента или группы компонентов λ (см. перечисление a) и примечания) и учтя виды отказов и результаты анализа последствий каждого вида отказа каждого компонента или группы компонентов в подсистеме, вычисляют частоту безопасных отказов λ_S и частоту опасных отказов λ_D.

Примечания

1 Частота отказов каждого из компонентов или группы компонентов — это частота отказов λ, которые происходят в течение относительно небольшого промежутка времени t, в случаях, если λt значительно меньше единицы.

2 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 подсистема состоит из небольшого числа компонентов и если любая ошибка в оценке вероятности безопасных и опасных отказов специфического компонента может оказать существенное влияние на оценку безопасной составляющей отказа;

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

e) вычисляют полные частоты опасного отказа $\Sigma\lambda_D$ подсистемы, полные частоты опасных отказов, обнаруженных диагностическими тестами $\Sigma\lambda_{DD}$, и полные частоты безопасных отказов $\Sigma\lambda_S$;

f) вычисляют диагностический охват подсистемы как $\Sigma\lambda_{DD}/\Sigma\lambda_D$,

g) вычисляют долю безопасных отказов подсистемы как $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Примечание — Диагностический охват каждой подсистемы в E/E/PE системе, связанной с безопасностью, должен учитываться в вычислении случайных отказов аппаратных средств (см. 7.4.3.2.2). Доля безопасных отказов должна быть принята во внимание при определении архитектурных ограничений на полноту безопасности аппаратных средств (см. 7.4.3.1).

Анализ, выполняемый для определения диагностического охвата и доли безопасных отказов, должен охватывать все компоненты, в том числе электрические, электронные, электромеханические, механические и т.п., необходимые подсистеме для выполнения функции(ий) безопасности, которые требуются E/E/PE системе, связанной с безопасностью. Для каждого из компонентов должны быть рассмотрены все возможные виды опасных отказов, приводящие к опасному состоянию, препятствуя реакции безопасности, если такая реакция определена или так или иначе ставит под угрозу полноту безопасности, E/E/PE систем, связанных с безопасностью.

Ошибки и отказы, которые, как минимум, должны быть обнаружены для достижения уместного диагностического охвата, или, как минимум, должны быть включены в определение безопасной составляющей отказа, приведены в таблице А.1.

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

Примечания

1 Пример вычисления диагностического охвата и безопасной составляющей отказа представлен в МЭК 61508-6, приложение С.

2 Для вычисления степени диагностического охвата можно использовать альтернативные методы, например моделирование ошибок с помощью подробных компьютерных моделей как схем E/E/PE систем, связанных с безопасностью, так и используемых при разработке электронных компонентов, например на уровне транзисторов в интегральной схеме.

С.2 Определение факторов диагностического охвата

При вычислении диагностического охвата для подсистемы (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 диагностический охват, 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 диагностического охвата 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 100 %-ного диагностического охвата. Однако для более сложных компонентов типа В (см. 7.4.3.1.3) должны быть учтены ограничения диагностического охвата для различных компонентов, представленных в таблице А.1. Этот анализ должен быть проведен для каждого компонента или группы компонентов каждой подсистемы и каждой E/E/PE системы, связанной с безопасностью.

Примечания

1 Рекомендуемые методы и средства для диагностических тестов (испытаний) и рекомендуемые максимальные диагностические охваты, которые могут потребоваться, приведены в приложении А, таблицах А.2 — А.15. Эти тесты проводят непрерывно или периодически (в зависимости от интервала диагностического тестирования). Требования таблиц А.2 — А.15 не заменяют требований приложения С.

2 Диагностические тесты могут обеспечить значительные преимущества в достижении функциональной безопасности E/E/PE систем, связанных 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 E/E/PE систем, связанных с безопасностью.

3 При расчетах диагностического охвата и путей его использования предполагается, что E/E/PE системы, связанные с безопасностью, успешно работают в присутствии другого опасного повреждения, обнаруженного диагностическими тестами. Если это предположение не верно, то E/E/PE систему, связанную с безопасностью, следует рассматривать как систему, действующую в режиме с высокой частотой запросов или с непрерывными запросами (см. 7.4.6.3 и 7.4.3.2.5).

4 Определение диагностического охвата приведено в МЭК 61508-4 (пункт 3.8.6) Важно отметить, что существуют альтернативные определения, но здесь они не применяются.

5 Диагностическое тестирование, используемое для обнаружения опасных отказов внутри подсистемы, может быть проведено другой подсистемой внутри E/E/PE системы, связанной с безопасностью.

6 Диагностические тесты могут проводиться непрерывно или периодически в зависимости от диагностического испытательного интервала. Зафиксированы случаи 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
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица D.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта Российской Федерации
ИСО/МЭК Руководство 51:1990	ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты
МЭК Руководство 104:1997	*
МЭК 60050-371:1984	*
МЭК 60300-3-2:2004	*
МЭК 61000-1-1:1992	*
МЭК 61000-2-5:1995	*
МЭК 61508-1:1998	ГОСТ Р МЭК 61508-1—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
МЭК 61508-3:1998	ГОСТ Р МЭК 61508-3—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
МЭК 61508-4:1998	ГОСТ Р МЭК 61508-4—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения
МЭК 61508-5:1998	ГОСТ Р МЭК 61508-5—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
МЭК 61508-6:2000	ГОСТ Р МЭК 61508-6—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2000 и МЭК 61508-3:1998
МЭК 61508-7:2000	ГОСТ Р МЭК 61508-7—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства
IEEE 352:1987	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Библиография

[1] IEC 61511-SER — Functional safety — Safety instrumented systems for the process industry sector — ALL PARTS

[2] IEC 61000-4 — Electromagnetic compatibility — Part 4: Testing and measurement techniques

[3] IEC 60050-191:1990 — International Electrotechnical Vocabulary (IEV). Chapter 191: Dependability and quality of service

[4] IEC 61164:1995 — Reliability growth — Statistical test and estimation methods

[5] IEC 60870-5-1:1990 — Telecontrol equipment and systems. Part 5: Transmission protocols — Section One: Transmission frame formats

[6] EN 50159-1 — Railway applications — Safety-related communication in closed transmission systems

[7] EN 50159-2 — Railway applications — Safety-related communication in open transmission systems

[8] EN 50205:2002 — Relays with forcibly guided (mechanically linked) contacts

[9] EN 60947-5-1:2004 — Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices

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 *В.Н. Копысов*
Технический редактор *Н.С. Гришанова*
Корректор *М.В. Бучная*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 02.07.2008. Подписано в печать 18.09.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал:
Печать офсетная. Усл. печ. л. 7,44. Уч.-изд. л. 6,90. Тираж 253 экз. Зак. 1143.

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

gost.e-ecolog.ru