ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-6— 2007

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

Часть 6

Руководство по применению ГОСТ Р МЭК 61508-2—2007 и ГОСТ Р МЭК 61508-3—2007

IEC 61508-6:2000
Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IDT)

Издание официальное

БЗ 4—2007/64

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 «Стандартизации 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 61508-6:2000 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2000 и МЭК 61508-3:1998» (IEC 61508-6:2000 «Functional safety of electrical / electronic / programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (подраздел 3.5).

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

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, определения и сокращения 3
Приложение A (справочное) Применение МЭК 61508-2 и МЭК 61508-3 4
Приложение B (справочное) Метод оценки вероятностей отказа аппаратных средств 11
Приложение C (справочное) Расчет диагностического охвата и доли безопасных отказов 36
Приложение D (справочное) Методика количественного определения влияния отказов аппаратных средств с общей причиной в E/E/PE системах 39
Приложение E (справочное) Применение таблиц полноты безопасности программного обеспечения в соответствии с МЭК 61508-3 49
Приложение F (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 60
Библиография 61

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)], используемые 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, важно, чтобы лица, ответственные за принятие решений, имели в своем распоряжении практические руководства по вопросам безопасности.

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)], используемых для выполнения функций безопасности. Этот унифицированный подход был принят для разработки рациональной и последовательной технической концепции 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 использованием в них нескольких систем защиты, в которых используются различные (например механические, гидравлические, пневматические, электрические, электронные, программируемые электронные) технологии. Следовательно, любая стратегия безопасности должна учитывать не только элементы, входящие в состав отдельных систем (например датчики, управляющие устройства и исполнительные механизмы), но также и 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 отказов10^{-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 6

Руководство по применению ГОСТ Р МЭК 61508-2—2007 и ГОСТ Р МЭК 61508-3—2007

Functional safety of electrical, electronic, programmable electronic safety-related systems.
Part 6. Guidelines on the application of GOST R IEC 61508-2—2007 and GOST R IEC 61508-3—2007

Дата введения — 2008 — 09 — 01

1 Область применения

1.1 Настоящий стандарт содержит информацию и руководящие указания по применению МЭК 61508-2 и МЭК 61508-3.

Краткий обзор требований МЭК 61508-2 и МЭК 61508-3 и определение функциональной последовательности их применения содержится в приложении А.

Пример методики расчета вероятности отказа аппаратных средств содержится в приложении В, которое следует применять совместно с МЭК 61508-2 (пункт 7.4.3 и приложение С) и приложением D настоящего стандарта.

Пример расчета диагностического охвата содержится в приложении С, которое следует применять совместно с МЭК 61508-2 (приложение С).

Метод количественной оценки влияния отказов аппаратных средств по общей причине на вероятность отказов — по приложению D.

Примеры применения таблиц полноты безопасности программного обеспечения, приведенных в МЭК 61508-3 (приложение А), для уровней полноты безопасности 2 и 3 — по приложению Е.

1.2 МЭК 61508-1 — МЭК 61508-4 являются основополагающими стандартами по безопасности, хотя они не применяются 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 51:1999. Стандарты МЭК 61508-1 — МЭК 61508-4 предназначены также для использования в качестве самостоятельных стандартов.

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

Примечание — 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.

1.4 Структура комплекса стандартов МЭК 61508-1 — МЭК 61508-7 с указанием роли МЭК 61508-6 в достижении функциональной безопасности E/E/PE систем, связанных с безопасностью, показана на рисунке 1.

Издание официальное

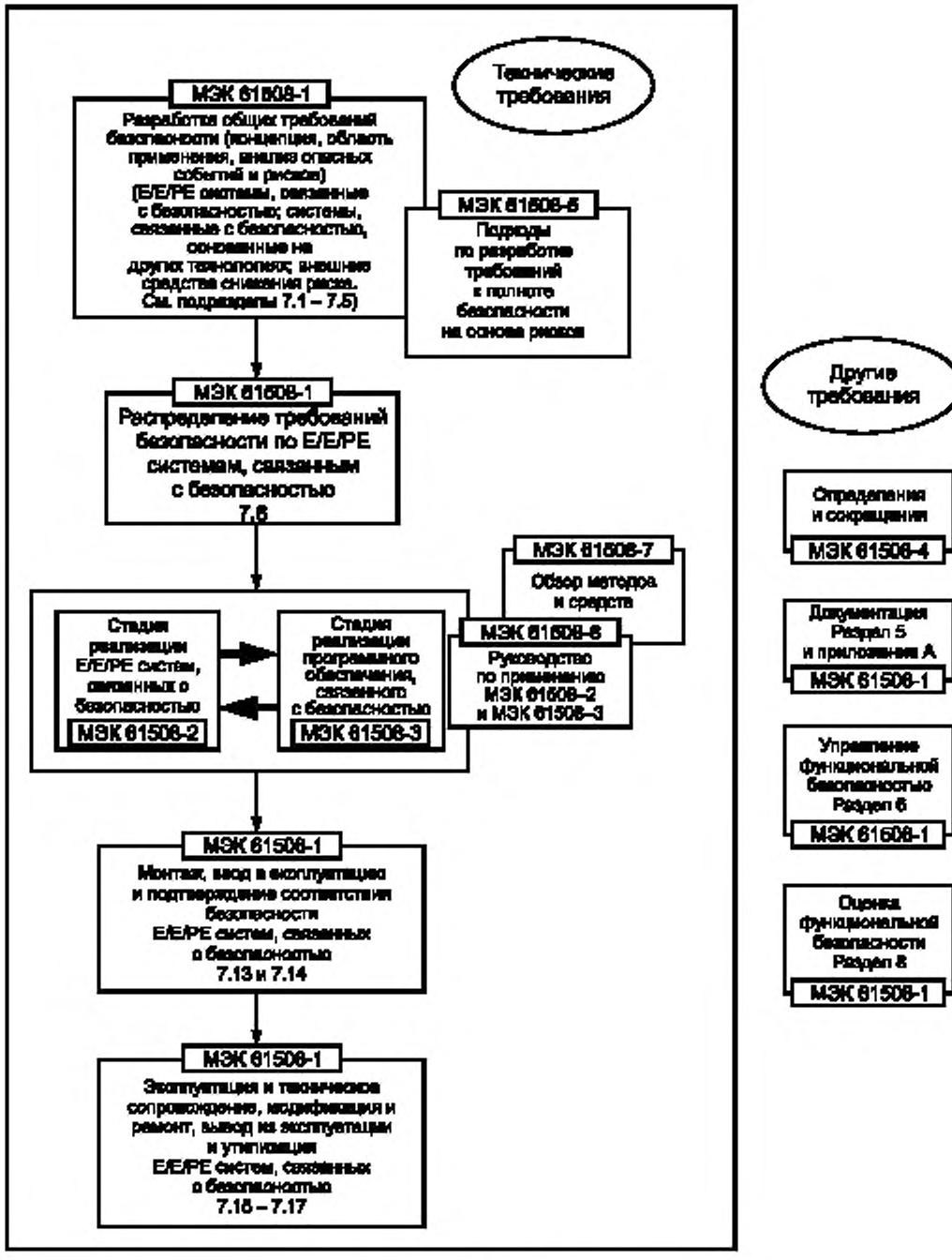


Рисунок 1 — Структура настоящего стандарта

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

ИСО/МЭК Руководство 51:1999 Аспекты безопасности — руководство по включению в стандарты

МЭК Руководство 104:1997 Руководство по подготовке стандартов по безопасности и использование базовых и групповых стандартов по безопасности

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

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

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

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. Определения и сокращения

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

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

3 Термины, определения и сокращения

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

Приложение А
(справочное)

Применение МЭК 61508-2 и МЭК 61508-3

А.1 Общие положения

Конкретные механизм, технологическая установка, а также другое оборудование могут в случае неправильной работы (например отказ электромеханических, электронных и/или программируемых электронных устройств) представлять опасность для людей и окружающей среды из-за возникновения опасных событий (например пожары, взрывы, избыточная радиация, попадание в механизмы и т. д.). Аварии оборудования могут возникать по причине физических отказов устройств (неожиданные аварии оборудования), либо систематических отказов (ошибки человека в технических условиях и конструкции конкретной системы при определенной комбинации причин приводят к систематическим отказам), либо некоторых внешних условий.

Общий подход, основанный на оценке рисков, для предотвращения и/или контроля отказов в электромеханических, электронных или программируемых электронных устройствах содержится в МЭК 61508-1.

Основная задача настоящего стандарта заключается в обеспечении безопасной автоматизации установок и оборудования, а его основная цель состоит в предотвращении:

- отказов систем управления, инициирующих другие события, которые, в свою очередь, могут привести к опасности (например утечка токсичных материалов, повторяющиеся удары механизмов и т. д.) и

- необнаруженных отказов систем защиты (например, в системах аварийной остановки), делающих эти системы недоступными в момент необходимости действий, связанных с безопасностью.

Требование проведения анализа опасности и риска для процесса/механизма, чтобы определить степень снижения риска, необходимую для удовлетворения критериям оценки риска для приложения, см. в МЭК 61508-1. Оценка риска основана на оценке как последствий (или серьезности), так и частоты (или вероятности) опасного события.

Требование использования степени снижения риска, определенной в процессе анализа, для решения о том, требуется ли одна или несколько систем, связанных с безопасностью[1)], и для выполнения каких функций обеспечения безопасности (каждая с заданной полнотой безопасности[2)]) требуются эти системы, содержится в МЭК 61508-1.

В МЭК 61508-2 и МЭК 61508-3 рассматриваются требования к функциям безопасности и полноте безопасности, установленные в МЭК 61508-1, для любой E/E/PE системы, связанной с безопасностью, а также устанавливаются требования к жизненному циклу безопасности, которые:

- применяются при разработке технического задания, проектировании и изменении аппаратных средств и программного обеспечения, а также

- фокусируются на средствах предотвращения и/или контроля случайных отказов аппаратных средств и систематических отказов (жизненные циклы безопасности E/E/PES и программного обеспечения[3)]).

МЭК 61508-2 и МЭК 61508-3 не содержат указаний, какой уровень полноты безопасности соответствует заданному требуемому приемлемому риску. Это решение зависит от многих факторов, включая характер применения, степень выполнения функций безопасности другими системами, а также социальные и экономические факторы (см. МЭК 61508-1 и МЭК 61508-5).

Требования МЭК 61508-2 и МЭК 61508-3 включают в себя:

- применение методов[4)] и средств, классифицированных в соответствии с уровнем полноты безопасности, чтобы избежать систематических отказов[5)] с помощью планово-предупредительных мер, и

[1)] Системы, необходимые для обеспечения функциональной безопасности и содержащие одно или несколько электрических (электромеханических), электронных или программируемых электронных (E/E/PE) устройств, называются системами E/E/PE, связанными с безопасностью, и включают в себя все оборудование, необходимое для реализации требуемой функции безопасности (см. МЭК 61508-4, пункт 3.4.1).

[2)] Уровень полноты безопасности определяется как один из четырех дискретных уровней. Уровень полноты безопасности 4 является наивысшим, а уровень полноты безопасности 1 — самым низшим (см. МЭК 61508-1, подпункт 7.6.2.9).

[3)] Чтобы сделать возможной четкую структуризацию требований настоящего стандарта, было принято решение упорядочить требования с помощью модели процесса разработки, в которой все этапы следуют в четкой последовательности с небольшим шагом (ее иногда называют потоковой моделью). Однако следует подчеркнуть, что может быть использован любой эквивалентный подход к описанию жизненного цикла при условии, что в плане обеспечения безопасности проекта будут описаны эквивалентные положения (см. МЭК 61508-1, раздел 6).

[4)] Требуемые методы и средства для каждого уровня полноты безопасности представлены в МЭК 61508-2 (таблицы приложений А и В) и МЭК 61508-3.

[5)] Систематические отказы обычно нельзя определить количественно. Причинами отказов бывают: ошибки при спецификации и проектировании технических средств и программного обеспечения; ошибки при учете условий окружающей среды (например, температуры) и ошибки в процессе работы (например слабый интерфейс).

- управление систематическими отказами (включая отказы программного обеспечения) и случайными отказами аппаратных средств с помощью конструктивных особенностей, таких как встроенные средства обнаружения повреждений, избыточность и особенности архитектуры (например диверсификация).

В МЭК 61508-2 гарантия того, что нужный уровень полноты безопасности будет удовлетворительным для опасных случайных отказов аппаратных средств, основывается на:

- требованиях к отказоустойчивости аппаратуры (см. МЭК 61508-2, таблицы 2 и 3) и
- диагностическом охвате и частоте контрольных испытаний подсистем и компонент с проведением анализа надежности, использующего соответствующие данные.

В МЭК 61508-2 и МЭК 61508-3 гарантия того, что нужный уровень полноты безопасности будет удовлетворительным для систематических отказов, достигается путем:

- правильного применения процедур управления безопасностью;
- использования компетентного персонала;
- выполнения предусмотренных действий по реализации жизненного цикла обеспечения безопасности, включая предусмотренные методы и средства[1)] и
- независимой оценки функциональной безопасности[2)].

Главная цель состоит в обеспечении того, что оставшиеся систематические отказы, соответствующие уровню полноты безопасности, не приведут к отказу E/E/PE системы, связанной с безопасностью.

МЭК 61508-2 был разработан, чтобы формализовать требования к обеспечению полноты безопасности аппаратных средств[3)] E/E/PE систем, связанных с безопасностью, включая датчики и оконечные элементы. Необходимы методы и средства, направленные против как случайных, так и систематических отказов аппаратных средств. Они, как указано выше, включают в себя соответствующую комбинацию средств по предотвращению неисправностей и управлению отказами. Если для обеспечения функциональной безопасности необходимы действия оператора, то приводятся требования к интерфейсу оператора. В МЭК 61508-2 для обнаружения случайных отказов аппаратных средств также определяются методы и средства диагностического тестирования, реализуемые на уровне программного обеспечения и аппаратных средств (например диверсификация).

МЭК 61508-3 был разработан, чтобы формализовать требования обеспечения полноты безопасности для программного обеспечения, как встроенного (включая диагностические средства обнаружения неисправностей), так и прикладного. МЭК 61508-3 требует использовать комбинированный подход, включающий исключение ошибок (обеспечение качества) и устойчивость к ошибкам (за счет архитектуры программного обеспечения), так как не существует известного способа проверить отсутствие отказов в достаточно сложном программном обеспечении, связанном с безопасностью, и, особенно, избежать ошибок в технических условиях и в проекте. МЭК 61508-3 требует принятия таких принципов разработки программного обеспечения, как проектирование сверху вниз, модульность, проверку на каждой стадии жизненного цикла разработки, проверку программных модулей и библиотек программных модулей, а также четкое документирование для облегчения контроля и проверки. Для различных уровней программного обеспечения требуются различные уровни гарантии того, что эти и связанные с ними принципы были правильно реализованы.

Разработчик программного обеспечения может быть или не быть частью организации, создающей всю E/E/PES. В любом случае необходимо тесное сотрудничество, особенно при разработке архитектуры программируемой электроники, когда требуется анализировать компромиссы между архитектурами аппаратных средств и программного обеспечения на предмет их вклада в обеспечение безопасности (см. МЭК 61508-2, рисунок 4).

А.2 Функциональные этапы применения МЭК 61508-2

Функциональные этапы применения МЭК 61508-2 представлены в настоящем приложении, рисунки А.1 и А.2. Функциональные этапы применения МЭК 61508-3 представлены на рисунке А.3.

Для МЭК 61508-2 можно выделить следующие функциональные этапы (см. приложение А, рисунки А.1 и А.2):

а) Определяют распределение требований безопасности (МЭК 61508-1). При необходимости модернизируют планирование безопасности в процессе разработки E/E/PES.

b) Определяют требования безопасности для E/E/PES, включая требования к полноте безопасности, для каждой функции безопасности (МЭК 61508-2, подраздел 7.2). Определяют требования к программному обеспечению и передают их поставщику и/или разработчику программного обеспечения для применения МЭК 61508-3.

[1)] Средства, альтернативные описанным в настоящем стандарте, можно использовать при условии, что при планировании обеспечения безопасности документируются оправдывающие обстоятельства (см. МЭК 61508-1, раздел 6).

[2)] Независимая оценка не всегда подразумевает проведение оценки третьей стороной (см. МЭК 61508-1, раздел 8).

[3)] Включая постоянное встроенное программное обеспечение или эквиваленты программного обеспечения (также называемые программно-аппаратными средствами), например специализированные интегральные схемы.

Примечание — На этой стадии необходимо рассмотреть возможность одновременных отказов в системе управления EUC и E/E/PE системе (системах), связанной с безопасностью, (см. МЭК 61508-1, подпункт 7.5.2.4). Такие отказы могут быть результатом отказов компонентов по общей причине, например, из-за влияния окружающей среды. Наличие подобных отказов может привести к большим по сравнению с ожидаемым значениям остаточного риска.

c) Начинают планирование подтверждения соответствия безопасности E/E/PES (см. МЭК 61508-2, подраздел 7.3).

d) Задают архитектуру (конфигурацию) логической подсистемы, датчиков и оконечных элементов. Вместе с поставщиком/разработчиком программного обеспечения анализируют архитектуру аппаратных средств, программного обеспечения и влияние на безопасность компромиссов между аппаратными средствами и программным обеспечением (см. МЭК 61508-2, рисунок 4). При необходимости анализ повторяют.

e) Разрабатывают модель архитектуры аппаратных средств для E/E/PE системы, связанной с безопасностью. Эту модель разрабатывают, проверяя отдельно каждую функцию безопасности, и определяют подсистему (компонент), используемую для реализации этой функции.

f) Устанавливают параметры для каждой подсистемы (компонента), используемой в E/E/PE системе, связанной с безопасностью. Для каждой подсистемы (компонента) определяют:

- временной интервал проведения процедур тестирования для отказов, которые не обнаруживаются автоматически;
- среднее время восстановления;
- диагностический охват (см. МЭК 61508-2, приложение C);
- вероятность отказа и
- долю безопасных отказов (см. МЭК 61508-2, приложение C).

g) Определяют архитектурные ограничения (см. МЭК 61508-2, таблицы 2 и 3).

h) Создают модель расчета надежности для каждой функции безопасности, которую должна реализовать E/E/PE система, связанную с безопасностью.

Примечание — Модель расчета надежности представляет собой математическую формулу, показывающую взаимосвязь между надежностью и соответствующими параметрами, связанными с оборудованием и условиями его использования.

i) Рассчитывают прогнозируемую надежность для каждой функции безопасности, используя соответствующую методику. Сравнивают результат с заданными характеристиками отказов, определенными в перечислении b), и требованиями в соответствии с МЭК 61508-2, подпункт 7.4.3.1, таблицы 2 и 3. Если прогнозируемая надежность не соответствует заданным характеристикам отказов и/или требованиям МЭК 61508-2, таблицы 2 и 3, то изменяют:

- если возможно, один или несколько параметров подсистемы [возвращаются к перечислению f)] и/или
- архитектуру аппаратных средств [возвращаются к перечислению d)].

Примечание — Существует множество методов моделирования, и аналитик должен выбрать наиболее соответствующий (перечень некоторых методов, которые могут быть использованы, приведен в МЭК 61508-2, подпункт 7.4.3.2.2, перечисление h), примечание 4).

j) Реализуют проект E/E/PE системы, связанной с безопасностью. Выбирают средства и методы для управления систематическими отказами аппаратных средств, отказами, вызванными влиянием окружающей среды, и эксплуатационными отказами (см. МЭК 61508-2, приложение A).

k) Загружают проверенное программное обеспечение (см. МЭК 61508-3) в соответствующие аппаратные средства (см. МЭК 61508-2, подраздел 7.5 и приложение B) и параллельно разрабатывают рабочие инструкции для пользователей и документацию для обслуживающего персонала по эксплуатации системы (см. МЭК 61508-2, подраздел 7.6 и приложение B). Учитывают аспекты, связанные с программным обеспечением (см. пункт A.3, перечисление f)).

l) Вместе с разработчиком программного обеспечения (см. МЭК 61508-3, подраздел 7.7) проводят подтверждение соответствия E/E/PES (см. МЭК 61508-2, подраздел 7.7 и приложение B).

m) Передают аппаратные средства и результаты подтверждения соответствия безопасности E/E/PES системным инженерам для дальнейшей интеграции в комплексную систему.

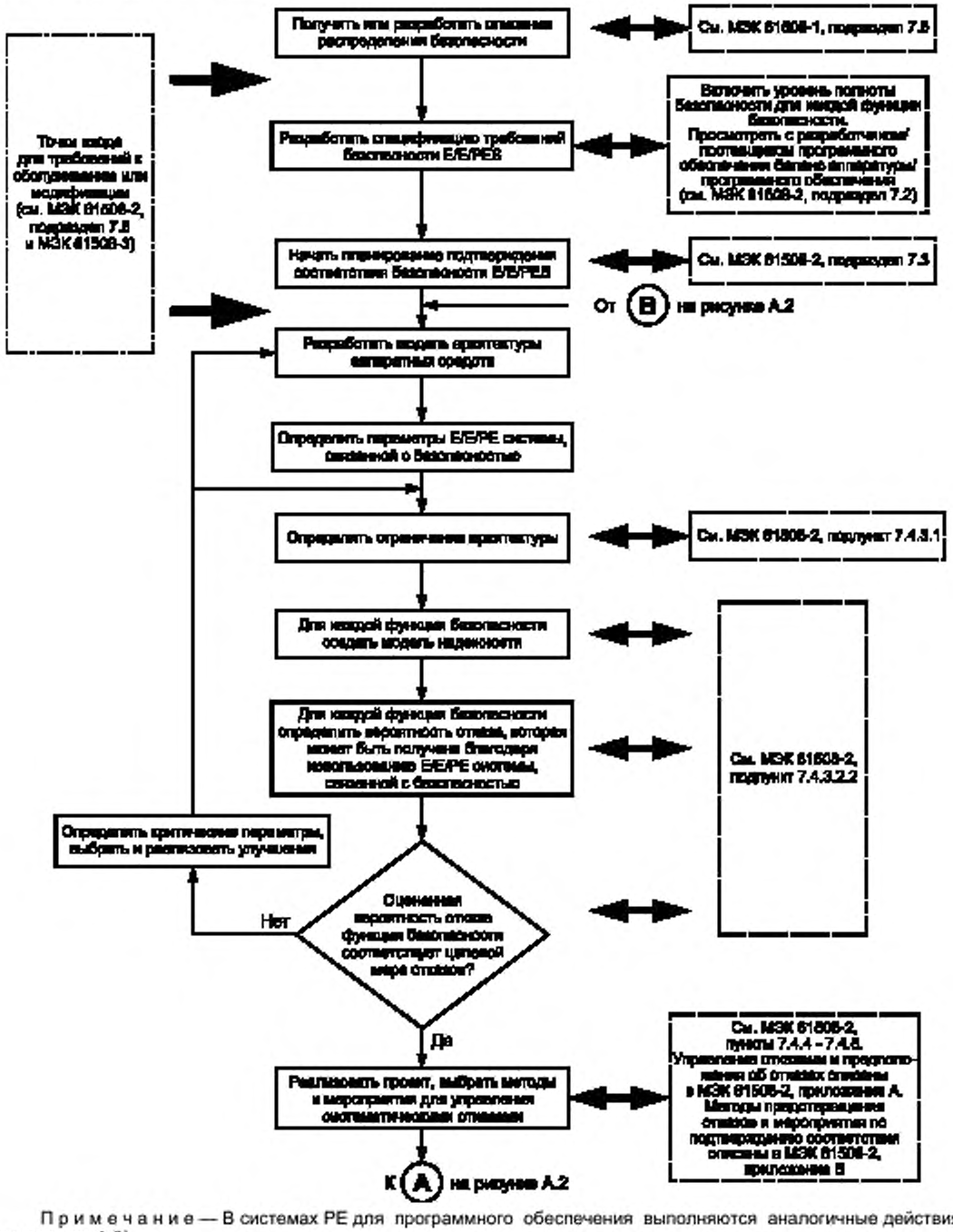
n) Если в процессе эксплуатации E/E/PES требуется модернизация/обслуживание, то при необходимости снова обращаются к МЭК 61508-2, подраздел 7.8.

В процессе жизненного цикла безопасности E/E/PES выполняется множество различных действий. Среди них верификация (см. МЭК 61508-2, подраздел 7.9) и оценка функциональной безопасности (см. МЭК 61508-1, раздел 8).

В процессе выполнения приведенных выше действий выбирают методы и средства для обеспечения безопасности E/E/PES, соответствующие требуемому уровню полноты безопасности. Для помощи с выбором таких методов и средств составлены таблицы, упорядочивающие различные методы/средства в соответствии с четырьмя уровнями полноты безопасности (см. МЭК 61508-2, приложение B). Краткий обзор каждого из методов и средств со ссылками на источники информации о них, включая перекрестные ссылки на эти таблицы, представлен в МЭК 61508-7, приложения A и B.

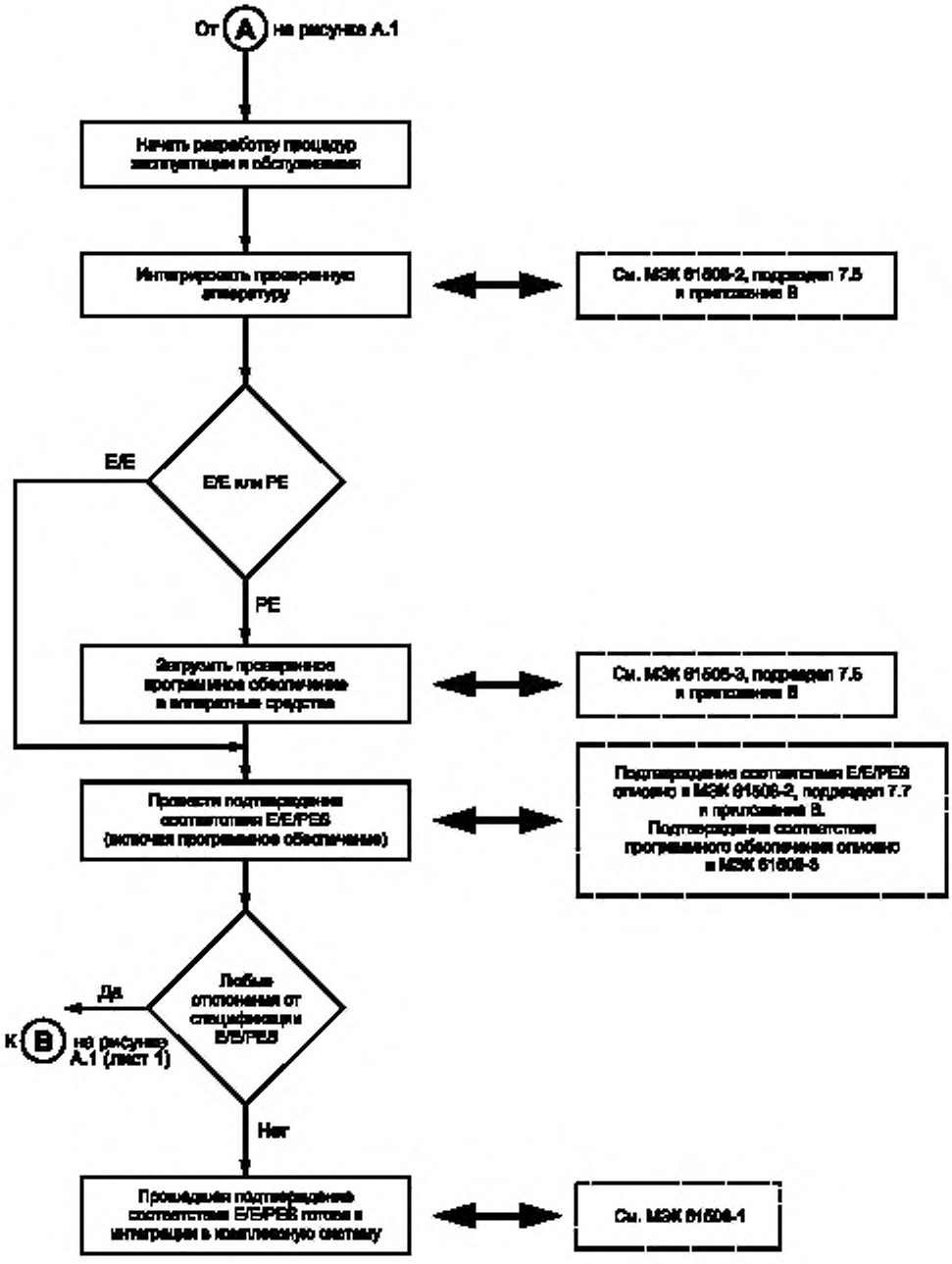
Один из возможных методов расчета вероятностей отказа аппаратных средств для E/E/PE систем, связанных с безопасностью, представлен в приложении B.

Примечание — При выполнении приведенных выше действий допускается применять средства, альтернативные указанным в настоящем стандарте при условии, что оправдывающие обстоятельства документируются в процессе планирования безопасности (см. МЭК 61508-1, раздел 6).



Примечание — В системах РЕ для программного обеспечения выполняются аналогичные действия (см. рисунок А.3).

Рисунок А.1 — Функциональные этапы применения МЭК 61508-2



Примечание — В системах PE для программного обеспечения выполняются аналогичные действия (см. рисунок А.3).

Рисунок А.2 — Функциональные этапы применения МЭК 61508-2 (продолжение)

А.3 Функциональные этапы применения МЭК 61508-3

Можно выделить следующие функциональные этапы применения МЭК 61508-3 (см. рисунок А.3):

a) Определяют требования для систем E/E/PE, связанных с безопасностью, и соответствующих компонент планирования безопасности (см. МЭК 61508-2, подраздел 7.3). При необходимости модернизируют планирование безопасности в процессе разработки программного обеспечения.

Примечание — На предыдущих стадиях жизненного цикла были:

- определены требуемые функции безопасности и соответствующие им уровни полноты безопасности (см. МЭК 61508-1, подразделы 7.4 и 7.5);
- распределены функции безопасности для назначенных систем E/E/PE, связанных с безопасностью (см. МЭК 61508-1, подраздел 7.6) и
- распределены реализуемые программно функции внутри каждой системы E/E/PE, связанной с безопасностью (см. МЭК 61508-2, подраздел 7.2).

b) Определяют архитектуру программного обеспечения для всех реализуемых программно функций безопасности (см. МЭК 61508-3, подраздел 7.4 и приложение А).

c) Вместе с поставщиком/разработчиком E/E/PES анализируют архитектуру аппаратных средств и программного обеспечения и влияние на безопасность компромиссов между аппаратными средствами и программным обеспечением (см. МЭК 61508-2, рисунок 4). При необходимости анализ повторяют.

d) Приступают к планированию проверки и подтверждения соответствия безопасности программного обеспечения (см. МЭК 61508-3, подразделы 7.3 и 7.9).

e) Проектируют, разрабатывают и проверяют/тестируют программное обеспечение в соответствии с:

- планированием безопасности программного обеспечения;
- уровнем полноты безопасности программного обеспечения;
- жизненным циклом безопасности программного обеспечения.

f) Завершают действия по окончательной проверке программного обеспечения и интегрируют проверенное программное обеспечение в соответствующие аппаратные средства (см. МЭК 61508-3, подраздел 7.5) и параллельно разрабатывают рабочие инструкции для пользователей и инструкции по эксплуатации для обслуживающего персонала системы программного обеспечения (см. МЭК 61508-3, подраздел 7.6 и приложение А, подраздел А.2, а также перечисление k) настоящего стандарта).

g) Вместе с разработчиком аппаратных средств (см. МЭК 61508-2, подраздел 7.7) проводят подтверждение соответствия безопасности программного обеспечения в интегрированных системах E/E/PE, связанных с безопасностью (см. МЭК 61508-3, подраздел 7.7).

h) Передают результаты подтверждения соответствия безопасности программного обеспечения системным инженерам для дальнейшей интеграции в комплексную систему.

i) Если в процессе эксплуатации потребуется модернизация программного обеспечения E/E/PES, то при необходимости снова возвращаются к соответствующей стадии, как описано в МЭК 61508-3, подраздел 7.8.

В процессе жизненного цикла безопасности программного обеспечения выполняют множество различных действий. В том числе проверку (см. МЭК 61508-3, подраздел 7.9) и оценку функциональной безопасности (см. МЭК 61508-3, раздел 8).

В процессе выполнения приведенных выше этапов выбирают средства и методы обеспечения безопасности программного обеспечения, соответствующие требуемой полноте безопасности. Для помощи в выборе таких методов и средств составлены таблицы, упорядочивающие различные методы/средства в соответствии с четырьмя уровнями полноты безопасности (см. МЭК 61508-3, приложение А). Обзор каждого из методов и средств со ссылками на источники информации о них, включая перекрестные ссылки на эти таблицы, представлен в МЭК 61508-7, приложение С.

Примеры применения таблиц полноты безопасности приведены в приложении Е настоящего стандарта, а МЭК 61508-7 включает в себя описание вероятностного подхода к определению полноты безопасности программного обеспечения для уже разработанного программного обеспечения (см. МЭК 61508-7, приложение D).

Примечание — При выполнении приведенных выше действий допускается применять средства, альтернативные указанным в настоящем стандарте при условии, что оправдывающие обстоятельства документируются в процессе планирования безопасности (см. МЭК 61508-1, раздел 6).

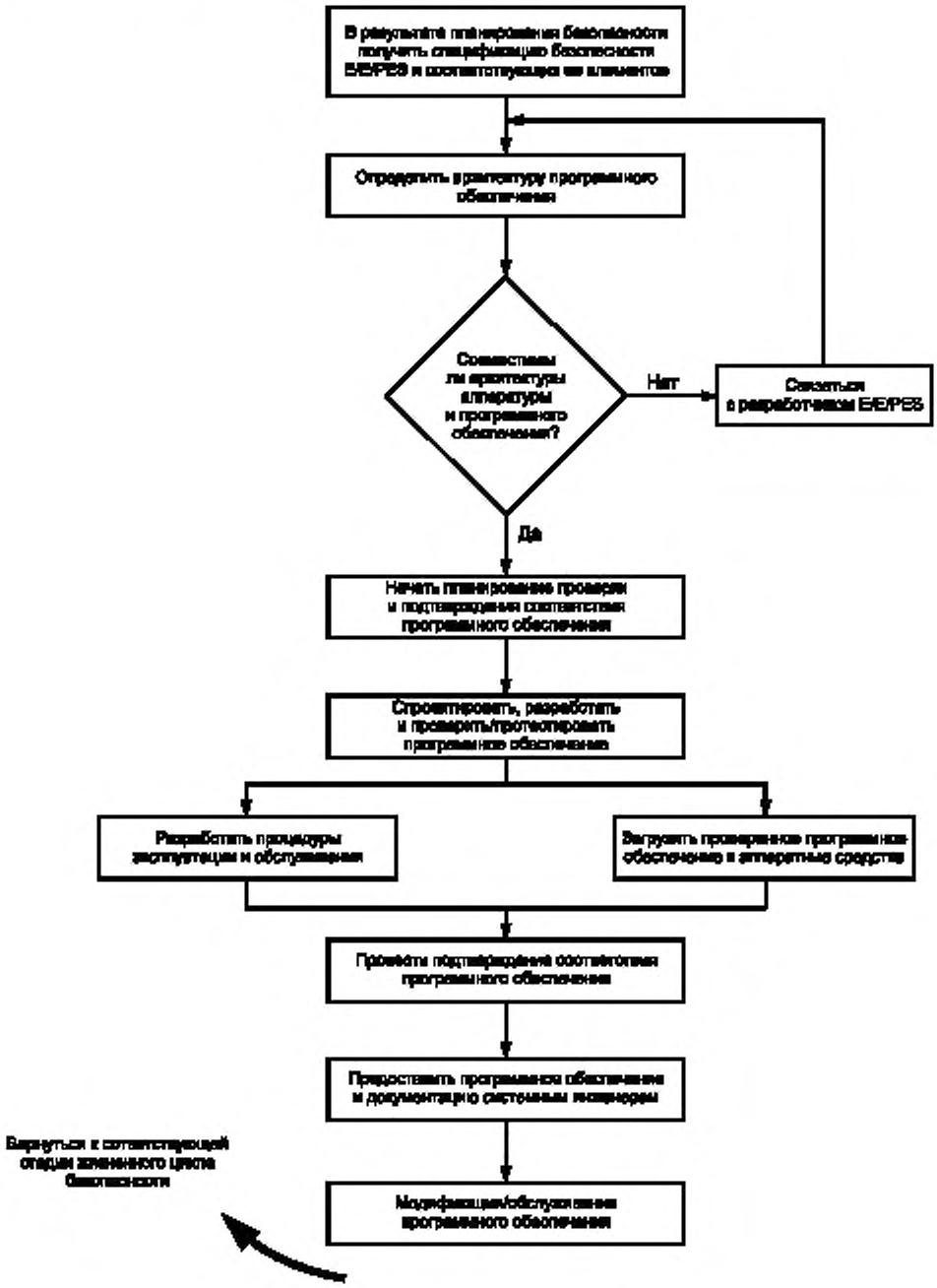


Рисунок А.3 — Функциональные этапы применения МЭК 61508-3

Приложение В
(справочное)

Метод оценки вероятностей отказа аппаратных средств

В.1 Общие положения

Настоящее приложение содержит один из методов расчета вероятностей отказа для E/E/PE систем, связанных с безопасностью, установленных в соответствии с МЭК 61508-1 — МЭК 61508-3. Метод не должен рассматриваться в качестве единственно возможного. Однако в данном методе реализуется относительно простой подход к оценке характеристик E/E/PE систем, связанных с безопасностью.

Существуют различные методы анализа уровня безопасности аппаратных средств E/E/PE систем, связанных с безопасностью. Наиболее распространенными методами являются метод блок-схем надежности (см. МЭК 61508-7, приложение С, пункт С.6.5) и метод, основанный на марковских моделях (см. МЭК 61508-7, приложение С, пункт С.6.4). Оба метода при правильном применении дают аналогичные результаты, но в случае сложных программируемых электронных подсистем (например, при перекрестном голосовании по нескольким каналам и автоматическом тестировании) метод блок-схем надежности дает некоторую потерю точности по сравнению с методом, основанным на марковских моделях.

При рассмотрении E/E/PE системы, связанной с безопасностью, в целом эта потеря точности может быть незначительной, если учитывается точность данных о надежности, используемых при анализе. Например, основная потеря точности при анализе уровня безопасности аппаратных средств для E/E/PE систем, связанных с безопасностью, зависит от приборов для измерения полей. Имеет ли значение потеря точности, можно определить только для конкретных условий. В случае сложных программируемых электронных подсистем результаты оценки полноты безопасности аппаратуры методом блок-схем надежности более пессимистичны, чем методом, основанным на марковских моделях (т.е. метод блок-схем надежности дает большую вероятность отказа). В настоящем приложении применяется метод блок-схем надежности.

Если отказ системы управления EUC инициирует обращение к E/E/PE системе, связанной с безопасностью, то вероятность возникновения опасного события зависит также и от вероятности отказа системы управления EUC. В этой ситуации необходимо рассмотреть возможность одновременного отказа компонентов системы управления EUC и E/E/PE системы, связанной с безопасностью, из-за механизмов отказа по общей причине. При неправильном анализе наличие подобных отказов может привести к бóльшим, по сравнению с ожидаемым, значениям остаточного риска.

Расчеты вероятностей отказа аппаратных средств E/E/PE систем, связанных с безопасностью, основываются на следующих предположениях:

- значение результирующей средней вероятности отказа выполнения функции безопасности для подсистемы меньше 10^{-1} или значение результирующей вероятности отказа в час для подсистемы меньше 10^{-5};
- частота отказов компонент постоянна в течение стадий жизни системы;
- подсистема датчиков (подсистема ввода) состоит из реального датчика(ов) и любых других компонент и соединительных проводов, вплоть до компоненты (компонент), но ее (их) не включая, где сигналы впервые объединяются с помощью процедуры голосования или другой процедуры (например, конфигурация каналов из двух датчиков, представленная на рисунке В.1 настоящего приложения);
- логическая подсистема включает в себя компоненту (компоненты), в которой(ых) сигналы вначале объединяются, и все другие компоненты, вплоть до тех компонент включительно, откуда результирующий сигнал(ы) передается(ются) подсистеме оконечных элементов;
- подсистема оконечных элементов (подсистема вывода) включает в себя компоненты и соединения, которые обрабатывают конечный сигнал(ы), получаемый(ые) от логической подсистемы, включая оконечный исполнительный компонент(ы);
- частоты отказов аппаратных средств, используемые в качестве входных данных для расчетов и таблиц, задаются для одного канала подсистемы (например, при использовании датчиков в виде архитектуры 2oo3 частота отказов задается для одного датчика, а влияние архитектуры 2oo3 рассчитывается дополнительно);
- частоты отказов и диагностический охват одинаковы для всех каналов в архитектуре подсистемы;
- общая частота отказов аппаратных средств канала подсистемы является суммой частоты опасных и частоты безопасных отказов для данного канала, которые полагают равными.

Примечание — Это предположение влияет на долю безопасных отказов (см. МЭК 61508-2, приложение С), но доля безопасных отказов не влияет на рассчитанные значения вероятности отказа, приведенные в настоящем приложении.

- для каждой функции безопасности существуют идеальные средства тестирования и устранения отказов (т.е. все отказы, оставшиеся необнаруженными, обнаруживаются при тестировании), влияние неидеального тестирования в соответствии с приложением В, пункт В.2.5;

- интервал времени между тестовыми испытаниями должен быть, по крайней мере, на порядок больше, чем продолжительность диагностического тестирования;

- для каждой подсистемы существует единый интервал времени между тестовыми испытаниями и среднее время восстановления.

Примечание — Среднее время восстановления включает в себя время, необходимое для обнаружения отказа в соответствии с МЭК 61508-2, подпункт 7.4.3.2.2, перечисление g), примечание. В настоящем приложении предполагаемое значение среднего времени восстановления одинаковое как для обнаруженных, так и необнаруженных отказов и включает в себя длительность диагностического тестирования, а не интервал между тестовыми испытаниями. Для необнаруженных отказов среднее время восстановления, используемое в расчетах, не должно включать в себя длительность диагностического тестирования, а так как среднее время восстановления всегда добавляется к временному интервалу между тестовыми испытаниями, который, по крайней мере, на порядок больше длительности диагностического тестирования, то ошибка будет незначительной;

- восстановить работоспособное состояние системы, нарушенное после возникновения всех известных отказов, могут несколько ремонтных команд;

- ожидаемый интервал между запросами на выполнение функции безопасности должен быть, по крайней мере, на порядок больше среднего времени восстановления;

- для всех подсистем, работающих в режиме низкой интенсивности запросов, и для архитектур 1oo2, 1oo2D и 2oo3, работающих в режиме высокой интенсивности запросов и непрерывном режиме, доля отказов, заданная диагностическим охватом, обнаруживается и устраняется за среднее время восстановления, приведенное в требованиях к полноте безопасности аппаратных средств.

Пример — Если предполагаемое среднее время восстановления равно 8 ч, то оно включает в себя длительность диагностического тестирования, которое обычно не превышает 1 ч, а оставшаяся часть среднего времени восстановления — это действительное время ремонта.

Примечание — Для канальных архитектур 1oo2, 1oo2D и 2oo3 предполагается выполнение любого ремонта в оперативном режиме. Если конфигурация E/E/PE системы, связанной с безопасностью, при любом обнаруживаемом отказе обеспечивает переход EUC в безопасное состояние, то это уменьшает среднюю вероятность отказа в обслуживании. Степень уменьшения вероятности зависит от диагностического покрытия;

- для канальных архитектур 1oo1 и 2oo2, работающих в режиме высокой интенсивности запросов или непрерывном режиме, система E/E/PE, связанная с безопасностью, всегда переходит в безопасное состояние после обнаружения опасного отказа; для этого ожидаемый интервал времени между запросами, по крайней мере, должен быть на порядок больше временного интервала диагностического тестирования или сумма временных интервалов диагностического тестирования и временных интервалов перехода в безопасное состояние должна быть меньше, чем время безопасной работы.

Примечание — Время безопасной работы определяется в МЭК 61508-2, подпункт 7.4.3.2.5 как интервал времени между отказом EUC или системы управления EUC (с потенциальной возможностью вызвать опасное событие) и возникновением опасного события, если функция безопасности не выполнена;

- если отказ источника питания приводит к обесточиванию E/E/PE системы, связанной с безопасностью, и инициирует переход системы в безопасное состояние, то источник питания не влияет на среднюю вероятность отказа по запросу для E/E/PE системы, связанной с безопасностью; если для перехода в безопасное состояние на систему подается питание или у источника питания существуют режимы отказов, которые могут приводить к небезопасной работе E/E/PE системы, связанной с безопасностью, то оценка должна учитывать источник питания;

- если используется терминальный канал, то он ограничивается только той частью рассматриваемой системы, которой обычно являются либо датчик, либо логическая подсистема, либо подсистема оконечных элементов;

- параметры и их обозначения представлены в таблице В.1.

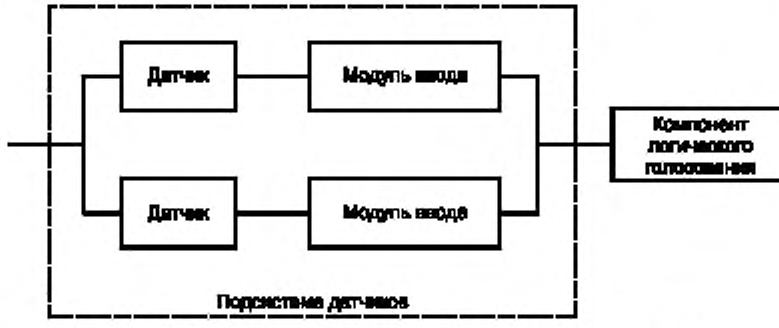


Рисунок В.1 — Пример конфигурации для двух каналов датчиков

Таблица В.1 — Параметры, используемые в настоящем приложении, и диапазоны их значений (применяется к архитектурам 1oo1, 1oo2, 2oo2, 1oo2D и 2oo3)

Обозначение	Параметр, единица измерения	Диапазон параметров в соответствии с таблицами В.2 — В.5 и В.10 — В.13
T_1	Интервал времени между процедурами тестирования, ч	Один месяц (730 ч)[1]. Три месяца (2190 ч)[1]. Шесть месяцев (4380 ч). Один год (8760 ч). Два года (17520 ч)[2]. 10 лет (87600 ч)[2]
MTTR	Среднее время восстановления, ч	8
DC	Диагностическое покрытие, дробь (в формулах), % (в остальных случаях)	0 %; 60 %; 90 %; 99 %
β	Доля необнаруженных отказов по общей причине (в таблицах В.2 — В.5 и В.10 — В.13 предполагается $\beta = 2 \times \beta_D$), дробь (в формулах), % (в остальных случаях)	2 %; 10 %; 20 %
β_D	Доля отказов, обнаруженных диагностическими тестами и имеющих общую причину (в таблицах В.2 — В.5 и В.10 — В.13 предполагается $\beta = 2 \times \beta_D$), дробь (в формулах), % (в остальных случаях)	1 %; 5 %; 10 %
λ	Интенсивность отказов для канала подсистемы, отказ/ч	$0{,}1\times10^{-6}$; $0{,}5\times10^{-6}$; 1×10^{-6}; 5×10^{-6}; 10×10^{-6}; 50×10^{-6}
PFD_G	Средняя вероятность отказа по запросу для группы голосующих каналов (если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно)	—
PFD_S	Средняя вероятность отказа по запросу для подсистемы датчиков	—
PFD_L	Средняя вероятность отказа по запросу для логической подсистемы	—
PFD_{FE}	Средняя вероятность отказа по запросу для подсистемы оконечных элементов	—
PFD_{SYS}	Средняя вероятность отказа по запросу для функции безопасности E/E/PE системы, связанной с безопасностью	—
PFH_G	Вероятность отказа для группы голосующих каналов (если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно), отказ/ч	—
PFH_S	Вероятность отказа для подсистемы датчиков, отказ/ч	—
PFH_L	Вероятность отказа для логической подсистемы, отказ/ч	—
PFH_{FE}	Вероятность отказа для подсистемы оконечных элементов, отказ/ч	—
PFH_{SYS}	Вероятность отказа для функции безопасности E/E/PE системы, связанной с безопасностью, отказ/ч	—
λ_D	Интенсивность опасных отказов для канала подсистемы, равная $0{,}5 \times \lambda$ (в предположении 50 % опасных отказов и 50 % безопасных отказов), отказ/ч	—
λ_{DD}	Интенсивность обнаруженных опасных отказов для канала подсистемы (это сумма всех интенсивностей обнаруженных опасных отказов для канала подсистемы), отказ/ч	—
λ_{DU}	Интенсивность необнаруженных опасных отказов для канала подсистемы (это сумма всех интенсивностей необнаруженных опасных отказов для канала подсистемы), отказ/ч	—

Окончание таблицы В.1

Обозначение	Параметр, единица измерения	Диапазон параметров в соответствии с таблицами В.2 — В.5 и В.10 — В.13
λ_{SD}	Интенсивность обнаруженных безопасных отказов для канала подсистемы (это сумма всех интенсивностей обнаруженных безопасных отказов для канала подсистемы), отказ/ч	—
t_{CE}	Эквивалентное среднее время простоя канала для архитектур 1oo1, 1oo2, 2oo2 и 2oo3 (это объединенное время простоя для всех компонентов канала подсистемы), ч	—
t_{GE}	Эквивалентное среднее время простоя голосующей группы для архитектур 1oo1, 1oo2, 2oo2 и 2oo3 (это объединенное время простоя для всех каналов в голосующей группе), ч	—
t_{CE}'	Эквивалентное среднее время простоя канала для архитектуры 1oo2D (это объединенное время простоя для всех компонентов канала подсистемы), ч	—
t_{GE}'	Эквивалентное среднее время простоя голосующей группы для архитектуры 1oo2D (это суммарное время простоя для всех каналов в голосующей группе), ч	—
T_2	Интервал времени между запросами, ч	—
[1] Только режим высокой интенсивности запросов и непрерывный режим. [2] Только режим низкой интенсивности запросов.		

В.2 Средняя вероятность отказа по запросу (для режима низкой интенсивности запросов)

В.2.1 Процедура расчета

Среднюю вероятность отказа в обслуживании функции безопасности для E/E/PE системы, связанной с безопасностью, определяют вычислением и суммированием средней вероятности отказа в обслуживании для всех подсистем, совокупность которых обеспечивает функцию безопасности. Так как рассматриваемые в настоящем приложении вероятности невелики, то средняя вероятность отказа по запросу для функции безопасности E/E/PE системы (см. рисунок В.2), связанной с безопасностью, PFD_{SYS} может быть вычислена по формуле

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE},$$

где PFD_S — средняя вероятность отказа по запросу для подсистемы датчиков;
PFD_L — средняя вероятность отказа по запросу для логической подсистемы;
PFD_{FE} — средняя вероятность отказа по запросу для подсистемы оконечных элементов.



Рисунок В.2 — Структура подсистем E/E/PE системы, связанной с безопасностью

Для определения средней вероятности отказа по запросу для каждой из подсистем необходимо строго придерживаться следующей процедуры для каждой подсистемы:

a) Рисуют структурную схему, изображающую компоненты подсистемы датчиков (подсистемы ввода), компоненты логической подсистемы или компоненты подсистемы оконечных элементов (подсистемы вывода). Компонентами подсистемы датчиков, например, могут быть датчики, защитные экраны, входные согласующие цепи; компонентами логической подсистемы — процессоры и сканеры; а компонентами подсистемы оконечных элементов — выходные согласующие цепи, экраны и исполнительные механизмы. Представляют каждую подсистему как одну либо более голосующих групп 1oo1, 1oo2, 2oo2, 1oo2D или 2oo3.

b) Применяют соответствующие таблицы В.2 — В.5, в которых приведены шестимесячные, годовые, двухлетние и 10-летние интервалы между процедурами тестирования. Данные таблицы предполагают, что среднее время восстановления для любого отказа после его обнаружения равно 8 ч.

c) Для каждой голосующей группы в подсистеме выбирают из таблиц В.2 — В.5:

- архитектуру (например 2oo3);

- диагностический охват для каждого канала (например 60 %);
- интенсивность отказов (в час) λ для каждого канала (например 5.0E-06);
- β-факторы отказа с общей причиной β и β_D для взаимосвязи между каналами в рассматриваемой архитектуре (например 2 % и 1 % соответственно).

Примечания

1 Предполагается, что все каналы в голосующей группе имеют одинаковые диагностические покрытия и интенсивности отказов (см. подраздел В.1).

2 В таблицах В.2 — В.5 (см. также таблицы В.10 — В.13) предполагается, что β-фактор в отсутствие диагностических тестов (также применяемый для необнаруженных опасных отказов при использовании диагностических тестов) β в 2 раза больше β-фактора для отказов, обнаруживаемых диагностическими тестами, β_D.

d) Получают из таблиц В.2 — В.5 среднюю вероятность отказа в обслуживании для голосующей группы.

e) Если функция безопасности зависит от нескольких голосующих групп датчиков или исполнительных механизмов, то совокупную среднюю вероятность отказа в обслуживании для подсистемы датчиков или подсистемы оконечных элементов PFD_S или PFD_{FE} задают следующими формулами:

$$PFD_S = \sum_i PFD_{Gi};$$

$$PFD_{FE} = \sum_i PFD_{Gi}.$$

где PFD_{Gi} и PFD_{Gj} — средние вероятности отказа в обслуживании для каждого из голосующей группы датчика или оконечного элемента, соответственно.

B.2.2 Архитектуры для режима низкой интенсивности запросов

Примечания

1 В настоящем пункте справедливые для нескольких архитектур формулы выводят там, где они встречаются впервые.

2 Формулы настоящего пункта справедливы для предположений, перечисленных в В.1.

B.2.2.1 Архитектура 1oo1

Данная архитектура предполагает использование одного канала, и любой опасный отказ приводит к нарушению функции безопасности при возникновении запроса на ее выполнение.

На рисунках В.3 и В.4 представлены структурная схема и схема расчета надежности. Интенсивность для канала λ_D задается формулой

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}.$$

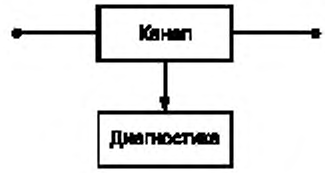


Рисунок В.3 — Структурная схема архитектуры 1oo1

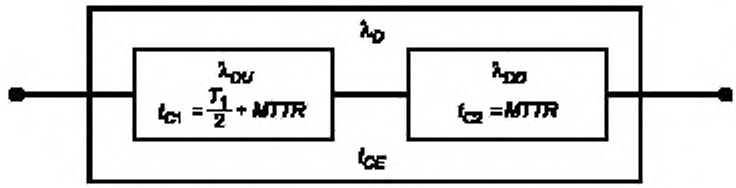


Рисунок В.4 — Схема расчета надежности архитектуры 1oo1

На рисунке В.4 показано, что канал можно рассматривать как состоящий из двух компонентов, одного с интенсивностью опасных отказов λ_{DU}, обусловленной необнаруженными отказами, а другого с интенсивностью опасных отказов λ_{DD}, обусловленной обнаруженными отказами. Эквивалентное среднее время простоя канала t_{CE} можно рассчитать, суммируя времена простоя для двух компонентов, t_{C1} и t_{C2}, прямо пропорционально вкладу каждого компонента в вероятность отказа канала:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right)\frac{\lambda_{DD}}{\lambda_D} MTTR .$$

Для каждой архитектуры интенсивность необнаруженных опасных отказов λ_{DU} и интенсивность необнаруженных опасных отказов λ_{DD} задаются как

$$\lambda_{DU} = \frac{\lambda}{2}(1-DC);\ \lambda_{DD} = \frac{\lambda}{2} DC .$$

Среднюю вероятность отказа выполнения функции безопасности канала *PFD* в течение времени простоя t_{CE} определяют из выражения

$$PFD = 1-e^{-\lambda_D t_{CE}} = \lambda_D t_{CE} ,$$

так как $\lambda_D t_{CE} << 1$.

Следовательно, средняя вероятность отказа по запросу для архитектуры 1oo1 PFD_G равна

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE} .$$

B.2.2.2 Архитектура 1oo2

Данная архитектура представляет собой два канала, соединенных параллельно, так что любой из каналов может выполнить функцию безопасности. Следовательно, для нарушения функции безопасности опасные отказы должны возникнуть в обоих каналах. Предполагается, что любое диагностическое тестирование только сообщает о найденных сбоях и не может изменить ни выходные состояния каналов, ни результат голосования.

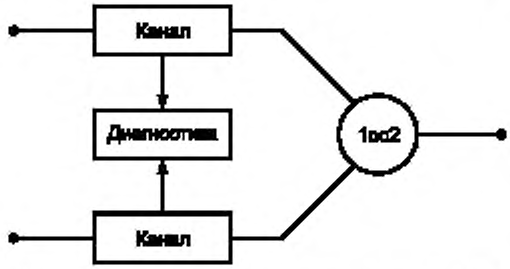


Рисунок B.5 — Структурная схема архитектуры 1oo2

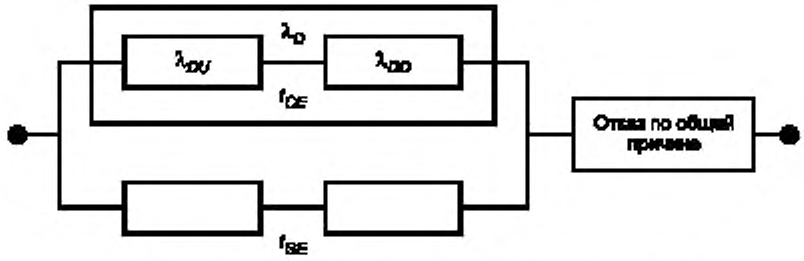


Рисунок B.6 — Схема расчета надежности архитектуры 1oo2

Структурная схема и схема расчета надежности архитектуры 1oo2 приведены на рисунках B.5 и B.6. Значение t_{CE} вычисляют в соответствии с B.2.2.1, но необходимо вычислить также и эквивалентное время простоя системы t_{GE} по формуле

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right)\frac{\lambda_{DD}}{\lambda_D} MTTR .$$

Для данной архитектуры 1oo1 средняя вероятность отказа по запросу PFD_G равна

$$PFD_G = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right).$$

B.2.2.3 Архитектура 2oo2

Данная архитектура представляет собой два канала, соединенных параллельно, и для выполнения функции безопасности необходима работа обоих каналов. Предполагается, что любое диагностическое тестирование только сообщает о найденных сбоях и не может изменить ни выходные состояния каналов, ни результат голосования.

Структурная схема и схема расчета надежности архитектуры 2oo2 представлены на рисунках B.7 и B.8.

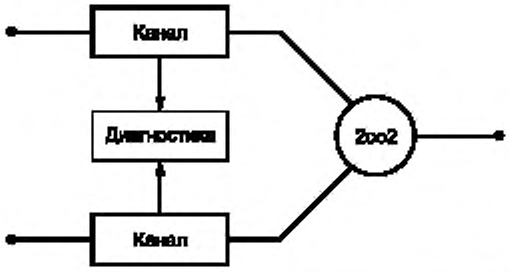


Рисунок B.7 — Структурная схема архитектуры 2oo2

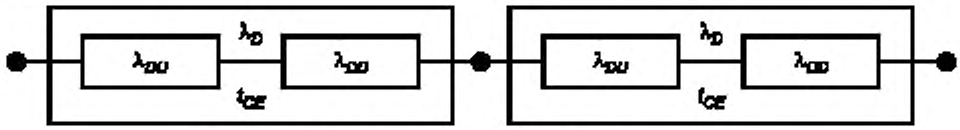


Рисунок B.8 — Схема расчета надежности архитектуры 2oo2

Значение t_{CE} вычисляют в соответствии с B.2.2.1, а средняя вероятность отказа по запросу PFD_G для данной архитектуры должна быть равна

$$PFD_G = 2\lambda_D t_{CE}.$$

B.2.2.4 Архитектура 1oo2D

Данная архитектура представляет собой два канала, соединенных параллельно. При нормальной работе для выполнения функции безопасности необходимы оба канала. Кроме того, если диагностическое тестирование обнаруживает отказ в любом канале, то результаты анализа устанавливаются так, чтобы общее выходное состояние совпадало с результатом, выдаваемым другим каналом. Если диагностическое тестирование обнаруживает отказы в обоих каналах или несоответствие между ними, причина которого не может быть идентифицирована, то выходной сигнал переводит систему в безопасное состояние. Для обнаружения несоответствия между каналами каждый канал может определять состояние другого канала независящим от другого канала способом.

Структурная схема и схема расчета надежности архитектуры 1oo2D представлены на рисунках B.9 и B.10.

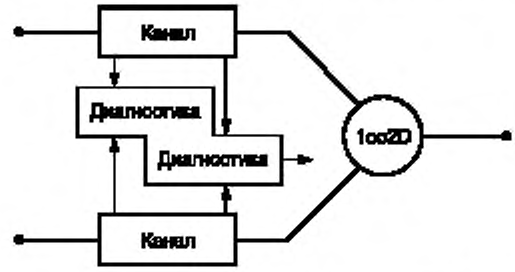


Рисунок B.9 — Структурная схема архитектуры 1oo2D

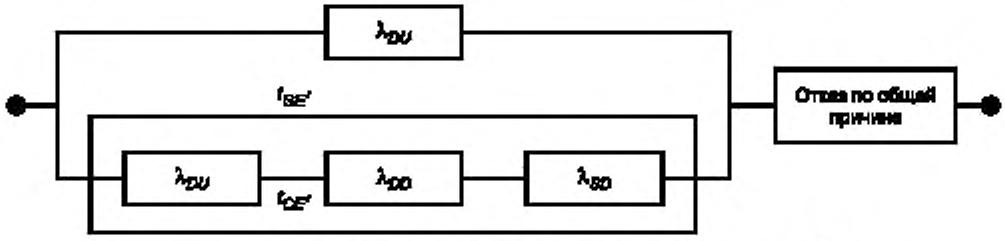


Рисунок B.10 — Схема расчета надежности архитектуры 1oo2D

Для каждого канала интенсивность обнаруженных безопасных отказов λ_{SD} определяют как

$$\lambda_{SD} = \frac{\lambda}{2} DC.$$

Значения эквивалентного среднего времени простоя отличаются от значений, приведенных для других архитектур в В.2.2, и поэтому их обозначают как $t_{CE'}$ и $t_{GE'}$. Эти значения определяют как

$$t_{CE'} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}};$$

$$t_{GE'} = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}.$$

Средняя вероятность отказа по запросу PFD_G для данной архитектуры равна

$$PFD_G = 2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\right) t_{CE'} t_{GE'} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right).$$

B.2.2.5 Архитектура 2oo3

Данная архитектура состоит из трех каналов, соединенных параллельно с мажорированием выходных сигналов так, что выходное состояние не меняется, если результат, выдаваемый одним из каналов, отличается от результата, выдаваемого двумя другими каналами.

Предполагается, что любое диагностическое тестирование только фиксирует найденные сбои и не может изменить ни выходные состояния каналов, ни результат голосования.

Структурная схема и схема расчета надежности архитектуры 2oo3 представлены на рисунках В.11 и В.12.

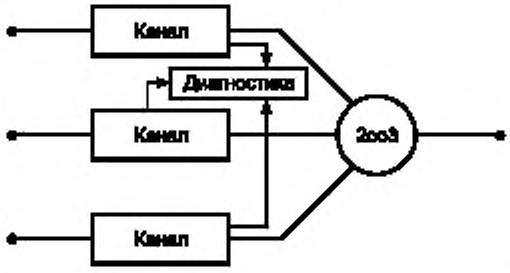


Рисунок В.11 — Структурная схема архитектуры 2oo3

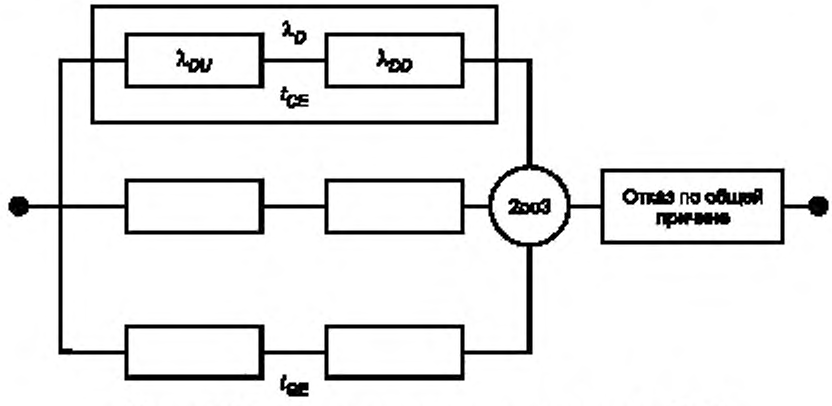


Рисунок В.12 — Схема расчета надежности архитектуры 2oo3

Значение t_{CE} вычисляют по В.2.2.1, а значение t_{GE} — по В.2.2.2. Средняя вероятность отказа по запросу PFD_G для данной архитектуры равна

$$PFD_G = 6\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right).$$

B.2.3 Подробные таблицы для режима низкой интенсивности запросов

Таблица B.2 — Средняя вероятность отказа по запросу в течение шестимесячного интервала между контрольными проверками при среднем времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	1.1 E-04			5.5E-04			1.1E-03		
	60 %	4.4E-05			2.2E-04			4.4E-04		
	90 %	1.1 E-05			5.7E-05			1.1E-04		
	99 %	1.5E-06			7.5E-06			1.5E-05		
1oo2	0 %	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60 %	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	90 %	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99 %	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo2 (см. примечание 2)	0 %	2.2E-04			1.1E-03			2.2E-03		
	60 %	8.8E-05			4.4E-04			8.8E-04		
	90 %	2.3E-05			1.1 E-04			2.3E-04		
	99 %	3.0E-06			1.5E-05			3.0E-05		
1oo2D	0 %	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60 %	8.8E-07	4.4E-06	8.8E-06	4.4E-06	2.2E-05	4.4E-05	8.9E-06	4.4E-05	8.8E-05
	90 %	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.2E-06	1.1E-05	2.2E-05
	99 %	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo3	0 %	2.2E-06	1.1E-05	2.2E-05	1.2E-05	5.6E-05	1.1E-04	2.7E-05	1.1E-04	2.2E-04
	60 %	8.9E-07	4.4E-06	8.8E-06	4.6E-06	2.2E-05	4.4E-05	9.6E-06	4.5E-05	8.9E-05
	90 %	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99 %	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06

Продолжение таблицы B.2

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	5.5E-03			1.1E-02			5.5E-02		
	60 %	2.2E-03			4.4E-03			2.2E-02		
	90 %	5.7E-04			1.1E-03			5.7E-03		
	99 %	7.5E-05			1.5E-04			7.5E-04		
1oo2	0 %	1.5E-04	5.8E-04	1.1E-03	3.7E-04	1.2E-03	2.3E-03	5.0E-03	8.8E-03	1.4E-02
	60 %	5.0E-05	2.3E-04	4.5E-04	1.1E-04	4.6E-04	9.0E-04	1.1E-03	2.8E-03	4.9E-03
	90 %	1.2E-05	5.6E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04	1.5E-04	6.0E-04	1.2E-03
	99 %	1.3E-06	6.5E-06	1.3E-05	2.6E-06	1.3E-05	2.6E-05	1.4E-05	6.6E-05	1.3E-04
2oo2 (см. примечание 2)	0 %	1.1E-02			2.2E-02			>1E-01		
	60 %	4.4E-03			8.8E-03			4.4E-02		
	90 %	1.1E-03			2.3E-03			1.1E-02		
	99 %	1.5E-04			3.0E-04			1.5E-03		

Окончание таблицы В.2

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo2D	0 %	1.5E-04	5.8E-04	1.1E-03	3.7E-04	1.2E-03	2.3E-03	5.0E-03	8.8E-03	1.4E-02
	60 %	4.6E-05	2.2E-04	4.4E-04	9.5E-05	4.5E-04	8.9E-04	6.0E-04	2.3E-03	4.5E-03
	90 %	1.1E-05	5.6E-05	1.1E-04	2.2E-05	1.1E-04	2.2E-04	1.1E-04	5.6E-04	1.1E-03
	99 %	1.3E-06	6.5E-06	1.3E-05	2.6E-06	1.3E-05	2.6E-05	1.3E-05	6.5E-05	1.3E-04
2oo3	0 %	2.3E-04	6.5E-04	1.2E-03	6.8E-04	1.5E-03	2.5E-03	1.3E-02	1.5E-02	1.9E-02
	60 %	6.3E-05	2.4E-04	4.6E-04	1.6E-04	5.1E-04	9.4E-04	2.3E-03	3.9E-03	5.9E-03
	90 %	1.2E-05	5.7E-05	1.1E-04	2.7E-05	1.2E-04	2.3E-04	2.4E-04	6.8E-04	1.2E-03
	99 %	1.3E-06	6.5E-06	1.3E-05	2.7E-06	1.3E-05	2.6E-05	1.5E-05	6.7E-05	1.3E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам в соответствии с В.2.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица В.3 — Средняя вероятность отказа по запросу для одногодичного интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.2E-04			1.1E-03			2.2E-03		
	60 %	8.8E-05			4.4E-04			8.8E-04		
	90 %	2.2E-05			1.1E-04			2.2E-04		
	99 %	2.6E-06			1.3E-05			2.6E-05		
1oo2	0 %	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	60 %	1.8E-06	8.8E-06	1.8E-05	9.0E-06	4.4E-05	8.8E-05	1.9E-05	8.9E-05	1.8E-04
	90 %	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.5E-06	2.2E-05	4.4E-05
	99 %	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06
2oo2 (см. примечание 2)	0 %	4.4E-04			2.2E-03			4.4E-03		
	60 %	1.8E-04			8.8E-04			1.8E-03		
	90 %	4.5E-05			2.2E-04			4.5E-04		
	99 %	5.2E-06			2.6E-05			5.2E-05		
1oo2D	0 %	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	60 %	1.8E-06	8.8E-06	1.8E-05	8.9E-06	4.4E-05	8.8E-05	1.8E-05	8.8E-05	1.8E-04
	90 %	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.4E-06	2.2E-05	4.4E-05
	99 %	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06
2oo3	0 %	4.6E-06	2.2E-05	4.4E-05	2.7E-05	1.1E-04	2.2E-04	6.2E-05	2.4E-04	4.5E-04
	60 %	1.8E-06	8.8E-06	1.8E-05	9.5E-06	4.5E-05	8.8E-05	2.1E-05	9.1E-05	1.8E-04
	90 %	4.4E-07	2.2E-06	4.4E-06	2.3E-06	1.1E-05	2.2E-05	4.6E-06	2.2E-05	4.4E-05
	99 %	4.8E-08	2.4E-07	4.8E-07	2.4E-07	1.2E-06	2.4E-06	4.8E-07	2.4E-06	4.8E-06

Окончание таблицы В.3

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	1.1 E-02			2.2E-02			>1E-01		
	60 %	4.4E-03			8.8E-03			4.4E-02		
	90 %	1.1 E-03			2.2E-03			1.1E-02		
	99 %	1.3E-04			2.6E-04			1.3E-03		
1oo2	0 %	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03	1.8E-02	2.4E-02	3.2E-02
	60 %	1.1E-04	4.6E-04	9.0E-04	2.8E-04	9.7E-04	1.8E-03	3.4E-03	6.6E-03	1.1E-02
	90 %	2.4E-05	1.1E-04	2.2E-04	5.1E-05	2.3E-04	4.5E-04	3.8E-04	1.3E-03	2.3E-03
	99 %	2.4E-06	1.2E-05	2.4E-05	4.9E-06	2.4E-05	4.8E-05	2.6E-05	1.2E-04	2.4E-04
2oo2 (см. примечание 2)	0 %	2.2E-02			4.4E-02			>1E-01		
	60 %	8.8E-03			1.8E-02			8.8E-02		
	90 %	2.2E-03			4.5E-03			2.2E-02		
	99 %	2.6E-04			5.2E-04			2.6E-03		
1oo2D	0 %	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03	1.8E-02	2.4E-02	3.2E-02
	60 %	9.4E-05	4.5E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03	1.5E-03	5.0E-03	9.3E-03
	90 %	2.2E-05	1.1E-04	2.2E-04	4.5E-05	2.2E-04	4.4E-04	2.3E-04	1.1E-03	2.2E-03
	99 %	2.4E-06	1.2E-05	2.4E-05	4.8E-06	2.4E-05	4.8E-05	2.4E-05	1.2E-04	2.4E-04
2oo3	0 %	6.8E-04	1.5E-03	2.5E-03	2.3E-03	3.8E-03	5.6E-03	4.8E-02	5.0E-02	5.3E-02
	60 %	1.6E-04	5.1E-04	9.4E-04	4.8E-04	1.1E-03	2.0E-03	8.4E-03	1.1E-02	1.5E-02
	90 %	2.7E-05	1.2E-04	2.3E-04	6.4E-05	2.4E-04	4.6E-04	7.1E-04	1.6E-03	2.6E-03
	99 %	2.5E-06	1.2E-05	2.4E-05	5.1E-06	2.4E-05	4.8E-05	3.1E-05	1.3E-04	2.5E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам в соответствии с В.2.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица В.4 — Средняя вероятность отказа по запросу для двухлетнего интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	4.4E-04			2.2E-03			4.4E-03		
	60 %	1.8E-04			8.8E-04			1.8E-03		
	90 %	4.4E-05			2.2E-04			4.4E-04		
	99 %	4.8E-06			2.4E-05			4.8E-05		
1oo2	0 %	9.0E-06	4.4E-05	8.8E-05	5.0E-05	2.2E-04	4.4E-04	1.1E-04	4.6E-04	8.9E-04
	60 %	3.5E-06	1.8E-05	3.5E-05	1.9E-05	8.9E-05	1.8E-04	3.9E-05	1.8E-04	3.5E-04
	90 %	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	99 %	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.2E-07	4.6E-06	9.2E-06

Продолжение таблицы В. 4

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0 %	8.8E-04			4.4E-03			8.8E-03		
	60 %	3.5E-04			1.8E-03			3.5E-03		
	90 %	8.8E-05			4.4E-04			8.8E-04		
	99 %	9.6E-06			4.8E-05			9.6E-05		
1oo2D	0 %	9.0E-06	4.4E-05	8.8E-05	5.0E-05	2.2E-04	4.4E-04	1.1E-04	4.6E-04	8.9E-04
	60 %	3.5E-06	1.8E-05	3.5E-05	1.8E-05	8.8E-05	1.8E-04	3.6E-05	1.8E-04	3.5E-04
	90 %	8.8E-07	4.4E-06	8.8E-06	4.4E-06	2.2E-05	4.4E-05	8.8E-06	4.4E-05	8.8E-05
	99 %	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.2E-07	4.6E-06	9.2E-06
2oo3	0 %	9.5E-06	4.4E-05	8.8E-05	6.2E-05	2.3E-04	4.5E-04	1.6E-04	5.0E-04	9.3E-04
	60 %	3.6E-06	1.8E-05	3.5E-05	2.1E-05	9.0E-05	1.8E-04	4.7E-05	1.9E-04	3.6E-04
	90 %	8.9E-07	4.4E-06	8.8E-06	4.6E-06	2.2E-05	4.4E-05	9.6E-06	4.5E-05	8.9E-05
	99 %	9.2E-08	4.6E-07	9.2E-07	4.6E-07	2.3E-06	4.6E-06	9.3E-07	4.6E-06	9.2E-06

Окончание таблицы В.4

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.2E-02			4.4E-02			>1E-01		
	60 %	8.8E-03			1.8E-02			8.8E-02		
	90 %	2.2E-03			4.4E-03			2.2E-02		
	99 %	2.4E-04			4.8E-04			2.4E-03		
1oo2	0 %	1.1E-03	2.7E-03	4.8E-03	3.3E-03	6.5E-03	1.0E-02	6.6E-02	7.4E-02	8.5E-02
	60 %	2.8E-04	9.7E-04	1.8E-03	7.5E-04	2.1E-03	3.8E-03	1.2E-02	1.8E-02	2.5E-02
	90 %	5.0E-05	2.3E-04	4.5E-04	1.1E-04	4.6E-04	9.0E-04	1.1E-03	2.8E-03	4.9E-03
	99 %	4.7E-06	2.3E-05	4.6E-05	9.5E-06	4.6E-05	9.2E-05	5.4E-05	2.4E-04	4.6E-04
2oo2 (см. примечание 2)	0 %	4.4E-02			8.8E-02			>1E-01		
	60 %	1.8E-02			3.5E-02			>1E-01		
	90 %	4.4E-03			8.8E-03			4.4E-02		
	99 %	4.8E-04			9.6E-04			4.8E-03		
1oo2D	0 %	1.1E-03	2.7E-03	4.8E-03	3.3E-03	6.5E-03	1.0E-02	6.6E-02	7.4E-02	8.5E-02
	60 %	2.0E-04	9.0E-04	1.8E-03	4.5E-04	1.8E-03	3.6E-03	4.3E-03	1.1E-02	1.9E-02
	90 %	4.4E-05	2.2E-04	4.4E-04	8.9E-05	4.4E-04	8.8E-04	4.7E-04	2.2E-03	4.4E-03
	99 %	4.6E-06	2.3E-05	4.6E-05	9.2E-06	4.6E-05	9.2E-05	4.6E-05	2.3E-04	4.6E-04
2oo3	0 %	2.3E-03	3.7E-03	5.6E-03	8.3E-03	1.1E-02	1.4E-02	>1E-01	>1E-01	>1E-01
	60 %	4.8E-04	1.1E-03	2.0E-03	1.6E-03	2.8E-03	4.4E-03	3.2E-02	3.5E-02	4.0E-02
	90 %	6.3E-05	2.4E-04	4.6E-04	1.6E-04	5.1E-04	9.4E-04	2.4E-03	4.0E-03	6.0E-03
	99 %	4.8E-06	2.3E-05	4.6E-05	1.0E-05	4.7E-05	9.2E-05	6.9E-05	2.5E-04	4.8E-04

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам в соответствии с В.2.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица B.5 — Средняя вероятность отказа по запросу для десятилетнего интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.2E-03			1.1E-02			2.2E-02		
	60 %	8.8E-04			4.4E-03			8.8E-03		
	90 %	2.2E-04			1.1E-03			2.2E-03		
	99 %	2.2E-05			1.1E-04			2.2E-04		
1oo2	0 %	5.0E-05	2.2E-04	4.4E-04	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03
	60 %	1.9E-05	8.9E-05	1.8E-04	1.1E-04	4.6E-04	9.0E-04	2.7E-04	9.6E-04	1.8E-03
	90 %	4.4E-06	2.2E-05	4.4E-05	2.3E-05	1.1E-04	2.2E-04	5.0E-05	2.2E-04	4.4E-04
	99 %	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.5E-06	2.2E-05	4.4E-05
2oo2 (см. примечание 2)	0 %	4.4E-03			2.2E-02			4.4E-02		
	60 %	1.8E-03			8.8E-03			1.8E-02		
	90 %	4.4E-04			2.2E-03			4.4E-03		
	99 %	4.5E-05			2.2E-04			4.5E-04		
1oo2D	0 %	5.0E-05	2.2E-04	4.4E-04	3.7E-04	1.2E-03	2.3E-03	1.1E-03	2.7E-03	4.8E-03
	60 %	1.8E-05	8.8E-05	1.8E-04	9.4E-05	4.4E-04	8.8E-04	2.0E-04	9.0E-04	1.8E-03
	90 %	4.4E-06	2.2E-05	4.4E-05	2.2E-05	1.1E-04	2.2E-04	4.4E-05	2.2E-04	4.4E-04
	99 %	4.4E-07	2.2E-06	4.4E-06	2.2E-06	1.1E-05	2.2E-05	4.4E-06	2.2E-05	4.4E-05
2oo3	0 %	6.2E-05	2.3E-04	4.5E-04	6.8E-04	1.5E-03	2.5E-03	2.3E-03	3.7E-03	5.6E-03
	60 %	2.1E-05	9.0E-05	1.8E-04	1.6E-04	5.0E-04	9.3E-04	4.7E-04	1.1E-03	2.0E-03
	90 %	4.6E-06	2.2E-05	4.4E-05	2.7E-05	1.1E-04	2.2E-04	6.3E-05	2.4E-04	4.5E-04
	99 %	4.4E-07	2.2E-06	4.4E-06	2.3E-06	1.1E-05	2.2E-05	4.6E-06	2.2E-05	4.4E-05

Продолжение таблицы B.5

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	4.4E-02			8.8E-02			>1E-01		
	90 %	1.1E-02			2.2E-02			>1E-01		
	99 %	1.1E-03			2.2E-03			1.1E-02		
1oo2	0 %	1.8E-02	2.4E-02	3.2E-02	6.6E-02	7.4E-02	8.5E-02	>1E-01	>1E-01	>1E-01
	60 %	3.4E-03	6.6E-03	1.1E-02	1.2E-02	1.8E-02	2.5E-02	>1E-01	>1E-01	>1E-01
	90 %	3.8E-04	1.2E-03	2.3E-03	1.1E-03	2.8E-03	4.9E-03	1.8E-02	2.5E-02	3.5E-02
	99 %	2.4E-05	1.1E-04	2.2E-04	5.1E-05	2.3E-04	4.5E-04	3.8E-04	1.3E-03	2.3E-03
2oo2 (см. примечание 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	8.8E-02			>1E-01			>1E-01		
	90 %	2.2E-02			4.4E-02			>1E-01		
	99 %	2.2E-03			4.5E-03			2.2E-02		

Окончание таблицы В.5

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	1.8E-02	2.4E-02	3.2E-02	6.6E-02	7.4E-02	8.5E-02	>1E-01	>1E-01	>1E-01
	60 %	1.5E-03	4.9E-03	9.2E-03	4.2E-03	1.1E-02	1.9E-02	7.1E-02	9.9E-02	>1E-01
	90 %	2.3E-04	1.1E-03	2.2E-03	4.7E-04	2.2E-03	4.4E-03	3.0E-03	1.2E-02	2.3E-02
	99 %	2.2E-05	1.1E-04	2.2E-04	4.4E-05	2.2E-04	4.4E-04	2.2E-04	1.1E-03	2.2E-03
2oo3	0 %	4.8E-02	5.0E-02	5.3E-02	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01	>1E-01
	60 %	8.3E-03	1.1E-02	1.4E-02	3.2E-02	3.5E-02	4.0E-02	>1E-01	>1E-01	>1E-01
	90 %	6.9E-04	1.5E-03	2.6E-03	2.3E-03	3.9E-03	5.9E-03	4.9E-02	5.4E-02	6.0E-02
	99 %	2.7E-05	1.2E-04	2.3E-04	6.4E-05	2.4E-04	4.6E-04	7.1E-04	1.6E-03	2.6E-03

Примечания

1 В настоящей таблице приведены примеры значений PFD_G, рассчитанные по формулам в соответствии с В.2.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFD_G эквивалентна PFD_S, PFD_L или PFD_{FE} соответственно (см. В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

В.2.4. Пример режима низкой интенсивности запросов

Рассмотрим функцию безопасности, для реализации которой нужна система SIL2. Пусть построенный на основе предыдущего опыта первоначальный вариант архитектуры всей системы включает одну группу из трех аналоговых датчиков давления с архитектурой 2oo3 на входе. Логическая подсистема рассматриваемой системы представляет собой PES с избыточностью с архитектурой 1oo2D и управляет одним закрывающим и одним дренажным клапаном, так как для обеспечения функции безопасности необходима работа как закрывающего, так и дренажного клапана. Архитектура всей системы представлена на рисунке В.13. Для этой системы оценим сначала функцию безопасности PFD_{SYS} при одногодичном периоде контрольных испытаний. Таблицы В.6 - В.8 являются фрагментами таблицы В.3 для соответствующих данных на рисунке В.13.

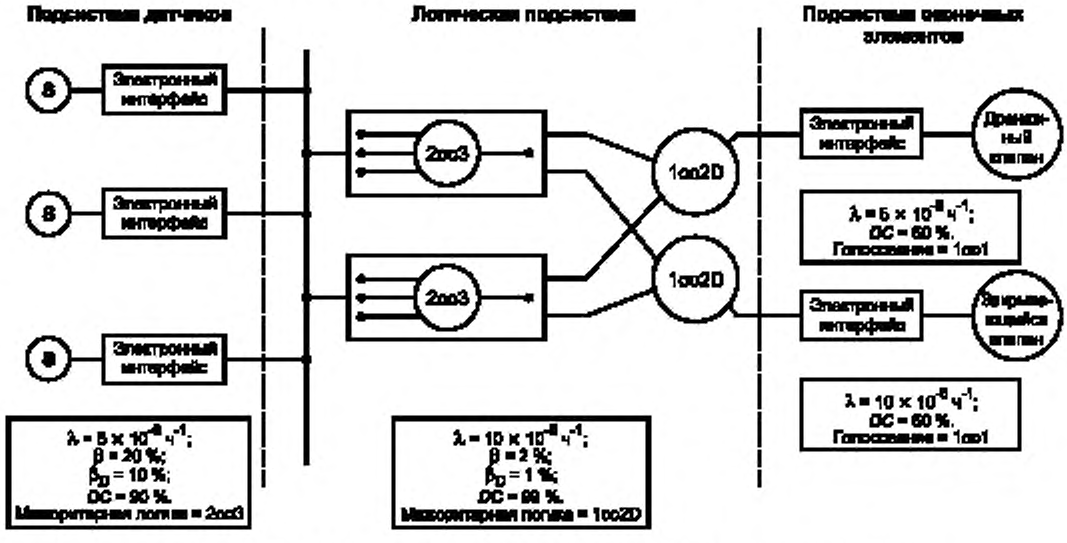


Рисунок В.13 — Архитектура системы рассматриваемого примера для режима низкой интенсивности запросов

Таблица В.6 — Средняя вероятность отказа по запросу для подсистемы датчиков в рассматриваемом примере для режима низкой интенсивности запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	DC	λ = 5.0E-06		
		β = 2 % β_D = 1 %	β =10 % β_D =5 %	β = 20 % β_D =10 %
2oo3	0 %	6.8E-04	1.5E-03	2.5E-03
	60 %	1.6E-04	5.1E-04	9.4E-04
	90 %	2.7E-05	1.2E-04	2.3E-04
	99 %	2.5E-06	1.2E-05	2.4E-05

Примечание —Настоящая таблица представляет собой фрагмент таблицы В.3.

Таблица В.7 — Средняя вероятность отказа по запросу для логической подсистемы в примере для режима низкой интенсивности запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	DC	λ = 1.0E-05		
		β = 2 % β_D = 1 %	β =10 % β_D =5 %	β = 20 % β_D =10 %
1oo2D	0 %	1.1E-03	2.7E-03	4.8E-03
	60 %	2.0E-04	9.0E-04	1.8E-03
	90 %	4.5E-05	2.2E-04	4.4E-04
	99 %	4.8E-06	2.4E-05	4.8E-05

Примечание — Настоящая таблица представляет собой фрагмент таблицы В.3.

Таблица В.8 — Средняя вероятность отказа по запросу для подсистемы оконечных элементов в примере для режима низкой интенсивности запросов (интервал контрольных испытаний равен одному году, а среднее время ремонта — 8 ч)

Архитектура	DC	λ = 5.0E-06	λ = 1.0E-05
1oo1	0 %	1.1E-02	2.2E-02
	60 %	4.4E-03	8.8E-03
	90 %	1.1E-03	2.2E-03
	99 %	1.3E-04	2.6E-04

Примечание — Настоящая таблица представляет собой фрагмент таблицы В.3.

Данные, представленные в таблицах В.6 — В.8, позволяют получить следующие значения:

- для подсистемы датчиков:

$PFD_S = 2{,}3 \times 10^{-4}$;

- для логической подсистемы:

$PFD_L = 4{,}8 \times 10^{-6}$;

- для подсистемы оконечных элементов:

$PFD_{FE} = 4{,}4 \times 10^{-3} + 8{,}8 \times 10^{-3}$

$= 1{,}3 \times 10^{-2}$.

Следовательно, для функции безопасности:

$PFD_{SYS} = 2{,}3 \times 10^{-4} + 4{,}8 \times 10^{-6} + 1{,}3 \times 10^{-2}$

$= 1{,}3 \times 10^{-2}$

= уровень полноты безопасности 1.

Для перевода системы, представленной на рисунке В.13, на уровень полноты безопасности 2, выполняют одно из следующих действий:

a) уменьшают интервал между контрольными проверками до 6 мес:

PFD_S = 1,1 × 10^{-4}

PFD_L = 2,6 × 10^{-6}

PFD_{FE} = 2,2 × 10^{-3} + 4,4 × 10^{-3}

= 6,6 × 10^{-3}

PFD_{SYS} = 6,7 × 10^{-3}

= уровень полноты безопасности 2;

b) заменяют архитектуру 1oo1 закрывающего клапана, представляющего собой выходное устройство с низкой надежностью, на 1oo2, предполагая, что β = 10 % и β_D = 5 %:

PFD_S = 2,3 × 10^{-4}

PFD_L = 4,8 × 10^{-6}

PFD_{FE} = 4,4 × 10^{-3} + 9,7 × 10^{-4}

= 5,4 × 10^{-3}

PFD_{SYS} = 5,6 × 10^{-3}

= уровень полноты безопасности 2.

B.2.5 Влияние неидеальных контрольных проверок

Отказы системы, связанной с безопасностью, не обнаруженные никакими диагностическими или контрольными испытаниями, обнаруживают только при совпадении запросов на выполнение функции безопасности, на которую влияет отказ. Следовательно, для таких полностью независимых отказов ожидаемая интенсивность запросов к системе безопасности определяет действительное время простоев.

Ниже приведен пример такой зависимости для архитектуры 1oo2, где T_2 — время между запросами к системе:

$$t_{CE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR;$$

$$t_{GE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR;$$

$$PFD_G = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta_D)\lambda_{DU}\right]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_1}{2} + MTTR\right) + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_2}{2} + MTTR\right).$$

Результаты для системы 1oo2 со 100 %-ными достоверными одногодичными контрольными испытаниями в сравнении с 50 %-ными достоверными контрольными испытаниями, где требуемый период контрольных испытаний T_2 предполагается равным 10 годам, приведены в таблице В.9. В рассматриваемом примере расчеты проводились при следующих предположениях: интенсивность отказов 1×10^{-5} в час; β = 10 %; β_D = 5 %.

Таблица В.9 — Неидеальные контрольные испытания

Архитектура	DC	λ = 1.0E-05	
		100 %-ные достоверные контрольные испытания	50 %-ные достоверные контрольные испытания (T_2 = 10 лет)
		β =10 % β_D = 5 %	β =10 % β_D = 5 %
1oo2	0 %	2.7E-03	6.6E-02
	60 %	9.7E-04	2.6E-02
	90 %	2.3E-04	6.6E-03
	99 %	2.4E-05	7.0E-04

B.3 Вероятность отказа в час (для режима работы высокой интенсивности запросов или непрерывного режима работы)

B.3.1 Процедура расчетов

Метод определения вероятности отказа функции безопасности для E/E/PE системы, связанной с безопасностью, работающей в режиме высокой интенсивности запросов или непрерывном режиме. То же, что и метод вычисления для режима низкой интенсивности запросов (см. В.2.1), за исключением того, что средняя вероятность отказа по запросу PFD_{SYS} заменяется на вероятность опасного отказа в час PFH_{SYS}.

Общую вероятность опасного отказа функции безопасности для E/E/PE системы, связанной с безопасностью, PFH_{SYS} определяют вычислением интенсивностей опасных отказов для всех подсистем, совокупность которых обеспечивает функцию безопасности, и суммированием полученных отдельных значений. Так как рассматриваемые в настоящем приложении вероятности малы, то используют формулу

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE},$$

где PFH_{SYS} — вероятность отказа в час для функции безопасности E/E/PE системы, связанной с безопасностью;

PFH_S — вероятность отказа в час для подсистемы датчиков;

PFH_L — вероятность отказа в час для логической подсистемы;

PFH_{FE} — вероятность отказа в час для подсистемы оконечных элементов.

B.3.2 Архитектуры для режима работы высокой интенсивности запросов или непрерывного режима работы

Примечания

1 В настоящем пункте справедливые для нескольких архитектур формулы выводят там, где они встречаются впервые. См. также B.2.2.

2 Формулы настоящего пункта справедливы для предположений, перечисленных в B.1.

B.3.2.1 Архитектура 1oo1

Структурная схема и схема расчета надежности архитектуры 1oo1 представлены на рисунках B.3 и B.4 соответственно. Для вычисления λ_D, t_{CE}, λ_{DU} и λ_{DD} используют те же формулы, что и в B.2.2.1.

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2};$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR;$$

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC);\ \lambda_{DD} = \frac{\lambda}{2} DC.$$

Если предположить, что система, связанная с безопасностью, при обнаружении любого отказа переводит EUC в безопасное состояние, то для архитектуры 1oo1

$$PFH_G = \lambda_{DU}.$$

B.3.2.2 Архитектура 1oo2

Структурная схема и схема расчета надежности архитектуры 1oo2 представлены соответственно на рисунках B.5 и B.6. Значение t_{CE} вычисляют по формуле, приведенной в B.3.2.1. Вероятность отказа PFH_G для архитектуры 1oo2 вычисляют по формуле

$$PFH_G = 2[(1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU}]^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU}.$$

B.3.2.3 Архитектура 2oo2

Структурная схема и схема расчета надежности архитектуры 2oo2 представлены соответственно на рисунках B.7 и B.8. Если предположить, что при обнаружении любого отказа каждый канал переводится в безопасное состояние, то для архитектуры 2oo2

$$PFH_G = 2\lambda_{DU}.$$

B.3.2.4 Архитектура 1oo2D

Структурная схема и схема расчета надежности архитектуры 1oo2D представлены соответственно на рисунках B.9 и B.10. Для архитектуры 1oo2D интенсивность обнаруженных безопасных отказов λ_{SD}, эквивалентное среднее время простоя $t_{CE'}$ и вероятность отказа PFH_G вычисляют по формулам:

$$\lambda_{SD} = \frac{\lambda}{2} DC;$$

$$t_{CE'} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}};$$

$$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE'} + \beta_D\lambda_{DD} + \beta\lambda_{DU}.$$

B.3.2.5 Архитектура 2oo3

Структурная схема и схема расчета надежности архитектуры 2oo3 представлены соответственно на рисунках B.11 и B.12. Значение t_{CE} вычисляют по формуле, приведенной в B.3.2.1. Вероятность отказа PFH_G для архитектуры 2oo3 вычисляют по формуле

$$PFH_G = 6[(1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU}]^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU}.$$

В.3.3 Подробные таблицы для режима работы высокой интенсивности запросов и непрерывного режима работы

Таблица В.10 — Вероятность отказа в час (в режиме высокой интенсивности запросов и непрерывном режиме) для одномесячного интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2 (см. примечание 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0 %	1.0E-09	5.0E-09	1.0E-08	5.0E-09	2.5E-08	5.0E-08	1.0E-08	5.0E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.0E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

Продолжение таблицы В.10

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.5E-06			5.0E-06			>1E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	3.7E-08	1.8E-07	3.5E-07	7.7E-08	3.6E-07	7.1E-07	5.4E-07	1.9E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.7E-07	1.3E-06	2.5E-06
2oo2 (см. примечание 2)	0 %	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		

Окончание таблицы В.10

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	5.4E-08	2.5E-07	5.0E-07	1.2E-07	5.2E-07	1.0E-06	9.5E-07	2.9E-06	5.3E-06
	60 %	3.6E-08	1.8E-07	3.5E-07	7.3E-08	3.5E-07	7.0E-07	4.3E-07	1.8E-06	3.6E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.5E-08	2.8E-07	5.5E-07	2.8E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.5E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	4.1E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	9.1E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.2E-08	2.8E-07	5.6E-07	4.4E-07	1.5E-06	2.9E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	3.0E-07	1.3E-06	2.6E-06

Примечания

1 В настоящей таблице приведены примеры значений PFH_G, рассчитанные по формулам в соответствии с В.3.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно (см. В.3.1 и В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица В.11 — Вероятность отказа в час (в режиме работы высокой интенсивности запросов и непрерывном режиме работы) для трехмесячного интервала между контрольными испытаниями и среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2 (см. примечание 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0 %	1.0E-09	5.0E-09	1.0E-08	5.1E-09	2.5E-08	5.0E-08	1.1E-08	5.0E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.1E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.4E-09	2.5E-08	5.0E-08	1.2E-08	5.1E-08	1.0E-07
	60 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.7E-09	3.6E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

Окончание таблицы В.11

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.5E-06			5.0E-06			>1E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	4.0E-08	1.8E-07	3.5E-07	9.2E-08	3.7E-07	7.2E-07	8.9E-07	2.2E-06	3.9E-06
	90 %	2.9E-08	1.4E-07	2.8E-07	6.1E-08	2.8E-07	5.5E-07	4.2E-07	1.5E-06	2.9E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.8E-07	1.3E-06	2.5E-06
2oo2 (см. примечание 2)	0 %	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	0 %	6.3E-08	2.6E-07	5.1E-07	1.5E-07	5.4E-07	1.0E-06	1.8E-06	3.6E-06	5.9E-06
	60 %	3.7E-08	1.8E-07	3.5E-07	7.9E-08	3.6E-07	7.1E-07	5.7E-07	1.9E-06	3.7E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	2.9E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0 %	9.0E-08	2.8E-07	5.3E-07	2.6E-07	6.3E-07	1.1E-06	4.5E-06	5.9E-06	7.6E-06
	60 %	5.1E-08	1.9E-07	3.6E-07	1.4E-07	4.1E-07	7.5E-07	2.0E-06	3.2E-06	4.7E-06
	90 %	3.2E-08	1.4E-07	2.8E-07	7.2E-08	2.9E-07	5.6E-07	7.1E-07	1.8E-06	3.1E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.6E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06

Примечания

1 В настоящей таблице приведены примеры значений PFH_G, рассчитанные по формулам в соответствии с В.3.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно (см. В.3.1 и В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица В.12 — Вероятность отказа в час (в режиме высокой интенсивности запросов и непрерывном режиме) для шестимесячного интервала между контрольными испытаниями и для среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %	β = 2 %, β_D = 1 %	β = 10 %, β_D = 5 %	β = 20 %, β_D = 10 %
1oo1 (см. примечание 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.4E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.6E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

Продолжение таблицы В. 12

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo2 (см. примечание 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0 %	1.0E-09	5.0E-09	1.0E-08	5.3E-09	2.5E-08	5.0E-08	1.1E-08	5.1E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.5E-09	1.8E-08	3.5E-08	7.2E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0 %	1.0E-09	5.0E-09	1.0E-08	5.8E-09	2.6E-08	5.1E-08	1.3E-08	5.3E-08	1.0E-07
	60 %	7.1E-10	3.5E-09	7.0E-09	3.8E-09	1.8E-08	3.5E-08	8.3E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.8E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

Окончание таблицы В.12

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.5E-06			5.0E-06			>1E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	4.6E-08	1.8E-07	3.6E-07	1.1E-07	3.9E-07	7.3E-07	1.4E-06	2.7E-06	4.3E-06
	90 %	3.0E-08	1.4E-07	2.8E-07	6.6E-08	2.9E-07	5.6E-07	5.5E-07	1.6E-06	3.0E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.2E-08	2.5E-07	5.1E-07	2.9E-07	1.3E-06	2.6E-06
2oo2 (см. примечание 2)	0 %	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		
1oo2D	0 %	7.6E-08	2.7E-07	5.2E-07	2.1E-07	5.9E-07	1.1E-06	3.1E-06	4.7E-06	6.8E-06
	60 %	3.9E-08	1.8E-07	3.5E-07	8.7E-08	3.7E-07	7.1E-07	7.8E-07	2.1E-06	3.8E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.6E-08	2.8E-07	5.5E-07	3.0E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0 %	1.3E-07	3.2E-07	5.5E-07	4.2E-07	7.7E-07	1.2E-06	8.4E-06	9.2E-06	1.0E-05
	60 %	6.7E-08	2.0E-07	3.7E-07	2.0E-07	4.6E-07	8.0E-07	3.6E-06	4.6E-06	6.0E-06
	90 %	3.6E-08	1.5E-07	2.8E-07	8.8E-08	3.1E-07	5.8E-07	1.1E-06	2.1E-06	3.4E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.5E-08	2.6E-07	5.1E-07	3.6E-07	1.4E-06	2.6E-06

Примечания

1 В настоящей таблице приведены примеры значений PFH_G, рассчитанные по формулам в соответствии с В.3.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно (см. В.3.1 и В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

Таблица B.13 — Вероятность отказа в час (в режиме высокой интенсивности запросов и непрерывном режиме) для одногодичного интервала между контрольными испытаниями и для среднего времени ремонта 8 ч

Архитектура	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	5.0E-08			2.5E-07			5.0E-07		
	60 %	2.0E-08			1.0E-07			2.0E-07		
	90 %	5.0E-09			2.5E-08			5.0E-08		
	99 %	5.0E-10			2.5E-09			5.0E-09		
1oo2	0 %	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	7.1E-10	3.5E-09	7.0E-09	3.7E-09	1.8E-08	3.5E-08	7.9E-09	3.6E-08	7.1E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.7E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo2 (см. примечание 2)	0 %	1.0E-07			5.0E-07			1.0E-06		
	60 %	4.0E-08			2.0E-07			4.0E-07		
	90 %	1.0E-08			5.0E-08			1.0E-07		
	99 %	1.0E-09			5.0E-09			1.0E-08		
1oo2D	0 %	1.0E-09	5.0E-09	1.0E-08	5.5E-09	2.5E-08	5.0E-08	1.2E-08	5.2E-08	1.0E-07
	60 %	7.0E-10	3.5E-09	7.0E-09	3.6E-09	1.8E-08	3.5E-08	7.3E-09	3.5E-08	7.0E-08
	90 %	5.5E-10	2.8E-09	5.5E-09	2.8E-09	1.4E-08	2.8E-08	5.5E-09	2.8E-08	5.5E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08
2oo3	0 %	1.1E-09	5.1E09	1.0E-08	6.6E-09	2.6E-08	5.1E-08	1.6E-08	5.5E-08	1.0E-07
	60 %	7.3E-10	3.5E-09	7.0E-09	4.1E-09	1.8E-08	3.5E-08	9.6E-09	3.7E-08	7.2E-08
	90 %	5.6E-10	2.8E-09	5.5E-09	2.9E-09	1.4E-08	2.8E-08	6.2E-09	2.8E-08	5.6E-08
	99 %	5.1E-10	2.5E-09	5.1E-09	2.5E-09	1.3E-08	2.5E-08	5.1E-09	2.5E-08	5.1E-08

Продолжение таблицы B.13

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5 0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (см. примечание 2)	0 %	2.5E-06			5.0E-06			>1E-05		
	60 %	1.0E-06			2.0E-06			1.0E-05		
	90 %	2.5E-07			5.0E-07			2.5E-06		
	99 %	2.5E-08			5.0E-08			2.5E-07		
1oo2	0 %	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	5.6E-08	1.9E-07	3.7E-07	1.6E-07	4.3E-07	7.7E-07	2.5E-06	3.7E-06	5.1E-06
	90 %	3.3E-08	1.4E-07	2.8E-07	7.7E-08	2.9E-07	5.7E-07	8.2E-07	1.9E-06	3.2E-06
	99 %	2.6E-08	1.3E-07	2.5E-07	5.3E-08	2.5E-07	5.1E-07	3.2E-07	1.3E-06	2.6E-06
2oo2 (см. примечание 2)	0 %	5.0E-06			1.0E-05			>1E-05		
	60 %	2.0E-06			4.0E-06			>1E-05		
	90 %	5.0E-07			1.0E-06			5.0E-06		
	99 %	5.0E-08			1.0E-07			5.0E-07		

Окончание таблицы В.13

Архитектура	DC	λ = 5.0E-06			λ = 1.0E-05			λ = 5.0E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	1.0E-07	2.9E-07	5.4E-07	3.1E-07	6.8E-07	1.1E-06	5.8E-06	6.9E-06	8.5E-06
	60 %	4.4E-08	1.8E-07	3.6E-07	1.0E-07	3.8E-07	7.3E-07	1.2E-06	2.5E-06	4.1E-06
	90 %	2.8E-08	1.4E-07	2.8E-07	5.7E-08	2.8E-07	5.5E-07	3.3E-07	1.4E-06	2.8E-06
	99 %	2.5E-08	1.3E-07	2.5E-07	5.1E-08	2.5E-07	5.1E-07	2.5E-07	1.3E-06	2.5E-06
2oo3	0 %	2.1E-07	3.8E-07	6.1E-07	7.3E-07	1.0E-06	1.4E-06	>1E-05	>1E-05	>1E-05
	60 %	9.9E-08	2.3E-07	4.0E-07	3.3E-07	5.8E-07	9.0E-07	6.8E-06	7.5E-06	8.4E-06
	90 %	4.4E-08	1.5E-07	2.9E-07	1.2E-07	3.3E-07	6.0E-07	1.9E-06	2.9E-06	4.1E-06
	99 %	2.7E-08	1.3E-07	2.5E-07	5.8E-08	2.6E-07	5.1E-07	4.4E-07	1.4E-06	2.7E-06

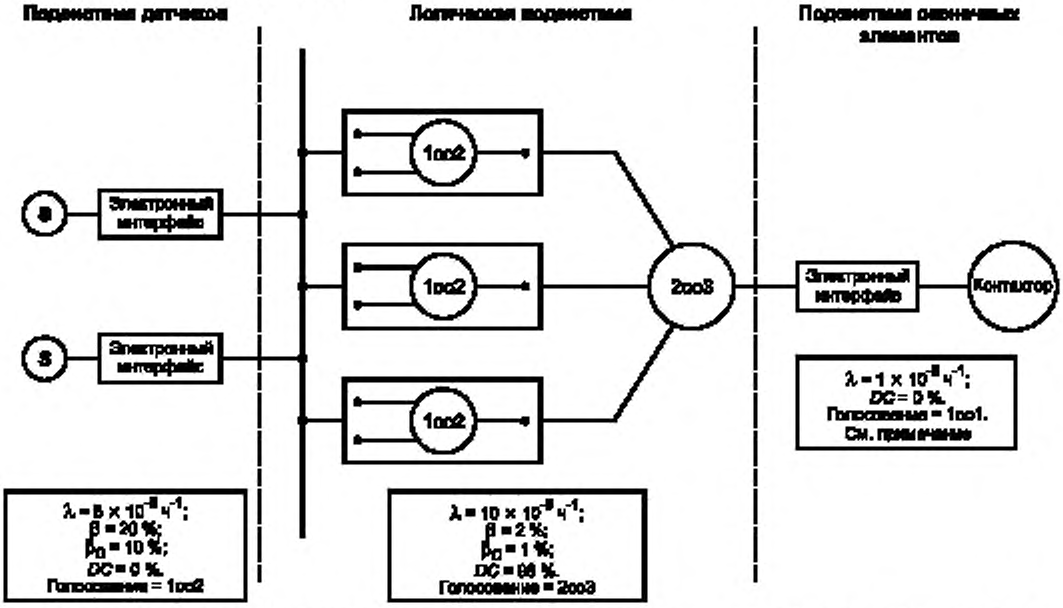
Примечания

1 В настоящей таблице приведены примеры значений PFH_G, рассчитанные по формулам в соответствии с В.3.2 и с учетом предположений, перечисленных в В.1. Если подсистема датчиков, логическая подсистема или подсистема оконечных элементов входит в состав только одной голосующей группы, то PFH_G эквивалентна PFH_S, PFH_L или PFH_{FE} соответственно (см. В.3.1 и В.2.1).

2 В настоящей таблице предполагается, что $\beta = 2\beta_D$. Для архитектур 1oo1 и 2oo2 значения β и β_D не влияют на среднюю вероятность отказа.

В.3.4. Пример режима высокой интенсивности запросов или непрерывного режима

Рассмотрим функцию безопасности, для реализации которой нужна система SIL2. Пусть, построенный на основе предыдущего опыта, первоначальный вариант архитектуры всей системы включает одну группу из двух датчиков с архитектурой 1oo2 на входе. Логическая подсистема, рассматриваемой системы, представляет собой PES с избыточностью с архитектурой 2oo3 и управляет одним закрывающим контактором. Архитектура описанной системы представлена на рисунке В.14. Для этой системы оценим сначала функцию безопасности при шестимесячном периоде контрольных испытаний. Таблицы В.14 — В.16 являются фрагментами таблицы В.12 для соответствующих данных на рисунке В.14.



Примечание — Доля безопасных отказов для подсистемы оконечных элементов превышает 60 %.

Рисунок В.14 — Архитектура системы рассматриваемого примера для режима высокой интенсивности запросов или непрерывного режима

Таблица В.14 — Вероятность отказа в час для подсистемы датчиков в рассматриваемом примере режима высокой интенсивности запросов или непрерывного режима (шестимесячный интервал контрольных испытаний и среднее время ремонта 8 ч)

Архитектура	*DC*	λ = 5.0E-06		
		β = 2 % β_D = 1 %	β =10 % β_D =5 %	β = 20 % β_D =10 %
1oo2	0 %	7.6E-08	2.7E-07	5.2E-07
	60 %	4.6E-08	1.8E-07	3.6E-07
	90 %	3.0E-08	1.4E-07	2.8E-07
	99 %	2.6E-08	1.3E-07	2.5E-07
Примечание — Настоящая таблица представляет собой фрагмент таблицы В.12.				

Таблица В.15 — Вероятность отказа в час для логической подсистемы в рассматриваемом примере режима высокой интенсивности запросов или непрерывного режима (шестимесячный интервал контрольных испытаний и среднее время ремонта 8 ч)

Архитектура	*DC*	λ = 5.0E-06		
		β = 2 % β_D = 1 %	β = 2 % β_D = 1 %	β = 2 % β_D = 1 %
2oo3	0 %	4.2E-07	7.7E-07	1.2E-06
	60 %	2.0E-07	4.6E-07	8.0E-07
	90 %	8.8E-08	3.1E-07	5.8E-07
	99 %	5.5E-08	2.6E-07	5.1E-07
Примечание — Настоящая таблица представляет собой фрагмент таблицы В.12.				

Таблица В.16 — Вероятность отказа в час для подсистемы оконечных элементов в рассматриваемом примере режима высокой интенсивности запросов или непрерывного режима (шестимесячный интервал контрольных испытаний и среднее время ремонта 8 ч)

Архитектура	*DC*	λ = 1.0E-06
1oo1	0 %	5.0E-07
	60 %	2.0E-07
	90 %	5.0E-08
	99 %	5.0E-09
Примечание — Настоящая таблица представляет собой фрагмент таблицы В.12.		

Данные таблиц В.14 — В.16 позволяют получить следующие значения:

- для подсистемы датчиков:

$PFH_S = 5{,}2 \times 10^{-7} / h$;

- для логической подсистемы:

$PFH_L = 5{,}5 \times 10^{-8} / h$;

- для подсистемы оконечных элементов:

$PFH_{FE} = 5{,}0 \times 10^{-7} / h$;

следовательно, для функции безопасности:

$PFH_{SYS} = 5{,}2 \times 10^{-7} + 5{,}5 \times 10^{-8} + 5{,}0 \times 10^{-7}$

$= 1{,}1 \times 10^{-6} / h$

≡ уровень полноты безопасности 1.

Для перевода системы на уровень полноты безопасности 2 выполняют одно из следующих действий:

a) изменяют тип и способ установки входного датчика для улучшения защиты от отказа с общей причиной, таким образом, снижая значение β от 20 % до 10 %, а β_D от 10 % до 5 %:

$PFH_S = 2{,}7 \times 10^{-7} / h$

$PFH_L = 5{,}5 \times 10^{-8} / h$

$PFH_{FE} = 5{,}0 \times 10^{-7} / h$

$PFH_{SYS} = 8{,}3 \times 10^{-7} / h$

= уровень полноты безопасности 2;

b) заменяют единственное выходное устройство двумя устройствами с архитектурой 1oo2 (β = 10 % и β_D = 5 %):

$PFH_S = 5{,}2 \times 10^{-7} / h$

$PFH_L = 5{,}5 \times 10^{-8} / h$

$PFH_{FE} = 5{,}1 \times 10^{-8} / h$

$PFH_{SYS} = 6{,}3 \times 10^{-7} / h$

= уровень полноты безопасности 2.

Подробности оценки вероятностей отказа приведены в [2] — [7].

Приложение С
(справочное)

Расчет диагностического охвата и доли безопасных отказов

Метод расчета диагностического охвата и доли безопасных отказов приведен в МЭК 61508-2, приложение С. Настоящее приложение содержит краткое описание использования этого метода для расчета диагностического охвата E/E/PE системы, связанной с безопасностью. Предполагается, что информация, представленная в МЭК 61508-2, доступна и при необходимости используется при получении значений, приведенных в таблице С.1. Возможные диапазоны диагностического охвата для некоторых подсистем или компонент E/E/PE систем, связанных с безопасностью, представлены в таблице С.2. Значения, представленные в таблице С.2, опираются на инженерные оценки.

Для вычисления всех значений таблицы С.1 потребовалась бы подробная схема аппаратных средств, с помощью которой можно определить влияние всех режимов отказов. Представленные в таблице С.1 значения приведены в качестве примера (для некоторых компонентов таблицы С.1 диагностический охват не определен, так как практически невозможно обнаружить все режимы отказов этих компонентов).

Таблица С.1 была сформирована следующим образом:

a) Для определения влияния каждого вида отказов каждого компонента на поведение системы без диагностических испытаний был проведен анализ видов и влияния отказов. Для каждого компонента приведены доли безопасных отказов *S* и опасных отказов *D* от общей интенсивности отказов, связанные с каждым видом отказов. Для простых компонентов деление на опасные и безопасные отказы может быть четко определено, в остальных случаях — основано на инженерной оценке. Для сложных компонентов, если детальный анализ каждого вида отказа невозможен, считают, что отказы делятся в соотношении: 50 % безопасных, 50 % — опасных. Для формирования таблицы С.1 использовались виды отказов, задаваемые именно таким распределением, хотя возможно и другое, более предпочтительное распределение по видам отказов.

b) Значения диагностического охвата для каждого конкретного диагностического испытания каждого компонента помещают в столбце DC_{comp} таблицы С.1. В таблице С.1 также приведены конкретные значения диагностических охватов для обнаружения как безопасных, так и опасных отказов. Было показано, что для простых компонентов (например, резисторов, конденсаторов и транзисторов) отказы из-за отсутствия контакта или короткого замыкания обнаруживаются с диагностическим охватом 100 %, тем не менее использование таблицы С.2 ограничивает диагностический охват значением 90 % для компонента *U*16 комплексного компонента типа B.

c) В столбцах 1 и 2 таблицы С.1 приведены интенсивности безопасных λ_S и опасных $\lambda_{DD} + \lambda_{DU}$ отказов для каждого компонента при отсутствии диагностических испытаний.

d) Обнаруженный опасный отказ считают фактически безопасным, что позволяет определить отношение между фактически безопасными отказами (т. е. любыми обнаруженными безопасными, необнаруженными безопасными или обнаруженными опасными отказами) и необнаруженными опасными отказами. Интенсивность фактически безопасных отказов определяют произведением значения интенсивности опасных отказов и значения диагностического охвата для опасных отказов и сложением результата со значением интенсивности безопасных отказов (см. столбец 3 таблицы С.1). Точно так же интенсивность необнаруженных опасных отказов определяют вычитанием диагностического охвата для опасных отказов из единицы и умножением результата на интенсивность опасных отказов (см. столбец 4 таблицы С.1).

e) В столбце 5 таблицы С.1 приведены значения интенсивности обнаруженных безопасных отказов, а в столбце 6 таблицы С.1— значения интенсивности обнаруженных опасных отказов, полученные умножением значения диагностического охвата на значения интенсивности безопасных и опасных отказов соответственно.

f) Использование таблицы С.1 дает следующие результаты:

- общая интенсивность безопасных отказов, включая обнаруженные опасные отказы:

$$\Sigma\lambda_S + \Sigma\lambda_{DD} = 9{,}9\times10^{-7};$$

- общая интенсивность необнаруженных опасных отказов:

$$\Sigma\lambda_{DU} = 5{,}1\times10^{-8};$$

- общая интенсивность отказов:

$$\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU} = 1{,}0\times10^{-6};$$

- общая интенсивность необнаруженных безопасных отказов:

$$\Sigma\lambda_{SU} = 2{,}7\times10^{-8};$$

- диагностический охват для безопасных отказов:

$$\frac{\sum \lambda_{SD}}{\sum \lambda_S} = \frac{3{,}38}{3{,}65} = 93\ \%;$$

- диагностический охват для опасных отказов (обычно называемый «диагностическим охватом»):

$$\frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{6{,}21}{6{,}72} = 92\ \%;$$

- доля безопасных отказов:

$$\frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{986}{365+672} = 95\ \%.$$

g) Без диагностических испытаний интенсивность отказов распределяется следующим образом: 35 % безопасных отказов и 65 % — опасных отказов.

Таблица С.1 — Расчет диагностического охвата и доли безопасных отказов

Компонент	№	Тип	Распределение на безопасные и опасные отказы для каждого вида отказов								Распределение на безопасные и опасные отказы для диагностического охвата и рассчитанных интенсивностей отказов ($\times 10^{-9}$ ч$^{-1}$)						
			OC		SC		Изменение значения		Фукциональные отказы		DC_{comp}		1	2	3	4	5	6
			S	D	S	D	S	D	S	D	S	D	λ_S	$\lambda_{DD}+\lambda_{DU}$	$\lambda_S+\lambda_{DD}$	λ_{DU}	λ_{SD}	λ_{DD}
Print	1	Печать	0,5	0,5	0,5	0,5	0	0	0	0	0,99	0,99	11,0	11,0	21,9	0,1	10,9	10,9
*CN*1	1	Con96pin	0,5	0,5	0,5	0,5					0,99	0,99	11,5	11,5	22,9	0.1	11,4	11,4
*C*1	1	100 нФ	1	0	1	0	0	0	0	0	1	0	3,2	0,0	3,2	0,0	3,2	0,0
*C*2	1	10 мкФ	0	0	1	0	0	0	0	0	1	0	0,8	0,0	0,8	0.0	0,8	0,0
*R*4	1	1 М	0,5	0,5	0,5	0,5					1	1	1,7	1,7	3,3	0,0	1,7	1,7
*R*6	1	100 К									0	0	0.0	0,0	0,0	0,0	0,0	0,0
*OSC*1	1	OSC24 МГц	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	1	16,0	16,0	32,0	0.0	16,0	16,0
*U*8	1	74HCT85	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
*U*16	1	MC68000-12	0	1	0	1	0,5	0,5	0,5	0,5	0,90	0,90	260,4	483,6	695,6	48,4	234,4	435,2
*U*26	1	74HCT74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	22,8	22,8	45,4	0,2	22,6	22,6
*U*27	1	74F74	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,99	0,99	14,4	14,4	28,7	0.1	14,3	14,3
*U*28	1	PAL16L8A	0	1	0	1	0	1	0	1	0,98	0,98	0,0	88,0	86,2	1,8	0,0	86,2
*T*1	1	BC817	0	0	0	0,67	0	0,5	0	0	1	1	0,0	0,2	0,4	0.0	0,0	0,2
Всего													365	672	986	50,9	338	621

S — безопасный отказ; *D* — опасный отказ; *OC* — потеря контакта; *SC* — короткое замыкание; DC_{comp} — диагностический охват для компонента

Примечания

1 Не обнаружен ни один вид отказа для компонента *R*6, т.е. его отказ не влияет на безопасность и готовность системы.

2 См. также таблицу В.1 (в настоящей таблице интенсивности отказов приведены только для отдельных рассматриваемых компонентов в канале, а не для каждого компонента).

Таблица С.2 — Уровни и диапазоны диагностического охвата различных подсистем (компонентов)

Компонент	Низкий диагностический охват	Средний диагностический охват	Высокий диагностический охват
Процессор (см. примечание 3):	в сумме менее 70 %	в сумме менее 90 %	—
- регистр	50 % — 70 %	85 % — 90 %	99 % — 99,99 %
- внутренняя регистровая память (см. примечание 3)	50 % — 60 %	75 % — 95 %	—
- блок кодирования и выполнения, включающий регистр тэгов (см. примечание 3)	50 % — 70 %	85 % — 98 %	—
- устройство вычисления адреса	50 % — 60 %	60 % — 90 %	85 % — 98 %
- счетчик команд	50 % — 70 %	—	—
- указатель стека	40 % — 60 %	—	
Шина:			
- модуль управления памятью	50 %	70 %	90 % — 99 %
- устройство управления шины	50 %	70 %	90 % — 99 %
Обработка прерываний	40 % — 60 %	60 % — 90 %	85 % — 98 %
Кварцевый тактовый генератор (см. примечание 4)	50 %	—	95 % — 99 %
Контроль выполнения программы:			
- временное (см. примечание 3)	40 % — 60 %	60 % — 80 %	—
- логическое (см. примечание 3)	40 % — 60 %	60 % — 90 %	—
- временное и логическое (см. примечание 5)	—	65 % — 90 %	90 % — 98 %
Постоянная память	50 % — 70 %	99%	99,99 %
Непостоянная память	50 % — 70 %	85 % — 90 %	99 % — 99,99 %
Дискретное оборудование:			
- цифровой ввод/вывод	70 %	90 %	99 %
- аналоговый ввод/вывод	50 % — 60 %	70 % — 85 %	99 %
- источник питания	50 % — 60 %	70 % — 85 %	99 %
Устройство связи и запоминающее устройство большой емкости	90 %	99,9 %	99,99 %
Электромеханические устройства	90 %	99 %	99,9 %
Датчики	50 % — 70 %	70 % — 85 %	99 %
Оконечные элементы	50 % — 70 %	70 % — 85 %	99 %

Примечания

1 Настоящую таблицу применяют совместно с МЭК 61508-2, таблица А.1, в котором приведены анализируемые виды отказов.

2 Если для диагностического охвата задан конкретный диапазон, верхние границы интервала могут быть определены только для узкого круга средств контроля или тестирования, которые реализуют чрезвычайно динамичную нагрузку для проверяемой функции.

3 В настоящее время для подсистем, схемы высокого диагностического охвата которых отсутствуют, средства и методы высокой достоверности диагностики неизвестны.

4 В настоящее время для кварцевых тактовых генераторов средства и методы средней достоверности неизвестны.

5 Низкий диагностический охват для комбинации временного и логического контроля выполнения программы является средним.

Полезную информацию можно найти в [8] — [10].

Приложение D
(справочное)

Методика количественного определения влияния отказов аппаратных средств с общей причиной в E/E/PE системах

D.1 Общие положения

Настоящий стандарт включает в себя ряд методов, рассматривающих систематические отказы. Однако независимо от того, насколько эффективны эти методы, существует остаточная вероятность возникновения систематических отказов. Это незначительно влияет на результаты расчета надежности для одноканальных систем, однако возможность появления отказов, способных повлиять на несколько каналов многоканальной системы, т.е. отказов по общей причине, приводит к существенным ошибкам при расчетах надежности многоканальных систем.

В настоящем приложении приводится описание методики, позволяющей учитывать отказы по общей причине при оценке безопасности многоканальных E/E/PE систем. Использование данной методики дает более точную оценку полноты безопасности такой системы, чем при игнорировании отказов по общей причине.

Данная методика используется для расчета значения β, β-фактора, часто используемого при моделировании отказов по общей причине. Описываемая методика может быть использована для оценки интенсивности отказов по общей причине в случае двух или более параллельно работающих систем, если известна интенсивность случайных отказов аппаратных средств для одной из этих систем (см. D.5). В некоторых случаях предпочтительнее альтернативные методики, например, если благодаря наличию данных об отказах по общей причине можно получить более точное значение β-фактора.

D.2 Краткий обзор

Считается, что отказы системы бывают двух видов:

- случайные отказы аппаратных средств;
- систематические отказы.

Предполагается, что отказы первого вида возникают случайно по времени для любого компонента и приводят к отказу канала системы, частью которого является соответствующий компонент. Существует некоторая вероятность того, что во всех каналах многоканальной системы могут произойти независимые случайные отказы аппаратных средств, вследствие чего все каналы одновременно окажутся неработоспособными. Так как предполагается, что такие отказы аппаратных средств возникают во времени случайно, вероятность таких отказов, одновременно возникающих в параллельных каналах, низка по сравнению с вероятностью отказа одного канала. Такая вероятность может быть рассчитана с помощью хорошо известных методов.

Однако некоторые отказы, например отказы по общей причине, являющиеся следствием одной причины, могут влиять на несколько каналов, что может быть следствием систематической ошибки (например, конструктивной или ошибки технических условий) или внешнего воздействия, ведущего к преждевременным случайным аппаратным отказам (например, избыточной температуры, возникающей из-за случайного отказа аппаратного средства, обычного вентилятора, что сокращает время жизни компонентов или нарушает заданные условия окружающей среды для их работы), или комбинации этих факторов. Так как отказы по общей причине чаще влияют на несколько каналов многоканальной системы, то вероятность такого отказа, скорее всего, будет доминирующим фактором при определении общей вероятности отказа многоканальной системы. Если не учитывать этот фактор, будет трудно получить правильную оценку уровня полноты безопасности.

Хотя отказы по общей причине являются следствием одной причины, они не обязательно проявляются во всех каналах одновременно. Например, при отказе вентилятора все каналы многоканальной E/E/PE системы могут отказать, что ведет к отказу по общей причине. Однако необязательно все каналы нагреваются с одинаковой скоростью или имеют общую критическую температуру. Следовательно, отказы возникают в разных каналах в разное время.

Архитектура программируемых систем позволяет им выполнять внутреннее диагностическое тестирование непосредственно во время работы, что может быть реализовано различными способами, например:

- один канал PES одновременно с обеспечением работы входного и выходного устройств может непрерывно выполнять внутреннюю проверку своей работы. На этапе проектирования можно достичь значения тестового охвата, равного 99 % (см. [11]). Если 99 % внутренних сбоев обнаружены до того, как они приведут к отказу, вероятность сбоев одного канала, которые могут, в конечном счете, стать частью отказов по общей причине, значительно снижается;

- помимо внутреннего тестирования каждый канал PES может отслеживать выходы других каналов многоканальной PES (или каждое PE-устройство может отслеживать другое PE-устройство системы, состоящей из нескольких PE-устройств). Следовательно, отказ, возникший в одном канале, может быть обнаружен, и один или несколько оставшихся неотказавших каналов будут выполнять перекрестный контроль и инициировать безопасное выключение (следует отметить, что перекрестный контроль эффективен, если состояние системы управления постоянно меняется, например, при наличии часто используемой в циклически работающем устройстве защитной

блокировки или при внесении в устройство небольших изменений, не влияющих на управляющую функцию). Интенсивность выполняемого перекрестного контроля может быть достаточно высока, поэтому непосредственно перед неодновременными отказами по общей причине перекрестный контроль, скорее всего, обнаружит первый отказавший канал и позволит перевести систему в безопасное состояние до момента отказа второго канала.

Например, для вентилятора скорость роста температуры и восприимчивость каналов несколько различаются, поэтому второй канал, возможно, откажет спустя несколько десятков минут после первого. Это позволяет после диагностического тестирования инициировать безопасное отключение первого отказавшего канала до того, как по общей причине откажет второй канал.

Таким образом:

- PE-системы обладают возможностью формировать барьеры защиты от отказов по общей причине и, следовательно, в меньшей степени подвержены им по сравнению с другими технологиями;

- для PE-систем можно использовать β-фактор, отличающийся от β-фактора для других технологий. Следовательно, оценки β-фактора, опирающиеся на предыдущие значения оценки интенсивности отказов, скорее всего, окажутся неправильными (ни одна из известных существующих моделей оценки вероятности отказа по общей причине не учитывает эффект автоматического перекрестного контроля);

- так как разнесенные во времени отказы по общей причине могут быть обнаружены с помощью диагностического тестирования до отказа всех каналов, подобные отказы могут не восприниматься как отказы по общей причине.

Существует три способа уменьшения вероятности потенциально опасных отказов по общей причине:

1) уменьшение общего числа случайных аппаратных и систематических отказов (это уменьшает площади эллипсов, представленных на рисунке D.1, приводя к уменьшению площади пересечения эллипсов);

2) максимальное увеличение независимости каналов (это уменьшает площадь пересечения эллипсов, представленных на рисунке D.1, не меняя площади самих эллипсов);

3) обнаружение неодновременных отказов по общей причине, когда неисправным становится только один канал, до того как станет неисправным второй, т. е. использование диагностического тестирования.

Настоящий стандарт использует эти три способа и требует подхода, состоящего из следующих трех этапов:

1) использование методов по МЭК 61508-3 для снижения общей вероятности систематических отказов до уровня, соизмеримого с вероятностью случайных аппаратных отказов;

2) количественное определение факторов, которые могут быть количественно определены, т. е. учет вероятности случайного аппаратного отказа, как определено в МЭК 61508-2;

3) определение отношения, связывающего вероятность отказа по общей причине с вероятностью случайного отказа аппаратных средств с использованием практических средств, которые считаются лучшими в настоящее время. В настоящем приложении описана методика определения этого отношения.

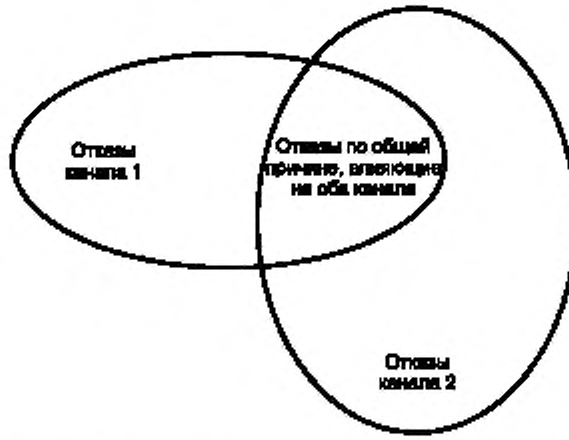


Рисунок D.1 — Связь между отказами с общей причиной и отказами отдельных каналов

Большинство методик оценки вероятности отказов по общей причине формируют прогнозы на основе вероятности случайного аппаратного отказа. Несомненно, непосредственной взаимосвязи между этими вероятностями нет, тем не менее на практике некоторая корреляция между ними была найдена и, возможно, является следствием эффектов второго порядка. Например, высокая вероятность случайного аппаратного отказа системы связана:

- с большим объемом обслуживания, который требует система. А вероятность систематического отказа, являющегося следствием обслуживания, зависит от числа проведенных сеансов обслуживания, что также повышает интенсивность воздействия человеческих ошибок, приводящее к отказам по общей причине. Таким образом возникает связь между вероятностью случайного аппаратного отказа и вероятностью отказа по общей причине, например, после каждого случайного аппаратного отказа требуется ремонт, а за ним тестирование и, возможно, повторная калибровка. Кроме того, для заданного уровня полноты безопасности система с большей вероятностью случайного аппаратного отказа требует более частого проведения контрольных испытаний и с большей глубиной/сложностью, что также увеличивает влияние человеческого фактора;

- со сложностью системы. Вероятность случайного аппаратного отказа зависит от числа компонентов и, следовательно, сложности системы. Сложную систему труднее понять, поэтому у нее выше вероятность появления систематических ошибок. Кроме того, сложность системы затрудняет обнаружение отказов путем анализа или тестирования и может приводить к тому, что часть логики системы будет выполняться только при редко встречающихся условиях. Это также приводит к появлению связи между вероятностью случайного аппаратного отказа и вероятностью отказа по общей причине.

Несмотря на ограничения рассматриваемых моделей, считается, что в настоящее время они представляют собой лучший способ оценки вероятности отказа по общей причине для многоканальной системы. Описываемый в настоящем подразделе метод для третьего этапа рассматриваемой в настоящем приложении методики основан на общепризнанной модели β-фактора.

При использовании модели β-фактора для E/E/PE-системы возникают следующие проблемы:

- выбор значения β-фактора. Многие источники (например, см. [11]) предлагают диапазоны возможных значений β-фактора, но не определяют их конкретные значения, оставляя выбор за пользователем. Чтобы решить эту проблему, методика, представленная в настоящем приложении, основывается на подходе, первоначально описанном в [12] и затем скорректированном в [13];

- модель β-фактора не учитывает развитые возможности диагностического тестирования современных PES, которыми можно воспользоваться для обнаружения неодновременных отказов по общей причине до того, как отказ полностью проявит себя. Для преодоления этой проблемы подход, описанный в [12] и скорректированный в [13], был изменен с тем, чтобы отразить влияние диагностического тестирования при оценке возможного значения β.

Функции диагностического тестирования, выполняющиеся внутри PES, обеспечивают непрерывное сравнение работы PES с заранее определенными состояниями. Эти состояния предварительно определяются программно или аппаратно (например с помощью контрольного таймера). Рассматриваемые таким образом функции диагностического тестирования можно считать дополнительными и частично различающимися для каналов, работающих в PES параллельно.

Также может использоваться метод перекрестного контроля каналов. Многие годы этот метод применялся в двухканальных системах с взаимной блокировкой, построенных исключительно на реле. Однако релейная технология обычно позволяет проводить перекрестное тестирование только во время изменения состояния каналов, что делает такое тестирование неподходящим для обнаружения неодновременных отказов по общей причине, если системы остаются в одном (например, включенном) состоянии в течение длительного времени. С помощью технологии PES перекрестный контроль может проводиться с высокой частотой.

D.3 Область применения методики

Область применения методики ограничена аппаратными отказами по общей причине по следующим причинам:

- модель β-фактора связывает вероятность отказов по общей причине с вероятностью случайных аппаратных отказов. Вероятность отказов по общей причине, затрагивающих систему в целом, зависит от сложности системы (в которой главную роль возможно играет пользовательское программное обеспечение), а не только от аппаратуры. Очевидно, что любые расчеты, основанные на вероятности случайного аппаратного отказа, не могут учитывать сложность программного обеспечения;

- информирование об отказах по общей причине обычно ограничивается аппаратными отказами, что является главной заботой производителей оборудования;

- моделирование систематических отказов (например, отказов программного обеспечения) считается практически неосуществимым;

- целью мероприятий, определенных в МЭК 61508-3, является снижение вероятности отказов по общей причине, связанных с программным обеспечением, до значения, приемлемого для необходимого уровня полноты безопасности.

Следовательно, оценка вероятности отказа по общей причине, выполненная по данной методике, связана только с аппаратными отказами. Эту методику не допускается использовать для получения общей интенсивности отказов, учитывающей вероятность отказа, связанного с программным обеспечением.

D.4 Особенности методики

Так как на датчики, логическую подсистему и оконечные элементы влияют, например различные условия окружающей среды, для каждой из этих подсистем настоящую методику применяют независимо. Например, логическую подсистему проще поместить в контролируемую среду, а датчики могут быть установлены снаружи и подвергнуты внешнему воздействию.

Программируемые электронные каналы предоставляют возможность для реализации разнообразных функций диагностического тестирования и способны:

- обеспечивать высокий диагностический охват в пределах конкретных каналов;
- контролировать дополнительные избыточные каналы;
- обеспечивать высокую частоту повторения;
- контролировать с повышенной частотой датчики и/или оконечные элементы.

Чаще всего отказы по общей причине не возникают одновременно во всех затронутых каналах. Поэтому, если частота повторения диагностического тестирования достаточно высока, большую часть отказов по общей причине можно обнаружить и, следовательно, устранить до того, как будут затронуты остальные доступные каналы.

Не все функции многоканальной системы, обеспечивающие устойчивость к отказам по общей причине, можно проверить с помощью диагностического тестирования. Однако эффективность этих функций, связанных с диверсификацией или независимостью, постоянно повышается. Любая функция, которая, возможно, увеличивает время между отказами каналов в случае неодновременного отказа по общей причине (или уменьшает долю одновременных отказов по общей причине), увеличивает вероятность обнаружения отказа при диагностическом тестировании и перевода установки в безопасное состояние. Следовательно, функции, связанные с устойчивостью к отказам по общей причине, делятся на функции, влияние которых предположительно возрастает при использовании диагностического тестирования, и влияние которых не меняется (см. таблицу D.1, столбцы X и Y соответственно).

Хотя для трехканальной системы вероятность отказов по общей причине, влияющих на все три канала, скорее всего значительно ниже вероятности отказов, влияющих на два канала, для упрощения методики предполагается, что вероятность отказов не зависит от числа затрагиваемых каналов, т.е. возникающий отказ по общей причине затрагивает все каналы.

Данных об аппаратных отказах по общей причине, необходимых для калибровки методики, не существует, поэтому данные таблиц в настоящем приложении основываются на инженерных оценках.

Иногда процедуры диагностического тестирования не рассматриваются как необходимые для обеспечения безопасности, поэтому их уровень обеспечения качества может быть ниже, чем процедур, обеспечивающих основные функции управления. Данная методика была разработана в предположении, что уровень полноты безопасности для диагностического тестирования соответствует требуемому. Следовательно, любые программные процедуры диагностического тестирования должны разрабатываться с использованием методов, соответствующих требуемому уровню полноты безопасности.

D.5 Использование β-фактора для вычисления вероятности отказа E/E/PE-системы, связанной с безопасностью, из-за отказов по общей причине

Влияние отказов по общей причине на многоканальную систему с диагностическим тестированием следует рассматривать в каждом из каналов системы.

Используя модель β-фактора, для интенсивности опасных отказов по общей причине получим $\lambda_D\beta$, где λ_D — интенсивность опасных случайных аппаратных отказов для каждого отдельного канала, а β — β-фактор в отсутствие диагностического тестирования, т. е. доля отказов одного канала, влияющих на все каналы.

Предположим, что отказы по общей причине влияют на все каналы, а промежуток времени между первым и остальными отказавшими каналами мал по сравнению с интервалом времени между последовательными отказами по общей причине.

Пусть в каждом канале применяется диагностическое тестирование, которое обнаруживает и вскрывает часть отказов. Отказы подразделяют на две категории: отказы, которые находятся вне охвата диагностического тестирования (т. е. не могут быть обнаружены), и отказы в пределах охвата (которые будут обнаружены диагностическим тестированием).

Поэтому общую интенсивность отказов системы, вызванных опасными отказами по общей причине, вычисляют по формуле

$$\beta_{DU}\beta + \lambda_{DD}\beta_D ,$$

где λ_{DU} — интенсивность необнаруженных отказов одного канала, т. е., интенсивность опасных отказов, находящихся за пределами охвата диагностического тестирования; очевидно, любое уменьшение β-фактора, являющееся следствием частоты проведения диагностического тестирования, не может повлиять на λ_{DU};

β — фактор отказов по общей причине для необнаруживаемых опасных отказов, который равен общему β-фактору, применяемому в отсутствие диагностического тестирования;

λ_{DD} — интенсивность обнаруженных опасных отказов одного канала (т. е. интенсивность опасных отказов одного канала), находящихся в пределах охвата диагностического тестирования; если частота проведения диагностического тестирования высока, доля обнаруженных отказов ведет к уменьшению значения β, т. е. β_D;

β_D — доля опасных отказов по общей причине, обнаруживаемых диагностическими тестами. С увеличением частоты проведения диагностического тестирования значение β_D становится меньше β.

Значение β определяется по таблице D.4 с помощью оценки $S = X + Y$ (см. D.6).

Значение β_D определяется по таблице D.4 с помощью оценки $S_D = X(Z + 1) + Y$.

D.6 Использование таблиц для оценки β

Оценку β-фактора рассчитывают отдельно для датчиков, логической подсистемы и оконечных элементов.

Для того чтобы свести к минимуму вероятность возникновения отказов по общей причине, следует сначала определить средства, эффективно защищающие от появления таких отказов. Реализация соответствующих средств в системе ведет к уменьшению значения β-фактора, используемого при оценке вероятности отказа системы из-за отказов по общей причине.

Мероприятия и соответствующие им значения (баллы) параметров X и Y, полученные с помощью инженерной оценки и описывающие вклад каждого из мероприятий в уменьшение числа отказов по общей причине, перечислены в таблице D.1. Так как датчики и оконечные элементы анализируются иначе, чем программируемая электроника, в таблице D.1 используются столбцы X_{LS} и Y_{LS} для программируемых электронных средств и столбцы X_{SF} и Y_{SF} для датчиков или оконечных элементов.

Программируемые электронные системы могут использовать интенсивное диагностическое тестирование, позволяющее обнаруживать неодновременные отказы по общей причине. Для учета диагностического тестирования при оценке β-фактора общий вклад каждого из мероприятий в таблице D.1 разделен с использованием инженерной оценки на наборы значений X и Y. Для каждого конкретного мероприятия отношение X:Y представляет собой меру повышения вклада этого мероприятия в борьбу с отказами по общей причине благодаря диагностическому тестированию.

Пользователь таблицы D.1 должен определить, какие мероприятия будут использованы для рассматриваемой системы, и сложить соответствующие мероприятиям баллы, приведенные в графах X_{LS} и Y_{LS} для логической подсистемы или в графах X_{SF} и Y_{SF} — для датчиков или оконечных элементов, получив суммы X и Y соответственно.

Коэффициент Z определяют по таблицам D.2 и D.3 по частоте и охвату диагностического тестирования с учетом примечания, определяющего, когда следует использовать ненулевое значение Z. Затем (при необходимости) рассчитывают сумму баллов S (см. D.5) по формуле $S = X + Y$ — для получения значения β (β-фактора для необнаруженных отказов) и $S_D = X(Z + 1) + Y$ — для получения значения β_D (β_D-фактора для обнаруженных отказов), где S или S_D — баллы, используемые в таблице D.4 для определения соответствующего β-фактора.

Таблица D.1 — Оценка мероприятий (барьеров) защиты программируемых электронных средств или датчиков/оконечных элементов от возникновения отказов по общей причине

Мероприятие	Логическая подсистема		Датчики и оконечные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Разделение/выделение				
Везде ли сигнальные кабели каналов разделены между собой	1,5	1,5	1,0	2,0
Расположены ли логические подсистемы каналов на отдельных печатных платах	3,0	1,0	—	—
Расположены ли логические подсистемы каналов в отдельных шкафах	2,5	0,5	—	—
Если датчики/оконечные элементы включают в себя собственную управляющую электронику, то расположена ли электроника для каждого канала на отдельной печатной плате	—	—	2,5	1,5
Если датчики/оконечные элементы включают собственную управляющую электронику, то расположена ли электроника для каждого канала в различных помещениях и различных шкафах	—	—	2,5	0,5
Диверсификация/избыточность				
Реализованы ли в каналах различные электрические технологии, например, один канал электронный или программируемый электронный, а для другого используются реле	7,0	—	—	—
Реализованы ли в каналах различные электронные технологии, например, один канал — электронный, а другой — программируемый электронный	5,0	—	—	—
Используют ли устройства различные физические принципы для датчиков, например, давления и температуры, анемометр с вертушкой и доплеровский датчик и т. д.	—	—	7,5	—
Используют ли устройства различные электрические принципы/конструкции, например, цифровые и аналоговые, с компонентами от различных производителей (но не уцененные) или с различной технологией	—	—	5,5	—

Продолжение таблицы D.1

Мероприятие	Логическая подсистема		Датчики и оконечные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Используют ли каналы повышенную избыточность с архитектурой MooN, где $N > M + 2$	2,0	0,5	2,0	0,5
Используют ли каналы повышенную избыточность с архитектурой MooN, где $N = M + 2$	1,0	0,5	1,0	0,5
Применяется ли низкая диверсификация, например, диагностическое тестирование аппаратуры использует одинаковую технологию	2,0	1,0	—	—
Применяется ли средняя диверсификация, например, диагностическое тестирование аппаратуры использует различную технологию	3,0	1,5	—	—
Были ли разработаны каналы различными конструкторами, которые не взаимодействовали между собой в процессе разработки	1,0	1,0	—	—
Использовались ли для каждого канала различные люди и различные методы тестирования в процессе его пуска	1,0	0,5	1,0	1,0
Обслуживается ли каждый канал в разное время разными людьми	2,5	—	2,5	—
Сложность/конструкция/применение/завершенность/опыт				
Предотвращает ли перекрестная связь между каналами обмен любой информацией, кроме используемой для диагностического тестирования или голосования	0,5	0,5	0,5	0,5
Превышает ли время использования в отрасли методов, применяемых для проектирования аппаратуры, 5 лет	0,5	1,0	1,0	1,0
Превышает ли время работы с этим же оборудованием в аналогичных условиях 5 лет	1,0	1,5	1,5	1,5
Проста ли система, например, имеет ли она не более 10 входов или выходов на канал	—	1,0	—	—
Защищены ли входы и выходы от возможного превышения безопасных значений напряжения и тока	1,5	0,5	1,5	0,5
С запасом ли рассчитаны все устройства/компоненты (например, с коэффициентом 2 или более)	2,0	—	2,0	—
Оценка/анализ и обратная связь				
Были ли изучены результаты анализа видов и влияния отказов или дерево неисправностей для того, чтобы установить источники отказов по общей причине, и устранены ли при проектировании предварительно известные источники отказов по общей причине	—	3,0	—	3,0
Рассматривались ли отказы по общей причине при анализе проекта при последующем внесении изменений в проект (требуется документальное доказательство действий по анализу проекта)	—	3,0	—	3,0
Все ли возможные отказы были полностью проанализированы и учтены в проекте (требуется документальное доказательство процедуры)	0,5	3,5	0,5	3,5
Процедуры/интерфейс пользователя				
Существует ли зафиксированная письменно схема работы, гарантирующая обнаружение отказов (или ухудшение характеристик) всех компонентов, установление корневых причин и проверку других аналогичных вопросов для аналогичных возможных причин отказов	—	1,5	0,5	1,5
Предусмотрены ли процедуры, обеспечивающие: разнесение обслуживания (включая настройку или калибровку) по времени любой части независимых каналов; возможность выполнения диагностического тестирования помимо ручных проверок, проводимых в ходе очередного обслуживания, между завершением обслуживания одного канала и началом обслуживания другого	1,5	0,5	2,0	1,0

Окончание таблицы D.1

Мероприятие	Логическая подсистема		Датчики и оконечные элементы	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Определено ли в документированных процедурах обслуживания, что обеспечивающие избыточность компоненты систем (например кабели и.т.д.) должны быть независимы друг от друга и закреплены в устройстве	0,5	0,5	0,5	0,5
Проводится ли обслуживание печатных плат и т. д. вне рабочего места, в компетентном ремонтном центре и проводится ли тестирование отремонтированных элементов перед их установкой	0,5	1,0	0,5	1,5
Обеспечивает ли система низкий диагностический охват (от 60 % до 90 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации	0,5	—	—	—
Обеспечивает ли система средний диагностический охват (от 90 % до 99 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации	1,5	1,0	—	—
Обеспечивает ли система высокий диагностический охват (> 99 %) и сообщает ли об отказах на уровне модуля, допускающего замену в процессе эксплуатации	2,5	1,5	—	—
Сообщает ли диагностическое тестирование системы об отказах на уровне модуля, допускающего замену в процессе эксплуатации	—	—	1,0	1,0
Компетентность/обучение/культура безопасности				
Обучены ли конструкторы (с помощью обучающей документации) понимать причины и следствия отказов по общей причине	2,0	3,0	2,0	3,0
Обучен ли обслуживающий персонал (с помощью обучающей документации) понимать причины и следствия отказов по общей причине	0,5	4,5	0,5	4,5
Контроль состояния окружающей среды				
Ограничен ли доступ персонала (закрытые шкафы, недоступное размещение компонентов и т.д.)	0,5	2,5	0,5	2,5
Возможно ли, что система всегда будет работать в заданных диапазонах температур, влажности, коррозии, пыли, вибрации и т.д., в которых ее работа была проверена, без использования внешнего контроля состояния окружающей среды	3,0	1,0	3,0	1,0
Все ли сигнальные и силовые кабели отделены друг от друга	2,0	1,0	2,0	1,0
Проверка влияния окружающей среды				
Было ли проверено, что система устойчива ко всем воздействиям окружающей среды (например ЭМС, температура, вибрация, ударные нагрузки, влажность) на уровне, заданном в соответствующих международных или национальных стандартах	10,0	10,0	10,0	10,0

Примечания

1 Ряд факторов, связанных с работой системы, трудно предсказать во время проектирования. В таких случаях конструкторы должны убедиться в том, что конечный пользователь системы уведомлен, например, о процедурах, используемых для достижения требуемого уровня полноты безопасности. Необходимая информация должна быть включена в сопроводительную документацию.

2 Значения *X* и *Y* основаны на инженерной оценке и учитывают как косвенное, так и прямое влияние мероприятий. Например, использование модулей, допускающих замену во время эксплуатации, приводит:

- к выполнению ремонтных работ производителем в соответствующих условиях вместо ремонтных работ, выполняемых на месте в менее подходящих условиях. Это вносит свой вклад в значения *Y*, так как снижается вероятность систематических отказов и, следовательно, отказов по общей причине;
- к снижению необходимости вмешательства человека на месте и к возможности быстрой замены неисправных модулей, не выключая системы, повышая таким образом эффективность диагностики для идентификации отказов до того, как они станут отказами по общей причине. Это заметно влияет на значения *X*.

Таблица D.2 — Значение Z: программируемая электроника

Диагностический охват	Периодичность диагностического тестирования		
	Менее 1 мин	От 1 до 5 мин	Более 5 мин
≥ 99 %	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Таблица D.3 — Значение Z: датчики или оконечные элементы

Диагностический охват	Периодичность диагностического тестирования			
	Менее 2 ч	От 2 ч до 2 дней	От 2 до 7 дней	Более 7 дней
≥ 99 %	2,0	1,5	1,0	0
≥ 90 %	1,5	1,0	0,5	0
≥ 60 %	1,0	0,5	0	0

Примечания

1 Данная методика наиболее эффективна, если при подсчете баллов равномерно учитываются все группы мероприятий, представленные в таблице D.1. Следовательно, рекомендуется, чтобы общая сумма баллов *X* и *Y* для каждой группы была не менее общей суммы баллов *X* и *Y*, деленной на 20. Например, если общая сумма баллов *X* + *Y* равна 80, то общая сумма баллов *X* + *Y* для любой из групп (например, для группы мероприятий «Процедуры/интерфейс пользователя») должна быть не менее четырех.

2 При использовании таблицы D.1 следует учитывать баллы для всех реализованных в системе мероприятий. Подсчет суммы баллов был разработан для учета тех мероприятий, которые не являются взаимно исключающими. Например, для системы, логические подсистемы каналов которой расположены в отдельных стойках, подсчитывают сумму баллов мероприятий таблицы D.1 «Расположены ли логические подсистемы каналов в отдельных шкафах» и «Расположены ли логические подсистемы каналов на отдельных печатных платах».

3 Если в датчиках или оконечных элементах используется программируемая электроника, их рассматривают как часть логической подсистемы, если они находятся в том же здании (транспортном средстве), что и устройство, являющееся главной частью логической подсистемы, и в качестве датчиков или оконечных элементов — если они расположены отдельно.

4 Для того, чтобы использовать ненулевое значение *Z*, нужно убедиться, что управляемое оборудование переходит в безопасное состояние до того, как неодновременный отказ по общей причине сможет повлиять на все каналы. Время, необходимое для обеспечения этого безопасного состояния, должно быть менее заявленного интервала диагностического тестирования. Ненулевое значение *Z* допускается использовать только в случае, если:

- система инициирует автоматическое выключение при обнаружении сбоя или
- безопасное выключение не инициируется после первого сбоя[1)], но диагностическое тестирование определяет местонахождение сбоя и может его локализовать, а также сохраняет способность перевода EUC в безопасное состояние после обнаружения любых последующих сбоев или

[1)] Необходимо учитывать действия системы при обнаружении сбоя. Например, простая система с архитектурой голосования 2oo3 должна быть выключена (или отремонтирована) после обнаружения одиночного отказа в течение времени, приведенного в таблице D.2 или D.3. Если система не выключена, отказ второго канала может привести к тому, что при голосовании два отказавших канала получат перевес голосов над оставшимся (работоспособным) каналом. У системы, которая автоматически сама меняет архитектуру голосования на 1oo2 при отказе одного канала и автоматически выключается при возникновении второго отказа, вероятность обнаружения неисправности второго канала повышается и, следовательно, ненулевое значение *Z* возможно.

- используют формальную систему работы, гарантирующую, что причина любого обнаруженного сбоя будет полностью проанализирована в течение заявленного периода диагностического тестирования и либо установка немедленно выключается, если сбой может привести к отказу по общей причине, либо канал, в котором произошел сбой, восстанавливается в течение заявленного интервала диагностического тестирования.

5 В обрабатывающих отраслях вряд ли возможно выключать EUC при обнаружении сбоя во время интервала диагностического тестирования в соответствии с таблицей D.2. Настоящая методика не должна восприниматься как содержащая строгое требование выключать технологические установки непрерывного производства при обнаружении подобных сбоев. Однако если выключение не производится, то уменьшить β-фактор с помощью использования диагностического тестирования для программируемых электронных средств невозможно. В ряде других отраслей выключение EUC во время интервала диагностического тестирования возможно. В этих случаях допускается использовать ненулевое значение Z.

6 Если диагностическое тестирование проводится модульно, то время повторения, приведенное в таблице D.2 или D.3, — это время между завершениями последовательного диагностического тестирования всего набора модулей. Диагностический охват — общий охват, обеспечиваемый всеми модулями.

Таблица D.4 — Расчет величины β или β_D

Баллы (S или S_D)	Значение β или β_D для	
	логической подсистемы	датчиков или оконечных элементов
120 или более	0,5 %	1 %
От 70 до 120	1 %	2 %
От 45 до 70	2 %	5 %
Менее 45	5 %	10 %

Примечания

1 Максимальные уровни β_D ниже обычно используемых, что объясняется использованием методов, описанных в настоящем стандарте, для уменьшения вероятности систематических отказов в целом и в результате — вероятности отказов по общей причине.

2 Значения β_D менее 0,5 % для логической подсистемы и 1 % — для датчиков трудно подтвердить.

D.7 Использование методики

Для демонстрации результата использования методики значения β и β_D для программируемых электронных средств приведены в таблице D.5.

Для всех групп мероприятий, кроме — «диверсификация/избыточность», были использованы типовые значения *X* и *Y*. Они были получены делением максимального значения баллов для конкретных групп на два.

Для систем с разнообразием (см. таблицу D.5) значения *X* и *Y* для группы «диверсификация/избыточность» были выведены, исходя из следующих мероприятий, рассмотренных в таблице D.1:

- одна система электронная, другая использует технологию реле;
- диагностическое тестирование аппаратуры использует различные технологии;
- разные конструкторы не взаимодействовали между собой в процессе проектирования;
- для пуска системы использовались различные методы тестирования и разный персонал;
- обслуживание проводится в разное время разными людьми.

Для систем с избыточностью (см. таблицу D.5) значения *X* и *Y* для группы «диверсификация/избыточность» были выведены, исходя из того, что диагностика аппаратуры проводилась независимой системой, использующей ту же технологию, что и системы с избыточностью.

В системах с разнообразием и в системах с избыточностью для величины *Z* использовались максимальные и минимальные значения, поэтому в таблице D.5 значения β и β_D представлены для четырех систем.

Таблица D.5 — Значения β и β_D для программируемых электронных средств

Группа мероприятий		Система с разнообразием и хорошим диагностическим тестированием	Система с разнообразием и плохим диагностическим тестированием	Система с избыточностью и хорошим диагностическим тестированием	Система с избыточностью и плохим диагностическим тестированием
Разделение/выделение	*X*	3,50	3,50	3,50	3,50
	Y	1,50	1,50	1,50	1,50
Диверсификация/избыточность	*X*	14,50	14,50	2,00	2,00
	Y	3,00	3,00	1,00	1,00
Сложность/конструкция/.....	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Оценка/анализ/....	*X*	0,25	0,25	0,25	0,25
	Y	4,75	4,75	4,75	4,75
Процедуры/интерфейс пользователя	*X*	3,50	3,50	3,50	3,50
	Y	3,00	3,00	3,00	3,00
Компетентность/обучение/...	*X*	1,25	1,25	1,25	1,25
	Y	3,75	3,75	3,75	3,75
Контроль состояния окружающей среды	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Проверка влияния окружающей среды	*X*	5,00	5,00	5,00	5,00
	Y	5,00	5,00	5,00	5,00
Диагностический охват	*Z*	2,00	0,00	2,00	0,00
X (всего)		33,5	33,5	21	21
Y (всего)		25,5	25,5	23,5	23,5
Сумма баллов *S*		59	59	44,5	44,5
β		2 %	2 %	5 %	5 %
Сумма баллов S_D		126	59	86,5	44,5
β_D		0,5 %	2 %	1 %	5 %

Полезная информация, связанная с отказами по общей причине, содержится в [11] — [13].

Приложение Е
(справочное)

Применение таблиц полноты безопасности программного обеспечения в соответствии с МЭК 61508-3

Е.1 Общие положения

Настоящее приложение содержит два примера применения таблиц полноты безопасности программного обеспечения, определенных в МЭК 61508-3, приложение А.

Первый пример представляет собой программируемую электронную систему, связанную с безопасностью, с уровнем полноты безопасности 2, которая используется для управления процессом на химическом заводе. Данная программируемая электронная система использует в прикладной программе многоступенчатую логику и служит примером прикладного программирования на языке с ограниченной варьируемостью.

Второй пример представляет собой программное приложение, разработанное на языке программирования высокого уровня, связанное с безопасностью, с уровнем полноты безопасности 3, которое управляет закрывающим устройством.

Оба примера служат руководством по применению таблиц полноты безопасности программного обеспечения, определенных в МЭК 61508-3, для различных реальных систем. Все исходные характеристики конкретной системы, необходимые для использования упомянутых выше таблиц полноты безопасности, должны иметь документальное обоснование, подтверждающее, что все описания используемых характеристик правильны и соответствуют конкретной реализации этой системы.

Е.2 Система с уровнем полноты безопасности 2

Установка, работающая на химическом заводе, состоит из нескольких реакторных баков, связанных промежуточными баками хранения, которые на некоторых стадиях цикла реакции заполняются инертным газом для предотвращения воспламенения и взрывов. Функции программируемой электронной системы, связанной с безопасностью, помимо прочих включают в себя: получение входных данных от датчиков; включение и блокировку клапанов, насосов и исполнительных механизмов; обнаружение опасных ситуаций и включение сигнала тревоги; сопряжение с распределенной системой управления в соответствии с требованиями, предъявляемыми спецификацией безопасности.

Предположения и характеристики системы:

- контроллер программируемой электронной системы, связанной с безопасностью, представляет собой программируемый логический контроллер (ПЛК);
- при анализе опасностей и рисков установлено, что необходимо использовать программируемую электронную систему, связанную с безопасностью, и для данного приложения нужен уровень полноты безопасности 2 (в соответствии с МЭК 61508-1 и МЭК 61508-2);
- хотя контроллер работает в реальном времени, требуется относительно небольшая скорость реакции;
- существуют интерфейсы с оператором и распределенной системой управления;
- исходный код программного обеспечения системы и схема программируемых электронных средств ПЛК недоступны для проверки, но оценены в соответствии с МЭК 61508-3 как соответствующие уровню полноты безопасности 2;
- в качестве языка программирования приложения использовалась многоступенчатая логика, программа создавалась с помощью системы разработки, предоставляемой поставщиком ПЛК;
- код приложения должен исполняться только на ПЛК одного типа;
- вся разработка программного обеспечения контролировалась лицом, независимым от команды разработчиков программного обеспечения;
- лицо, независимое от команды разработчиков программного обеспечения, наблюдало за приемочными испытаниями и утвердило их результаты;
- изменения (если необходимы) санкционируются лицом, независимым от команды разработчиков программного обеспечения.

Примечание — Определение независимого лица — в соответствии с МЭК 61508-4, пункт 3.8.10.

Интерпретация МЭК 61508-3, приложение А, для данного примера представлена в таблицах Е.1 — Е.10.

Примечания

1 В графе «ссылка» таблиц Е.1 — Е.10 пункты (например В.2.4, С.3.1) — это ссылки на МЭК 61508-7, а таблицы (например таблица В.7) — это ссылки на МЭК 61508-3.

2 Информация о распределении ответственности между поставщиком и пользователем при использовании языков программирования с ограниченной варьируемостью приведена в МЭК 61508-3 (примечания к 7.4.3 — 7.4.5).

Таблица Е.1 — Спецификация требований к безопасности программного обеспечения (см. МЭК 61508-3, подраздел 7.2)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Автоматизированные средства спецификации	B.2.4	R	Используются средства разработки, поставленные производителем ПЛК
2a Полуформальные методы	Таблица B.7	R	Обычно используются причинно-следственные схемы, циклограммы и функциональные блоки для спецификации требований к программному обеспечению ПЛК
2b Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временну́ю логику, VDM и Z	C.2.4	R	Не используются для языков программирования с ограниченной варьируемостью
Примечание — Требования к безопасности программного обеспечения определены на естественном языке.			

Таблица Е.2 — Программное обеспечение, проектирование и разработка: архитектура (см. МЭК 61508-3, пункт 7.4.3)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Обнаружение и диагностика сбоев	C.3.1	R	Проверка диапазона данных, сторожевой таймер, ввод/вывод, средства связи. В случае ошибки поднимает тревогу (см. 3a)
2 Обнаружение и исправление ошибок	C.3.2	R	Встраивается с пользовательскими функциями: требуется тщательный выбор
3a Программирование с проверкой ошибок	C.3.3	R	Выделяет часть многоступенчатой логики ПЛК для проверки некоторых важных условий безопасности (см. 1)
3b Методы «подушки безопасности»	C.3.4	R	Проверяет разрешенные комбинации ввода/вывода на мониторе независимого компьютера, обеспечивающего безопасность
3c Многовариантное программирование	C.3.5	R	Требуется прикладной задачей (см. 3b)
3d Блоки восстановления	C.3.6	R	Встраивается с пользовательскими функциями: требуется тщательный выбор
3e Восстановление предыдущего состояния	C.3.7	R	Встраивается с пользовательскими функциями: требуется тщательный выбор
3f Прямое восстановление	C.3.8	R	Встраивается с пользовательскими функциями: требуется тщательный выбор
3g Повторный запуск механизмов восстановления после ошибок	C.3.9	R	Используется в соответствии с требованиями прикладной задачи (см. 2 и 3b)
3h Сохранение достигнутых состояний	C.3.10	R	Не используется для программирования с ограниченной варьируемостью
4 Постепенное отключение функций	C.3.11	R	Не используется для программирования с ограниченной варьируемостью
5 Исправление ошибок методами искусственного интеллекта	C.3.12	NR	Не используется для программирования с ограниченной варьируемостью
6 Динамическая реконфигурация	C.3.13	NR	Не используется для программирования с ограниченной варьируемостью

Окончание таблицы Е.2

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
7a Структурные методы, включая, например JSD, MASCOT, SADT и Yourdon	С.2.1	HR	Методы потоков данных и логических таблиц данных могут использоваться, по крайней мере, для описания архитектуры
7b Полуформальные методы	Таблица В.7	R	Могут быть использованы для интерфейса DCS
7c Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временну́ю логику, VDM и Z	С.2.4	R	Редко используются для программирования с ограниченной варьируемостью
8 Автоматизированные средства разработки спецификаций	В.2.4	R	Используются средства разработки, поставленные производителем ПЛК
Примечание — Некоторые из этих методов нецелесообразно использовать при программировании на языках с ограниченной варьируемостью.			

Таблица Е.3 — Проектирование и разработка программного обеспечения: средства поддержки и язык программирования (см. МЭК 61508-3, пункт 7.4.4)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Выбор соответствующего языка программирования	С.4.6	HR	Обычно используется многоступенчатая логика и часто используются фирменные языки поставщика ПЛК
2 Строго типизированные языки программирования	С.4.1	HR	Используется структурированный текст по МЭК 61131-3 [14]
3 Подмножество языка	С.4.2	—	Остерегайтесь использования сложных «макроинструкций», прерываний, которые изменяют цикл сканирования ПЛК, и т. д.
4a Сертифицированные средства	С.4.3	HR	Поставляется производителем ПЛК
4b Инструментальные средства: заслуживающие доверия на основании опыта использования	С.4.4	HR	Используются средства разработки, предлагаемые поставщиком ПЛК, а также собственные инструменты, разработанные в ходе работы над несколькими проектами
5a Сертифицированный транслятор	С.4.3	HR	Поставляется производителем ПЛК
5b Трансляторы, заслуживающие доверия на основании опыта использования	С.4.4	HR	Не используется для языков программирования с ограниченной варьируемостью
6 Библиотека проверенных/сертифицированных модулей и компонентов	С.4.5	HR	Функциональные блоки, части программы

Таблица Е.4 — Проектирование и разработка программного обеспечения: подробная модель (см. МЭК 61508-3, пункты 7.4.5 и 7.4.6)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1a Структурные методы, включая, например JSD, MASCOT, SADT и Yourdon	С.2.1	HR	Не используется для языков программирования с ограниченной варьируемостью
1b Полуформальные методы	Таблица В.7	HR	Используются причинно-следственные схемы, циклограммы, функциональные блоки, типичные для языков программирования с ограниченной варьируемостью
1c Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временну́ю логику, VDM и Z	С.2.4	R	Не используется для языков программирования с ограниченной варьируемостью

Окончание таблицы Е.4

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
2 Средства автоматизированного проектирования	В.3.5	R	Используются средства разработки, поставленные производителем ПЛК
3 Программирование с защитой	С.2.5	R	Включается в программное обеспечение системы
4 Модульный подход	Таблица В.9	HR	Используется упорядочение и группировка многоступенчатой логики программы ПЛК для максимального увеличения модульности требуемых функций
5 Стандарты (предприятий) проектирования и кодирования	Таблица В.1	HR	Используются собственные соглашения для документации и удобства эксплуатации
6 Структурное программирование	С.2.7	HR	Для рассматриваемого примера аналогично модульности
7 Библиотека проверенных/сертифицированных модулей и компонентов (если возможно)	С.4.5	HR	Используются
Примечание — Проектирование и разработка включают в себя системное проектирование программного обеспечения, проектирование и кодирование программных модулей.			

Таблица Е.5 — Проектирование и разработка программного обеспечения: проверка и интеграция программных модулей (см. МЭК 61508-3, пункты 7.4.7 и 7.4.8)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Вероятностное тестирование	С.5.1	R	Не используется для языков программирования с ограниченной варьируемостью
2 Динамический анализ и тестирование	В.6.5, таблица В.2	R	Используются
3 Регистрация и анализ данных	С.5.2	HR	Запись исходных данных и результатов тестирования
4 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных
5 Моделирование производительности	С.5.20, таблица В.6	HR	Не используется для языков программирования с ограниченной варьируемостью
6 Тестирование интерфейса	С.5.3	R	Включено в функциональное тестирование и тестирование методом черного ящика

Таблица Е.6 — Интеграция программируемых электронных средств (аппаратура и программное обеспечение) (см. МЭК 61508-3, подраздел 7.5)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных
2 Моделирование производительности	С.5.20, таблица В.6	R	Если система ПЛК собирается для заводских приемочных испытаний

Таблица Е.7 — Безопасность программного обеспечения, проверка (см. МЭК 61508-3, подраздел 7.7)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Вероятностное тестирование	С.5.1	R	Не используется для языков программирования с ограниченной варьируемостью
2 Имитация/моделирование	Таблица В.5	R	Не используется для языков программирования с ограниченной варьируемостью, но все чаще используется при разработке систем ПЛК
3 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, анализ граничных значений и декомпозиция входных данных

Таблица Е.8 — Модификация программного обеспечения (см. МЭК 61508-3, подраздел 7.8)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Анализ влияния	С.5.23	HR	Выполняют анализ последствий для изучения того, насколько влияние предлагаемых изменений ограничено модульной структурой всей системы
2 Повторная верификация измененных программных модулей	С.5.23	HR	Повторение предыдущих тестов
3 Повторная верификация программных модулей, на которые оказывают влияние изменения в других модулях	С.5.23	HR	Повторение предыдущих тестов
4 Повторное подтверждение соответствия системы	С.5.23	R	Если анализ последствий показал необходимость модификации системы, то после выполнения ее модификации обязательно проводится повторное подтверждение соответствия системы
5 Управление конфигурацией программного обеспечения	С.5.24	HR	Поддерживает базовую конфигурацию, изменения в ней, влияние на другие системные требования
6 Регистрация и анализ данных	С.5.2	HR	Выполняется запись исходных данных и результатов тестирования

Таблица Е.9 — Проверка программного обеспечения (см. МЭК 61508-3, подраздел 7.9)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Формальное доказательство	С.5.13	R	Не используется для языков программирования с ограниченной варьируемостью
2 Вероятностное тестирование	С.5.1	R	Заменяется опытом эксплуатации существующих компонентов
3 Статический анализ	В.6.4, таблица В.8	HR	Выполняют анализ перекрестных ссылок использования переменных, условий и т. д.
4 Динамический анализ и тестирование	В.6.5, таблица В.2	HR	Используются автоматические средства тестирования для облегчения регрессивного тестирования

Окончание таблицы 9

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
5 Метрики сложности программного обеспечения	С.5.14	R	Не используется для языков программирования с ограниченной варьируемостью
Тестирование и интеграция программных модулей	См. таблицу Е.5		
Тестирование интеграции программируемой электроники	См. таблицу Е.6		
Тестирование (приемочные испытания) программной системы	См. таблицу Е.7		

Таблица Е.10 — Оценка функциональной безопасности (см. МЭК 61508-3, раздел 8)

Метод/средство	Ссылка	SIL2	Интерпретация (в настоящем приложении)
1 Таблица контрольных проверок	В.2.5	R	Используется
2 Таблицы решений и таблицы истинности	С.6.1	R	Используется ограниченно
3 Метрики сложности программного обеспечения	С.5.14	R	Не используется для языков программирования с ограниченной варьируемостью
4 Анализ отказов	Таблица В.4	R	На системном уровне анализ отказов использует причинно-следственные схемы, но для языков программирования с ограниченной варьируемостью этот метод не используется
5 Анализ отказов по общей причине разнообразного программного обеспечения (если оно действительно используется)	С.6.3	R	Не используется для языков программирования с ограниченной варьируемостью
6 Блок-схемы надежности	С.6.5	R	Не используется для языков программирования с ограниченной варьируемостью

Е.3 Система с уровнем полноты безопасности 3

Рассматриваемая программная система сравнительно велика с точки зрения системы безопасности, так как включает более 30000 строк исходного кода. Кроме того, в ней используются обычные встроенные функции, по крайней мере, две различные операционные системы и уже существующий код более ранних проектов (проверенных в эксплуатации). В целом система состоит более чем из 100000 строк исходного кода.

Аппаратные средства (включая датчики и исполнительные механизмы) представляют собой двухканальную систему, выходы которой подключены к оконечным элементам по схеме логического «И» (AND).

Предположения и характеристики системы:

- немедленная реакция не требуется, но обеспечивается максимальное время реакции;
- интерфейсы с оператором существуют для датчиков, исполнительных механизмов и оповещателей;
- исходный код операционных систем, графических процедур и коммерческих программных продуктов не доступен;
- система, скорее всего, в дальнейшем будет модернизироваться;
- специально разработанное программное обеспечение использует один из распространенных процедурных языков;
- компоненты программной системы, исходный код для которых недоступен, реализованы разными способами с помощью инструментальных средств от разных поставщиков, и их объектный код был создан разными трансляторами;
- программное обеспечение работает на нескольких процессорах, доступных на рынке в соответствии с требованиями МЭК 61508-2;
- встроенные системы соответствуют требованиям МЭК 61508-2 для управления отказами аппаратных средств и для их предотвращения;
- разработка программного обеспечения контролировалась независимой организацией.

Примечание — Определение независимой организации приведено в МЭК 61508-4, пункт 3.8.12.

Интерпретация МЭК 61508-3, приложение А, для данного примера представлена в таблицах Е.11 — Е.20.

Примечание — В графе «ссылка» таблиц Е.11 — Е.30 пункты (например В.2.4, С.3.1) — это ссылки на МЭК 61508-7, а таблицы (например таблица В.7) — это ссылки на МЭК 61508-3.

Таблица Е.11 — Спецификация требований к безопасности программного обеспечения (см. МЭК 61508-3, подраздел 7.2)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Автоматизированные средства разработки спецификации	B.2.4	HR	Используются средства, поддерживающие выбранные методы
2a Полуформальные методы	Таблица B.7	HR	Используются блок-схемы, циклограммы, диаграммы переходов состояний
2b Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временну́ю логику, VDM и Z	C.2.4	R	Используются только в исключительном случае

Таблица Е.12 — Проектирование и разработка программного обеспечения: проектирование архитектуры программного обеспечения (см. МЭК 61508-3, пункт 7.4.3)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Обнаружение и диагностика сбоев	C.3.1	HR	Используется для тех отказов датчиков, исполнительных механизмов и средств передачи данных, которые не охватываются средствами встроенной системы в соответствии с МЭК 61508-2
2 Обнаружение и исправление ошибок	C.3.2	R	Используется только для внешней передачи данных
3a Программирование с проверкой ошибок	C.3.3	R	Используется для проверки правильности результатов прикладных функций
3b Методы «подушки безопасности»	C.3.4	R	Используются для некоторых функций, связанных с безопасностью, если отсутствуют средства 3a и 3c
3c Многовариантное программирование	C.3.5	R	Используется для некоторых функций, исходный код которых недоступен
3d Блоки восстановления	C.3.6	R	Не используется
3e Восстановление предыдущего состояния	C.3.7	R	Не используется
3f Прямое восстановление	C.3.8	R	Не используется
3g Повторный запуск механизмов восстановления после ошибок	C.3.9	R	Не используется
3h Сохранение достигнутых состояний	C.3.10	R	Не используется (достаточно средств 3a, 3b и 3c)
4 Постепенное отключение функций	C.3.11	HR	Используется вследствие природы технического процесса
5 Исправление ошибок методами искусственного интеллекта	C.3.12	NR	Не используется
6 Динамическая реконфигурация	C.3.13	NR	Не используется
7a Структурные методы, включая, например JSD, MASCOT, SADT и Yourdon	C.2.1	HR	Необходимо использовать вследствие размера системы
7b Полуформальные методы	Таблица B.7	HR	Используются блок-схемы, циклограммы, диаграммы перехода состояний
7c Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временную логику, VDM и Z	C.2.4	R	Не используются
8 Автоматизированные средства разработки спецификаций	B.2.4	HR	Используются средства, поддерживающие выбранные методы

Таблица Е.13 — Проектирование и разработка программного обеспечения: средства поддержки и язык программирования (см. МЭК 61508-3, пункт 7.4.4)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Выбор соответствующего языка программирования	С.4.6	HR	Выбирается язык высокого уровня с полной варьируемостью
2 Строго типизированные языки программирования	С.4.1	HR	Используют
3 Подмножество языка	С.4.2	HR	Определяют подмножество выбранного языка
4a Сертифицированные средства	С.4.3	HR	Недоступны
4b Инструментальные средства: заслуживающие доверия на основании опыта использования	С.4.4	HR	Доступны и используют
5a Сертифицированный компилятор	С.4.3	HR	Недоступен
5b Трансляторы, заслуживающие доверия на основании опыта использования	С.4.4	HR	Доступны и используют
6 Библиотека проверенных/сертифицированных модулей и компонент	С.4.5	HR	Доступна и используют

Таблица Е.14 — Проектирование и разработка программного обеспечения: подробный проект (см. МЭК 61508-3, пункты 7.4.5 и 7.4.6)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1a Структурные методы, включая, например JSD, MASCOT, SADT и Yourdon	С.2.1	HR	Широко используются. В частности SADT и JSD
1b Полуформальные методы	Таблица В.7	HR	Используются конечные автоматы/диаграммы перехода состояний, блок-схемы, циклограммы
1c Формальные методы, включая, например CCS, CSP, HOL, LOTOS, OBJ, временну́ю логику, VDM и Z	С.2.4	R	Используются только в исключительных случаях для некоторых очень важных компонент
2 Средства автоматизированого проектирования	В.3.5	R	Используются для выбранных методов
3 Программирование с защитой	С.2.5	R	В прикладном программном обеспечении в явном виде используются средства, которые могут быть эффективны, кроме автоматически вставляемых компилятором
4 Модульный подход	Таблица В.9	HR	Используются: ограниченный размер программного модуля, скрытие информации/инкапсуляция, одна входная/выходная точка в подпрограммах и функциях, полностью определенный интерфейс и т. д.
5 Стандарты (предприятия) проектирования и кодирования	Таблица В.1	HR	Используются стандарты (предприятия) для кодирования, ограниченно используются прерывания, указатели и рекурсии, не используются динамические объекты и переменные, безусловные переходы и т. д.
6 Структурное программирование	С.2.7	HR	Используют
7 Библиотека проверенных/сертифицированных модулей и компонентов (по возможности)	С.4.5	HR	Доступен и используют
Примечание — Проектирование и разработка включают в себя системное проектирование программного обеспечения, проектирование и кодирование программных модулей.			

Таблица Е.15 — Проектирование и разработка программного обеспечения: проверка и интеграция программных модулей (см. МЭК 61508-3, пункты 7.4.7 и 7.4.8)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Вероятностное тестирование	С.5.1	R	Используется для программных модулей, исходный код которых недоступен, а определение граничных значений и классов эквивалентности для тестовых данных затруднено
2 Динамический анализ и тестирование	В.6.5, таблица В.2	HR	Используются для программных модулей, исходный код которых доступен. Выполняют: контрольные примеры, разработанные с помощью анализа граничных значений, моделирование производительности, разделение входных данных на классы эквивалентности, структурное тестирование
3 Регистрация и анализ данных	С.5.2	HR	Используют запись входных данных и результатов тестирования
4 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Используют для программных модулей, исходный код которых недоступен, и для проверки интеграции. Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, прототипирование, анализ граничных значений, разделение данных на классы эквивалентности и декомпозиция входных данных
5 Моделирование производительности	С.5.20, таблица В.6	HR	Используют при проверке интеграции на конкретном оборудовании
6 Тестирование интерфейса	С.5.3	HR	Не используют

Таблица Е.16 — Интеграция программируемой электроники (аппаратных средств и программного обеспечения) (см. МЭК 61508-3, подраздел 7.5)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Используют как дополнительные тесты при интеграции программного обеспечения (см. таблицу Е.15). Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, прототипирование, анализ граничных значений, разделение данных на классы эквивалентности и декомпозиция входных данных
2 Моделирование производительности	С.5.20, таблица В.6	HR	Широко используют

Таблица Е.17 — Подтверждение соответствия безопасности программного обеспечения (см. МЭК 61508-3, подраздел 7.7)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Вероятностное тестирование	С.5.1	R	Не используют для подтверждения соответствия
2 Имитация/моделирование	Таблица В.5	HR	Конечные автоматы, моделирование производительности, прототипирование и анимация
3 Функциональное тестирование и тестирование методом черного ящика	В.5.1, В.5.2, таблица В.3	HR	Выбираются входные данные для тестирования всех заданных функциональных блоков, включая обработку ошибок. Используются: тестовые примеры, полученные с помощью причинно-следственных схем, прототипирование, анализ граничных значений, разделение данных на классы эквивалентности и декомпозиция входных данных

Таблица Е.18 — Модификация программного обеспечения (см. МЭК 61508-3, подраздел 7.8)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Анализ влияния	С.5.23	HR	Используют
2 Повторная верификация измененных программных модулей	С.5.23	HR	Используют
3 Повторная верификация программных модулей, на которые оказывают влияние изменения в других модулях	С.5.23	HR	Используют
4 Повторная верификация системы в целом	С.5.23	HR	Использование зависит от результатов анализа последствий
5 Управление конфигурацией программного обеспечения	С.5.24	HR	Используют
6 Регистрация и анализ данных	С.5.2	HR	Используют

Таблица Е.19 — Проверка программного обеспечения (см. МЭК 61508-3, подраздел 7.9)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Формальное доказательство	С.5.13	R	Используется только в исключительных случаях, для некоторых очень важных классов
2 Вероятностное тестирование	С.5.1	R	Включено в таблицу Е.15
3 Статический анализ	В.6.4, таблица В.8	HR	Для всего вновь разработанного кода используются: анализ граничных значений, таблица контрольных проверок, анализ потоков управления, анализ потоков данных, проверка разработки программ, анализ проектов
4 Динамический анализ и тестирование	В.6.5, таблица В.2	HR	Включено в таблицу Е.15
5 Метрики сложности программного обеспечения	С.5.14	R	Используют в минимальной степени
Тестирование и интеграция программных модулей			См. таблицу Е.15
Тестирование интеграции программируемой электроники			См. таблицу Е.16
Тестирование (подтверждение соответствия) программной системы			См. таблицу Е.17

Таблица Е.20 — Оценка функциональной безопасности (МЭК 61508-3, раздел 8)

Метод/средство	Ссылка	SIL3	Интерпретация (в настоящем приложении)
1 Таблица контрольных проверок	B.2.5	R	Используют
2 Таблицы решений и таблицы истинности	C.6.1	R	Используют в ограниченной степени
3 Метрики сложности программного обеспечения	C.5.14	R	Используют в минимальной степени
4 Анализ отказов	Таблица B.4	R	Интенсивно используют анализ диагностического дерева отказов, а причинно-следственные диаграммы используют в ограниченной степени
5 Анализ отказов по общей причине разнообразного программного обеспечения (если действительно используется)	C.6.3	R	Используют
6 Блок диаграммы надежности	C.6.5	R	Используют

Приложение F
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица F.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта Российской Федерации
ИСО/МЭК 51:1999	ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты
МЭК 104:1997	*
ИСО/МЭК 2382-14:1998	*
МЭК 61508-1:1998	ГОСТ Р МЭК 61508-1—2006 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
МЭК 61508-2:2000	ГОСТ Р МЭК 61508-2—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
МЭК 61508-3:1998	ГОСТ Р МЭК 61508-3—2006 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—2006 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения
МЭК 61508-5:1998	ГОСТ Р МЭК 61508-5—2006 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
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

* 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 61078:2006	Analysis techniques for dependability — Reliability block diagram method
[3]	IEC 61165:2006	Application of Markov techniques
[4]	BS 5760	Reliability of system equipment and components — Part 2: Guide to assessment of reliability
[5]	D. J. Smith	Reliability, maintainability and risk — Practical methods for engineers, Butterworth-Heinemann, 5th edition, 1997, ISBN 0-7506-3752-8
[6]	R. Billington and R. N. Allan	Reliability evaluation of engineering systems. Plenum, 1992, ISBN 0-306-44063-6
[7]	W. M. Goble	Evaluating control system reliability — Techniques and applications, Instrument Society of America, 1992, ISBN 1-55617-128-5
[8]	*Reliability Analysis Center (RAC)*	Failure Mode/Mechanism Distributions, 1991, Department of Defense, United States of America, PO Box 4700, 201 Mill Street, Rome, NY 13440-8200, Organization report number: FMD-91, NSN 7540-01-280-5500
[9]		Qualität und Zuverlassigkeit technischer Systême, Théorie, Praxis, Management, Dritte Auflage, 1991, Allessandro Birolini, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed.
[10]	MIL-HDBK-217F	Military Handbook Reliability prediction of electronic equipment, 2 December 1991, Department of Defense, United States of America, Washington DC 20301
[11]		Programmable electronic systems in safety-related applications. Part 2: General technical guidelines. Health and Safety Executive, HMSO, ISBN 0 11 883906 3, 1987
[12]		Assigning a numerical value to the beta factor common-cause evaluation, Humphreys, R. A., Proc. Reliability '87
[13]		UPM3.1: *A pragmatic approach to dependent failures assessment for standard systems*, AEA Technology, Report SRDA-R-13, ISBN 085 356 4337, 1996
[14]	IEC 61131-3:2003	Programmable controllers — Part 3: Programming languages

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; диагностический охват; оценка вероятности отказа аппаратных средств; полнота безопасности программного обеспечения

Редактор *В. Н. Колысов*
Технический редактор *В. Н. Прусакова*
Корректор *М. С. Кабашова*
Компьютерная верстка *В. Н. Романовой*

Сдано в набор 02.07.2008. Подписано в печать 18.11.2008. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 7,90. Уч.-изд. л. 6,90. Тираж 253 экз. Зак. 1557

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru