ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-5— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 5

Разработка аппаратных средств изделия

ISO 26262-5:2011

Road vehicles — Functional safety — Part 5: Product development at the hardware level

(IDT)

Издание официальное

Москва
Стандартинформ
2015

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 17 ноября 2014 г. № 1623-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-5:2011 «Дорожные транспортные средства. Функциональная безопасность. Часть 5. Разработка аппаратных средств изделия» (ISO 26262-5:2011 «Road vehicles — Functional safety — Part 5: Product development at the hardware level»).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии по стандартизации в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2015

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 . . . 2
3 Термины, определения и сокращения . . . 2
4 Требования соответствия настоящему стандарту . . . 2
4.1 Общие требования . . . 2
4.2 Интерпретация таблиц . . . 3
4.3 Требования и рекомендации, зависимые от значения УПБА . . . 3
5 Начальная подстадия разработки аппаратных средств изделия . . . 3
5.1 Цель . . . 3
5.2 Общие положения . . . 3
5.3 Входная информация . . . 4
5.4 Требования и рекомендации . . . 4
5.5 Результаты работы . . . 5
6 Спецификация требований к аппаратным средствам системы безопасности . . . 5
6.1 Цели . . . 5
6.2 Общие положения . . . 5
6.3 Входная информация . . . 5
6.4 Требования и рекомендации . . . 5
6.5 Результаты работы . . . 7
7 Проектирование аппаратных средств . . . 7
7.1 Цели . . . 7
7.2 Общие положения . . . 7
7.3 Входная информация . . . 8
7.4 Требования и рекомендации . . . 8
7.5 Результаты работы . . . 12
8 Оценка метрик архитектуры аппаратных средств . . . 12
8.1 Цель . . . 12
8.2 Общие положения . . . 12
8.3 Входная информация . . . 13
8.4 Требования и рекомендации . . . 13
8.5 Результаты работы . . . 16
9 Оценка нарушений цели безопасности вследствии случайных отказов аппаратных средств . . . 16
9.1 Цель . . . 16
9.2 Общие положения . . . 16
9.3 Входная информация . . . 16
9.4 Требования и рекомендации . . . 17
9.5 Результаты работы . . . 23
10 Интеграция и тестирование аппаратных средств . . . 23
10.1 Цель . . . 23
10.2 Общие положения . . . 23

10.3 Входная информация 24
10.4 Требования и рекомендации 24
10.5 Результаты работы 26
Приложение А (справочное) Обзор и поток документов стадии разработки аппаратных средств изделия 27
Приложение В (справочное) Классификация видов отказов элементов аппаратных средств 29
Приложение С (обязательное) Метрики архитектуры аппаратных средств 31
Приложение D (справочное) Оценка охвата диагностикой 35
Приложение Е (справочное) Пример вычисления метрик архитектуры аппаратных средств: метрики одиночного сбоя и метрики скрытого сбоя 60
Приложение F (справочное) Применение коэффициентов масштабирования 69
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 71
Библиография 72

Введение

Комплекс стандартов ИСО 26262 является адаптацией комплекса стандартов МЭК 61508 и предназначен для применения электрических и/или электронных (Э/Э) систем в дорожно-транспортных средствах.

Это адаптация распространяется на все виды деятельности в процессе жизненного цикла систем, связанных с безопасностью, включающих электрические, электронные и программные компоненты.

Безопасность является одним из важнейших вопросов в автомобилестроении. Создание новых функциональных возможностей не только в таких системах, как содействие водителю, силовые установки, управление динамикой автомобиля, но и в активных и пассивных системах безопасности тесно связано с деятельностью по проектированию систем безопасности. Разработка и интеграция этих функциональных возможностей повышает необходимость использования процессов разработки систем безопасности и обеспечения доказательств того, что все обоснованные цели системы безопасности выполнены.

С ростом сложности технологий, программного обеспечения и мехатронных устройств увеличиваются риски, связанные с систематическими отказами и случайными отказами оборудования. Чтобы предотвратить эти риски, комплекс стандартов ИСО 26262 включает соответствующие требования и процессы.

Безопасность системы достигается за счет ряда мер безопасности, которые реализуются с применением различных технологий (например, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных) и применяются на различных уровнях процесса разработки. Несмотря на то, что настоящий стандарт касается функциональной безопасности Э/Э систем, подход, рассматриваемый в настоящем стандарте, может быть использован для разработки связанных с безопасностью систем, основанных на других технологиях. Настоящий стандарт:

a) обеспечивает жизненный цикл систем безопасности автомобиля (менеджмент, разработку, производство, эксплуатацию, обслуживание, вывод из эксплуатации) и поддерживает адаптацию необходимых действий для выполнения этих стадий жизненного цикла;

b) обеспечивает разработанный специально для автотранспорта основанный на риске подход для определения уровней полноты безопасности [уровни полноты безопасности автомобиля (УПБА)];

c) использует значения УПБА при спецификации соответствующих требований, чтобы предотвратить неоправданный остаточный риск;

d) устанавливает требования к мерам проверки соответствия и подтверждения, которые обеспечивают достижение достаточного и приемлемого уровня безопасности;

e) устанавливает требования к взаимодействию с поставщиками.

На функциональную безопасность влияют процессы разработки (в том числе спецификация требований, реализация, внедрение, интеграция, верификация, подтверждение соответствия и управление конфигурацией), процессы производства и обслуживания, а также процессы управления.

Вопросы безопасности тесно связаны с любыми опытно-конструкторскими работами, реализующими функционал и обеспечивающими качество создаваемых изделий, а также с результатами таких работ. Настоящий стандарт рассматривает связанные с безопасностью проблемы, касающиеся опытно-конструкторских работ и их результатов.

На рисунке 1 показана общая структура комплекса ИСО 26262. В нем для различных стадий разработки изделия используется эталонная V-модель процесса. На рисунке 1:

- залитая область в виде символа «V» представляет взаимосвязь между ИСО 26262-3, ИСО 26262-4, ИСО 26262-5, ИСО 26262-6 и ИСО 26262-7;
- ссылки на конкретную информацию даны в виде: «m-n», где «m» представляет собой номер части настоящего стандарта, а «n» указывает на номер раздела этой части.

Пример — 2-6 ссылается на пункт 6 ИСО 26262-2.

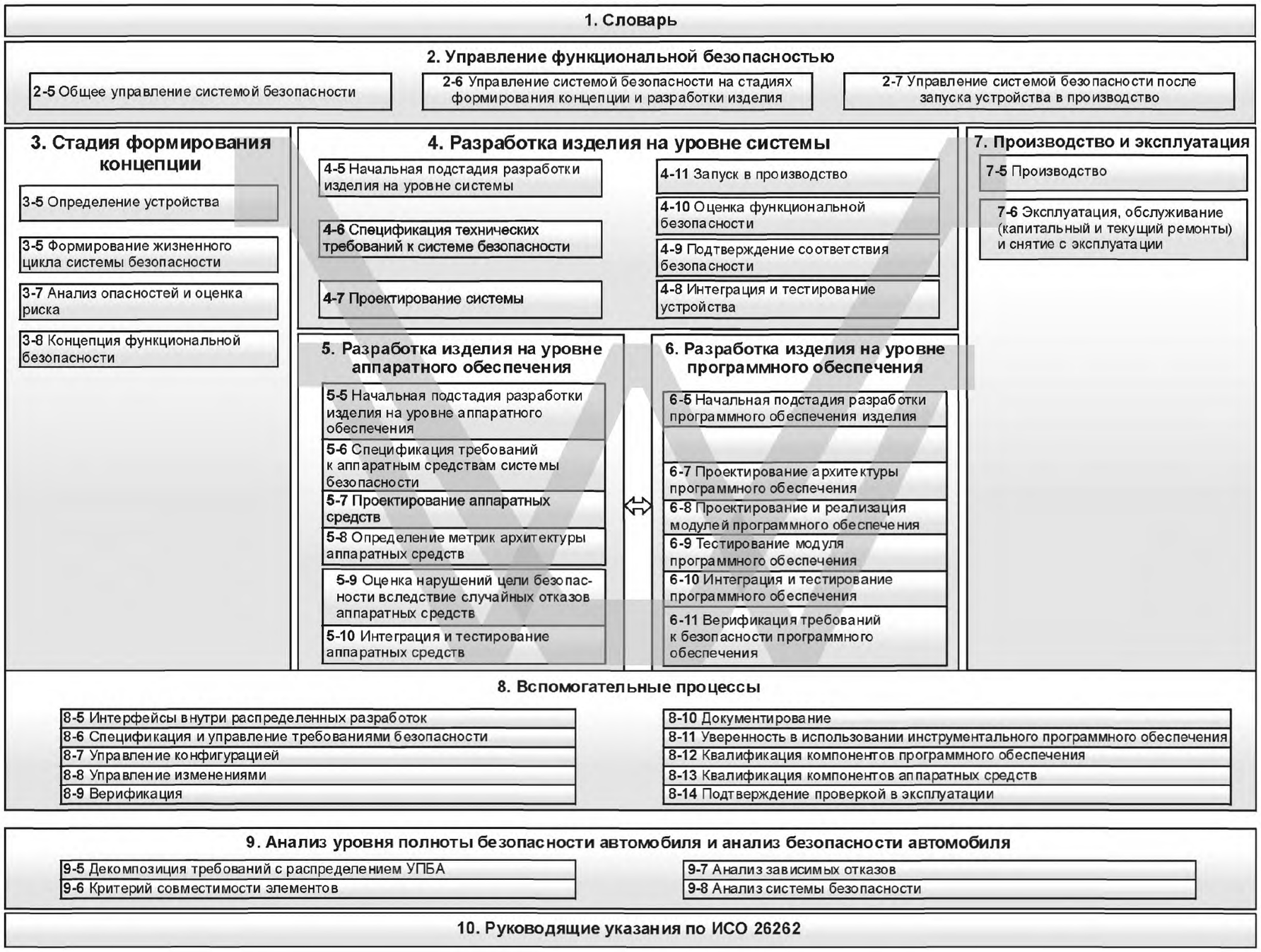


Рисунок 1 — Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 5

Разработка аппаратных средств изделия

Road vehicles. Functional safety. Part 5. Product development at the hardware level

Дата введения — 2015—10—01

1 Область применения

Настоящий стандарт применяется к связанным с безопасностью системам, включающим в себя одну или несколько электрических и/или электронных (Э/Э) систем, которые установлены в серийно производимых легковых автомобилях с максимальной массой (брутто) транспортного средства до 3500 кг. Настоящий стандарт не применяется для уникальных Э/Э систем в транспортных средствах специального назначения, таких как транспортные средства, предназначенные для водителей с ограниченными возможностями.

Системы и их компоненты, находящиеся в производстве или на стадии разработки до даты публикации настоящего стандарта, не входят в его область применения. Если разрабатываемые автомобили или их модификации используют системы и их компоненты, выпущенные до публикации настоящего стандарта, то только модификации этих систем должны быть разработаны в соответствии с настоящим стандартом.

Настоящий стандарт рассматривает возможные опасности, вызванные некорректным поведением Э/Э связанных с безопасностью систем, а также некорректным взаимодействием этих систем. Настоящий стандарт не рассматривает опасности, связанные с поражением электрическим током, возгоранием, задымлением, перегревом, излучением, токсичностью, воспламеняемостью, химической активностью, коррозией и подобные опасности, если они непосредственно не вызваны некорректным поведением Э/Э связанных с безопасностью систем.

Настоящий стандарт не рассматривает номинальные рабочие характеристики Э/Э систем, даже если для таких систем существуют стандарты, посвященные их функциональным рабочим характеристикам (например, активные и пассивные системы безопасности, тормозные системы, адаптивный круиз-контроль).

Настоящий стандарт устанавливает требования к разработке изделия на уровне аппаратных средств для автомобильной промышленности, в том числе:

- требования для инициализации разработки изделия на уровне аппаратных средств,
- спецификацию требований к безопасности аппаратных средств,
- требования к проектированию аппаратных средств,
- метрики архитектуры аппаратных средств,
- требования к оценке нарушения цели безопасности из-за случайных отказов аппаратных средств, а также интеграции и тестирования аппаратных средств.

Требования настоящего стандарта для элементов аппаратных средств применимы как к непрограммируемым, так и к программируемым элементам, таким как ASIC, FPGA и PLD. Кроме того, для программируемых электронных элементов, применимы требования ИСО 26262-6, а также разделов 11 и 12 ИСО 26262-8:2011.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО 26262-1:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 1. Термины и определения (ISO 26262-2:2011, Road vehicles — Functional safety — Part 1: Vocabulary)

ИСО 26262-2:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 2. Управление функциональной безопасностью (ISO 26262-2:2011, Road vehicles — Functional safety — Part 2: Management of functional safety)

ИСО 26262-3:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 3. Стадия формирования концепции (ISO 26262-3:2011, Road vehicles — Functional safety — Part 3: Concept phase)

ИСО 26262-4:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 4. Разработка изделия на уровне системы (ISO 26262-4:2011, Road vehicles — Functional safety — Part 4: Product development at the system level)

ИСО 26262-6:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 6. Разработка программного обеспечения изделия (ISO 26262-6:2011, Road vehicles — Functional safety — Part 6: Product development at the software level)

ИСО 26262-7:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 7. Производство и эксплуатация (ISO 26262-7:2011, Road vehicles — Functional safety — Part 7: Production and operation)

ИСО 26262-8:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 8. Вспомогательные процессы (ISO 26262-8:2011, Road vehicles — Functional safety — Part 8: Supporting processes)

ИСО 26262-9:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 9. Анализ уровня полноты безопасности автомобиля и анализ безопасности автомобиля (ISO 26262-9:2011, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses)

3 Термины, определения и сокращения

В настоящем стандарте применены термины, определения и сокращения по ИСО 26262-1.

4 Требования соответствия настоящему стандарту

4.1 Общие требования

Для соответствия настоящему стандарту должно быть выполнено каждое его требование, если для этого требования не выполняется одно из следующих условий:

a) в соответствии с настоящим стандартом предусмотрена настройка действий по обеспечению безопасности, поэтому данное требование не применяется, или

b) существует обоснование того, что несоблюдение данного требования допустимо, а также показано соответствие этого обоснования настоящему стандарту.

Информация, обозначенная как «примечание» или «пример», должна использоваться только для понимания или для уточнения соответствующего требования, и не должна толковаться как самостоятельное требование или быть для него полной или исчерпывающей.

Результаты действий по обеспечению безопасности представлены как результаты работы. В пунктах «Предварительные требования» перечисляется информация, которая должна быть доступна как результат работы предыдущей стадии. Так как некоторые требования разделов настоящего стандарта зависят от УПБА или могут быть адаптированы, то некоторые результаты работы в качестве предварительных условий могут не понадобиться.

В пунктах «Дополнительная информация» содержится информация, которую можно учитывать, но которой в некоторых случаях настоящий стандарт не требует, чтобы она была результатом работы предыдущей стадии. Такая информация может быть доступна из внешних источников, от лиц или организаций, которые не несут ответственность за деятельность по обеспечению функциональной безопасности.

4.2 Интерпретация таблиц

В настоящем стандарте используются нормативные или справочные таблицы в зависимости от их контекста. Перечисленные в таблице различные методы вносят вклад в уровень уверенности в достижении соответствия с рассматриваемым требованием. Каждый метод в таблице включен либо в

a) последовательный список методов (он обозначен порядковым номером в левой колонке, например, 1, 2, 3) или

b) альтернативный список методов (он обозначен номером с последующей буквой в левом столбце, например, 2a, 2в, 2c).

В случае последовательного списка должны применяться все методы согласно рекомендациям для соответствующего значения УПБА. Если будут применяться другие методы, отличные от перечисленных, то должно быть дано обоснование, что они удовлетворяют соответствующим требованиям.

В случае альтернативного списка должна применяться подходящая комбинация методов в соответствии с указанным значением УПБА независимо от того, перечислены в таблице эти комбинации или нет. Если перечисленные методы имеют разные степени рекомендуемости их применения для некоторого значения УПБА, то следует отдать предпочтение методам с более высокой степенью рекомендуемости. Должно быть дано обоснование, что выбранная комбинация методов выполняет соответствующее требование.

Примечание — Обоснование, основанное на методах, перечисленных в таблице, является достаточным. Но это не означает, что существует какое-то предубеждение за или против применения методов, не перечисленных в таблице.

Для каждого метода степень рекомендуемости его применения зависит от значения УПБА и классифицируется следующим образом:

- «+ +» означает, что метод очень рекомендуется для определенного значения УПБА;
- «+» означает, что метод рекомендуется для определенного значения УПБА;
- «О» означает, что метод не имеет рекомендации за или против его применения для определенного значения УПБА.

4.3 Требования и рекомендации, зависимые от значения УПБА

Требования или рекомендации каждого подраздела должны соблюдаться для значений УПБА A, B, C и D, если не указано иное. Эти требования и рекомендации связаны со значениями УПБА цели безопасности. Если в соответствии с требованиями раздела 5 ИСО 26262-9 декомпозиция УПБА была выполнена на более ранней стадии разработки, то значения УПБА, полученные в результате декомпозиции, должны соблюдаться.

Если в настоящем стандарте значение УПБА дается в круглых скобках, то соответствующий подпункт должен рассматриваться как рекомендация, а не требование для этого значения УПБА. Это не относится к круглым скобкам в нотации, связанной с декомпозицией УПБА.

5 Начальная подстадия разработки аппаратных средств изделия

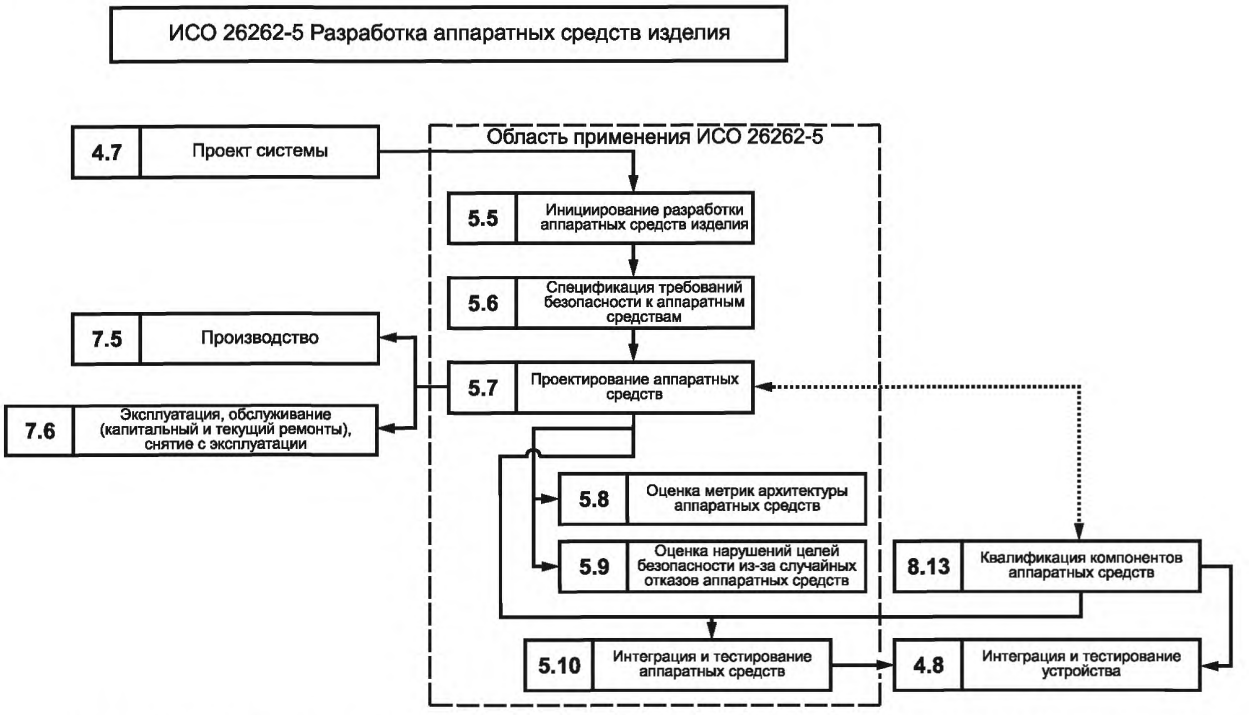
5.1 Цель

Цель начальной подстадии разработки аппаратных средств изделия заключается в определении и планировании действий по обеспечению функциональной безопасности для отдельных подстадий разработки аппаратных средств. Включены также необходимые вспомогательные процессы, описанные в ИСО 26262-8.

Эти спланированные действия по обеспечению безопасности конкретных аппаратных средств будут включены в план по обеспечению безопасности (см. пункт 6.4.3 ИСО 26262-2 и подраздел 5.4 ИСО 26262-4).

5.2 Общие положения

Следует спланировать действия и процессы, необходимые для разработки аппаратных средств, удовлетворяющих требованиям безопасности. Рисунок 2 иллюстрирует шаги процесса разработки аппаратных средств изделия, необходимые для выполнения требований настоящего стандарта, а также интеграцию этих шагов в контексте настоящего стандарта.



Примечание — На рисунке конкретный раздел каждой части настоящего стандарта указан следующим образом: «m-n», где «m» представляет собой номер части и «n» указывает номер раздела, например, «4-7» представляет раздел 7 ИСО 26262-4.

Рисунок 2 — Эталонная модель стадии разработки аппаратных средств изделия

Для разработки аппаратных средств изделия необходимы следующие действия и процессы:

- реализация технической концепции обеспечения безопасности аппаратных средств;
- анализ возможных сбоев аппаратных средств и их последствий; а также
- координация с разработкой программного обеспечения.

В отличие от подстадий разработки программного обеспечения, настоящий стандарт содержит два раздела, описывающие количественные оценки общей архитектуры аппаратных средств устройства.

В разделе 8 описаны две метрики для оценки эффективности архитектуры аппаратных средств устройства и реализованные механизмы безопасности, обрабатывающие случайными отказами аппаратных средств.

В качестве дополнения к разделу 8 в разделе 9 описываются два альтернативных варианта оценки с помощью глобального вероятностного подхода и с помощью анализа сечений того, является ли достаточно низким остаточный риск нарушения цели безопасности, для определения влияния каждого выявленного сбоя элемента аппаратных средств, нарушающего цели безопасности.

5.3 Входная информация

5.3.1 Предварительные требования

Необходима следующая информация:

- план проекта (уточненный) в соответствии с пунктом 5.5.1 ИСО 26262-4;
- план по обеспечению безопасности (уточненный) в соответствии с пунктом 5.5.2 ИСО 26262-4;
- план интеграции и тестирования устройства (уточненный) в соответствии с пунктом 5.5.3 ИСО 26262-4.

5.3.2 Дополнительная информация

Следующая информация может быть учтена:

- отчет о квалификации (компонентов или частей аппаратных средств).

5.4 Требования и рекомендации

5.4.1 План обеспечения безопасности в соответствии с ИСО 26262-2 должен быть достаточно подробным, включая определение соответствующих методов и мер, относящихся к действиям по разработке аппаратных средств изделия, согласованным с планируемыми действиями в ИСО 26262-6.

5.4.2 Процесс разработки аппаратных средств для устройства, включая методы и инструменты, должен быть согласован со всеми подстадиями разработки аппаратных средств и согласован с подстадиями разработки системы и программного обеспечения так, чтобы требования в реализуемой последовательности подстадий сохраняли свою точность и согласованность в процессе разработки аппаратных средств.

5.4.3 Должна быть выполнена настройка действий жизненного цикла системы безопасности для разработки аппаратных средств изделия в соответствии с требованиями пункта 6.4.5 ИСО 26262-2 на основе эталонной модели стадии, приведенной на рисунке 2.

5.4.4 Должно быть определено повторное использование компонентов аппаратных средств или использование квалифицированных компонентов или частей аппаратных средств, а результаты настройки действий по обеспечению безопасности должны быть документально оформлены.

5.5 Результаты работы

5.5.1 План по обеспечению безопасности (уточненный)

В результате выполнения требований 5.4.1—5.4.4.

6 Спецификация требований к аппаратным средствам системы безопасности

6.1 Цели

Первой целью настоящего раздела является формирование спецификации требований к аппаратным средствам системы безопасности. Они выводятся из технической концепции обеспечения безопасности и спецификации проекта системы.

Второй целью является верификация согласованности требований к аппаратным средствам системы безопасности с технической концепцией обеспечения безопасности и спецификацией проекта системы.

Третьей целью настоящего раздела является формирование подробной спецификации программно-аппаратного интерфейса, инициированного в разделе 7 ИСО 26262-4.

6.2 Общие положения

Технические требования к системе безопасности распределяются для аппаратных средств и программного обеспечения. Из требований, которые распределяются и для аппаратных средств, и для программного обеспечения, далее выделяются только требования для аппаратных средств системы безопасности. Затем требования к аппаратным средствам системы безопасности детализируются, с учетом ограничений проекта и влияния этих ограничений проекта на аппаратные средства.

6.3 Входная информация

6.3.1 Предварительные требования

Необходима следующая информация:

- план по обеспечению безопасности (уточненный) в соответствии с 5.5;
- техническая концепция обеспечения безопасности в соответствии с пунктом 7.5.1 ИСО 26262-4;
- спецификация проекта системы в соответствии с пунктом 7.5.2 ИСО 26262-4;
- спецификация программно-технического интерфейса в соответствии с пунктом 7.5.3 ИСО 26262-4.

6.3.2 Дополнительная информация

Следующая информация может быть учтена:

- спецификация требований к программному обеспечению системы безопасности (см. пункт 6.5.1 ИСО 26262-6).

6.4 Требования и рекомендации

6.4.1 Спецификация требований к аппаратным средствам системы безопасности для элементов аппаратных средств устройства должна быть получена из технических требований к системе безопасности, распределенных для аппаратных средств.

6.4.2 Спецификация требований к аппаратным средствам системы безопасности должна включать каждое требование к аппаратным средствам, связанное с безопасностью, в том числе:

Примечание — Требования к аппаратным средствам системы безопасности, описанные в перечислениях a), b), c), d) включают атрибуты, необходимые для обеспечения эффективности вышеупомянутых механизмов безопасности.

a) требования к аппаратным средствам системы безопасности и соответствующие атрибуты механизмов безопасности для управления внутренними отказами элементов аппаратных средств, включая внутренние механизмы безопасности для охвата кратковременных сбоев, когда показано, что они связаны, например, с используемой технологией.

Пример — Атрибуты могут идентифицировать возможности синхронизации и обнаружения для сторожевого устройства;

b) требования к аппаратным средствам системы безопасности и соответствующие атрибуты механизмов безопасности, обеспечивающие для элемента устойчивость к внешним по отношению к этому элементу сбоям.

Пример — Функциональное поведение, требуемое для электронного блока управления, в случае внешнего отказа, такого как разрыв цепи на входе электронного блока управления;

c) требования к аппаратным средствам системы безопасности и необходимые атрибуты механизмов безопасности, соответствующие требованиям к безопасности других элементов.

Пример — Диагностика датчиков или исполнительных механизмов;

d) требования к аппаратным средствам системы безопасности и соответствующие атрибуты механизмов безопасности, обеспечивающие обнаружение внутренних или внешних отказов и формирование сигналов о них.

Примечание — Требования к аппаратным средствам системы безопасности, описанные в перечислении d), относятся и к механизмам безопасности, предотвращающим скрытые отказы.

Пример — Заданное время реакции на отказ аппаратных средств механизма безопасности соответствует интервалу сбоеустойчивости;

e) требования к аппаратным средствам системы безопасности, не специфицирующие механизмы безопасности.

Пример — Такими требованиями могут быть:

- требования к элементам аппаратных средств для обеспечения достижения целевых значений случайных отказов аппаратных средств, как описано в 6.4.3 и 6.4.4;

- требования о предотвращении конкретного поведения (например, «сигнал на выходе конкретного датчика не должен быть неустойчивым»);

- требования, распределенные элементам аппаратных средств, реализующим целевую функциональность;

- требования, определяющие правила проектирования жгутов или разъемов.

6.4.3 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должны учитываться целевые значения, установленные в соответствии с разделом 7 ИСО 26262-4 для метрик, представленных в разделе 8 настоящего стандарта, при выводе значений элементов аппаратных средств устройства.

Примечание — Данная деятельность может включать в себя разделение целевых значений в случае распределенной разработки, как указано в разделе 5 ИСО 26262-8.

6.4.4 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должны учитываться целевые значения, установленные в соответствии с разделом 7 ИСО 26262-4, для процедур, представленных в разделе 9 настоящего стандарта, при выводе значений элементов аппаратных средств устройства.

Примечание — Данная деятельность может включать в себя разделение целевых значений в случае распределенной разработки, как указано в разделе 5 ИСО 26262-8.

6.4.5 Требования к аппаратным средствам системы безопасности должны быть определены в соответствии с разделом 6 ИСО 26262-8.

6.4.6 Должны быть определены критерии оценки для верификации проекта аппаратных средств устройства или элемента, в том числе: условия окружающей среды (температура, вибрация, электромагнитные помехи и др.), конкретные условия эксплуатации (напряжение питания, циклограмма и т. д.) и конкретные требования для компонент:

a) для верификации квалификацией компонентов или части аппаратных средств средней сложности критерии должны удовлетворять требованиям раздела 13 ИСО 26262-8;

b) для верификации тестированием критерии должны удовлетворять требованиям раздела 10.

6.4.7 Интервал сбоеустойчивости для механизмов безопасности должен удовлетворять требованиям к аппаратным средствам системы безопасности, как определено в пункте 6.4.2.3 ИСО 26262-4.

6.4.8 Интервал обнаружения множественного сбоя должен удовлетворять требованиям к аппаратным средствам системы безопасности, как определено в пункте 6.4.4.3 ИСО 26262-4.

Примечания

1 Если значения УПБА для целей безопасности равны C и D и если соответствующая концепция обеспечения безопасности не устанавливает конкретного значения, то интервал обнаружения множественного сбоя может быть задан равным или ниже значение времени цикла «включения-выключения» питания устройства.

2 Соответствующее значение интервала обнаружения множественного сбоя также может быть обосновано методом количественного анализа возникновения случайных отказов аппаратных средств (см. раздел 9).

6.4.9 Требования к аппаратным средствам системы безопасности должны быть верифицированы в соответствии с требованиями разделов 6 и 9 ИСО 26262-8, в целях обеспечения доказательств их:

a) согласованности с технической концепцией обеспечения безопасности, спецификацией проекта системы и спецификацией аппаратных средств;

b) полноты относительно технических требований к системе безопасности, распределяемых элементу аппаратных средств;

c) согласованности с соответствующими требованиями к программному обеспечению системы безопасности;

d) корректности и точности.

6.4.10 Спецификация программно-аппаратного интерфейса, сформированная в соответствии с требованиями раздела 7 ИСО 26262-4, должна быть в достаточной степени уточнена, чтобы обеспечить правильное управление и использование аппаратных средств программным обеспечением, а также должна описывать каждую связанную с безопасностью зависимость между аппаратными средствами и программным обеспечением.

6.4.11 Лица, ответственные за разработку аппаратных средств и программного обеспечения, несут солидарную ответственность за проверку адекватности уточненной спецификации программно-аппаратного интерфейса.

6.5 Результаты работы

6.5.1 Спецификация требований к аппаратным средствам системы безопасности (включая квалификационные критерии и критерии тестирования)

В результате выполнения требований 6.4.1—6.4.8.

6.5.2 Спецификация программно-аппаратного интерфейса (уточненная)

В результате выполнения требований 6.4.10 и 6.4.11.

Примечание — Данный результат работы совпадает с результатом работы по пункту 6.5.2 ИСО 26262-6.

6.5.3 Отчет о верификации требований аппаратных средств системы безопасности

В результате выполнения требований 6.4.9.

7 Проектирование аппаратных средств

7.1 Цели

Первой целью данного раздела является разработка аппаратных средств в соответствии со спецификацией проекта системы и требованиями к аппаратным средствам системы безопасности.

Второй целью данного раздела является проверка проекта аппаратных средств на соответствие спецификации проекта системы и требований к аппаратным средствам системы безопасности.

7.2 Общие положения

Проект аппаратных средств включает в себя проект архитектуры аппаратных средств и детальный проект аппаратных средств. Проект архитектуры аппаратных средств представляет все компоненты аппаратных средств и их взаимодействие друг с другом. Детальный проект аппаратных средств — это проект аппаратных средств на уровне электрических схем, представляющих взаимодействие между частями аппаратных средств, из которых состоят компоненты аппаратных средств.

Для того, чтобы разработать единый проект аппаратного средства, он должен удовлетворять как требованиям к аппаратным средствам системы безопасности, так и всем требованиям, не связанным с

безопасностью. Следовательно, на этой подстадии связанные и не связанные с безопасностью требования применяются в одном процессе разработки.

7.3 Входная информация

7.3.1 Предварительные требования

Необходима следующая информация:

- спецификация требований к аппаратным средствам системы безопасности в соответствии с 6.5.1;
- спецификация программно-аппаратного интерфейса (уточненная) в соответствии с требованиями 6.5.2;
- спецификация проекта системы в соответствии с пунктом 7.5.2 ИСО 26262-4;
- план обеспечения безопасности (уточненный) в соответствии с 5.5.

7.3.2 Дополнительная информация

Следующая информация может быть учтена:

- спецификация требований к программному обеспечению системы безопасности (см. пункт 6.5.1 ИСО 26262-6).

7.4 Требования и рекомендации

7.4.1 Проект архитектуры аппаратных средств

7.4.1.1 Архитектура аппаратных средств должна реализовать требования к аппаратным средствам системы безопасности, определенные в разделе 6.

7.4.1.2 Каждый компонент аппаратных средств должен наследовать наибольшее значение УПБА, специфицированное для требований к аппаратным средствам системы безопасности, которые он реализует.

Примечание — Каждая характеристика компонента аппаратных средств будет наследовать наибольшее значение УПБА, специфицированное для требований к аппаратным средствам системы безопасности, которые он реализует.

7.4.1.3 Если в процессе проекта архитектуры аппаратных средств системы безопасности для требований аппаратных средств системы безопасности выполнятся декомпозиция УПБА, то она должна применяться в соответствии с требованиями раздела 5 ИСО 26262-9.

7.4.1.4 Если элемент аппаратного средства выполнен из подэлементов, которые имеют различные распределенные значения УПБА, или подэлементов, которым значения УПБА не назначены, и связанных с безопасностью подэлементов, то каждый из них рассматривается в соответствии с самым высоким значением УПБА, пока не будут выполнены критерии совместимости подэлементов в соответствии с требованиями ИСО 26262-9.

7.4.1.5 Должна поддерживаться прослеживаемость между требованиями аппаратных средств системы безопасности и их реализацией вплоть до компонентов аппаратных средств самого низкого уровня.

Примечание — Прослеживаемость не требуется до уровня детального проектирования аппаратных средств и значения УПБА не назначаются частям аппаратных средств.

7.4.1.6 Для того чтобы предотвратить отказы, вызванные высокой сложностью, проект архитектуры аппаратных средств должен обладать следующими свойствами, используя принципы, перечисленные в таблице 1:

a) модульность;
b) адекватный уровень детализации;
c) простоту.

Таблица 1 — Свойства модульного проектирования аппаратных средств

Свойства		УПБА			
		A	B	C	D
1	Иерархичность проекта	+	+	+	+
2	Точно определенные интерфейсы связанных с безопасностью компонентов аппаратных средств	++	++	++	++

Окончание таблицы 1

Свойства		УПБА			
		A	B	C	D
3	Предотвращение излишней сложности интерфейсов	+	+	+	+
4	Предотвращение излишней сложности компонентов аппаратных средств	+	+	+	+
5	Ремонтопригодность (обслуживание)	+	+	++	++
6	Тестируемость[a)]	+	+	++	++
[a)] Тестируемость включает в себя тестируемость в процессе разработки и эксплуатации.					

7.4.1.7 В процессе проектирования архитектуры аппаратных средств должны быть рассмотрены нефункциональные причины отказа связанных с безопасностью компонентов аппаратных средств, включая следующие, если такие применимы: температура, вибрация, вода, пыль, электромагнитные помехи, перекрестные помехи, возникающие либо от других аппаратных компонент архитектуры аппаратных средств, либо от их окружения.

7.4.2 Детальное проектирование аппаратных средств

7.4.2.1 Для того, чтобы избежать общих ошибок проектирования, должен применяться соответствующий накопленный опыт согласно требованиям пункта 5.4.2.7 ИСО 26262-2.

7.4.2.2 В процессе детального проектирования аппаратных средств должны быть рассмотрены нефункциональные причины отказа связанной с безопасностью части аппаратных средств, включая следующие, если такие применимы: температура, вибрация, вода, пыль, электромагнитные помехи, коэффициент шума, перекрестные помехи, возникающие либо от других аппаратных частей компонента аппаратных средств, либо от ее окружения.

7.4.2.3 Условия эксплуатации частей аппаратных средств, используемых в детальном проектировании аппаратных средств, должны соответствовать специфицированным для них диапазонам значений эксплуатационных параметров и параметров окружающей среды.

7.4.2.4 Должны быть рассмотрены надежные принципы проектирования.

Примечание — Надежность принципов проектирования может быть показана с помощью контрольных карт на основе методов управления качеством.

Пример — Консервативная спецификация компонентов.

7.4.3 Анализ безопасности

7.4.3.1 Для выявления причин отказов и их последствий должен выполняться анализ безопасности проекта аппаратных средств в соответствии с таблицей 2 и требованиями раздела 8 ИСО 26262-9.

Примечания

1 Первоначальной целью анализа безопасности является поддержка спецификации проекта аппаратных средств. Впоследствии анализ безопасности может быть использован для верификации проекта аппаратных средств (см. 7.4.4).

2 В целях поддержки спецификации проекта аппаратных средств может быть уместным и достаточным качественный анализ.

Таблица 2 — Анализ безопасности проекта аппаратных средств

Методы		УПБА			
		A	B	C	D
1	Дедуктивный анализ[a)]	o	+	++	++
2	Индуктивный анализ[b)]	++	++	++	++
Примечание — Уровень детализации анализа соизмерим с уровнем детализации проекта. Оба метода могут, в определенных случаях, выполняться на различных уровнях детализации. [a)] Типичным дедуктивным методом анализа является FTA. [b)] Типичным индуктивным методом анализа является FMEA.					

7.4.3.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для каждого связанного с безопасностью компонента или части аппаратных средств с учетом рассматриваемой цели безопасности анализ безопасности должен определить следующее:

a) безопасные сбои;

b) одиночные сбои или остаточные сбои;

c) множественные сбои (или воспринимаемые, обнаруживаемые, или скрытые).

Примечания

1 В большинстве случаев анализ может быть ограничен двойными сбоями. Но иногда в технической концепции обеспечения безопасности (например, при реализации избыточных механизмов безопасности) могут быть рассмотрены множественные сбои более второго порядка.

2 Идентификация двойных сбоев не требует систематического анализа каждой возможной комбинации из двух сбоев аппаратных средств, но, как минимум, необходимо рассмотреть комбинации, которые следуют из технической концепции обеспечения безопасности (например, комбинацию двух сбоев, где один сбой влияет на связанный с безопасностью элемент, а другой сбой влияет на соответствующий механизм безопасности, предназначенный для достижения или поддержания безопасного состояния).

7.4.3.3 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должно быть обеспечено доказательство эффективности механизмов безопасности, предотвращающих одиночные сбои.

С этой целью:

a) должно быть обеспечено доказательство способности механизмов безопасности поддерживать безопасное состояние или безопасно перейти в безопасное состояние (в частности, соответствующие возможности смягчения отказа в течении периода сбоеустойчивости) и

b) должен быть оценен диагностический охват по отношению к остаточным неисправностям.

Примечания

1 Сбой, который может произойти в любое время (например, не только при включении питания) не может рассматриваться, как эффективно охваченный, если значение интервала его диагностических проверок, сложенное со значением времени реакции на сбой соответствующего механизма безопасности, больше, чем соответствующее значение интервала сбоеустойчивости.

2 Если можно показать, что сбой происходит только при включении питания и вероятность его возникновения ничтожно мала во время движения транспортного средства, то для таких сбоев принято выполнять тестирования при пуске после подачи питания.

3 Для структурирования обоснования могут быть использованы такие виды анализа, как FMEA или FTA.

4 В зависимости от знаний о виде отказов элементов аппаратных средств и их последствий для более высоких уровней, оценка может быть выполнена либо с помощью глобального охвата диагностикой элемента аппаратных средств, либо более детальной оценкой охвата вида отказов.

5 Для выполнения начального шага оценки охвата диагностикой, в которой требуемое значение охвата диагностикой поддерживается надлежащим обоснованием, может быть использовано приложение D.

7.4.3.4 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должно быть обеспечено доказательство эффективности механизмов безопасности, предотвращающих скрытые сбои.

С этой целью:

a) должны быть обеспечены доказательства обнаружения отказа и возможности уведомить водителя в течение допустимого времени обнаружения множественного сбоя для скрытых сбоев для того, чтобы определить, какие сбои остаются скрытыми и какие сбои являются не скрытыми; и

b) должен быть оценен диагностический охват для скрытых сбоев.

Примечания

1 Сбой не может рассматриваться как охваченный, если значение интервала его диагностических проверок, сложенное со значением времени реакции на сбой соответствующего механизма безопасности, больше, чем соответствующее значение времени обнаружения множественного сбоя для скрытых сбоев.

2 Для структурирования обоснования могут быть использованы такие виды анализа, как FMEA или FTA.

3 Для выполнения начального шага оценки охвата диагностикой, в которой требуемое значение охвата диагностикой поддерживается надлежащим обоснованием, может быть использовано приложение D.

4 В зависимости от знаний о виде отказов элементов аппаратных средств и их последствий для более высоких уровней, оценка может быть выполнена либо с помощью глобального охвата диагностикой элемента аппаратных средств, либо более детальной оценкой охвата вида отказов.

7.4.3.5 При необходимости на основе анализа зависимых отказов в соответствии с требованиями раздела 7 ИСО 26262-9, должно быть обеспечено доказательство того, что проект аппаратных средств соответствует его требованиям о независимости.

7.4.3.6 Если при проектировании аппаратных средств появляются новые опасности, еще не охваченные существующей целью безопасности, то они должны быть учтены и оценены методом анализа опасностей и оценки рисков в соответствии с требованиями процесса управления изменениями, представленными в ИСО 26262-8.

Примечание — Вновь выявленные опасности, еще не отраженные в существующей цели безопасности, как правило, являются нефункциональными опасностями. Нефункциональные опасности выходят за рамки области применения настоящего стандарта, но они могут быть при анализе опасностей и оценке рисков снабжены следующим пояснением «Данной опасности значение УПБА не назначается, поскольку они выходят за рамки области применения настоящего стандарта». Тем не менее значение УПБА может быть назначено в качестве рекомендации.

7.4.4 Верификация проекта аппаратных средств

7.4.4.1 Проект аппаратных средств должен быть верифицирован в соответствии с требованиями раздела 9 ИСО 26262-8, на соответствие и полноту по отношению к требованиям к аппаратным средствам системы безопасности. Для достижения этой цели должны быть рассмотрены методы, перечисленные в таблице 3.

Таблица 3 — Верификация проекта аппаратных средств

Методы		УПБА			
		A	B	C	D
1a	Сквозной контроль проекта аппаратных средств[a)]	++	+	o	o
1b	Осмотр (контроль) проекта аппаратных средств[a)]	+	++	++	++
2	Анализ безопасности	В соответствии с 7.4.3			
3a	Моделирование[b)]	o	+	+	+
3b	Разработка аппаратных средств прототипированием[b)]	o	+	+	+

Примечание — Область применения этого отчета по верификации является техническая корректность проекта аппаратных средств.

[a)] Методы 1a и 1b служат для проверки полноты и правильности выполнения требований к аппаратным средствам системы безопасности для проекта аппаратных средств.

[b)] Методы 3a и 3b служат для проверки аппаратных средств в конкретных точках (например, используя метод внесения неисправностей), для которых аналитические методы 1 и 2 считается не достаточными.

7.4.4.2 Если во время проектирования аппаратных средств обнаружено, что выполнение какого либо требования к аппаратным средствам системы безопасности не возможно, то выдается запрос на изменение в соответствии с требованиями процесса управления изменениями, представленными в ИСО 26262-8.

7.4.5 Производство, эксплуатация, обслуживание и вывод из эксплуатации

7.4.5.1 Если анализ безопасности показал важность связанных с безопасностью специальных характеристик, то они должны быть специфицированы. Атрибуты, связанных с безопасностью специальных характеристик, должны включать:

a) меры верификации в процессе производства и эксплуатации, а также

b) критерии допустимости этих мер.

Пример — Анализ безопасности проекта аппаратных средств, который опирается на новые сенсорные технологии (например, камера или радарные датчики), может выявить актуальность специальной процедуры установки этих датчиков. В таком случае на этапе производства могут быть необходимы дополнительные меры верификации для этих компонентов.

7.4.5.2 Должны быть специфицированы инструкции по монтажу, демонтажу и выводу из эксплуатации связанных с безопасностью элементов аппаратных средств, если эти операции могут повлиять на техническую концепцию обеспечения безопасности.

7.4.5.3 Должна быть обеспечена прослеживаемость связанных с безопасностью элементов аппаратных средств в соответствии с требованиями пункта 5.4.1.2 ИСО 26262-7.

Примечание — Прослеживаемость может включать в себя адекватную маркировку или другую идентификацию элементов аппаратных средств, чтобы указать, что они связанны с безопасностью.

7.4.5.4 Должны быть специфицированы инструкции по эксплуатации связанных с безопасностью элементов аппаратных средств, если процессы эксплуатации могут повлиять на техническую концепцию обеспечения безопасности.

7.5 Результаты работы

7.5.1 Спецификация проекта аппаратных средств

В результате выполнения требований 7.4.1 и 7.4.2.

7.5.2 Отчет по анализу безопасности аппаратных средств

В результате выполнения требований 7.4.3.

7.5.3 Отчет о верификации проекта аппаратных средств

В результате выполнения требований 7.4.4.

7.5.4 Спецификация требований к производству, эксплуатации, обслуживанию и выводу из эксплуатации

В результате выполнения требований 7.4.5.

8 Оценка метрик архитектуры аппаратных средств

8.1 Цель

Целью настоящего раздела является оценка архитектуры аппаратных средств устройства на соответствие требованиям с помощью метрик архитектуры аппаратных средств.

8.2 Общие положения

Данный раздел описывает две метрики архитектуры аппаратных средств для оценки эффективности архитектуры устройства из-за случайных отказов аппаратных средств.

Эти метрики и связанные с ними целевые значения применяются ко всем аппаратным средствам устройства и являются дополнением к оценке нарушения цели безопасности из-за случайных отказов аппаратных средств, описанной в разделе 9.

Случайные отказы аппаратных средств, для которых используются эти метрики, ограничены отказами, связанными с безопасностью электрических и электронных частей аппаратных средств устройства, а именно теми, которые могут внести значительный вклад в нарушение или достижение цели безопасности, а также одиночными, остаточными и скрытыми сбоями этих частей. Для электромеханических частей аппаратных средств рассматриваются только виды и интенсивности электрических отказов.

Примечание — Элементы аппаратных средств с множественными сбоями более второго порядка могут быть исключены из расчетов, если нельзя показать, что они имеют отношение к технической концепции обеспечения безопасности.

Метрики архитектуры аппаратных средств могут быть применены многократно во время проектирования архитектуры аппаратных средств и детального проектирования аппаратных средств.

Метрики архитектуры аппаратных средств зависят от всего комплекса аппаратных средств устройства. Выполнение целевых показателей, предписанных для метрик архитектуры аппаратных средств, достигается для каждой цели безопасности, которую реализует устройство.

Такие метрики архитектуры аппаратных средств определяются для достижения следующих целей:

- быть объективно оцениваемыми: метрики должны быть верифицируемыми и достаточно точными, чтобы дифференцировать различные архитектуры;
- выполнять оценку окончательного проекта (выполнение точных расчетов для детального проекта аппаратных средств);
- сделать возможной оценку архитектуры аппаратных средств по критерию достигнуто/не достигнуто заданное значение УПБА;
- определить, достаточен ли охват механизмами безопасности, чтобы предотвратить риск от одиночного или остаточного сбоя в архитектуре аппаратных средств (метрика одиночного сбоя);

- определить, достаточен ли охват механизмами безопасности, чтобы предотвратить риск от скрытых сбоев в архитектуре аппаратных средств (метрика скрытого сбоя);
- устранять одиночные, остаточные и скрытые сбои;
- обеспечить надежность при неустойчивости интенсивности отказов в аппаратных средствах;
- рассматривать только элементы, связанные с безопасностью;
- поддерживать применение для элементов на различных уровнях, например, целевые значения могут быть распределены поставляемым элементам аппаратных средств.

Пример — Для облегчения распределенной разработки, целевые значения могут быть распределены микроконтроллерам или электронным блокам управления.

8.3 Входная информация

8.3.1 Предварительные требования

Следующая информация должна быть доступна:
- спецификация требований к аппаратным средствам системы безопасности в соответствии с 6.5.1.
- спецификация проекта аппаратных средств в соответствии с 7.5.1;
- отчет по анализу безопасности аппаратных средств в соответствии с 7.5.2.

8.3.2 Дополнительная информация

Следующая информация может быть учтена:
- техническая концепция обеспечения безопасности (см. 7.5.1 ИСО 26262-4);
- спецификация проекта системы (см. 7.5.2 ИСО 26262-4).

8.4 Требования и рекомендации

8.4.1 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Понятия охват диагностикой, метрика одиночного сбоя и метрика скрытого сбоя, рассмотренные в приложении C, применяются к требованиям 8.4.2—8.4.9.

8.4.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Охват диагностикой связанных с безопасностью элементов аппаратных средств механизмами безопасности должен быть оценен по остаточным сбоям и по соответствующим скрытым сбоям.

Примечания

1 Для выполнения начального шага оценки охвата диагностикой, в которой требуемое значение охвата диагностикой поддерживается надлежащим обоснованием, могут быть использованы таблицы D.1—D.14.

2 В зависимости от знаний о виде отказов элементов аппаратных средств и их последствий для более высоких уровней, оценка может быть выполнена либо с помощью глобального охвата диагностикой элемента аппаратных средств, либо более детальной оценкой охвата вида отказов.

8.4.3 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должны быть определены, используемые в анализе, расчетные значения интенсивностей отказов частей аппаратных средств:

a) используя данные об интенсивностях отказов частей аппаратных средств из признанных источников промышленности; или

Пример — Общепризнанными отраслевыми источниками для определения интенсивностей отказов частей аппаратных средств считаются: IEC/TR 62380, IEC 61709, MIL HDBK 217 F notice 2, RIAC HDBK 217 Plus, UTE C80-811, NPRD 95, EN 50129:2003, Annex C, IEC 62061:2005, Annex D, RIAC FMD97 и MIL HDBK 338.

Примечание — Значения интенсивностей отказов, приведенные в этих базах данных, как правило, считается пессимистическими;

b) используя статистику, основанную на данных, полученных из эксплуатации или испытаний. В этом случае оцененная интенсивность отказов должна иметь достаточный уровень доверия; или

c) используя экспертную оценку, основанную на инженерном подходе, использующем количественные и качественные методы. В основе экспертной оценки лежат структурированные критерии. Эти критерии должны быть установлены до выполнения оценки интенсивностей отказов.

Примечание — Критериями экспертной оценки могут быть опыт эксплуатации, тестирование, анализ надежности и новизна проекта.

8.4.4 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Если достаточное доказательство расчетных значений интенсивностей отказов при одиночном или скрытом

сбое не может быть выполнено, то должны быть предложены альтернативные средства (например, дополнительные механизмы безопасности для выявления и управления этими сбоями).

Примечание — «Достаточное доказательство» означает, например, что в нем интенсивность отказов должна быть определена с помощью одного из методов, перечисленных в 8.4.3.

8.4.5 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для каждой цели безопасности количественное целевое значение метрики одиночного сбоя в соответствии с требованиями 7.4.4.2 ИСО 26262-4 должно быть основано на одном из следующих источников рекомендуемых целевых значений:

a) полученных из вычисления метрик архитектуры аппаратных средств, для которых применены аналогичные хорошо зарекомендовавшие себя принципы проектирования; или

Примечание — Два аналогичных проекта имеют схожие функциональные возможности и аналогичные цели безопасности с теми же значениями УПБА;

b) полученных из таблицы 4.

Таблица 4 — Возможный источник для получения целевого значения метрики одиночного сбоя

	УПБА B	УПБА C	УПБА D
Метрика одиночного сбоя	≥ 90 %	≥ 97 %	≥ 99 %

Примечание — Этот количественный целевой показатель предназначен для обеспечения:
- руководства проектированием и
- доказательства того, что проект соответствует целям безопасности.

8.4.6 Данное требование распространяется на значения УПБА (B), (C) и D цели безопасности. Для каждой цели безопасности количественное целевое значение метрики скрытого сбоя в соответствии с требованиями 7.4.4.2 ИСО 26262-4 должно быть основано на одном из следующих источников рекомендуемых целевых значений:

a) полученных из вычисления метрик архитектуры аппаратных средств, для которых применены аналогичные хорошо зарекомендовавшие себя принципы проектирования; или

Примечание — Два аналогичных проекта имеют схожие функциональные возможности и аналогичные цели безопасности с теми же значениями УПБА;

b) полученных из таблицы 5.

Таблица 5 — Возможный источник для получения целевого значения метрики скрытого сбоя

	УПБА B	УПБА C	УПБА D
Метрика скрытого сбоя	≥ 60 %	≥ 80 %	≥ 90 %

Примечание — Этот количественный целевой показатель предназначен для обеспечения:
- руководства проектированием и
- доказательства того, что проект соответствует целям безопасности.

8.4.7 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для каждой цели безопасности комплекс аппаратных средств устройства в целом должен соответствовать одному из следующих вариантов:

a) достижению целевого значения метрики одиночного сбоя, как описано в 8.4.5; или

b) достижению соответствующих целей, предусмотренных на уровне элементов аппаратных средств, которые являются достаточными для соответствия целевому значению метрики одиночного сбоя, назначенной для всего комплекса аппаратных средств устройства, согласно требованию 8.4.5, с обоснованием соответствия с этими целями на уровне элементов аппаратных средств.

Примечания

1 Если устройство содержит различные виды элементов аппаратных средств с существенно разными уровнями интенсивности отказов, то существует риск, что для соответствия с метриками архитектуры аппаратных средств рассматриваются только элементы аппаратных средств с наибольшей величиной интенсивности отказов. (Одним из примеров, когда это может произойти, является метрика одиночного сбоя, для которой соответствие

может быть достигнуто путем учета интенсивности отказов в проводниках/предохранителях/разъемах без учета интенсивности отказов частей аппаратных средств со значительно более низкой интенсивностью отказов). Назначение соответствующих значений целевых метрик для каждого вида аппаратных средств помогает избежать такую ситуацию.

2 Кратковременные сбои рассматриваются, когда показано, что они актуальны, например, в связи с используемой технологией. Они могут быть учтены путем спецификации и проверки выделенного для них целевого значения метрики одиночного сбоя (как это указано в примечании 1) или с помощью качественного обоснования, основанного на верификации эффективности внутренних механизмов безопасности, реализованных для охвата этих кратковременных сбоев.

3 Если цель не достигнута, то обоснование того, как достигается цель безопасности, будет оцениваться, как указано в 4.1.

4 Некоторые или все соответствующие цели безопасности можно рассматривать вместе для определения метрики одиночного сбоя, но в этом случае целевой метрикой считается наибольшее для рассматриваемых целей безопасности значение УПБА.

8.4.8 Данное требование распространяется на значения УПБА (B), (C) и D цели безопасности. Для каждой цели безопасности комплекс аппаратных средств всего устройства должен соответствовать одному из следующих вариантов:

a) достижению целевого значения метрики скрытого сбоя, как описано в 8.4.6; или

b) достижению соответствующих целей, предусмотренных на уровне элементов аппаратных средств, которые являются достаточными для соответствия целевому значению метрики скрытого сбоя, назначенной для комплекса аппаратных средств всего устройства, согласно требованию 8.4.6, с обоснованием соответствия этим целям на уровне элементов аппаратных средств; или

c) достижению целевых значений охвата диагностикой скрытых сбоев идентично целевому значению, указанному в 8.4.6 для метрики скрытого сбоя (рассматривается как охват диагностикой), для каждого элемента аппаратных средств со сбоями, которые могут привести к недоступности механизма безопасности (предназначенного для предотвращения сбоев, вызывающих нарушения цели безопасности). Этот вариант применяется, когда каждый механизм безопасности, недоступность которого может способствовать нарушению цели безопасности, предназначен для обнаружения сбоев.

Примечания

1 Вариант перечисления c) применяется только в тех случаях, где каждый соответствующий механизм безопасности предназначен для обнаружения сбоев. Предполагается, что в этом случае потенциально скрытые сбои целевой функциональности выявляются путем обнаружения этими механизмами безопасности. В других случаях этот вариант не может быть применен и варианты перечислений a) и b) являются единственно возможными.

2 В случае варианта перечисления c) метрика не рассчитывается, оценивается только охват элементов аппаратных средств механизмами безопасности в отношении скрытых сбоев.

3 Если устройство содержит различные виды элементов аппаратных средств с существенно разными уровнями интенсивности отказов, то существует риск, что для соответствия с метриками архитектуры аппаратных средств рассматриваются только элементы аппаратных средств с наибольшей величиной интенсивности отказов. (Одним из примеров, когда это может произойти, является метрика одиночного сбоя, для которой соответствие может быть достигнуто путем учета интенсивности отказов в проводниках/предохранителях/разъемах без учета интенсивности отказов частей аппаратных средств со значительно более низкой интенсивностью отказов). Назначение соответствующих значений целевых метрик для каждого вида аппаратных средств помогает избежать такую ситуацию.

4 Если цель не достигнута, то обоснование того, как достигается цель безопасности, будет оцениваться, как указано в 4.1.

5 Некоторые или все соответствующие цели безопасности можно рассматривать вместе для определения метрики скрытого сбоя, но в этом случае целевой метрикой считается наибольшее для рассматриваемых целей безопасности значение УПБА.

8.4.9 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Чтобы представить доказательства технической корректности и полноты в соответствии с требованиями раздела 9 ИСО 26262-8 должен быть подготовлен отчет о верификации результатов применяемых методов в 8.4.7 и 8.4.8.

Примечание — Тщательная верификация метрики одиночного сбоя гарантирует, что учитывается только интенсивность отказов связанных с безопасностью элементов аппаратных средств, так что метрика не искажается ненадлежащим образом из-за излишних связанных с безопасностью элементов аппаратных средств, в которых невозможны одиночные или остаточные сбои (например, путем добавления излишних элементов аппаратных средств в механизм безопасности).

8.5 Результаты работы

8.5.1 Анализ эффективности архитектуры устройства по предотвращению случайных отказов аппаратных средств

В результате выполнения требований 8.4.1—8.4.8.

8.5.2 Отчет группы экспертов об эффективности архитектуры устройства по предотвращению случайных отказов аппаратных средств

В результате выполнения требований 8.4.9.

9 Оценка нарушений цели безопасности вследствие случайных отказов аппаратных средств

9.1 Цель

Целью требований настоящего раздела является формирование применимых критериев для обоснования того, что остаточный риск нарушения цели безопасности из-за случайных отказов аппаратных средств устройства, является достаточно низким.

Примечание — «Достаточно низкий» означает «сопоставим с остаточными рисками для уже находящихся в эксплуатации устройствах».

9.2 Общие положения

Предлагается два альтернативных метода (см. 9.4) для оценки того, насколько остаточный риск нарушений цели безопасности является достаточно низким.

Оба метода оценивают остаточный риск нарушения цели безопасности из-за однократных, остаточных и вероятных двойных сбоев. Могут быть также рассмотрены множественные сбои, если показано, что они охвачены концепцией обеспечения безопасности. В настоящем анализе будет рассмотрен охват механизмами безопасности остаточных и двойных сбоев, а также будет рассмотрена продолжительность воздействия для двойных сбоев.

Первый способ заключается в использовании вероятностной метрики, которая называется «вероятностная метрика случайных отказов аппаратных средств» (PMHF), для оценки нарушения рассматриваемой цели безопасности, используя, например, количественный метод FTA, и сравнение результатов этой количественной оценки с целевым значением.

Второй метод заключается в отдельной оценке каждого остаточного и одиночного сбоя, и каждого двойного сбоя, приводящего к нарушению рассматриваемой цели безопасности. Этот метод анализа также может называться анализом сечений.

Примечание — В контексте анализа надежности, сечение дерева сбоев представляет собой набор базовых событий, чье появление приводит к появлению события на вершине дерева.

Выбранный метод может применяться многократно в процессе проектирования архитектуры аппаратных средств и детального проектирования аппаратных средств.

Область применения настоящего раздела ограничена случайными отказами аппаратных средств данного устройства. При выполнении анализа рассматриваются электрические и электронные части аппаратных средств. Для электромеханических частей аппаратных средств, рассматриваются только электрические виды отказов и интенсивность отказов.

9.3 Входная информация

9.3.1 Предварительные требования

Следующая информация должна быть доступна:

- спецификация требований к аппаратным средствам системы безопасности в соответствии с 6.5.1;
- спецификация проекта аппаратных средств в соответствии с 7.5.1;
- отчет по анализу безопасности аппаратных средств в соответствии с 7.5.2.

9.3.2 Дополнительная информация

Следующая информация может быть учтена:

- техническая концепция обеспечения безопасности (см. пункт 7.5.1 ИСО 26262-4);
- спецификация проекта системы (см. пункт 7.5.2 ИСО 26262-4).

9.4 Требования и рекомендации

9.4.1 Общие положения

Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Устройство должно удовлетворять требованиям 9.4.2 или 9.4.3.

9.4.2 Оценка вероятностной метрики случайных отказов аппаратных средств (PMHF)

9.4.2.1 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. В соответствии с требованиями 7.4.4.3 ИСО 26262-4 должны быть определены количественные целевые значения максимальной вероятности нарушения каждой цели безопасности из-за случайных отказов аппаратных средств с помощью одного из источников a), b) или c) ссылочных целевых значений:

a) таблицы 6 или

b) эксплуатационных данных устройств, созданных на основе аналогичных хорошо зарекомендовавших себя принципов проектирования или

c) количественных методов анализа, применяемых для аналогичных хорошо зарекомендовавших себя принципов проектирования, используя значения интенсивности отказов в соответствии с 8.4.3.

Примечания

1 Абсолютные величины этих количественных целевых значений, полученных из источников a), b) или c) не имеют никакого значения, но они полезны только для сравнения нового проекта с существующим. Они предназначены обеспечить выполнение цели проекта, описанной в 9.1, и доступность доказательства того, что проект выполняет цели безопасности.

2 Два проекта аналогичны, если имеют схожие функциональные возможности и аналогичные цели безопасности с теми же значениями УПБА.

Таблица 6 — Возможный источник для вывода целевых значений случайных отказов аппаратных средств

УПБА	Целевые значения случайных отказов аппаратных средств
D	$< 10^{-8}$ ч$^{-1}$
C	$< 10^{-7}$ ч$^{-1}$
B	$< 10^{-7}$ ч$^{-1}$

Примечание — Количественные целевые значения, представленные в данной таблице, могут быть адаптированы, как указано в 4.1, чтобы соответствовать конкретному использованию устройства (например, если устройство способно нарушить цель безопасности за время большее, чем типичное время использования легкового автомобиля).

9.4.2.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Количественно целевые значения требований 9.4.2.1 должны быть выражены в терминах средней вероятности в час в течение срока службы устройства.

9.4.2.3 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Доказательство того, что целевые значения требования 9.4.2.1 были достигнуты, должен предоставить количественный анализ архитектуры аппаратных средств для одиночного, остаточного и двойного сбоя. Этот количественный анализ должен учитывать:

a) архитектуру устройства;

b) оцененную интенсивность отказов для видов отказов каждой части аппаратных средств, которая может вызвать одиночный или остаточный сбой;

c) оцененную интенсивность отказов для видов отказов каждой части аппаратных средств, которая может вызвать двойной сбой;

d) диагностический охват связанных с безопасностью элементов аппаратных средств механизмами безопасности;

e) продолжительность воздействия в случае двойных сбоев.

Примечания

1 Виды отказов элементов аппаратных средств, которые могут вызвать одновременно отказ связанного с безопасностью элемента аппаратных средств и его механизма безопасности, анализируются количественными методами. Они могут быть одиночными, остаточными или множественными сбоями.

2 Продолжительность воздействия сбоя начинается с момента его возникновения и включает в себя:

a) интервал обнаружения множественного сбоя, связанного с каждым механизмом безопасности, или срок службы автомобиля, если сбой не отображается водителю (скрытый сбой);

b) максимальную продолжительность поездки (в случае, если водителю предлагается остановиться безопасным способом); и

c) средний интервал времени нахождения автомобиля в автомастерской (в случае, если водитель предупрежден о необходимости ремонта автомобиля).

Таким образом, продолжительность воздействия зависит от типа используемого мониторинга (например, постоянного мониторинга, периодического самотестирования, водительского мониторинга, отсутствие мониторинга) и вида реакции на обнаруженную неисправность. Она может быть равна нескольким миллисекундам в случае непрерывного мониторинга, запускающего переход в безопасное состояние. Она может быть равна сроку службы автомобиля, если мониторинг отсутствует.

Пример предположений о среднем времени работы до ремонта автомобиля, в зависимости от типа сбоя:

- 200 поездок автомобиля при снижении параметров комфорта;
- 50 поездок автомобиля при снижении эффективности функций поддержки вождения;
- 20 поездок автомобиля при желтом предупреждающем сигнале или воздействии на поведение автомобиля при его вождении;
- одна поездка автомобиля при красном предупреждающем сигнале.

Время, затраченное на ремонт, как правило, не рассматривается (за исключением оценки опасности, которой может подвергаться обслуживающий персонал).

Среднюю продолжительность поездки транспортного средства можно считать равной 1 часу.

3 В большинстве случаев множественные отказы более второго порядка, вносят незначительный количественный вклад в достижение целевых значений. Тем не менее, в некоторых конкретных случаях (очень высокая интенсивность отказов или низкий охват диагностикой), необходимо обеспечить два резервных механизма безопасности для достижения цели. Если техническая концепция обеспечения безопасности основана на избыточных механизмах безопасности, то при анализе рассматриваются множественные отказы более второго порядка.

4 При выполнении начального шага оценки охвата диагностикой механизмов безопасности, использующих комплексные диагностики, для обеспечения требуемых значений ОД, поддержанных надлежащим обоснованием, для механизмов безопасности могут быть использованы таблицы D.1—D.14.

5 Ситуации, когда устройство отключено от питания, не включаются при расчете средней вероятности отказов в час, тем самым предотвращая искусственное снижение значения средней вероятности отказов в час. Таким образом, для устройства, которое работает только 1 ч в день, остальные 23 ч не учитываются при расчете этого целевого значения времени эксплуатации.

6 Если цель не достигнута, то обоснование того, как достигается цель безопасности, будет оцениваться, как указано в 4.1.

7 В зависимости от знаний о виде отказов элементов аппаратных средств и их последствий для более высоких уровней, оценка может быть выполнена либо с помощью глобального охвата диагностикой элемента аппаратных средств, либо более детальной оценкой охвата вида отказов.

9.4.2.4 Данное требование распространяется на значения УПБА C и D цели безопасности. Одиночный сбой, происходящий в части аппаратного средства должен считаться допустимым только тогда, когда приняты специальные меры.

Примечание — Специальные меры могут включать:

a) особенности проекта такие, как проектирование части аппаратного средства с запасом (например, по уровню электрического напряжения или температуры), или такие, как физическое разделение (например, шаг контактов на печатной плате);

b) типовой тест со специальный входной информацией для уменьшения риска возникновения данного вида отказов;

c) испытание на отказ;

d) специальный механизм управления, как часть плана управления; и

e) установление, связанных с безопасностью особых характеристик.

9.4.2.5 Данное требование распространяется на значения УПБА C и D цели безопасности. Часть аппаратных средств должна рассматриваться специальными мерами (в примечании к 9.4.2.4 приведены примеры специальных мер), если ее охват диагностикой (для остаточных сбоев) ниже, чем 90 %.

Примечание — Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае расчет охвата производится аналогично расчету метрики одиночного сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.2.6 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Интенсивности отказов частей аппаратных средств, используемые при анализе, должны быть оценены в соответствии с требованиями 8.4.3.

9.4.2.7 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для того чтобы избежать количественного разночтения при объединении значений интенсивностей отказов из различных источников, они должны быть промасштабированы с помощью коэффициента масштабирования, что обеспечивает их согласованность. Масштабирование возможно, если существует обоснование коэффициента масштабирования между двумя источниками отказов.

Примечание — В приложении F приводится руководство по применению коэффициентов масштабирования.

9.4.3 Оценка каждой причины нарушения цели безопасности

9.4.3.1 Метод оценки каждой причины нарушения цели безопасности из-за случайных отказов аппаратных средств иллюстрируется блок-схемами на рисунках 3 и 4. Каждый одиночный сбой оценивается с помощью критериев возникновения сбоя. Каждый остаточный сбой оценивается с помощью критериев, объединяющих критерии возникновения сбоя и критерии эффективности механизма безопасности.

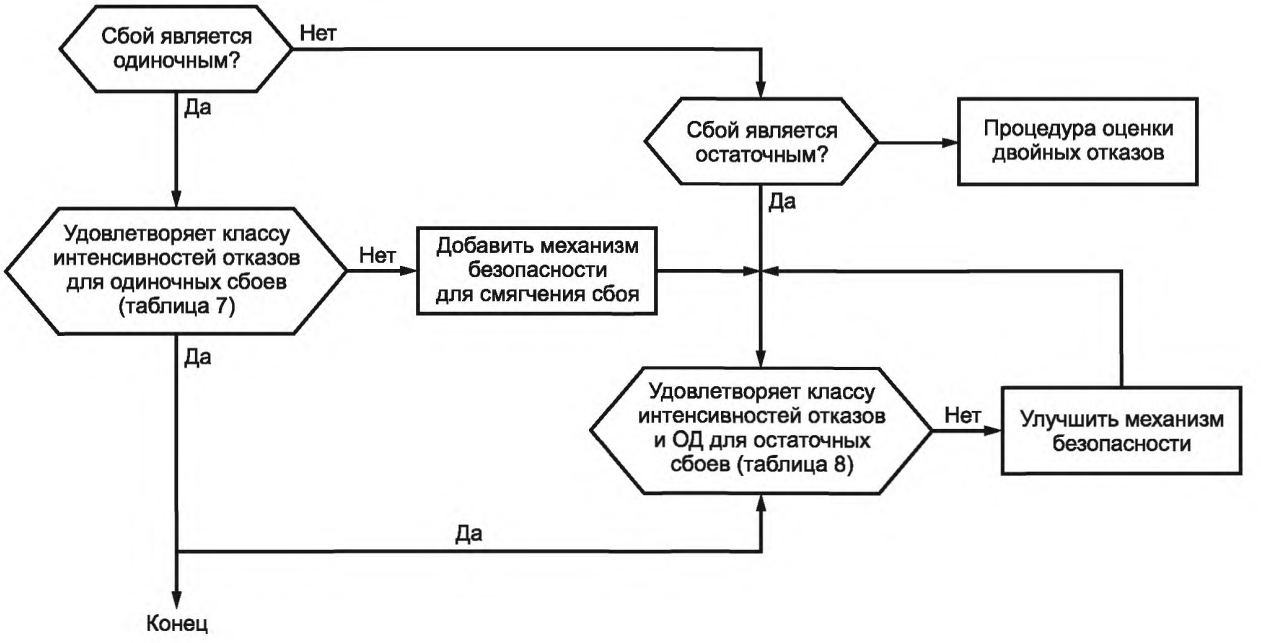


Рисунок 3 — Процедура оценки для одиночных и остаточных сбоев

Процедура, применяемая для двойных отказов, показана в виде блок-схемы на рисунке 4. Каждый двойной отказ сначала оценивается на его достоверность. Двойной отказ не считается достоверным, если оба сбоя, приводящие к отказу, обнаруживаются или воспринимаются за достаточно короткое время с достаточным охватом. Если двойной отказ является достоверным, то вызывающие его сбои затем оцениваются с использованием объединенного критерия возникновения сбоев и эффективности механизма безопасности. Процедуры оценки, представленные на рисунках 3 и 4, применяются на уровне частей аппаратных средств (транзисторы и т. д.).

Примечание — Для сложных частей аппаратных средств, например микроконтроллеров, целесообразно применять эту процедуру на более детальном уровне: для процессора, ОЗУ, ПЗУ и т. д.

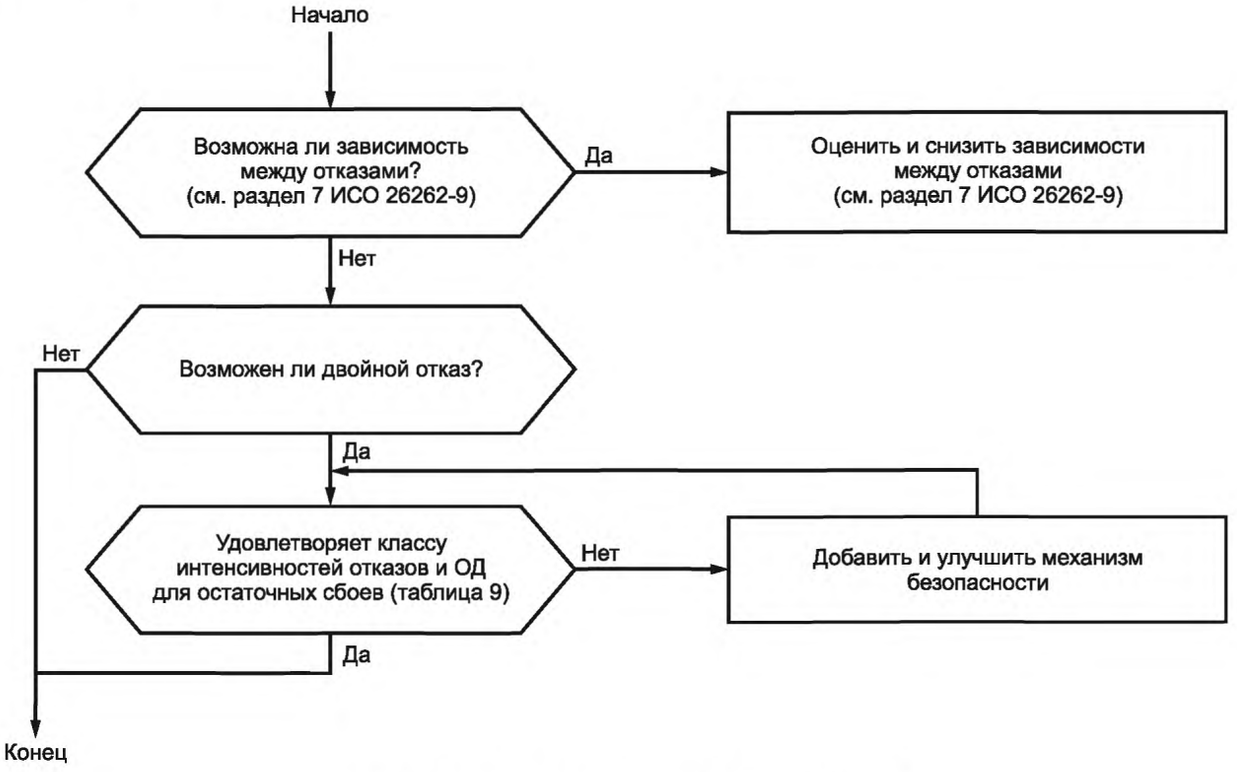


Рисунок 4 — Процедура оценки двойных отказов

9.4.3.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Отдельная оценка каждого одиночного сбоя, остаточного сбоя и двойного отказа, нарушающих рассматриваемую цель безопасности, должна осуществляться на уровне части аппаратных средств. Эта оценка должна представить доказательства, что каждый одиночный сбой, остаточный сбой и двойной отказ, нарушающие рассматриваемую цель безопасности, удовлетворяет соответствующим требованиям 9.4.3.3—9.4.3.12.

Примечания

1 Этот анализ можно рассматривать как обзор сечений, где отсутствие или неполнота охвата рассматривается как сбой.

2 В большинстве случаев множественные отказы более второго порядка, вносят незначительный вклад. Тем не менее, в некоторых конкретных случаях (очень высокая интенсивность отказов или низкий охват диагностикой), необходимо обеспечить два резервных механизма безопасности. Если техническая концепция обеспечения безопасности основана на избыточных механизмах безопасности, то при анализе рассматриваются множественные отказы более второго порядка.

3 Для сложных частей аппаратных средств, например микроконтроллеров, может быть целесообразно применять эту процедуру на более детальном уровне: для процессора, ОЗУ, ПЗУ и т. д.

9.4.3.3 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Ранжирование классов интенсивностей отказов для интенсивности отказов частей аппаратных средств определяется следующим образом:

Примечание — Классы 1, 2 и 3 для интенсивностей отказов вводятся для интенсивностей возникновения отказов. Эти классы аналогичны уровням возникновения 1, 2 и 3, используемым в FMEA, соответственно, где уровень 1 соответствует видам отказов с самой низкой интенсивностью возникновения.

a) интенсивность отказов, соответствующая интенсивности отказов класса 1, должна быть меньше, чем целевое значение УПБА, равное D деленное на 100, если не применяются требования 9.4.3.4.

Примечание — Могут быть использованы целевые значения, указанные в таблице 6;

b) интенсивность отказов, соответствующая интенсивности отказов класса 2, должна быть меньше или равна, увеличенной в 10 раз интенсивности отказов, соответствующей интенсивности отказов класса 1;

c) интенсивность отказов, соответствующая интенсивности отказов класса 3, должна быть меньше или равна, увеличенной в 100 раз интенсивности отказов, соответствующей интенсивности отказов класса 1 и

d) интенсивность отказов, соответствующая интенсивности отказов класса i, $i > 3$ должна быть меньше или равна, увеличенной в $10^{(i-1)}$ раз интенсивности отказов, соответствующей интенсивности отказов класса 1.

Примечания

1 Назначение класса интенсивности отказов основано на интенсивности отказов части аппаратных средств.

2 В случае, когда небольшое число частей (таких как микроконтроллер) имеют интенсивность отказов выше, чем верхний предел интенсивности отказов класса i, то этим частям может быть назначен класс возникновения i, если результирующая средняя интенсивность отказов частей, назначенных для класса i, ниже, чем верхний предел интенсивности отказов класса i.

9.4.3.4 При ранжировании классов интенсивностей отказов может быть использован делитель ниже, чем 100, если предоставляется обоснование. В этом случае должна быть обеспечена поддержка корректности ранжирования при совместном рассмотрении одиночных сбоев, остаточных сбоев и сечений более высокого уровня.

Пример — Обоснование может быть основано на количестве минимальных сечений.

9.4.3.5 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Одиночный сбой, возникающий в части аппаратных средств, считается приемлемым только, если в результате ранжирования интенсивность отказов части аппаратных средств соответствует целевым значениям, приведенным в таблице 7.

Таблица 7 — Целевые значения классов интенсивностей отказов частей аппаратных средств для одиночных сбоев

УПБА цели безопасности	Класс интенсивностей отказов
D	Класс 1 интенсивностей отказов + специальные меры[a)]
C	Класс 2 интенсивностей отказов + специальные меры[a)] или класс 1 интенсивностей отказов
B	Класс 2 интенсивностей отказов или класс 1 интенсивностей отказов
[a)] Примеры специальных мер приведены в примечании требования 9.4.2.4.	

Примечание — При оценке класса интенсивностей отказов может быть рассмотрена доля безопасных сбоев для части аппаратных средств.

9.4.3.6 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Остаточный сбой, возникающий в части аппаратных средств, считается приемлемым, если в результате ранжирования интенсивность отказов соответствует целевым значениям, приведенным в таблице 8 для охвата диагностикой (для остаточных сбоев) соответствующей части аппаратных средств.

Примечание — Рассматриваемая интенсивность отказов является интенсивностью отказов части аппаратных средств и не учитывает эффективность механизмов безопасности.

Таблица 8 — Классы с максимальной интенсивностью отказов для заданного охвата диагностикой части аппаратных средств — остаточные сбои

УПБА цели безопасности	Охват диагностикой остаточных сбоев			
	≥ 99,9 %	≥ 99 %	≥ 90 %	< 90 %
D	Класс 4 интенсивностей отказов	Класс 3 интенсивностей отказов	Класс 2 интенсивностей отказов	Класс 1 интенсивностей отказов + специальные меры[a)]
C	Класс 5 интенсивностей отказов	Класс 4 интенсивностей отказов	Класс 3 интенсивностей отказов	Класс 2 интенсивностей отказов + специальные меры[a)]
B	Класс 5 интенсивностей отказов	Класс 4 интенсивностей отказов	Класс 3 интенсивностей отказов	Класс 2 интенсивностей отказов
[a)] Примеры специальных мер приведены в примечании требования 9.4.2.4.				

Примечания

1 Таблица 8 устанавливает связь между классом с максимальной интенсивностью отказов, который позволено задавать целевому значению УПБА, и охватом диагностикой. Классы с более низкой интенсивностью отказов являются приемлемыми, но не требуемыми.

2 «Классы с более низкой интенсивностью отказов» означает классы интенсивностей отказов с более низким номером. Например, «Классы с более низкой интенсивностью отказов» для класса 3 интенсивностей отказов означает классы 2 и 1 интенсивностей отказов.

3 Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае вычисление охвата осуществляется аналогично расчету метрики одиночного сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.3.7 Данное требование распространяется на значения УПБА C и D цели безопасности. Для классов интенсивностей отказов i, $i > 3$, остаточный сбой считается приемлемым, если охват диагностикой больше или равно $[100 - 10^{(3 - i)}]$ % для значения УПБА, равного D, или больше или равно $[100 - 10^{(4 - i)}]$ % для значения УПБА, равного C.

Примечания

1 Рассматриваемая интенсивность отказов является интенсивностью отказов части аппаратных средств и не учитывает эффективность механизмов безопасности.

2 Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае вычисление охвата осуществляется аналогично расчету метрики одиночного сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.3.8 Данное требование распространяется на значение УПБА D цели безопасности. Двойной отказ считается возможным, если:

a) одна или обе участвующие части аппаратных средств имеют охват диагностикой (для скрытых сбоев) менее 90 %; или

b) один из двойного сбоя, вызывающего двойной отказ, остается скрытым в течение времени, превышающего интервал обнаружения множественного сбоя, как определено в требовании 6.4.8.

Примечание — Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае вычисление охвата осуществляется аналогично расчету метрики скрытого сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.3.9 Данное требование распространяется на значение УПБА C цели безопасности. Двойной отказ считается возможным, если:

a) одна или обе участвующие части аппаратных средств имеют охват диагностикой (для скрытых сбоев) менее 80 %; или

b) один из двойного сбоя, вызывающего двойной отказ, остается скрытым в течение времени, превышающего интервал обнаружения множественного сбоя, как определено в требовании 6.4.8.

Примечание — Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае вычисление охвата осуществляется аналогично расчету метрики скрытого сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.3.10 Данное требование распространяется на значения УПБА C и D цели безопасности. Двойной отказ, который не является возможным, должен считаться соответствующим целевому значению цели безопасности и, следовательно, допустимым.

9.4.3.11 Данное требование распространяется на значения УПБА C и D цели безопасности. Двойной сбой, происходящий в части аппаратных средств и способствующий возможному двойному отказу, считается допустимым, если соответствующая часть аппаратных средств соответствует целевым значениям для ранжированного класса интенсивностей отказов и охвата диагностикой (для скрытых сбоев), приведенных в таблице 9.

Примечание — Рассматриваемая интенсивность отказов является интенсивностью отказов части аппаратных средств. Таким образом, она не рассматривает эффективность механизмов безопасности.

Таблица 9 — Целевые значения класса интенсивностей отказов и охвата диагностикой части аппаратных средств для двойных сбоев

УПБА цели безопасности	Охват диагностикой скрытых сбоев		
	≥ 99 %	≥ 90 %	< 90 %
D	Класс 4 интенсивностей отказов	Класс 3 интенсивностей отказов	Класс 2 интенсивностей отказов
C	Класс 5 интенсивностей отказов	Класс 4 интенсивностей отказов	Класс 3 интенсивностей отказов

Примечания

1 Таблица 8 устанавливает связь между классом с максимальной интенсивностью отказов, который позволено задавать целевому значению УПБА, и охватом диагностикой. Классы с более низкой интенсивностью отказов являются приемлемыми, но не требуемыми.

2 «Классы с более низкой интенсивностью отказов» означает классы интенсивностей отказов с более низким номером. Например, «Классы с более низкой интенсивностью отказов» для класса 3 интенсивностей отказов означает классы 2 и 1 интенсивностей отказов.

3 Доля безопасных сбоев части аппаратных средств может быть учтена при определении охвата механизмами безопасности. В этом случае вычисление охвата осуществляется аналогично расчету метрики скрытого сбоя, но на уровне части аппаратных средств, а не на уровне устройства.

9.4.3.12 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Ранжированный класс интенсивностей отказов, используемой в анализе интенсивности отказов части аппаратных средств, должен быть обоснован с помощью источников интенсивностей отказов, описанных в 8.4.3. Если в анализе используются интенсивности отказов от нескольких источников данных, то интенсивности должны быть промасштабированы, как описано в 9.4.2.7.

9.4.4 Отчет по верификации

Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Должен быть подготовлен отчет по верификации анализа, выполняемого в соответствии с набором требований 9.4.2 или 9.4.3 для того, чтобы представить доказательства его технической корректности и полноты в соответствии с требованиями раздела 9 ИСО 26262-8:2011.

9.5 Результаты работы

9.5.1 Анализ нарушений цели безопасности в результате случайных отказов аппаратных средств

В результате выполнения требований 9.4.2 или 9.4.3.

9.5.2 Спецификация специальных мер для аппаратных средств

При необходимости, в том числе обоснование эффективности специальных мер, в результате выполнения требований

9.4.2.4, 9.5.3, 9.4.2.5, 9.4.3.5 и 9.4.3.6.

9.5.3 Экспертный отчет по оценке нарушений цели безопасности в результате случайных отказов аппаратных средств

В результате выполнения требований 9.4.4.

10 Интеграция и тестирование аппаратных средств

10.1 Цель

Целью настоящего раздела является обеспечение, путем проведения испытаний, соответствия разработанных аппаратных средств требованиям к их безопасности.

Требования 10.4.1—10.4.6 применяются к элементу аппаратных средств.

10.2 Общие положения

Целью действий, описанных в настоящем разделе, является интеграция элементов аппаратных средств и тестирование проекта аппаратных средств, чтобы проверить его соответствие требованиям к безопасности аппаратных средств для соответствующего УПБА.

Интеграция и тестирование аппаратных средств отличается от деятельности по квалификации компонентов аппаратных средств, описанной в разделе 13 ИСО 26262-8:2011, которая свидетельствует для компонентов и частей аппаратных средств на промежуточном уровне о пригодности их использования в качестве частей устройств, систем или элементов, разработанных в соответствии с настоящим стандартом.

10.3 Входная информация

10.3.1 Предварительные требования

Следующая информация должна быть доступна:

- план по обеспечению безопасности (уточненный) в соответствии с 5.5;
- план тестирования и интеграции устройства (уточненный) в соответствии с пунктом 5.5.3 ИСО 26262-4;
- спецификация требований к безопасности аппаратных средств в соответствии с 6.5.1;
- спецификация проекта аппаратных средств в соответствии с 7.5.1.

10.3.2 Дополнительная информация

- план проекта (уточненный) (см. пункт 5.5.1 ИСО 26262-4);
- отчет по анализу безопасности аппаратных средств (см. 7.5.2).

10.4 Требования и рекомендации

10.4.1 Действия по интеграции и тестированию аппаратных средств должны быть выполнены в соответствии с требованиями раздела 9 ИСО 26262-8.

10.4.2 Действия по интеграции и тестированию аппаратных средств должны быть согласованы с планом интеграции и тестирования устройства, приведенным в пункте 5.5.5 ИСО 26262-4.

Примечание — Если применяется декомпозиция УПБА, как определено в разделе 5 ИСО 26262-9, то до декомпозиции к УПБА применяются соответствующие мероприятия по интеграции декомпозированных элементов, а также дополнительные действия.

10.4.3 Испытательное оборудование должно быть под контролем системы мониторинга качества.

10.4.4 Чтобы сформировать необходимые тестовые примеры для выбранных тестов интеграции аппаратных средств, необходимо использовать подходящую комбинацию методов, перечисленных в таблице 10.

Таблица 10 — Методы получения тестовых примеров для тестирования интеграции аппаратных средств

Методы		УПБА			
		A	B	C	D
1a	Анализ требований	++	++	++	++
1b	Анализ внешних и внутренних интерфейсов	+	++	++	++
1c	Генерация и анализ классов эквивалентности[a)]	+	+	++	++
1d	Анализ граничных значений[b)]	++	++	++	++
1e	Ошибки, предполагаемые на основе знаний и опыта[c)]	+	+	++	++
1f	Анализ функциональных зависимостей	+	+	++	++
1g	Анализ общих предельных условий, последовательностей и источников зависимых отказов	+	+	++	++
1h	Анализ состояния окружающей среды и прецедентов эксплуатации	+	++	++	++
1i	Стандарты, если существуют[d)]	+	+	+	+
1j	Анализ значимых вариантов[e)]	++	++	++	++

[a)] Для того чтобы эффективно получить необходимые тесты, может быть выполнен анализ сходств.

[b)] Например, значения, приближающиеся к границам и пересекающие границы между указанными значениями, и значения извне диапазона указанных значений.

[c)] «Тесты, предполагаемых ошибок» могут быть основаны на данных, собранных в процессе обучения, или из экспертной оценки, или из обоих источников. Может быть использован FMEA.

[d)] Существующие стандарты включают ИСО 16750 и ИСО 11452.

[e)] Анализ значимых вариантов включает в себя анализ на наихудший случай.

10.4.5 Действия по интеграции и тестированию аппаратных средств должны включать проверку полноты и корректности реализации механизмов безопасности в соответствии с требованиями к безопасности аппаратных средств.

Для достижения этих целей, должны быть рассмотрены методы, перечисленные в таблице 11.

Таблица 11 — Тесты интеграции аппаратных средств для проверки полноты и корректности реализации механизмов безопасности в соответствии с требованиями к безопасности аппаратных средств

Методы		УПБА			
		A	B	C	D
1	Функциональное тестирование[a)]	++	++	++	++
2	Тестирование с введением неисправности[b)]	+	+	++	++
3	Тестирование электрических параметров[c)]	++	++	++	++

[a)] Функциональное тестирование направлено на проверку достижения устройством специфицированных характеристик. На вход устройства подаются данные, которые адекватно характеризует его предполагаемую нормальную работу. Выходные данные сравниваются с приведенными в спецификации. Отклонения от спецификации и признаки неполноты спецификации анализируются.

[b)] Тестирование с введением неисправности основано на включении сбоев в аппаратные изделия и на анализе полученной реакции. Это тестирование применяется, когда определен механизм безопасности. Применимо также моделирование введения сбоя (например, введение сбоя в модель логической схемы на основе списка соединений) особенно, когда тестирование с введением сбоя очень трудно выполнить для реального аппаратного изделия. Например, демонстрацию реакции механизмов безопасности на кратковременные сбои в частях аппаратных средств, таких как микроконтроллер, очень трудно реализовать введением сбоев в аппаратные средства на уроне изделия, так как это требует тесты с облучением.

[c)] Электрические испытания направлены на проверку соблюдения требований к безопасности аппаратных средств внутри специфицированного (статического и динамического) диапазона напряжений.

10.4.6 Действия по интеграции и тестированию аппаратных средств должны включать проверку надежности аппаратных средств при внешних стрессовых воздействиях.

Для достижения этих целей, должны быть рассмотрены методы, перечисленные в таблице 12.

Таблица 12 — Тесты интеграции аппаратных средств для проверки надежности и работы под воздействием внешних стрессовых воздействиях

Методы		УПБА			
		A	B	C	D
1a	Испытания на воздействие окружающих условий при выполнении проверки основных функций[a)]	++	++	++	++
1b	Расширенное функциональное испытание[b)]	+	++	++	++
1c	Статистический тест[c)]	+	+	++	++
1d	Тестирование на наихудший случай[d)]	++	++	++	++
1e	Тестирование в запредельных условиях[e)]	+	+	++	++
1f	Механическое испытание[f)]	+	+	++	++
1g	Ускоренное испытание на долговечность[g)]	+	+	++	++
1h	Испытание на механическую износостойкость[h)]	+	++	++	++
1i	Испытание на электромагнитную совместимость и на устойчивость к электростатическим разрядам[i)]	+	+	+	+
1j	Химические испытания[j)]	++	++	++	++

[a)] Во время испытаний на воздействие окружающих условий при выполнении проверки основных функций аппаратные средства помещаются в различные условия окружающей среды и оценивается выполнение требований к аппаратным средствам. Может быть применен ИСО 16750-4.

Окончание таблицы 12

[b] Расширенное функциональное тестирование проверяет функциональное поведение устройства для редко встречающихся значений входных условий (например, экстремальные значения циклограммы), или находящихся за пределами спецификации аппаратного средства (например, неправильная команда). В таких ситуациях, наблюдаемое поведение элемента аппаратных средств сравнивается со специфицированными требованиями.

[c] Статистические тесты выполняют проверку элемента аппаратных средств, на вход которого подаются данные, выбранные в соответствии с ожидаемым статистическим распределением реальной циклограммы. Критерии приемлемости определяются тем, что статистическое распределение результатов подтверждает требуемую интенсивность отказов.

[d] Тестирование на наихудший случай выполняют проверку ситуаций, выявленных в результате анализа на наихудший случай. В таком тесте, условия окружающей среды меняются до их максимально допустимых предельных значений, определенных в спецификации. Проверяется соответствующая реакция аппаратных средств и сравнивается со специфицированными требованиями.

[e] При тестировании в запредельных условиях элементы аппаратных средств проверяются при экологических или функциональных ограничениях, постепенно увеличивающихся до значений более серьезных, чем для них специфицировано, пока они не перестают работать, или они будут разрушены. Целью этого теста является определение запаса прочности тестируемых элементов, относительно требуемых показателей работы.

[f] Механическое испытание распространяется на механические свойства, такие как прочность на разрыв.

[g] Ускоренное испытание на долговечность направлено на предсказание поведения в процессе эволюции изделия в нормальных условиях эксплуатации. При ускоренном испытании изделие подвергая его более высоким нагрузкам, чем ожидалось в течение его срока службы. Ускоренные испытания основаны на аналитической модели ускорения влияния вида отказов.

[h] Целью этих испытаний является определение среднего времени до отказа или максимального числа циклов, которое элемент может выдержать. Тест может выполняться до отказа или получения повреждения.

[i] Для испытаний на электромагнитную совместимость могут быть применены ИСО 7637-2, ИСО 7637-3, ИСО 10605, ИСО 11452-2 и ИСО 11452-4, а на устойчивость к электростатическим разрядам — ИСО 16750-2.

[j] Для химических испытаний может быть применен ИСО 16750-5.

10.5 Результаты работы

10.5.1 Отчет по интеграции и тестированию аппаратных средств

В результате выполнения требований 10.4.1—10.4.6.

Приложение А
(справочное)

Обзор и поток документов стадии разработки аппаратных средств изделия

Таблица А.1 содержит обзор целей, предварительных условий и результатов работы конкретных стадий разработки аппаратных средств изделия.

Таблица А.1 — Обзор разработки аппаратных средств изделия

Раздел	Цели	Предварительные требования	Результаты работы
5 Инициирование разработки аппаратных средств изделия	Цель инициирования разработки аппаратных средств изделия заключается в определении и планировании действий по обеспечению функциональной безопасности для отдельных подстадий разработки аппаратных средств. Кроме того, необходимо включить вспомогательные процессы, описанные в ИСО 26262-8. Эти спланированные действия по обеспечению безопасности конкретных аппаратных средств будут включены в план по обеспечению безопасности (см. 6.4.3 ИСО 26262-2 и 5.4 ИСО 26262-4)	План проекта (уточненный) (см. 5.5.1 ИСО 26262-4). План по обеспечению безопасности (уточненный) (см. 5.5.2 ИСО 26262-4). План интеграции и тестирования устройства (уточненный) (см. 5.5.3 ИСО 26262-4)	5.5.1 План по обеспечению безопасности (уточненный)
6 Спецификация требований к аппаратным средствам системы безопасности	Первой целью настоящего раздела является формирование спецификации требований к аппаратным средствам системы безопасности. Они выводятся из технической концепции обеспечения безопасности и спецификации проекта системы. Второй целью является проверка согласованности требований к аппаратным средствам системы безопасности с технической концепцией обеспечения безопасности и спецификацией проекта системы. Третьей целью настоящего раздела является формирование подробной спецификации программно-аппаратного интерфейса, инициированного в разделе 7 ИСО 26262-4	План по обеспечению безопасности (уточненный) (см. 5.5). Техническая концепция обеспечения безопасности (см. 7.5.1 ИСО 26262-4). Спецификация проекта системы (см. 7.5.2 ИСО 26262-4). Спецификация программно-аппаратного интерфейса (см. 7.5.3 ИСО 26262-4)	6.5.1 Спецификация требований к аппаратным средствам системы безопасности (включая квалификационные критерии и критерии тестирования). 6.5.2 Спецификация программно-аппаратного интерфейса (уточненная). 6.5.3 Отчет о верификации требований аппаратных средств системы безопасности
7 Проектирование аппаратных средств	Первой целью данного раздела является разработка аппаратных средств в соответствии со спецификацией проекта системы и требованиями к аппаратным средствам системы безопасности. Второй целью данного раздела является проверка проекта аппаратных средств на соответствие спецификации проекта системы и требований к аппаратным средствам системы безопасности	Спецификация требований к аппаратным средствам системы безопасности (см. 6.5.1). Спецификация программно-аппаратного интерфейса (уточненная) (см. 6.5.2). Спецификация проекта системы см. 7.5.2 ИСО 26262-4). План по обеспечению безопасности (уточненный) (см. 5.5)	7.5.1 Спецификация проекта аппаратных средств. 7.5.2 Отчет по анализу безопасности аппаратных средств. 7.5.3 Отчет о верификации проекта аппаратных средств. 7.5.4 Спецификация требований к производству, эксплуатации, обслуживанию и выводу из эксплуатации

Окончание таблицы А.1

Раздел	Цели	Предварительные требования	Результаты работы
8 Оценка метрик архитектуры аппаратных средств	Целью настоящего раздела является оценка архитектуры аппаратных средств устройства на соответствие требованиям к обработке сбоев с помощью метрик архитектуры аппаратных средств	Спецификация требований к аппаратным средствам системы безопасности (см. 6.5.1). Спецификация проекта аппаратных средств (см. 7.5.1). Отчет по анализу безопасности аппаратных средств (см. 7.5.2)	8.5.1 Анализ эффективности архитектуры устройства по предотвращению случайных отказов аппаратных средств. 8.5.2 Отчет группы экспертов об эффективности архитектуры устройства по предотвращению случайных отказов аппаратных средств
9 Оценка нарушений цели безопасности из-за случайных отказов аппаратных средств	Целью требований настоящего раздела является формирование доступных критериев для обоснования того, что остаточный риск нарушения цели безопасности из-за случайных отказов аппаратных средств устройства, является достаточно низким	Спецификация требований к аппаратным средствам системы безопасности (см. 6.5.1). Спецификация проекта аппаратных средств (см. 7.5.1). Отчет по анализу безопасности аппаратных средств (см. 7.5.2)	9.5.1 Анализ нарушений цели безопасности в результате случайных отказов аппаратных средств. 9.5.2 Спецификация специальных мер для аппаратных средств. 9.5.3 Экспертный отчет по оценке нарушений цели безопасности в результате случайных отказов аппаратных средств
10 Интеграция и тестирование аппаратных средств	Целью настоящего раздела является обеспечение, путем проведения испытаний, соответствия разработанных аппаратных средств требованиям к их безопасности	План по обеспечению безопасности (уточненный) (см. 5.5). План тестирования и интеграции устройства (уточненный) (см. 5.5.3 ИСО 26262-4). Спецификация требований к безопасности аппаратных средств (см. 6.5.1). Спецификация проекта аппаратных средств (см. 7.5.1)	10.5.1 Отчет по интеграции и тестированию аппаратных средств

Приложение В
(справочное)

Классификация видов отказов элементов аппаратных средств

Виды отказов элементов аппаратных средств могут быть классифицированы, как показано на рисунке В.1. Блок-схема, представленная на рисунке В.2, описывает, как вид отказа элемента аппаратных средств может попасть в одну из этих классификаций.

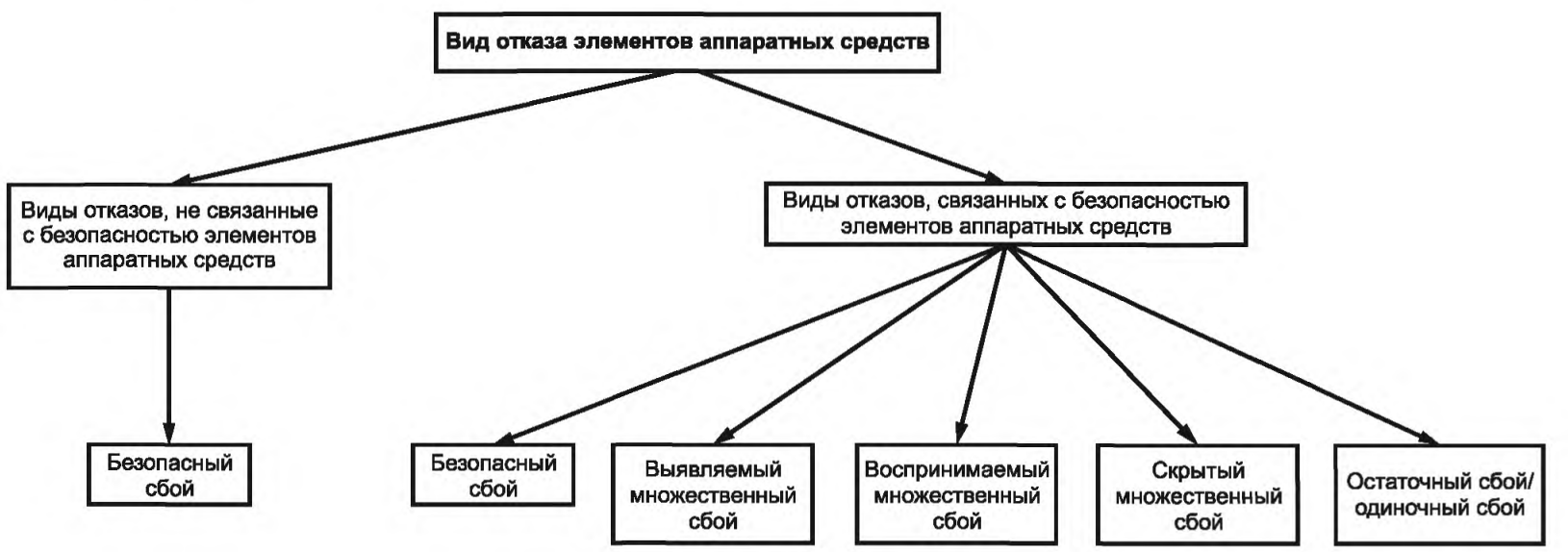
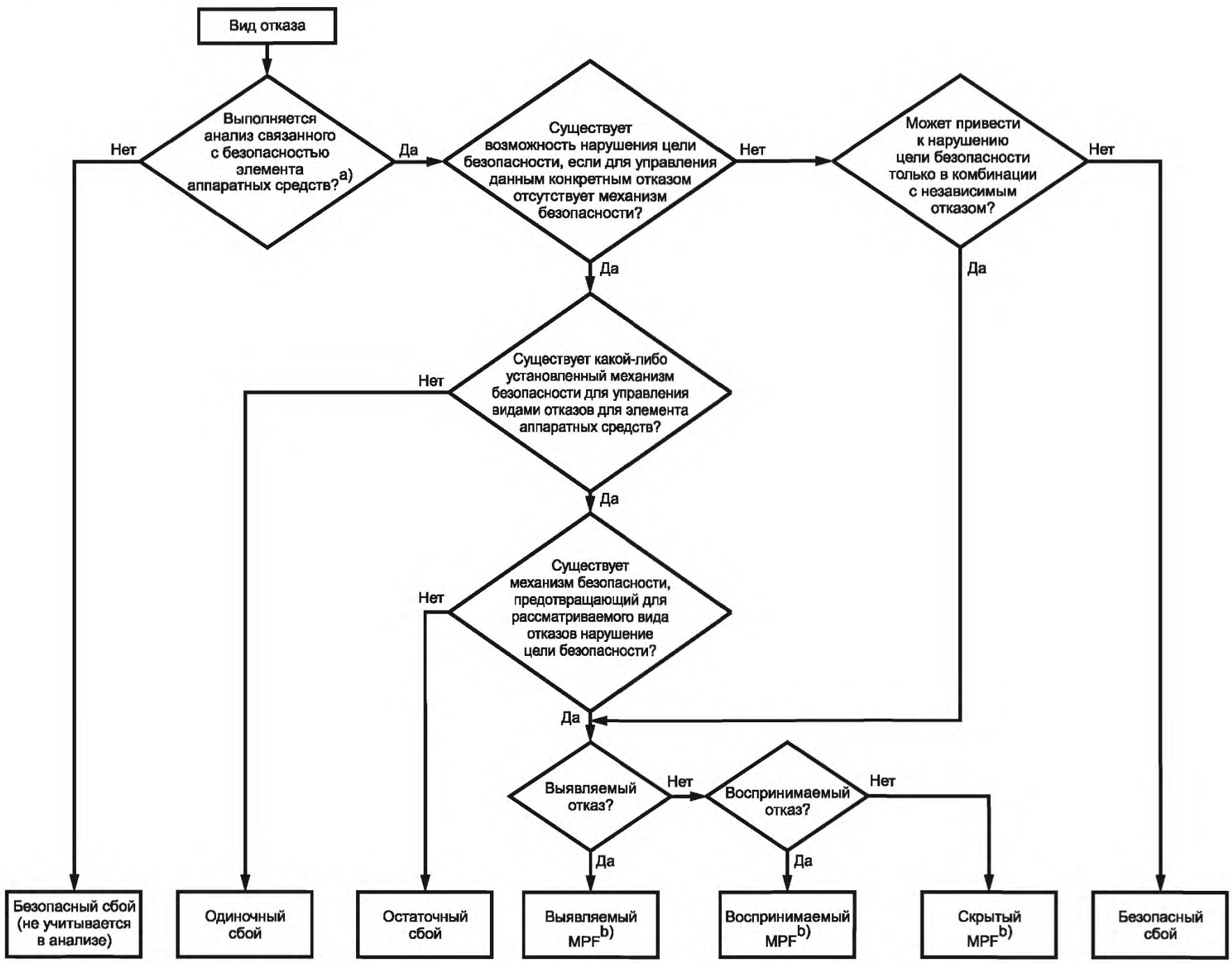


Рисунок В.1 — Классификация видов отказов элементов аппаратных средств



a) Элементы с отказами, которые несущественно увеличивают вероятность нарушения цель безопасности, могут быть исключены из анализа и их виды отказов могут быть классифицированы как безопасные отказы, например, элементы аппаратных средств, сбои которых вносят вклад только в множественные отказы с $n > 2$, если только они не рассматриваются в технической концепции обеспечения безопасности.

b) MPF означает множественный сбой.

Примечания

1 Множественные сбои с n > 2 считаются безопасными сбоями, если они не рассматриваются в технической концепции обеспечения безопасности.

2 Один и тот же сбой может быть отнесен к различным классам, если рассматриваются различные цели безопасности.

Рисунок В.2 — Пример классификации видов отказов

Приложение С
(обязательное)

Метрики архитектуры аппаратных средств

С.1 Классификация и охват диагностикой сбоев

С.1.1 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Метрики архитектуры аппаратных средств должны быть определены для аппаратных средств устройства и только для связанных с безопасностью элементов аппаратных средств, у которых существует возможность внести существенный вклад в нарушение цели безопасности.

Пример — Элементы аппаратных средств, множественные сбои которых имеют n > 2, могут быть исключены из расчетов, если они не рассматриваются в технической концепции обеспечения безопасности.

С.1.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Каждый сбой, происходящий в связанном с безопасностью элементе аппаратных средств, должен быть классифицирован в соответствии с рисунком В.1, как:

a) одиночный сбой;
b) остаточный сбой.

Пример — Элемент аппаратных средств может иметь сбои «обрыв цепи», «короткое замыкание на массу», и «короткое замыкание на линию высокого напряжения», но только сбои «обрыв цепи» и «короткое замыкание на массу» охватываются механизмами безопасности. Сбой «короткое замыкание на линию высокого напряжения» является остаточным сбоем, так как он не охватывается механизмом безопасности, если он приводит к нарушению заданной цели безопасности;

c) множественный сбой;
d) безопасный сбой.

Рисунок С.1 дает графическое представление классификации сбоев связанных с безопасностью элементов аппаратных средств устройства.

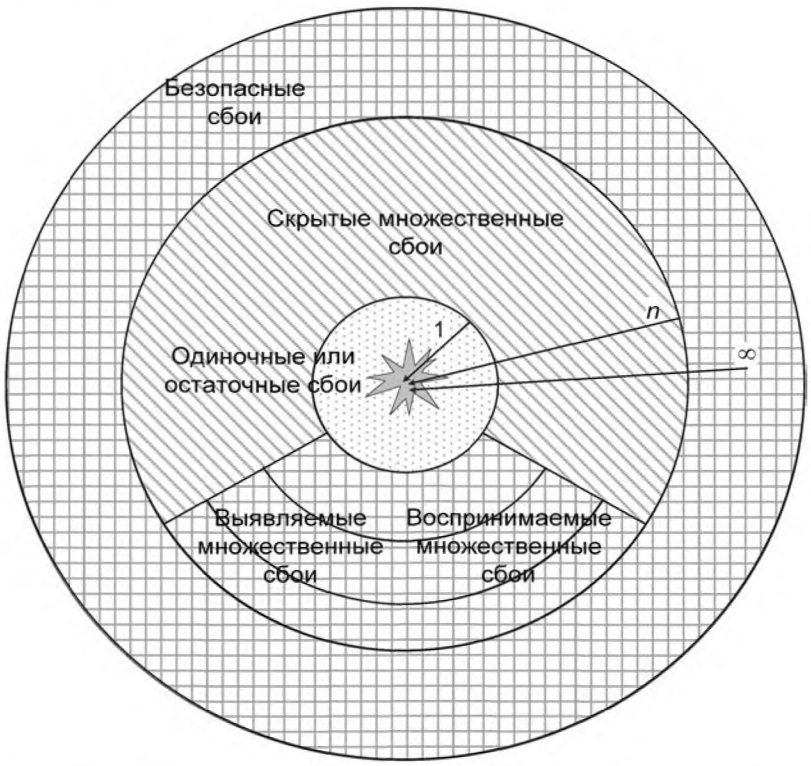


Рисунок С.1 — Классификация сбоев связанных с безопасностью элементов аппаратных средств устройства

В этом графическом представлении:

- расстояние n представляет собой число независимых одновременно присутствующих сбоев, вызывающих нарушение цели безопасности (n = 1 для одиночного или остаточного сбоя, n = 2 для двойного сбоя и т. д.);
- сбои с расстоянием, равным до значения n, расположены в районе между окружностями n и n – 1;
- множественные сбои с расстоянием строго больше n = 2 следует рассматривать как безопасные сбои, если они не рассматриваются в технической концепции обеспечения безопасности.

Примечание — Кратковременные сбои, для которых механизм безопасности возвращает устройство в состояние без сбоя, можно рассматривать как выявляемые множественные сбои, даже если водитель никогда не сообщал об их существовании.

Пример — В случае использования кода коррекции ошибок для защиты памяти от кратковременных сбоев, устройство будет возвращаться в состояние без сбоя, если механизм безопасности, кроме передачи корректного значения в ЦП, изменяет значение ошибочного бита на обратное внутри массива памяти (например, путем перезаписи скорректированного значения).

Интенсивность отказов λ каждого связанного с безопасностью элемента аппаратных средств может быть поэтому выражена в соответствии с уравнением (С.1) (предполагая, что все сбои независимы и распределены экспоненциально), а именно:

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}, \quad (C.1)$$

где λ_{SPF} — интенсивность отказов, связанных с одиночными сбоями элемента аппаратных средств;

λ_{RF} — интенсивность отказов, связанных с остаточными сбоями элемента аппаратных средств;

λ_{MPF} — интенсивность отказов, связанных с множественными сбоями элемента аппаратных средств;

λ_{S} — интенсивность отказов, связанных с безопасными сбоями элемента аппаратных средств.

Интенсивность отказов, связанных с множественными сбоями элемента аппаратных средств λ_{MPF}, может быть выражена уравнением (С.2) следующим образом:

$$\lambda_{MPF} = \lambda_{MPF,\,DP} + \lambda_{MPF,\,L}, \quad (C.2)$$

где $\lambda_{MPF,\,DP}$ — интенсивность отказов, связанных с воспринимаемыми или выявляемыми множественными сбоями элемента аппаратных средств;

$\lambda_{MPF,\,L}$ — интенсивность отказов, связанных со скрытыми сбоями элемента аппаратных средств.

Интенсивность отказов, связанных с остаточными сбоями, может быть определена с помощью охвата диагностикой механизмов безопасности, которые предотвращают множественные сбои элемента аппаратных средств. Уравнение (С.3) дает консервативную оценку интенсивности отказов, связанных с остаточными сбоями:

$$K_{DC,\,RF} = (1 - \lambda_{RF,\,est}/\lambda) \times 100,$$

$$\lambda_{RF} \le \lambda_{RF,\,est} = \lambda \times (1 - K_{DC,\,RF}/100), \quad (C.3)$$

где $\lambda_{RF,\,est}$ — расчетная интенсивность отказов, связанных с остаточными сбоями;

$K_{DC,\,RF}$ — значение охвата диагностикой остаточных сбоев, выраженное в процентах.

Интенсивность отказов, связанных со скрытыми сбоями, может быть определена с помощью охвата диагностикой механизмов безопасности, которые предотвращают скрытые сбои элемента аппаратных средств. Уравнение (С.4) дает консервативную оценку интенсивности отказов, связанных со скрытыми сбоями:

$$K_{DC,\,MPF,L} = (1 - \lambda_{MPF,\,L,\,est}/\lambda) \times 100,$$

$$\lambda_{MPF,\,L} \le \lambda_{MPF,\,est} = \lambda \times (1 - K_{DC,\,MPF,\,L}/100), \quad (C.4)$$

где $\lambda_{MPF,\,L,\,est}$ — расчетная интенсивность отказов, связанных со скрытыми сбоями;

$K_{DC,\,MPF,\,L}$ — значение охвата диагностикой скрытых сбоев, выраженное в процентах.

Примечания

1 Для данной цели может быть использовано приложение D в качестве основного подхода для расчета заявленного охвата диагностикой и его поддержки надлежащим обоснованием.

2 Если рассмотренные выше оценки считаются слишком консервативными, то детальный анализ видов отказов элемента аппаратных средств может отнести каждый вид отказов к одному из классов сбоев (одиночные сбои, остаточные сбои, скрытые, выявляемые или воспринимаемые множественные сбои или безопасные сбои) для заданной цели безопасности и определить интенсивности каждого вида отказов. Для классификации сбоев может быть использована блок-схема приложения В.

С.2 Метрика одиночного сбоя

С.2.1 Данная метрика отражает устойчивость устройства к одиночным и остаточным сбоям, которая реализуется или охватом механизмами безопасности или в процессе проектирования (в основном допускаются безопасные сбои). Большое значение метрики одиночного сбоя означает, что отношение одиночных сбоев к остаточным сбоям в аппаратных средствах устройства является низким.

С.2.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для определения метрики одиночного сбоя необходимо использовать уравнение (С.5):

$$1 - \frac{\sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW}\lambda} = \frac{\sum_{SR,HW}(\lambda_{MPF} + \lambda_{S})}{\sum_{SR,HW}\lambda}, \quad (C.5)$$

где $\sum_{SR,HW}\lambda_x$ является суммой значений λ_x, связанных с безопасностью элементов аппаратных средств устройства для рассматриваемых метрик.

Примечания

1 Для данной метрики рассматриваются только связанные с безопасностью элементы аппаратных средств устройства, отказы которых могут внести существенный вклад в нарушение цели безопасности.

Пример — Элементы аппаратных средств, множественные сбои которых имеют n > 2, могут быть исключены из расчетов, если эти сбои не рассматриваются в технической концепции обеспечения безопасности.

2 Рисунок С.2 дает графическое представление метрики одиночного сбоя.

3 Пример расчета метрики скрытого сбоя приведен в приложении Е.

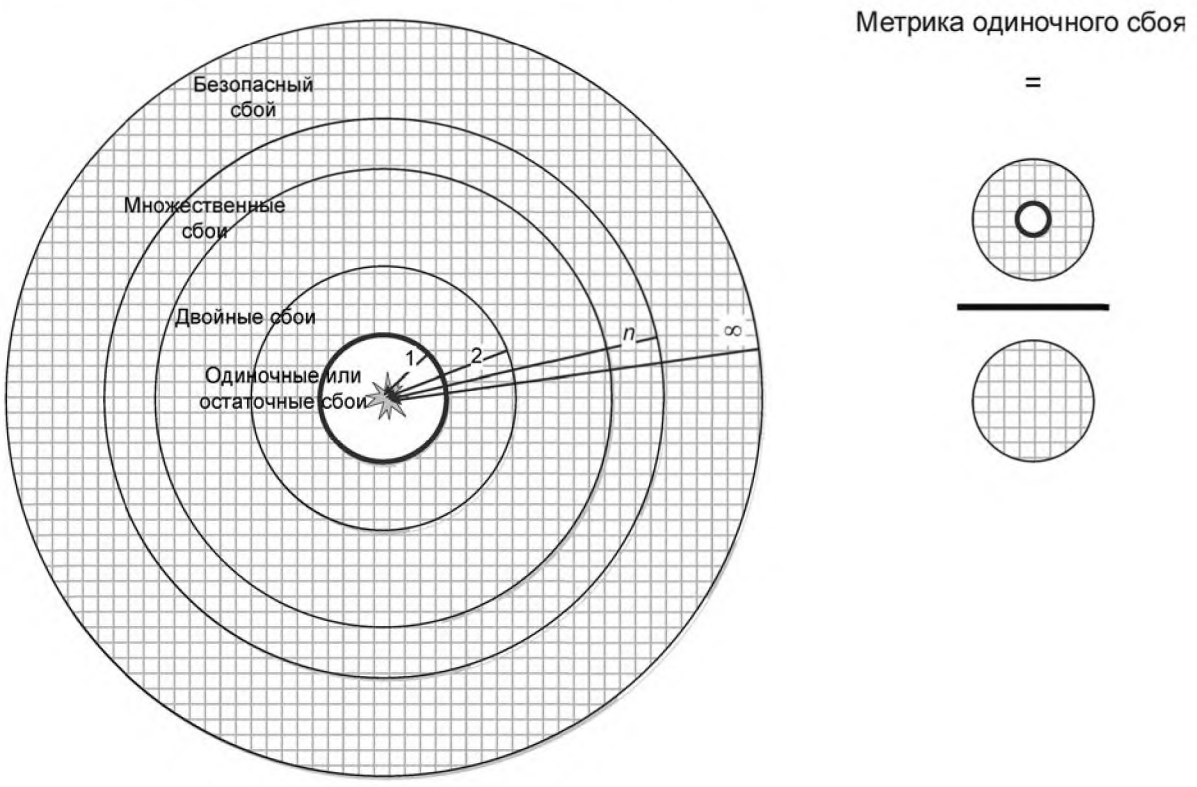


Рисунок С.2 — Графическое представление метрики одиночного сбоя

С.3 Метрика скрытого сбоя

С.3.1 Данная метрика отражает устойчивость устройства к скрытым сбоям, которая реализуется или охватом сбоев механизмами безопасности или самим водителем, понимающим, что перед нарушением цели безопасности происходит сбой, или в процессе проектирования (в основном допускаются безопасные сбои). Большое значение метрики скрытого сбоя означает, что часть скрытых сбоев в аппаратных средствах устройства низка.

С.3.2 Данное требование распространяется на значения УПБА (B), C и D цели безопасности. Для определения метрики скрытого сбоя необходимо использовать уравнение (С.6):

$$1 - \frac{\sum_{SR,HW}(\lambda_{MPF,latent})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR,HW}(\lambda_{MPF,\text{perceived или detected}} + \lambda_S)}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}, \quad (C.6)$$

где $\sum_{SR,HW}\lambda_x$ является суммой значений λ_x, связанных с безопасностью элементов аппаратных средств устройства для рассматриваемых метрик.

Примечания

1 Для данной метрики рассматриваются только связанные с безопасностью элементы аппаратных средств устройства, отказы которых могут внести существенный вклад в нарушение цели безопасности.

Пример — Элементы аппаратных средств, множественные сбои которых имеют n > 2, могут быть исключены из расчетов, если эти сбои не рассматриваются в технической концепции обеспечения безопасности.

2 Рисунок С.3 дает графическое представление метрики скрытого сбоя.

3 Пример расчета метрики скрытого сбоя приведен в приложении Е.

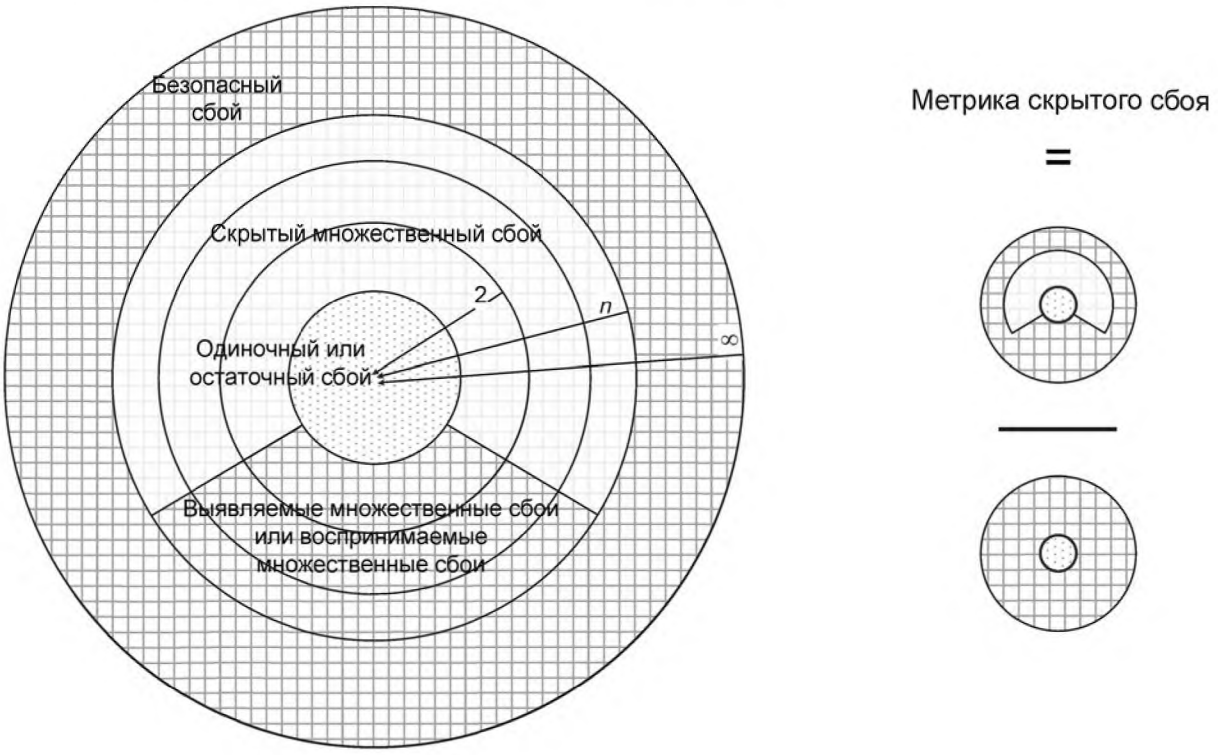


Рисунок С.3 — Графическое представление метрики скрытого сбоя

Приложение D
(справочное)

Оценка охвата диагностикой

D.1 Общие положения

Данное приложение предназначено для использования:

a) при оценке охвата диагностикой для получения обоснования:

1) соответствия с метриками одиночного сбоя и скрытого сбоя, определенными в разделе 8;

2) соответствия оценки нарушения цели безопасности из-за случайных отказов аппаратных средств, как это определено в разделе 9;

b) в качестве руководства по выбору соответствующих механизмов безопасности, которые должны быть реализованы в Э/Э архитектуре для обнаружения отказов элементов.

На рисунке D.1 представлена общая структура аппаратных средств встроенной системы. Типичные сбои или отказы элементов аппаратных средств этой системы приведены в таблице D.1, которая также включает рекомендации для охвата диагностикой. Каждый элемент из левой колонки связан с одним или более сбоями, которые рассматриваются в правых от элемента колонках. Перечень не претендует на полноту и может быть дополнен известными сбоями или связанными с конкретным применением.

На дополнительные подробности о механизмах безопасности, связанных с этими сбоями элементов, в каждой строке дается ссылка (на таблицы D.2—D.14). Эффективность этих типовых механизмов безопасности для данных элементов категоризируется в соответствии с их способностью охвата вышеперечисленных сбоев для достижения низкого (60 %), среднего (90 %) или высокого (99 %) охвата диагностикой этого элемента.

Определение для сбоев и соответствующих им механизмов безопасности уровней охвата диагностикой может отличаться от представленного в таблице D.1 в зависимости от:

c) разнообразия источников вида сбоя, выявляемого диагностикой;

d) эффективности механизма безопасности;

e) конкретной реализации механизма безопасности;

f) выполнения во времени механизма безопасности (периодичности);

g) реализованных в системе технологий аппаратных средств;

h) вероятности видов отказов аппаратных средств системы;

i) результатов более детального анализа сбоев и их классификации на ряд подклассов с различными уровнями охвата диагностикой.

Таким образом, таблица D.1 содержит рекомендации, которые могут быть адаптированы в результате анализа элементов системы.

Эти рекомендации не учитывают конкретные ограничения, которые могут быть указаны в концепции безопасности во избежание нарушения целей безопасности. Эти ограничения, такие как временные аспекты (периодичность диагностики), например, не учитываются при оценке общего типового охвата диагностикой механизмом безопасности. Они будут рассмотрены при оценке конкретного охвата диагностикой механизмом безопасности, используемым в устройстве, чтобы избежать нарушения его целей безопасности.

Пример — Механизм безопасности может обеспечить высокое значение общего типового охвата диагностикой в настоящем приложении, но если используемый интервал диагностических проверок больше, чем интервал диагностических проверок, необходимый для обеспечения соответствующего интервала сбоеустойчивости, то конкретный охват диагностикой по отношению к предотвращению нарушения цели безопасности, будет значительно ниже.

Поэтому таблицы D.1—D.14 могут быть использованы для начальной оценки охвата диагностикой этими механизмами безопасности с заявленными значениями охвата диагностикой, поддерживаемыми надлежащими обоснованиями. Кроме того, данная информация предназначена, чтобы помочь определить виды сбоев или отказов элемента; однако соответствующие виды отказов в конечном счете зависят от применения, в котором используются эти элементы.

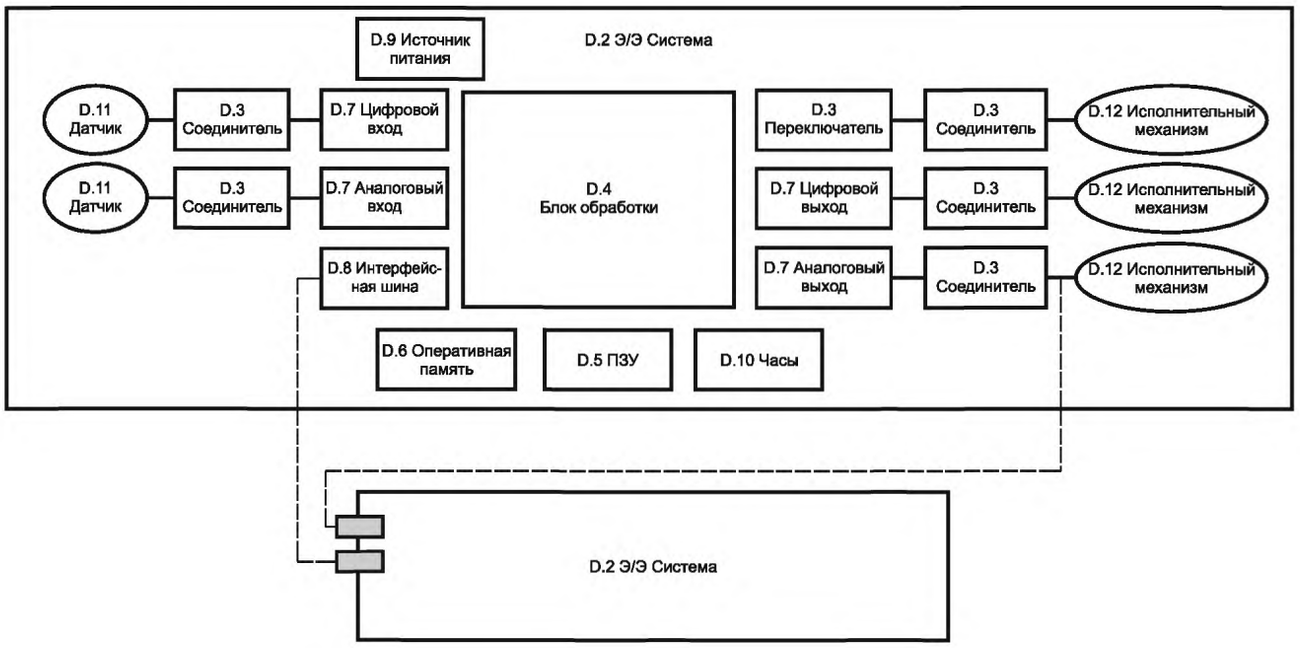


Рисунок D.1 — Общая структура аппаратных средств системы

Таблицы D.2—D.14 поддерживают информацией таблицу D.1, давая рекомендации по методам диагностических тестов. Методы и средства, представленные в таблицах D.1—D.14, не являются исчерпывающими. Могут быть использованы и другие методы, если представлены свидетельства, что они поддерживают необходимый охват диагностикой. Если это обосновано, то можно оценить более высокий охват диагностикой, до 100 % для простых или сложных элементов.

Т а б л и ц а D.1 — Виды сбоев и отказов, которые подлежат рассмотрению при определении охвата диагностикой

Элемент	См. таблицы	Анализируемые виды отказов для охвата диагностикой 60 %, 90 % и 99 %		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Общие элементы				
Э/Э системы	D.2	Нет общей модели сбоя. Необходим детальный анализ	Нет общей модели сбоя. Необходим детальный анализ	Нет общей модели сбоя. Необходим детальный анализ
Электрические элементы				
Реле	D.3	Не включение или не отключение. Приваренные контакты	Не включение или не отключение. Отдельные приваренные контакты	Не включение или не отключение. Отдельные приваренные контакты.
Соединительные жгуты, включая холодную пайку и разъемы		Обрыв цепи. Короткое замыкание на массу	Обрыв цепи. Короткое замыкание на массу (связь по постоянному току). Короткое замыкание напряжения аккумулятора. Короткое замыкание между соседними контактами	Обрыв цепи. Короткое замыкание на массу (связь по постоянному току). Короткое замыкание напряжения аккумулятора. Короткое замыкание между соседними контактами. Дрейф сопротивления между контактами

Продолжение таблицы D.1

Элемент	См. таблицы	Анализируемые виды отказов для охвата диагностикой 60 %, 90 % и 99 %		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Датчики, включая переключатели сигналов	D.11	Нет общей модели сбоя. Необходим детальный анализ. Типичные виды охватываемых отказов: - недопустимые значения; - константные в рабочем диапазоне	Нет общей модели сбоя. Необходим детальный анализ. Типичные виды охватываемых отказов: - недопустимые значения; - смещения; - константные в рабочем диапазоне	Нет общей модели сбоя. Необходим детальный анализ. Типичные виды охватываемых отказов: - недопустимые значения; - смещения; - константные в рабочем диапазоне; - колебания
Исполнительные элементы (исполнительный механизм, сигнальные лампы, звуковое устройство, дисплей компьютера)	D.12	Нет общей модели сбоя. Необходим детальный анализ	Нет общей модели сбоя. Необходим детальный анализ	Нет общей модели сбоя. Необходим детальный анализ
Общие полупроводниковые элементы				
Источник питания	D.9	Пониженное и повышенное напряжение	Дрейф. Пониженное и повышенное напряжение	Дрейф и колебания. Пониженное и повышенное напряжение. Перепады напряжения
Устройство синхронизации	D.10	Константные отказы[a)]	Сбои при постоянном токе[b)]	Модель сбоя при постоянном токе[b)]. Некорректная частота. Периодическая неустойчивость синхронизации
Постоянная память	D.5	Константные отказы[a)] в данных и адресах, а также в интерфейсах управления, шинах управления и управляющей логике	Сбои при постоянном токе[b)] в данных и адресах (включая адресные шины в том же блоке), а также в интерфейсах управления, шинах управления и управляющей логике	Модель сбоя при постоянном токе[b)] в данных и адресах (включая адресные шины в том же блоке), а также в интерфейсах управления, шинах управления и управляющей логике
Память с произвольным доступом	D.6	Константные отказы[a)] в данных и адресах, а также в интерфейсах управления, шинах управления и управляющей логике	Сбои при постоянном токе[b)] в данных и адресах (включая адресные шины в том же блоке и неспособность записать в ячейку), а также в интерфейсах управления, шинах управления и управляющей логике. Исправимая ошибка[c)] одноразрядного регистра	Модель сбоя при постоянном токе[b)] в данных и адресах (включая адресные шины в том же блоке и неспособность записать в ячейку), а также в интерфейсах управления, шинах управления и управляющей логике. Исправимая ошибка[c)] одноразрядного регистра

Продолжение таблицы D.1

Элемент		См. таблицы	Анализируемые виды отказов для охвата диагностикой 60 %, 90 % и 99 %		
			Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Цифровое устройство ввода/вывода		D.7	Константные отказы[a] (включая внешние для микроконтроллера сигнальные линии)	Сбои при постоянном токе[b] (включая внешние для микроконтроллера сигнальные линии)	Модель сбоя при постоянном токе[b] (включая внешние для микроконтроллера сигнальные линии). Дрейф и колебания
Аналоговое устройство ввода/вывода			Константные отказы[a] (включая внешние для микроконтроллера сигнальные линии)	Сбои при постоянном токе[b] (включая внешние для микроконтроллера сигнальные линии). Дрейф и колебания	Сбои при постоянном токе[b] (включая внешние для микроконтроллера сигнальные линии). Дрейф и колебания
Модули обработки	АЛУ — информационные каналы	D.4/D.13	Константные отказы[a]	Константные отказы[a] на уровне логического элемента	Модель сбоя при постоянном токе[b]. Исправимая ошибка[c] (для последовательностных схем)
	Регистры (блок регистров общего назначения, регистры DMA), внутреннее ЗУ	D.4	Константные отказы[a]	Константные отказы[a] на уровне логического элемента. Исправимая ошибка[c] (для последовательностных схем)	Модель сбоя при постоянном токе[b], включая отсутствие, неверную или множественную адресацию. Исправимая ошибка[c]
	Вычисление адреса (блок загрузки и хранения, логика адресации DMA, память и шины интерфейсов)	D.4/D.5/ D.6	Константные отказы[a]	Константные отказы[a] на уровне логического элемента	Модель сбоя при постоянном токе[b], включая отсутствие, неверную или множественную адресацию. Исправимая ошибка[c] (для последовательностных схем)
	Устройство обработки прерываний	D.4/D.10	Пропуск прерывания или непрерывные прерывания	Пропуск прерывания или непрерывные прерывания. Некорректное выполнение прерывания	Пропуск прерывания или непрерывные прерывания. Некорректное выполнение прерывания. Неверный приоритет. Медленное или подверженное влиянию помех устройство обработки прерываний вызывает пропуски или задержки в обслуживании прерываний
	Управляющая логика (контроллер последовательности, логика кодирования и выполнения, включая управление регистром признаков и стеком)	D.4/D.10	Нет выполнения кода. Выполнение очень медленное. Переполнение стека/потеря значимости	Неправильный код или нет выполнения. Выполнение очень медленное. Переполнение стека/потеря значимости	Неправильный код или нет выполнения. Некорректное выполнение. Выполнение очень быстрое или очень медленное. Переполнение стека/потеря значимости

Продолжение таблицы D.1

Элемент		См. таблицы	Анализируемые виды отказов для охвата диагностикой 60 %, 90 % и 99 %		
			Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Модули обработки	Регистры конфигурации	D.4	—	Неправильное значение константного отказа[a)]	Искажение данных в регистрах (исправимые ошибки). Модель сбоя при константном отказе[a)]
	Другие подэлементы, не принадлежащие предыдущим классам	D.4/D.13	Константные отказы[a)]	Константные отказы[a)] на уровне логического элемента	Модель сбоя при постоянном токе[b)]. Модель исправимой ошибки[c)] (для последовательностных схем)
Коммуникация	Коммуникация на кристалле, включая управление доступом к шине	D.14	Константные отказы[a)] (в сигналах данных, управления, адреса и разрешения конфликтов)	Модель сбоя при постоянном токе[b)] (в сигналах данных, управления, адреса и разрешения конфликтов). Блокировки по времени. Арбитраж не выполняется или выполняется непрерывно	Модель сбоя при постоянном токе[b)] (в сигналах адреса, управления, адреса и разрешения конфликтов). Блокировки по времени. Арбитраж не выполняется или выполняется непрерывно или неправильно. Исправимые ошибки (для последовательностных схем)
	Передача данных (должна быть проанализирована с приложением D ИСО 26262-6)	D.8	Отказ однорангового коммуникационного узла сети. Повреждение сообщения. Задержка сообщения. Потеря сообщения. Непреднамеренное повторение сообщения	Предыдущие и повторное упорядочивание. Введение сообщения	Предыдущие и нелегальное проникновение

Примечания

1 Более высокое значение охвата диагностикой может быть заявлено на основе анализа. Аналогично, будет получено более низкое значение охвата, если доминирующий вид отказов в списке отсутствует.

2 Кратковременные сбои рассматриваются, когда показано, что это актуально, например в случае использования микроэлектронной технологии.

3 Виды отказов для устройств обработки могут быть сведены к моделям сбоям при переменном токе таким, как сбои переходных процессов (замедленное повышение и уменьшение напряжения в узлах на используемой частоте) и задержки в линиях связи. Сбои такого типа, как ожидается, будут возрастать с уменьшением геометрических размеров, реализуемых используемой технологией. Обычно тесты для этих типов сбоев выполняются при включении или выключении питания, или в обоих случаях, в связи с их интрузивной природой (влияние тестов на режимы работы в процессе тестирования) и их способностью рано выявлять отказы при тестах в пределах рабочего режима. Так как они трудно поддаются количественной оценке, эти виды отказов, как правило, не включают в расчет интенсивности отказов.

4 Если должным образом реализовать, то методы, полученные моделированием константных отказов (например, тестирование N-Detect) и выполненные в условиях применения, как известно, являются эффективными для моделей сбоев при постоянном токе, а также для моделей переходных процессов.

[a)] «Константный» — это вид отказа, который может быть описан всеми нулями («0») или единицами («1») на выводах элемента. Это справедливо только для элементов, у которых интерфейсы выводятся на контакты элемента.

Окончание таблицы D.1

[b] «Модель сбоев при постоянном токе» включает в себя следующие модели отказов: константные отказы, константные неисправности типа обрыв, обрыв или высокое сопротивление выходов, а также короткие замыкания между сигнальными линиями. В данном случае не предполагается требовать исчерпывающего анализа, например требовать исчерпывающего анализа неисправностей типа короткое замыкание, которые могут влиять на любую теоретическую комбинацию любого сигнала внутри микроконтроллера или в многослойной печатной плате. Анализируются основные сигнальные линии или сильно связанные соединения, выявленные с помощью анализа на уровне топологии.

[c] «Модели исправимых ошибок» (например, изменение состояния бита) являются результатом кратковременных сбоев, вызванные альфа-частицами, образовавшимися в результате процесса распада, нейтронами и т. д. Эти кратковременные сбои также включают в себя нарушение в результате единичного сбоя и нарушение в результате единичного кратковременного сбоя.

Таблица D.2 — Системы

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обнаружение отказов путем мониторинга в режиме он-лайн	D.2.1.1	Низкий	Зависит от охвата диагностикой обнаружения отказов
Компаратор	D.2.1.2	Высокий	Зависит от качества сравнения
Схема голосования по мажоритарному принципу	D.2.1.3	Высокий	Зависит от качества устройства голосования
Принципы динамического управления	D.2.2.1	Средний	Зависит от охвата диагностикой обнаружения отказов
Мониторинг аналогового сигнала предпочтительнее мониторинга цифровых состояний включения — выключения	D.2.2.2	Низкий	—
Программное самотестирование с перекрестным обменом между двумя независимыми модулями	D.2.3.3	Средний	Зависит от качества самопроверки

Таблица D.3 — Электрические элементы

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обнаружение отказов путем мониторинга в режиме он-лайн	D.2.1.1	Высокий	Зависит от охвата диагностикой обнаружения отказов
Примечание — В данной таблице рассматриваются только механизмы безопасности, предназначенные для электрических элементов. Общие методы, такие как метод, основанный на сравнении данных (см. D.2.1.2), также способны обнаруживать отказы электрических элементов, но не включены в данную таблицу (они включены в таблицу D.2).			

Таблица D.4 — Модули обработки

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Программное самотестирование: предельное количество комбинаций (одноканальное)	D.2.3.1	Средний	Зависит от качества самопроверки
Программное самотестирование с перекрестным обменом между двумя независимыми модулями	D.2.3.3	Средний	Зависит от качества самопроверки

Окончание таблицы D.4

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Самотестирование, обеспечиваемое аппаратными средствами (одноканальное)	D.2.3.2	Средний	Зависит от качества самопроверки
Программное обеспечение с разнообразной избыточностью (один канал аппаратных средств)	D.2.3.4	Высокий	Зависит от качества разнообразия. Отказы по общей причине могут уменьшить значение охвата диагностикой
Взаимное сравнение программным обеспечением	D.2.3.5	Высокий	Зависит от качества сравнения
Избыточность аппаратных средств (жесткая двухядерная конфигурация, ассиметричная избыточность, запрограммированная обработка)	D.2.3.6	Высокий	Зависит от качества избыточности. Отказы по общей причине могут уменьшить значение охвата диагностикой
Тестирование регистра конфигурации	D.2.3.7	Высокий	Только для регистров конфигурации
Выявление переполнения стека/потери значимости	D.2.3.8	Низкий	Тестирование только границ стека
Интегрированный контроль непротиворечивости аппаратных средств	D.2.3.9	Высокий	Охватывает только недопустимые исключительные состояния аппаратных средств
Примечание — В данной таблице рассматриваются только механизмы безопасности, предназначенные для модулей обработки. Общие методы, такие как метод, основанный на сравнении данных (см. D.2.1.2), также способны обнаруживать отказы электрических элементов, но не включены в данную таблицу (они включены в таблицу D.2).			

Таблица D.5 — Постоянная память

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Бит четности	D.2.5.2	Низкий	—
Контроль памяти, используя коды обнаружения и исправления ошибок (EDC)	D.2.4.1	Высокий	Эффективность зависит от числа избыточных битов. Может быть использован для коррекции ошибок
Модифицируемая контрольная сумма	D.2.4.2	Низкий	Зависит от числа и битовых ошибок в тестируемой области
Сигнатура памяти	D.2.4.3	Высокий	—
Дублирование блоков	D.2.4.4	Высокий	—

Таблица D.6 — Память с произвольным доступом

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Тестирующая комбинация для памяти с произвольным доступом	D.2.5.1	Средний	Высокий охват для константных отказов. Не охватывает связанные отказы. Может подходить для работы при защите прерываний

Окончание таблицы D.6

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Тесты «марш» для памяти с произвольным доступом	D.2.5.3	Высокий	Зависит от порядка чтения записи для охвата связанной ячейки. Тест обычно не реализуется во время выполнения
Бит четности	D.2.5.2	Низкий	—
Контроль памяти, используя коды обнаружения и исправления ошибок (EDC)	D.2.4.1	Высокий	Эффективность зависит от числа избыточных битов. Может быть использован для коррекции ошибок
Дублирование блоков	D.2.4.4	Высокий	Отказы по общей причине могут уменьшить значение охвата диагностикой
Выполнение контрольной суммы	D.2.5.4	Высокий	Эффективность сигнатуры зависит полиномиально от длины блока информации, который должен быть защищен. Необходимо внимательно следить, чтобы значения, используемые для определения контрольных сумм, не изменялись во время вычисления контрольной суммы. Вероятность равна единице, деленной на максимальное значение контрольной суммы, если возвращается случайный код

Таблица D.7 — Аналоговые и цифровые устройства ввода/вывода

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обнаружение отказов путем мониторинга в режиме он-лайн (цифровой ввод/вывод)[a)]	D.2.1.1	Средний	Зависит от охвата диагностикой обнаружения отказов
Тестирующая комбинация	D.2.6.1	Высокий	Зависит от типа комбинации
Кодовая защита для цифрового ввода/вывода	D.2.6.2	Низкий	Зависит от типа кодирования
Многоканальное параллельное выходное устройство	D.2.6.3	Высокий	—
Средство контроля выходов	D.2.6.4	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	D.2.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала

[a)] Цифровой ввод/вывод может быть периодическим.

Таблица D.8 — Коммуникационные шины (последовательные, параллельные)

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Однобитовая избыточность аппаратных средств	D.2.7.1	Низкий	—
Многобитовая избыточность аппаратных средств	D.2.7.2	Средний	—
Повторное считывание отправленного сообщения	D.2.7.9	Средний	—
Полная избыточность аппаратных средств	D.2.7.3	Высокий	Отказы по общей причине могут уменьшить значение охвата диагностикой
Анализ с использованием тестирующих комбинаций	D.2.7.4	Высокий	—
Избыточность при передаче	D.2.7.5	Средний	Зависит от типа избыточности. Эффективен только для кратковременных сбоев
Информационная избыточность	D.2.7.6	Средний	Зависит от типа избыточности
Счетчик блоков данных	D.2.7.7	Средний	—
Мониторинг получения блоков данных по времени	D.2.7.8	Средний	—
Комбинация информационной избыточности, счетчика блоков данных и мониторинга получения блоков данных по времени	D.2.7.6, D.2.7.7 и D.2.7.8	Высокий	Для систем без аппаратного резервирования или тестирующих комбинаций, высокий охват может требоваться для комбинации этих механизмов безопасности

Таблица D.9 — Источник питания

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Управление напряжением или током (вход)	D.2.8.1	Низкий	—
Управление напряжением или током (выход)	D.2.8.2	Высокий	—

Таблица D.10 — Контроль последовательности выполнения программ/синхронизация

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Контрольный датчик времени с отдельной временной базой без временного окна	D.2.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	D.2.9.2	Средний	Зависит от временного ограничения для временного окна
Логический контроль последовательности выполнения программ	D.2.9.3	Средний	Эффективен только для отказов синхронизации, если внешние временные события влияют на логический процесс выполнения программы. Обеспечивает охват внутренних отказов технических средств (например, ошибки частоты прерывания), которые могут вызвать нарушение последовательности выполнения программного обеспечения

Окончание таблицы D.10

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Комбинация временного и логического контроля последовательности выполнения программ	D.2.9.4	Высокий	—
Зависимая от времени комбинация временного и логического контроля последовательности выполнения программ	D.2.9.5	Высокий	Обеспечивает охват внутренних отказов технических средств, которые могут вызвать нарушение последовательности выполнения программного обеспечения. При реализации асимметричных проектов обеспечивает охват последовательности коммуникаций между основным устройством и устройством контроля. Примечание — Метод должен быть разработан с учетом неустойчивости синхронизации при выполнении прерываний, загрузки ЦП, и т. д.

Таблица D.11 — Датчики

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обнаружение отказов путем мониторинга в режиме он-лайн	D.2.1.1	Низкий	Зависит от охвата диагностикой обнаружения отказов
Тестирующая комбинация	D.2.6.1	Высокий	—
Сравнение/голосование на входе (1oo2, 2oo3 или более высокая избыточность)	D.2.6.5	Высокий	Только если поток данных изменяется во время диагностического тестового интервала
Допустимый диапазон датчика	D.2.10.1	Низкий	Обнаруживает короткие замыкания на массу или на линию высокого напряжения и некоторые обрывы цепи
Корреляция датчика	D.2.10.2	Высокий	Обнаруживает отказы в диапазоне работы датчика
Проверка обоснованности датчика	D.2.10.3	Средний	—

Таблица D.12 — Исполнительные элементы

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Обнаружение отказов путем мониторинга в режиме он-лайн	D.2.1.1	Низкий	Зависит от охвата диагностикой обнаружения отказов
Тестирующая комбинация	D.2.6.1	Высокий	—
Мониторинг (т. е. согласованность управления)	D.2.11.1	Высокий	Зависит от охвата диагностикой обнаружения отказов

Таблица D.13 — Комбинаторная и последовательностная логика

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Программное самотестирование:	D.2.3.1	Средний	—
Самотестирование, обеспечиваемое аппаратными средствами (одноканальное)	D.2.3.2	Высокий	Эффективность зависит от типа самопроверки. Наиболее подходящим уровнем для этого теста является уровень логического элемента

Таблица D.14 — Коммуникации на кристалле

Механизмы/меры безопасности	См. обзор методов	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Однобитовая аппаратная избыточность	D.2.7.1	Низкий	—
Многобитовая аппаратная избыточность	D.2.7.2	Средний	Многобитовая избыточность может обеспечить высокий охват надлежащим чередованием данных, адресов и линий управления, и если она объединена с некоторым полным резервированием, например, для схемы разрешения конфликтов
Полная аппаратная избыточность	D.2.7.3	Высокий	Отказы по общей причине могут уменьшить значение охвата диагностикой
Тестирующая комбинация	D.2.6.1	Высокий	Зависит от типа комбинации
Примечание — Данная таблица рассматривает охват для коммуникационных шин внутри микропроцессора.			

D.2 Обзор методов для встроенных самодиагностических тестов

D.2.1 Электрические устройства

Главная цель. Управление отказами в электромеханических элементах.

D.2.1.1 Обнаружение отказов путем мониторинга в режиме он-лайн

Примечание — Ссылка на данный механизм/меру приведена в таблицах D.2, D.3, D.7, D.11 и D.12.

Цель. Обнаружение отказов путем мониторинга поведения системы во время ее нормальной работы (в режиме он-лайн).

Описание. При определенных условиях, отказы могут быть обнаружены с помощью информации (например) о поведении системы во времени. Например, если коммутатор нормально активизируется и если при этом коммутатор не изменяет состояния за предполагаемое время, то этот отказ может быть обнаружен. Обычными способами невозможно локализовать такой отказ.

Примечание — В общем случае не существует конкретных элементом аппаратных средств для реализации схемы мониторинга в режиме он-лайн. Мониторинг в режиме он-лайн обнаруживает аномальное поведение системы по отношению к определенным условиям ее активизации. Например, если такой параметр инвертируется, когда скорость автомобиля отличается от нуля, то обнаружение несоответствия между этим параметром и скоростью транспортного средства приводит к обнаружению отказа.

D.2.1.2 Компаратор

Примечание — Ссылка на данный механизм/меру приведена в таблице D.2.

Цель. Оперативное обнаружение (не одновременное) отказов в независимых программном обеспечении и аппаратных средствах.

Описание. Выходные сигналы независимых аппаратных средств или выходная информация независимого программного обеспечения сравнивают циклически или непрерывно компаратором. Сам компаратор может быть внешне тестируемым или же может использовать самоконтролируемую технологию. Обнаруживаемые различия в поведении формируют информацию для сообщений об отказах. Например, два блока обработки обмениваются данными (включая результаты, промежуточные результаты и тестовые данные) друг с другом. Сравнение данных осуществляется с использованием программного обеспечения в каждом блоке и обнаруживаемые различия приводят к сообщению об отказе.

D.2.1.3 Схема голосования по мажоритарному принципу

Примечание — Ссылка на данный механизм/меру приведена в таблице D.2.

Цель. Обнаружение и парирование отказов, по меньшей мере, в одном из трех аппаратных каналов.

Описание. Модуль голосования, использующий мажоритарный принцип (2 из 3, 3 из 4 или m из n), используется для обнаружения и парирования отказов.

Примечание — В отличие от компаратора, метод голосования по мажоритарному принципу повышает готовность путем обеспечения функциональных возможностей резервного канала даже после потери одного из каналов.

D.2.2 Электрические элементы

Примечание — Ссылка на данный механизм/меру приведена в таблице D.2.

Главная цель. Управление отказами в полупроводниковых элементах.

D.2.2.1 Принципы динамического управления

Примечание — Ссылка на данный механизм/меру приведена в таблице D.2.

Цель. Обнаружение статических отказов путем динамической обработки сигналов.

Описание. Принудительное изменение других статических сигналов (генерируемых извне или внутри) помогает обнаруживать статические отказы в элементах. Этот метод часто ассоциируется с электромеханическими элементами.

D.2.2.2 Мониторинг аналогового сигнала предпочтительнее мониторинга цифровых состояний включения — выключения

Примечание — Ссылка на данный механизм/меру приведена в таблице D.2.

Цель. Повышение уверенности в измеряемых сигналах.

Описание. Везде, где есть выбор, используются аналоговые сигналы вместо цифровых состояний включения — выключения. Например, текущие или безопасные состояния представлены уровнями аналогового сигнала, как правило, с контролем уровня допуска сигнала. В случае цифрового сигнала, его можно контролировать при аналоговом входе. Этот метод обеспечивает непрерывность мониторинга и более высокий уровень доверия к устройству передачи, снижая необходимую частоту периодического тестирования, выполняемого для выявления отказов передаваемой функции датчика.

D.2.3 Модули обработки

Главная Цель. Распознавать отказы, которые приводят к неправильным результатам в модулях обработки.

D.2.3.1 Программное самотестирование

Примечание — Ссылка на данный механизм/меру приведена в таблицах D.4 и D.13.

Цель. Выполняемое программным обеспечением оперативное обнаружение отказов в модулях обработки и других подэлементах, состоящих из физических устройств памяти (например, регистры) или функциональных блоков (например, дешифратор команд или шифратор/дешифратор устройства обнаружения и коррекции ошибок) или обоих типов устройств.

Описание: Обнаружение отказа полностью реализуется программным обеспечением, которое выполняет самотестирование, используя комбинацию данных или набор комбинаций данных для проверки физической памяти (например, регистров данных и адреса) или функциональных блоков (например, дешифратор команд) или обоих.

Примеры

1 Модуль обработки данных проверяется на корректность функционирования посредством использования, по меньшей мере, одного шаблона на инструкцию. Если инструкция не выполняется в связанных с безопасностью программах, то он может быть исключена из тестирования, но может быть ограничен охват, поскольку не все логические элементы процессора будут проверены. В общем, возможно, что не все выделенные и специальные регистры, основные таймеры и исключения могут быть охвачены. Охват зависимостей в последовательности команд, такой как реализуется при конвейерной обработке или вызывающей виды сбоев, связанные с синхронизацией, может быть ограни-

чен. Определение фактического охвата тестируемых логических элементов (в отличие от охваченных инструкций) обычно требует серьезного моделирования сбоев. Данный тест дает очень ограниченные (или не дает вовсе) возможности оценки охвата исправимых ошибок.

2 В случае подэлементов, таких как шифратор/дешифратор EDC, программное обеспечение может прочитать предварительно написанные специально поврежденные слова для тестирования поведения логики EDC. Поврежденные слова могут быть написаны с помощью самого программного теста, если EDC и интерфейс памяти имеют аппаратный переключатель для доступа как к данным, так и к битам кода. Охват зависит от количества и «богатства» шаблонов. Данный тест не обеспечивает охват исправимых ошибок.

D.2.3.2 Самотестирование, обеспечиваемое аппаратными средствами (одноканальное)

Примечание — Ссылка на данный механизм/меру приведена в таблицах D.4 и D.13.

Цель. Оперативное обнаружение отказов в процессоре и других подэлементах с использованием специальных аппаратных средств, которые увеличивают скорость и расширяют область обнаружения отказов.

Описание. Дополнительные специальные аппаратные средства обеспечивают функции самотестирования для обнаружения отказов в процессоре и других подэлементах (например, шифратор/дешифратор EDC) на уровне логических элементов. Данный тест может обеспечить высокий охват. Обычно он запускается в процессе инициализации или отключения процессора вследствие его интрузивной природы (средства тестирования влияют на режим работы процессора). Обычно используется для обнаружения множественных сбоев.

Пример — В случае подэлементов, таких как шифратор/дешифратор EDC, специальный механизм аппаратных средств, такой как встроенное самотестирование логики, может быть добавлен для генерации входных комбинаций для шифратора/дешифратора и проверки ожидаемых результатов. Обычно входные данные создаются генератором случайных чисел. Охват данного метода зависит от количества и «богатства» комбинаций — но обычно охват достаточно высок в связи с автоматической генерацией комбинаций. Данный тест не обеспечивает охват исправимых ошибок.

D.2.3.3 Программное самотестирование с перекрестным обменом между двумя независимыми модулями

Примечание — Ссылка на данный механизм/меру приведена в таблицах D.2 и D.4.

Цель. Выполняемое программным обеспечением оперативное обнаружение отказов в модулях обработки, состоящих из физических устройств памяти (например, регистры) и функциональных блоков (например, дешифратор команд).

Описание: Обнаружение отказа осуществляется только с помощью двух или более модулей обработки, программное обеспечение каждого из которых выполняет дополнительные функции, которые реализуют самотестирование (например, используя комбинацию блуждающих битов) для проверки физической памяти (регистры данных и адреса) и функциональных блоков (например дешифратор команд). Затем модули обработки обмениваются результатами. Данный тест дает очень ограниченные (или не дает вовсе) возможности оценки охвата исправимых ошибок.

D.2.3.4 Программное обеспечение с разнообразной избыточностью (в одном канале аппаратных средств)

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение отказов в модулях обработки динамическим сравнением программного обеспечения.

Описание. Проект состоит из двух избыточных различных реализаций программного обеспечения в одном канале аппаратных средств. В некоторых случаях использование различных ресурсов аппаратных средств (например, RAM и ROM памяти различного размера) может увеличить охват диагностикой.

Одна из реализаций, называется основной путь, отвечает за расчеты, которые, если вычислены с ошибкой, могут привести к опасности. Вторая реализация, называется резервный путь, несет ответственность за проверку расчетов по основному пути и принимать меры, если обнаружен сбой. Часто резервный путь реализуется с использованием других алгоритмических конструкций и другого кода для обеспечения разнообразия программного обеспечения. После завершения вычисления по обоим путям осуществляется сравнение выходных данных двух избыточных программных реализаций. Обнаруженные различия приводят к сообщению об отказе (см. рисунок D.2). Проект включает в себя методы для координации двух путей и повторной синхронизации путей для исправимых ошибок.

Вообще сравнение включает в себя некоторый тип гистерезиса и фильтрации, что допускает незначительные различия, связанные с различными путями реализации программного обеспечения. Примером разнообразия алгоритмов являются: A + B = C вместо C – B = A и при этом один путь использует обычные расчеты, а другой

путь — математику дополнительного двоичного кода. Результат резервного пути может быть столь же простым, как проверка величины или ограничения скорости в расчетах по основному пути.

Примечание — В связи с возможными отказами по общей причине между основным и резервным путями для проверки работы основного контроллера с помощью диагностических запросов и ответов (см. [21]) может быть использован дополнительный сторожевой процессор.

Другим вариантом этого механизма защиты является реализация резервного пути, как точной копии основного пути (или реализовать основной путь дважды). Такая версия без избыточного программного обеспечения обеспечивает только охват исправимых ошибок. Средний охват может быть достигнут, если код выполняется в третий раз с известными входами, генерирующими выходы, которые должны быть проверены сравнением с набором ожидаемых результатов. Результаты этого метода имеет очень легкий критерий прошел/не прошел (предполагается, что сравниваемые результаты точно совпадут) и легкую реализацию (резервный канал не разрабатывается), но данный подход включает в себя необходимость сохранения истории параметров (например, динамических состояний, интеграторов, ограничений скорости и т. д.).

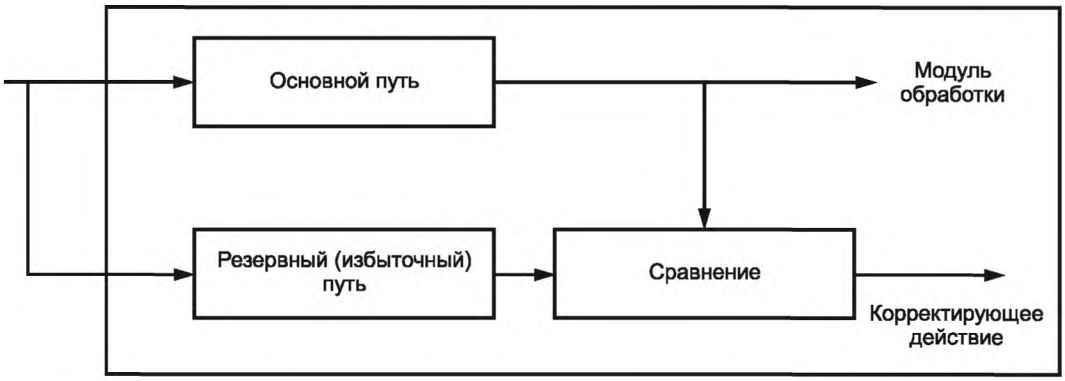


Рисунок D.2 — Сравнение избыточного программного обеспечения в одном модуле обработки

D.2.3.5 Взаимное сравнение программным обеспечением в отдельных модулях обработки

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение отказов в модуле обработки динамическим сравнением программного обеспечения.

Описание. Два модуля обработки взаимно обмениваются данными (включая результаты, промежуточные результаты и тестовые данные). Сравнение данных осуществляется программным обеспечением каждого модуля и обнаруженные различия приводят к сообщению об отказе (см. рисунок D.3). Такой подход обеспечивает разнообразие аппаратных средств и программного обеспечения, если используются различные типы процессоров, а также отдельные алгоритмы, коды и компиляторы. Такой проект включает в себя методы, предотвращающие ложные обнаружения ошибок из-за различий между процессорами (например, неустойчивость цикла синхронизации, коммуникационные задержки, инициализация процессора).

Пути могут быть реализованы на отдельных ядрах двухъядерного процессора. В этом случае метод включает в себя анализ, позволяющий понять виды отказов по общей причине, связанные с общим кристаллом и корпусом этих двух ядер.



Рисунок D.3 — Сравнение избыточного программного обеспечения на различных модулях обработки

D.2.3.6 Избыточность аппаратных средств (жесткая двухядерная конфигурация, ассиметричная избыточность, запрограммированная обработка)

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение отказов в модулях обработки последовательным сравнением внутренних или внешних результатов или тех и других, полученных из двух модулей обработки, работающих в жесткой конфигурации (на одном кристалле многопроцессорной системы).

Описание. В одной из версий этого типа диагностического метода — жесткая двухядерная конфигурация — два симметричных процессора находятся на одном кристалле (см. [22]). Модули обработки выполняют дублирующие операции в жесткой конфигурации (или с задержкой с установленным периодом) и результаты сравниваются. Любое несоответствие результатов приводит к состоянию ошибки и затем обычно выполняется сброс этого состояния. Этот механизм очень эффективен для кратковременных ошибок и отказов в арифметико-логическом устройстве. В зависимости от уровня избыточности, охват может быть распространен на адресные шины памяти и регистры конфигурации. Преимущество данного метода в том, что для параллельных путей не требуются отдельные коды, а недостаток в том, что имеющиеся два модуля обработки обеспечивают выполнение только одного модуля обработки. В хороших проектах выявляются и устраняются отказы по общей причине (например, отказы из-за общей синхронизации). Такой подход, сам по себе, не обеспечивает охват диагностикой систематические ошибки.

Возможны другие виды избыточности аппаратных средств, например, асимметричная избыточность. В таких архитектурах (например, см. [25]), отличающийся и специализированный блок обработки тесно связан с главными модулями обработки посредством интерфейса, позволяющего пошаговое сравнение внутренних и внешних результатов. Такой вид избыточности очень эффективен для сбоев при постоянном токе и для исправимых ошибок. Кроме того, интерфейс уменьшает сложность и сокращает задержку обнаружения ошибок, например, на для сбоев, влияющих на блок регистров модуля обработки. Для параллельного пути и специализированного блока обработки, который может быть меньше основного, не требуется отдельный код. Разнообразие аппаратных средств обеспечивает эффективный охват отказов по общей причине и систематических отказов. Недостатком данного подхода является необходимость детального анализа для доказательства охвата диагностикой.

Возможна также запрограммированная обработка: модули обработки могут быть разработаны со специальными методами распознавания отказов или схемами коррекции отказов. Эти подходы могут гарантировать высокий охват для очень маленьких процессоров с ограниченными функциональными возможностями или они могут быть пригодны для подмодуля процессора, такого как арифметико-логическое устройство [26]. Аппаратные средства и программное обеспечение с запрограммированной обработкой можно совместить с использованием подходов, таких как Vital Coded Processor [27]. Может быть необходим детальный анализ для доказательства охвата диагностикой.

D.2.3.7 Тестирование регистра конфигурации

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение отказов в регистрах конфигурации модуля обработки. Отказы могут быть связаны с аппаратными средствами (константные значения или ошибки, вызванные сменой состояний устройства) или с программным обеспечением (неправильно сохраненное значение или повреждение значения регистра в результате ошибки программного обеспечения).

Описание. Установки регистра конфигурации считываются и сравниваются с закодированными ожидаемыми параметрами (например, маски). Если установки не совпадают, в регистры перезагружают их целевые значения. Если ошибка сохраняется на протяжении заранее определенного числа проверок, то формируется сообщение об ошибке.

D.2.3.8 Выявление переполнения стека/потери значимости

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение переполнения стека/потери значимости.

Описание. Границы стека в энергозависимой памяти загружаются с предопределенными значениями. Периодически значения проверяются, и если они изменились, то обнаруживаются потоки записей до или после границы. Тест не нужен, если записи вне границ стека управляются блоком управления памятью.

D.2.3.9 Интегрированный контроль непротиворечивости аппаратных средств

Примечание — Ссылка на данный механизм/меру приведена в таблице D.4.

Цель. Оперативное обнаружение недопустимых условий в модуле обработки.

Описание. Большинство процессоров снабжены механизмами, которые возбуждают исключительные состояния аппаратных средств при обнаружении ошибок (например, деление на ноль, неправильные коды операций).

Чтобы захватить такие условия и изолировать систему от подобных ошибок, может быть использована обработка прерываний по этим ошибкам. Как правило, для обнаружения систематических отказов используется контроль аппаратных средств, но он также может быть использован для обнаружения определенных видов случайных сбоев аппаратных средств. Данный метод обеспечивает низкий охват для некоторых ошибок кодирования и считается «хорошей практикой» при проектировании.

D.2.4 Постоянная память

Главная Цель. Выявить модификации информации в постоянной памяти.

Примечание — В зависимости от типа реализации памяти одиночный сбой может повлиять на несколько ячеек памяти. Например, обрыв шины выборки строки ячеек памяти не позволит прочитать всю строку ячеек памяти. Этот тип отказа может быть легче обнаружить, если тестируется несколько ячеек памяти.

D.2.4.1 Контроль памяти, используя коды обнаружения и исправления ошибок (EDC)

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.5 и D.6.

Цель. Обнаружить каждый однобитовый отказ, каждый двухбитовый отказ, некоторые трехбитовые отказы и некоторые многобитовые отказы в слове (как правило, 32, 64 или 128 бит).

Описание. Каждое слово в памяти расширяется несколькими избыточными битами для выработки модифицированного кода Хэмминга с расстоянием Хэмминга, равным, по меньшей мере, 4. При каждом считывании слова проверка избыточных битов может указывать, произошло ли искажение. При обнаружении различий выдается сообщение об отказе.

Данная процедура может быть также использована для обнаружения отказов адресации при вычислении избыточных битов при объединении слова данных с его адресом. С другой стороны, для отказов адресации вероятность обнаружения зависит от количества битов EDC для случайных возвращаемых данных (например, разрыв адресной шины или короткое замыкание одной адресной шины на другую так, что возвращается среднее значение двух ячеек). Охват равен 0 %, если ошибка адресации приводит к совершенно другой выбранной ячейке.

Для отказа разрешения записи ячейки в памяти с произвольным доступом EDC может обеспечить высокий охват, если ячейка не может быть инициализирована. Охват равен 0 %, если отказ разрешения записи ячейки влияет на всю ячейку после ее инициализации.

Примечание — Данную технологию часто называют ECC (Error Correcting Code — Код коррекции ошибок).

D.2.4.2 Модифицируемая контрольная сумма

Примечание — Ссылка на данный механизм/меру приведена в таблицах D.5.

Цель. Обнаружить каждый однобитовый отказ.

Описание. Контрольная сумма блока памяти образуется соответствующим алгоритмом, который обрабатывает все слова в блоке памяти. Эта контрольная сумма может храниться как дополнительное слово в постоянной памяти, либо может быть добавлена как дополнительное слово в блок памяти для того, чтобы алгоритм контрольной суммы выработал заранее заданное значение. При последующем тестировании памяти контрольная сумма создается снова с использованием того же алгоритма, и результат сравнивается с запомненным или заданным значением. При обнаружении различий вырабатывается сообщение об ошибке [20]. Вероятность пропущенного обнаружения составляет $1/(2^{\text{значение контрольной суммы}})$, если возвращается случайный результат. Если конкретные нарушения данных являются более вероятными, то некоторые контрольные суммы могут обеспечить лучшую выявляемость, чем для случайных результатов.

D.2.4.3 Сигнатура памяти

Примечание — Ссылка на данный механизм/меру приведена в таблице D.5.

Цель. Обнаружить каждый однобитовый отказ и большинство многобитовых отказов.

Описание. Содержимое блока памяти «сжимается» (с использованием аппаратных или программных средств) в один или более байтов с использованием алгоритма контроля с помощью избыточного циклического кода (CRC). Типичный алгоритм CRC рассматривает все содержимое блока памяти как побайтовый или побитовый последовательный поток данных, в котором выполняется непрерывное полиномиальное деление с использованием полиномиального генератора. Остаток от деления сохраняется и представляет собой сжатое содержимое памяти — «сигнатуру» памяти. Сигнатура вычисляется каждый раз при последующем тестировании и сравнивается с уже запомненным значением. При обнаружении различий выдается сообщение об ошибке.

CRC являются особенно эффективным для обнаружения пакетных ошибок. Эффективность сигнатуры зависит от отношения значения многочлена к длине блока защищаемой информации. Вероятность пропущенного обнаружения равна единице, деленной на удвоенное значение контрольной суммы, если возвращается случайный результат [20].

Примечание — 8-битовая сигнатура CRC обычно не используется для современной памяти размером более 4K.

D.2.4.4 Дублирование блоков (например, двойная память с аппаратным или программным сравнением)

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.5 и D.6.

Цель. Обнаружить каждый битовый отказ.

Описание. Адресное пространство дублируется в двух областях памяти. Первая область памяти функционирует в нормальном режиме. Вторая область памяти содержит ту же самую информацию и имеет параллельный доступ к первой. Их выходы сравниваются, и при обнаружении различий выдается сообщение об ошибке. В зависимости от проекта подсистемы памяти хранение инвертированных данных в одной из двух областей может повысить охват диагностикой. Охват может быть снижен, если существуют виды отказов (например, общие шины адреса, отсутствие запрета на запись), которые являются общими для обоих блоков, или если в результате физического размещения ячеек памяти логически не связанные ячейки расположены близко друг к другу.

D.2.5 Память с произвольным доступом

Главная Цель. Обнаружить отказы во время адресации, записи, запоминания и считывания.

Примечание — В зависимости от типа реализации памяти одиночный сбой может повлиять на несколько ячеек памяти. Например, обрыв шины выборки строки ячеек памяти не позволит прочитать всю строку ячеек памяти. Этот тип отказа может быть легче обнаружить, если тестируется несколько ячеек памяти.

D.2.5.1 Тестирующая комбинация для памяти с произвольным доступом

Примечание — Ссылка на данный механизм/меру приведена в таблице D.6.

Цель. Обнаружить преимущественно статические битовые отказы.

Описание. Комбинация битов, за которой следует дополнение этой комбинации битов, записывается в ячейки памяти.

Ячейки ОЗУ обычно тестируются индивидуально. Содержимое ячейки сохраняется, а затем в ячейку записываются все «0». Содержимое ячейки затем проверяется считыванием нулевых значений. Процедура повторяется, но в ячейку записываются все «1» и выполняется считывание их содержимого обратно. Если вызывает озабоченность вид отказов при переходе от «1» к «0», то могут быть выполнены дополнительные запись и чтение всех «0». Затем восстанавливается первоначальное содержимое ячейки (см. [20], раздел 4.2.1). Тест эффективен при обнаружении константных отказов и кратковременных отказов, но не может выявить большинство исправимых ошибок, сбоев адреса и сбоев связанных ячеек.

Примечания

1 Тест часто реализуется в фоновом режиме с блокировкой прерываний во время испытания каждой отдельной ячейки.

2 Поскольку реализация теста включает в себя считывание только что записанное значение, то оптимизирующие компиляторы имеют тенденцию оптимизировать тест. Если используется оптимизирующий компилятор, то хорошей практикой является проверка тестового кода на уровне ассемблера.

3 В некоторых ОЗУ возможен сбой, связанный с тем, что последняя операция доступа к памяти выполняется как чтение. Если это возможный вид отказа, то диагностика может проверить две ячейки вместе, сначала записав «0» вместо «1» и «1» в следующую ячейку, а затем проверить, считывается «0» из первой ячейки.

D.2.5.2 Бит четности

Примечание — Ссылка на данный механизм/меру приведена в таблице D.6.

Цель. Обнаружить отказы из-за единственного поврежденного бита или нечетного числа поврежденных битов в одном слове (обычно 8 бит, 16 бит, 32 бита, 65 бита или 128 бит).

Описание. Каждое слово в памяти расширяется на один бит (бит четности), который дополняет каждое слово до четного или нечетного числа логических единиц. Четность слова данных проверяется при каждом чтении. При обнаружении ложного числа единиц выдается сообщение об отказе. Выбор четности или нечетности должен осуществляться так, чтобы всякий раз в случае отказа не выдавалось ничего, кроме нулевого (0) или единичного (1) слова, вырабатывалось уведомление о том, что это слово неправильно закодировано.

Данная процедура также может быть использована для обнаружения отказов адресации, если четность определяется для объединения слова данных с его адресом. С другой стороны, для отказов адресации существует 50 %-ная вероятность обнаружения случайных возвращаемых данных (например, разрыв адресной шины или короткое замыкание одной адресной шины на другую так, что возвращается среднее значения двух ячеек). Охват равен 0 %, если ошибка адресации приводит к совершенно другой выбранной ячейке.

При отказах разрешения записи в ячейку памяти с произвольным доступом данный метод может обнаружить 50 % отказов, если ячейка не может быть инициализирована. Охват равен 0 %, если отказ разрешения записи в ячейку влияет на всю ячейку после ее инициализации.

D.2.5.3 Тесты «марш» для памяти с произвольным доступом

Примечание — Ссылка на данный механизм/меру приведена в таблице D.6.

Цель. Обнаружить преимущественно устойчивые битовые отказы, отказы от переходных процессов в битах, отказы адресации и отказы связанных ячеек.

Описание. Комбинация из «0» и «1» записывается в ячейки памяти по определенной схеме и в определенном порядке проверяется.

«Маршевый» тест состоит из конечной последовательности «маршевых» элементов, а «маршевый» элемент является конечной последовательностью операций, применяемых последовательно к каждой ячейке в матрице памяти. Так, например, операция может состоять из записи «0» в ячейку, записи «1» в ячейку, чтение ожидаемого «0» из ячейки, и чтение ожидаемой «1» из ячейки. Если ожидаемая «1» не считывается, то обнаруживается отказ. Уровень охвата для связанных ячеек зависит от порядка записи/чтения.

В главе 4 [20] описан ряд различных «маршевых» тестов, предназначенных для обнаружения различных видов отказов памяти с произвольным доступом: константных сбоев, кратковременных сбоев (неспособность перейти от единичного состояния к нулевому состоянию или от нулевого состояния к единичному состоянию, но не для обоих переходов), сбоев адресации и сбоев связанных ячеек. Тесты такого типа не являются эффективными для обнаружения исправимых ошибок.

Примечание — Эти тесты, как правило, запускаются только при инициализации или отключении.

D.2.5.4 Выполнение контрольной суммы/контроля циклическим избыточным кодом (CRC)

Примечание — Ссылка на данный механизм/меру приведена в таблице D.6.

Цель. Обнаружить однобитовые и несколько многобитовых отказов в памяти с произвольным доступом

Описание. Контрольная сумма/CRC создается подходящим алгоритмом, который использует каждое слово в блоке памяти. Контрольная сумма сохраняется в качестве дополнительного слова в памяти с произвольным доступом. Так как блок памяти обновляется, то контрольная сумма памяти с произвольным доступом/CRC также обновляется, удаляя старое значение данных и добавляя новое значение данных, которое будет храниться в памяти. Периодически контрольная сумма/CRC вычисляются для блока данных и сравниваются с сохраненной контрольной суммой/CRC. Если будет обнаружено различие, то формируется сообщение об отказе. Вероятность пропущенного обнаружения равна единицы, деленной на размер контрольной суммы/CRC, если возвращается случайный результат. Охват диагностикой может уменьшаться при увеличении объема памяти.

D.2.6 Устройства ввода/вывода и интерфейсы

Главная Цель. Обнаружение отказов в устройствах ввода/вывода (цифровых и аналоговых) и предотвращение дальнейшей передачи недопустимых выходных данных.

D.2.6.1 Тестирующая комбинация

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.7, D.11, D.12 и D.14.

Цель. Обнаружить статические отказы (константные отказы) и перекрестные помехи.

Описание. Этот метод реализует независимое от потока данных циклическое тестирование входных и выходных элементов. В нем используются определенные тестирующие комбинации для сравнения с соответствующими этим тестирующим комбинациям предполагаемыми значениями. Охват теста зависит от степени независимости между информацией тестирующей комбинации, восприятием и оценкой тестирующей комбинации. В хорошем проекте тестирующие комбинации не должны неблагоприятно влиять на функциональное поведение системы.

D.2.6.2 Кодовая защита

Примечание — Ссылка на данный механизм/меру приведена в таблице D.7.

Цель. Обнаружить случайные отказы аппаратных средств и систематические отказы в потоке данных ввода/вывода.

Описание. Процедура, реализующая кодовую защиту, защищает вводимую и выводимую информацию от систематических и случайных отказов аппаратных средств. Кодовая защита обеспечивает зависимое от потока данных обнаружение отказов входных и выходных модулей, основываясь на избыточности информации и/или временной избыточности. Обычно избыточная информация налагается на входные и/или выходные данные; тем самым обеспечиваются средства для мониторинга правильности операций входных и выходных схем. Возможно применение многих методов — например, сигнал несущей частоты может налагаться на выходной сигнал датчика. После этого логический модуль может проверить наличие несущей частоты, либо на выходе канала могут быть добавлены

избыточные кодовые биты для контроля достоверности прохождения сигнала между логическим модулем и оконечным исполнительным механизмом.

D.2.6.3 Многоканальное параллельное выходное устройство

Примечание — Ссылка на данный механизм/меру приведена в таблице D.7.

Цель. Обнаружить случайные отказы аппаратных средств (константные отказы), отказы, обусловленные внешними воздействиями, временные отказы, отказы адресации, постепенные отказы и кратковременные отказы.

Описание. Это зависимое от потока данных многоканальное параллельное выходное устройство с независимыми выходами для обнаружения случайных аппаратных отказов. Обнаружение отказов осуществляется с помощью внешних компараторов. При появлении отказа система может быть непосредственно выключена. Это устройство эффективно только в том случае, если поток данных изменяется в интервале диагностических проверок.

D.2.6.4 Средство контроля выходов

Примечание — Ссылка на данный механизм/меру приведена в таблице D.7.

Цель. Обнаружить отдельные отказы, отказы, обусловленных внешними воздействиями, временные отказы, отказы адресации, постепенные отказы (для аналоговых сигналов) и кратковременные отказы.

Описание. Это устройство, зависимое от потока данных, сравнивает выходные данные с независимыми входными данными для обеспечения совместимости с областью их допустимых значений (время, диапазон). Обнаруженный отказ не всегда относится к неправильному выходному сигналу. Это устройство эффективно только в том случае, если поток данных изменяется в интервале диагностических проверок.

D.2.6.5 Сравнение/голосование входных данных

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.7 и D.11.

Цель. Обнаружить отдельные отказы, отказы, обусловленных внешними воздействиями, временные отказы, отказов адресации, постепенные отказы (для аналоговых сигналов) и кратковременные отказы.

Описание. Это устройство, зависимое от потока данных, сравнивает независимые входные данные для обеспечения совместимости с областью их допустимых значений (время, диапазон). Реализуемая избыточность может быть 1 из 2, 2 из 3 или более лучшая. Это устройство эффективно только в том случае, если поток данных изменяется в интервале диагностических проверок.

D.2.7 Коммуникационные шины

Главная Цель. Обнаружить отказы, обусловленные искажениями при передаче информации.

D.2.7.1 Однобитовая избыточность аппаратных средств

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.8 и D.14.

Цель. Обнаружить каждый отказ нечетного бита, то есть 50 % всех возможных битовых отказов в потоке данных.

Описание. Коммуникационная шина расширяется на одну линию (бит) и эта дополнительная линия (бит) используется для обнаружения отказов путем проверки на четность.

D.2.7.2 Многобитовая избыточность аппаратных средств

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.8 и D.14.

Цель. Обнаружить отказы в процессе передачи по шине и в последовательных каналах связи.

Описание. Шина расширяется на две или более линий (битов) и эти дополнительные линии (биты) используются для обнаружения отказов методом кода Хэмминга.

D.2.7.3 Полная избыточность аппаратных средств

Примечание — Ссылки на данный механизм/меру приведены в таблицах D.8 и D.14.

Цель. Обнаружить отказы в процессе передачи данных путем сравнения сигналов двух шин.

Описание. Шина дублируется и дополнительные линии (биты) используются для обнаружения отказов.

Пример — Двойной канал реализации FlexRay: шина дублирована, и дополнительные линии (биты) используются, чтобы обнаружить отказы.

D.2.7.4 Анализ с использованием тестирующих комбинаций

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружить статические отказы (константные отказы) и перекрестные помехи.

Описание. Осуществляется независимое от потока данных циклическое тестирование маршрутов данных. Используется определенная тестирующая комбинация для сравнения наблюдаемых значений с соответствующими предполагаемыми значениями.

Охват теста зависит от степени независимости между информацией тестирующей комбинации, восприятием и оценкой тестирующей комбинации. В качественном проекте тестирующие комбинации не должны неблагоприятно влиять на функциональное поведение системы.

D.2.7.5 Избыточность при передаче

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружить кратковременные отказы при обмене по шине.

Описание. Информация передается последовательно несколько раз. Данный метод эффективен только для обнаружения кратковременных отказов.

D.2.7.6 Информационная избыточность

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружение отказов при обмене по шине.

Описание. Данные передаются блоками вместе с вычисленными контрольной суммой или CRC (см. [28] и [29]) для каждого блока. После этого приемник повторно вычисляет контрольную сумму полученных данных. Результат сравнивается с полученной контрольной суммой. Для CRC охват зависит от длины охватываемых данных, размера CRC (количество бит) и полинома. CRC может быть ориентирован на более вероятные виды коммуникационных отказов базовых технических средств (например ошибки в линии передачи пакетов данных).

Идентификатор сообщения может быть включен в вычисление контрольной суммы/CRC, чтобы обеспечить охват искажений в этой части сообщения (подмену).

a) Низкий охват диагностикой: расстояние Хэмминга 2 или меньше.

Пример — Значение CRC для информации сообщения содержится в сообщении. Размер CRC 5 бит и полином 0x12 обеспечивает расстояние Хэмминга 2 для данных длиной менее 2048 бит. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC.

b) Средний охват диагностикой: расстояние Хэмминга 3 или более.

Примеры

1 Значение CRC для информации сообщения содержится в сообщении. Размер CRC 8 бит и полином 0x97 обеспечивает расстояние Хэмминга 4 для данных длиной менее 119 бит. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC (обычно используется в шинах локальных сетей).

2 Значение CRC для информации сообщения и идентификатор сообщения содержатся в сообщении. Размер CRC 10 бит и полином 0x319 обеспечивает расстояние Хэмминга 4 для данных длиной менее 501 бит. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC.

3 Значение CRC для информации сообщения и идентификатор сообщения содержатся в сообщении. Размер CRC 15 бит и полином 0x4599 обеспечивает расстояние Хэмминга 5 для данных длиной менее 127 бит. Кроме того, могут быть обнаружены пакеты до 15 ошибок. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC (как используется в локальной сети контроллеров (CAN)).

4 Значение CRC для информации сообщения содержится в сообщении. Размер CRC 24 бита и полином 0x5D6DCB обеспечивает расстояние Хэмминга CRC, равное 6, для данных длиной менее или равной 248 байт, и расстояние Хэмминга CRC, равное 4, для данных длиной больше 248 байт. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC (как используется во FlexRay для фрейма CRC).

5 Значение CRC для заголовка сообщения, включая идентификатор сообщения содержатся в сообщении. Размер CRC 11 бит и полином 0x385 обеспечивает расстояние Хэмминга 6 для данных длиной менее или равной 20 бит. Передающее устройство включает в себя упомянутое значение CRC, а приемное устройство подтверждает данные после вычисления и сравнения значения CRC (как используется во FlexRay для заголовка CRC).

Примечания

1 Высокий охват может быть достигнут для искажений данных и идентификатора, однако, общий высокий уровень охвата не может быть достигнут только путем проверки согласованности данных и идентификатора с сигна-

турой, независимо от эффективности сигнатуры. В частности, сигнатура не охватывает потерю сообщения или непреднамеренное повторение сообщения.

2 Если алгоритм контрольной суммы имеет расстояние Хэмминга менее 3, то высокий охват при искажениях данных и идентификатора все еще может быть востребован, если существует надлежащее обоснование.

D.2.7.7 Счетчик блоков данных

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружить потери блоков данных. Блоком данных является связный набор данных, передаваемый от одного контроллера на другой контроллер(ы). Каждый уникальный блок данных имеет идентификатор сообщения.

Описание: Каждый отдельный связанный с безопасностью блок данных включает в себя счетчик как часть сообщения, который передается по шине. Счетчик увеличивается в результате создания каждого последующего передаваемого блока. Приемное устройство в состоянии обнаруживать любую потерю блока данных или его не обновление, если в результате проверки выяснилось, что значение счетчика увеличилось на единицу.

Специальная версия счетчика блоков данных должна включать отдельные сигнальные счетчики, которые связаны с обновлением данных, связанных с безопасностью. В этой ситуации, если блок данных содержит несколько частей связанных с безопасностью данных, то для каждой части связанных с безопасностью данных обеспечивается свой счетчик.

D.2.7.8 Мониторинг получения блоков данных во времени

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружить потерю данных между передающим узлом и принимающим узлом.

Описание. Приемное устройство отслеживает каждый предполагаемый идентификатор связанного с безопасностью сообщения по времени между получением достоверных блоков данных с этим идентификатором сообщения. Отказ может означать слишком длительное время между сообщениями. Данный метод предназначен для обнаружения потери непрерывности работы канала связи или потери непрерывности передачи одного конкретного сообщения (не получены блоки данных, связанные с конкретным идентификатором сообщения).

D.2.7.9 Повторное считывание отправленного сообщения

Примечание — Ссылка на данный механизм/меру приведена в таблице D.8.

Цель. Обнаружить отказы в коммуникационной шине.

Описание. Передатчик повторно считывает из коммуникационной шины отправленное им сообщение и сравнивает его с исходным сообщением.

Примечания

1 Данный механизм защиты используется в CAN-протоколе.

2 Высокий охват может быть достигнут при повреждении данных и идентификатора, однако, общий высокий уровень охвата не может быть достигнут только путем проверки согласованности данных и идентификатора. Другие виды отказов, такие как непреднамеренное повторение сообщения, не всегда охватываются настоящим механизмом безопасности.

D.2.8 Источник питания

Главная цель. Обнаружить отказы, вызванные дефектами в источнике питания.

D.2.8.1 Управление напряжением или током (вход)

Примечание — Ссылка на данный механизм/меру приведена в таблице D.9.

Цель. Оперативное обнаружение неправильного поведения входных значений тока или напряжения.

Описание. Контроль входного напряжения или тока.

D.2.8.2 Управление напряжением или током (на выходе)

Примечание — Ссылка на данный механизм/меру приведена в таблице D.9.

Цель. Оперативное обнаружение неправильного поведения выходных значений тока или напряжения.

Описание. Контроль выходного напряжения или тока.

D.2.9 Временной и логический контроль последовательности выполнения программ

Примечание — Ссылки на данную группу механизмов/мер приведены в таблице D.10.

Главная Цель. Обнаружить искаженную последовательность программы. Искаженная программная последовательность появляется в том случае, если отдельные элементы программы (например, программные модули, подпрограммы или команды) обрабатываются в неправильной последовательности, или в несоответствующий период времени, или если сбилась тактовая частота процессора.

D.2.9.1 Контрольный датчик времени с отдельной временной базой без временного окна

Примечание — Ссылка на данный механизм/меру приведена в таблице D.10.

Цель. Контролировать поведение и последовательность выполнения программ.

Описание. Внешние средства определения времени с отдельной базой времени (например, контрольный датчик времени) периодически переключаются для контроля поведения компьютера и последовательности выполнения программ. Важно, чтобы точки запуска были правильно установлены в программе. Контрольный датчик времени не переключается с некоторым фиксированным периодом, однако задается его максимальный интервал.

D.2.9.2 Контрольный датчик времени с отдельной временной базой и временным окном

Примечание — Ссылка на данный механизм/меру приведена в таблице D.10.

Цель. Контролировать поведение и последовательность выполнения программ.

Описание. Внешние средства определения времени с отдельной базой времени (например, контрольный датчик времени) периодически переключаются для контроля поведения компьютера и последовательности выполнения программ. Важно, чтобы точки запуска были правильно установлены в программе (например, не во время выполнения процедуры обработки прерывания). Для контрольного датчика времени задаются нижняя и верхняя границы. Если программная последовательность выполняются больше или меньше ожидаемого времени, то выполняется некоторое действие

D.2.9.3 Логический контроль последовательности выполнения программ

Примечание — Ссылка на данный механизм/меру приведена в таблице D.10.

Цель. Контролировать правильную последовательность выполнения отдельных частей программы.

Описание. Правильная последовательность выполнения отдельных частей программы контролируется программным обеспечением (процедура подсчета, ключевая процедура) или внешними средствами контроля (см. [23] и [24]). Важно, чтобы точки проверки располагались в программе так, чтобы контролировались пути, которые могут привести к опасной ситуации, если из-за одиночного или множественного сбоя эти пути не смогут завершиться или последовательность их выполнения будет неправильной. Последовательности могут обновляться между каждой функцией вызова или более тесно связаны с выполнением программы.

D.2.9.4 Комбинация временного и логического контроля последовательности выполнения программ

Примечание — Ссылка на данный механизм/меру приведена в таблице D.10.

Цель. Контролировать поведение и корректность последовательности выполнения отдельных частей программы.

Описание. Средство контроля времени (например, контрольный датчик времени), контролирующее программную последовательность, вновь запускается только в случае, если последовательность модулей программы выполняется правильно. Данный метод является комбинацией методов D.2.9.3 и D.2.9.1 или D.2.9.2.

D.2.9.5 Комбинация временного и логического контроля последовательности выполнения программ с временной зависимостью

Примечание — Ссылка на данный механизм/меру приведена в таблице D.10.

Цель. Контролировать поведение, корректность последовательности и время выполнения отдельных разделов программы.

Описание. Реализуется стратегия контроля выполнения программы, где точки обновления программного обеспечения, как ожидается, находятся внутри относительного временного окна. Результат последовательности контроля выполнения программы и вычисление времени контролируется внешними средствами мониторинга.

D.2.10 Датчики

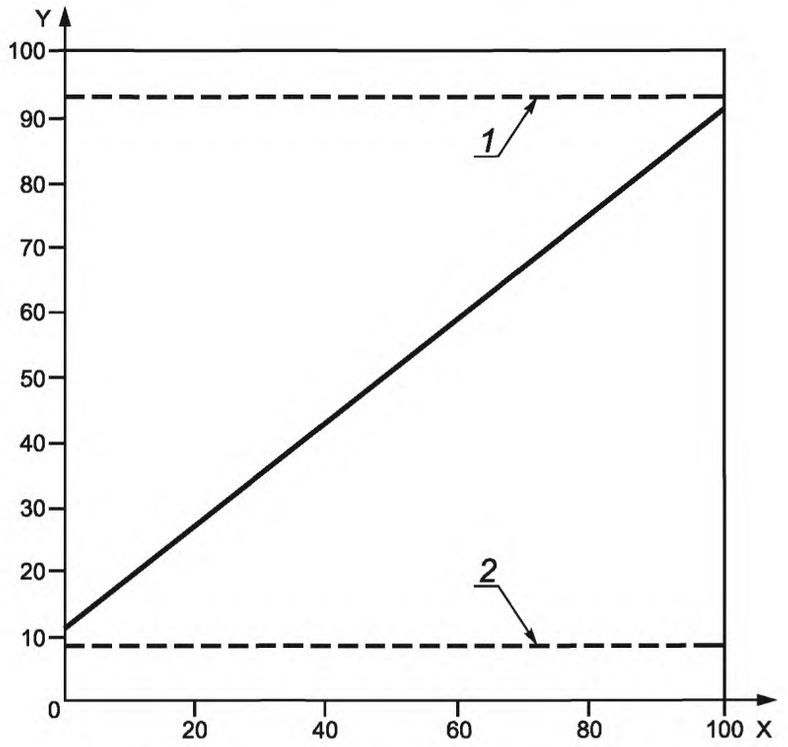
Главная Цель. Управлять отказами датчиков системы.

D.2.10.1 Допустимый диапазон датчика

Примечание — Ссылка на данный механизм/меру приведена в таблице D.11.

Цель. Обнаружить короткие замыкания датчика на массу или шину питания и некоторые разрывы электрических цепей.

Описание: Область допустимых значений находится в средней части диапазона электрических датчиков (см. рисунок D.4). Если показания датчика находится в области недопустимых значений, то это указывает на электрические проблемы датчика, например, короткое замыкание датчика на массу или шину питания. Обычно информацию с датчиков считывает электронный блок управления, используя АЦП.



X — физическое показание датчика в %; Y — измеренное показание датчика в % от опорного напряжения; *1* — верхняя граница допустимого диапазона; *2* — нижняя граница допустимого диапазона

Рисунок D.4 — Датчик с границами области допустимого диапазона его значений

D.2.10.2 Корреляция датчика

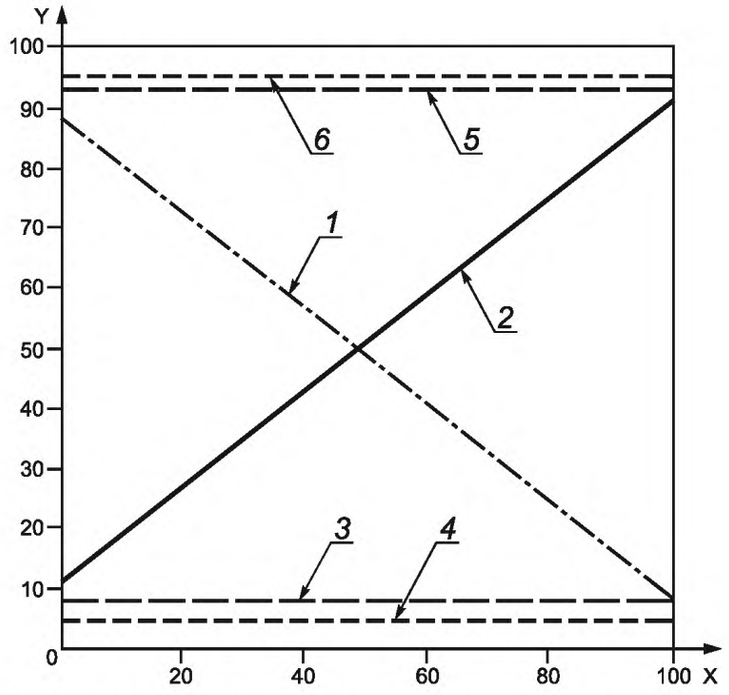
Примечание — Ссылка на данный механизм/меру приведена в таблице D.11.

Цель. Обнаружить дрейфы датчика в его рабочем диапазоне, смещения или другие ошибки, используя избыточный датчик.

Описание. Сравнение двух идентичных или аналогичных датчиков для обнаружения отказов в их рабочем диапазоне, таких как дрейфы, смещения или константные отказы. На рисунке D.5 представлен пример двух одинаковых датчиков, но с противоположным наклоном измеряемой характеристики. Заметим, что значения границ допустимого диапазона для датчиков различны. Обычно информацию с датчиков считывает электронный блок управления, используя АЦП.

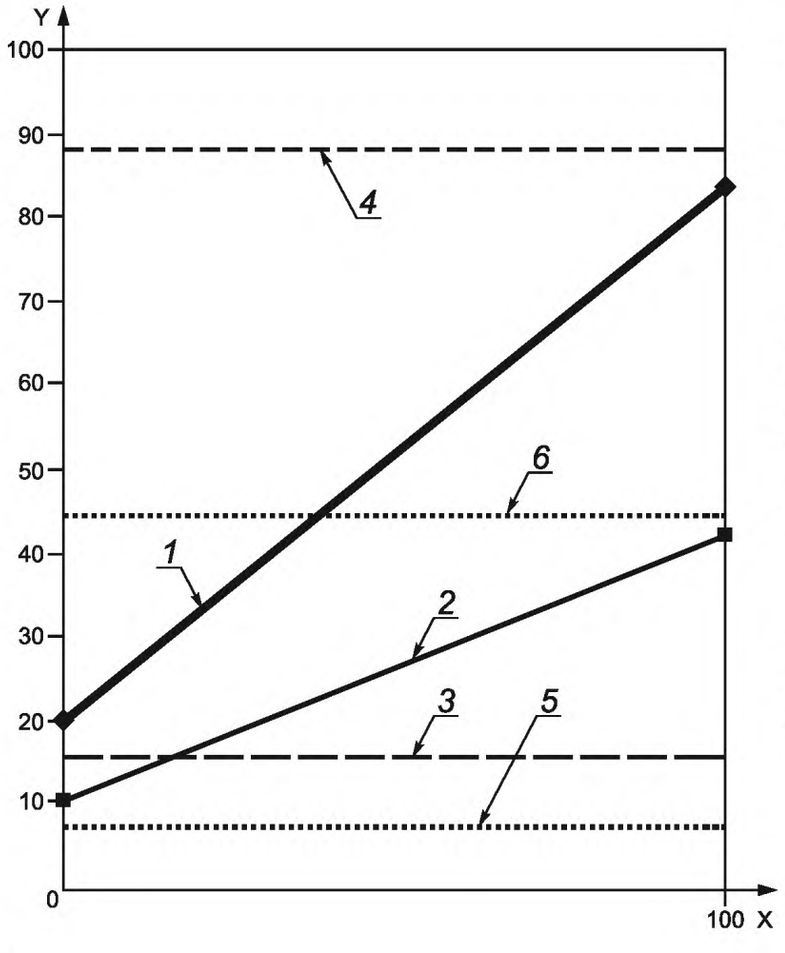
В примере, показанном на рисунке D.5, значения датчиков будут преобразованы к одинаковому наклону измеряемой характеристики, а также будет выполнено сравнение значений датчиков с целью их согласованности в пределах пороговых значений. Пороговые значения выбирается с учетом допуска АЦП и разновидностей электрических элементов. Оба датчика опрашиваются ЭБУ в одно и то же время, насколько это возможно, чтобы избежать ложных отказов из-за динамически изменяющихся показаний датчика.

Методы диагностики, основанные на равенстве углов наклона характеристик измерения датчиков, не обнаруживают ситуации, когда два датчика вместе закорочены, давая коррелированные показания в точке пересечения, или при отказах по общей причине, когда один компонент, например АЦП, одинаково повреждает значения обоих датчиков. Альтернативный подход, основанный на одном полном и одном половинном углах наклона характеристик измерения датчиков, приведен на рисунке D.6.



X — физическое показание датчика в %; Y — измеренное показание датчика в % от опорного напряжения; *1* — датчик 1; *2* — датчик 2; *3* — нижняя граница диапазона датчика 1; *4* — нижняя граница диапазона датчика 2; *5* — верхняя граница диапазона датчика 1; *6* — верхняя граница диапазона датчика 2

Рисунок D.5 — Датчики с границами областей допустимых значений, у которых равны, но имеют противоположный наклон характеристики измерения



D.2.10.3 Проверка обоснованности датчика

Примечание — Ссылка на данный механизм/меру приведена в таблице D.11.

Цель. Обнаружить дрейфы датчика в диапазоне, уходы нуля или другие ошибки, используя несколько различных датчиков.

Описание. Сравнение двух (или более) датчиков, измеряющих различные свойства, для обнаружения отказов в областях их допустимых значений таких, как дрейфы, уходы нуля или константные отказы. Измерения датчиков преобразуются в эквивалентные значения с использованием модели, обеспечивающей сравнение.

X — физическое показание датчика в %; Y — измеренное показание датчика в % от опорного напряжения; *1* — датчик 1; *2* — датчик 2; *3* — нижняя граница диапазона датчика 1; *4* — верхняя граница диапазона датчика 1; *5* — нижняя граница диапазона датчика 2; *6* — верхняя граница диапазона датчика 2

Рисунок D.6 — Датчики с границами областей допустимых значений, у которых углы наклона характеристик измерения различаются в два раза

Пример — Сравнение датчиков позиции дроссельной заслонки бензинового двигателя, давления во всасывающем коллекторе и массы воздушного потока выполняется после преобразования значения каждого из них в значение расхода воздуха. Использование разнообразных датчиков уменьшает проблему систематических ошибок.

D.2.11 Исполнительные элементы

Главная Цель. Управлять отказами в исполнительных элементах системы.

D.2.11.1 Мониторинг

П р и м е ч а н и е — Ссылка на данный механизм/меру приведена в таблице D.12.

Цель. Обнаружить неверную работу исполнительного элемента.

Описание. Работа исполнительного элемента контролируется.

П р и м е ч а н и е — Мониторинг исполнительного элемента может производиться на уровне физических измерений параметров (который может иметь высокий охват), а так же на уровне системы, рассматривая влияние отказа исполнительного элемента.

Примеры

1 Для вентилятора охлаждающего радиатор, процедура мониторинга на уровне системы использует датчик температуры для обнаружения отказа вентилятора охлаждающего радиатор. При мониторинге физических параметров измеряется напряжение или ток или оба вместе на входах вентилятора охлаждения радиатора.

2 Для перемещения дроссельной заслонки в желаемое положение используется управление с обратной связью. Фактическое положение измеряется и сравнивается с ожидаемым положением дроссельной заслонки, определяемым из положения дроссельной заслонки, которое задается командой водителя, и модели желаемой характеристики работы двигателя. Если эти два значения различаются друг от друга с учетом гистерезиса, то может быть сформировано сообщение об ошибке.

Приложение Е
(справочное)

Пример вычисления метрик архитектуры аппаратных средств: метрики одиночного сбоя и метрики скрытого сбоя

В настоящем приложении приводится пример расчета метрики одиночного сбоя и метрики скрытого сбоя для каждой цели безопасности конкретного устройства в соответствии с требованиями перечисления а) 8.4.7 и 8.4.8.

В рассматриваемом примере система реализует две функции, выполняемые в одном электронном блоке управления, представленном на рисунке Е.1.

Функция 1 имеет один вход (температура, измеренная датчиком R3) и один выход (клапан 2, управляемый I71) и предназначена для того, чтобы открыть клапан 2, когда температура превышает 90 °С.

Если через I71 ток не протекает, то клапан 2 открыт.

Соответствующая цель безопасности 1 формулируется следующим образом: «Клапан 2 не должен быть закрыт дольше *x* мс при температуре выше 100 °С». Данной цели безопасности назначается значение УПБА, равное В. Безопасное состояние: клапан 2 открыт.

Значение датчика R3 считывается блоком АЦП микроконтроллера. Значение сопротивления R3 уменьшается при повышении температуры. Данный вход не контролируется. Выходной каскад, управляемый Т71, контролируется аналоговым входом InADC1 (механизм безопасности SM1 в таблицах рисунков Е.2 и Е.3). В данном примере предполагается, что механизм безопасности SM1 может обнаружить определенные виды отказов Т71 с 90 %-ным охватом диагностикой, приводящие к нарушению цели безопасности. Если SM1 обнаруживает отказ, то активируется безопасное состояние, но никакая лампа не включается. Таким образом, считается, что охват диагностикой скрытых сбоев составляет только 80 % (водитель заметит отказ, так как начнется ухудшение функционирования автомобиля).

У функции 2 два входа (скорость вращения колеса измеряется с помощью датчиков I1 и I2, генерирующих импульсы) и один выход (клапан 1, управляемый I61) и она предназначена, чтобы открыть клапан 1, если скорость автомобиля превышает 90 км/час.

Если через I61 ток не протекает, то клапан 1 открыт.

Соответствующая цель безопасности 2 формулируется следующим образом: «Клапан 1 не должен быть закрыт дольше, чем *y* мс, если скорость превышает 100 км/час». Данной цели безопасности назначается значение УПБА, равное С. Безопасное состояние: клапан 1 открыт.

Количество сгенерированных датчиками I1 и I2 импульсов считывается микроконтроллером. Скорость вращения колеса вычисляется по среднему значению импульсов, получаемых от датчиков в единицу времени. Механизм безопасности 2 (SM2 в таблицах рисунков Е.2 и Е.3) сравнивает оба входа. Он обнаруживает отказы каждого входа с охватом диагностикой, равным 99 %. В случае противоречивости на выходе Out 1 устанавливается значение «0» и клапан 1 открывается (нулевое значение напряжения на базе транзистора закрывает вентиль; нулевое значение напряжения на I61 открывает клапан 1). Таким образом, выявляется 99 % сбоев, которые могут нарушить цель безопасности, и выполняется переход в безопасное состояние. При переходе в безопасное состояние включается лампа L1. Таким образом, эти сбои являются на 100 % воспринимаемыми. Оставшийся 1 % сбоев является остаточными сбоями и не скрытыми сбоями.

Выходной каскад управления Т61 контролируется аналоговым входом InADC2 (механизм безопасности SM3 в таблицах рисунков Е.2 и Е.3). Скорость вращения колеса вычисляется по среднему значению импульсов, получаемых от датчиков.

Микроконтроллер не имеет внутренней избыточности. Если нет никакой подробной информации о соотношении безопасных сбоев сложной части, то можно предположить консервативное отношение для безопасных сбоев, равное 50 %. Также предполагается общий охват, равный 90 %, по отношению к нарушению цели безопасности, используя внутреннее самотестирование и внешнюю сторожевую схему (механизм безопасности SM4 в таблицах рисунков Е.2 и Е.3). Сторожевая схема получает прямой сигнал через выход Out 0 микроконтроллера. Если сторожевая схема больше не обновляется, то ее выходное значение будет низким. Обнаружение сбоя механизмом безопасности SM4 (сторожевая схема и самотестирование микроконтроллера) переводит обе функции в их безопасные состояния и включает L1. Таким образом, считается, что охват диагностикой скрытых сбоев будет равен 100 %.

L1 представляет собой светодиодный индикатор на приборной панели, он горит при обнаружении множественного отказа, из которых только часть может быть обнаружена, и указывает водителю, что безопасное состояние функции 1 (клапан 1 открыт) было активировано.

Примечания

1 Отказы жгута проводов в данном примере не рассматриваются.

2 Модель сбоя, используемая для данной электронной части, может отличаться в зависимости от применения.

Пример — Модель сбоя резистора зависит от того, где он используется, в схеме цифрового входа (например, R11, R12, R13, ...) или аналогового входа (например, R63). В первом случае моделью сбоя может быть «разрыв/замыкание» тогда, как во втором случае, это может быть «разрыв/замыкание/дрейф».

Примечание — Первая метрика используется только для охвата вида отказов механизмами безопасности, целью которых является предотвращение нарушений цели безопасности. Вторая метрика используется только для охвата вида отказов механизмами безопасности, целью которых является предотвращение скрытых отказов среди этого вида отказов.

Пример — Вид отказов «разрыв» для R21 может нарушить цель безопасности 2 в отсутствии механизма безопасности. Механизм безопасности 3 обнаруживает этот вид отказов с охватом 99 % и переводит систему в безопасное состояние. При обнаружении этого вида отказов, будет выдано предупреждение; охват вида отказов в случае скрытых отказов составляет 100 %.

Примечание — В данном примере были рассмотрены предположения о распределении вида отказов в элементах аппаратных средств. Если никакое конкретное распределение вида отказов не может быть обосновано или предложено, то можно предположить равномерное распределение видов отказов.

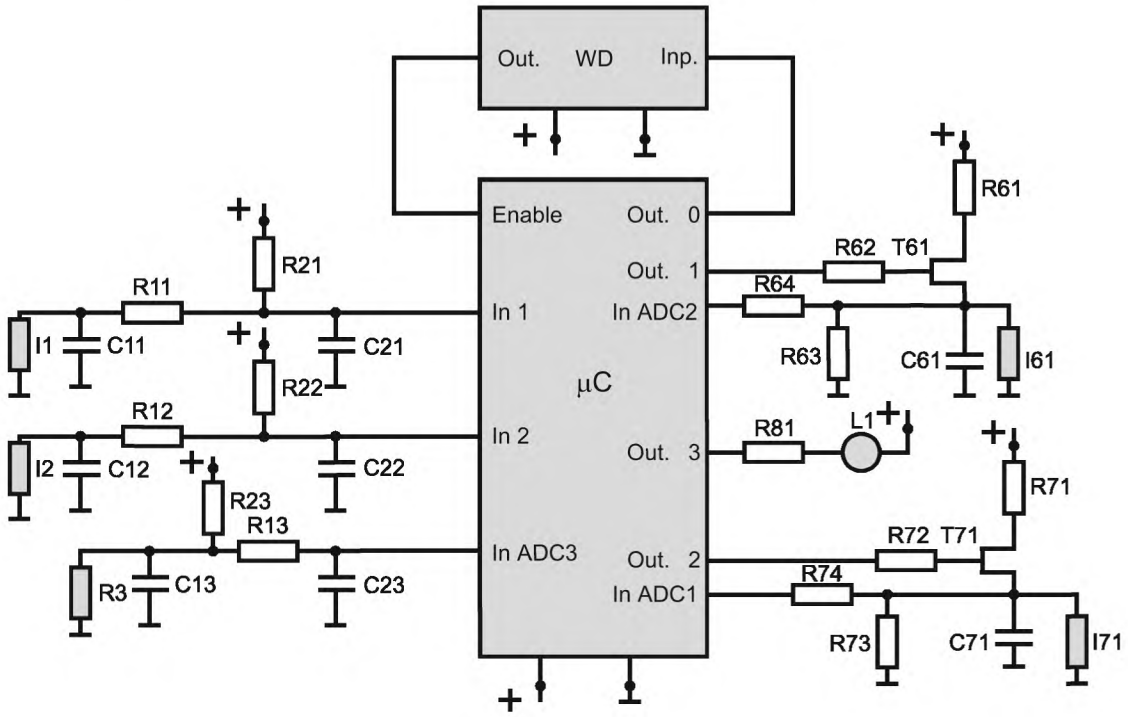


Рисунок Е.1 — Схема рассматриваемого примера

Обратите внимание на то, что в таблицах рисунков Е.2 и Е.3 охват механизмом безопасности конкретного вида отказов элемента аппаратного средства называют «охватом вида отказов».

Наименование компонента	Интенсивность отказа/FIT	Учитывается ли в расчетах связанный с безопасностью компонент?	Вид отказа	Распределение интенсивностей отказов	Какой вид отказа может нарушить цель безопасности в отсутствие механизмов безопасности?	Имеется ли механизм(ы) безопасности, позволяющий предотвратить нарушение цели безопасности?	Охват вида отказов, нарушающего цель безопасности	Интенсивность остаточных отказов для одиночных сбоев/FIT	Может ли вид отказов привести к нарушению цели безопасности в сочетании с независимым отказом другого компонента?	Есть ли средства обнаружения? Есть ли механизм(ы) безопасности, предотвращающий скрытые отказы среди этого вида отказов?	Охват вида отказов в случае скрытых отказов	Интенсивность отказов от скрытых множественных сбоев/FIT
R3. Примечание 1	3	Да	Разрыв	30 %	X	Нет	0 %	0,9				
			Замыкание	10 %								
			Дрейф 0,5	30 %								
			Дрейф 2	30 %	X		0 %	0,9				
R13. Примечания 1, 2 и 7	2	Да	Разрыв	90 %	X	Нет	0 %	1,8				
			Замыкание	10 %	X		0 %	0,2				
R23. Примечание 1	2	Да	Разрыв	90 %		Нет						
			Замыкание	10 %	X		0 %	0,2				
C13. Примечания 3 и 7	2	Да	Разрыв	20 %	X	Нет	0 %	0,4				
			Замыкание	80 %								
C23	2	Нет	Разрыв	20 %								
			Замыкание	80 %								
Сторожевая схема (WD)	20	Да	Константная «1» на вых.	50 %					X	Нет	0 %	10
			Константный «0» на вых.	50 %								
T71	5	Да	Вентиль откр.	50 %		SM1				SM1		
			Вентиль закр.	50 %	X		90 %	0,25	X		80 %	0,45

Рисунок Е.2 — Цель безопасности 1

Наименование компонента	Интенсивность отказа/FIT	Учитывается ли в расчетах связанный с безопасностью компонент?	Вид отказа	Распределение интенсивностей отказов	Какой вид отказа может нарушить цель безопасности в отсутствие механизмов безопасности?	Имеется ли механизм(ы) безопасности, позволяющий предотвратить нарушение цели безопасности?	Охват вида отказов, нарушающего цель безопасности	Интенсивность остаточных отказов для одиночных сбоев/FIT	Может ли вид отказов привести к нарушению цели безопасности в сочетании с независимым отказом другого компонента?	Есть ли средства обнаружения? Есть ли механизм(ы) безопасности, предотвращающий скрытые отказы среди этого вида отказов?	Охват вида отказов в случае скрытых отказов	Интенсивность отказов от скрытых множественных сбоев/FIT
R71. Примечания 2 и 7	2	Да	Разрыв	90 %						Нет		
			Замыкание	10 %					X		0 %	0,2
R72. Примечания 2 и 7	2	Да	Разрыв	90 %						Нет		
			Замыкание	10 %					X		0 %	0,2
R73	2	Нет	Разрыв	90 %								
			Замыкание	10 %								
R74. Примечания 2 и 7	2	Да	Разрыв	90 %					X	Нет	0 %	1,8
			Замыкание	10 %					X		0 %	0,2
I71	5	Нет	Разрыв	70 %								
			Замыкание	20 %								
C71. Примечание 3	2	Да	Разрыв	20 %					X	Нет		0,4
			Замыкание	80 %								
R81	2	Нет	Разрыв	90 %								
			Замыкание	10 %								
L1	10	Нет	Разрыв	90 %								
			Замыкание	10 %								
Микроконтроллер	100	Да	Все	50 %	X	SM4	90 %	5	X	SM4	100 %	0
			Все	50 %								
							Σ = 9,65				Σ = 13,25	

Рисунок Е.2, лист 2

Общая интенсивность отказов — 163.

Общее количество связанных с безопасностью отказов — 142.

Общее количество не связанных с безопасностью отказов — 21.

Метрика одиночных сбоев = 1 – (9,65/142) = 93,2 %

Метрика скрытых сбоев = 1 – (13,25/(142 – 9,65)) = 90,0 %

Цели безопасности 1 назначено значение УПБА, равное B, для которого, если используется таблица 4, рекомендуется значение метрики одиночных сбоев ≥ 90 % и, если используется таблица 5, рекомендуется значение метрики скрытых сбоев ≥ 60 %. Рассчитанное значение метрики одиночных сбоев 93,2 % удовлетворяет рекомендуемому значению метрики, а также рассчитанное значение метрики скрытых сбоев 90 % удовлетворяет рекомендуемому значению метрики.

Примечания

1 Виды отказов «разрыв» на R3 и R13 и «замыкание» на R23 являются одиночными сбоями. Они непосредственно приводят к нарушению цели безопасности и никакой механизм безопасности не охватывает сбои этих частей аппаратных средств.

2 Целью данной части аппаратного средства является электрическая защита. Вид отказа «замыкание» означает потерю защиты.

3 Целью данной части аппаратного средства является защита от электростатических разрядов. Вид отказа «разрыв» означает потерю защиты.

4 Целью данной части аппаратного средства является электрическая защита. Один вид отказов приводит к потере электрической защиты. Другой вид отказов может нарушить цель безопасности в отсутствие механизмов безопасности.

5 Элементы, отказы которых не могут внести существенный вклад в нарушение цели безопасности, не учитываются в расчетах. Элементы L1 и R81 реализуют механизм безопасности для предотвращения скрытых сбоев среди двойных сбоев. Множественные сбои с $n > 2$ считаются безопасными сбоями.

6 Сбои, которые непосредственно ведут к нарушению цели безопасности (одиночные сбои или остаточные сбои), не могут больше вносить вклад в совокупность скрытых сбоев. Поэтому, например, интенсивность скрытых отказов вида «вентиль закрыт» для T71 вычисляется следующим образом:

$$\lambda_{MPF,\,L} = [(\lambda_{T71} \times \text{Распределение_интесивностей_отказов}_{\text{вентиль закрыт}}) - \lambda_{T71RF}] \times (1 - \text{Охват}_{\text{скрытых_отказов}}) = [(5 \times 0{,}1) - 0{,}05] \times (1 - 0{,}8) = 0{,}09.$$

7 Классификация видов отказов вследствие электростатических разрядов или нарушения электрической защиты основана на анализе каждого конкретного случая и учитывает вероятность электростатических разрядов или электрической нагрузки и характерные последствия от влияния электростатических разрядов или электрической нагрузки на цель безопасности. Если, например, в течение срока службы автомобиля произойдет электростатический разряд и его последствия могут привести к нарушению цели безопасности в отсутствие данной защиты, то вид отказов, ведущий к потере защиты, классифицируется как одиночный сбой. Настоящее приложение является примером обработки таких случаев в метриках. На практике электростатические разряды или напряжение электромагнитных помех не имеют такого влияния на типовые проекты, аналогичные рассматриваемому в настоящем примере.

Рисунок Е.2, лист 3

Наименование компонента	Интенсивность отказа/FIT	Учитывается ли в расчетах связанный с безопасностью компонент?	Вид отказа	Распределение интенсивностей отказов	Какой вид отказа может нарушить цель безопасности в отсутствие механизмов безопасности?	Имеется ли механизм(ы) безопасности, позволяющий предотвратить нарушение цели безопасности?	Охват вида отказов, нарушающего цель безопасности	Интенсивность остаточных отказов для одиночных сбоев/FIT	Может ли вид отказов привести к нарушению цели безопасности в сочетании с независимым отказом другого компонента?	Есть ли средства обнаружения? Есть ли механизм(ы) безопасности, предотвращающий скрытые отказы среди этого вида отказов?	Охват вида отказов в случае скрытых отказов	Интенсивность отказов от скрытых множественных сбоев/FIT
1	2	3	4	5	6	7	8	9	10	11	12	13
R11. Приложения 1, 6 и 7	2	Да	Разрыв	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			Замыкание	10 %	X		99 %	0,002	X		100 %	0
R12. Приложения 1, 6 и 7	2	Да	Разрыв	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			Замыкание	10 %	X		99 %	0,002	X		100 %	0
R21. Приложение 2	2	Да	Разрыв	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			Замыкание	10 %	X		99 %	0,002	X		100 %	0
R22. Приложение 2	2	Да	Разрыв	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			Замыкание	10 %	X		99 %	0,002	X		100 %	0
C11. Приложения 1, 6 и 7	2	Да	Разрыв	20 %	X	SM2	99 %	0,004	X	SM2	100 %	0
			Замыкание	80 %	X		99 %	0,016	X		100 %	0
C12. Приложения 1, 6 и 7	2	Да	Разрыв	20 %	X	SM2	99 %	0,004	X	SM2	100 %	0
			Замыкание	80 %	X		99 %	0,016	X		100 %	0
C21	2	Да	Разрыв	20 %		SM2				SM2		
			Замыкание	80 %	X		99 %	0,016	X		100 %	0
C22	2	Да	Разрыв	20 %		SM2				SM2		
			Замыкание	80 %	X		99 %	0,016	X		100 %	0
I1	4	Да	Разрыв	70 %	X	SM2	99 %	0,028	X	SM2	100 %	0
			Замыкание	20 %	X		99 %	0,008	X		100 %	0
			Дрейф 0,5	5 %	X		99 %	0,002	X		100 %	0
			Дрейф 2	5 %								

Рисунок Е.3 — Цель безопасности 2

Наименование компонента	Интенсивность отказа/FIT	Учитывается ли в расчетах связанный с безопасностью компонент?	Вид отказа	Распределение интенсивностей отказов	Какой вид отказа может нарушить цель безопасности в отсутствие механизмов безопасности?	Имеется ли механизм(ы) безопасности, позволяющий предотвратить нарушение цели безопасности?	Охват вида отказов, нарушающего цель безопасности	Интенсивность остаточных отказов для одиночных сбоев/FIT	Может ли вид отказов привести к нарушению цели безопасности в сочетании с независимым отказом другого компонента?	Есть ли средства обнаружения? Есть ли механизм(ы) безопасности, предотвращающий скрытые отказы среди этого вида отказов?	Охват вида отказов в случае скрытых отказов	Интенсивность отказов от скрытых множественных сбоев/FIT
I2	4	Да	Разрыв	70 %	X	SM2	99 %	0,028	X	SM2	100 %	0
			Замыкание	20 %	X		99 %	0,008	X		100 %	0
			Дрейф 0,5	5 %	X		99 %	0,002	X		100 %	0
			Дрейф 2	5 %								
Сторожевая схема (WD)	20	Да	Константная «1» на вых.	50 %					X	Нет	0 %	10
			Константный «0» на вых.	50 %								
T61	5	Да	Вентиль откр.	50 %		SM3				SM3		
			Вентиль закр.	50 %	X		90 %	0,25	X		100 %	0
R61. Приложения 3 и 6	2	Да	Разрыв	90 %						Нет		
			Замыкание	10 %					X		0 %	0,2
R62. Приложения 3 и 6	2	Да	Разрыв	90 %						Нет		
			Замыкание	10 %					X		0 %	0,2
R63	2	Нет	Разрыв	90 %								
			Замыкание	10 %								
R64. Приложения 1 и 6	2	Да	Разрыв	90 %					X	Нет	0 %	1,8
			Замыкание	10 %					X		0 %	0,2

Рисунок Е.3, лист 2

Наименование компонента	Интенсивность отказа/FIT	Учитывается ли в расчетах связанный с безопасностью компонент?	Вид отказа	Распределение интенсивностей отказов	Какой вид отказа может нарушить цель безопасности в отсутствие механизмов безопасности?	Имеется ли механизм(ы) безопасности, позволяющий предотвратить нарушение цели безопасности?	Охват вида отказов, нарушающего цель безопасности	Интенсивность остаточных отказов для одиночных сбоев/FIT	Может ли вид отказов привести к нарушению цели безопасности в сочетании с независимым отказом другого компонента?	Есть ли средства обнаружения? Есть ли механизм(ы) безопасности, предотвращающий скрытые отказы среди этого вида отказов?	Охват вида отказов в случае скрытых отказов	Интенсивность отказов от скрытых множественных сбоев/FIT
I61	5	Нет	Разрыв	70 %								
			Замыкание	20 %								
C61. Приложения 4 и 6	2	Да	Разрыв						X	Нет	0 %	0,4
			Замыкание	80 %								
R81	2	Нет	Разрыв	90 %								
			Замыкание	10 %								
L1	10	Нет	Разрыв	90 %								
			Замыкание	10 %								
Микроконтроллер	100	Да	Все	50 %	X	SM4	90 %	5	X	SM4	100 %	0
			Все	50 %								
								Σ = 5,48				Σ = 12,80

Общая интенсивность отказов — 176.

Общее количество связанных с безопасностью отказов — 157.

Общее количество не связанных с безопасностью отказов —19.

Метрика одиночных сбоев = 1 – (5,48/157) = 96,5 %

Метрика скрытых сбоев = 1 – (13,99/(157 – 5,48)) = 91,6 %

Цели безопасности 2 назначено значение УПБА, равное С, для которого, если используется таблица 4, рекомендуется значение метрики одиночных сбоев ≥ 97 % и, если используется таблица 5, рекомендуется значение метрики скрытых сбоев ≥ 80 %. Рассчитанное значение метрики одиночных сбоев 96,5 % не удовлетворяет рекомендуемому значению метрики, а рассчитанное значение метрики скрытых сбоев 91,6 % удовлетворяет рекомендуемому значению метрики.

Рисунок Е.3, лист 3

Примечания

1 Целью данной части аппаратного средства является электрическая защита. Один вид отказов приводит к потере электрической защиты. Другой вид отказов может нарушить цель безопасности в отсутствие механизмов безопасности.

2 Оба вида отказов могут нарушить цель безопасности в отсутствие механизмов безопасности, так как в обоих случаях импульсы, измеряющие скорость, не передаются. Это приводит к получению неправильного значения скорости. Датчик является датчиком с открытым коллектором.

3 Целью данной части аппаратного средства является электрическая защита. Вид отказа «замыкание» означает потерю защиты.

4 Целью данной части аппаратного средства является защита от электростатических разрядов. Вид отказа «разрыв» означает потерю защиты.

5 Элементы, отказы которых не могут внести существенный вклад в нарушение цели безопасности, не учитывается в расчетах. L1 и R81 являются элементами, которые реализуют механизм безопасности для предотвращения скрытых сбоев среди двойных сбоев. Множественные сбои с $n > 2$ считаются безопасными сбоями.

6 Классификация видов отказов вследствие электростатических разрядов или нарушения электрической защиты основана на анализе каждого конкретного случая и учитывает вероятность электростатических разрядов или электрической нагрузки и характерные последствия от влияния электростатических разрядов или электрической нагрузки на цель безопасности. Если, например, в течение срока службы автомобиля произойдет электростатический разряд и его последствия могут привести к нарушению цели безопасности в отсутствие данной защиты, то вид отказов, ведущий к потере защиты, классифицируется как одиночный сбой. Настоящее приложение является примером обработки таких случаев в метриках. На практике электростатические разряды или напряжение электромагнитных помех не имеют такого влияния на типовые проекты, аналогичные рассматриваемому в настоящем примере. Более того, предполагается, что в данном случае SM4 не охватывает эти виды отказов, даже если они могут привести к некоторому повреждению микроконтроллера.

7 Потеря электрической защиты вызовет неправильное входное значение, которое будет обнаружено SM2, и, следовательно, не будет считаться скрытым сбоем.

Рисунок Е.3, лист 4

Приложение F
(справочное)

Применение коэффициентов масштабирования

Коэффициент масштабирования является фактором, который используется для объединения отказов из нескольких источников в расчетах вероятностных метрик для случайных отказов аппаратных средств (PMHF).

Целевые значения, определенные в 9.4.2.1, для PMHF для каждой цели безопасности могут быть получены из одного из трех источников:

- таблицы 6; или
- полевых данных устройств, использовавших подобные хорошо зарекомендовавшие себя принципы разработки; или
- результатов количественных методов анализа, применявшихся при аналогичных хорошо зарекомендовавших себя принципах разработки, для интенсивностей отказов, источники которых указаны в 8.4.3.

Чтобы убедиться, что проект аппаратных средств соответствует заданным целевым значениям, интенсивности отказов рассчитываются для частей аппаратных средств. Интенсивность отказов частей аппаратных средств может быть оценена на основе одного из трех источников, описанных в 8.4.3:

a) данных об интенсивностях отказов частей аппаратных средств из признанных источников промышленности; или

b) статистических данных, полученных из эксплуатации или испытаний (с достаточным уровнем доверия); или

c) экспертной оценки, основанной на инженерном подходе, использующем количественные и качественные методы.

Таким образом, в расчетах для различных частей аппаратных средств устройства могут быть использованы различные источники интенсивностей отказов.

Пусть T_a, T_b и T_c — три возможных источника для определения целевых значений PMHF, а также F_a, F_b и F_c — три возможных источника для оценки интенсивности отказов частей аппаратных средств. Пусть $\pi_{F_i \to F_j}$ будет коэффициентом масштабирования между источниками F_i и F_j. Данный коэффициент может быть использован для масштабирования интенсивности отказов части аппаратного средства на основе источника F_i относительно интенсивности отказов на основе источника F_j, как определено в формуле (F.1):

$$\pi_{F_i \to F_j} = \frac{\lambda_{k.F_j}}{\lambda_{k.F_i}}, \quad \text{(F.1)}$$

где $\lambda_{k.F_j}$ — интенсивность отказов части аппаратного средства, полученная из источника F_j;

$\lambda_{k.F_i}$ — интенсивность отказов той же части аппаратного средства, полученная из источника F_i.

В этом случае, зная соответствующий коэффициент масштабирования, можно для аналогичной части аппаратного средства из интенсивности отказов, полученной из источника F_i, вычислить интенсивность отказов, полученную источника F_i, по формуле (F.2):

$$\lambda_{k.F_j} = \pi_{F_i \to F_j} \times \lambda_{k.F_i}. \quad \text{(F.2)}$$

В таблице F.1 перечислены возможные сочетания целевых значений и интенсивностей отказов.

Примечания

1 Целевые значения в таблице 6 основаны на расчетах с использованием справочных данных, предполагая, что эти справочные данные очень пессимистичны.

2 Если источник целевых данных и интенсивностей отказов части аппаратного средства одинаков, то масштабирование не выполняется.

Таблица F.1 — Возможные сочетания источников целевых значений и интенсивностей отказов, обеспечивающие согласование интенсивностей отказов в расчетах

Источник данных для интенсивностей отказов частей аппаратных средств	Источник данных для целевых значений		
	Таблица 6. Перечисление a) 9.4.2.1	Полевые данные. Перечисление b) 9.4.2.1	Количественный анализ. Перечисление c) 9.4.2.1
Накопленные базы данных. Перечисление a) 8.4.3	$\lambda_{k.F_a}$ a)	$\lambda_{k.F_b} = \pi_{F_a \to F_b} \times \lambda_{k.F_a}$	b)

Окончание таблицы F.1

Источник данных для интенсивностей отказов частей аппаратных средств	Источник данных для целевых значений		
	Таблица 6. Перечисление a) 9.4.2.1	Полевые данные. Перечисление b) 9.4.2.1	Количественный анализ. Перечисление c) 9.4.2.1
Статистические данные. Перечисление b) 8.4.3	$\lambda_{k.F_a} = \pi_{F_b \to F_a} \times \lambda_{k.F_b}$	$\lambda_{k.F_b}$	b)
Экспертная оценка. Перечисление c) 8.4.3	$\lambda_{k.F_a} = \pi_{F_c \to F_a} \times \lambda_{k.F_c}$	$\lambda_{k.F_b} = \pi_{F_c \to F_a} \times \lambda_{k.F_c}$	b)

[a] Для некоторых типов частей аппаратных средств различные справочники могут дать различные оценки интенсивности отказов для одного и того же типа частей аппаратных средств. Таким образом, коэффициент масштабирования может быть использован для масштабирования интенсивностей отказов части аппаратного средства, используя различные справочники.

[b] При согласованном подходе, интенсивности отказов имеют тот же источник, что и интенсивности отказов, используемые при расчете целевого значения.

Масштабирование возможно, если имеются достаточные доказательства, что существует коэффициент между двумя возможными источниками целевых значений.

Например, если существуют достаточные данные о системе «предшественнице», то ее интенсивность отказов можно считать ожидаемой для системы, реализуемой рассматриваемым устройством.

Пример — Можно показать, что 10^{-8}/ч с 99 %-ным уровнем уверенности аналогично 10^{-9}/ч с 70 %-ным уровнем уверенности. Таким образом, интенсивности отказов на основе признанных отраслевых источников с 99 %-ным уровнем уверенности можно масштабировать для отказов на основе статистических данных с 70 %-ным уровнем уверенности, используя коэффициент масштабирования $\pi_{F_a \to F_b} = (10^{-9}/ч)/(1^{-8}/ч) = 1/10$, или наоборот.

Примечание — Опираясь на опыт, 99 %-ный уровень уверенности можно применять для интенсивностей отказов на основе признанных отраслевых источников, упомянутых в 8.4.3.

Пример — Из предыдущего проекта были получены интенсивности отказов, рассчитанные из данных справочника, и данные гарантийного обслуживания. В результате было получено:

$$\lambda_{справочник} / \lambda_{гарантия} = \pi_{F_b \to F_a} = 10, \quad (F.3)$$

где $\lambda_{справочник}$ — ***интенсивности отказов, рассчитанные из данных справочника;***

$\lambda_{гарантия}$ — ***интенсивности отказов, рассчитанные из данных гарантийного обслуживания;***

$\pi_{F_b \to F_a}$ — ***полученный коэффициент масштабирования.***

Если в новом проекте используются справочные данные для определения интенсивностей отказов за исключением одной части аппаратного средства (часть 1 аппаратного средства), для которой имеются только данные гарантийного обслуживания, то с помощью масштабирования можно определить справочные данные для этой части аппаратного средства:

$$\lambda_{1,\ справочник} = \pi_{F_b \to F_a} \times \lambda_{1,\ гарантия}, \quad (F.4)$$

где $\lambda_{1,\ справочник}$ — ***интенсивности отказов части 1 аппаратного средства, рассчитанные из данных справочника;***

$\lambda_{1,\ гарантия}$ — ***интенсивности отказов части 1 аппаратного средства, рассчитанные из данных гарантийного обслуживания.***

Например, если $\lambda_{1,\ гарантия} = 9 \times 10/ч$, ***то может быть рассчитано значение***

$$\lambda_{1,\ справочник} = (9 \times 10^{-9}) \times 10 = (9 \times 10^{-8})/ч.$$

Используя полученное значение $\lambda_{1,\ справочник}$, ***может быть выполнена согласованная оценка нарушения цели безопасности из-за случайных отказов аппаратных средств.***

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 26262-1:2011	—	*
ИСО 26262-2:2011	—	*
ИСО 26262-3:2011	—	*
ИСО 26262-4:2011	—	*
ИСО 26262-6:2011	—	*
ИСО 26262-7:2011	—	*
ИСО 26262-8:2011	—	*
ИСО 26262-9:2011	—	*

* 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] ISO 7637-2, Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only

[2] ISO 7637-3, Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines

[3] ISO 10605, Road vehicles — Test methods for electrical disturbances from electrostatic discharge

[4] ISO 11452-2, Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 2: Absorber-lined shielded enclosure

[5] ISO 11452-4, Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 4: Harness excitation methods

[6] ISO 16750-2, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 2: Electrical loads

[7] ISO 16750-4, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 4: Climatic loads

[8] ISO 16750-5, Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 5: Chemical loads

[9] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[10] IEC 61709, Electronic components — Reliability — Reference conditions for failure rates and stress models for conversion

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

[12] IEC/TR 62380, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment

[13] EN 50129:2003, Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling

[14] MIL HDBK 217 F notice 2, Military handbook: Reliability prediction of electronic equipment

[15] MIL HDBK 338, Military handbook: Electronic reliability design handbook

[16] NPRD 95, Non-electronic Parts Reliability Data

[17] RIAC FMD 97, Failure Mode/Mechanism Distributions

[18] RIAC HDBK 217 Plus, Reliability Prediction Models

[19] UTE C80-811, Reliability methodology for electronic systems

[20] VAN DE GOOR, A.J.: Testing Semiconductor Devices, Theory and Practice, A.J. van de Goor/ComTex Publishing, 1999

[21] SUNDARAM, P. and D'AMBROSIO, J.G., Controller Integrity in Automotive Failsafe System Architectures, SAE 2006 World Congress, 2006-01-0840

[22] FRUELING, T., Delphi Secured Microcontroller Architecture, SAE 2000 World Congress, SAE#2000-01-1052

[23] MAHMOOD, A. and MCCLUSKEY, E.J., «Concurrent Error Detection Using Watchdog Processors — A Survey», IEEE Trans. Computers, 37(2), 160—174 (1988)

[24] LEAPHART, E., CZERNY, B., D'AMBROSIO, J., et al, Survey of Software Failsafe Techniques for Safety-Critical Automotive Applications, SAE 2005 World Congress, 2005-01-0779

[25] MARIANI, R., FUHRMANN, P., VITTORELLI, B., Cost-effective Approach to Error Detection for an Embedded Automotive Platform, 2006-01-0837, SAE 2006 World Congress & Exhibition, April 2006, Detroit, MI, USA

[26] PATEL, J., FUNG, L. «Concurrent Error Detection in ALU's by Recomputing with Shifted Operands», IEEE Transactions on Computers, Vol. C-31, pp. 417—422, July 1982

[27] FORIN, P., Vital Coded Microprocessor: Principles and Application for various Transit Systems, Proc. IFAC-GCCT, Paris, France, 1989

[28] RAMABADRAN, T.V.; Gaitonde, S.S. (1988). «A tutorial on CRC computations». IEEE Micro 8 (4): 62—75, 1988

[29] Koopman, Philip; Chakravarty, Tridib (2004). Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks The International Conference on Dependable Systems and Networks, DSN-2004,

gost.e-ecolog.ru

УДК 62-783:614.8:331.454:006.354 ОКС 43.040.10 Т51

Ключевые слова: функциональная безопасность; жизненный цикл систем; транспортные средства; электрические компоненты; электронные компоненты; программируемые электронные компоненты и системы; аппаратные средства, разработка

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *С.В. Смирнова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 20.08.2015. Подписано в печать 26.10.2015. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 8,84. Уч.-изд. л. 7,95. Тираж 32 экз. Зак. 3344.

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

gost.e-ecolog.ru