ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-10— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 10

Руководящие указания по ИСО 26262

ISO 26262-10:2012
Road vehicles – Functional safety – Part 10: Guideline on ISO 26262
(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 стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 17 ноября 2014 г. № 1624-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-10:2012 «Дорожные транспортные средства. Функциональная безопасность. Часть 10. Руководящие указания по ИСО 26262» (ISO 26262-10:2012 «Road vehicles — Functional safety — Part 10: Guideline on ISO 26262»).

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 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 ... 1
3 Термины, определения и сокращения ... 2
4 Основные понятия ИСО 26262 ... 2
4.1 Функциональная безопасность систем транспортного средства (связь с МЭК 61508) ... 2
4.2 Устройство, система, элемент, компонент, часть аппаратного средства и модуль программного обеспечения ... 4
4.3 Отношения между сбоями, ошибками и отказами ... 6
5 Отдельные вопросы, связанные с управлением безопасностью ... 7
5.1 Результат работы ... 7
5.2 Меры подтверждения ... 7
5.3 Обоснования безопасности ... 9
6 Стадия формирования концепции и разработка системы ... 11
6.1 Общие положения ... 11
6.2 Пример анализа опасностей и оценки рисков ... 11
6.3 Замечания о классификации управляемости ... 11
6.4 Внешние меры ... 12
6.5 Пример объединения целей безопасности ... 13
7 Структура требований к процессу обеспечения безопасности. Последовательность выполнения требований к безопасности ... 14
8 Разработка аппаратных средств ... 15
8.1 Классификация случайных сбоев аппаратных средств ... 15
8.2 Пример оценки интенсивности остаточных отказов и метрики локального одиночного сбоя ... 20
8.3 Об аппаратных средствах ... 30
9 Общеиспользуемый элемент безопасности ... 31
9.1 Разработка общеиспользуемого элемента безопасности ... 31
9.2 Сценарии использования ... 32
10 Пример подтверждения проверкой эксплуатацией ... 38
10.1 Общие положения ... 38
10.2 Определение устройства и определение кандидата, проверенного эксплуатацией ... 39
10.3 Анализ изменений ... 39
10.4 Целевые значения для проверки эксплуатацией ... 39
11 О декомпозиции значений УПБА ... 40
11.1 Цель декомпозиции значений УПБА ... 40
11.2 Описаниие декомпозиции значений УПБА ... 40
11.3 Пример декомпозиции значений УПБА ... 40
Приложение А (справочное) ИСО 26262 и микроконтроллеры ... 44
Приложение В (справочное) Формирование и применение дерева неисправностей ... 72
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации ... 87
Библиография ... 87

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.

Эта 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.

1. Словарь

2. Управление функциональной безопасностью

- **2-5** Общее управление системой безопасности
- **2-6** Управление системой безопасности на стадиях формирования концепции и разработки изделия
- **2-7** Управление системой безопасности после запуска устройства в производство

3. Стадия формирования концепции

- **3-5** Определение устройства
- **3-5** Формирование жизненного цикла системы безопасности
- **3-7** Анализ опасностей и оценка риска
- **3-8** Концепция функциональной безопасности

4. Разработка изделия на уровне системы

- **4-5** Начальная подстадия разработки изделия на уровне системы
- **4-6** Спецификация технических требований к системе безопасности
- **4-7** Проектирование системы
- **4-8** Интеграция и тестирование устройства
- **4-9** Подтверждение соответствия безопасности
- **4-10** Оценка функциональной безопасности
- **4-11** Запуск в производство

5. Разработка изделия на уровне аппаратного обеспечения

- **5-5** Начальная подстадия разработки изделия на уровне аппаратного обеспечения
- **5-6** Спецификация требований к аппаратным средствам системы безопасности
- **5-7** Проектирование аппаратных средств
- **5-8** Определение метрик архитектуры аппаратных средств
- **5-9** Оценка нарушений цели безопасности вследствие случайных отказов аппаратных средств
- **5-10** Интеграция и тестирование аппаратных средств

6. Разработка изделия на уровне программного обеспечения

- **6-5** Начальная подстадия разработки программного обеспечения изделия
- **6-7** Проектирование архитектуры программного обеспечения
- **6-8** Проектирование и реализация модулей программного обеспечения
- **6-9** Тестирование модуля программного обеспечения
- **6-10** Интеграция и тестирование программного обеспечения
- **6-11** Верификация требований к безопасности программного обеспечения

7. Производство и эксплуатация

- **7-5** Производство
- **7-6** Эксплуатация, обслуживание (капитальный и текущий ремонты) и снятие с эксплуатации

8. Вспомогательные процессы

- **8-5** Интерфейсы внутри распределенных разработок
- **8-6** Спецификация и управление требованиями безопасности
- **8-7** Управление конфигурацией
- **8-8** Управление изменениями
- **8-9** Верификация
- **8-10** Документирование
- **8-11** Уверенность в использовании инструментального программного обеспечения
- **8-12** Квалификация компонентов программного обеспечения
- **8-13** Квалификация компонентов аппаратных средств
- **8-14** Подтверждение проверкой в эксплуатации

9. Анализ уровня полноты безопасности автомобиля и анализ безопасности автомобиля

- **9-5** Декомпозиция требований с распределением УПБА
- **9-6** Критерий совместимости элементов
- **9-7** Анализ зависимых отказов
- **9-8** Анализ системы безопасности

10. Руководящие указания по ИСО 26262

Рисунок 1 – Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 10

Руководящие указания по ИСО 26262

Road vehicles. Functional safety. Part 10. Guideline on ISO 26262

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 область его 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).

В настоящем стандарте сделан краткий обзор комплекса ИСО 26262, а также даны дополнительные объяснения к нему. Настоящий стандарт предназначен для улучшения понимания других частей комплекса ИСО 26262, носит только справочный характер и описывает общие понятия ИСО 26262. Объяснения даются как для общих понятий, так и для их конкретного содержания.

В случае расхождения между требованиями, рекомендациями или данными, используемыми в настоящем стандарте и в другой части комплекса ИСО 26262, применяются требования, рекомендации или данные, определенные в другой части комплекса ИСО 26262.

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)

Издание официальное

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 26262-5:2011 Дорожно-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)

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 применимы термины, определения и сокращения по ИСО 26262-1:2011.

4 Основные понятия ИСО 26262

4.1 Функциональная безопасность систем транспортного средства (связь с МЭК 61508)

Серия МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», является базовым стандартом МЭК в области функциональной безопасности. Это означает, что стандарты по функциональной безопасности, разрабатываемые для других секторов промышленности, будут основываться на требованиях МЭК 61508.

В автомобильной промышленности существует ряд областей, где МЭК 61508 применяется непосредственно. Некоторые из этих областей и их отличия в ИСО 26262 описаны ниже.

МЭК 61508 основывается на модели «управляемого оборудования» (например, промышленное предприятие, имеющее свою систему управления) следующим образом:

a) анализ опасностей идентифицирует опасности в управляемом оборудовании (в том числе в системе управления оборудованием), к которым будут применяться меры по снижению риска. Это может быть достигнуто с помощью Э/Э/ПЭ систем или систем, связанных с безопасностью, основанных на других технологиях (например, предохранительный клапан), или внешних мер по снижению риска (например, физические меры предосторожности предприятия). Настоящий стандарт содержит нормативную схему классификации опасностей транспортного средства в зависимости от их важности, вероятности влияния на них внешнего воздействия и управляемости;

b) снижение рисков, задаваемое Э/Э/ПЭ системам обеспечивается так называемыми функциями безопасности. Эти функции безопасности вместе с другими реализуются либо как отдельная система безопасности, либо могут быть включены в систему управления предприятием. Реализовывать отдельные системы безопасности в транспортном средстве не всегда разумно, так как безопасность транспортного средства зависит от поведения самих систем управления.

ИСО 26262 реализует концепцию целей безопасности и концепцию обеспечения безопасности, следующим образом:

- анализ опасностей и оценка рисков определяет опасности и опасные события, которые должны быть предотвращены, смягчены или должны контролироваться;

- цель безопасности формулируется для каждого опасного события;

- уровень полноты безопасности автомобиля (УПБА) связан с каждой целью безопасности;

- концепцией обеспечения функциональной безопасности является описание функциональности системы, связанной с безопасностью, которая необходима для достижения цели(ей) безопасности;

- технической концепцией обеспечения безопасности является положение о том, как эта функциональность реализуется на уровне системы аппаратными средствами и программным обеспечением;

- требования к программному обеспечению системы безопасности и требования к ее аппаратным средствам устанавливают конкретные требования к системе безопасности, которые будут реализованы в процессе проектирования программного обеспечения и аппаратных средств.

Пример — Система подушек безопасности:

- одной из опасностей является непреднамеренное их раскрытие;

- соответствующая цель безопасности заключается в том, что подушка безопасности не раскрывается, если не происходит аварии, требующей ее раскрытия;

- концепция обеспечения функциональной безопасности может определить дополнительную функцию для обнаружения столкновения автомобиля;

- техническая концепция обеспечения безопасности может определить реализацию двух независимых датчиков ускорения по различным осям и двух независимых схем запуска раскрытия. Петарда запускается, если обе схемы срабатывают.

МЭК 61508 предназначен для отдельных систем или систем невысокой сложности. Система создается и тестируется, затем устанавливается на предприятии и после этого для нее выполняется подтверждение соответствия системе безопасности. Для рынка массовых изделий, таких как транспортные средства, подтверждение соответствия системе безопасности выполняется перед началом их массового (серийного) производства. Поэтому порядок действий, выполняемых на стадиях жизненного цикла, описанный в ИСО 26262, иной. Так, например, в ИСО 26262-7 представлены требования к производству, которые в МЭК 61508 отсутствуют.

В МЭК 61508 не рассматриваются конкретные требования к управлению разработкой несколькими организациями и цепочками поставок, в то время как в ИСО 26262 этот вопрос рассматривается подробно, включая и соглашение об интерфейсе разработки (см. раздел 5 26262-8 «Взаимодействие в совместных разработках»), так как автотранспортные системы создаются одним или несколькими поставщиками заказчика, например производителем автотранспортных средств, поставщиком заказчика или заказчиком.

МЭК 61508 не содержит нормативных требований к классификации опасности. ИСО 26262 схему классификации опасностей автомобиля содержит. Данная схема признает, что опасность в системе автомобиля не обязательно приводит к аварии. Это зависит от результатов анализа, выполненного для лиц, подвергающихся риску: действительно ли они подвергаются опасности, если она возникает, и в состоянии ли они принять меры по управлению результатами опасных событий. На рисунке 2 приведен пример такого подхода для отказа, который влияет на управляемость движущегося транспортного средства.

Примечание — Данный подход призван лишь продемонстрировать, что не всегда существует прямая связь между произошедшим отказом и аварией. Это не выявляется в процессе анализа опасностей и оценки рисков, хотя оцениваемые параметры в этом процессе связаны с вероятностями переходов между состояниями, показанными на рисунке 2.

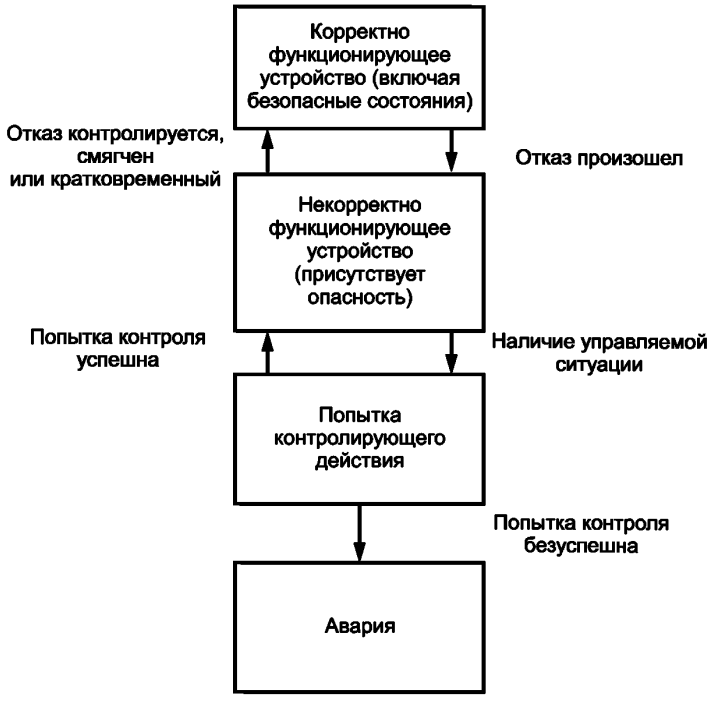


Рисунок 2 — Модель конечного автомата для оценки риска автомобиля

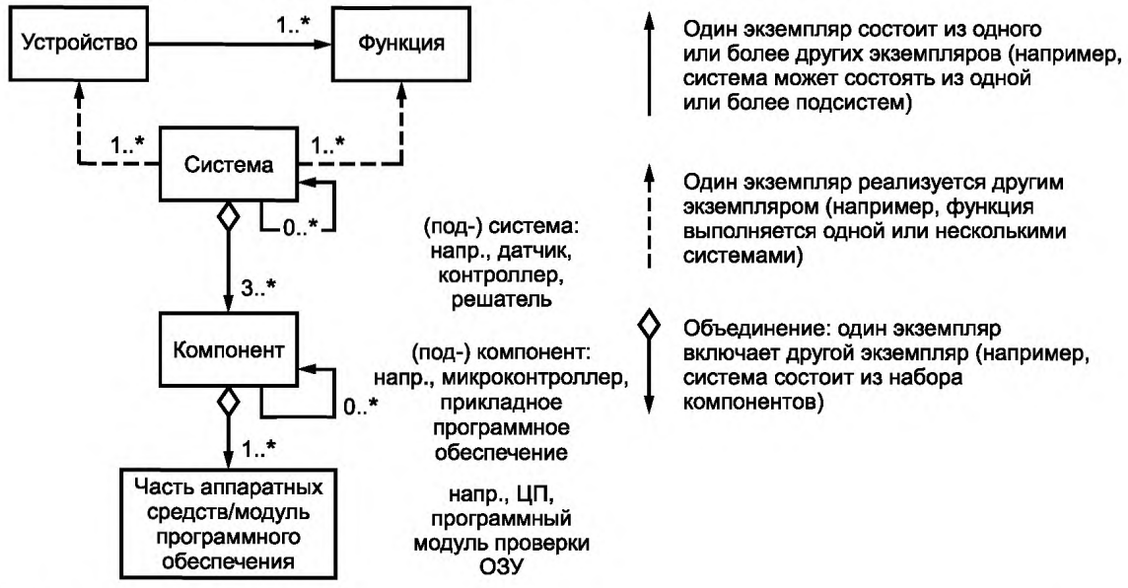
Требования для разработки аппаратных средств (ИСО 26262-5) и программного обеспечения (МСО 26262-6) адаптированы для современного автомобилестроения. В частности, ИСО 26262-6 содержит требования, связанные с разработкой на основе модели; МЭК 61508 предусматривает применения конкретных методов. Применение любого альтернативного метода должно быть подробно обосновано. Для методов, перечисленных в ИСО 26262, предоставляются конкретные цели. Для достижения этих целей могут быть применены предусмотренные методы или предусмотрено обоснование достижения цели альтернативными методами.

Требования к системе безопасности в настоящем стандарте определяется уровнем полноты безопасности автомобиля (УПБА), а не уровнем полноты безопасности (УПБ). Основное различие состоит в том, что УПБ в МЭК 61508 задается в вероятностных терминах (см. таблицу 3 МЭК 61508-1). В МЭК 61508 указано: «Принято считать, что только по отношению к полноте безопасности аппаратных средств возможно дать количественную оценку и использовать надежные методы предсказания при оценке того, будут ли достигнуты планируемые величины отказов. При определении того, будут ли достаточны меры предосторожности для достижения планируемых величин отказов по отношению к полноте безопасности, связанной с систематическими отказами, должны быть использованы качественные методы и обоснования». УПБА основан не на таком вероятностном требовании, касающемся возникновения опасности. Однако существуют вероятностные цели, связанные с соблюдением требований УПБА.

4.2 Устройство, система, элемент, компонент, часть аппаратного средства и модуль программного обеспечения

Термины устройство, система, элемент, компонент, часть аппаратного средства и модуль программного обеспечения определены в ИСО 26262-1. На рисунке 3 представлена взаимосвязь устройства, системы, элемента, компонента, части аппаратного средства и модуля программного обеспечения. На рисунке 4 показано, что может входить в устройство. В устройстве можно выделить систему, подсистему или компонент. Полученный в результате выделения элемент, соответствующий критериям системы, может быть системой или подсистемой. Термин подсистема используется, когда важно подчеркнуть, что элемент является частью более крупной системы. Компонент является логически и технически отдельным элементом не уровня системы. Часто термин компонент применяют к элементу, который состоит только из частей и блоков, но также может быть применен к элементу, состоящему из элементов нижнего уровня конкретной области технологии, например электрической/электронной технологии (см. рисунок 4).

Пример — Для микроконтроллера или СИС может быть использована следующая декомпозиция: весь микроконтроллер является компонентом, блок обработки (например, процессор) является его частью, регистры внутри блока обработки (например, блок регистров процессора) являются подчастью. В случае анализа микроконтроллера может быть необходима декомпозиция с более высоким уровнем детализации. Чтобы помочь в этом, можно декомпозировать часть на подчасти, которые могут быть далее декомпозированы на базовые / элементарные подчасти.



Примечания

1 В этой диаграмме, в зависимости от контекста, термин «элемент» может применяться к объектам «система», «компонент», «аппаратная часть» и «модуль программного обеспечения» согласно п. 1.32 ИСО 26262-1.

2 Как определено в ИСО 26262-1, система, по крайней мере, состоит из датчика, контроллера и исполнительного механизма, например, как минимум, из 3 связанных элементов.

3 * означает, что возможны *N* элементов.

Рисунок 3 — Взаимосвязь устройства, системы, элемента, компонента, части аппаратного средства и модуля программного обеспечения

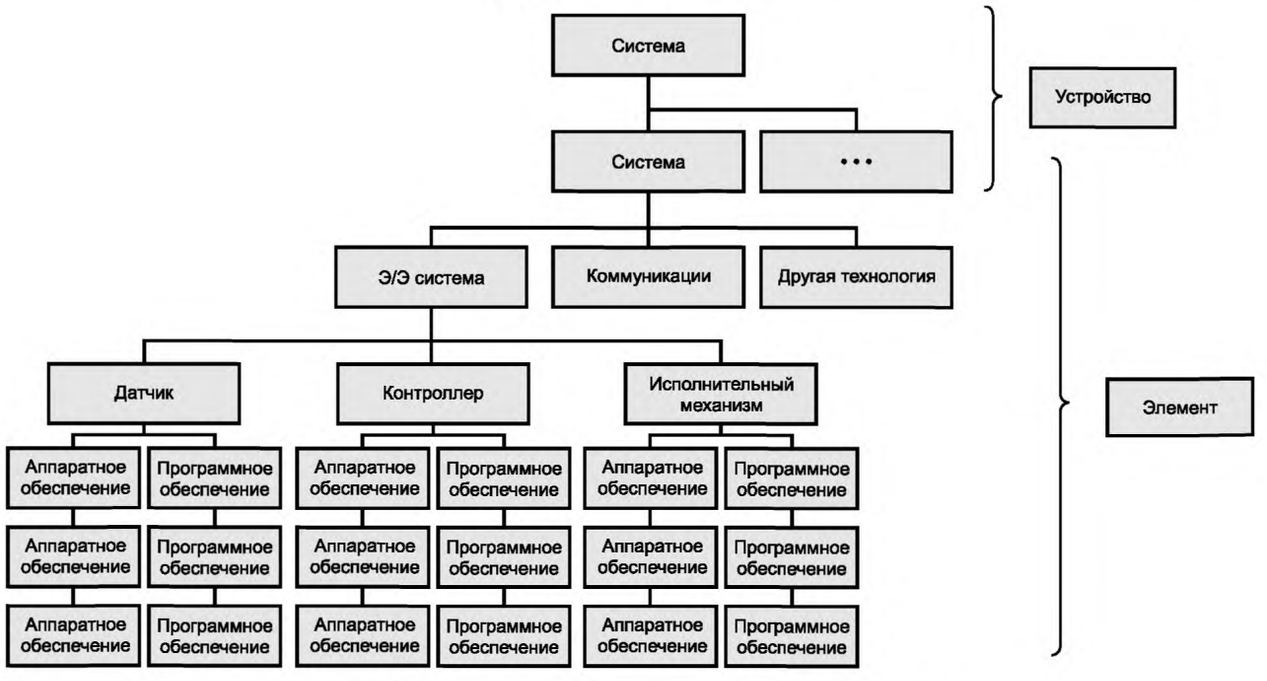


Рисунок 4 — Пример выделения компонентов в устройстве

4.3 Отношения между сбоями, ошибками и отказами

Термины сбой, ошибка и отказ определяются в ИСО 26262-1. На рисунке 5 представлен процесс последовательного развития сбоя в ошибку и ошибки в отказ для трех различных типов причин их появления, связанных с систематическими проблемами программного обеспечения, случайными проблемами аппаратных средств и систематическими проблемами аппаратных средств. Систематические сбои (см. ИСО 26262-1) обусловлены проблемами на стадиях спецификации и проектирования. К систематическим сбоям относят сбои программного обеспечения и некоторую часть сбоев аппаратных средств. Случайные сбои аппаратных средств (см. ИСО 26262-1) обусловлены физическими процессами, такими как износ, физическая деградация или аномальные внешние условия. На уровне компонентов каждый из различных типов сбоев может привести к различным отказам. Однако отказы на уровне компонента являются сбоями на уровне устройства. Отметим, что в этом примере на уровне автомобиля сбои, связанные с различными причинами, могут привести к одинаковому отказу. Подмножество отказов на уровне устройства будут представлять собой опасности (см. ИСО 26262-1), если дополнительные факторы внешней среды позволяют отказу внести свой вклад в аварийный сценарий.

Пример — Если транспортное средство начинает вести себя неожиданно при пересечении перекрестка, то может произойти авария, например оценивается тяжесть, воздействие и управляемость риска опасного события «транспортное средство «скачет» при пересечении перекрестка» («скакать» — делать резкие отрывистые движения).

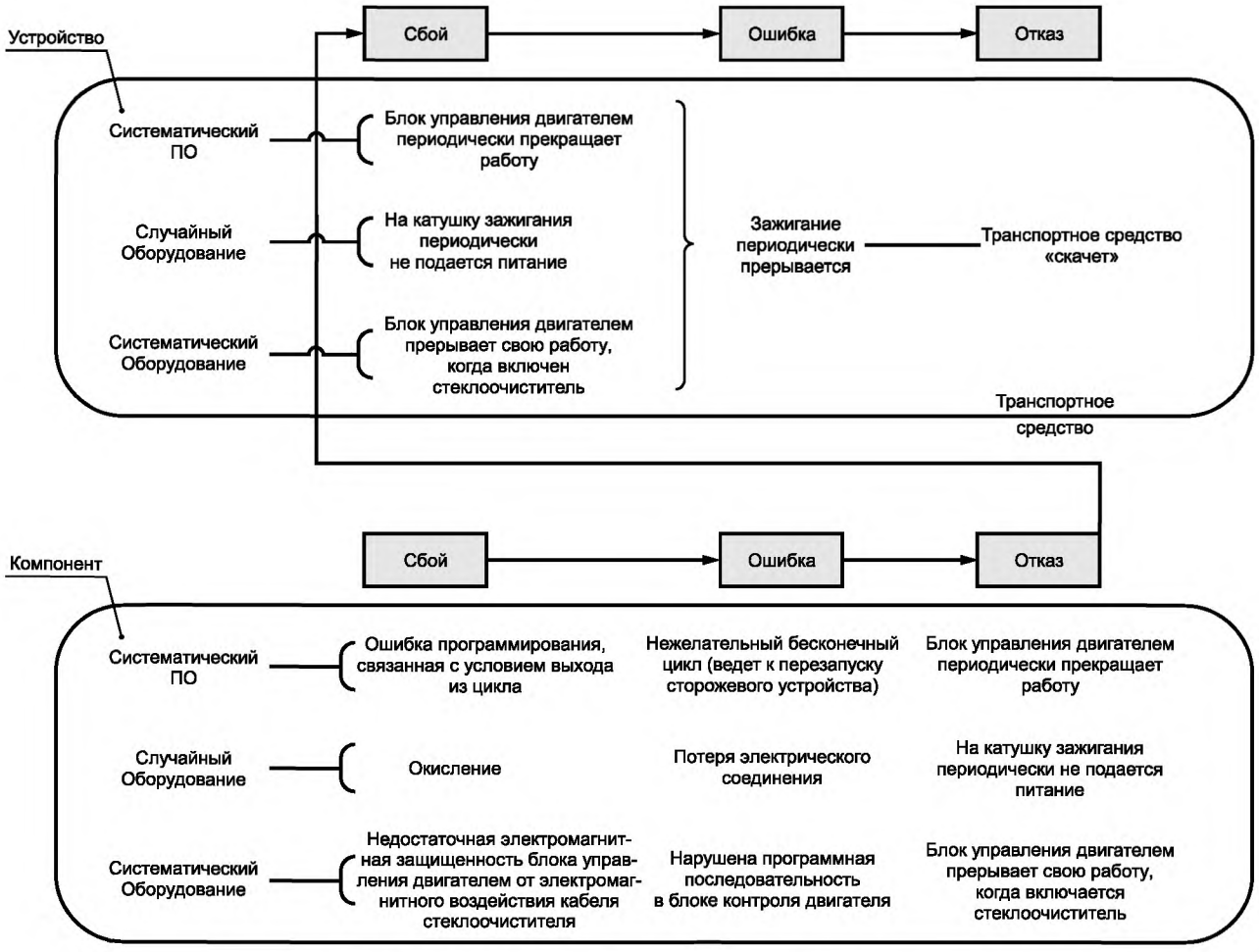


Рисунок 5 — Пример сбоев, приводящих к отказам

5 Отдельные вопросы, связанные с управлением безопасностью

5.1 Результат работы

Данный подраздел описывает термин «результат работы».

Результат работы является результатом выполнения соответствующих требований настоящего стандарта (см. ИСО 26262-1). Таким образом, документально оформленный результат работы может обеспечить доказательство соответствия с этими требованиями безопасности.

Пример — Спецификация требований является результатом работы, который может быть документально оформлен с помощью базы данных требований или в виде текстового файла. Исполняемая модель является результатом работы, которая может быть представлена файлами на языке моделирования, которые могут быть выполнены, например, программными инструментальными средствами для решения задач моделирования.

Документация на результат работы [см. раздел 10 («Документирование») ИСО 26262-8] является записью выполненных действий по обеспечению безопасности, требований к системе безопасности или связанной информации. Такая документация не ограничивается какой-либо формой или средой.

Пример — Документация на результат работы может быть представлена в виде электронных или бумажных файлов, отдельным документом или набором документов. Она может быть объединена с документацией на другие результаты работы или с документацией, непосредственно не связанной с функциональной безопасностью.

Для того чтобы избежать дублирования информации, могут быть использованы перекрестные ссылки между или внутри документации.

5.2 Меры подтверждения

5.2.1 Общие положения

В настоящем стандарте определенные результаты работы оцениваются во время последующих действий либо частично мерами подтверждения, либо частично действиями по верификации. Данный подраздел описывает различия между мерами верификации и подтверждения.

С одной стороны, действия по верификации выполняются с целью определения полноты и правильности спецификации или реализации требований к системе безопасности. Верификация результатов работы может включать в себя:

- отчеты по верификации спецификации или реализации требований безопасности, полученных из требований безопасности более высокого уровня, в отношении их полноты и правильности, или
- выполнение тестов или проверку результатов тестирования для обеспечения доказательств выполнения установленных требований безопасности устройством или его элементом(ами).

Действия по верификации установлены в ИСО 26262-3, ИСО 26262-4, ИСО 26262-5 и ИСО 26262-6.

Кроме того, общие требования к действиям по верификации в настоящем стандарте установлены в разделе 9 ИСО 26262-8 (Верификация), а в дальнейшем детали, специфичные для верификации требований безопасности, установлены в разделе 6 ИСО 26262-8 (Спецификация и менеджмент требованиями к системе безопасности).

С другой стороны, выполняются меры подтверждения для оценки достижения устройством функциональной безопасности, включая подтверждения:

- надлежащих определения, адаптации и выполнения действий по обеспечению безопасности, выполняемых во время разработки устройства, и реализованных процессов безопасности в соответствии с требованиями настоящего стандарта, а также
- надлежащего содержания результатов работы относительно соответствующих требований настоящего стандарта.

Меры подтверждения установлены в разделе 6 (Управление созданием системы безопасности на стадиях формирования концепции и разработки изделия) ИСО 26262-2.

Пример — Если декомпозиция УПБА применяется на стадии проектирования системы, то:

- верификация полученного проекта системы выполняется в соответствии с технической концепцией системы безопасности (см. 7.4.8 ИСО 26262-4) и

- подтверждение правильности применения декомпозиции УПБА может быть выполнено как часть оценки функциональной безопасности, в соответствии с разделом 5 ИСО 26262-9 (Декомпозиция требований с распределением УПБА), включая подтверждение того, что был выполнен анализ зависимых отказов и он обосновывает выполнение требования достаточной независимости между элементами, которые реализуют соответствующие требования избыточности системы безопасности.

5.2.2 Оценка функциональной безопасности

Если самое большое значение УПБА целей безопасности устройства равно значению C или D, то выполнение оценки функциональной безопасности заключается в оценке достижения устройством функциональной безопасности. В ИСО 26262-2 некоторые аспекты оценки функциональной безопасности рассматриваются отдельно, например аудит функциональной безопасности и отчеты о подтверждении.

Оценка функциональной безопасности включает в себя:

a) рассмотрение вопроса о целесообразности и эффективности реализуемых мер обеспечения безопасности, которые могут быть оценены в процессе разработки устройства;

b) оценку результатов работы, требуемых планом обеспечения безопасности. Рассмотрению отдельных результатов работы придается особое значение. Ими являются отчеты о подтверждении и планы подтверждения соблюдения такими результатами работы соответствующих требований настоящего стандарта; а также

c) один или более аудитов функциональной безопасности для оценки осуществления процессов, необходимых для функциональной безопасности.

Оценка функциональной безопасности может быть выполнена повторно или обновлена.

Примеры

1 Оценка функциональной безопасности обновляется из-за изменения устройства или элемента (элементов) этого устройства, которое определяется технологией управления изменениями, так как оно оказывает влияние на функциональную безопасность устройства [см. раздел 8 ИСО 26262-8 (Управление изменениями)].

2 Повторная оценка функциональной безопасности может быть вызвана информацией об оценке функциональной безопасности, которая включает рекомендации по условному принятию или отклонению функциональной безопасности устройства. В этом случае повторная оценка включает в себя рекомендации, полученные из предыдущей(их) оценки(ок) функциональной безопасности, включая оценку проведенных корректирующих действий, если они применимы.

Если самое большое значение УПБА целей безопасности устройства равно значению B, то оценка функциональной безопасности может не выполняться или может быть выполнена менее строго. Однако, даже если оценка функциональной безопасности не выполняется, то должны быть выполнены другие меры подтверждения, например отчеты о подтверждении оценки опасности и анализа рисков, о плане обеспечения безопасности, о плане интеграции и тестирования устройства, о плане подтверждения соответствия, о подходящем анализе безопасности, о подтверждении проверкой в эксплуатации (если применимо) и о полноте обоснования безопасности (см. таблицу 1 ИСО 26262-2).

Если самое большое значение УПБА целей безопасности устройства равно значению A, то в настоящем стандарте нет никакого требования или рекомендации о проведении или непроведении оценки функциональной безопасности. Однако отчеты о подтверждении анализа опасностей и оценки рисков и о подходящем анализе безопасности по-прежнему выполняются.

В случае распределенной разработки, область применения оценки функциональной безопасности включает в себя полученные результаты работы, а также выполненные процессы и меры обеспечения безопасности заводом-изготовителем транспортного средства и поставщиками в цепочке поставок устройства [см. ИСО 26262-2 и раздел 5 (Взаимодействие в совместных разработках) ИСО 26262-8].

Цель оценки функциональной безопасности заключается в оценке достижения устройством функциональной безопасности, которая возможна только на уровне устройства. Таким образом, оценка функциональной безопасности на территории поставщика (который разрабатывает элементы устройства) выполняется только в ограниченном объеме, результаты которой, по существу, являются исходной информацией для последующих действий по оценке функциональной безопасности (на стороне заказчика). Как конечный потребитель разработанного устройства, изготовитель транспортного средства назначает лицо (несколько лиц) для выполнения оценки функциональной безопасности в полном объеме, чтобы судить о достижении устройством функциональной безопасности. Это обоснование включает в себя рекомендации по принятию, условному принятию или отклонению результатов оценки функциональной безопасности устройства.

Примечание — В случае если поставщик первого Уровня несет ответственность за разработку устройства, включая интеграцию транспортного средства, то такой поставщик берет на себя вышеупомянутую роль изготовителя транспортного средства.

На практике оценка функциональной безопасности при распределенной разработке может быть разделена на выполнение:

- оценки функциональной безопасности в ограниченном объеме на территории поставщика, затрагивая поставщиков в цепочке поставок. Применяется значение УПБА, являющееся самым высоким унаследованным значением УПБА (от целей безопасности устройства), для всех элементов устройства, которые разрабатываются поставщиком (см. также 5.4.5 ИСО 26262-8); и
- окончательной оценки функциональной безопасности, включающей в себя обоснование достижения функциональной безопасности интегрированным устройством, например выполняемой изготовителем транспортного средства. Применяемое значение УПБА является наибольшим значением УПБА целей безопасности устройства (см. также ИСО 26262-2).

Пример — Производитель автомобиля разрабатывает устройство, у которого цель безопасности 1 (ЦБ 1) имеет значение УПБА, равное D, а цель безопасности 2 (ЦБ 2) имеет значение УПБА, равное А, и планирует выполнить оценку функциональной безопасности этого устройства. Вполне возможно, что, например, поставщик второго или третьего Уровня разрабатывает элементы для этого устройства только со значениями УПБА, равными А, то есть только элементы, которые наследуют значение УПБА ЦБ 2, равное А [если, однако, это применимо, см. раздел 6 ИСО 26262-9 (Критерии совместимости элементов)]. В настоящем стандарте не существует требования или рекомендации (ни за, ни против), о выполнении оценки функциональной безопасности на территории такого поставщика для такого разрабатываемого устройства.

Область применения, процедура (например, результаты работы должны быть предоставлены поставщиком, результаты работы должны быть рассмотрены заказчиком) и выполнение оценки функциональной безопасности, касающиеся взаимодействия между заказчиком и поставщиком указываются в соответствующем соглашении об интерфейсе разработки [см. раздел 5 ИСО 26262-8 (Взаимодействие в совместных разработках)].

Пример — Соглашение об интерфейсе разработки между изготовителем транспортного средства (заказчик) и поставщиком первого Уровня. Соглашение об интерфейсе разработки между поставщиком первого Уровня (заказчик) и поставщиком второго Уровня.

Один из возможных способов выполнения оценки функциональной безопасности в случае распределенной разработки заключается в том, что изготовитель транспортного средства и каждый из поставщиков в цепочке поставок решает те вопросы по оценке [см. перечисления a), b) и c) выше], за которые соответствующая сторона несет ответственность, а именно:

- поставщик рассматривает меры обеспечения безопасности, реализованные при разработке элементов, включая их целесообразность и эффективность, чтобы обеспечить соответствие с целями безопасности или требованиями безопасности (предусмотренными заказчиком или разработанными поставщиком), и оценивает свои реализуемые процессы и полученные результаты работы. Поставщик также оценивает возможное влияние разработанных элементов на функциональную безопасность устройства, например выявляет, могут ли реализованные меры по обеспечению безопасности привести к новым опасностям;
- изготовитель транспортного средства оценивает функциональную безопасность интегрированного устройства. Часть оценки может быть основана на результатах работы или информации, предоставленной одним или более поставщиками, включая сообщения об оценках функциональной безопасности, выполненных на территории поставщика.

Примечание — Заказчик может оценить меры обеспечения безопасности, осуществляемые поставщиком, и результаты работы, предоставляемые поставщиком. Заказчик может также оценить процессы, осуществляемые поставщиком на территории поставщика (см. 5.4.4.8 ИСО 26262-8).

5.3 Обоснования безопасности

5.3.1 Объяснение обоснований безопасности

Целью обоснования безопасности является обеспечение четкого, всеобъемлющего и аргументированного объяснения, поддержанного доказательством, что при работе в целевом контексте в устройстве отсутствуют необоснованные риски.

Приведенные ниже руководящие указания даны для области применения настоящего стандарта.

Существуют три основных элемента обоснования безопасности, а именно:

- требования;
- доказательство и
- материалы, подтверждающие безопасность, например результаты работы в соответствии с требованиями настоящего стандарта.

Соотношение между этими тремя элементами в контексте настоящего стандарта представлено на рисунке 6.

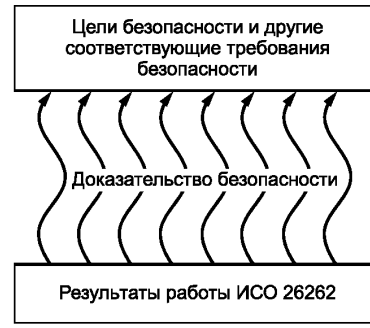


Рисунок 6 — Ключевые элементы обоснования безопасности [2]

Доказательство безопасности реализует отношение между материалами, подтверждающими безопасность, и целями. Ролью доказательства безопасности часто пренебрегают. Можно представить многостраничный документ с доказательствами без четкого объяснения, как эти доказательства связаны с целями безопасности. Доказательство и материалы, подтверждающие безопасность, являются важными элементами обоснования безопасности и рассматриваются всегда вместе. Доказательство без материалов, подтверждающих безопасность, является необоснованным и потому неубедительным. Материалы, подтверждающие безопасность, без доказательства являются необъяснимыми, в результате отсутствует ясность в том, как были достигнуты цели безопасности. Обоснования безопасности передаются в виде разработанных и представленных отчетов с обоснованием безопасности. Роль отчета с обоснованием безопасности заключается в объединении доказательства безопасности с соответствующими отчетами о получении материалов, подтверждающих безопасность (например, протоколы испытаний).

Доказательства безопасности, используемые в настоящее время в других отраслях, часто включаются в отчеты с обоснованием безопасности в виде обычного текста. Обычным текстом можно описать, как цель безопасности была интерпретирована, распределена и декомпозирована, в конечном счете, доходя до ссылок на доказательства, которые демонстрируют выполнение заявленных характеристик безопасности для нижнего уровня. Кроме того, становится все более популярным использование графических представлений доказательства безопасности (например, требования — доказательства безопасности — материалы, подтверждающие безопасность, в средстве представления структурирования цели [2]), чтобы явно и наглядно представить отдельные элементы доказательства безопасности (требования, заявленные характеристики, материалы, подтверждающие безопасность, и контекст) и отношения, которые существуют между этими элементами (например, как отдельные требования поддерживаются конкретными заявленными характеристиками безопасности, каким образом заявленные характеристики безопасности поддерживаются материалами, подтверждающими безопасность, и предполагаемым контекстом, который определен для доказательства безопасности).

Доказательство безопасности, которое рассматривает безопасность, непосредственно используя характеристики реализуемого устройства (например, поведение синхронизации сторожевого таймера), часто называют доказательством безопасности изделия. Доказательство безопасности, которое рассматривает безопасность, используя характеристики процесса разработки и оценки (например, представления, принятые при проектировании), часто называют доказательством безопасности процесса.

Оба типа доказательства безопасности могут быть использованы для достижения обоснованного доказательства безопасности устройства, где доказательство безопасности процесса может рассматриваться как обеспечение уверенности в материалах, подтверждающих безопасность, используемых при доказательстве безопасности изделия.

5.3.2 Жизненный цикл разработки обоснования безопасности

Разработку обоснования безопасности можно рассматривать как дополнительную деятельность, которая интегрируется с остальными стадиями разработки жизненного цикла системы безопасности.

Примечание — План обеспечения безопасности может включать в себя планирование дополнительных шагов и предварительных версий обоснования безопасности.

Такой подход формирует промежуточные версии обоснования безопасности основных стадий разработки изделия. Например, предварительная версия обоснования безопасности может быть создана после верификации технических требований системы безопасности; промежуточная версия обоснования безопасности может быть создана после верификации проекта системы и окончательная версия может быть создана непосредственно перед оценкой функциональной безопасности.

Обоснование безопасности оформляется в виде отчета о подтверждении, как указано в 6.4.7 ИСО 26262-2 (Меры подтверждения: виды, независимость и полномочия).

Если устройство модифицируется, то оценивается влияние на обоснование безопасности и, при необходимости, обоснование безопасности обновляется с учетом модификаций.

6 Стадия формирования концепции и разработка системы

6.1 Общие положения

В настоящем разделе представлен обзор принципов, лежащих в основе анализа опасностей и классификации рисков, и рассмотрены упрощенные примеры понятий.

6.2 Пример анализа опасностей и оценки рисков

6.2.1 Общие положения

Рассмотрим пример устройства управления блоком накопления энергии, встроенного в транспортное средство. В данном примере предположим, что накапливаемая энергия должна расходоваться только тогда, когда транспортное средство движется со скоростью, равной или превышающей 15 км/ч. Расход накапливаемой энергии при скорости менее 15 км/ч может привести к перегреву и последующему разрушению блока.

6.2.2 Анализ 1

a) Определение опасности:

- отказ, приводящий к нежелательному расходу энергии блоком, может привести к разрушению блока.

b) Опасное событие:

В данном примере предположим, что дорожная ситуация для анализа опасностей и оценки рисков является следующей:

- движение автомобиля в «пробках» со скоростью менее 15 км/ч.

Происходит нежелательное расходование энергии из-за отказа в устройстве. Блок накопления энергии разрушается, нанося серьезный вред водителю и пассажирам транспортного средства.

c) Классификация выявленного опасного события

Разрушение приводит к опасным для жизни травмам с сомнительным выживанием для людей, находящихся в транспортном средстве, поэтому тяжесть оценивается как S3.

Автомобиль движется в «пробках» со скоростью менее 15 км/ч. На основе статистики трафика для целевого рынка данного транспортного средства воздействие такой ситуации может быть оценено как E3 (происходящее в течение 1 % — 10 % среднего времени работы автомобиля).

Способность водителя или пассажиров транспортного средства управлять отказом устройства и разрушением блока рассматривается как неправдоподобное событие: в данном случае управляемость может быть оценена как C3 (трудноконтролируемое или неконтролируемое событие).

Применяя таблицу 4 ИСО 26262-3, получим значение УПБА, равное C.

6.2.3 Анализ 2

a) Определение опасности:

- отказ не приводит к расходу энергии блоком.

b) Опасное событие:

- любая ситуация в процессе управления автомобилем.

Отказ устройства происходит, но он не приводит к расходу какой-либо энергии из блока накопления энергии и поэтому никакой вред не наносится.

c) Классификация выявленного опасного события

Поскольку отказ устройства не наносит вреда, тяжесть классифицируется как S0 и управляемость не определяется. Поэтому цель безопасности не определяется.

6.3 Замечания о классификации управляемости

Как поясняется в разделе 7 ИСО 26262-3 (Анализ опасностей и оценка рисков), управляемость оценивается вероятностью того, что водитель или другой участник движения могут избежать конкретного вреда.

В простейшем случае рассматривается только один результат для данного опасного события, а управляемость представляет собой оценку вероятности того, что этого результата можно избежать. Тем не менее, могут быть и другие случаи. Например, возможные тяжелые последствия (например, класс тяжести последствий S2) можно относительно легко предотвратить (например, в случае

управляемости C1), однако менее тяжелых последствий (например, класс тяжести последствий S1) бывает гораздо труднее избежать (например, в случае управляемости C3). Если предположить, что класс воздействия E4, то следующий набор полученных значений УПБА, показывает, что необязательно самый высокий класс тяжести последствий приводит к самому высокому значению УПБА:

- E4, S2, C1 => значение УПБА, равное A;
- E4, S1, C3 => значение УПБА, равное B.

В данном примере значение УПБА, равное B, представляет собой соответствующую классификацию опасного события.

6.4 Внешние меры

6.4.1 Общие положения

Внешняя мера является отдельной и независимой от устройства мерой, которая снижает или смягчает риски, связанные с отказом данного устройства.

6.4.2 Пример 1 зависимых от транспортного средства внешних мер

Автомобиль A оснащен ручным механизмом привода коробки передач, который можно оставить на любой передаче, в том числе нейтральной, при выключенном зажигании. Транспортное средство B оснащено автоматической коробкой передач, у которой, при выключенном зажигании, включена одна передача и нормально замкнуто сцепление. Оба автомобиля имеют дополнительное устройство, электрический стояночный тормоз (EPB).

Для рассматриваемых транспортных средств анализируется следующий сценарий:

- автомобиль на парковке (зажигание выключено, водитель отсутствует);
- местом парковки является тротуар с наклонным участком, расположенным на территории города с большим населением;
- отказом является внезапная потеря работоспособности EPB.

В этом случае автомобиль A, оставаясь на нейтральной передаче при выключенном зажигании (ситуация, которая соответствует разумно предсказуемому, неправильному использованию), возможно, будет двигаться, если его оставить без присмотра. Оценивая данную ситуацию, можно определить следующие классы: для управляемости — равный C3, тяжести последствий — равный S2 или выше, в зависимости от наличия поблизости лиц, которые могут быть уязвимы, и воздействия — более E0. В зависимости от диапазона реально назначаемого класса воздействия, диапазон значений УПБА классифицируется между QM и C.

Однако автомобиль B, у которого передача всегда включена, двигаться не будет, поэтому опасность не возникает. Зависимые от транспортного средства внешние меры, включенные в проект этого автомобиля, способствовали ликвидации риска для рассматриваемого сценария, но только если можно показать, что автоматическая коробка передач и EPB достаточно независимы.

6.4.3 Пример 2 зависимых от транспортного средства внешних мер

Автомобиль A оснащен системой динамической стабилизации в дополнение к системе повторного запуска двигателя. Автомобиль B оборудован только системой повторного запуска двигателя.

Для рассматриваемых транспортных средств анализируется следующий сценарий:

- автомобиль движется со скоростью выше средней (50 км/ч < υ < 90 км/ч);
- дорога мощеная, сухая и проходит в пригородной зоне;
- транспортное средство приближается к среднему значению кривизны в изгибе дороги;
- скорость транспортного средства и кривизна дороги таковы, что боковая составляющая ускорения выше среднего значения;
- отказ системы повторного запуска двигателя, заключающийся в нежелательном выключении двигателя, приводит к внезапной потере тягового усилия во время выполнения сценария.

В результате внезапной потери тягового усилия у транспортного средства появляется момент рыскания, требующий от водителя восстановить управление автомобилем рулевым колесом. Можно показать, что автомобиль B при выполнении этого маневра будет иметь низкую управляемость, что может дать значения для УПБА, равные C или D. С другой стороны, система динамической стабилизации транспортного средства A ограничивает последствия боковой неустойчивости. В результате управляемость для транспортного средства A будет ниже. Таким образом, зависимые от транспортного средства внешние меры, представленные системой динамической стабилизации, способствуют снижению риска для этого сценария. Однако это справедливо лишь в том случае, если можно показать, что рассматриваемый отказ системы повторного запуска двигателя не может повлиять на систему динамической стабилизации и для этих систем данный отказ не является зависимым.

6.5 Пример объединения целей безопасности

6.5.1 Введение

Цели безопасности — это требования к безопасности верхнего уровня для данного устройства. Из них формируются требования к функциональной безопасности, чтобы избежать необоснованного риска опасного события. Цели безопасности определяются на стадии формирования концепции в соответствии с требованиями 7.4.8 ИСО 26262-3. Если цели безопасности похожи или ссылаются на одну и ту же опасность в различных ситуациях, то они могут быть объединены в одну цель безопасности с самыми высокими значением УПБА из объединяемых целей безопасности. Дальнейшая разработка может упроститься с уменьшением количества целей безопасности, которые в то же время должны охватывать все выявленные опасности.

6.5.2 Общие положения

В следующем примере устройство, цели безопасности и классификации значений УПБА используются только для иллюстрации процесса объединения целей безопасности. Данный пример не отражает применения настоящего стандарта для аналогичных реальных проектов. В частности, он не касается идентификации видов отказов, анализа ситуации и оценки воздействия на уровне автомобиля.

Для простоты, данный пример ограничивается композицией двух целей безопасности, но тот же самый подход может быть распространен и на большее количество исходных целей безопасности.

6.5.3 Определение функции

Рассмотрим транспортное средство, оснащенное системой электрического стояночного тормоза (EPB). Система EPB, включенная по конкретному запросу водителя, формирует тормозной момент на задних колесах автомобиля, чтобы предотвратить непреднамеренные движения автомобиля во время его стоянки (функция парковки).

6.5.4 Цели безопасности, применяемые для одной и той же опасности в различных ситуациях

6.5.4.1 Анализ опасностей и оценка рисков

Для упрощения примера рассмотрим следующий вид отказа функции парковки:

- непреднамеренное приведение в действие стояночного тормоза.

Примечание — В данном контексте термин «непреднамеренное приведение в действие» означает срабатывание функции без запроса водителя.

Данный вид отказа может по-разному воздействовать на транспортное средство в зависимости от конкретной сложившейся ситуации в момент возникновения отказа, что отражено в таблице 1.

6.5.4.2 Разработка целей безопасности

Как показано выше, одинаковые цели безопасности и безопасные состояния применимы к обеим ситуациям. Итак, цель безопасности может быть определена следующим образом:

- цель безопасности: предотвратить включение функции парковки без запроса водителя, когда транспортное средство двигается;
- безопасное состояние: EPB не работает;
- значение УПБА: наибольшее значение УПБА, определенное в таблице 1, задается данной цели безопасности.

Таблица 1 — Цели безопасности, полученные для одной и той же опасности в в различных ситуациях

Вид отказа	Опасность	Конкретная ситуация	Опасное событие	Возможные последствия	УПБА	Цель безопасности	Безопасное состояние
Непреднамеренное приведение в действие стояночного тормоза	Неожиданное замедление	Высокая скорость, ИЛИ поворот, ИЛИ низкое поверхностное трение	Неожиданное замедление на высокой скорости, ИЛИ поворот, ИЛИ низкое поверхностное трение	Потеря устойчивости автомобиля	Более высокое значение УПБА	Предотвратить включение функции парковки без запроса водителя, когда транспортное средство двигается	EPB не работает
Непреднамеренное приведение в действие стояночного тормоза	Неожиданное замедление	Скорость ниже средней И высокое поверхностное трение	Неожиданное замедление на скорости ниже средней И высокое поверхностное трение	Заднее столкновение со следующим автомобилем	Более низкое значение УПБА	Предотвратить включение функции парковки без запроса водителя, когда транспортное средство двигается	EPB не работает

7 Структура требований к процессу обеспечения безопасности. Последовательность выполнения требований к безопасности

Последовательность разработки и выполнения требований к безопасности в соответствии с настоящим стандартом показаны на рисунках 7 и 8 и описаны ниже. На этих рисунках конкретные разделы настоящего стандарта указаны следующим образом: «*m*-*n*», где «*m*» означает номер части настоящего стандарта, а «*n*» указывает номер раздела или подраздела в этой части.

Анализ опасностей и оценка риска выполняется для определения рисков и определения целей безопасности для снижения этих рисков. (См. раздел 7 ИСО 26262-3 Анализ опасностей и оценка рисков.)

Затем формируется концепция функциональной безопасности, которая определяет требования функциональной безопасности, обеспечивающие выполнение целей безопасности. Данные требования определяют механизмы обеспечения безопасности и другие меры обеспечения безопасности, которые будут использоваться в данном устройстве. Кроме того, определяются элементы архитектуры системы, которые обеспечивают выполнение этих требований. (См. раздел 8 ИСО 26262-3, Концепция функциональной безопасности.)

Далее формируется техническая концепция обеспечения безопасности, которая определяет технические требования к системе безопасности и их распределение по элементам системы, реализуемым в проекте системы. Эти технические требования к системе безопасности укажут разбиение этих элементов между аппаратными средствами и программным обеспечением. (См. раздел 6 ИСО 26262-4, Спецификация технических требований к системе безопасности.)

Проект системы будет разработан в соответствии с техническими требованиями системы безопасности. Их реализация может быть определена в спецификации проекта системы. (См. раздел 7 ИСО 26262-4, Проект системы.)

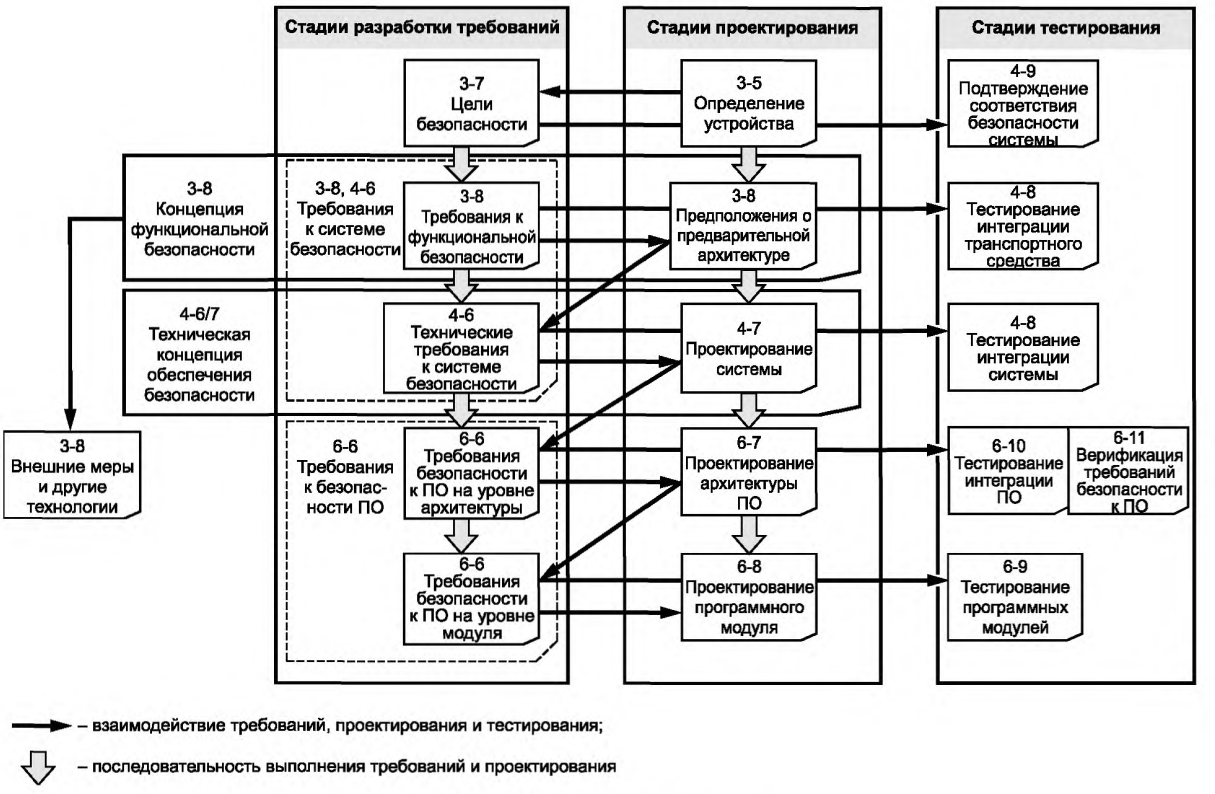
Наконец, чтобы выполнить технические требования к системе безопасности и проекту системы, будут указаны требования к аппаратным средствам и программному обеспечению системы безопасности. (См. раздел 6 ИСО 26262-5, Спецификация требований к безопасности аппаратных средств, и раздел 6 ИСО 26262-6, Спецификация требований к безопасности программного обеспечения).

Рисунок 7 иллюстрирует взаимосвязь между стадиями формирования требований и разработки аппаратных средств, которые определены в настоящем стандарте.



Рисунок 7 — Начинающаяся от формирования концепции последовательность разработки требований безопасности, проектирования и тестирования для аппаратных средств

Рисунок 8 иллюстрирует взаимосвязь между подстадиями формирования требований, разработки и тестирования для программного обеспечения, определяемую настоящим стандартом.



ПО — программное обеспечение

Рисунок 8 — Начинающаяся от формирования концепции последовательность разработки требований безопасности, проектирования и тестирования для программного обеспечения

Проектирование системы

Проектирование системы — это непрерывный процесс уточнения от определения устройства (3—6) до формирования предположений предварительной архитектуры и проекта системы (4—7).

Зависимость между уровнями тестирования

Спецификации тестов и тестовых примеров на каждом уровне в основном зависят от соответствующих требований и проекта. Они не зависят от спецификаций тестов, тестовых примеров и результатов тестов на других уровнях тестирования. Спецификации тестов обычно зависят от среды тестирования.

Зависимость уровней тестирования от уровней требований и проектирования

Спецификации тестов и тестовые примеры формируются из требований и используют информацию о проекте одного и того же уровня проектирования.

Пример — Для выполнения тестирования необходима информация о проекте.

Верификация требований к программному обеспечению системы безопасности

Стадия верификации требований к программному обеспечению системы безопасности (6-11) требует интеграции программного обеспечения и аппаратных средств.

Внешние меры и другие технологии

Подтверждение соответствия внешних меры и других технологий выполняется на уровне транспортного средства.

8 Разработка аппаратных средств

8.1 Классификация случайных сбоев аппаратных средств

8.1.1 Общие положения

В общем случае при рассмотрении комбинаций сбоев ограничиваются комбинациями из двух независимых сбоев аппаратных средств, если анализ, выполненный на основе функциональной или

технической концепции обеспечения безопасности не показал, что *n*-кратный сбой с $n > 2$ являются существенным. Следовательно, для заданной цели безопасности и заданного элемента аппаратных средств, сбой может быть классифицирован в большинстве случаев как:

a) одиночный сбой;

b) остаточный сбой;

c) обнаруживаемый двойной сбой;

d) воспринимаемый двойной сбой;

e) скрытый двойной сбой;

f) безопасный сбой.

Пояснения и примеры различных классов сбоев приведены ниже.

8.1.2 Одиночный сбой

Данный сбой:

- может непосредственно привести к нарушению цели безопасности; и
- является сбоем элемента аппаратного средства, для которого ни один механизм безопасности не предотвращает некоторые из таких сбоев элемента аппаратного средства от нарушения цели безопасности.

Пример — Неконтролируемый резистор, для которого хотя бы один вид отказа (например, обрыв цепи) имеет возможность нарушить цель безопасности.

Примечание — Если часть аппаратного средства имеет, по крайней мере, один механизм безопасности (например, сторожевое устройство микроконтроллера), то ни один сбой этой части не классифицируется как одиночный сбой. Сбои, для которых механизмы безопасности не предотвращают нарушения цели безопасности, классифицируются как остаточные сбои.

8.1.3 Остаточный сбой

Данный сбой:

- может непосредственно привести к нарушению цели безопасности; и
- является сбоем элемента аппаратного средства, для которого, по крайней мере, один механизм безопасности предотвращает некоторые из таких сбоев элемента аппаратного средства от нарушения цели безопасности.

Пример — Если оперативная память (RAM) модуля проверяется только с помощью механизма безопасности, использующего тест шахматного кода, то некоторые виды сбоев типа замыкания не обнаруживаются. Нарушение целей безопасности из-за этих сбоев не предотвращается механизмом безопасности. Такие сбои являются примерами остаточных сбоев.

Примечание — В таком случае значение охвата диагностикой механизма безопасности менее 100%.

8.1.4 Обнаруживаемый двойной сбой

Данный сбой:

- вносит вклад в нарушение цели безопасности;
- может привести к нарушению цели безопасности только в сочетании с другим, отличающимся от него, независимым сбоем аппаратного средства, связанным с этим двойным сбоем; и
- обнаруживается механизмом безопасности, который не позволяет ему быть скрытым.

Примеры

1 Флэш-память защищена контролем по четности. Сбой одного бита, который выявляется и в соответствии с технической концепцией обеспечения безопасности инициируется такая реакция, как отключение устройства и информирование водителя с помощью контрольной лампы.

2 Флэш-память защищена механизмом обнаружения ошибки и исправления кода (EDC). Сбои в логике EDC обнаруживаются тестированием и в соответствии с технической концепцией обеспечения безопасности инициируется реакция такая, как информирование водителя с помощью контрольной лампы.

Если происходит кратковременный сбой и механизм безопасности восстанавливает устройство в состояние без сбоя, то такой сбой можно рассматривать как обнаруживаемый двойной сбой, даже если водитель никогда не будет информирован о его существовании.

Пример — Кратковременное переключение бита, которое корректируется механизмом обнаружения ошибки и исправления кода (EDC) перед передачей данных в центральный процессор и корректируется в дальнейшем, записывая правильное значение. Можно вести журнал, чтобы различать прерывистые сбои от истинных кратковременных сбоев.

8.1.5 Воспринимаемый двойной сбой

Данный сбой:

- вносит вклад в нарушение цели безопасности, но будет приводить к нарушению цели безопасности только в сочетании с другим, отличающимся от него, независимым сбоем аппаратного средства, связанным с этим двойным сбоем и
- воспринимается водителем в течение установленного времени независимо от того был или не был обнаружен данный сбой механизмом безопасности.

Пример — Двойной сбой может быть воспринят водителем, если функциональность значительно и однозначно пострадала от последствия данного сбоя.

Примечание — Если двойной сбой воспринимается водителем, а также выявляется механизмом безопасности, то он может классифицироваться как обнаруживаемый либо воспринимаемый двойной сбой, но не оба одновременно. Это связано с тем, что метрика скрытого сбоя будет рассчитываться неправильно, так как один сбой будет вносить вклад в обнаруживаемые двойные сбои, а также в воспринимаемые двойные сбои, учитывая этот сбой дважды.

8.1.6 Скрытый двойной сбой

Данный сбой:

- вносит вклад в нарушение цели безопасности, но будет приводить к нарушению цели безопасности только в сочетании с другим, отличающимся от него, независимым сбоем и
- не обнаруживается механизмом безопасности и не воспринимается водителем. До появления второго независимого сбоя система все еще действует и водителю об этом сбое не сообщается.

Примеры

1 Флэш-память защищена механизмом EDC. Значение постоянного сбоя в одном разряде корректируется EDC при чтении, но данный сбой не исправляется во флэш-памяти и сигнал о нем водителю не подается. В этом случае данный сбой не может привести к нарушению цели безопасности (так как неисправный бит корректируется), но он не является ни обнаруживаемым (о единичном сбое бита не сообщается), ни воспринимаемым (так как не влияет на функциональность применения). Если в логике EDC происходит дополнительный сбой, то он может привести к потере управления над данным одиночным сбоем бита и возможному нарушению цели безопасности.

2 Флэш-память защищена механизмом EDC. Сбой в логике EDC приводит к неготовности EDC, которая тестом не выявляется.

8.1.7 Безопасный сбой

Безопасными могут быть сбои одной из двух категорий:

a) все n-кратные сбои с $n > 2$, если концепция обеспечения безопасности не показывает, что они вносят соответствующий вклад в нарушение цели безопасности, или

b) сбои, которые не вносят вклад в нарушение цели безопасности.

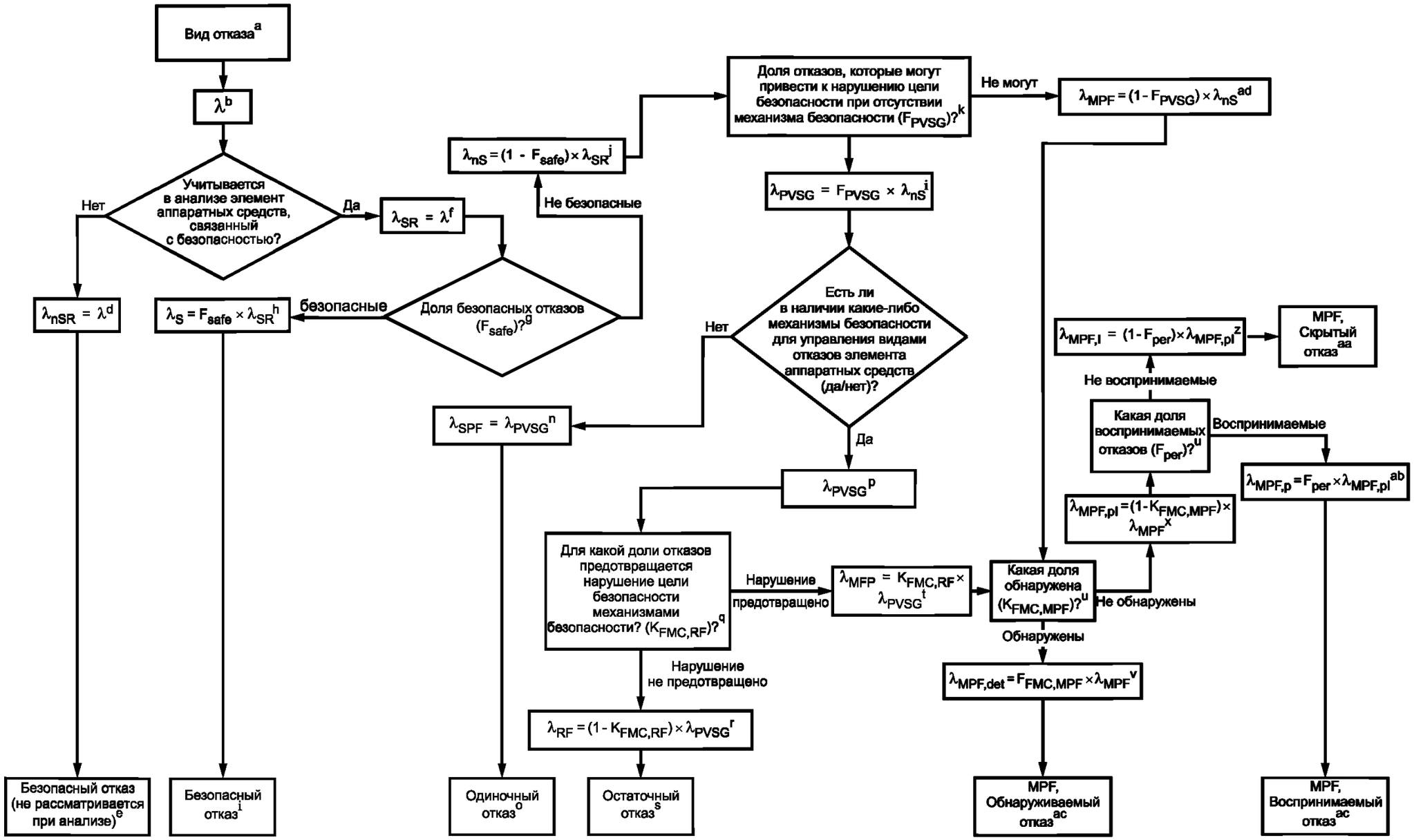
Примеры

1 Флэш-память защищена механизмами EDC и циклического контроля избыточности (CRC). Сбой в одном разряде корректируется EDC, но о нем водителю не сообщается. Сбою не дают возможность нарушить цель безопасности, но EDC об этом не сообщает. Если логика EDC выходит из строя, то сбой обнаруживается механизмом CRC и система отключается. И только если во флэш-памяти присутствует сбой в одном разряде, и логика EDC вышла из строя, и в механизме CRC произошли нарушения при вычислении контрольной суммы CRC, то может произойти нарушение цели безопасности ($n = 3$).

2 Три соединенные последовательно резисторы решают проблему одиночного сбоя типа короткого замыкания, так как короткое замыкание каждого резистора можно считать безопасным сбоем, и для нарушения цели безопасности необходимо, чтобы произошли три независимых коротких замыкания ($n = 3$).

8.1.8 Блок-схема классификации сбоев и вычисление вклада каждого класса сбоев

Виды отказов элемента аппаратного средства могут быть классифицированы, как показано на рисунке B.1 ИСО 26262-5, и используя блок-схему, описанную на рисунке B.2 ИСО 26262-5. На рисунке 9 представлен расчет интенсивностей различных отказов на основе базовой интенсивности отказов и охвата различных видов отказов (остаточных по сравнению со скрытыми).



[a] Анализируемый вид отказа.

[b] λ — интенсивность отказов, связанная с рассматриваемым видом отказов.

[c] Если какой-либо анализируемый вид отказа элемента аппаратных средств связан с безопасностью, то этот элемент аппаратных средств связан с безопасностью.

Рисунок 9 — Классификация категорий отказов и расчет соответствующих интенсивностей отказов

[d] λ_{nSR} — интенсивность отказов, «не связанных с безопасностью». $\lambda_{nSR} = \lambda$, если все виды отказов рассматриваемого элемента аппаратных средств не связаны с безопасностью.

[e] Сбои, не связанные с безопасностью, являются безопасными сбоями и не включены в метрику одиночных сбоев или метрику скрытых сбоев.

[f] λ_{SR} — интенсивность отказов, «связанных с безопасностью». Их включают в метрику одиночных сбоев или метрику скрытых сбоев.

[g] F_{safe} — часть безопасных сбоев этого вида отказов. Безопасные сбои вносят незначительный вклад в нарушение цели безопасности. Для сложных элементов аппаратных средств (например, микроконтроллеров) трудно дать точное значение. В этом случае может быть принята консервативная оценка для $F_{safe} = 0,5$ (то есть 50%).

[h] λ_S — интенсивность отказов для «безопасных» сбоев. $\lambda_S = \lambda_{SR} \times F_{safe}$.

[i] λ_S будет вносить вклад в общую интенсивность безопасных сбоев.

[j] λ_{nS} — интенсивность «не безопасных» отказов. Они включают одиночные сбои, остаточные сбои и множественные сбои (с n = 2). $\lambda_{nS} = (1 - F_{safe}) \times \lambda_{SR}$.

[k] F_{PVSG} — часть λ_{nS}, которые могут непосредственно нарушить цель безопасности, если не учитывать какие-либо возможные механизмы безопасности для предотвращения таких отказов.

[l] λ_{PVSG} — интенсивность отказов от сбоев, которые могут непосредственно нарушить цель безопасности, если не учитывать какие-либо возможные механизмы безопасности для предотвращения таких отказов. $\lambda_{PVSG} = F_{PVSG} \times \lambda_{nS}$.

[m] Определяют, являются ли сбои, приводящие к рассматриваемому виду отказа, одиночными сбоями. Они являются таковыми, если не реализован механизм безопасности, который предотвращает для любого сбоя рассматриваемого элемента аппаратных средств нарушение цели безопасности.

[n] λ_{SPF} — интенсивность отказов от «одиночных сбоев». Если не существует хотя бы одного механизма безопасности для управления отказами рассматриваемого элемента аппаратных средств, то все λ_{PVSG} — одиночные сбои.

[o] λ_{SPF} будет вносить вклад в общую интенсивность одиночных сбоев.

[p] Если у рассматриваемого элемента аппаратных средств есть хотя бы один механизм безопасности, который предотвращает хотя бы один из его отказов от нарушения цели безопасности, то сбои, приводящие к рассматриваемому отказу, не являются одиночными сбоями. В последующей процедуре λ_{PVSG} разделяется на интенсивности остаточных сбоев и обнаруживаемых, воспринимаемых и скрытых множественных сбоев.

[q] Какую часть λ_{PVSG} механизмы безопасности предотвращают от нарушения цели безопасности? Эта часть эквивалентна охвату вида отказа по отношению к остаточным сбоям (см. также приложение Е ИСО 26262-5 «Пример вычисления метрик архитектуры аппаратных средств: метрики одиночного сбоя и метрики скрытого сбоя»). $K_{FMC,RF}$ — аббревиатура охвата вида отказа по отношению к остаточным сбоям.

[r] λ_{RF} — интенсивность отказов от «остаточных сбоев». $\lambda_{RF} = (1 - K_{FMC,RF}) \times \lambda_{PVSG}$.

[s] λ_{RF} — вклад остаточных сбоев в общую интенсивность отказов.

[t] λ_{MPF} — интенсивность отказов от «множественных сбоев». $\lambda_{MPF} = K_{FMC,RF} \times \lambda_{PVSG}$.

[u] Идентификация обнаруживаемых и не обнаруживаемых сбоев. $K_{FMC,MPF}$ — охват вида отказов по отношению к множественным сбоям.

Примечание — Существует два источника множественных сбоев:
- сбои, которые могут привести к нарушению цели безопасности, но для их предотвращения существуют механизмы безопасности;
- сбои, которые сами по себе не могут привести к нарушению цели безопасности, но которые вносят вклад в сценарий множественного отказа.
В зависимости от источника множественного сбоя, охват вида отказа по отношению к множественным сбоям может варьироваться.

[v] $\lambda_{MPF,det}$ — интенсивность отказов от «множественных обнаруживаемых сбоев». $\lambda_{MPF,det} = \lambda_{MPF} \times K_{FMC,MPF}$.

[w] $\lambda_{MPF,det}$ — вклад обнаруживаемых множественных сбоев в общую интенсивность отказов.

[x] $\lambda_{MPF,pl}$ — интенсивность отказов от «множественных воспринимаемых или скрытых сбоев».

[y] F_{per} — доля $\lambda_{MPF,pl}$, которая воспринимается водителем.

[z] $\lambda_{MPF,l}$ — интенсивность отказов от «множественных скрытых сбоев».

[aa] $\lambda_{MPF,l}$ — вклад множественных скрытых сбоев в общую интенсивность отказов.

[ab] $\lambda_{MPF,p}$ — интенсивность отказов от «множественных воспринимаемых сбоев».

[ac] $\lambda_{MPF,p}$ — вклад множественных воспринимаемых сбоев в общую интенсивность отказов.

[ad] λ_{MPF} — интенсивность отказов от «множественных сбоев».

Рисунок 9, Лист 2

8.1.9 Расчет интенсивности отказов от множественных сбоев, связанных с механизмами безопасности на основе программного обеспечения от случайных отказов аппаратных средств

Хотя систематические сбои программного обеспечения и аппаратных средств в настоящем стандарте количественно не определяются, интенсивность отказов может быть рассчитана для случайных отказов аппаратных средств аппаратных ресурсов, поддерживающих выполнение механизмов безопасности на основе программного обеспечения от случайных отказов аппаратных средств.

Если на этих аппаратных ресурсах совместно реализуются функции, которые могут непосредственно нарушить цель безопасности, то выбираются модели сбоев так, чтобы отразить данную ситуацию и рассмотреть возможные зависимые отказы.

8.2 Пример оценки интенсивности остаточных отказов и метрики локального одиночного сбоя

8.2.1 Общие положения

Данный пример демонстрирует способ оценки интенсивности остаточных отказов $\lambda_{RF,Sensor}$, интенсивности одиночных отказов λ_{SPF} и локализованной версии метрики M_{SPFM} одиночных сбоев датчика. В данном примере значение датчика сравнивается со значением другого датчика, которые оба измеряют ту же физическую величину и имеют известные допуски. Значения датчика A_Master используются функцией применения. Значения другого датчика, A_Checker, используются исключительно для подтверждения значений датчика A_Master.

Такой контроль выполняется в соответствии с требованиями приложения D ИСО 26262-5, либо как «проверка обоснованности датчика», либо как «сравнение / голосование на входе».

В данном примере классифицируются и оцениваются только сбои датчика A_Master. Отказы датчика A_Checker не рассматриваются.

Так как датчик A_Master имеет определенный механизм безопасности, то все остальные сбои, которые могут нарушить цель безопасности и которые не контролируются (т. е. нарушение цели безопасности не предотвращается), классифицируются как остаточные сбои. Интенсивность одиночных отказов λ_{SPF} (по определению) равна нулю.

8.2.2 Технические требования обеспечения безопасности для датчика A_Master

Граница безопасной эксплуатации датчика A_Master показана на рисунке 10 и считается заданной в данном примере (ее вывод из цели безопасности здесь не обсуждается). Она может быть выражена с помощью следующих терминов:

$$\mu_{SafRel,A,min} = \text{Максимум } (C_{PVSG};\ v \times (1 + a)),$$

где C_{PVSG} — постоянная величина;

$\mu_{SafRel,A,min}$ — связанная с безопасностью нижняя граница датчика A_Master;

v — измеряемая физическая величина;

a — постоянная величина.

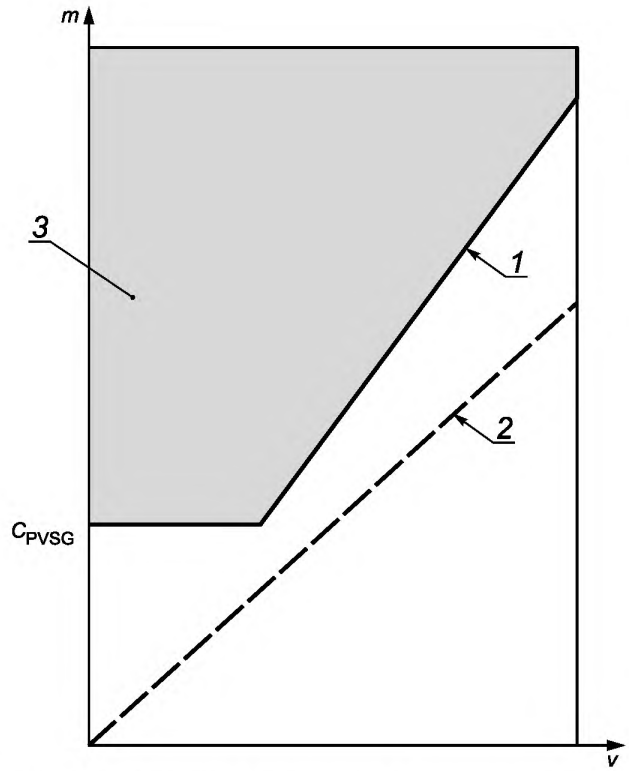
Связанный с безопасностью отказ датчика происходит, когда

$$m_{A,Master} \geq \mu_{SafRel,A,min},$$

где $m_{A,Master}$ — значение, получаемое от датчика A_Master.

Требование безопасности заключается в обнаружении и управлении связанным с безопасностью отказом датчика A_Master в течение времени сбоеустойчивости T_{SenA}.

На рисунке 10 по оси X откладывается измеряемое значение реальной физической величины v, а по оси Y значение $m_{A,Master}$, полученное от датчика A_Master. Пунктирная линия показывает возвращаемое значение идеального датчика (т. е. датчик с нулевым допуском) в качестве эталона. Сплошная линия показывает $\mu_{SafRel,A,min}$. Если значение $m_{A,Master}$, получаемое от датчика A_Master, находится на или выше сплошной линии, то может произойти нарушение цели безопасности.



1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master;
2 — возвращаемое значение идеального датчика с нулевым допуском (как эталон);
3 — сбои с возможным нарушением цели безопасности

Рисунок 10 — Граница безопасной эксплуатации датчика A_Master

8.2.3 Описание механизма безопасности

Элементами механизмов безопасности являются датчик A_Checker и аппаратный монитор, который состоит из микроконтроллера с встроенным программным обеспечением. Программа сравнивает значения двух датчиков друг с другом, с периодом времени, значение которого меньше времени сбоеустойчивости T_{SenA}. Оценка проводится следующим образом:

$$\Delta_A = m_{A,Master} — m_{A,Shecker}$$

Если $\Delta_A \geq \Delta_{Max}$, то значение состояния отказа ИСТИНА.

Если значение состояния отказа ИСТИНА, то выполняется переход в безопасное состояние.

В этом алгоритме:

$m_{A,Master}$ — значение, полученное от датчика A_Master;

$m_{A,Shecker}$ — значение, полученное от датчика A_Checker;

Δ_{Max} — предопределенный константный максимальной порог, использующийся в качестве критерия прохождения / непрохождения.

Предполагается, что датчики имеют следующие известные допуски:

$$m_{A,Master} = v \pm C_{A,Master};$$
$$m_{A,Shecker} = v \pm C_{A,Shecker},$$

где $m_{A,Master}$ — значение, полученное от датчика A_Master;

$m_{A,Shecker}$ — значение, полученное от датчика A_Checker;

$C_{A,Master}$ — постоянная величина, представляющая допуск датчика A_Master;

$C_{A,Shecker}$ — постоянная величина, представляющая допуск датчика A_Checker;

v — измеряемая физическая величина.

Значение Δ_{Max} выбрано так, что отказ датчика A_Master, который может нарушить цель безопасности, обнаруживается. Для предотвращения выявления ложных отказов, Δ_{Max} выбран с учетом допусков каждого датчика и других допусков, объединенных в $C_{A,other}$, например, связанных с влиянием выполнения измерения в разное время:

$\Delta_{Max} \geq C_{A,Master} + C_{A,Shecker} + C_{A,other}$.

При таком подходе, наихудшим случаем необнаружения отказа является:

$$\mu_{A,Master,wc} = m_{A,Shecker} + \Delta_{Max} = v + C_{A,Shecker} + \Delta_{Max},$$

где $\mu_{A,Master,wc}$ — наихудший случай порога обнаружения, т.е. максимальное значение $m_{A,Master}$ датчика A_Master, которое не обнаруживается как отказ;

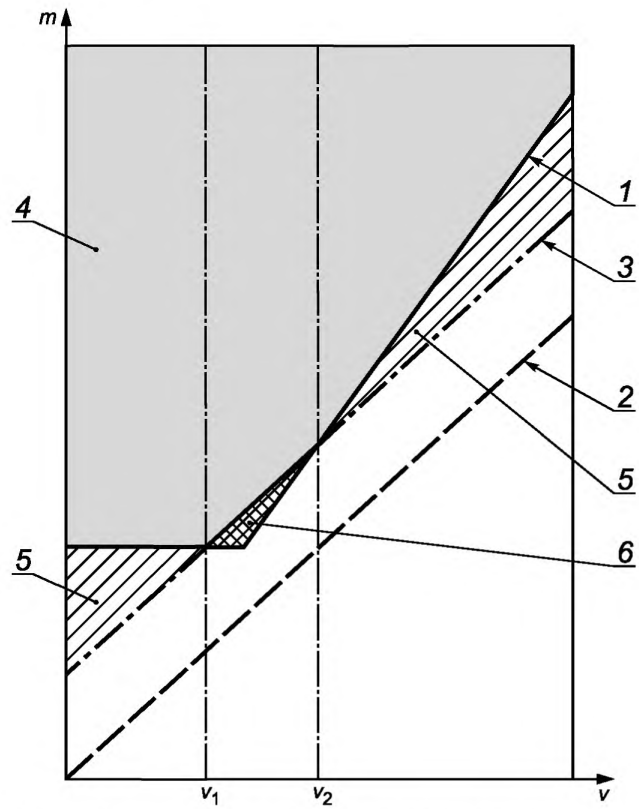
$m_{A,Shecker}$ — значение, полученное от датчика A_Checker;

Δ_{Max} — предопределенный константный максимальной порог, использующийся в качестве критерия прохождения / непрохождения;

v — измеряемая физическая величина.

Каждое значение $m_{A,Master}$ более $\mu_{A,Master,wc}$ классифицируется как отказ датчика.

В зависимости от значений допуска, возможны различные сценарии выявления отказов. Два примера представлены на рисунках 11 и 12.



1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — двойные обнаруживаемые сбои; *5* — обнаруживаемые сбои, не нарушающие цели безопасности; *6* — остаточные сбои

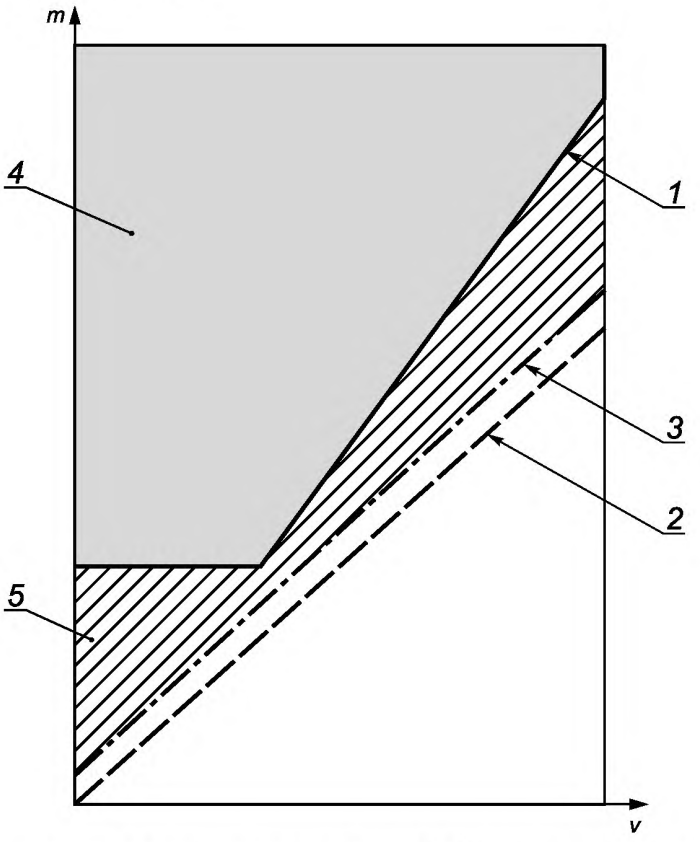
Рисунок 11 — Пример 1 наихудшего случая порога обнаружения (слишком высокий)

На рисунке 11 указателями показаны три области.

Область *5* — «Обнаруживаемые сбои, не нарушающие цели безопасности». Это сбои, обнаруживаемые механизмом безопасности, так как они находятся выше наихудшего случая порога обнаружения $\mu_{A,Master,wc}$, но само по себе не приводят к нарушению цели безопасности, потому что они ниже связанной с безопасностью нижней границы $\mu_{SafRel,A,min}$.

Область *4* — «Двойные обнаруживаемые сбои». Эти сбои могут привести к нарушению цели безопасности, но они обнаруживаются и смягчаются механизмом безопасности. Они находятся выше наихудшего случая порога обнаружения $\mu_{A,Master,wc}$ и связанной с безопасностью нижней границы $\mu_{SafRel,A,min}$. Природа двойственности таких сбоев объясняется тем, что для возможного нарушения цели безопасности необходимы и отказ механизма безопасности и отказ датчика.

Область *6* — «Остаточные сбои». Это сбои не обнаруживаются механизмом безопасности и могут непосредственно привести к нарушению цели безопасности. Область $\mu_{SafRel,A,min} < \mu_{A,Master,wc}$ для $v \in [v_1, v_2]$ лежит ниже наихудшего случая порога обнаружения $\mu_{A,Master,wc}$, но выше связанной с безопасностью нижней границы $\mu_{SafRel,A,min}$.



1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — двойные обнаруживаемые сбои; *5* — обнаруживаемые сбои, не нарушающие цели безопасности

Рисунок 12 — Пример 2 наихудшего случая порога обнаружения ($M_{SPFM,Sensor}$ = 100 %)

В случае, представленном на рисунке 12, худший случай порога обнаружения $\mu_{A,Master,wc}$ всегда меньше связанной с безопасностью нижней границы $\mu_{SafRel,A,min}$. В данном случае интенсивность остаточных отказов равна нулю, и локальная метрика одиночных сбоев $M_{SPFM,Sensor}$ датчика равна 100 %.

8.2.4 Оценка примера 1, описанного на рисунке 11

8.2.4.1 Общие положения

Из рисунка 11 видно, что существуют условия, при которых значения наихудшего случая порога обнаружения $\mu_{A,Master,wc}$ выше значений связанной с безопасностью нижней границы $\mu_{SafRel,A,min}$ датчика A_Master:

для $v \in [v_1, v_2]$: $\mu_{SafRel,A,min} \leq \mu_{A,Master,wc}$.

Для определения интенсивности остаточных отказов $\lambda_{RF,Sensor}$ и $M_{SPFM,Sensor}$ в этих условиях необходим дальнейший анализ, пример которого приведен ниже. В приложении D ИСО 26262-5 установлены следующие виды отказов:

Таблица 2 — Пример видов отказов датчика

Элемент	См. таблицы	Анализируемые виды отказов для 60/90/99 % ОД		
		Низкий (60 %)	Средний (90 %)	Высокий (99 %)
Общие элементы				
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

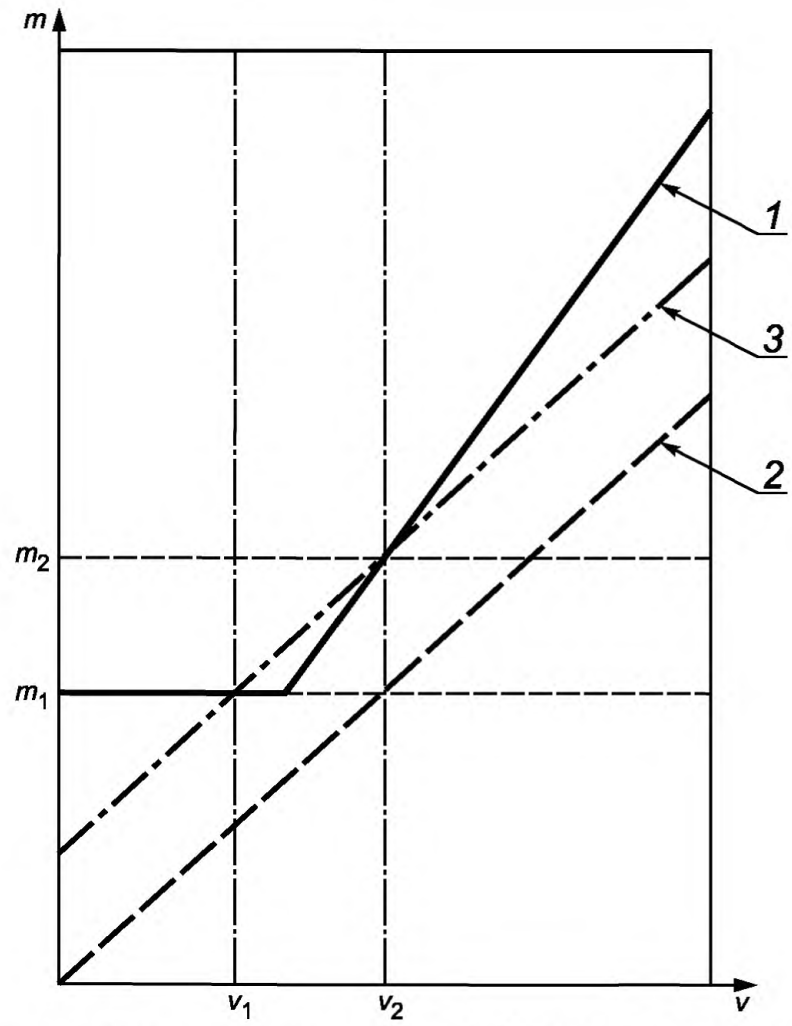
В этом примере оценивается только постоянное значение m константных отказов (в диапазоне). Для полной оценки интенсивности остаточных отказов датчика и $M_{SPFM,Sensor}$ необходимо оценить все другие виды отказов.

Для анализа выделяем три различных сценария константных сбоев для датчика (см. рисунок 13):

1) константное значение датчика $m > m_2$;

2) константное значение датчика $m < m_1$;

3) константное значение датчика $m_1 \le m \le m_2$.



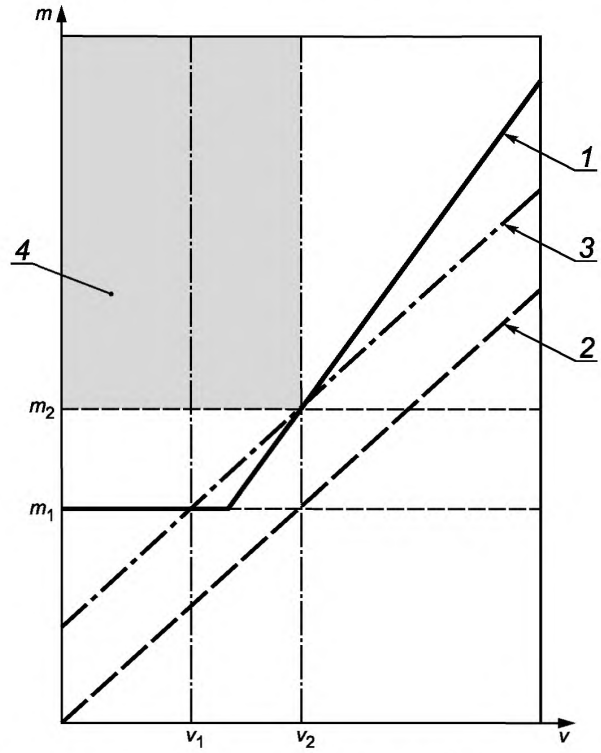
1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$.

Рисунок 13 — Сценарии константных сбоев

Влияние константного сбоя датчика на уровне системы зависит от текущей физической величины v, например, константный сбой со значением m_2 может нарушить цель безопасности для физической величины $v \le v_2$. Для значений $v > v_2$ этот сбой не нарушит цель безопасности. В последующем анализе, вероятность p_{RF} сбоя быть остаточным сбоем оценивается с учетом порогов обнаружения, а также физических величин v и распределения их вероятностей.

8.2.4.2 Сценарий 1. Сбой из-за константного значения датчика при $m > m_2$

Если $v \le v_2$, сбой может нарушить цель безопасности (см. рисунок 14). Отклонение датчика, однако, всегда выше наихудшего случая порога обнаружения $\mu_{A,Master,wc}$, так как связанный с безопасностью отказ датчика обнаруживается и обрабатывается вовремя. Каждый сбой является обнаруживаемым двойным сбоем. Вероятность p_{RF} остаточного сбоя в случае $v \le v_2$ равна нулю.

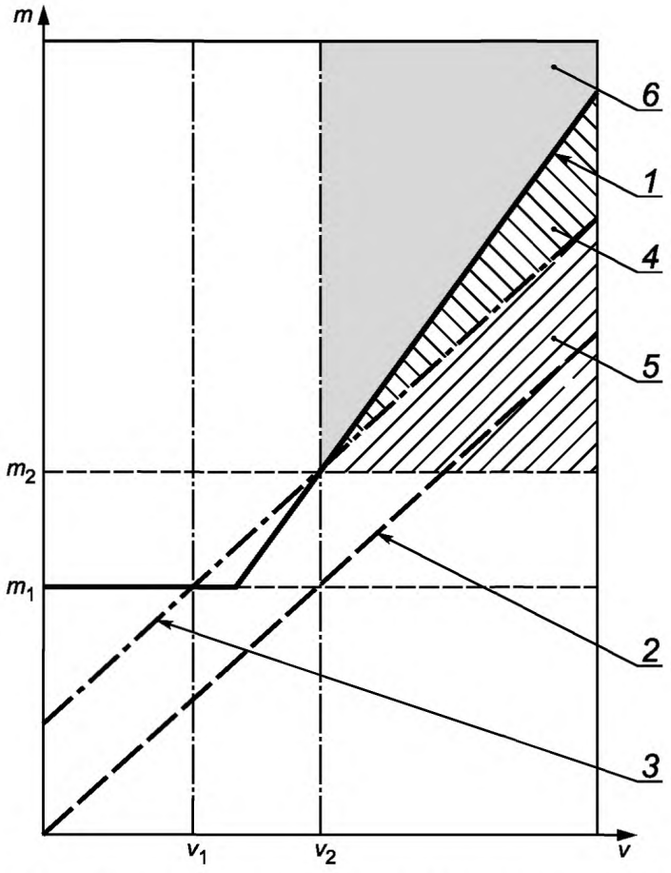


1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — двойные обнаруживаемые сбои

Рисунок 14 — Классификация константных сбоев при $m > m_2$ для $v \le v_2$

Если $v > v_2$ сбой не всегда может нарушить цель безопасности (см. рисунок 15). Если сбой может нарушить цель безопасности (область *6* на рисунке 15), то он будет выше наихудшего случая порога обнаружения и выявлен вовремя. При этом некоторые сбои (области *4* и *5* на рисунке 15) не могут считаться безопасными, даже если $v > v_2$, и потому они не могут привести к нарушению цели безопасности, но у них есть возможность нарушить цель безопасности, если $v \le v_2$. Некоторые из этих сбоев лежат выше наихудшего случая порога обнаружения и обнаруживаются (область *4* рисунка 15). Вероятность p_{RF} остаточного сбоя в случае $v > v_2$ равна нулю.

Константные сбои при $m > m_2$ могут нарушить цель безопасности, если $v \le v_2$, поэтому они не могут считаться безопасными сбоями. Поскольку все сбои обнаруживаются и обрабатываются до того, как они могут привести к нарушению цели безопасности, они являются обнаруживаемыми двойными сбоями, поэтому вероятность $p_{RF_stuck@m>m2}$ остаточного сбоя для константных сбоев при $m > m_2$ равна нулю.

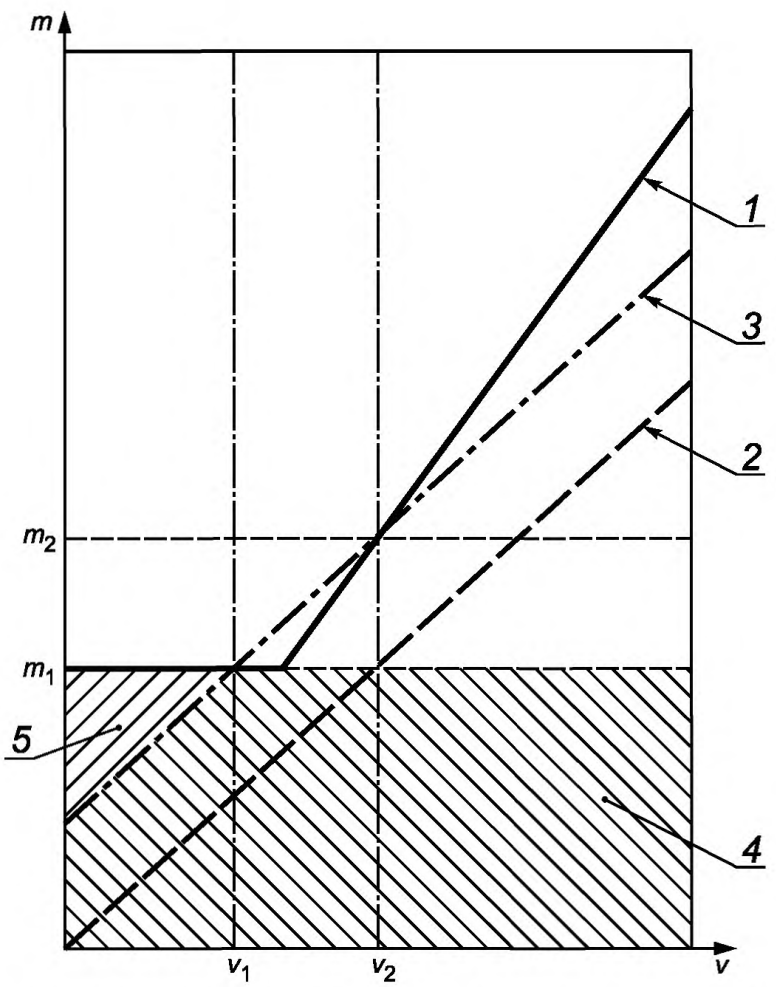


1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — обнаруживаемые сбои, не нарушающие цели безопасности; *5* — необнаруживаемые сбои, не нарушающие цели безопасности; *6* — двойные обнаруживаемые сбои

Рисунок 15 — Классификация константных сбоев при $m > m_2$ для $v > v_2$

8.2.4.3 Сценарий 2. Сбой из-за константного значения датчика при $m < m_1$

Константный сбой при с $m < m_1$ представлен на рисунке 16. Данные сбои являются безопасными сбоями, так как они не могут привести к связанным с безопасностью отказам, поскольку они всегда ниже наихудшего случая порога обнаружения для всего диапазона физических значений *v*. Таким образом, результирующая вероятность $p_{RF_stuck@m<m1}$ остаточного сбоя для всего диапазона физической величины *v* равна нулю.



1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — необнаруживаемые безопасные сбои; *5* — обнаруживаемые безопасные сбои

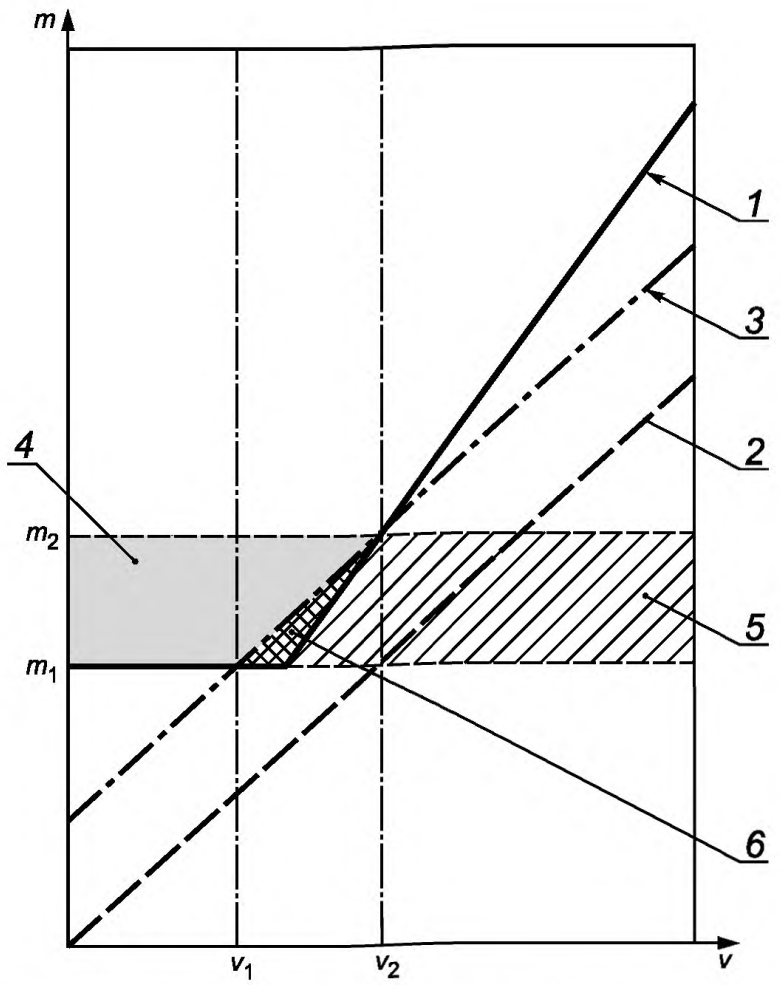
Рисунок 16 — Классификация константных сбоев при $m < m_1$

8.2.4.4 Сценарий 3. Сбой из-за константного значения датчика при $m \in [m_1, m_2]$

Возможное нарушение цели безопасности и обнаружение константного сбоя при $m \in [m_1, m_2]$ зависят от текущего значения физической величины v (см. рисунок 17), то есть вероятность нарушения цели безопасности зависит от текущего значения v в момент сбоя. Вероятность константного остаточного сбой $p_{RF_stuck@m\in[m1,m2]}$ вычисляется для трех различных интервалов значений v в момент возникновения сбоя:

- $v < v_1$;
- $v_1 \le v \le v_2$; и
- $v > v_2$.

Для каждого из этих условий, вероятность остаточного сбоя вычисляется отдельно. Результирующая вероятность остаточного сбоя рассчитывается с использованием значения этих трех вероятностей.



1 — связанная с безопасностью нижняя граница $\mu_{SafRel,A,min}$ датчика A_Master; *2* — возвращаемое значение идеального датчика с нулевым допуском (как эталон); *3* — наихудший случай порога обнаружения $\mu_{A,Master,wc}$; *4* — двойные обнаруживаемые сбои; *5* — сбои, не нарушающие цель безопасности, но остающиеся необнаруживаемыми; *6* — остаточные сбои

Рисунок 17 — Классификация константных сбоев при $m \in [m_1, m_2]$

В зависимости от текущего значения *v*, сбои могут быть обнаруживаемыми двойными сбоями (область *4*), остаточными сбоями (область *6*) или не имеющими возможность нарушить цель безопасности (область *5*).

$$p_{RF_stuck@m\in[m1,m2]} = p_{RF_stuck@m\in[m1,m2],v<v1} \times p_{v<v1} + p_{RF_stuck@m\in[m1,m2],v1\le v\le v2} \times p_{v1\le v\le v2} + p_{RF_stuck@m\in[m1,m2],v>v2} \times p_{v>v2},$$

где $p_{RF_stuck@m\in[m1,m2]}$ — вероятность того, что константное значение *m* сбоя датчика при $m \in [m_1, m_2]$ проявляется в виде остаточного сбоя;

$p_{RF_stuck@m\in[m1,m2],v<v1}$ — вероятность того, что константное значение *m* сбоя датчика при $m \in [m_1, m_2]$ проявляется в виде остаточного сбоя, если $v < v_1$ в момент сбоя;

$p_{v<v1}$ — вероятность того, что $v < v_1$ в момент сбоя;

$p_{RF_stuck@m\in[m1,m2],v1\le v\le v2}$ — вероятность того, что константное значение *m* сбоя датчика при $m \in [m_1, m_2]$ проявляется в виде остаточного сбоя, если $v_1 \le v \le v_2$ в момент сбоя;

$p_{v1\le v\le v2}$ — вероятность того, что $v_1 \le v \le v_2$ в момент сбоя;

$p_{RF_stuck@m\in[m1,m2],v>v2}$ — вероятность того, что константное значение *m* сбоя датчика при $m \in [m_1, m_2]$ проявляется в виде остаточного сбоя, если $v > v_2$ в момент сбоя;

$p_{v>v2}$ — вероятность того, что $v > v_2$ в момент сбоя;

$p_{v<v1} + p_{v1\le v\le v2} + p_{v>v2} = 1$.

Если $v < v_1$, то константные отказы могут нарушить цель безопасность, но обнаруживаются вовремя. Вероятность $p_{RF_stuck@m\in[m1,m2],v<v1}$ остаточного сбоя равна нулю.

Если $v > v_2$, то константные отказы не имеют возможность нарушить цель безопасность, но они не обнаруживаются. Поэтому рано или поздно значение *v* окажется между v_1 и v_2, $p_{RF_stuck@m\in[m1,m2],v>v2} = p_{RF_stuck@m\in[m1,m2],v1\le v\le v2}$.

Если $v_1 \le v \le v_2$, то вероятность $p_{RF_stuck@m\in[m1,m2],v1\le v\le v2}$ остаточного сбоя равна нулю.

Задача точного определения вероятности достаточно долгого пребывания в области остаточных сбоев, что может привести к нарушению цели безопасности, является нетривиальной. Она может зависеть от таких параметров, как:

- динамическое поведение физической величины v и ее соответствующее распределение вероятностей, например, значение температуры является скорее статической величиной тогда, как значение углового положения работающего электродвигателя является скорее динамического величиной;
- распределение вероятностей значений v в $v \in [v_1, v_2]$;
- время реакции программы наблюдения, например, из-за времен фильтрации. В рассматриваемом примере одиночного события с $\Delta_A \ge \Delta_{Max}$ достаточно для обнаружения отказа датчика и переключения в безопасное состояние. Однако обычно счетчик ошибок реализуется так, что необходимо более одного события для оценки отказа датчика и переключения в безопасное состояние. Восстановление счетчика ошибок, например сброс счетчика ошибок, как только обнаружено одно не связанное с безопасностью событие (в данном примере это будет соответствовать $\Delta_A < \Delta_{Max}$), может оказать существенное влияние на способность программы наблюдения обнаруживать отказы, которая резко снижается;
- необходимое число измеряемых отклонений связанного с безопасностью датчика, которое может привести к нарушению цели безопасности. Кроме того, может представлять интерес число обоснованных измерений, которые должны быть выполнены между двумя измеряемыми отклонениями связанного с безопасностью датчика, так чтобы цель безопасность больше не нарушалась.

Если точная подробная информация о каждом влияющем параметре не доступна, то есть все основания использовать экспертную оценку и инженерные практики (например, используя равномерное распределение для неизвестных распределений вероятностей) для получения консервативной оценки.

Оценив вероятности $p_{RF,stuck@m>m2}$, $p_{RF,stuck@m<m1}$ и $p_{RF,stuck@m\in[m1,m2]}$, может быть рассчитана вероятность $p_{RF,stuck@m}$ константного остаточного сбоя датчика:

$p_{RF,stuck@m} = p_{RF,stuck@m<m1} \times p_{m<m1} + p_{RF,stuck@m\in[m1,m2]} \times p_{m1\le m\le m2} + p_{RF,stuck@m>m2} \times p_{m>m2}$,

где: $p_{m<m1}$ — вероятность константного отказа при $m < m_1$;

$p_{m1\le m\le m2}$ — вероятность константного отказа при $m_1 \le m \le m_2$;

$p_{m>m2}$ — вероятность константного отказа при $m > m_2$;

$p_{m<m1} + p_{m1\le m\le m2} + p_{m>m2} = 1$.

8.2.4.5 Окончательная оценка интенсивности остаточных отказов

Если каждый соответствующий вид отказа FM_i оценивать так же, как описано выше, то общая вероятность $P_{RF,Sensor}$ сбоя датчика, проявляющегося как остаточный сбой, может быть вычислено по формуле:

$$p_{RF,Sensor} = \sum_i p_{FM,I} \times p_{RF,FM,I},$$

где: $p_{FM,I}$ — вероятность вида отказа FM_i;

$p_{RF,FM,I}$ — вероятность этого вида отказа FM_i, проявляющегося как остаточный сбой;

$\sum_i p_{FM,I} = 1$.

Зная эту вероятность, можно оценить интенсивность остаточных отказов, как:

$\lambda_{RF,Sensor} = p_{RF,Sensor} \times \lambda_{Sensor}$,

а также значение $M_{SPFM,Sensor}$

$M_{SPFM,Sensor} = 1 - \lambda_{RF,Sensor} / \lambda_{Sensor} = 1 - p_{RF,Sensor}$.

8.2.4.6 Улучшение $SPFM_{Sensor}$

Эффективным способом снижения остаточной интенсивности отказов датчика является снижение величины Δ_{Max}. Снижение Δ_{Max} может быть выполнено без значительного увеличения ложного обнаружения отказов при следующих условиях:

- распределение вероятностей допусков может показать, что оцениваемый сценарий наихудшего случая крайне маловероятен. Таким образом, вероятность ложной тревоги достаточно низка, и поэтому допустима;
- повторное проектирование системы может привести к улучшению значения допуска.

Следует отметить, что в данном примере оцениваются только сбои датчика, но не сбои в оставшейся части канала с датчиком. Неисправность разделяемых ресурсов аппаратных средств, которая может привести к неисправной работе обоих датчиков или которая могла бы исказить значения обоих датчиков, например, АЦП микроконтроллера, оценивается отдельно. Кроме того, выполняется анализ зависимых отказов, как указано в разделе 7 ИСО 26262-9 (Анализ зависимых отказов).

8.3 Об аппаратных средствах

8.3.1 Применение настоящего стандарта для микроконтроллеров

Микроконтроллеры являются неотъемлемой частью современных Э/Э автомобильных систем. Они могут быть разработаны в качестве общеиспользуемого элемента безопасности (ОЭБ, см. раздел 9).

Сложность их создания преодолевается применением объединенных качественных и количественных методов анализа безопасности частей и подчастей микроконтроллера, выполняемых на соответствующем уровне абстракции, т.е. от блок-схемы до уровня списка соединений и топологии во время стадий формирования концепции и разработки изделия.

В приложении А представлены руководящие указания и не исчерпывающий перечень примеров применения настоящего стандарта для микроконтроллеров.

В приложении А описан метод для расчета интенсивности отказов микроконтроллеров, в том числе, как рассматривать постоянные и кратковременные сбои.

Приложение А включает в себя примеры:

- анализа зависимых отказов;
- предотвращения систематических отказов при проектировании микроконтроллера;
- верификации механизмов безопасности микроконтроллера; а также
- выполнения автономного анализа микроконтроллера на уровне системы.

8.3.2 Методы анализа системы безопасности

В приложении В обсуждаются методы анализа видов сбоев системы, включая индуктивный и дедуктивный анализ, и приведен пример анализа дерева сбоев.

8.3.3 Продолжительность воздействия при расчете вероятностной метрики для случайных отказов аппаратных средств (PMHF)

Как описано в 9.4.2.3 ИСО 26262-5, количественный анализ представляет свидетельства о том, что целевые значения требования 9.4.2.1 ИСО 26262-5 были достигнуты. Как показано в 9.4.2.3 ИСО 26262-5, этот количественный анализ учитывает продолжительность воздействия в случае двойных сбоев.

На основе примечания 2 к 9.4.2.3 ИСО 26262-5 продолжительность воздействия начинается с момента возникновения сбоя и включает в себя:

- интервал обнаружения множественно сбоя, связанный с каждым механизмом безопасности, или срок службы автомобиля, если сбой не отображается водителю (скрытый сбой);
- максимальную продолжительность поездки (в случае, если водителю предлагается остановиться в безопасном режиме); и
- средний интервал времени нахождения автомобиля в автомастерской (в случае, если водитель предупрежден о необходимости ремонта автомобиля).

Следующий пример демонстрирует один из способов учета продолжительности воздействия. В данном примере предполагается, что требуемая функциональность (блока задачи «*m*») контролируется механизмом безопасности «*sm*».

Значение вероятностной метрики M_{PMHF} случайных отказов аппаратных средств, с учетом условной вероятности того, что отказ блока задачи происходит при условии отказа механизма безопасности, может быть рассчитана по формуле:

$$M_{PMHF} = [\lambda_{m,RF} \times T_{Lifetime} + \lambda_{m,DPF} \times T_{Lifetime} \times 0{,}5 \times (\lambda_{sm,DPF,latent} \times T_{Lifetime} + \lambda_{sm,DPF,detected} \times \tau_{SM})] / T_{Lifetime},$$

где M_{PMHF} — значение вероятностной метрики случайных отказов аппаратных средств (PMHF);

$\lambda_{m,RF}$ — интенсивность остаточных отказов требуемой функциональности (блока задачи «*m*»);

$\lambda_{m,DPF}$ — интенсивность двойных отказов блока задачи «*m*»;

$T_{Lifetime}$ — срок жизни транспортного средства;

$\lambda_{sm,DPF,latent}$ — интенсивность скрытых двойных отказов механизма безопасности «*sm*»;

$\lambda_{sm,DPF,detected}$ — интенсивность обнаруживаемых двойных отказов механизма безопасности «*sm*»;

τ_{SM} — интервал выявления множественных сбоев механизма безопасности «*sm*».

Если величина терма $\lambda_{m,RF} \times \lambda_{sm,DPF,detected} \times \tau_{SM}$, представляющего вероятность отказа задачи, в сочетании с отказом соответствующего механизма безопасности в одном τ_{SM}, очень мала [например, если величина τ_{SM} одного порядка с длительностью одной поездки (даже с $\lambda_{m,DPF} = \lambda_{sm,DPF,latent} = 1000$ FIT вклад $\leq 10^{-12}$ 1/ч в данном примере)], то ею можно пренебречь, упростив предыдущую формулу:

$$M_{PMHF} = \lambda_{RF} + 0{,}5 \times \lambda_{m,DPF} \times \lambda_{sm,DPF,latent} \times T_{Lifetime}.$$

Если условная вероятность не применяется, например порядок отказа не имеет значения, то формула упрощается до:

$$M_{PMHF} = \lambda_{RF} + \lambda_{m,DPF} \times \lambda_{sm,DPF,latent} \times T_{Lifetime}.$$

9 Общеиспользуемый элемент безопасности

9.1 Разработка общеиспользуемого элемента безопасности

В автомобильной промышленности разрабатываются общеиспользуемые элементы для различных применений и для различных заказчиков. Эти общие элементы могут разрабатываться независимо различными организациями. В таких случаях формируются предположения о требованиях и проекте, включая требования к системе безопасности, которые определяются для элемента на более высоких уровнях проектирования и внешним по отношению к элементу проектом.

Разработанный таким образом элемент называют общеиспользуемым элементом безопасности (ОЭБ). ОЭБ является связанным с безопасностью элементом, который не разрабатывается для конкретного устройства. Это означает, что он не разрабатывается для конкретного транспортного средства.

ОЭБ может быть системой, множеством систем, подсистемой, компонентом программного обеспечения, компонентом аппаратных средств или частью. Примеры ОЭБ включают: системные контроллеры, электронные блоки управления, микроконтроллеры, программное обеспечение, реализующее коммуникационный протокол, или компонент программного обеспечения AUTOSAR.

ОЭБ не может быть устройством, так как разработка устройства всегда выполняется для конкретного транспортного средства, предназначенного для серийного производства. Если ОЭБ является системой, то эта система не разрабатывается для конкретного транспортного средства и поэтому не является устройством.

ОЭБ отличаются от квалифицированных компонентов, описанных в разделе 12 ИСО 26262-8 (Квалификация компонентов программного обеспечения) и раздела 13 ИСО 26262-8 (Квалификация компонентов аппаратных средств), следующим:

- ОЭБ разрабатывается на основе предположений в соответствии с настоящим стандартом. Он предназначен для использования в ряде различных устройств, если в процессе интеграции ОЭБ может быть установлено подтверждение соответствия сформированных для него предположений;
- квалификация компонентов программного обеспечения и аппаратных средств рассматривает вопрос об использовании уже существующих элементов для устройства, разрабатываемого в соответствии с настоящим стандартом. Эти компоненты не обязательно предназначены для повторного использования либо разработаны в соответствии с настоящим стандартом.

Таблица 3 описывает предполагаемое использование квалификации, ОЭБ и подтверждение проверкой в эксплуатации для различных элементов программного обеспечения.

Классификация компонентов программного обеспечения в таблице 3 выполнена в соответствии с требованиями, описанными в 7.4.6 ИСО-26262-6.

Таблица 3 — Классификация компонентов программного обеспечения

Классификация компонентов программного обеспечения	Часть 6 для устройства	Часть 8, раздел 12. Квалификация компонента программного обеспечения	Часть 6 для ОЭБ	Часть 8, раздел 14. Подтверждение проверкой в эксплуатации
Вновь разработанный	Используется	Не используется	Используется	Не используется
Повторно используемый с изменениями	Используется	Не используется	Используется	Используется[a)]
Повторно используемый без изменений	Не используется	Используется	Используется (если разрабатывается как ОЭБ)	Используется

[a)] См. 14.4.4 ИСО 26262-8.

При разработке ОЭБ применяемые действия по обеспечению безопасности настраиваются, как описано в 6.4.5.6 ИСО 26262-2. Такая настройка разработки ОЭБ не означает, что какая-либо стадия

жизненного цикла системы безопасности может быть опущена. Если некоторые стадии не выполняются при разработке ОЭБ, то они будут выполнены в процессе разработки устройства.

УПБА для ОЭБ означает способность ОЭБ соответствовать предполагаемым требованиям безопасности, определенным для данного значения УПБА. Следовательно, УПБА определяет требования настоящего стандарта, которые применяются для разработки этого ОЭБ.

Таким образом, разработка ОЭБ выполняется на основе предположений, требуемой функциональности и используемого контекста, включающего в себя внешние интерфейсы. Эти предположения устанавливаются таким образом, чтобы охватить наибольшее множество элементов так, чтобы ОЭБ мог в дальнейшем использоваться во многих различных, но похожих устройствах. Если некоторые стадии не выполняются при разработке ОЭБ, то они будут выполнены в процессе разработки устройства.

Подтверждение соответствия этих предположений устанавливается в контексте самого устройства в процессе интеграции ОЭБ.

Можно построить устройство из множества ОЭБ, непосредственно взаимодействующих друг с другом. В этом случае обоснованность выполнения предположений одного ОЭБ устанавливается с учетом его взаимодействий.

Если подтверждение соответствия предположений, лежащих в основе разработки ОЭБ, не может быть установлена во время интеграции ОЭБ в устройство, то должны быть сделаны изменения либо в ОЭБ, либо в устройстве в соответствии с требованиями раздела 8 ИСО 26262-8 (Управление изменениями).

9.2 Сценарии использования

9.2.1 Общие положения

Разработка ОЭБ включает формирование предположений для предварительных условий соответствующей стадии разработки изделия, например, для компонента программного обеспечения, который представляет собой часть проекта архитектуры программного обеспечения, такой стадией является подстадия, описанная в разделе 7 ИСО 26262-6. Нет необходимости формировать предположения для всех предварительных условий, например, для плана обеспечения безопасности.

На рисунке 18 показана связь между предположениями и разработкой ОЭБ. Разработка ОЭБ может начинаться на определенном иерархическом уровне требований и проекта. Каждая часть информации о требованиях или предварительных условиях проекта предварительно определяется со статусом «предполагаемая».

Корректная реализация требований к ОЭБ (полученных из предполагаемых требований более высокого уровня и предположений о внешнем по отношению к ОЭБ проекте) будет верифицирована в процессе разработки ОЭБ.

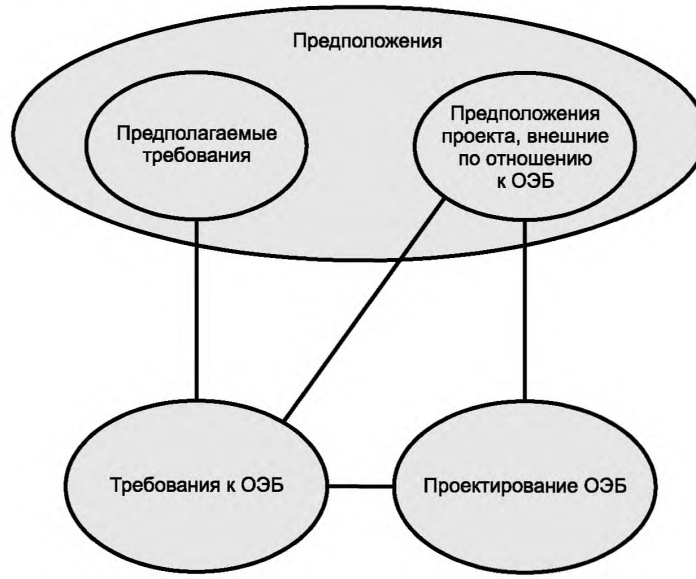


Рисунок 18 — Связь между предположениями и разработкой ОЭБ

Корректная реализация требований к ОЭБ (выведенных из предполагаемых требований более высокого уровня и предположений внешнего по отношению к ОЭБ проекта) будут верифицированы в ходе разработки ОЭБ. Подтверждение соответствия этих требований и предположений в таком случае устанавливается в процессе разработки устройства.

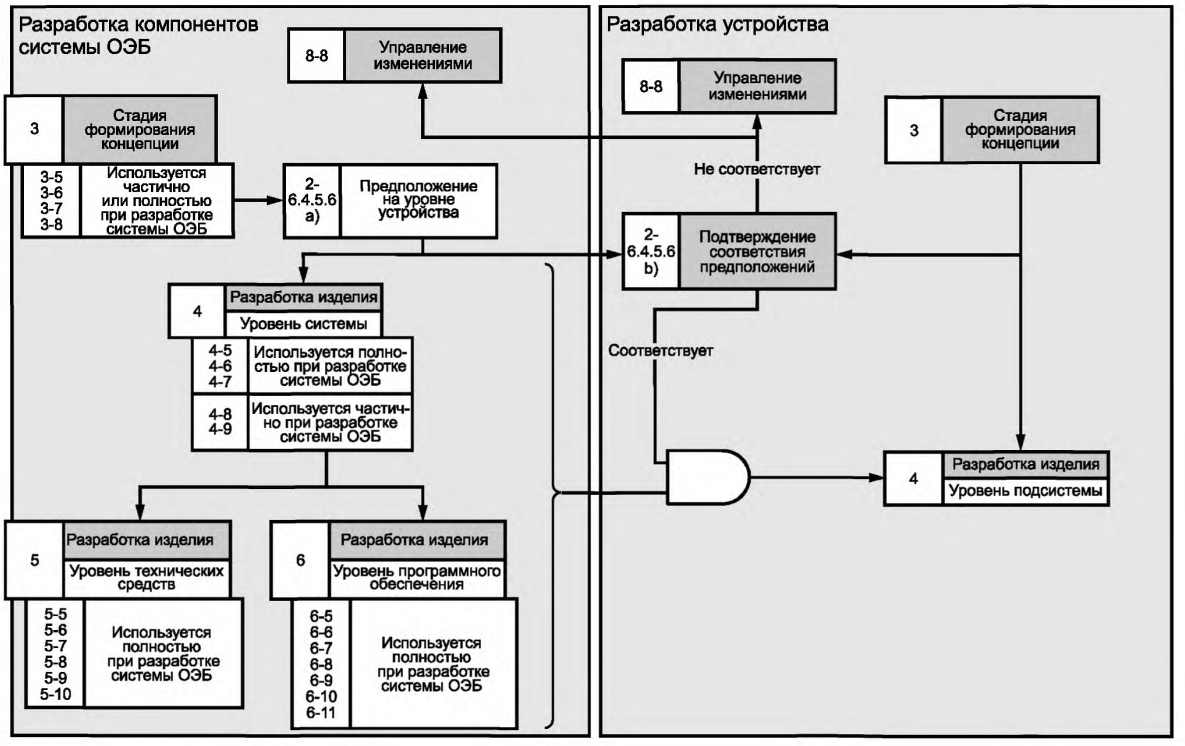
Аналогично, действия по верификации демонстрируют, что разработанный ОЭБ, на любом уровне, согласуется с требованиями контекста, где они используются. Например, если используется компонент программного обеспечения, разработанный как общеиспользуемый, то верификация спецификации программного обеспечения может продемонстрировать, что требования спецификации проектирования архитектуры программного обеспечения выполнены. Такой акт о проверке может быть получен, если разработка ОЭБ завершена, а разработка устройства достигает стадии, на которой формулируются требования к элементу системы безопасности.

Некоторые типичные примеры ОЭБ приведены ниже, а именно: система, компонент аппаратных средств и компонент программного обеспечения.

9.2.2 Разработка системы как общеиспользуемого элемента безопасности

В настоящем пункте показано, как настройка концепции ОЭБ применяется к новой Э/Э системе, которая может быть интегрирована разными производителями транспортных средств.

Пусть для данного примера система реализует следующую функциональность: по соответствующим запросам водитель при определенных состояниях автомобиля может как активизировать некоторую функцию, так и отключать ее. Последовательность операций приведена на рисунке 19.



Примечания

1 В зависимости от конкретной природы ОЭБ может потребоваться некоторая дополнительная настройка требований.

2 В зависимости от конкретной природы ОЭБ некоторые требования частей 3 и 4 не могут быть применены, поэтому они применяются лишь частично.

3 Хотя все разделы настоящего стандарта не представлены на рисунке 19, но это не означает, что они не применяются.

Рисунок 19 — Разработка системы как ОЭБ

Шаг 1a. Определение области применения ОЭБ

На основе предположений разработчик ОЭБ определяет цель, функционал и внешние интерфейсы ОЭБ.

Примерами таких предположений об области применения ОЭБ могут быть:

- система предназначена для автомобилей с полной массой до 1800 кг;
- система предназначена для переднеприводных автомобилей;
- система предназначена для максимального наклона дороги на 32%;
- система имеет интерфейсы с другими внешними системами, чтобы получить необходимую информацию об автомобиле;
- функциональные требования:
- система активизирует функцию по запросу водителя при определенных состояниях автомобиля;
- система отключает функцию по запросу водителя.

Шаг 1b. Предположения о требованиях безопасности к ОЭБ

Для разработки ОЭБ необходимо сделать предположения по определению устройства, целям безопасности устройства и соответствующим требованиям функциональной безопасности, связанным с функциональностью ОЭБ, для того, чтобы определить технические требования безопасности ОЭБ.

Примерами предположений о требованиях к функциональной безопасности, определяемых для ОЭБ могут быть:

- система не активизирует функцию при высокой скорости автомобиля (УПБА *x*);
- система не отключает функцию, если запрос водителя не обнаружен (УПБА *y*).

Для достижения предполагаемых целей безопасности определяются конкретные предположения о контексте.

Примерами предположений о контексте ОЭБ могут быть:

- внешний источник будет предоставлять информацию для требуемого УПБА, позволяющую системе обнаруживать надлежащее состояние транспортного средства (УПБА *x*);
- внешний источник будет предоставлять информацию о запросе водителя для требуемого УПБА (УПБА *y*).

Шаг 2. Разработка ОЭБ

Если технические требования безопасности сформированы из предполагаемых требований к функциональной безопасности устройства, то ОЭБ разрабатывается в соответствии с требованиями настоящего стандарта.

Шаг 3. Результаты работы

В конце разработки ОЭБ должны быть получены результаты, которые показывают, что сформированные технические требования безопасности выполняются. Вся необходимая информация о результатах работы затем поступает к интегратору устройства, в том числе требования к безопасности ОЭБ и предположения, сделанные о контексте.

Шаг 4. Интеграция ОЭБ в устройство

В процессе разработки устройства определяются цели безопасности и требования функциональной безопасности. Требования функциональной безопасности устройства согласовываются с требованиями функциональной безопасности, предполагаемыми для ОЭБ, чтобы установить их обоснованность.

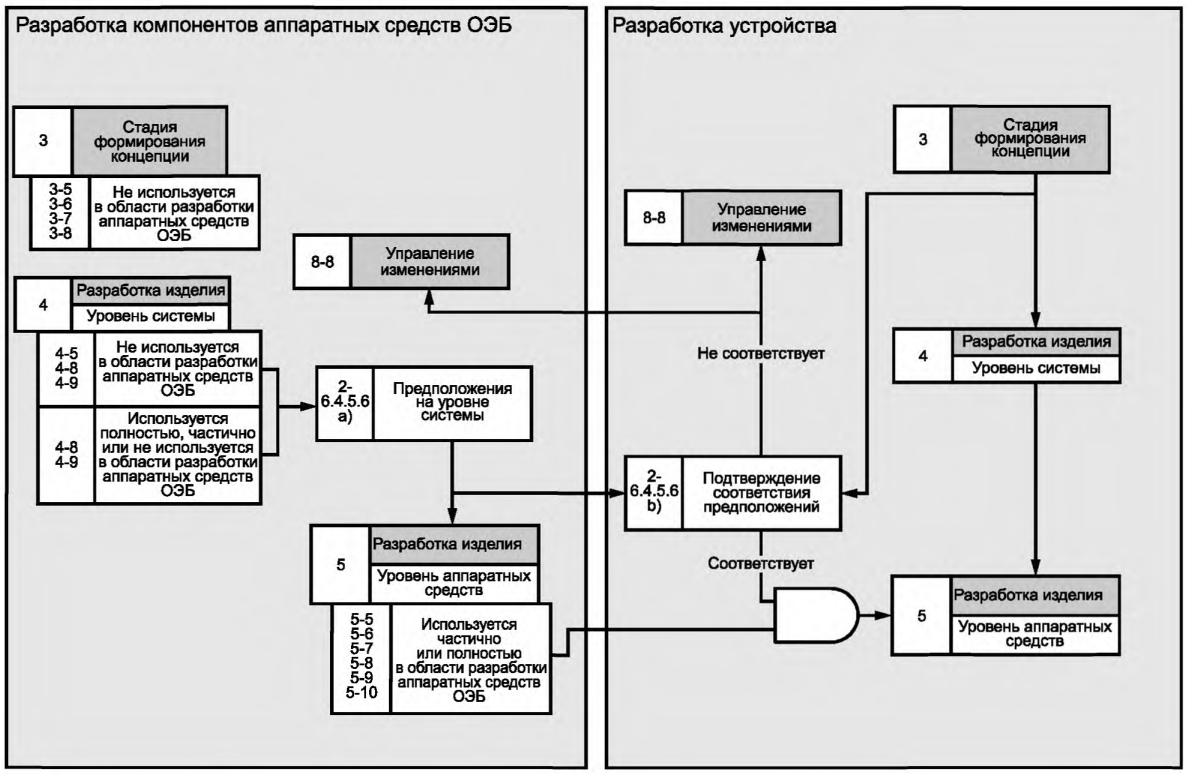
В случае несоответствия предположения для ОЭБ, начиная с анализа влияния, реализуется технология управления изменениями в соответствии с требованиями раздела 8 ИСО 26262-8 (Управление изменениями). Возможные результаты включают в себя:

- несоответствие может считаться приемлемым в связи с достижением цели безопасности, и никакие действия не предпринимаются;
- несоответствие может оказать влияние на достижение цели безопасности и привести к необходимости изменения определения устройства либо концепции функциональной безопасности;
- несоответствие может оказать влияние на цель безопасности и привести к необходимости изменения в общем компоненте безопасности (включая, возможно, изменение самого компонента).

9.2.3 Разработка компонента аппаратных средств как общеиспользуемого элемента безопасности

9.2.3.1 Общие положения

В настоящем пункте пример микроконтроллера, представленного в приложении А, используется в качестве примера компонента аппаратных средств, разрабатываемого как ОЭБ. Последовательность действий процесса разработки приведена на рисунке 20.



Примечания

1 В зависимости от конкретной природы ОЭБ может потребоваться некоторая дополнительная адаптация требований.

2 В зависимости от конкретной природы ОЭБ некоторые требования части 5 не могут быть применены, поэтому они применяются лишь частично.

3 Хотя все разделы настоящего стандарта не представлены на рисунке 20, но это не означает, что они не применяются.

Рисунок 20 — Разработка компонента аппаратных средств как ОЭБ

9.2.3.2 Шаг 1. Предположения на уровне системы

Разработка микроконтроллера (см. рисунок 20), как ОЭБ, начинается (шаг 1) с предположения атрибутов и требований на уровне системы в соответствии с 6.4.5.6 ИСО 26262-2.

Данная стадия может быть разбита на две подстадии (1a и 1b) на основе анализа некоторых справочных приложений. Эти требования являются предполагаемыми для предварительных условий при разработке изделия аппаратных средств (таблица А.1 ИСО 26262-5); примеры см. ниже.

9.2.3.3 Шаг 1a. Предположения о технических требованиях безопасности

Ниже приведены некоторые примеры предполагаемых технических требований безопасности, созданные для рассматриваемого примера микроконтроллера.

Предположения о технических требованиях безопасности (шаг 1a):

a) отказы памяти команд процессора ослабляются механизмом(ами) безопасности аппаратного средства, по крайней мере, до целевого значения (например, 90%), определенного для метрики одиночного сбоя на уровне части аппаратного средства (может быть также выражено в терминах требуемого ОД);

b) вклад микроконтроллера в суммарную вероятность нарушения цели безопасности составляет не более 10% от допустимой вероятности для соответствующего УПБА;

c) микроконтроллер реализует безопасное состояние, определяемое как включение низкого уровня на все выходы управления вводом-выводом, когда запускается сброс;

d) любые реализованные механизмы безопасности, связанные с выполняемой функцией, завершают ее менее чем за 10 миллисекунд (задаваемая часть времени сбоеустойчивости);

e) интерфейсы отладки микроконтроллера не используются во время связанной с безопасностью эксплуатации. Таким образом, любые сбои в логике отладки будут считаться безопасными сбоями;

f) присутствует модуль защиты памяти, чтобы обеспечить возможность разделения запрограммированных задач с различными значениями УПБА.

Значение УПБА задается на данном шаге.

9.2.3.4 Шаг 1b. Предположения о проектировании на уровне системы

Ниже представлены некоторые примеры внешних по отношению к ОЭБ предположений о проектировании на уровне системы:

a) система будет реализовывать механизм безопасности для источника питания микроконтроллера для обнаружения видов отказов, связанных с повышенным и пониженным напряжениями;

b) система будет реализовывать механизм безопасности на основе обрабатываемого методом окна сторожевого устройства, внешнего по отношению к микроконтроллеру, для обнаружения отказов синхронизации или последовательности программы микроконтроллера;

c) будет выполняться программно реализованный тест для обнаружения скрытых сбоев в механизме безопасности микроконтроллера, реализующем обнаружение и коррекцию ошибок (SM4);

d) тест на основе программного обеспечения (SM2) выполняется при включении зажигания для проверки отсутствия скрытых сбоев при логическом контроле последовательности программы процессора (SM1).

9.2.3.5 Шаг 2. Разработка аппаратных средств

На основании этих решений (предполагаемые технические требования к системе безопасности и предположения, связанные с внешним проектом по отношению к ОЭБ) в соответствии с требованиями ИСО 26262-5 разрабатывается ОЭБ (шаг 2) и формируются все соответствующие результаты работы. Например, оценка нарушения цели безопасности из-за случайных отказов аппаратных средств (см. результат работы, представленный в 9.5.1 ИСО 26262-5) осуществляется рассмотрением предположений ОЭБ, включающих любые значения интенсивности отказов во времени (FIT), найденные в предполагаемых технических требованиях к системе безопасности. На основе предположений ОЭБ в соответствии с ИСО 26262-9 выполняется анализ безопасности и анализ зависимых отказов внутренних по отношению к микроконтроллеру.

Для микроконтроллера в примере А.3.5 требование безопасности a) выполняется, потому что метрика одиночного сбоя памяти превышает целевое значение 90%, определенное на уровне части аппаратного средства (99,8%, постоянные сбои и 99,69% кратковременные сбои). Предположение c) о проекте системы реализуется механизмом безопасности SM4.

9.2.3.6 Шаг 3. Результаты работы

В конце разработки микроконтроллера (шаг 3) системному интегратору предоставляется необходимая информация о результатах работы, которая включает следующие документы: предполагаемые требования, предположения, связанные с внешним проектом по отношению к ОЭБ и соответствующие результаты, полученные в соответствии с настоящим стандартом (например, отчет о вероятности нарушения цели безопасности из-за случайных отказов аппаратных средств).

9.2.3.7 Шаг 4. Интеграция ОЭБ в устройство

Если разработанный как ОЭБ микроконтроллер рассматривается в контексте стадии разработки аппаратных средств устройства, то выполняется обоснованность выполнения всех предположений для ОЭБ, включая предполагаемые технические требования к системе безопасности ОЭБ и предположения, связанные с внешним проектом по отношению к ОЭБ (этап 4). Вполне вероятно, что будут возникать несоответствия между предположениями для ОЭБ и требованиями к системе. Например, разработчик устройства может принять решение не применять предполагаемый внешний компонент. Как следствие, оценка нарушения цели безопасности из-за случайных отказов аппаратных средств, выполненная разработчиком ОЭБ, не может больше соответствовать устройству.

В случае несоответствия предположения для ОЭБ, начиная с анализа влияния, выполняется технология управления изменениями в соответствии с требованиями раздела 8 ИСО 26262-8 (Управление изменениями). Возможные результаты включают в себя:

- несоответствие может считаться приемлемым в связи с достижением цели безопасности, и никакие действия не предпринимаются;

- несоответствие может оказать влияние на достижение цели безопасности и привести к необходимости изменения концепции функциональной безопасности либо технических требований к системе безопасности;

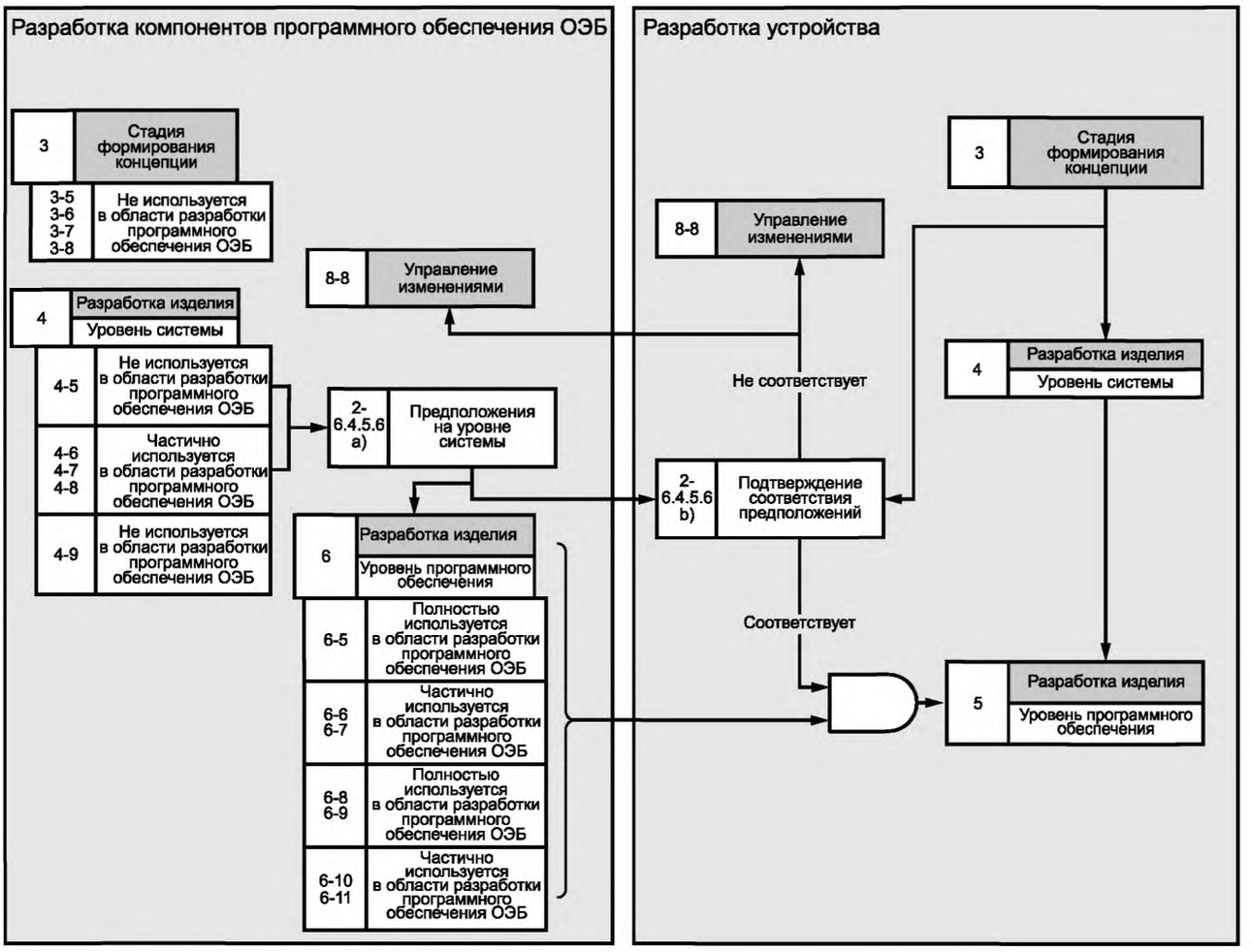
- несоответствие может оказать влияние на достижение цели безопасности и привести к необходимости изменения в общем компоненте безопасности (включая, возможно, изменение самого компонента);

- несоответствие может оказать влияние на достижение цели безопасности, поэтому пересчитываются метрики безопасности, и если пересчитанные метрики показывают, что проект отвечает целям системы, то в изменениях нет необходимости.

9.2.4 Разработка компонента программного обеспечения как общеиспользуемого элемента безопасности

9.2.4.1 Общие положения

В настоящем пункте представлены различные шаги применения концепции ОЭБ для новых среднего или низкого уровня компонент программного обеспечения. Последовательность действий процесса разработки приведена на рисунке 21.



Примечания

1 В зависимости от конкретной природы ОЭБ может потребоваться некоторая дополнительная адаптация требований.

2 В зависимости от конкретной природы ОЭБ некоторые требования части 6 не могут быть применены, поэтому они применяются лишь частично.

3 Хотя все разделы настоящего стандарта не представлены на рисунке 21, но это не означает, что они не применяются.

Рисунок 21 — Разработка компонента программного обеспечения как ОЭБ

9.2.4.2 Шаг 1а. Предположения об области применения компонента программного обеспечения как ОЭБ

На данном шаге устанавливаются соответствующие предположения о цели компонента программного обеспечения, его границах, окружении и функциональных возможностях.

Примерами таких предположений являются:

- программный компонент интегрируется в заданную многоуровневую архитектуру программного обеспечения;

- любые возможные взаимовлияния, вызванные компонентом программного обеспечения, обнаруживаются и обрабатываются его окружением;

- компонент программного обеспечения обеспечивает выполнение функций, представленных в списке функциональных требований программного обеспечения.

9.2.4.3 Шаг 1b. Предположения о требованиях к безопасности для компонента программного обеспечения

На шаге 1b формируются предположения на основе требований к безопасности более высокого уровня, которые могут влиять на программный компонент, чтобы для него вывести требования к безопасности. Например, если заданный набор данных, обрабатываемый компонентом программного обеспечения, характеризуется высоким уровнем полноты безопасности (УПБА *x*), то в результате требованиями к безопасности программного обеспечения, задаваемыми для ОЭБ, могут быть:

- компонент программного обеспечения должен обнаруживать любые повреждения следующих входных данных: список входных данных (УПБА *x*);
- компонент программного обеспечения должен предупреждать о следующих состояниях ошибок: список состояний ошибок (УПБА *x*);
- для любого обнаруженного состояния ошибки по умолчанию должно возвращаться значение статуса сбоя (УПБА *x*);
- компонент программного обеспечения должен возвращать получаемые результаты контроля циклическим избыточным кодом и статус (УПБА *x*).

9.2.4.4 Шаг 2. Разработка компонента программного обеспечения

Как только необходимые предположения о компоненте программного обеспечения явно установлены, то в соответствии с требованиями ИСО 26262-6 разрабатывается ОЭБ для его значения УПБА (УПБА *x* в данном примере). Формируются все соответствующие результаты работы для последующей интеграции в различных контекстах, в том числе результаты работы, связанные с верификацией предполагаемых требований к безопасности программного обеспечения.

9.2.4.5 Шаг 3. Интеграция компонента программного обеспечения в новом конкретном контексте

Перед интеграцией компонента программного обеспечения с другими компонентами программного обеспечения в новом конкретном контексте выполняется подтверждение соответствия всех предположений для этого ОЭБ в рассматриваемом контексте. Такое подтверждение соответствия выполняется для предполагаемых требований безопасности программного обеспечения с их значениями УПБА и для всех предположений, сделанные о цели, границах, окружении и функциональных возможностях компонента программного обеспечения (см. 9.2.4.2 и 9.2.4.3).

В случае, если некоторые предположения рассматриваемого компонента программного обеспечения не соответствуют этому новому контексту, то инициируется анализ влияния в соответствии с требованиями раздела 8 ИСО 26262-8 (Управление изменениями). Возможные результаты анализа влияния включают в себя:

- несоответствия являются приемлемыми для достижения требований безопасности, применяемых на уровне проектирования архитектуры программного обеспечения, и никаких дальнейших действий не предпринимается;
- несоответствия влияют на достижение требований безопасности, применяемых на уровне проектирования архитектуры программного обеспечения. В зависимости от конкретного случая применяется технология управления изменениями в соответствии с требованиями раздела 8 ИСО 26262-8 (Управление изменениями) либо для компонента программного обеспечения, либо для требований к безопасности, применяемых на уровне проектирования архитектуры программного обеспечения.

Примечание — В случае если интеграция компонента программного обеспечения в конкретный проект архитектуры программного обеспечения приводит к проблеме совместимости связанных с безопасностью элементов программного обеспечения, для которых определены различные значения УПБА, то должны быть выполнены критерии совместимости элементов в соответствии с требованиями раздела 6 ИСО 26262-9 (Критерии совместимости элементов) или, в противном случае, элементам с низкими значениями УПБА будут определены более высокие значения УПБА.

10 Пример подтверждения проверкой эксплуатацией

10.1 Общие положения

В данном разделе в качестве примера описаны устройство и требования к нему. Цель безопасности, его значение УПБА и последующие требования приведены для иллюстрации подтверждения проверкой эксплуатацией, определенной в разделе 14 ИСО 26262-8 (подтверждение проверкой эксплуатацией). Данный пример не отражает применение настоящего стандарта для аналогичного реального примера.

10.2 Определение устройства и определение кандидата, проверенного эксплуатацией

Изготовитель транспортного средства хочет интегрировать новую функциональность в новый автомобиль. В рассматриваемом примере устройство, реализующее эту функциональность, состоит из датчиков, одного электронного блока управления, включающего в себя готовые аппаратные средства и программное обеспечение, необходимые для реализации функциональности, и один исполнительный механизм.

Некорректность выполнения функциональности оценивается изготовителем транспортного средства значением УПБА, равным С. Соответствующая цель безопасности, из которой получаем в качестве требования функциональной безопасности значение УПБА, равное С, которое определяется для электронного блока управления.

Поставщик электронного блока управления предлагает использовать уже существующий электронный блок управления.

Анализируются различия между предыдущим использованием электронного блока управления и его предполагаемым использованием в новом применении. Анализ показывает, что программное обеспечение должно быть модифицировано для реализации новых функциональных возможностей изменением данных калибровки, но аппаратные средства электронного блока управления могут быть использованы без изменений. Поставщик намерен для аппаратных средств электронного блока управления заменить демонстрацию соответствия требованиям ИСО 26262-5 подтверждением проверкой эксплуатацией. Поэтому аппаратные средства электронного блока управления становятся кандидатом, проверяемым эксплуатацией.

10.3 Анализ изменений

Для установления доверия проверке эксплуатацией, поставщик выполняет анализ изменений проверенного эксплуатацией кандидата.

Этот анализ показывает, что не было никаких изменений, которые могли бы оказать влияние на безопасность поведения проверенного эксплуатацией кандидата, с самого начала его производства.

Более того, анализ показывает, что различия между предыдущим использованием проверенного эксплуатацией кандидата и его целевым использованием не имеют никакого влияния на безопасность, так как:

- граничные значений параметров кандидата находятся внутри заданных пределов;
- предыдущее окружение интеграции требует такого же поведения техники; и
- причина и следствия на границе кандидата одинаковы в предыдущем и будущем окружении интеграции.

10.4 Целевые значения для проверки эксплуатацией

Чтобы установить доверие к подтверждению проверкой эксплуатацией, поставщик оценивает общее количество часов работы проверенного эксплуатацией кандидата. Поставщик также анализирует эксплуатационные данные за период технического обслуживания для любого связанного с безопасностью события, то есть любое сообщение о событии, которое могло бы вызвать или способствовать нарушению цели безопасности, или требование безопасности, относящееся к целевому использованию кандидата в новом устройстве.

Выполняется оценка всей истории обслуживания с учетом количества произведенных транспортных средств со встроенным, проверенным эксплуатацией кандидатом, датой производства и данных о типичном использовании транспортного средства в данном сегменте рынка (количество часов вождения автомобиля в год).

История обслуживания включает информацию о возвращении в процессе эксплуатации различных транспортных средств, оснащенных проверяемым эксплуатацией кандидатом, связанную с:

- гарантийными претензиями;
- анализами дефектов в процессе эксплуатации; или
- возвращением бракованных частей от производителей транспортных средств.

На дату начала разработки аппаратных средств устройства, результаты такого анализа показывают, что связанных с безопасностью событий в процессе эксплуатации не происходило. Общее количество часов вождения, по оценкам, меньше целевого значения, определенного для статуса «проверен эксплуатацией» для значения УПБА, равного С, но удовлетворяет интервалу периода технического обслуживания, определенному в 14.4.5.2.5 ИСО 26262-8.

Выводы:

- разработчики устройства могут далее взять на себя ответственность, что для аппаратных средств электронного блока управления результаты проверкой эксплуатацией можно предварительно предсказать;
- для получения статуса «проверен в эксплуатации» необходимо постоянно собирать информацию в процессе эксплуатации (см. 14.4.5.2.5 ИСО 26262-8 и 14.4.5.2.6 ИСО 26262-8).

11 О декомпозиции значений УПБА

11.1 Цель декомпозиции значений УПБА

Целью декомпозиции УПБА является применение избыточности, чтобы соответствовать цели безопасности для систематических отказов. Декомпозиция УПБА может привести к избыточным требованиям и к реализации этих соответствующих декомпозированных значений УПБА достаточно независимыми элементами.

11.2 Описание декомпозиции значений УПБА

Декомпозиция значений УПБА связана с распределением избыточных требований безопасности для достаточно независимых элементов устройства. Избыточность в данном контексте не обязательно подразумевает классическое модульное резервирование (см. 2.94 ИСО 26262-1).

Пример — Центральный процессор электронного блока управления может контролироваться избыточным контрольным процессором, оба из которых независимо друг от друга способны инициировать заданное безопасное состояние, даже если контрольный процессор не может выполнять функциональные требования, определенные для электронного блока управления.

Декомпозицию значений УПБА можно рассматривать только в контексте систематических отказов, то есть в рамках методов и мер, применяемых для снижения вероятности таких отказов. При декомпозиции значений УПБА требования к оценке метрик архитектуры аппаратных средств и оценке нарушения цели безопасности из-за случайных отказов аппаратных средств остаются неизменными (см. 5.4.5 ИСО 26262-9).

Пример — Декомпозиция со значением УПБА B(D) не означает, что целевое значение УПБА, равное D, для оценки метрик архитектуры аппаратных средств декомпозируется на отдельные целевые значения УПБА, равные B, для каждого элемента аппаратных средств. Как указано в 8.2 ИСО 26262-5, целевые значения могут быть распределены элементам аппаратных средств, но такие целевые значения назначаются индивидуально на основе анализа, начинающегося на уровне аппаратных средств всего устройства. На уровне устройства целевая метрика применяется в соответствии с целью безопасности.

В декомпозированной таким образом архитектуре соответствующая цель безопасности нарушается только тогда, когда оба элемента одновременно нарушают декомпозированные для них требованиям безопасности.

Допустимые настоящим стандартом декомпозиции описаны в разделе 5 ИСО 26262-9 (Декомпозиция требований с распределением УПБА).

11.3 Пример декомпозиции значений УПБА

11.3.1 Общие положения

Устройство и требования к нему, описанные в данном подразделе, используются в качестве примера. Цель безопасности, ее значение УПБА и следующие за ними требования предназначены только для иллюстрации процесса декомпозиции значения УПБА. Данный пример не отражает применение настоящего стандарта для аналогичного реального примера.

11.3.2 Определение устройства

Рассмотрим пример системы с исполнительным механизмом, который срабатывает по запросу водителя с помощью переключателя на приборной панели. В данном примере исполнительный механизм выполняет некоторую функцию для удобства водителя, если транспортное средство не двигается, но может привести к опасным событиям, если автомобиль двигается со скоростью более 15 км/час.

Для данного примера исходная архитектура устройства может быть описана следующим образом:

- входной сигнал переключателя на приборной панели считывается специальным электронным блоком управления (именуемым в данном примере «электронный блок управления исполнительным механизмом (ЭБУИМ)»), который подает питание на исполнительный механизм по выделенной линии питания;

- транспортное средство оборудовано устройством также с электронным блоком управления, которое способно обеспечить информацию о скорости транспортного средства. Для данного примера предполагается, что электронный блок управления предоставляет информацию о том, что скорость транспортного средства превышает 15 км/ч, и значение УПБА для этого требования равно С. В дальнейшем этот электронный блок управления будем называть «электронным блоком, управляемым скоростью (ЭБУС).

11.3.3 Анализ опасностей и оценка рисков

Опасным событием, рассматриваемым в анализе, является включение — водителем или без его запроса — исполнительного механизма во время движения автомобиля со скоростью выше 15 км/ч.

Для рассматриваемого примера УПБА, связанный с этим опасным событием, классифицируется, как УПБА, равный С.

11.3.4 Соответствующая цель безопасности

Цель безопасности 1. Предотвратить включение исполнительного механизма при движении транспортного средства со скоростью более 15 км/ч. Значение УПБА равно С.

11.3.5 Предварительная архитектура и концепция обеспечения безопасности

11.3.5.1 Общая структура системы с исполнительным механизмом

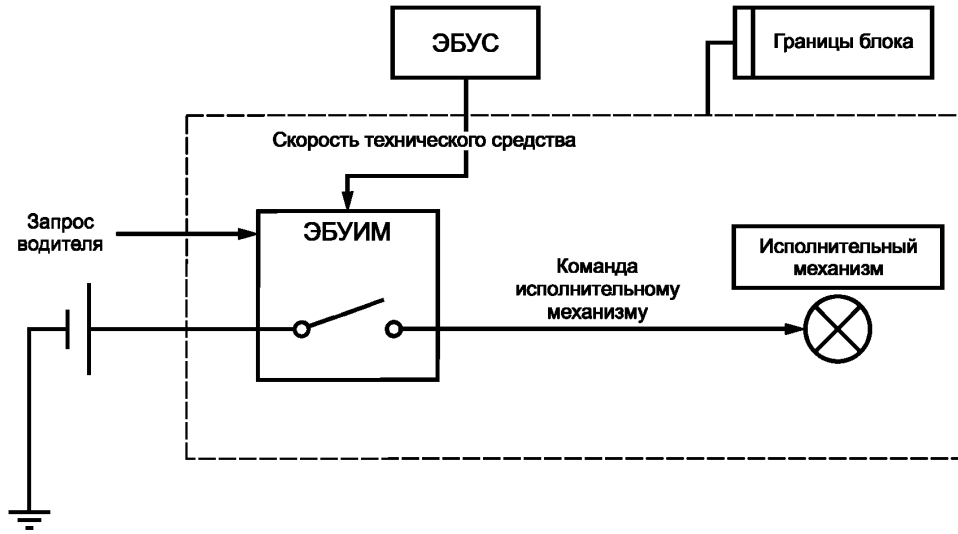


Рисунок 22 — Границы устройства

11.3.5.2 Цель элементов (первоначальная архитектура):

- ЭБУС передает в ЭБУИМ значение скорости транспортного средства;
- ЭБУИМ отслеживает запросы водителя, проверяет, не превысила ли скорость автомобиля значение, равное 15 км/ч, и если скорость не превышена, то при запросе водителя выдается команда исполнительному механизму;
- исполнительный механизм выполняет свои функции, если на него подается питание.

11.3.6 Концепция функциональной безопасности

11.3.6.1 Общие положения

Настоящий пример концепции функциональной безопасности используется только в качестве иллюстрации декомпозиции значения УПБА, он не является исчерпывающим и не включает в себя все требования функциональной безопасности.

Требование А1. ЭБУС посылает точную информацию о скорости транспортного средства в ЭБУИМ. => Значение УПБА равно С.

Требование А2. ЭБУИМ не подает питание на исполнительный механизм, если скорость автомобиля превышает 15 км/ч. => Значение УПБА равно С.

Требование А3. Исполнительный механизм приводится в действие только при подаче на него питания от ЭБУИМ. => Значение УПБА равно С.

11.3.6.2 Усовершенствованная концепция безопасности устройства

Разработчики имеют возможность ввести дополнительный (избыточный) элемент, аварийный выключатель, как показано на рисунке 23. Вводя этот избыточный элемент, ЭБУИМ разрабатывается со значением УПБА, равным или ниже значения УПБА, равного С, в соответствии с результатами декомпозиции значения УПБА.

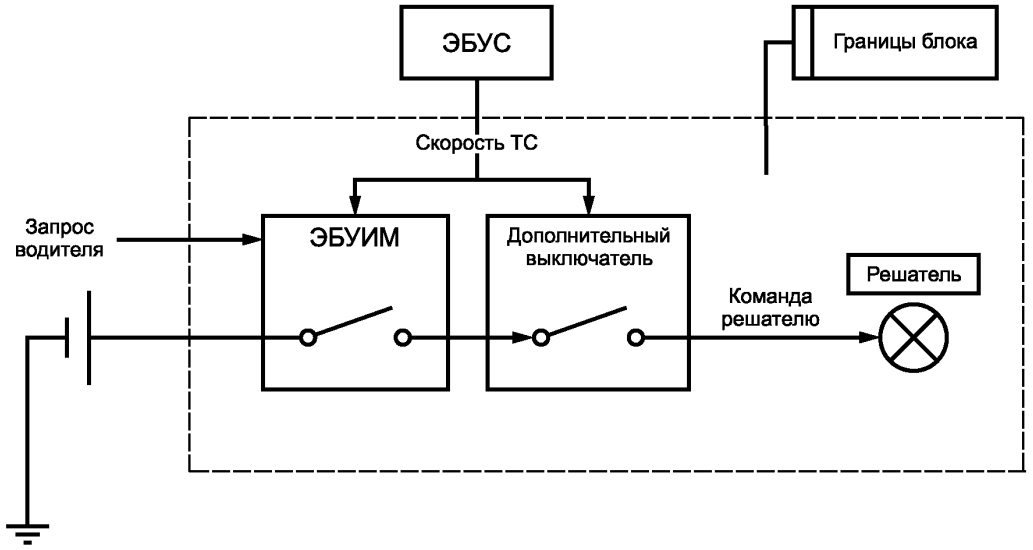


Рисунок 23 — Вторая итерация проекта устройства

Цель элементов (усовершенствованная архитектура) на рисунке 23:

- ЭБУС передает в ЭБУИМ значение скорости транспортного средства;
- ЭБУИМ отслеживает запросы водителя, проверяет, не превысила ли скорость автомобиля значение, равное 15 км/ч, и если скорость не превышена, то при запросе водителя выдается команда исполнительному механизму;
- на шине питания между ЭБУИМ и исполнительным механизмом находится дополнительный выключатель. Он включается, если скорость транспортного средства меньше или равна 15 км/ч, и выключается, когда скорость превышает 15 км/ч. Он делает это независимо от состояния шины питания (его источник питания не зависит от источника питания исполнительного механизма).

Требования функциональной безопасности для усовершенствованной архитектуры представлены ниже.

Требование В1. ЭБУС посылает точную информацию о скорости транспортного средства в ЭБУИМ. => Значение УПБА равно С.

Альтернатива. Предотвращается некорректная передача информации о том, что скорость транспортного средства меньше или равна 15 км/ч. => Значение УПБА равно С.

Требование В2. ЭБУИМ не подает питание на исполнительный механизм, если скорость автомобиля превышает 15 км/ч. => Значение УПБА равно X(C) (см. таблицу 4).

Требование В3. ЭБУС посылает точную информацию о скорости транспортного средства в аварийный выключатель. => Значение УПБА равно С.

Требование В4. Аварийный выключатель находится в разомкнутом состоянии, если скорость транспортного средства превышает 15 км/ч. => Значение УПБА равно Y(C) (см. таблицу 4).

Требование В5. Исполнительный механизм приводится в действие только при подаче на него питания от ЭБУИМ и аварийный выключатель находится в замкнутом состоянии. => Значение УПБА равно С.

Чтобы позволить декомпозицию значения УПБА, разработчики добавляют требование независимости в случае необходимости:

Требование В6. Показана достаточная независимость ЭБУИМ и аварийного выключателя. => Значение УПБА равно С.

Первоначальное требование A2 было заменено дополнительными требованиями B2 и B4, оба из которых удовлетворяют цели безопасности, и поэтому декомпозиция значения УПБА может быть применена.

Таблица 4 — Возможные декомпозиции

	Требование B2. УПБА равно X(C)	Требование B4. УПБА равно Y(C)
Возможность 1	УПБА равно C(C) для требований	УПБА равно QM(C) для требований
Возможность 2	УПБА равно B(C) для требований	УПБА равно A(C) для требований
Возможность 3	УПБА равно A(C) для требований	УПБА равно B(C) для требований
Возможность 4	УПБА равно QM(C) для требований	УПБА равно C(C) для требований

Приложение А
(справочное)

ИСО 26262 и микроконтроллеры

А.1 Общие положения

Целью данного приложения является рассмотрение не исчерпывающего списка примеров использования микроконтроллеров в контексте применения настоящего стандарта.

А.2 Микроконтроллер, его части и подчасти

Микроконтроллер (MCU или μC) представляет собой небольшой компьютер на одной интегральной схеме, включающий процессор, генератор тактовых импульсов, таймеры, периферийные устройства, порты ввода/вывода и память. Кристалл часто содержит как память для программ, реализованную в виде постоянной памяти (например, флэш-ПЗУ или однократно программируемую постоянную память), так и некоторый объем памяти с произвольным доступом.

Как показано на рисунке, иерархически весь микроконтроллер может рассматриваться как компонент, а блок обработки (например, процессор) как часть. Как описано в примере 4.2 и более подробно в А.3.3, в некоторых случаях (например, в зависимости от типа используемого механизма безопасности на уровне микроконтроллера или системы), каждая часть может быть далее разделена на подчасти (например, блок регистров ЦП и его внутренние регистры).

Такое представление является логическим представлением микроконтроллера. Оно не обязательно соответствует его физической реализации, и не обязательно отражает зависимости между частями и подчастями.

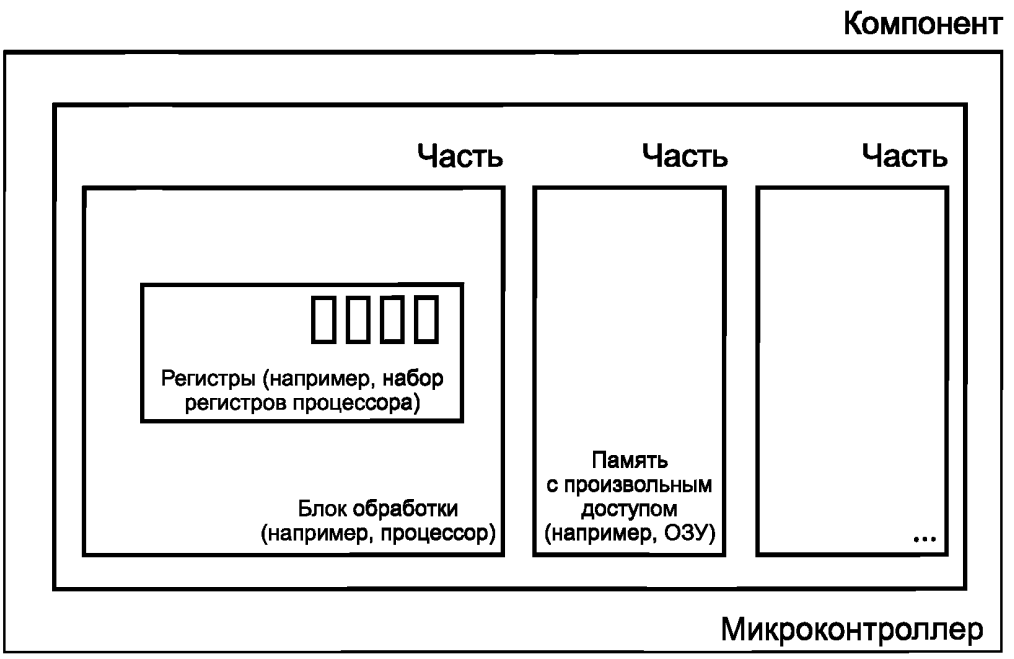


Рисунок А.1 — Микроконтроллер, его части и подчасти

В приложении D ИСО 26262-5 и, в частности, в таблице D.1 ИСО 26262-5 представлен список частей и подчастей микроконтроллера. Части или подчасти, не включенные в таблицу D.1 ИСО 26262-5, могут быть классифицированы по аналогии с уже определенными частями или подчастями. В таблице А.1 приведены некоторые примеры.

Таблица А.1 — Пример классификации частей и подчастей микроконтроллера, рассмотренного в ИСО 26262-5

Элементы в таблице D.1 ИСО 26262-5	Примеры для микроконтроллера	
	Часть	Подчасть
Источник питания	Встроенный регулятор напряжения (EVR), модуль управления электропитанием (PMU)	

Окончание таблицы А.1

Элементы в таблице D.1 ИСО 26262-5	Примеры для микроконтроллера	
	Часть	Подчасть
Устройство синхронизации	Схема фазовой синхронизации (PLL), кольцевой генератор, блок генерации синхросигналов (CGU), дерево синхронизации	
Постоянная память	FLASH, EEPROM, ROM, однократно программируемая (OTP) постоянная память	Массив элементов памяти, дешифратор адреса, интерфейсная схема, тестовая / избыточная логика, контроллеры памяти
Память с произвольным доступом	RAM, кеш-память	Массив элементов памяти, дешифратор адреса, интерфейсная схема, тестовая / избыточная логика, контроллеры памяти
Аналоговое и цифровое устройства ввода/вывода	Универсальные интерфейсы ввода/вывода (GPIO), широтно-импульсный модулятор (PWM)	
	Аналого-цифровой преобразователь (ADC), цифроаналоговый преобразователь (DAC)	
	Центральный процессор (CPU)	Арифметико-логическое устройство (ALU), информационные каналы CPU
		Блок регистров, внутренняя RAM CPU, такие как небольшие кэш-памяти данных
		Модуль загрузки и хранения и интерфейсы шины
		Секвенсер, кодирование и логика выполнения, включая регистры признака и управление стеком
		Контроллеры локальной памяти CPU, включая контроллеры кэш-памяти
	Контроллер прерываний	Регистры конфигурации контроллера прерываний
	Универсальные таймеры	
Средства коммуникации	Коммуникация на кристалле, включая управление доступом к шине	Матричный коммутатор каналов или коммутируемая сеть устройств. Протокол, разрядность данных и преобразование тактовых сигналов (например, мосты между шинами)
	Коммуникация на кристалле, используя прямой доступ к памяти (DMA)	Логика адресации DMA, адресные регистры DMA, буферные регистры DMA
	Последовательный периферийный интерфейс (SPI), интерфейс к запоминающему устройству с последовательной выборкой (SMI), интерфейс межсоединения ИС (I2C), интерфейс локальной сети контроллеров (CAN), синхронизируемая по времени локальная сеть контроллеров (TTCAN), автомобильный сетевой коммуникационный протокол (FlexRay), коммутируемая локальная сеть (LIN), односторонняя полубайтовая передача (SENT), Ethernet, интерфейс распределенных систем (DSI), интерфейс периферийных датчиков (PSI5)	

Данная таблица является примером: список частей/подчастей и декомпозиция микроконтроллера могут быть различными.

А.3 Общее описание разработки микроконтроллера и анализа безопасности в соответствии с настоящим стандартом

А.3.1 Общие положения

Если микроконтроллер разрабатывается как часть разрабатываемого устройства в соответствии с требованиями настоящего стандарта, то он должен удовлетворять требованиям безопасности, которые выводятся из целей безопасности устройства на верхнем уровне. Для метрик архитектуры аппаратных средств и вероятностной метрики для случайных отказов аппаратных средств устройства распределяются целевые значения, при этом микроконтроллер является лишь одним из элементов устройства. Как видно из примера, описанного в 8.2 ИСО 26262-5, чтобы сделать распределенную разработку более легкой, целевые значения могут быть распределены самому микроконтроллеру. Анализ безопасности микроконтроллера выполняется на основе требований и рекомендаций, определенных в 7.4.3 ИСО 26262-5 и в разделе 8 (Анализ безопасности) ИСО 26262-9.

С другой стороны, в случае, если целевое устройство еще не существует, то микроконтроллер может быть разработан, как общеиспользуемый элемент безопасности (ОЭБ, см. раздел 8 настоящего стандарта). В этом случае, разработка осуществляется на основе предположений об условиях использования микроконтроллера (Предположения Использования — ПИ), затем устанавливается обоснованность предположений на основе требований к микроконтроллеру, полученных из целей безопасности того устройства, в котором микроконтроллер должен использоваться.

Описанные ниже в данном приложении исследования и связанные с ними примеры выполнены, предполагая, что микроконтроллер является общеиспользуемым элементом безопасности, но описанные методы (например, метод вычисления интенсивности отказов микроконтроллера) остаются допустимыми и для микроконтроллера, который не является общеиспользуемым элементом безопасности. Если эти исследования проводятся для автономного микроконтроллера, то делаются соответствующие предположения. В А.3.9 описывается процедура адаптации и верификации результатов этих исследований и допущений на уровне системы. Для автономного микроконтроллера каждое требование ИСО 26262-5, ИСО 26262-8 и ИСО 26262-9 (например, связанное с анализом безопасности, анализом зависимых отказов, верификацией и т.д.) остается в силе.

А.3.2 Качественный и количественный анализ микроконтроллера

Как видно из 8.2 ИСО 26262-9, качественный и количественный анализ безопасности выполняются на соответствующем уровне абстракции во время стадий формирования концепции и разработки изделия. Для микроконтроллера:

a) качественный анализ полезен при выявлении отказов. Один из возможных способов, когда он может быть выполнен, использует информацию, полученную из блок-схем микроконтроллера, и информацию, полученную из приложения D ИСО 26262-5.

Примечания

1 Приложение D ИСО 26262-5 может быть использовано в качестве отправной точки для анализа охвата диагностикой (DC) с заявленным значением DC, поддержанным надлежащим обоснованием.

2 Качественный анализ включает анализ зависимых отказов, рассмотренный ниже в А.3.6 (Пример анализа зависимых отказов);

b) количественный анализ выполняется, используя совокупность:

I) данных о структурировании на уровне логических блоков;

II) сведений, полученных из описания микроконтроллера на уровне межрегистровых передач (RTL) (для получения функциональной информации) и на уровне таблицы связей логических элементов (для получения функциональной и структурной информации);

III) сведений для оценки возможных не специфицированных взаимодействий подфункции (зависимых отказов, см. А.3.6);

IV) информации о схеме размещения, доступной только на заключительной стадии;

V) информации о верификации охвата диагностикой некоторых конкретных видов сбоев, таких как сбои типа короткое замыкание. Эту информацию можно применять только в некоторых случаях, например при сравнении части и ее соответствующего механизма безопасности;

VI) результатов экспертной оценки с обоснованием и тщательным рассмотрением эффективности мер на уровне системы.

Примечания

1 Анализ зависимых отказов выполняется качественными методами, потому что не существует общего и достаточно надежного количественного метода для оценки таких отказов.

2 Эта информация может появляться постепенно в процессе разработки микроконтроллера. Поэтому анализ может повторяться по мере появления новой информации.

Примеры

1 Оценка зависимых отказов начинается на ранней стадии проектирования. Чтобы выявить и избежать возможные источники зависимых отказов или обнаружить их влияние на обеспечение безопасности «системы на кристалле» специфицируются меры проектирования. На завершающей стадии проектирования используется подтверждение схеме размещения.

2 Во время выполнения первого шага количественного анализа, может быть доступна таблица связей предварительного размещения логических элементов для предварительного тестопригодного проектирования (DFT), а затем, используя таблицу связей окончательного размещения логических элементов для окончательного тестопригодного проектирования, анализ повторяют;

с) поскольку части и подчасти микроконтроллера могут быть реализованы в одном физическом компоненте, то как анализ зависимых отказов, так и анализ независимости от помех или на их отсутствие являются важными для микроконтроллеров. Более подробно см. А.3.6.

А.3.3 Метод вычисления интенсивностей отказов для микроконтроллера

А.3.3.1 Общие положения

Требования и рекомендации для расчета интенсивности отказов в целом определены в ИСО 26262-5, а требования для расчета метрик приведены в приложении С.

Следуя примеру, приведенному в приложении Е ИСО 26262-5, интенсивности отказов и метрики могут быть вычислены для микроконтроллеров следующим образом:

- во-первых, микроконтроллер декомпозируется на части или подчасти.

Примечания

1 Предположения о независимости выявленных частей верифицируются при анализе зависимых отказов.

2 Необходимый уровень детализации (например, если выбрать уровень частей или, если спуститься до уровня подчастей или уровня элементарных подчастей) может зависеть от стадии анализа и используемых механизмов безопасности (внутри микроконтроллера или на уровне системы).

Примеры

1 Если функциональные возможности процессора контролируются другим процессором, работающих в жестко параллельном режиме (в однокристальной многопроцессорной системе), то анализ не должен рассматривать каждый процессор и каждый регистр внутри процессора, в то время как более подробно может быть необходимо рассмотреть компаратор такой жёсткой конфигурации. Если, с другой стороны, функциональные возможности процессора контролируются самотестирующим программным обеспечением, то может быть целесообразен подробный анализ различных подчастей процессора.

2 Уверенность в результате вычисления пропорциональна степени детализации: низкий уровень детализации может быть подходящим для анализа на стадии концепции, в то время как более высокий уровень детализации может быть подходящим для анализа на стадии разработки.

Примечание — В связи со сложностью современных микроконтроллеров (сотни или тысячи частей и подчастей), чтобы гарантировать полноту анализа, было бы полезно поддерживать процесс декомпозиции автоматическими средствами. Необходимо быть внимательным при анализе на уровне микроконтроллера через границы модуля. Разбиения делаются на иерархическом уровне межрегистровых передач, если это возможно;

- во-вторых, значения интенсивностей отказов каждой части или подчасти могут быть вычислены с помощью одного из следующих двух методов:

1) Если общая интенсивность отказов всего кристалла микроконтроллера (т.е. без учета корпуса и крепления кристалла) определяется, как количество отказов в единицу времени (FIT), то можно предположить, что интенсивность отказов части или подчасти, равна занимаемой этой частью или подчастью площади кристалла микроконтроллера (то есть площадь, занимаемая логическими элементами, тригерами и линиями связи), деленной на общую площадь кристалла микроконтроллера и умноженной на общую интенсивность отказов.

Примечания

1 Для чипов с различными сигналами и устройствами питания, этот подход применяется для каждого типа устройств, а общая интенсивность отказов для цифровых устройств может не совпадать с аналоговыми и устройствами питания.

2 Может быть полезным детальное знание микроконтроллера.

Пример — Если процессор занимает 3 % всей площади микроконтроллера, то можно предположить, что его интенсивность отказов равна 3 % от общей интенсивности отказов микроконтроллера.

2) Если базовые интенсивности отказов, т.е. интенсивности отказов базовых подчастей, таких как логические элементы микроконтроллера, заданы, то интенсивность отказов части или подчасти может считаться равной сумме количества этих базовых подчастей, умноженной на их интенсивность отказов.

Примечания

1 Может быть полезным детальное знание микроконтроллера.

2 Примеры о том, как получить базовые значения интенсивности отказов, см. в А.3.4;

- оценка завершается путем классификации сбоев на безопасные сбои, остаточные сбои, выявленные двойные сбои и скрытые двойные сбои.

Пример — Некоторые фрагменты блока отладки, реализованные внутри процессора, связаны с безопасностью (так как сам процессор связан с безопасностью), но они сами по себе не могут привести к непосредственному нарушению цели безопасности либо их появление не может значительно увеличить вероятность нарушения цели безопасности;

- наконец, определяется охват вида отказов, связанных с остаточными и скрытыми сбоями этой части или подчасти.

Пример — Охват вида отказов, связанных с конкретной интенсивностью отказов, может быть определен разделением подчасти на более мелкие подчасти и для каждой из них вычислением ожидаемой способности охватить каждую подчасть механизмами безопасности. Например, охват вида отказов, связанных с отказами в блоке регистров процессора, может быть определен разделением блока регистров на более мелкие подчасти, каждая из которых связана с конкретным регистром (например, R0, R1, ...) и вычислением охвата этого вида отказов механизмом безопасности для каждого из них, например, объединяя охват вида отказов для каждого из соответствующих видов отказов на нижнем уровне.

Примечания

1 На эффективность механизмов безопасности могут повлиять зависимые отказы. Адекватные меры рассматриваются в А.3.6.

2 Поскольку на этом уровне анализа не может быть рассмотрена способность обнаружения сбоя водителем транспортного средства, то концепция воспринимаемого сбоя не применяется на уровне микроконтроллера. См. А.3.9 для получения дополнительной информации о том, как объединить информацию на уровне микроконтроллера с применением.

3 В связи со сложностью современных микроконтроллеров (миллионы логических схем) для вычисления и верификации количества безопасных сбоев и особенно охвата определенного вида отказов можно использовать методы введения неисправностей. См. А.3.8.2 для уточнения деталей. Метод введения неисправностей не является единственным, возможны и другие подходы, как описано в А.3.8.2.

А.3.3.2 Как рассматривать кратковременные сбои

В примечании 2 к 8.4.7 ИСО 26262-5 указано, что 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 или с помощью качественного обоснования.

Если используется количественный подход, то интенсивности отказов и метрики для кратковременных сбоев могут быть вычислены, следуя примеру, приведенному в приложении Е ИСО 26262-5, в котором реализуется следующий метод:

- во-первых, микроконтроллер делится на части или подчасти, как в А.3.3.

Примечание — Вследствие количества и плотности элементов памяти в RAM результирующие интенсивности отказов для кратковременных сбоев могут быть значительно выше, чем те, которые относятся к обрабатывающей логике или другим частям микроконтроллера. Таким образом, как рекомендовано в примечании 1 к 8.4.7 ИСО 26262-5, полезно отдельно вычислять интенсивность отказов (и метрику) для оперативной памяти и для других частей микроконтроллера;

- во-вторых, интенсивности отказов каждой части или подчасти вычисляются с использованием базовой интенсивности отказа для неустойчивых сбоев.

Пример — В соответствии с методом, указанным в А.3.3, базовая интенсивность отказа может быть вычислена как функция от базовой интенсивности одиночных отказов одного элемента и неустойчивых одиночных событий и соответствующей рассматриваемой части схемы (например, выраженной в количестве триггеров и логических элементов). В А.3.4 представлены примеры того, как получить базовые значения интенсивности отказов;

- наконец, оценка завершается классификацией сбоев на безопасные сбои и остаточные сбои, например количество безопасных сбоев, связанных с интенсивностью отказов данной части или подчасти.

Примечание — Для оценки количества безопасных кратковременных сбоев, когда существует явная зависимость от прикладного программного обеспечения, и если это программное обеспечение недоступно в процессе разработки микроконтроллера, то оценка 50% на 50% может быть приемлемой. Если прикладное программное обеспечение доступно или если есть прямая зависимость от архитектуры микроконтроллера, то для определения этого значения предпочтительным является конкретный анализ.

Пример — Сбой в регистре, хранящем связанную с безопасностью константу (т.е. только один раз записанное значение, но считываемое в каждом такте, и если оно неверно, то происходит нарушение цели безопасности), никогда не безопасно. Если вместо этого, например, каждые 10 мс происходит запись в регистр значения, которое используется для связанного с безопасностью расчета только один раз, спустя 1 мс после записи, то случайный кратковременный сбой в регистре приведет в 90% случаев к безопасному сбою, потому что сбой в этом регистре за оставшиеся 90% времени такта не приведет к нарушению цели безопасности.

Примечания

1 Как видно из примечании 2 к 8.4.7 ИСО 26262-5, кратковременные сбои могут быть учтены с помощью метрики одиночного сбоя. Кратковременные сбои не рассматриваются так, как рассматриваются скрытые сбои. Охват вида отказов, вычисляемый для скрытых сбоев, не вычисляется для кратковременных сбоев, так как их основная причина быстро исчезает (по определению кратковременных сбоев). Кроме того, предполагается, что в подавляющем большинстве случаев их влияние будет быстро устранено, например, следующим циклом выключения питания, удаляющим ошибочное состояние триггера или ячейки памяти, которое было изменено кратковременным сбоем до того, как второй сбой может привести к возникновению множественного отказа. В особых случаях это может быть недопустимо и могут понадобиться дополнительные меры, однако они могут быть рассмотрены в зависимости от конкретной ситуации.

2 Кратковременные сбои, возникшие в одной подчасти, непреднамеренно не распространяются к другим подчастям, если это подчасти логически не связаны.

3 Некоторые из значений охвата диагностикой механизмами безопасности, определенные в таблицах D.2– D.14 приложения D ИСО 26262-5, действительны только для постоянных сбоев. Это важное различие может быть найдено в соответствующем описании механизма безопасности, в котором написано, как значение охвата может рассматриваться для кратковременных сбоев.

Пример — Типичное значение охвата RAM тестом «марш» (таблица D.6 ИСО 26262-5) оценивается как высокое. Однако в соответствующем описании (D.2.5.3 ИСО 26262-5) указано, что эти типы тестов не являются эффективными при обнаружении исправимых ошибок. Поэтому, например, охват RAM тестом «марш» кратковременных сбоев равен нулю.

Если используется качественный подход, то дается обоснование на основе проверки эффективности механизмов безопасности, реализованных (или внутри микроконтроллера или на уровне системы) для охвата кратковременных сбоев.

Пример — Для элементов канала передачи данных временная избыточность при обработке данных (т.е. обработка одной и той же информации несколько раз) уже будет гарантировать высокий уровень защиты от кратковременных сбоев.

А.3.4 Получение значений базовой интенсивности отказов, которые могут использоваться для микроконтроллеров

А.3.4.1 Общие положения

Как указано в 8.4.3 ИСО 26262-5, данные об интенсивностях отказов могут быть получены из признанных отраслевых источников. В следующем списке даны примеры стандартов и справочников, из которых можно получить значение базовой интенсивности отказа для метода, определенного в А.3.3 и А.3.3.2:

- для постоянных сбоев: данные, предоставленные промышленностью полупроводников, или использование стандартов, таких как МЭК/ТО 62380 [8], SN 29500 [6].

Примечание — Для постоянных сбоев: данные, предоставленные промышленностью полупроводников, могут быть основаны на значении числа (случайных) отказов, деленном на эквивалентное число часов работы прибора. Существующие полевые данные или полученные из ускоренных испытаний (как определено в стандартах, таких как JEDEC и AEC) масштабируются до режима работы (например, температуры, периодов включения/выключения) и предполагается, что интенсивности отказов постоянны (отказы случайные, распределены экспоненциально). Числовые значения могут быть представлены в виде максимального количества отказов в единицу времени (FIT) на основе уровня доверительной вероятности статистических методов получения выборок;

- для кратковременных сбоев: данные, предоставленные промышленностью полупроводников, полученные из JEDEC стандартов, таких как JESD89, ITRS (International Technology Roadmap for Semiconductor).

Примечание — Если должным образом подтвердить доказательствами, то базовые интенсивности отказов, полученные из стандартов и справочников, могут быть сформированы с учетом других факторов, таких как плотность расположения регистров и вероятность возникновения постоянных сбоев между включением и выключением зажигания и т.д.

А.3.4.2 Пример расчета интенсивности отказов (FIT) микроконтроллера на кристалле по МЭК/ТО 62380

В 8.4.3 ИСО 26262-5 установлено, что значения интенсивностей отказов могут быть получены из признанных отраслевых источников, например, МЭК/ТО 62380, МЭК 61709, MIL 217 F HDBK notice 2, RIAC HDBK 217 Plus. Ниже

приведен пример оценки интенсивности отказов (FIT) аппаратных средств, необходимой для поддержки количественного анализа с использованием методов, подробно описанных в МЭК/ТО 62380 [8]. Модель интенсивности отказов (FIT) для полупроводникового прибора по МЭК/ТО 62380 рассматривает интенсивность отказов прибора, как сумму трех значений: для микроконтроллера на кристалле, для корпуса и для электрического интерфейса, полученных в условиях повышения нагрузки.

Примечание — 1 FIT (количество отказов в единицу времени) соответствует одному отказу за 109 ч работы прибора.

А.3.4.2.1 Пример расчета интенсивности отказов микроконтроллера на кристалле

Для расчета базовой интенсивности отказов (FIT) микроконтроллера на кристалле (т.е. до применения фактора снижения для условий эксплуатации) необходимо рассмотреть четыре ключевых элемента:

- λ_1 — базовая интенсивность отказов (FIT) для транзистора, связанная с используемой технологией изготовления;
- N — количество реализованных транзисторов;
- α — фактор снижения из-за зрелости процесса; так как технология становится зрелой, начальная интенсивность отказов транзисторов экспоненциально снижается до асимптотического уровня;
- λ_2 — технологический процесс, определяющий интенсивность отказов (FIT), который не зависит от числа транзисторов или времени.

Эти факторы объединены в формуле в 7.3.1 МЭК/ТО 62380:2004 [8] («MATHEMATICAL MODEL»).

Выбор параметров может быть сделан на основе технологического процесса и типа используемого логического элемента. В таблице 16 из [8] приведены значения для КМОП-логики, аналоговых схем и нескольких типов памяти (SRAM, DRAM, EEPROM, flash EEPROM и т. д.).

Таблица А.2 демонстрирует вычисление интенсивностей отказов, используемых в примере, рассмотренном в А.3.5. Для фактора снижения из-за зрелости процесса предполагается, что год изготовления — 2008.

Таблица А.2 — Пример вычисления интенсивностей отказов

Элемент схемы	λ_1	N	α	λ_2	Базовое значение FIT
ЦП, состоящий из 50 тыс. логических элементов	$3,4 \times 10^{-6}$	200000 (4 транзистора в логическом элементе)	10	1,7	1,72
Статическое ОЗУ — 16 kB	$1,7 \times 10^{-7}$	786432 (6 транзисторов для ячейки статического ОЗУ с низким потреблением)	10	8,8	8,802
Сумма					10,52

Примечания

1 Для заданного типа элементов можно использовать несколько значений λ_1 и λ_2. В этом случае сторона, проводившая оценку, гарантирует, что выбранное значение наилучшим образом соответствует метрикам конкретной используемой технологии производства, и обеспечивает надлежащее обоснование.

2 Для упрощения расчета, оценку можно сделать для одинаковых для всего устройства значений λ_1 и λ_2.

3 Фактор снижения интенсивностей отказов из-за зрелости процесса был введен в связи с использованием закона Мура и того факта, что интенсивности отказов прибора являются более или менее постоянными. Если интенсивность отказов одного транзистора не будет меняться, то интенсивность отказов устройства в соответствии с законом Мура должна увеличиваться. Но это не наблюдается. Таким образом, интенсивность отказов транзистора не может оставаться постоянной при ее изменении в функциональных узлах. В [8] предлагается использовать дату изготовления. Возможно, чтобы отразить изменения технологического процесса, для конкретного узла может быть использован год первого введения технологии его изготовления, а не год его изготовления. Для достижения независимости от поставщиков кремния может быть использован год из ITRS (Международной дорожной карты для полупроводниковых технологий) [9].

4 Для расчета интенсивности отказов для всего микроконтроллера на кристалле используется число эквивалентных логических элементов N. Число эффективных эквивалентных транзисторов вычисляется путем умножения эквивалентного количества логических элементов на число транзисторов в представителе этого логического элемента. При расчете интенсивности отказов микроконтроллера на кристалле для КМОП цифровой логики вклад каждого элемента цифровой логики модуля (например, процессора, шины обмена сообщениями (CAN), таймера, FlexRay (автомобильного сетевого коммуникационного протокола), последовательного периферийного интерфейса) входит в N.

5 Для аналоговых частей или для микроконтроллера, построенного в основном на аналоговых технологиях, может быть использована позиция «Линейные схемы» в таблице 16 «МОП-структура: стандартные схемы (3)» в [8], если более точные данные не обеспечиваются поставщиком микроконтроллера.

6 При расчете вклада схем ввода/вывода в интенсивность отказов (FIT) такие схемы могут быть представлены некоторым числом эквивалентных транзисторов элементов КМОП цифровой логики, как показано в примечании 4, если более точные данные не обеспечиваются поставщиком микроконтроллера.

После того, как базовое значение интенсивности отказов (FIT) для микроконтроллера на кристалле сформировано, применяется фактор снижения, чтобы учесть влияние температуры и времени работы. Этот фактор снижения учитывает:

- температуру перехода транзистора микроконтроллера на кристалле, которая рассчитывается на основе:
- потребляемой мощности микроконтроллером на кристалле;
- теплового сопротивления корпуса, зависимого от типа корпуса, количества выводов на корпусе и потока воздушного охлаждения;
- прикладной профиль, который устанавливает 1 для *Y* стадий эксплуатации, каждая из которых характеризуется «временем нахождения во включенном состоянии» в процентном отношении от времени жизни прибора и температурой окружающей среды. В [8] предусмотрено два эталонных автомобильных профиля: «устройство управления двигателем» и «салон автомобиля»;
- энергию активации и частоту для каждого типа технологии, чтобы воспользоваться уравнением Аррениуса (Arrhenius).

Для данного примера предполагаем, что микроконтроллер на КМОП технологии потребляет 0,5 Вт. Микроконтроллер на кристалле помещен в 144-контактный плоский корпус с выводами с четырех сторон и охлаждается за счет естественной конвекции. Микроконтроллер подвергается воздействию температуры профиля «устройство управления двигателем». В результате увеличение температуры перехода ΔT_j равно 26,27°C. Для применения уравнения Аррениуса предполагается, что энергия активации равна 0,3 эВ. Используя формулу для фактора снижения из [8] получим, что его значение равно 0,17.

Если применить фактор снижения, то получаем эффективное значение интенсивности отказов (FIT) для компонента, как показано в таблице А.3.

Таблица А.3 — Пример вычисления эффективной интенсивности отказов (FIT) для компонентов

Элемент схемы	Базовое значение FIT	Фактор снижения от температуры	Эффективое значение FIT
ЦП, состоящий из 50 тыс. логических элементов	1,72	0,17	0,29
Статическое ОЗУ — 16 kB	8,80	0,17	1,50
Сумма			1,79

Примечание — Данные, характерные для рассматриваемого изделия, такие как тепловые характеристики корпуса, производственный процесс, уравнение Аррениуса и т.д., могут быть использованы для замены общих факторов в [8] для достижения более точной оценки интенсивности отказов (FIT).

А.3.4.2.2 Альтернативный расчет фактора снижения по МЭК/ТО 62380

Несмотря на то, что интенсивность отказов, получаемая согласно методике, представленной в [8], больше соответствует текущим данными по надежности, может быть полезным получение более консервативных данных, например более близким из давно использующихся справочников по интенсивностям отказов, таких как SN 29500. Эта задача может быть достигнута путем небольшого изменения используемой формулы вычисления фактора снижения от температуры.

Формула, используемая из 7.3.1 документа [8] («MATHEMATICAL MODEL»), для расчета фактора снижения от температуры δ_τ использует следующие параметры:

$(\pi_t)_i$ — *i*-й температурный коэффициент, связанный с *i*-й температурой перехода интегральной схемы используемого профиля;

τ_i — *i*-е относительное время работы интегральной схемы при *i*-й температуре перехода используемого профиля;

τ_{on} — относительное общее время работы интегральной схемы с $\tau_{on} = \sum_{i=1}^{y} \tau_i$;

τ_{off} — относительное время, когда интегральная схема хранит информацию (или не выполняет операций).

$\tau_{on} + \tau_{off} = 1$.

Для получения консервативной оценки фактора снижения от температуры устанавливают, что значение τ_{off} равно нулю. В результате получаем несколько отличную от формулы для вычисления δ_τ формулу для вычисления консервативного значения коэффициента снижения $\delta_{\tau,\ \text{консервативное}}$:

$$\delta_{\text{консервативное}} = \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on}}.$$

Применение этих формул приводит к величине фактора снижения от температуры равного 2,91, что приводит к результатам, представленным в таблице А.4.

Таблица А.4 — Пример вычисления эффективной интенсивности отказов (FIT) для компонентов

Элемент схемы	Базовое значение FIT	Фактор снижения от температуры	Эффективое значение FIT
ЦП, состоящий из 50 тыс. логических элементов	1,72	2,91	5,01
Статическое ОЗУ — 16 kB	8,80	2,91	25,61
Сумма			30,62

А.3.4.2.3 Пример влияния корпуса на интенсивность отказов

Интенсивность отказов, связанная с корпусом, рассчитывается по формуле, приведенной в 7.3.1 документа [8] («MATHEMATICAL MODEL») с использованием следующих параметров:

π_α — коэффициент влияния, связанный с разницей коэффициентов теплового расширения подложки и материала корпуса;

$(\pi_n)_i$ — i-й коэффициент влияния, связанный с числом ежегодных циклов колебаний температуры корпуса с амплитудой ΔT_i;

ΔT_i — i-я амплитуда колебаний температуры используемого профиля;

λ_3 — базовая интенсивность отказов корпуса интегральной схемы.

Для данного примера предполагаем, что микроконтроллер на КМОП технологии потребляет 0,5 Вт. Микроконтроллер на кристалле помещен в 144-контактный плоский корпус с выводами с четырех сторон и охлаждается за счет естественной конвекции. В результате увеличение температуры перехода ΔT_j равно 26,27 °С. Микроконтроллер подвергается воздействию температуры профиля «устройство управления двигателем».

Коэффициент влияния π_α рассчитывается по формуле, приведенной в 7.3.1 документа [8] («MATHEMATICAL MODEL»), с учетом линейных коэффициентов теплового расширения α_s и α_c для подложки и компонента соответственно. В данном примере предполагаем, что подложка из стеклоэпоксидной смолы (FR4), а корпус пластиковый, для которых из таблиц получаем значения α_s = 16 и α_c = 21,5.

Так как для автомобильного профиля число циклов в год ≤ 8760, то $(\pi_n)_i$ рассчитывается по формуле, приведенной в 7.3.1 документа [8] («Математическое выражение оценки фактора влияния $(\pi_n)_i$»), где n_i — число циклов в год с амплитудой ΔT_i.

Для расчета λ_3 в FIT используется формула для корпусов, у которых штырьки выводов расположены по краям, считая, что ширина корпуса равна 20 мм, а шаг штырьков выводов — 0,5 мм (таблица 17б в [8]).

Используя температурный профиль «устройство управления двигателем», для общей интенсивности отказов корпуса получим $\lambda_{\text{корпуса}}$ = 207 FIT.

Интенсивность отказов корпуса может быть равномерно распределена между штырьками выводов, что приводит к интенсивности отказов штырька $\lambda_{\text{штырька}}$ = 1,44 FIT.

Примечание — Оценка интенсивности отказов корпуса основана на знании конструкции и тепловых характеристик корпуса и печатной платой системы. Вместо применения [8] может быть использована совместная консервативная оценка интенсивности FIT корпуса поставщиком микроконтроллера и разработчиком системы.

А.3.4.2.4 Пример отказов в результате электрического перенапряжения

Интенсивность отказов для всего устройства из-за электрического перенапряжения может быть рассчитана по формуле, приведенной в 7.3.1 документа [8] («MATHEMATICAL MODEL»). Если устройство имеет непосредственный контакт с внешней средой, т.е. устройство представляет собой интерфейс, то π_I равно единице. Если устройство не является интерфейсом, то есть оно не имеет непосредственного контакта с внешней средой и π_I равно нулю.

В [8] предлагаются различные значения λ_{EOS} (EOS — электрическое перенапряжение) для различных электрических сред. К сожалению, электрическая среда автомобиля не представлена. Вместо нее можно выбрать среду «гражданская авионика (бортовые ЭВМ)», для которой λ_{EOS} = 20 FIT.

Это приводит к интенсивности отказов из-за электрических перенапряжений для всего устройства, либо $\lambda_{\text{перенапряжение}}$ = 20 FIT, если устройство имеет непосредственный контакт с внешней средой, либо $\lambda_{\text{перенапряжение}}$ = 0 FIT в любом другом случае.

Прогнозирование воздействия электрического перенапряжения на устройство не является тривиальной задачей. Если нельзя утверждать о каких либо особых воздействиях, то значение $\lambda_{перенапряжение}$ можно добавить к $\lambda_{кристалла}$, увеличив общую интенсивность отказов микроконтроллера на кристалле всего устройства.

Примечание — В некоторых стандартах электрические перенапряжения считают систематическими отказами и их уменьшают до нулевого значения FIT при расчете метрик случайных отказов.

A.3.5 Пример количественного анализа

Ниже приведен пример количественного анализа с использованием метода, описанного в A.3.3.

Примечания

1 Числовые значения, используемые в данном примере (например, интенсивности отказов, количество безопасных сбоев и охват вида отказов) используются в качестве примеров. Они могут отличаться для разных архитектур.

2 Следующие примеры декомпозируют некоторую часть микроконтроллера на уровне подчастей. Как уже обсуждалось в A.3.3, необходимый уровень детализации может зависеть от стадии анализа и от используемых механизмов безопасности.

3 В следующих примерах используется количественный подход для вычисления заданного целевого значения «метрики одиночных сбоев» для кратковременных сбоев. Как уже обсуждалось в A.3.3.2, кратковременные сбои могут быть также учтены с использованием качественного обоснования.

В данном примере рассматривается небольшая часть микроконтроллера, точнее только две его части:

a) небольшой процессор, разделенный на пять подчастей: блок регистров, АЛУ, блок загрузки-хранения, управляющая логика и блок отладки. Каждая подчасть разделена еще на несколько подчастей;

b) оперативная память (16 Кб) разделена на три подчасти: массив ячеек, дешифратор адреса, а также логика проверки конца строки и управление резервными строками (избыточностью) оперативной памяти.

Примечания

1 Значения FIT, приведенные в данном примере, не учитывают периферийные устройства или другие характеристики, такие как упаковка, технологическое манипулирование или перенапряжение. Они приведены только в качестве примера возможного способа вычисления интенсивности отказов (FIT). По этой причине, данные значения не сопоставимы со значениями интенсивности отказов (FIT) для всего микроконтроллера в корпусе, как показано, например, в SN 29500.

2 Целью следующего примера является отказ от требования учитывать каждую самую маленькую подчасть микроконтроллера при анализе на уровне системы. При анализе на уровне системы может быть достаточной детализация на уровне компонентов или частей. Целью данного примера является предоставление доказательств того, что для автономно работающего микроконтроллера может быть необходим более глубокий анализ (например, на уровне подчастей) для того, чтобы вычислить с необходимой точностью интенсивности отказов и охват видов отказов частей и подчастей, которые будут использоваться впоследствии системными инженерами. Другими словами, без точного и подробного анализа автономно работающего микроконтроллера бывает очень трудно получить хорошие данные для анализа на уровне системы.

Рассматриваются следующие четыре механизма безопасности:

1) механизм безопасности технических средств (SM1), выполняющий логический мониторинг последовательности программ процессора. Данный механизм безопасности способен обнаружить конкретный охват определенных сбоев в логике управления, которые могут нарушить последовательное выполнение программного обеспечения. Однако, этот механизм безопасности не обнаруживает сбои (например, неверные арифметические операции), приводящие к неправильным данным.

Примечание — В данном примере предполагается, что каждый из обнаруженных постоянных однобитовых сбоев, влияющих на процессор, подает сигнал системе (например, путем активации выходного сигнала микроконтроллера). На уровне системы установлено требование о надлежащем использовании этого сигнала (например, перевести в безопасное состояние и информировать водителя). При подозрительных кратковременных сбоях процессор может попробовать удалить этот сбой путем перезапуска. Если удалить не удалось, то это означает, что сбой является постоянным, и, следовательно, сигнал о нем может быть передан в систему, как описано выше. Если сбой исчезает (то есть это был действительно кратковременный сбой), то работа центрального процессора может быть продолжена;

2) механизм безопасности на основе программного обеспечения от случайных отказов аппаратных средств (SM2), выполняющийся при включении зажигания для проверки отсутствия скрытых сбоев в логическом мониторинге последовательности программ процессора (SM1);

3) исправление одиночных ошибок и обнаружение двойных ошибок кодом с обнаружением ошибок (EDC) в оперативной памяти (SM3).

Примечание — В данном примере предполагается, что о каждом обнаруженном постоянном однобитовом сбое — даже если он корректируется механизмом EDC — поступает сигнал в программное обеспечение

(например, с помощью прерываний) и программное обеспечение реагирует соответствующим образом. На уровне системы установлено требование о надлежащем использовании этого события (например, перевести в безопасное состояние и информировать водителя). При подозрительных кратковременных сбоях, исправляемых механизмом EDC, процессор может попробовать удалить эти сбои, повторно записав в память правильное значение. Если сбой устранить не удалось, то это означает, что он является постоянным и, следовательно, сигнал о нем может быть передан в систему, как описано выше. Если сбой исчезает (то есть это был действительно кратковременный сбой), то работа центрального процессора может быть продолжена. Чтобы отличить перемежающиеся и кратковременные сбои, можно применить метод подсчета числа исправлений.

4) механизм безопасности на основе программного обеспечения от случайных отказов аппаратных средств (SM4), выполняющийся при включении зажигания для проверки отсутствия скрытых сбоев в EDC (SM3).

Таблица А.5 разделена на три отдельных расчета для лучшего восприятия.

Таблица А.5 рассматривает виды отказов на уровне подчастей. В таблице А.6 показано, как могут быть определены виды отказов низкого уровня и, следовательно, как может быть вычислено общее распределение отказов в соответствии с подходом, описанным в А.3.9.

Пример — Таблица А.6 показывает, что интенсивность отказов от постоянного сбоя в триггере X1 и его схеме объединения по входу равна 0,01 FIT. Суммируя каждый из этих видов отказов низкого уровня, можно вычислить интенсивность отказов от постоянного сбоя в логике АЛУ в целом (0,07 FIT). С помощью той же процедуры, путем суммирования каждой интенсивности отказов, связанной с подчастью, можно вычислить интенсивность отказов (FIT) от постоянных сбоев в АЛУ.

Примечание — «Поднимаясь» по абстрактному дереву отказов (т.е. от видов отказов на низком уровне к видам отказов на более высоком уровне), интенсивности различных видов отказов подчастей могут быть объединены, чтобы вычислить интенсивность видов отказов более высокого уровня, особенно если эти виды отказов более высокого уровня определяются в более общем виде.

Пример — Если вид отказов более высокого уровня (например, на уровне части) определяется как «неправильная команда, выполняемая процессором», то интенсивность этого вида отказов может быть комбинацией интенсивностей многих видов отказов на уровне подчастей, таких как постоянный сбой в блоке конвеерной обработки, постоянный сбой в блоке регистров и т. д. Таким образом, если имеются интенсивности отказов низкого уровня, то интенсивность отказов более высокого уровня может быть вычислена снизу вверх (предполагается, что сбои независимы).

Примечание — Столбцы таблиц А.5 и А.6 могут быть соотнесены с блок-схемой классификации сбоев и классами сбоев, вносящих вклад в расчеты, описанные в 7.1.7:

- интенсивность отказов (FIT) равна λ;
- количество безопасных сбоев равно F_{safe};
- охват вида отказов в случае нарушения цели безопасности равен $K_{FMC,RF}$;
- интенсивность отказов от остаточного или одиночного сбоя равна λ_{SPF} или λ_{RF} в зависимости от того, является отказ одиночным или остаточным. В примере одиночные сбои не рассматриваются, так что эта интенсивность отказов всегда равна λ_{RF};
- охват вида отказов в случае скрытых отказов равна $K_{FMC,MPF}$, и
- интенсивность отказов скрытого множественного сбоя равна λ_{MPF}.

Таблица А.5 — Пример количественного анализа (на уровне подчастей)

Часть	Подчасть	Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Постоянные отказы						Кратковременные отказы					
				Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
Блок регистров	Регистр R0	СБ	Постоянный сбой	0,0029	0 %	SM1	40%	0,00174	SM1	100%	0,00000	0,032005	0 %	SM1	40 %	0,01920
			Кратковременный сбой													
	Регистр R1	СБ	Постоянный сбой	0,0029	0 %	SM1	40 %	0,00174	SM1	100%	0,00000	0,032005	0 %	SM1	40 %	0,01920
			Кратковременный сбой													
Центральный процессор	Регистр R2	СБ	Постоянный сбой	0,0029	0 %	SM1	20 %	0,00232	SM1	100%	0,00000	0,032005	0 %	SM1	10 %	0,02880
			Кратковременный сбой													
	Регистр R3	СБ	Постоянный сбой	0,0029	0 %	SM1	20 %	0,00232	SM1	100%	0,00000	0,032005	0 %	SM1	10 %	0,02880
			Кратковременный сбой													
	АЛУ	СБ	Постоянный сбой	0,0384	0 %	SM1	20 %	0,02784	SM1	100%	0,00000	0,032005	0 %	SM1	10 %	0,02880
			Кратковременный сбой													
	Блок умножения	СБ	Постоянный сбой	0,0290	0 %	SM1	20 %	0,02320	SM1	100%	0,00000	0,00038	20 %	SM1	10 %	0,00027
			Кратковременный сбой									0,00037	70 %	SM1	10 %	0,00010

Продолжение таблицы А.5

Часть	Подчасть		Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Постоянные отказы								Кратковременные отказы				
					Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
Центральный процессор	АЛУ	Блок деления	СБ	Постоянный сбой	0,0232	0 %	SM1	20 %	0,01856	SM1	100 %	0,00000					
				Кратковременный сбой									0,00036	70 %	SM1	10 %	0,00010
	Управляющая логика	Блок конвеерной обработки	СБ	Постоянный сбой	0,0174	0 %	SM1	90 %	0,00174	SM1	100 %	0,00000					
				Кратковременный сбой									0,00103	20 %	SM1	90 %	0,00008
		Секвенсер	СБ	Постоянный сбой	0,0406	0 %	SM1	90 %	0,00406	SM1	100 %	0,00000					
				Кратковременный сбой									0,00307	50 %	SM1	90 %	0,00015
		Управление стеком	СБ	Постоянный сбой	0,0029	0 %	SM1	70 %	0,00087	SM1	100 %	0,00000					
				Кратковременный сбой									0,000325	50 %	SM1	40 %	0,00010
	Блок хранения загрузки	Генератор адреса	СБ	Постоянный сбой	0,0174	0 %	SM1	60 %	0,00696	SM1	100 %	0,00000					
				Кратковременный сбой									0,00103	10 %	SM1	60 %	0,00037
		Блок загрузки	СБ	Постоянный сбой	0,0145	0 %	SM1	50 %	0,00725	SM1	100 %	0,00000					
				Кратковременный сбой									0,000345	10 %	SM1	50 %	0,00016
		Блок хранения	СБ	Постоянный сбой	0,0145	0 %	SM1	50 %	0,00725	SM1	100 %	0,00000					
				Кратковременный сбой									0,000345	10 %	SM1	50 %	0,00016

Продолжение таблицы А.5

Часть	Подчасть		Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Постоянные отказы: Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Кратковременные отказы: Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
Центральный процессор	Блок отладки	Внутренняя логика отладки	СБ	Постоянный сбой	0,0058	20%	Нет	0%	0,00464	Нет							
				Кратковременный сбой									0,00017	20 %	Нет	0 %	0,00014
		Интерфейс отладки	НСБ	Постоянный сбой	0,0783												
				Кратковременный сбой									0,001635				
				Σ					0,11049			0,00000					0,00014

Общая интенсивность отказов — 0,29000.
Общая интенсивность связанных с безопасностью отказов — 0,21170.
Общая интенсивность не связанных с безопасностью отказов — 0,0783.

Метрика одиночных сбоев — 47,8%. Метрика скрытых сбоев — 100,0%.

Общая интенсивность отказов — 0,13708.
Общая интенсивность связанных с безопасностью отказов — 0,13545.
Общая интенсивность не связанных с безопасностью отказов — 0,00164.

Метрика одиночных сбоев — 27,91%.

Продолжение таблицы А.5

Часть	Подчасть		Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Постоянные отказы								Кратковременные отказы				
					Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
Память с произвольным доступом	ОЗУ (16 КБ)	Биты данных ОЗУ	СБ	Постоянный сбой	1,5000	0 %	SM3	96,9 %	0,04688	SM3	100 %	0,00000					
				Кратковременный сбой									131,072	0 %	SM3	40 %	0,40894
		Дешифратор адреса	СБ	Постоянный сбой	0,0087	0 %	Нет	0 %	0,00870								
				Кратковременный сбой									0,000335	0 %	Нет	40 %	0,00034
		Тестирование/ избыточность	СБ	Постоянный сбой	0,0058	50 %	Нет	0 %	0,00290								
				Кратковременный сбой									0,00033	90 %	Нет	10 %	0,00003
					Σ				0,05848			0,00000					0,40931

Общая интенсивность отказов — 1,51450
Общая интенсивность связанных с безопасностью отказов — 1,51450
Общая интенсивность не связанных с безопасностью отказов — 0,00000

Общая интенсивность отказов — 131,07
Общая интенсивность связанных с безопасностью отказов — 131,07
Общая интенсивность не связанных с безопасностью отказов — 0,00

Метрика одиночных сбоев — 96,1%. Метрика скрытых сбоев — 100,0%.

Метрика одиночных сбоев — 99,69%.

Продолжение таблицы А.5

					Постоянные отказы								Кратковременные отказы				
Часть	Подчасть		Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
Механизм безопасности	SM1	Логика обнаружения	СБ	Постоянный сбой	0,0029	0 %			0,00174	SM2	90 %	0,00029					
				Кратковременный сбой									0,000105				
		Генератор аварийных сигналов	СБ	Постоянный сбой	0,0029	50 %			0,00174	SM2	90 %	0,00015					
				Кратковременный сбой									0,000055				
	SM3	Блок кодирования EDC	СБ	Постоянный сбой	0,0029	0 %	SM3	90 %	0,0029	SM4	90 %	0,00026					
				Кратковременный сбой									0,000325	0 %	Нет	0 %	0,00033
		Блок декодирования EDC	СБ	Постоянный сбой	0,0029	0 %	SM3	90 %	0,0029	SM4	90 %	0,00026					
				Кратковременный сбой									0,000325	0 %	Нет	0 %	0,00033
		Генератор аварийных сигналов	СБ	Постоянный сбой	0,0029	50 %				SM4	90 %	0,00015					
				Кратковременный сбой													
		Биты EDC в ОЗУ	СБ	Постоянный сбой	0,328125	0 %	SM3	96,9 %	0,01025	SM4	90 %	0,03179					
				Кратковременный сбой									28,6720	0 %	SM3	99,69 %	0,02880
								Σ	0,00058			0,00058					0,09011

Окончание таблицы А.5

Общая интенсивность отказов	— 0,34263.	Общая интенсивность отказов	— 26,67281.
Общая интенсивность связанных с безопасностью отказов	— 1, 34263.	Общая интенсивность связанных с безопасностью отказов	— 26,67281.
Общая интенсивность не связанных с безопасностью отказов	— 0,00000.	Общая интенсивность не связанных с безопасностью отказов	— 0,00000.

Метрика одиночных сбоев — 99,8 %. Метрика скрытых сбоев — 90,4 %. Метрика одиночных сбоев — 99,69 %.

Примечания

1 Количество безопасных сбоев — это доля вида отказов, которые не нарушают цель безопасности ни в отсутствие механизмов безопасности, ни в комбинации с независимым отказом другой подчасти.

2 Охват вида отказов вычисляется с помощью детального анализа возможностей SM1, чтобы охватить каждую подчасть. В данном примере регистры R0 и R1 выбраны компилятором для передачи параметров функции, поэтому они имеют более высокую вероятность вызвать нарушение последовательности программ, обнаруживаемое SM1. Цель данного примера состоит в обеспечении доказательств того, что с помощью детального анализа можно определить различия в охвате подчастей.

3 Охват вида отказов в EDC (SM3) вычисляется, например, с подробным анализом сочетания высокой вероятности EDC обнаружения однобитовых и двухбитовых ошибок с более низкой вероятностью обнаружения (может быть менее 90%) многобитовых ошибок. Это показано в Таблице А.6.

4 Некоторые подчасти могут быть охвачены несколькими механизмами безопасности. В таких случаях результирующий охват вида отказов объединяет охват для каждого вида отказов, определенного в результате детального анализа.

5 Данный пример показывает, что без надлежащего охвата в EDC многобитовых ошибок и без охвата дешифратора адреса памяти достаточно трудно достичь высокого значения метрики одиночного сбоя.

6 Данный пример показывает, что некоторые механизмы безопасности могут привести к непосредственному нарушению цели безопасности, и поэтому они учитываются при расчете остаточных сбоев. В данном примере сбой в EDC (SM3) может повредить данные о ходе выполнения программы без соответствующего сбоя в памяти.

7 Данный пример показывает, что в микроконтроллере могут совместно существовать подчасти, которые, возможно, не связаны с безопасностью, но которые невозможно четко отделить или отличить от связанных с безопасностью подчастей (блок отладки внутренней логики). При этом другие части (отладочный интерфейс) могут быть легко отделены и заблокированы таким образом, что их можно без риска рассматривать как не связанные с безопасностью.

Таблица А.6 — Пример количественного анализа (для низкоуровневых отказов)

					Постоянные отказы								Кратковременные отказы				
Часть	Подчасть	Элементарные подчасти	Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
ЦП	АЛУ	АЛУ	СБ	Постоянный сбой в триггере *X*1 и его схеме объединения по входу	0,01009	0%	SM1	40 %	0,00174	SM1	100%	0,00000					
				Одиночный сбой и одиночный кратковременный сбой в триггере *X*1 и его схеме объединения по входу									0,032005	0%	SM1	40%	0,01920
				Постоянный сбой в триггере *X*2 и его схеме объединения по входу	0,0150	0%	SM1	40 %	0,00174	SM1	100%	0,00000					
				Одиночный сбой и одиночный кратковременный сбой в триггере *X*2 и его схеме объединения по входу									0,032005	0%	SM1	40%	0,01920
				и т. д.	…	…	…	…	…	…	…	…	…	…	…	…	…
				Σ	0,0348				0,02784			0,00000	0,00038				0,00027
ОЗУ	ЗУ (16 КБ)	Биты данных ОЗУ	СБ	Постоянный сбой, вызывающий не более двух битовых ошибок в одном кодируемом слове	1,3500	0%	SM3	100 %	0,00000	SM1	100%	0,00000					
				Не более двух одиночных сбоев в одном кодируемом слове									129,76128	0%	SM3	100%	0,00000
				Постоянный сбой, вызывающий более двух битовых ошибок в одном кодируемом слове	0,1500	0%	SM3	68,8 %	0,04688	SM1	100%	0,00000					

Окончание таблицы А.6

Часть				Постоянные отказы					Кратковременные отказы				
ОЗУ	Подчасть	Элементарные подчасти	Компонент связан с безопасностью? Компонент не связан с безопасностью?	Вид отказов	Интенсивность отказов (FIT)	Величина безопасных сбоев (см. примечание 1)	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)	Механизм(ы) безопасности, предотвращающий скрытые сбои	Охват вида отказа относительно скрытых отказов	Интенсивность отказов от скрытых множественных сбоев (FIT)	Интенсивность отказов (FIT)	Величина безопасных сбоев	Механизм(ы) безопасности, предотвращающий нарушение цели безопасности	Охват вида отказа относительно нарушения цели безопасности	Интенсивность отказов от остаточных и одиночных сбоев (FIT)
ЗУ (16 КБ)	Биты данных ОЗУ	СБ	Более двух одиночных сбоев в одном кодируемом слове	Σ	1,5000				0,04688			0,00000	131,0720	0%	SM3	68,8%	0,40894

Примечания

1 На этом уровне детализации можно выяснить, что некоторые отказы на низком уровне (например, одиночный сбой и одиночный кратковременный сбой в триггере *X2* и его схеме объединения по входу) являются безопасными (например, потому, что этот бит редко используется архитектурой АЛУ).

2 Интенсивность отказов памяти от одиночного постоянного сбоя, вызывающего $n > 2$ битовых ошибок, например, вычисляется с учетом информации о топологии памяти, структуры дешифратора адреса и т.д.

3 Охват ошибок EDC (SM3) в трех и более битах вычисляется, если выполнен детальный анализ, рассматривающий количество битов в каждом кодируемом слове (в данном случае 32) и количество битов кода (в данном случае 7). В зависимости от этих параметров, охват может быть гораздо выше.

А.3.6 Пример анализа зависимых отказов

Общие требования и рекомендации, связанные с идентификацией, оценкой и учетом зависимых отказов, соответственно, определены в ИСО 26262-9.

Анализ зависимых отказов структурирован на следующие этапы:

1) определить части, на которые могут повлиять зависимые отказы.

Примечания

1 Структуры частей, о которых в концепции обеспечения безопасности микроконтроллера утверждается, что они независимы друг от друга, могут быть чувствительны к зависимому отказу.

2 Это определение может быть поддержано дедуктивным анализом безопасности. События считаются независимыми, если анализ двойных и множественных отказов дает полезную информацию о частях уязвимых для зависимых отказов;

2) определить источники возможных зависимых отказов.

Рассматриваются источники, перечисленные в данном приложении, а также другие предсказуемые физические и логические источники зависимых отказов (общеиспользуемые логические части и сигналы), в том числе результаты, связанные с сосуществованием функций с различными УПБА;

3) определить механизм связи между частями, позволяющий возникновение зависимых отказов;

4) качественно описать и оценить меры по предотвращению зависимых отказов;

5) качественно описать и оценить меры, используемые в процессе проектирования, по ограничению влияния, вызванного оставшимися зависимыми отказами, на каждую структуру частей, которые определены в перечислении 1).

Примечание — Как указано в примечании к 7.4.2 ИСО 26262-9, анализ зависимых отказов выполняется качественно, потому что не существует никакого общего и достаточно надежного метода для количественного анализа таких отказов.

Как указано в примечании 1 к 7.4.4 ИСО 26262-9, оценка зависимых отказов может быть выполнена применением соответствующих таблиц контрольных проверок, например с помощью таблиц контрольных проверок, полученных из практического опыта. Таблицы контрольных проверок обеспечивают аналитикам характерные примеры первопричин и факторов связи зависимых отказов, такие как: тот же самый проект, тот же процесс, такой же компонент, тот же интерфейс и уровень близости.

В таблице А.7 перечислены области (см. 7.4.4 ИСО 26262-9), для которых выполняется оценка зависимых отказов. В данной таблице также даны краткие примеры источников и механизмов связи, которые могли бы привести к зависимым отказам, с примерами мер их предотвращения или обнаружения.

Примечание — Перечисленные меры являются лишь некоторыми из возможных вариантов. Возможны другие меры по предотвращению или обнаружению зависимых отказов, например, механизмы безопасности на уровне системы.

Таблица А.7 — Области оценки зависимых отказов, их возможные источники и связанные с ними меры

Области 7.4.4 ИСО 26262-9	Примеры возможных источников и механизмов связи	Примеры мер
Случайные отказы аппаратных средств	Физические дефекты могут влиять как на часть, так на ее механизм безопасности таким образом, что может произойти нарушение цели безопасности	Можно устранить с помощью таких мер, как физическое разделение, разнообразие, производственные испытания и т.д.
Ошибки разработки	Ошибки разработки могут быть причиной зависимого отказа, например, перекрестные помехи, неправильная реализация функциональности, ошибки спецификации, неправильная конфигурация микроконтроллера и т.д. (см. также А.3.7)	Можно устранить с помощью таких мер, как определение процесса разработки, разнообразие, правила проектирования, механизмы защиты конфигурации и т.д.
Сбои производства	Сбои производства могут быть причиной зависимого отказа, например, сбои, связанные с несоосностью фотошаблонов	Можно устранить с помощью тщательного тестирования производства микроконтроллеров
Ошибки монтажа	Ошибки монтажа могут быть причиной зависимого отказа, например, при установке микроконтроллера на печатной плате, помехи соседних частей и т.д.	Можно устранить с помощью заводского испытания печатной платы, руководства по монтажу и т.д.

Окончание таблицы А.7

Области 7.4.4 ИСО 26262-9	Примеры возможных источников и механизмов связи	Примеры мер
Ошибки ремонта	Ошибки ремонта могут быть причиной зависимого отказа, например, сбои в столбце / строке памяти, хранящей информацию о запасных частях	Можно устранить с помощью заводских испытаний, руководства по ремонту и т. д.
Факторы окружающей среды	Типичные факторы окружающей среды: температура, электромагнитные помехи, влажность, механические нагрузки и т.д.	Можно устранить с помощью квалификационных испытаний, стресс-тестов, специальных датчиков, разнообразия и т. д.
Отказы общих внутренних и внешних ресурсов	Для микроконтроллеров типичными общими ресурсами являются устройства синхронизации, установки в исходное состояние и питания, включая устройства распределения питания	Можно устранить с помощью круглосуточного наблюдения, внутреннего или внешнего контроля питания, распределения разнообразия и т. д.
Воздействие вследствие конкретных ситуаций, например износ, старение	Механизмы старения и износа, например, электромиграция и т.д.	Можно устранить с помощью правил проектирования, квалификационных испытаний, разнообразия пусконаладочных испытаний и т.д.

В настоящий пункт не включены логические отказы общих ресурсов с возможностями воздействия на поведение нескольких частей или механизмов безопасности в микроконтроллере. Они рассматриваются в процессе стандартного качественного и количественного анализа.

Пример — Типичными примерами, попадающими в эту категорию, являются контроллер прямого доступа к памяти, контроллер прерываний и логика тестирования/отладки.

А.3.7 Пример методов или мер для обнаружения или предотвращения систематических отказов в процессе проектирования микроконтроллера

Общие требования и рекомендации, связанные с архитектурой аппаратных средств и детальным проектированием, определены в 7.4.1 ИСО 26262-5 и 7.4.2 ИСО 26262-5, соответственно. Кроме того требования, связанные с верификацией аппаратных средств, приведены в 7.4.4 ИО 26262-5.

Микроконтроллер разработан на основе стандартизированного процесса разработки. Примерами обеспечения доказательства того, что для предотвращения систематических отказов во время разработки микроконтроллера принимаются достаточные меры, являются следующие два подхода:

a) использование таблицы контрольных проверок, такой как представлена в таблице А.8, а также

b) предоставление обоснования, с использованием результатов полевых данных для аналогичных изделий, разработанных на основе того же процесса, как и целевое устройство.

Т а б л и ц а А.8 — Пример методов или мер для обеспечения соответствия требованиям ИСО 26262-5 в процессе разработки микроконтроллера

Требования ИСО 26262-5	Стадия проектирования	Метод / мера	Цель
7.4.1.6 Свойства модульного проектирования	Начало проектирования	Структурированное описание и формирование модулей	Описание функциональности схемы структурировано таким образом, что оно легко читается, то есть функциональную схему можно интуитивно понять на основе описания без дополнительных усилий
7.4.1.6 Свойства модульного проектирования		Описание проекта на HDL	Описание функций на высокоуровневом языке описания аппаратных средств, например VHDL или Verilog
7.4.4 Верификация проекта аппаратных средств		Моделирование на HDL	Функциональная верификация схемы, описанной на VHDL или Verilog, моделированием
7.4.4 Верификация проекта аппаратных средств		Функциональное тестирование на уровне модулей (используя, например, HDL для испытательных стендов)	Функциональная верификация «снизу — вверх»

Продолжение таблицы А.8

Требования ИСО 26262-5	Стадия проектирования	Метод / мера	Цель
7.4.4 Верификация проекта аппаратных средств	Начало проектирования	Высокоуровневое функциональное тестирование	Верификация микроконтроллера (всей схемы)
7.4.2.4 Надежные принципы проектирования		Ограниченное использование асинхронных конструкций	Предотвращение типичных проблем синхронизации в процессе синтеза, предотвращение неоднозначности в процессе моделирования и синтеза, связанных с трудностями создаваемой модели, проектирование тестируемости. Это не исключает, что для некоторых типов схем, таких как логика сброса или для очень маломощных микроконтроллеров, может быть полезна асинхронная логика: в этом случае, целью является предложить дополнительную осторожность при обращении и проверке этих схем
7.4.2.4 Надежные принципы проектирования		Синхронизация основных входов и управление метастабильностью	Предотвращение неоднозначного поведения схемы в результате нарушения времен установки и промежуточного хранения
7.4.4 Верификация проекта аппаратных средств		Функциональная и структурная управляемая охватом верификация (с охватом целей верификации в процентах)	Количественная оценка примененных сценариев верификации в процессе функционального тестирования. Целевой уровень охвата определен и показан
7.4.2.4 Надежные принципы проектирования	Начало проектирования	Соблюдение руководств по кодированию	Строгое соблюдение стиля кодирования приводит к синтаксически и семантически корректному коду схемы
7.4.4 Верификация проекта аппаратных средств		Применение средств проверки кода	Автоматическая верификация правил кодирования («Стиль кодирования») инструментальными средствами проверки кода
7.4.4 Верификация проекта аппаратных средств		Документальное оформление результатов моделирования	Документальное оформление всех данных, необходимых для успешного моделирования, чтобы проверить указанную функцию схемы
7.4.4 Верификация проекта аппаратных средств	Синтез	Моделирование логической схемы на основе списка соединений для проверки ограничений синхронизации или статический анализ задержки распространения сигнала (STA)	Независимая проверка достигаемого ограничения синхронизации во время синтеза
7.4.4 Верификация проекта аппаратных средств		Сравнение списка соединений логических элементов с эталонной моделью (формальный тест на эквивалентность)	Проверка функциональной эквивалентности синтезируемого списка соединений логических элементов
7.4.1.6 Свойства модульного проектирования		Документальное оформление ограничений, результатов и средств синтеза	Документальное оформление всех сформированных ограничений, которые необходимы для оптимального синтеза при генерации окончательного списка соединений логических элементов

Продолжение таблицы А.8

Требования ИСО 26262-5	Стадия проектирования	Метод / мера	Цель
7.4.1.6 Свойства модульного проектирования	Синтез	Процедуры, основанные на сценарии	Воспроизводимость результатов и автоматизация циклов синтеза
7.4.2.4 Надежные принципы проектирования		Достаточный запас времени для технологических процессов, которые применяются менее трех лет	Обеспечение устойчивости реализуемой функциональности схемы даже при серьезной флуктуации процесса и параметров
7.4.1.6 Свойства модульного проектирования (тестируемость)	Включение теста и генерация тестового примера	Тестопригодное проектирование (в зависимости от охвата тестом, в %)	Избежать не тестируемые или плохо тестируемые структуры, чтобы достигнуть высокий тестовый охват для заводских испытаний или тестирования в режиме он-лайн
7.4.1.6 Свойства модульного проектирования (тестируемость)		Доказательство тестового охвата применением средств автоматической генерации тестового примера (ATPG), на основе достигаемого тестового охвата, в %	Определение ожидаемого тестового охвата для синтезируемых тестовых примеров («Сканирование пути», BIST) в процессе испытаний проекта. Целевой уровень охвата и модели отказа определены и представлены
7.4.4 Верификация проекта аппаратных средств	Включение теста и генерация тестового примера	Моделирование логической схемы на основе списка соединений при запущенном тесте для проверки ограничений синхронизации или статический анализ задержки распространения сигнала (STA)	Независимая проверка достигаемого ограничения синхронизации во время выполнения теста
7.4.4 Верификация проекта аппаратных средств		Сравнение логической схемы на основе списка соединений логических элементов при запущенном тесте с эталонной моделью (формальный тест на эквивалентность)	Проверка функциональной эквивалентности списка соединений логических элементов при запущенном тесте
7.4.4 Верификация проекта аппаратных средств	Размещение, трассировка, генерация топологии	Моделирование логической схемы на основе списка соединений логических элементов после трассировки для проверки ограничений синхронизации или статический анализ задержки распространения сигнала (STA)	Независимая проверка достигаемого ограничения синхронизации во время завершения трассировки
7.4.4 Верификация проекта аппаратных средств		Анализ сети питания	Демонстрация устойчивости сети питания и эффективности механизмов, связанных с безопасностью. Например испытание при падении внутреннего сопротивления.

Окончание таблицы А.8

Требования ИСО 26262-5	Стадия проектирования	Метод / мера	Цель
7.4.4 Верификация проекта аппаратных средств	Размещение, трассировка, генерация топологии	Сравнение логической схемы на основе списка соединений логических элементов после трассировки с эталонной моделью (формальный тест на эквивалентность)	Проверка функциональной эквивалентности списка соединений логических элементов после завершения трассировки
7.4.4 Верификация проекта аппаратных средств		Проверка правил проектирования DRC	Проверка правил процесса проектирования
7.4.4 Верификация проекта аппаратных средств		Проверка соответствия топологии схеме (LVS)	Независимая проверка трассировки
7.4.5 Производство, эксплуатация, обслуживание и вывод из эксплуатации 9.4.2.4 Специальные меры	Связанные с безопасностью специальные характеристики процесса производства микросхем	Определение достижимого тестового охвата заводского испытания	Оценка тестового охвата во время заводских испытаний связанных с безопасностью характеристик микроконтроллера.
7.4.5 Производство, эксплуатация, обслуживание и вывод из эксплуатации 9.4.2.4 Специальные меры		Определение мер обнаружения и удаления ранних отказов	Обеспечение надежности выпускаемых чипов. В большинстве, но не в каждом процессе, целостность оксидного слоя затвора (GOI) является ключевым механизмом раннего отказа. Для отбраковки ранних отказов из-за GOI имеется много обоснованных методов: стабилизация изделия тренировкой при высокой температуре / высоком напряжении (Burn-In), эксплуатация при больших токах, большие напряжения и т.д. Однако эти методы бесполезны, если GOI в процессе не вносит основной вклад в ранние отказы.
7.4.5 Производство, эксплуатация, обслуживание и вывод из эксплуатации 10 Интеграция и тестирование аппаратных средств	Квалификация компонента аппаратных средств	Определение и выполнение квалификационных испытаний, таких как тестирование при снижении напряжения, тестирование срока службы в условиях высокотемпературного нагрева (HTOL), а также функциональные контрольные примеры	Для микроконтроллера со встроенным средством выявления снижения напряжения тестируется его функциональность, чтобы проверить, что выходы микроконтроллера устанавливаются в определенное состояние (например, в исходное состояние при остановке работы микроконтроллера) или что о снижении напряжения сообщается другим способом (например, путем увеличения сигнала безопасного состояния), когда любое из питающих напряжений, контролируемое средством выявления снижения напряжения, достигает нижней границы, определенной для правильной работы. Для микроконтроллера без встроенного средства выявления снижения напряжения тестируется его функциональность, чтобы убедиться, устанавливает ли микроконтроллер свои выходы в определенное состояние (например, в исходное состояние при остановке работы микроконтроллера), когда напряжение питания падает от номинального значения до нуля. В противном случае определяется предположение использования и рассматриваются внешние меры

Более того, можно рассмотреть следующие общие руководящие принципы:

c) документальное оформление каждой проектной деятельности, комплектов испытаний и инструментов, используемых для функционального моделирования и результатов этого моделирования;

d) верификация каждой деятельности и ее результатов, например, моделированием, проверкой эквивалентности, временным анализом или проверкой технологических ограничений;

e) применение мер для воспроизводимости и автоматизации процесса реализации проекта (на основе сценария, автоматизации работы и последовательности действий при реализации проекта).

Примечание — Это подразумевает возможность зафиксировать версии инструментальных средств, чтобы в будущем обеспечить воспроизводимость в соответствии с принятыми требованиями.

f) использование (мягких и жестких ядер третьей стороны) проверенных макроблоков с соблюдением каждого ограничения и поведения, определенных поставщиком макроядер, если это практически возможно.

А.3.8 Верификация проекта аппаратных средств микроконтроллера

А.3.8.1 Общие положения

Согласно 7.4.4.1 ИСО 26262-5, проект аппаратных средств верифицируется в соответствии с указаниями раздела 9 ИСО 26262-8 (Оценка нарушения цели безопасности из-за случайных отказов аппаратных средств), на соответствие и полноту относительно требований безопасности к аппаратным средствам.

Внесение неисправностей является лишь одним из возможных способов верификации, возможны и другие подходы.

Пример — Если существуют современные решения, такие как протоколы высокого уровня для элементов коммуникации, то используется либо экспертная оценка, либо проверенные ранее результаты (например, программное обеспечение для шины обмена сообщениями автомобильных систем в соответствии с МЭК 61784).

Выбор и глубина верификации может зависеть от стадии анализа и от используемых механизмов безопасности (внутри микроконтроллера или на уровне системы).

Пример — Следуя причинам, упомянутым в примере 1 п. А.3.3, в случае избыточности аппаратных средств (например, использовать решение на базе двухядерного процессора, ядра которого работают в режиме жесткого параллелизма), в котором выходы из двух идентичных процессоров сравниваются аппаратными средствами на каждом тактовом цикле), проверку охвата вида отказов не нужно выполнять для каждого внутреннего регистра каждого процессора. Вместо этого может быть необходима более детальная проверка интерфейсов процессора и компаратора.

А.3.8.2 Верификация, использующая моделирование при внесении сбоя

Как уже упоминалось в таблице 3 ИСО 26262-5, моделирование с внесением сбоя во время стадии разработки является допустимым методом для верификации полноты и корректности реализации механизма безопасности относительно требований безопасности аппаратных средств.

В частности для микроконтроллеров, для которых использующее внесение сбоя тестирование нарушения в результате единичного события на уровне аппаратных средств нецелесообразно или даже невозможно для некоторых видов сбоев. Таким образом, для выполнения шага верификации внесение сбоя полезно при использовании расчетных моделей (например, при внесении сбоя на уровне списка соединений логических элементов).

Примечания

1 Метод внесения сбоя может быть использован как в случае постоянных (например, константных сбоев), так и кратковременных (например, нарушения в результате единичного события) сбоев.

2 Таблица D.1 ИСО 26262-5 показывает, что для некоторых элементов при отсутствии других подходящих доказательств необходимо учитывать виды сбоев при постоянном токе (отличные от константных «0» и «1»), чтобы иметь возможность претендовать на высокий уровень их диагностического охвата. Там также отмечено, что не предполагается требовать, чтобы анализ этих видов сбоев был исчерпывающим, так как известно, что реализованные должным образом методы, основанные на моделировании константных сбоев (например, тестирование с *N*-кратным обнаружением сбоя, см. [3]—[5]), также являются эффективным средством верификации видов сбоев при постоянном токе.

Примеры

1 Подходящим способом, упрощающим верификацию видов сбоев при постоянном токе, может быть предоставление доказательства того, что сбои типа «разрыв» или «короткое замыкание» составляют небольшую часть от всех видов сбоев при постоянном токе, то есть их значительно меньше, чем константных «0» или «1» сбоев.

2 Так как исчерпывающая полнота не требуется, то анализ видов сбоев при постоянном токе может быть применен к подмножеству подчастей микроконтроллера, выбираемых в зависимости от возможного влияния на них видов сбоев при постоянном токе (например, компараторы) или на основе статистики.

3 «Реализованное должным образом» тестирование с N-кратным обнаружением сбоя означает, что N различных обнаружений одного и того же сбоя гарантированы набором шаблонов (т.е. «насыщенностью» шаблона). Значение N может быть в диапазоне от 5 до 10.

4 В общем случае, механизмы безопасности аппаратных средств могут быть более эффективными при обнаружении каждого вида сбоя при постоянном токе и могут быть легче верифицированы с использованием, например, подхода с N-кратным обнаружением сбоя. С другой стороны, в случае механизма безопасности, основанного на программном обеспечении и работающего со случайными отказами аппаратных средств, может оказаться достаточно трудно с помощью подхода с N-кратным обнаружением сбоя получить высокий уровень уверенности в «насыщенности» шаблона из-за возможного изменения контекста между последующими выполнениями теста во время выполнения программы. В этом случае могут быть применены альтернативные решения (например, см. [7]).

Примечание — Метод внесения сбоя также может быть использован для введения сбоев типа замыкания в конкретные места на основе анализа топологии или для проверки влияния зависимых отказов, таких как внесение сбоев в схемы синхронизации и сброса.

Метод внесения сбоя в модели проекта может быть успешно использован при верификации безопасных сбоев и расчете их количества и охвата этого вида отказов, например, как показано в А.3.3 и А.3.3.2.

Пример — Если сбои вызывают измеримый эффект, то они вносятся и выявляются в точках наблюдения, в которых они хорошо определены. Кроме того, рассматриваемый метод может быть использован при вычислении и верификации значений охвата вида отказов, т.е. выполняется внесение сбоев, которые способны вызвать измеримый эффект, и их выявление, если эти сбои были обнаружены механизмами безопасности в интервале сбоеустойчивости.

Примечание — Доверие вычислению и верификации при внесении сбоя пропорционально качеству и полноте используемого для запуска тестируемой схемы испытательного стенда, количеству внесенных сбоев и уровню детализации представления схемы.

Пример — Описание логических элементов на уровне списка соединений подходит для внесения сбоя при анализе постоянных сбоев, таких как константные сбои. Для максимального увеличения скорости выполнения теста могут быть полезны методы FPGA. Также для константных сбоев приемлемым подходом является анализ на «уровне регистровых передач» при условии, что показана связь с уровнем логических схем.

А.3.9 Настройка и проверка автономного анализа микроконтроллера на уровне системы

Для настройки и верификации автономного анализа микроконтроллера на уровне системы необходимо:

a) подробно преобразовать описанные виды отказов микроконтроллера в описание видов отказов на высоком уровне, необходимое для анализа на уровне системы.

Примечания

1 Это может быть выполнено с помощью (восходящего) процесса «снизу — вверх» (показанного на рисунке А.2), используя метод, описанный в А.3.2, А.3.3 и А.3.5. Возможно идентифицировать подробные описания видов отказов микроконтроллера и объединить их до уровня компонентов.

2 Начальное подробное описание позволяет количественно и точно описать распределение отказов микроконтроллера, так как в противном случае используются качественные предположения для описания распределения.

3 Как описано в А.3.3, необходимая степень детализации может зависеть от стадии анализа и от используемых механизмов безопасности;

b) охват вида отказов, вычисляемый на уровне части или подчасти, может быть улучшен мерами на уровне применения.

Пример — На уровне автономного микроконтроллера охват вида отказов периферийных АЦП считается нулевым, потому что внутри микроконтроллера не реализуются механизмы безопасности для охвата этих сбоев. Тем не менее, на уровне применений АЦП включена в замкнутый контур и ее сбои обнаруживаются проверкой согласованности, реализованной программным обеспечением. В этом случае охват вида отказов этой подчасти может быть увеличен благодаря механизму безопасности на уровне применения;

c) охват вида отказов, вычисляемый на уровне подчасти, может быть рассчитан при некоторых конкретных предположениях («предположения применения»).

Примечание — В этом случае предположения проверяются на уровне применений, и если они оказываются не действующими, то могут быть сделаны другие предположения и охват вида отказов пересчитывается на основе новых предположений.

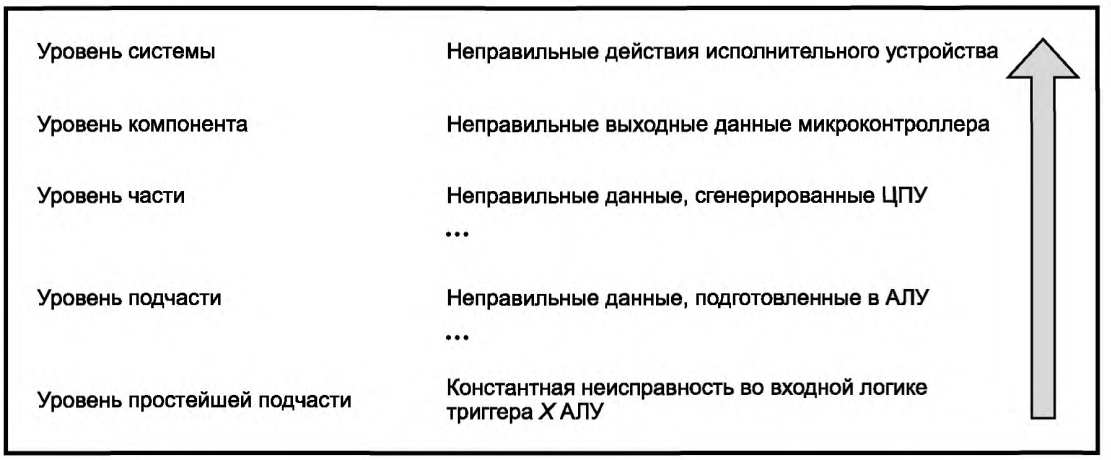


Рисунок А.2 — Пример восходящего подхода получения описания видов отказов на уровне системы

Пример — На уровне автономного микроконтроллера постоянный скрытый сбой памяти считается обнаруживаемым, потому что код с обнаружением ошибок (EDC) сообщает процессору о каждом исправлении одиночной ошибки. Предполагалось, что для обработки данного события должна быть реализована управляющая программа. Тем не менее, из соображений производительности эта управляющая программа реализована не была и, следовательно, предположение более не действует. Альтернативная мера заключается в программировании микроконтроллера так, чтобы он отправлял признак (флаг) о коррекции ошибки непосредственно во внешний мир. Охват скрытого сбоя памяти может быть пересчитан.

А.3.10 Пример документации по безопасности для микроконтроллера, как общеиспользуемого элемента безопасности (ОЭБ)

В пункте 9.2.3.6 указано, что для разработки микроконтроллера, как ОЭБ, системному интегратору предоставляется необходимая информация о результатах работы, которая включает следующие документы: предполагаемые требования, предположения, связанные с внешним по отношению к ОЭБ проектом, и применимые результаты работы.

Исходя из этого, документация по безопасности для микроконтроллера, как ОЭБ, может включать в себя следующие документы или подмножества из них, как указано в соглашении об интерфейсе разработки (DIA):

- обоснование безопасности, связанное с микроконтроллером, см. 6.5.3 ИСО 26262-2;
- план обеспечения безопасности для микроконтроллера, см. 6.5.1 ИСО 26262-2 и 5.5 ИСО 26262-5;
- другие планы, как показано в ИСО 26262-8, в соответствующих случаях, такие как план управления конфигурацией, план управления изменениями, план анализа влияния и запроса на изменение, план верификации, план управления документацией и план квалификации программных инструментальных средств;
- доказательства, связанные с выполнением применимых шагов плана обеспечения безопасности, как показано в ISO 26262-2;
- спецификации аппаратных средств, как показано в ИСО 26262-5, например, спецификация требований к безопасности аппаратных средств, спецификация программно-аппаратного интерфейса (HSI) и спецификация проекта аппаратных средств;
- отчеты, связанные с выполнением применимых шагов плана верификации и других планов, как указано в ИСО 26262-5 и ИСО 26262-8, например, отчет по верификации требований безопасности аппаратных средств, отчет по верификации проекта аппаратных средств и отчет по верификации и интеграции аппаратных средств;
- отчеты, связанные с анализом безопасности, как указано в ИСО 26262-5, ИСО 26262-8 и ИСО 26262-9, такие как отчет по анализу безопасности аппаратных средств, экспертный отчет об эффективности архитектуры микроконтроллера по обеспечению требований к случайным отказам аппаратных средств, экспертный отчет по оценке нарушения цели безопасности из-за случайных отказов аппаратных средств и результаты анализа зависимых отказов.

Примечание — В DIA указано, какие документы предоставляются и какой уровень детализации предоставляется клиенту микроконтроллера.

Кроме того, стоит собрать следующую информацию:

- описание жизненного цикла в соответствии с настоящим стандартом, подготовленное специально для микроконтроллера; список соответствующих результатов работы (описание тех результатов работы по жизненному циклу, соответствующему настоящему стандарту, которые применимы для микроконтроллера);
- описание безопасной архитектуры микроконтроллера с абстрактным описанием функциональных возможностей микроконтроллера и описанием механизмов безопасности;

- описание «предположений применения» (Assumptions of Use) микроконтроллера для его целевого использования, в том числе предположение о безопасном состоянии микроконтроллера, предположения об интервале сбоеустойчивости и интервале выявления множественных сбоев, предположения о контексте микроконтроллера, включая внешние интерфейсы;

- описание конфигурации микроконтроллера и связанные аппаратные и/или программные процедуры по управлению отказом после его обнаружения;

- описание результатов анализа безопасности на уровне микроконтроллера, которые полезны для системных интеграторов, такие как описание моделей сбоев, моделей отказов и интенсивностей отказов, учитываемых при анализе, метрики архитектуры аппаратных средств (метрики одиночного сбоя и скрытого сбоя), вероятностная метрика для случайных отказов аппаратных средств (PMHF), оценка каждой причины нарушения цели безопасности (см. 9.4.3 ИСО 26262-5), описание источников зависимых отказов, описание предполагаемых или принятых мер для предотвращения или обнаружения зависимых отказов, описание «предположений применения», на которых основан анализ безопасности (например, программные механизмы безопасности, устраняющие случайные отказы аппаратных средств и т.д.);

- описание процесса оценки функциональной безопасности; список мер подтверждения и описание уровня независимости; краткое описание процесса предотвращения систематических отказов в микроконтроллере.

Примечание — Данная документация может быть объединена в один документ под названием «Руководство по безопасности» или «Указания по применению безопасности» микроконтроллера, как общеиспользуемого элемента безопасности.

Приложение В
(справочное)

Формирование и применение дерева неисправностей

В.1 Общие положения

FTA и FMEA — два наиболее распространенных метода анализа сбоев и отказов устройства и элементов. FMEA является индуктивным («снизу—вверх», см. рисунок В.1) подходом, рассматривающим отказы отдельных частей системы и влияние этих отказов на всю систему. FTA является дедуктивным («сверху—вниз», см. рисунок В.2) подходом, начинающим анализ с нежелательного поведения системы и определяющим возможные причины такого поведения.

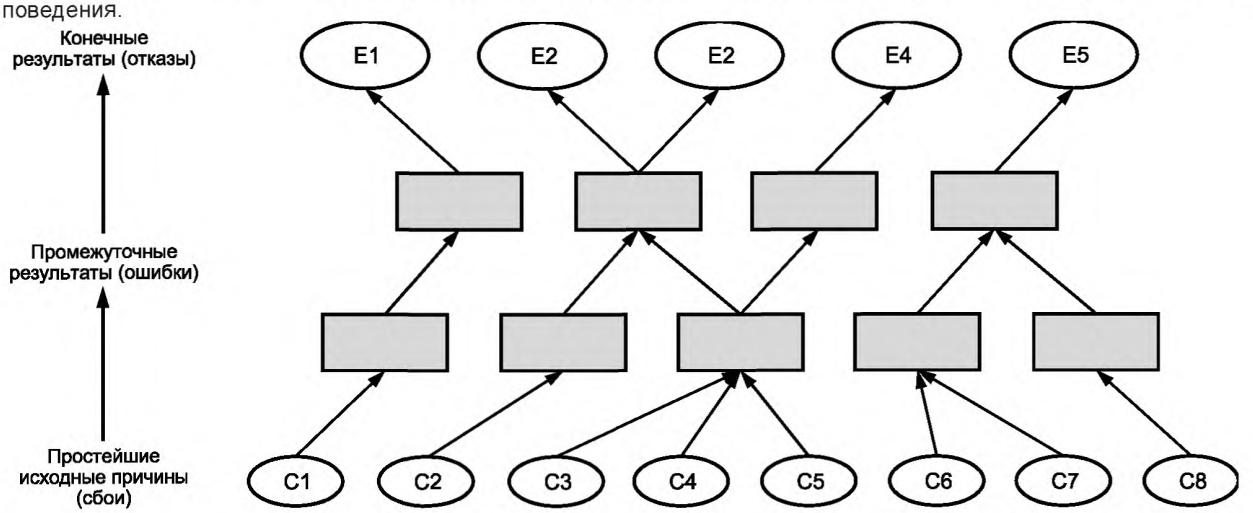


Рисунок В.1 — Иллюстрация метода FMEA («снизу — вверх»)

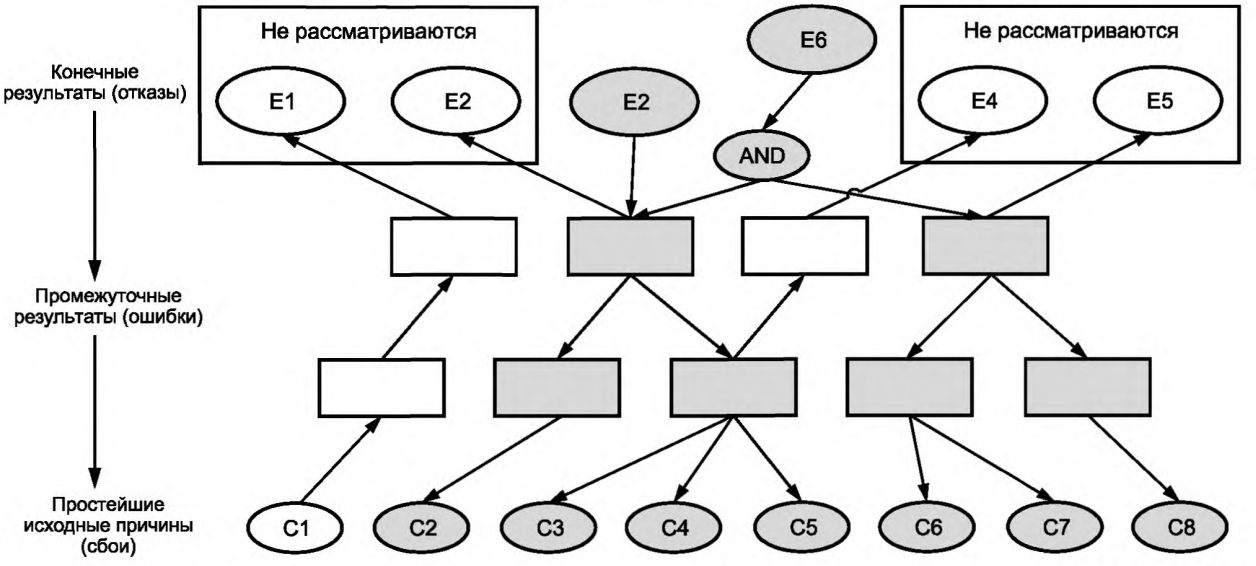


Рисунок В.2 — Иллюстрация метода FTA («сверху—вниз»)

Эти подходы дополняют друг друга, как указано в примечании таблицы 2 подпункта 7.4.3.1 ИСО 26262-5: «Уровень детализации анализа соизмерим с уровнем детализации проекта. Оба метода, в некоторых случаях, могут осуществляться на различных уровнях детализации». Овалы «Сх» на рисунках В.1 и В.2 представляют собой компоненты либо технических средств, либо программного обеспечения. Обычно для анализа опасностей вплоть до уровня компонентов используется FTA. Затем с помощью FMEA снизу вверх анализируются отказы компонентов, чтобы установить их виды и определить механизмы безопасности, для устранения неисправностей на нижнем уровне дерева неисправностей. Желательно избегать дублирования работы, которое возникает на пересечении между FTA моделированием и FMEA. Для серийно выпускаемых частей системы результаты FMEA в модели дерева отказов предпочтительно рассматривать как интенсивности отказов базовых событий.

Примечание — Как указано в 7.4.2.1 ИСО 26262-9, вклад зависимых отказов оценивается качественно, потому что не существует никакого общего и достаточно надежного метода для количественной оценки таких отказов. Таким образом, количественный метод, представленный в настоящем приложении, относится только к определяемым количественно зависимым отказам, таким, как показанный на рисунке B.9 вклад по общей причине от постоянного сбоя SM1 в сечениях дерева отказов как для кратковременного сбоя, так и постоянного сбоя регистра R0.

B.2 Объединение FTA и FMEA

Системы состоят из многих частей и подчастей. FTA и FMEA могут быть объединены для выполнения анализа безопасности с необходимым балансом подходов сверху вниз и снизу вверх. На рисунке B.3 показан возможный способ объединения FTA и FMEA. На данном рисунке базовые события получены из FMEA для различных отказов (обозначенных FMEA A–E в данном примере), который выполняется на более низком уровне абстракции (например, на уровне подчасти, части или компонента). В этом примере FMEA B не влияет на базовые события 1 и 2, а FMEA D влияет на оба.

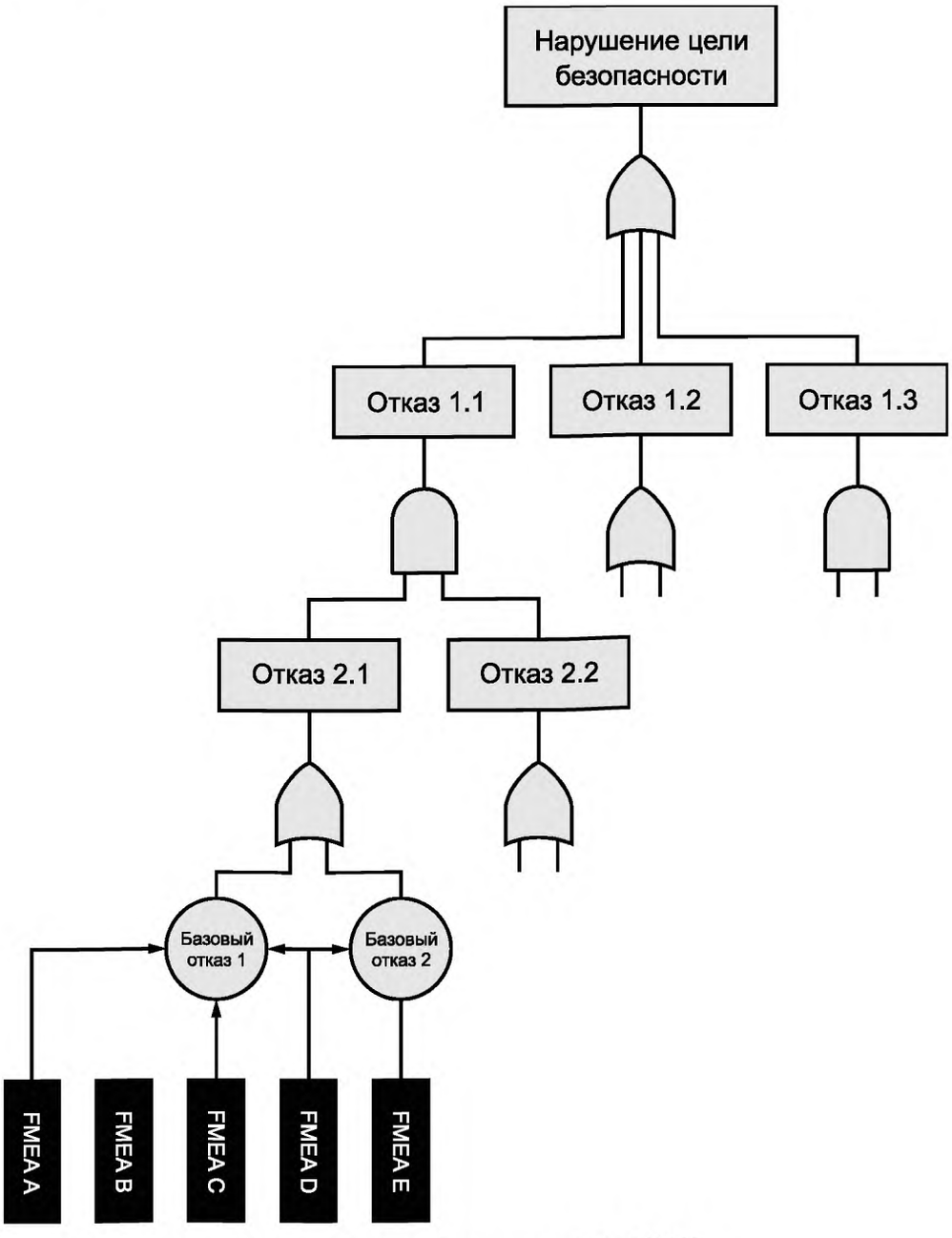


Рисунок B.3 — Объединение FTA и FMEA

B.3 Пример дерева неисправностей

B.3.1 Общие положения

Для микроконтроллера, описанного в примере приложения А, может быть построено дерево неисправностей. Данный пример не является примером интеграции FMEA и FTA, но демонстрирует построение дерева неисправностей.

Дерево неисправностей построено для каждой строки таблицы А.5, преобразуя ее в ветвь дерева. Полное дерево неисправностей представлено на рисунках В.6— В.21. Пример дерева неисправностей используется для иллюстрации двух методов оценки, является ли остаточный риск нарушений цели безопасности достаточно низким. Вероятность нарушения цели безопасности оценивается для каждой ветви дерева неисправностей. Поэтому вероятность нарушения цели безопасности на верхнем уровне не рассчитывается.

Дерево неисправностей не используется для определения диагностического охвата или метрик одиночного и скрытого сбоев. Если диагностический охват определяется, например с помощью FMEA, то его результаты могут быть использованы в дереве неисправностей, поэтому может быть рассчитана вероятность отказа системы в течение ее срока службы.

На рисунке В.4 представлены в общем виде примеры FTA для одиночного, остаточного и двойного сбоев.

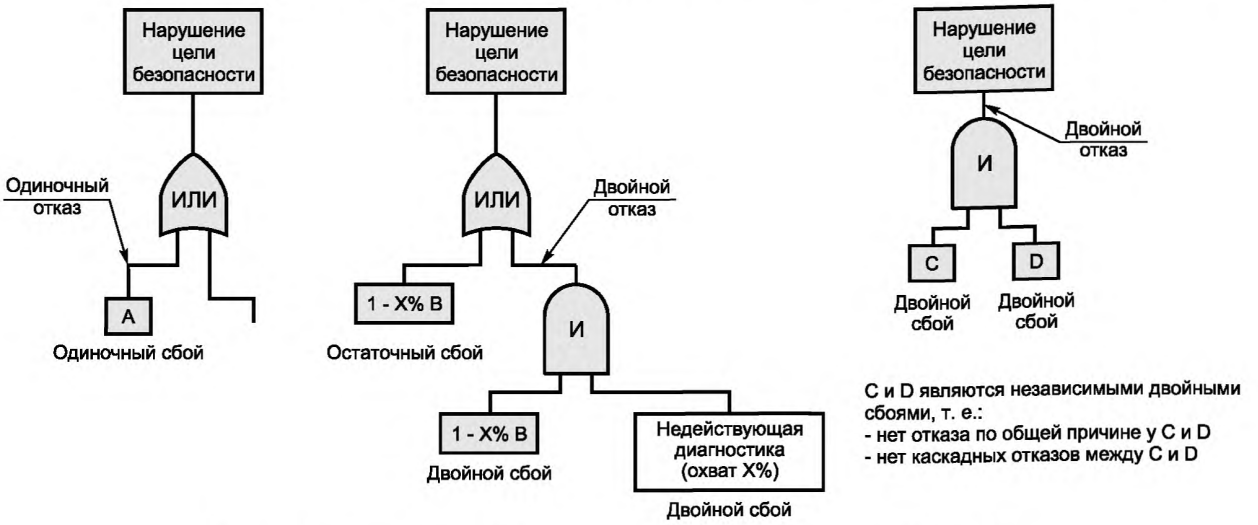


Рисунок В.4 — Примеры FTA для одиночного, остаточного и двойного сбоев

B.3.2 Пример создания ветви дерева неисправностей

В качестве примера подробно описано создание одной ветви — ветви дерева неисправностей для регистра R0. На рисунке В.9 показано, что первые две строки таблицы А.5 объединены оператором ИЛИ. Это предполагает, что постоянные и кратковременные отказы регистра R0 являются независимыми видами отказов. Поскольку интенсивности кратковременных отказов и диагностический охват известны, то кратковременные сбои включены в дерево неисправностей таким же образом, как постоянные сбои. Если интенсивности отказов и диагностический охват не известны, то кратковременные сбои могут быть обработаны отдельно, как описано в примечании 2 к 8.4.7 ИСО 26262-5.

Примечание — В рассматриваемом примере показан способ объединения постоянных и кратковременных сбоев. Согласно примечанию 2 к 8.4.7 ИСО 26262-5 если показано, что кратковременные сбои актуальны, то они включаются в анализ. Так как для данного примера кратковременные сбои актуальны и оцениваются количественно, то они включены в дерево неисправностей аналогичным образом, как и постоянные сбои.

Сначала рассматривается построение ветви для кратковременных сбоев, которая состоит из события, представляющего кратковременные сбои с интенсивностью отказов, равной 0,032005 FIT ($3{,}2005\times10^{-11}$ / ч работы), соединенного со входом оператора И. Второй вход этого оператора И связан с выходом оператора ИЛИ, на входе которого два события: связанное с охватом отказов данного вида с фиксированной вероятностью 60 % (1 — охват вида отказов, связанных с нарушением цели безопасности), и связанное с вероятностью отказа механизма безопасности SM1 от скрытых сбоев. Символ r под блоком события представляет значение интенсивности отказов в час, а символ Q представляет значение вероятности отказа данного блока или ветви в течение ожидаемого срока службы системы.

Примечание — Событие с фиксированной вероятностью доминирует над событием, описываемым ветвью, представляющей диагностический охват и скрытые отказы механизма безопасности SM1. На практике значением диагностического охвата вместе с интенсивностью скрытых отказов механизма безопасности SM1 (выход оператора 19 на рисунке В.9) можно пренебречь, упрощая дерево. Тем не менее, метрика скрытых сбоев оценивается и проверяется на соответствие.

Скрытый сбой может привести к неспособности системы обнаружить кратковременный отказ, который включен в диагностический охват и обычно должен быть обнаружен. Необходимо отметить, что следует учитывать порядок следования комбинации скрытых/первичных сбоев. Если скрытый сбой механизма безопасности происходит до первичного сбоя, то первичный сбой не может быть обнаружен, и уменьшение опасных последствий не происходит. Это представлено небольшим блоком *L*, указывающим, что это событие должно произойти последним в последовательности с другим событием оператора И.

Блок SM1 построен в соответствии с представленным в таблице А.5 механизмом безопасности и реализует логику обнаружения и генерацию аварийных сигналов для постоянных сбоев. Кратковременные сбои не включаются, поскольку они не вызывают скрытые сбои, так как вероятность того, что они происходят одновременно с первичным сбоем очень низка и поэтому не учитывается. Это согласуется с примечанием 2 8.4.7 ИСО 26262-5, в котором кратковременные сбои учитываются только для метрики одиночных сбоев. Логика обнаружения имеет значение интенсивности отказов r = 0,0029 FIT.

Отказы логики обнаружения далее диагностируются механизмом безопасности SM2 с охватом диагностикой 90 %, соединенным оператором И с блоком SM1, который вычисляет вероятность скрытых сбоев SM1. Механизм безопасности SM2 выявляет скрытые сбои в SM1 и выполняется при каждом включении ключа зажигания. Согласно 9.4.2.3 ИСО 26262-5 среднюю продолжительность поездки автомобиля можно рассматривать равной до одного часа. Один час представлен записью *tau* = 1 под блоком события DL LATENT1, вероятность которого умножается на 0,9 (охват диагностикой скрытых сбоев SM2 равен 90%). Доля сбоев генерации аварийных сигналов, не охваченная SM2, представлена стандартным значением интенсивности отказов события ALARM LATENT, умноженным на 0,1 (10 % = 100 % — охват диагностикой скрытых сбоев SM2).

Ветвь, представляющая постоянные сбои строится аналогичным образом. Подчеркивание блока SM1 треугольной формы указывает на то, что это не просто копия существующего блока SM1 для ветви дерева для кратковременных сбоев, это тот же вид отказов. Это может быть полезно при анализе отказов по общей причине. Например, на рисунке В.9 операторы И блоков TRANS R0 и PERM R0 содержат общую ветвь.

Пример в таблице А.5 содержит безопасные сбои. При рассмотрении безопасных сбоев, уточняется интенсивность отказов для базовых событий. Например, для кратковременных сбоев АЛУ (строка 10 в таблице А.5, 20% безопасных сбоев) значение 0,00038 FIT умножается на 0,8 (100% — 20%), в результате имеем $3{,}8\times10^{-13}$ / ч × 0,8 = $=3{,}04\times10^{-13}$ / ч.

В.4 Вероятностный анализ с использованием дерева отказов

Типичными количественными характеристиками отказов компонентов являются интенсивности их отказов. Для сложного дерева отказов с несколькими операторами И и ИЛИ, отдельные интенсивности отказов не могут быть объединены в общую интенсивность отказов системы. Например, система, состоящая из двух блоков, которые соединены оператором И и имеют экспоненциальные распределения, для которых обе интенсивности отказов λ_1 и λ_2 очень малы (оба значения λt очень малы, где t представляет собой время службы системы), будет иметь приблизительную вероятность отказа равную $\lambda_1 t\lambda_2 t$ или $\lambda_1\lambda_2 t^2$.

Если значение ASIL системы равно D и целевые интенсивности отказов используются из таблицы 7 ИСО 26262-5, то вероятность целевых отказов в час составляет $< 10^{-8}$/ч, которая относится к другому временному периоду, чем $\lambda_1\lambda_2 t^2$. Одним из способов справиться с ситуацией является умножение целевой вероятности отказов в час 10^{-8}/ч на время службы системы 10^{-8}/ч t и убедиться, что $\lambda_1\lambda_2 t^2 \le 10^{-8}$/ч t или $\lambda_1\lambda_2 t \le 10^{-8}$/ч. Это требует данных о сроке службы системы, которые могут быть получены из прошлых профилей использования или системных требований. Дерево неисправностей в настоящем приложении было создано, полагая, что произвольно выбранное значение срока службы системы равно 5000 ч.

Для ветви R0 TRANSIENT вероятность не выявления отказа в первую очередь связана с недостаточным охватом диагностикой (Q = 0,6), а не со скрытыми сбоями ($Q = 2{,}175\times10^{-9}$). Это типично для большинства практических систем, у которых значение охвата диагностикой не равно или не близко к 100 %. Для тех случаев, когда вероятности скрытых сбоев незначительны, удаление их из анализа FTA значительно упрощает анализ. Тем не менее метрика скрытых сбоев документально оформляется в виде отдельной части обоснования безопасности.

Согласно 9.4.3 ИСО 26262-5 вероятность, связанного с безопасностью сбоя оценивается на уровне части аппаратного средства. Если этот анализ осуществляется с помощью FTA, то FTA структурируется таким образом, чтобы оценка на уровне части аппаратного средства могла быть выполнена.

В данном примере это показано на рисунке В.6. В 9.4.3.5 и 9.4.3.6 ИСО 26262-5 требования приведены в виде соотношений между интенсивностью отказов класса частей аппаратного средства и их охватом диагностикой. Если оценка осуществляется с помощью FTA, полезно преобразовать требования, представленные в 9.4.3.5 и 9.4.3.6 ИСО 26262-5, в эффективное требование, связанное с интенсивностью остаточных отказов или одиночных отказов части аппаратного средства. Если, например, интенсивность отказов класса 1 выбирается, как целевое значение УПБА, равное D, деленное на 100, а целевое значение УПБА, равное D, выбирается так, чтобы оно было $< 10^{-8}$ $ч^{-1}$, то требование 9.4.3.6 ИСО 26262-5 может быть представлено как $\lambda_{RF,\text{части аппар. ср.}} \le 10^{-10}$ $ч^{-1}$, где $\lambda_{RF,\text{части аппар. ср}}$ является интенсивностью остаточных отказов части аппаратного средства. На рисунке В.6 показано, что вероятность отказа ЦПУ, который может привести к нарушению цели безопасности в течение срока службы 5000 ч, будет равна $1{,}040631\times10^{-6}$. Это приводит к соответствующему значению вероятности, равному $2{,}08\times10^{-10}$ в час. Поскольку эта величина больше требуемой интенсивности остаточных отказов, то требования 9.4.3.6 не будут выполнены.

Применение FTA, как описано для оценки выполнения 9.4.3.5 или 9.4.3.6 ИСО 26262-5, является консервативным, поскольку эффективные требования относятся к интенсивности остаточных отказов или одиночных отказов части аппаратного средства. Однако FTA предоставляет вероятность, включая также сценарии с двойными отказами.

Поскольку FTA не рассматривает требования 9.4.3.11 ИСО 26262-5, то необходим дополнительный анализ для получения доказательств, что соответствующие требования, касающиеся сценариев с двойными отказами, выполнены.

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.

B.5 Пример дерева отказов

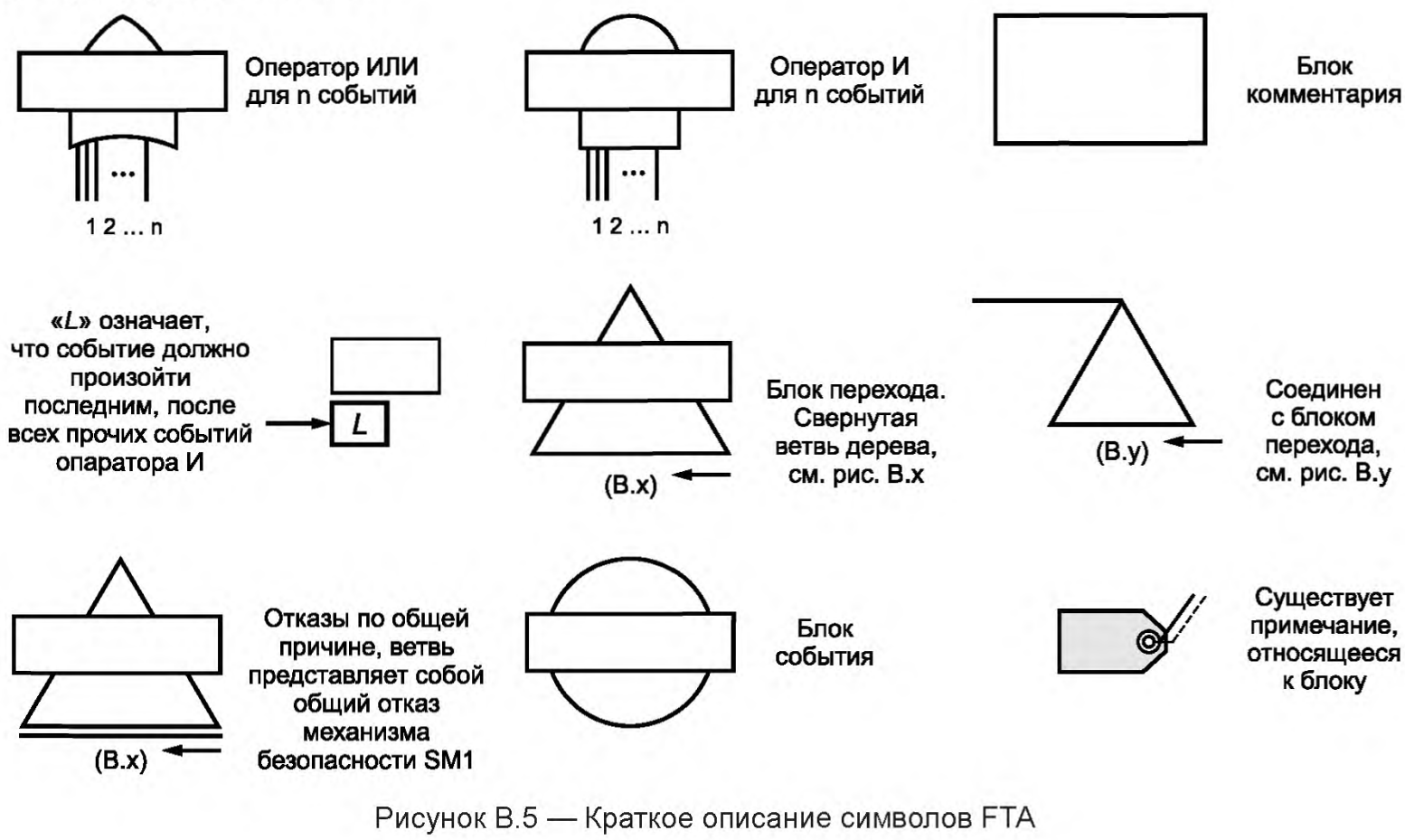


Рисунок B.5 — Краткое описание символов FTA

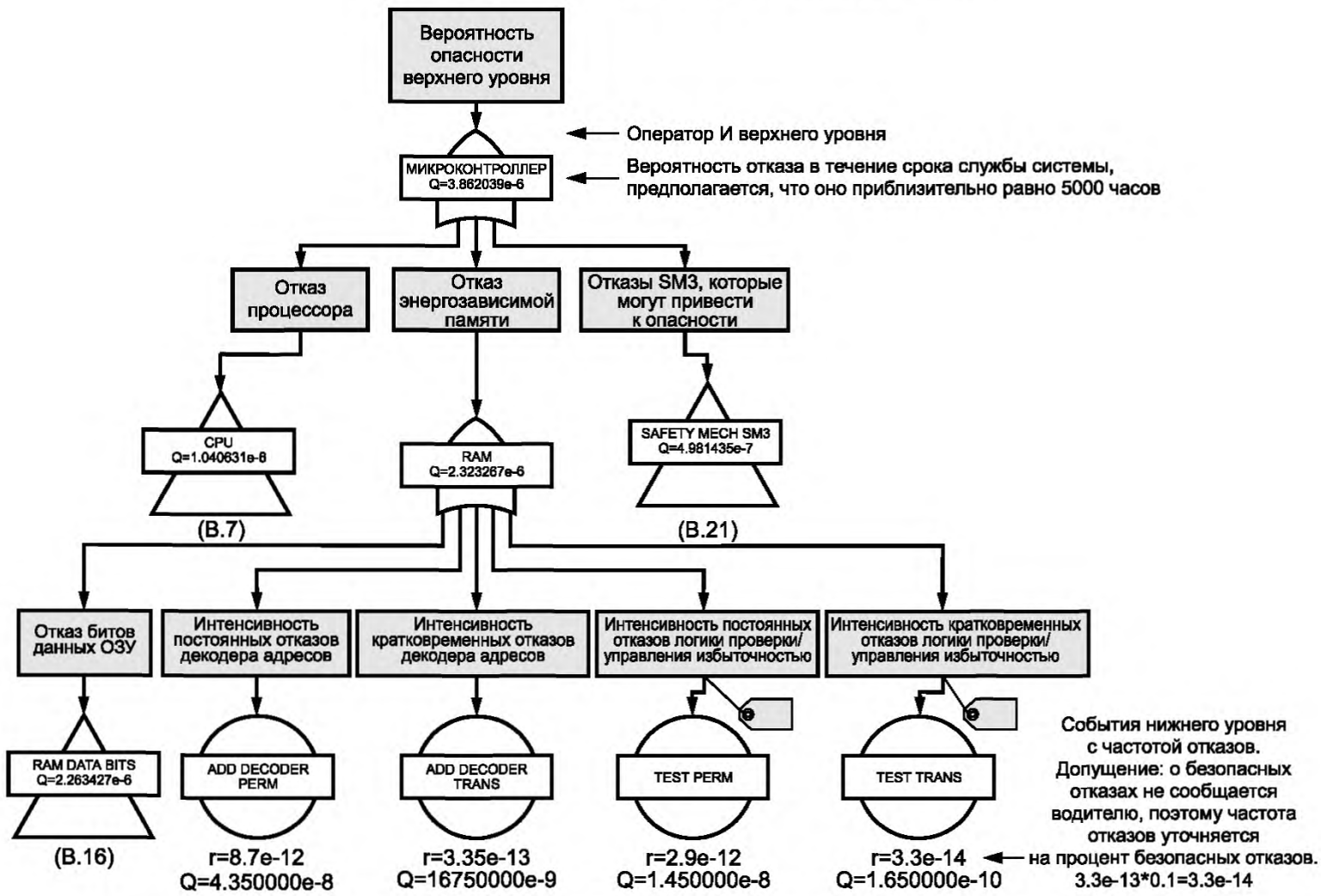


Рисунок B.6 — Верхний уровень дерева неисправностей

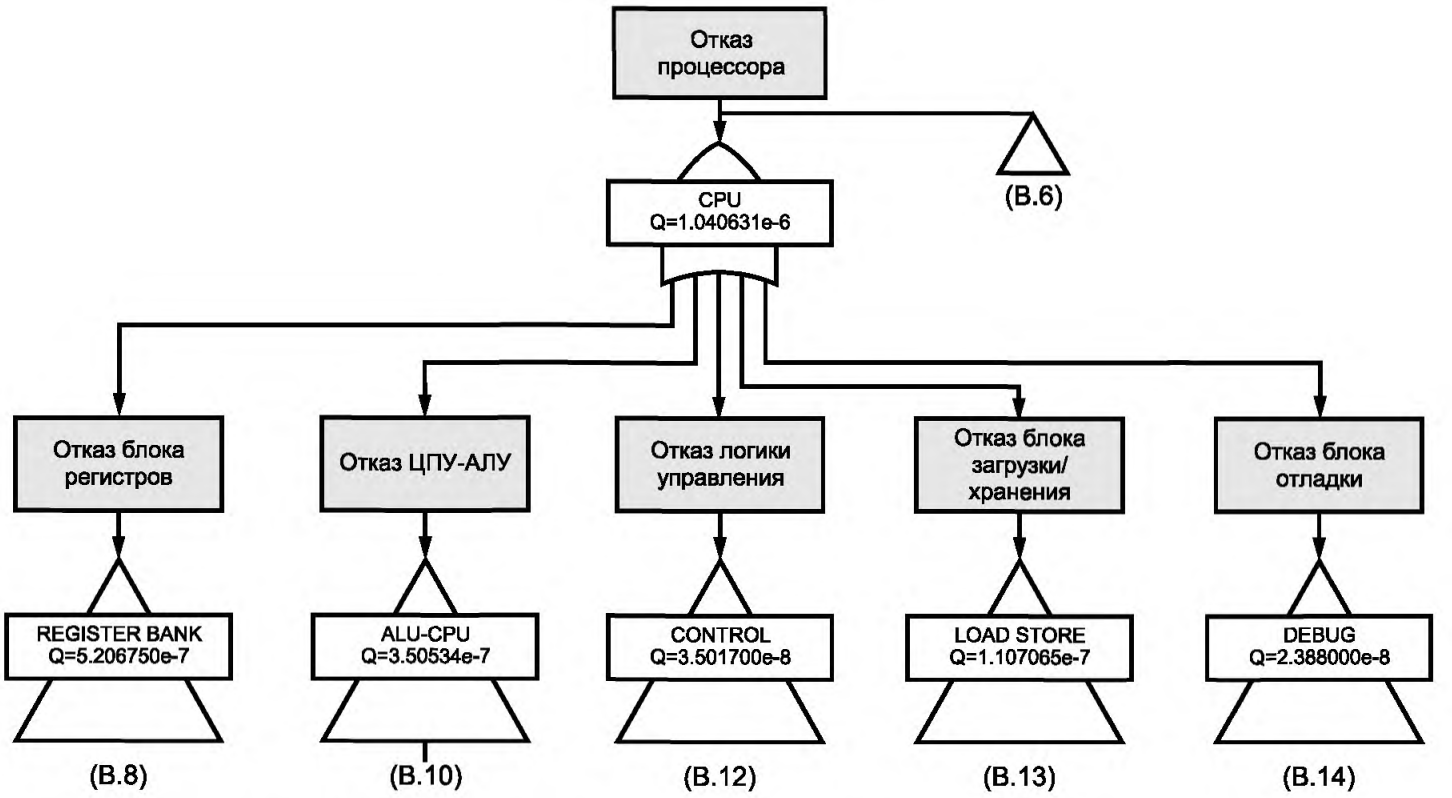


Рисунок B.7 — Ветвь, представляющая CPU, дерева неисправностей верхнего уровня

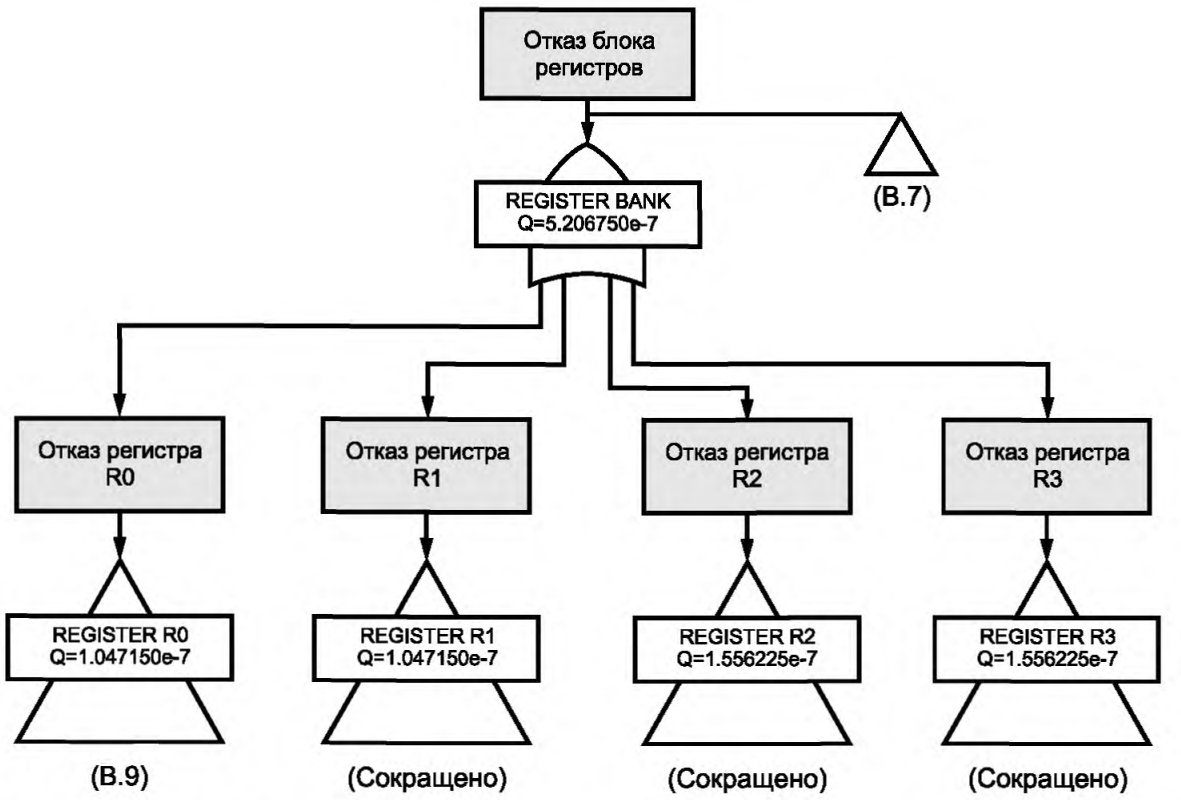


Рисунок B.8 — Ветвь, представляющая блок регистров CPU, дерева неисправностей верхнего уровня

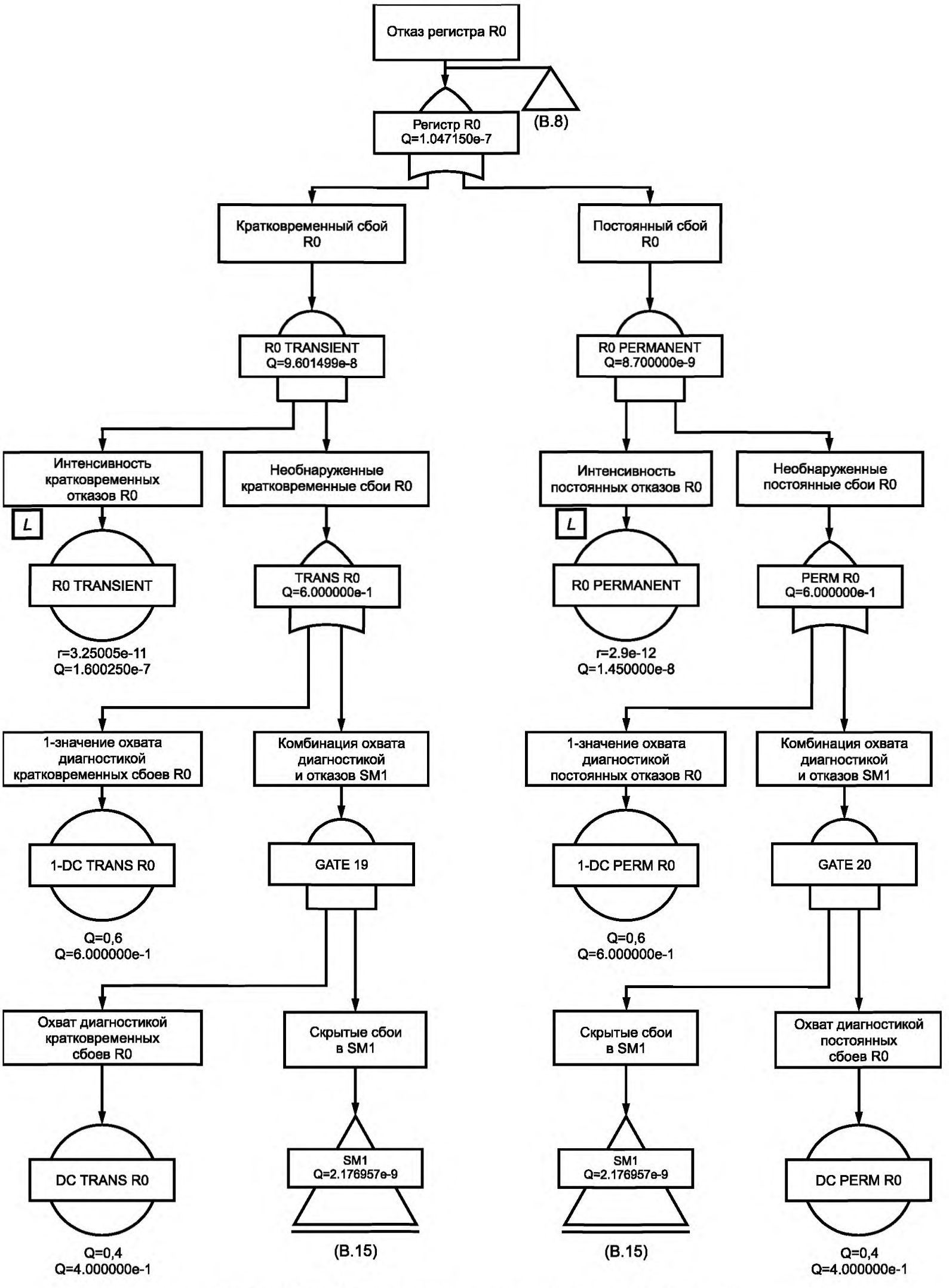


Рисунок В.9 — Ветвь дерева неисправностей для регистра R0

За исключением значений охвата диагностикой, на рисунке В.9 представлено типичное дерево отказов, которое можно использовать для любого регистра, поэтому конкретные деревья отказа для регистров 1, 2 и 3 не показаны.

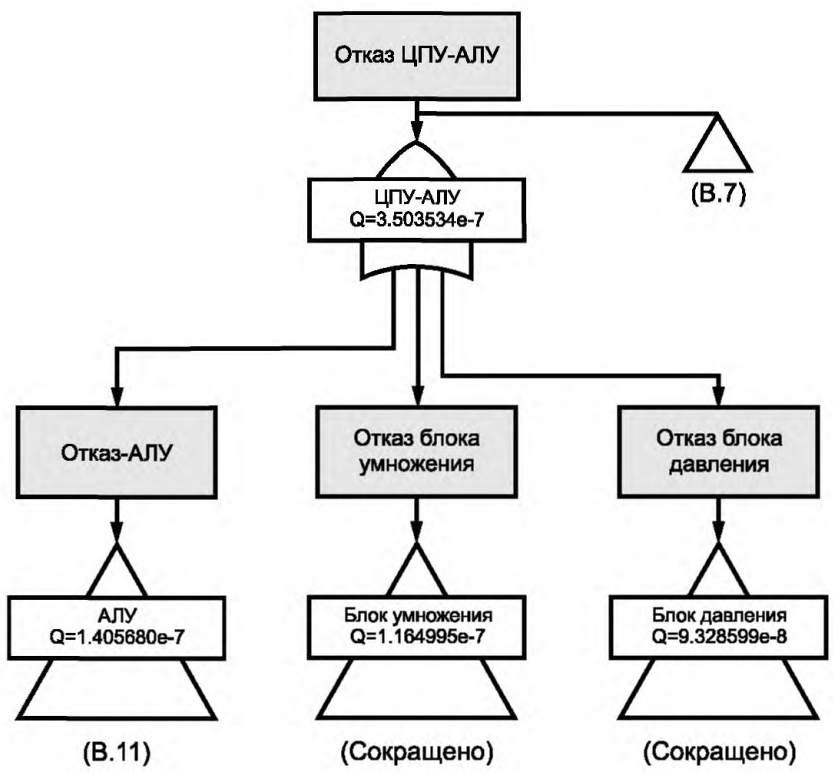


Рисунок В.10 — Ветвь, представляющая ЦПУ-АЛУ дерева неисправностей верхнего уровня

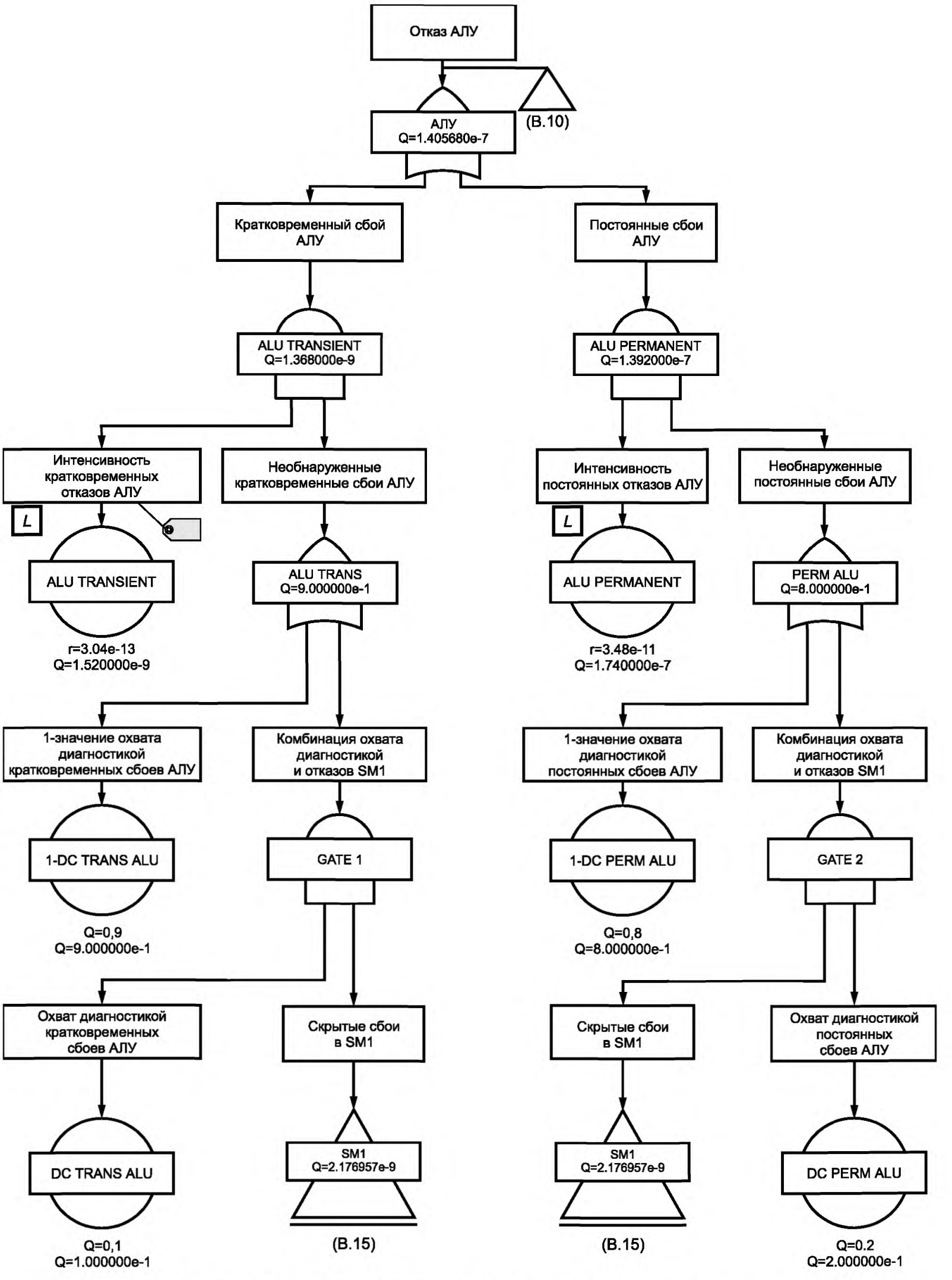


Рисунок В.11 — Ветвь дерева неисправностей, представляющая АЛУ

За исключением значений охвата диагностикой и интенсивностей FIT на рисунке В.11 представлено типичное дерево отказов, которое можно использовать для блока умножения, блока деления, устройства конвейерной обработки, секвенсера, устройства управления стэком, устройства формирования адресов, устройств загрузки и хранения, поэтому конкретные ветви дерева отказов для этих устройств не показаны.

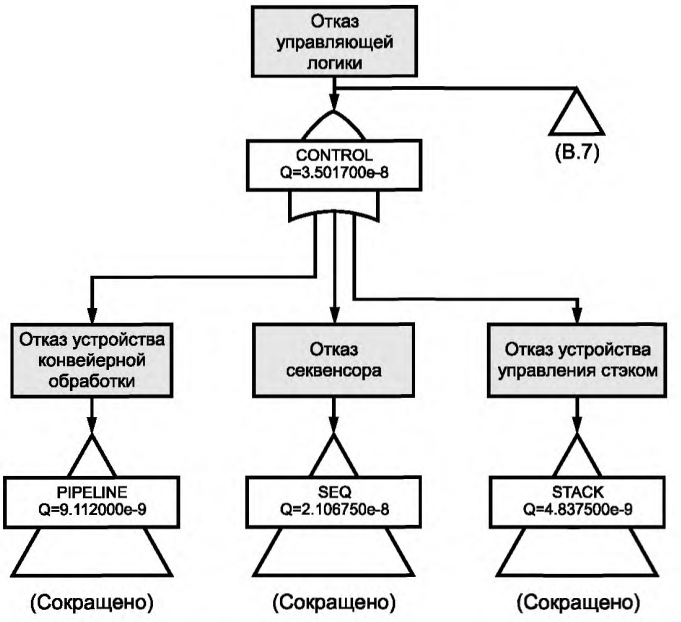


Рисунок В.12 — Ветвь дерева неисправностей верхнего уровня, представляющая устройство управления

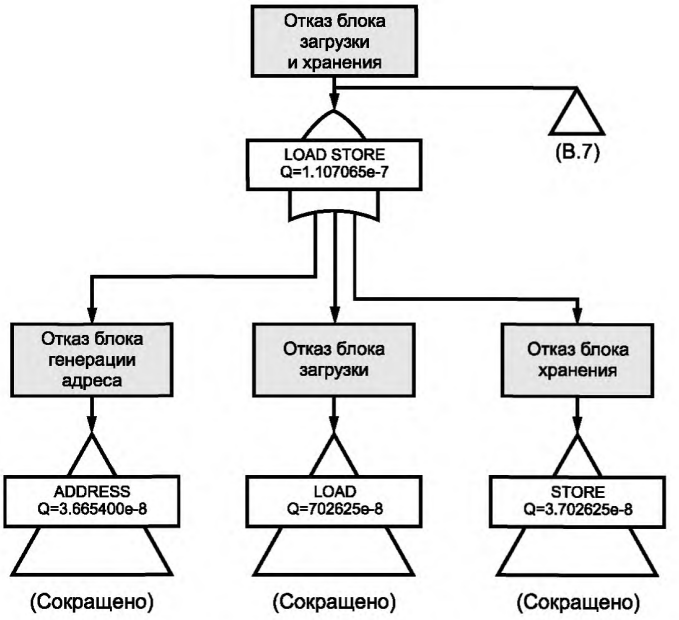


Рисунок В.13 — Ветвь дерева неисправностей верхнего уровня, представляющая блок загрузки и хранения

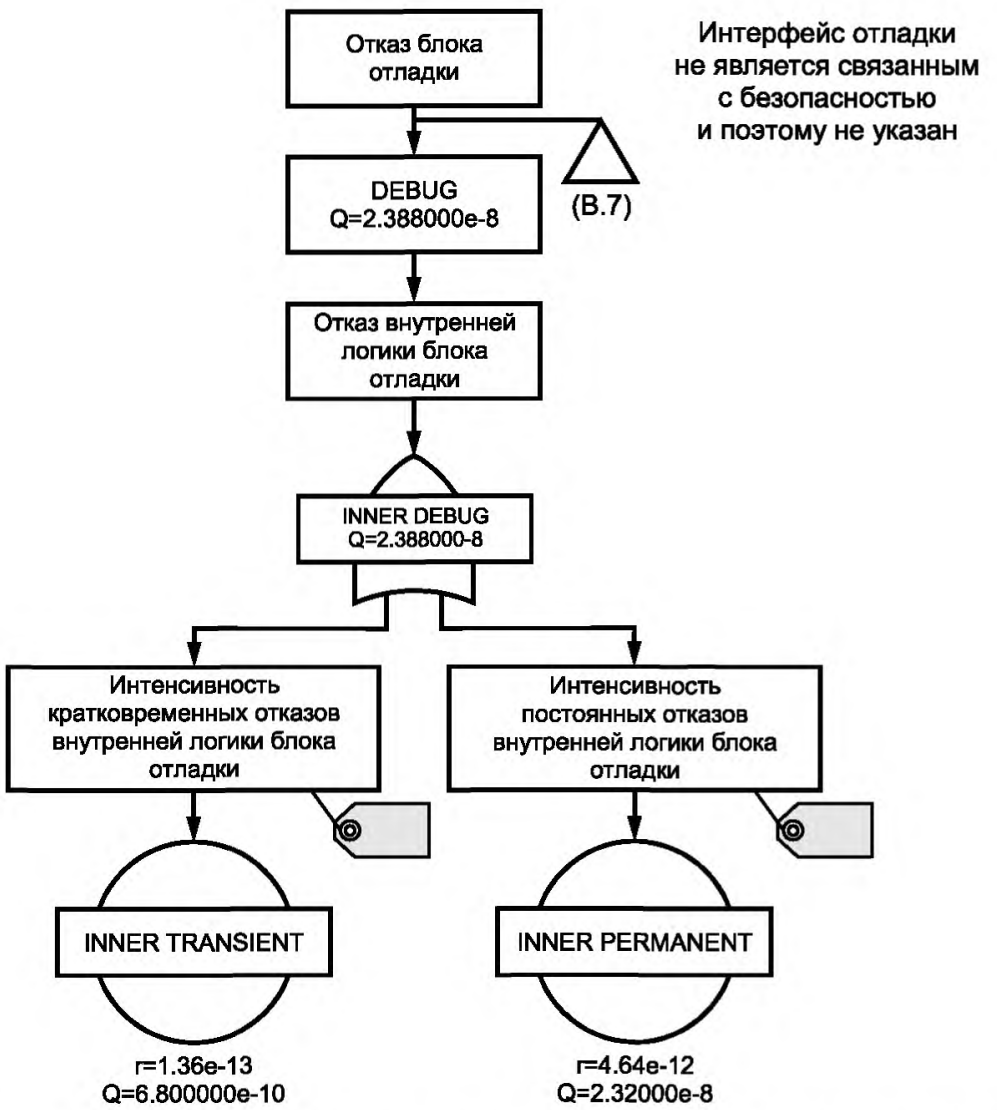


Рисунок В.14 — Ветвь дерева неисправностей, представляющая отладчик

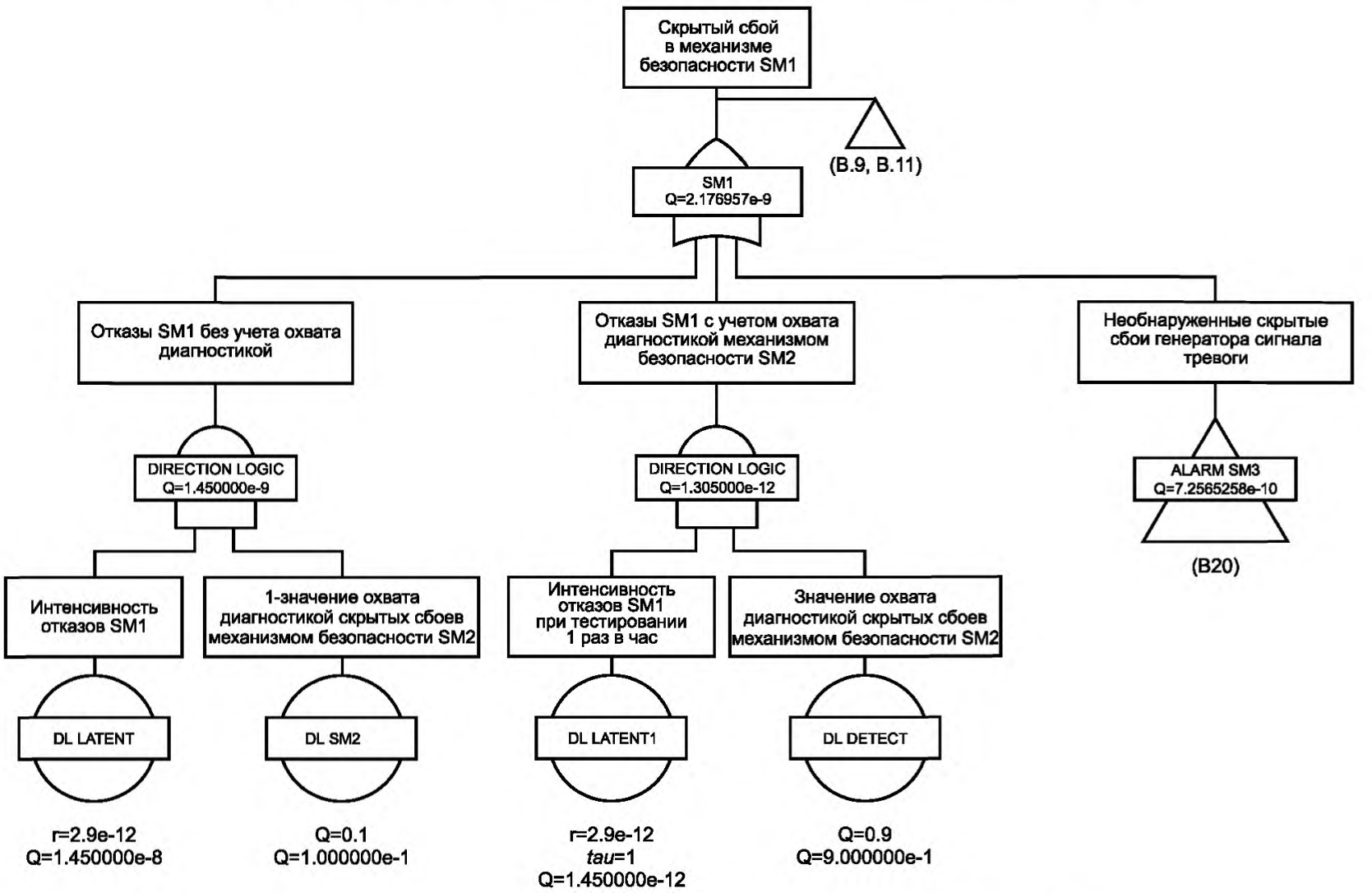


Рисунок В.15 — Охват скрытых сбоев механизмом безопасности SM2

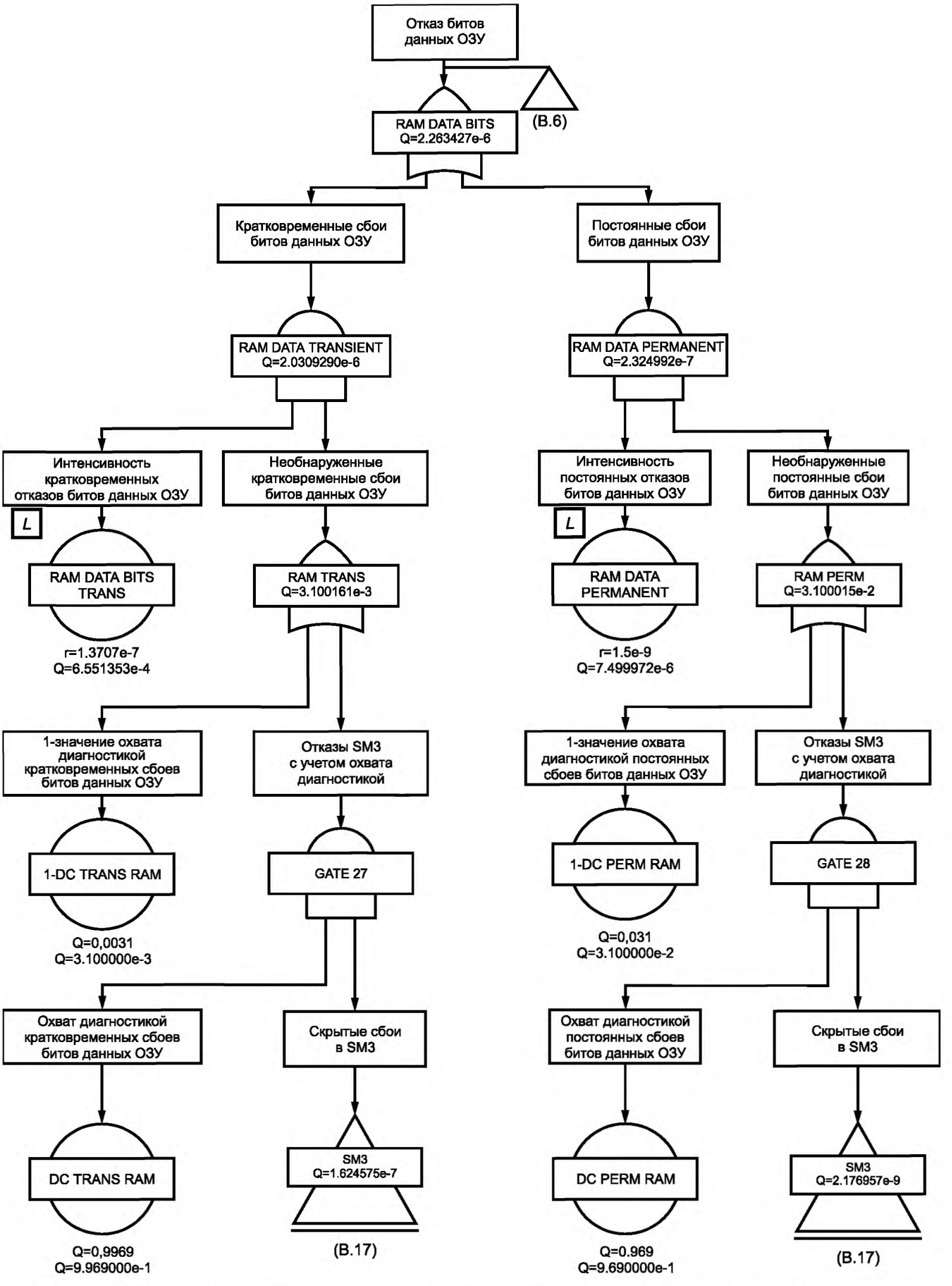


Рисунок В.16 — Ветвь дерева неисправностей верхнего уровня, представляющая энергозависимую память

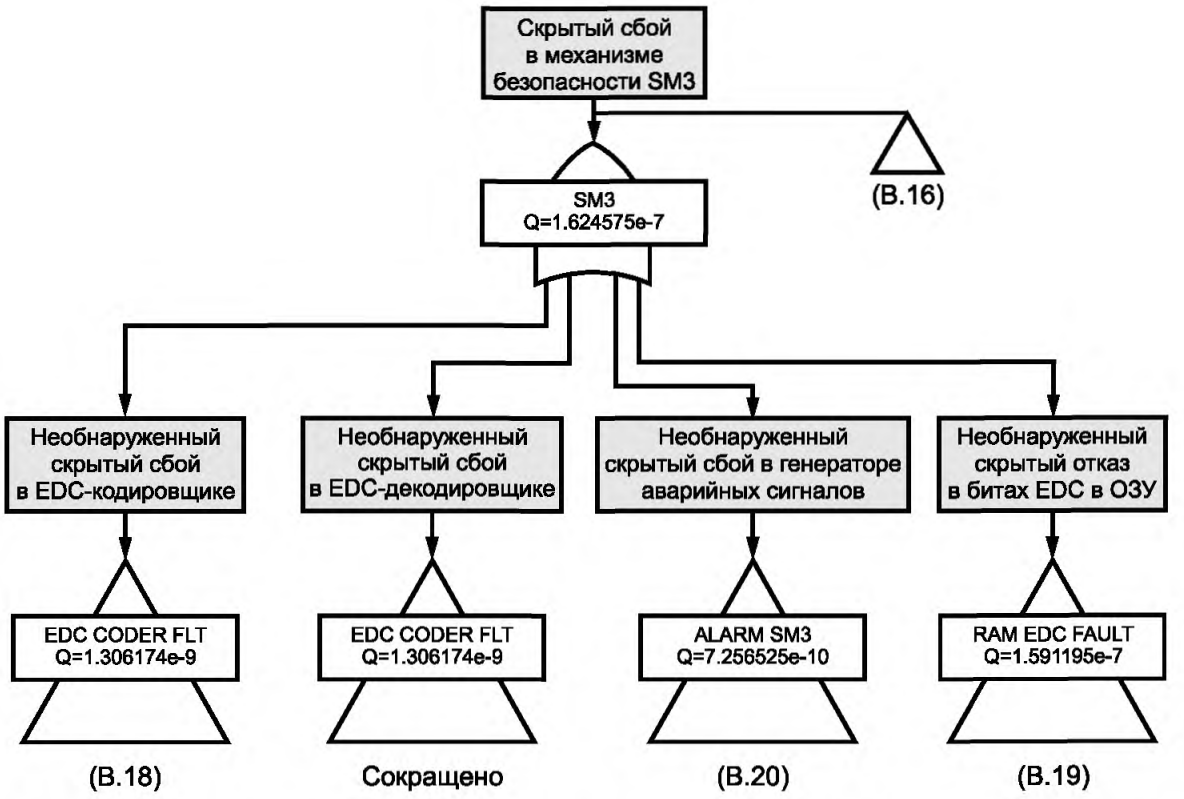


Рисунок B.17 — Ветвь дерева неисправностей, представляющая механизм безопасности SM3. Верхний уровень

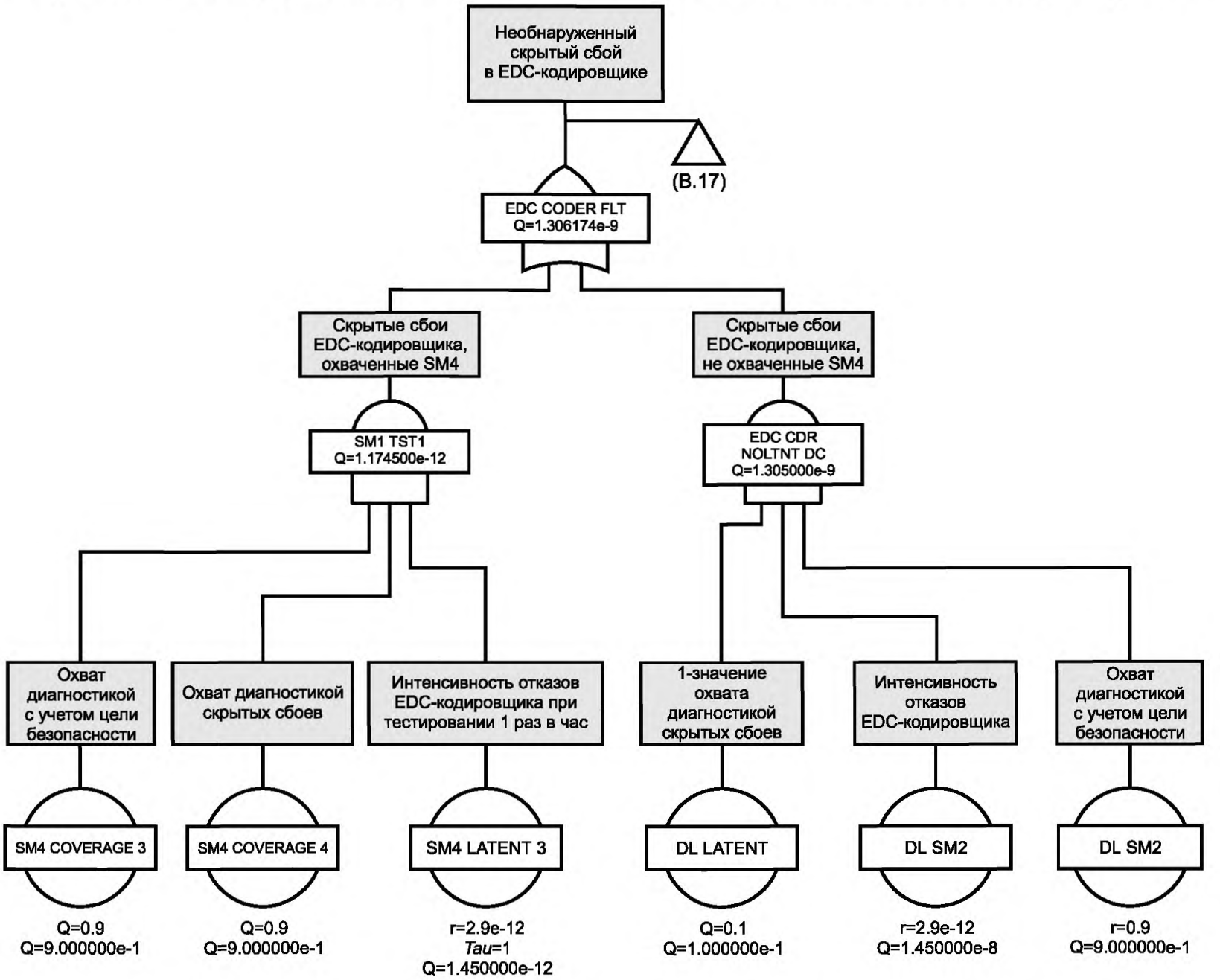


Рисунок B.18 — Ветвь дерева неисправностей, представляющая кодировщик механизма EDC

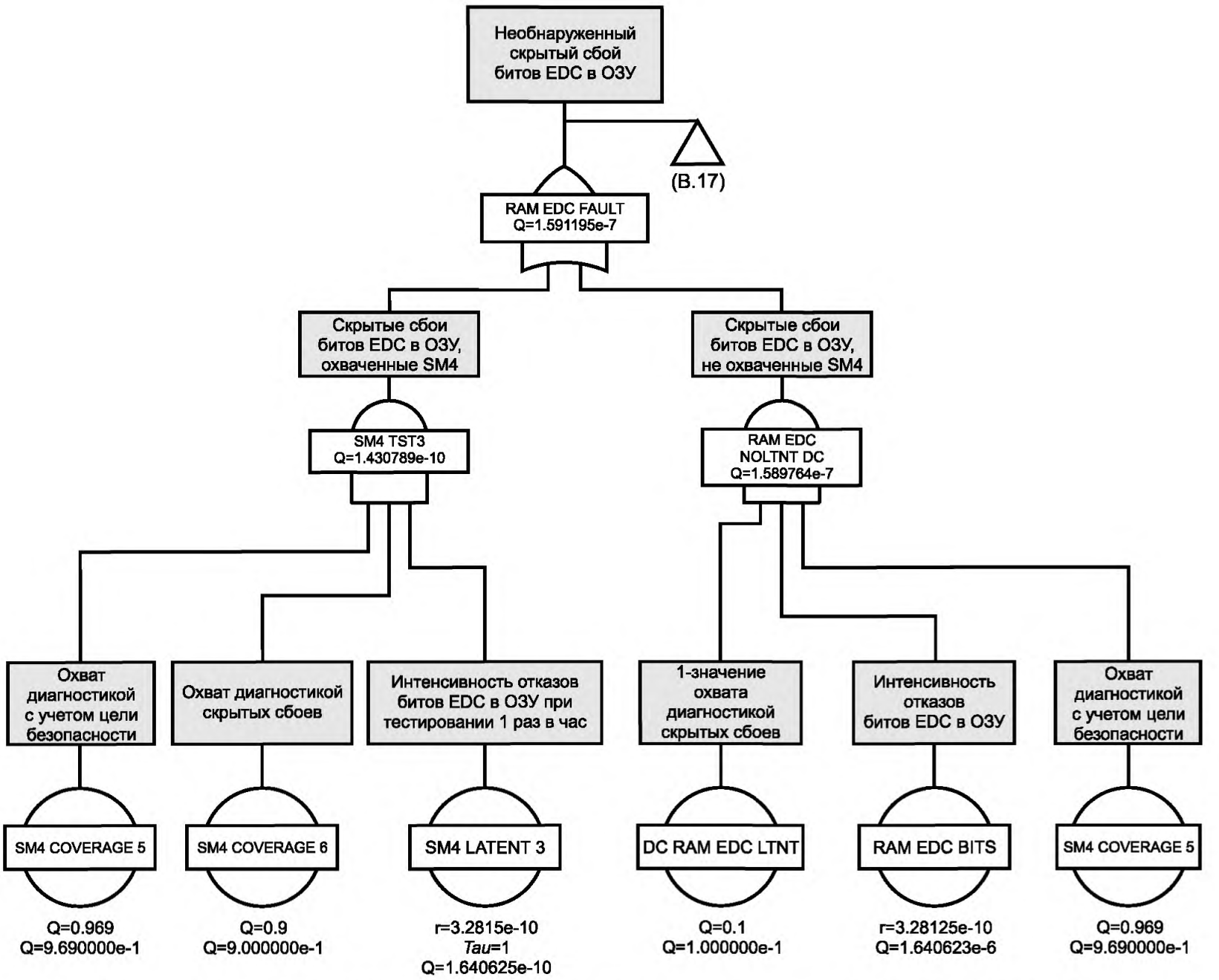


Рисунок B.19 — Ветвь дерева неисправностей, представляющая скрытые сбои битов EDC в ОЗУ

За исключением значений охвата диагностикой на рисунке B.19 представлено типичное дерево неисправностей, которое можно использовать для декодера механизма EDC, поэтому конкретные деревья неисправностей для этой ветви не показаны.

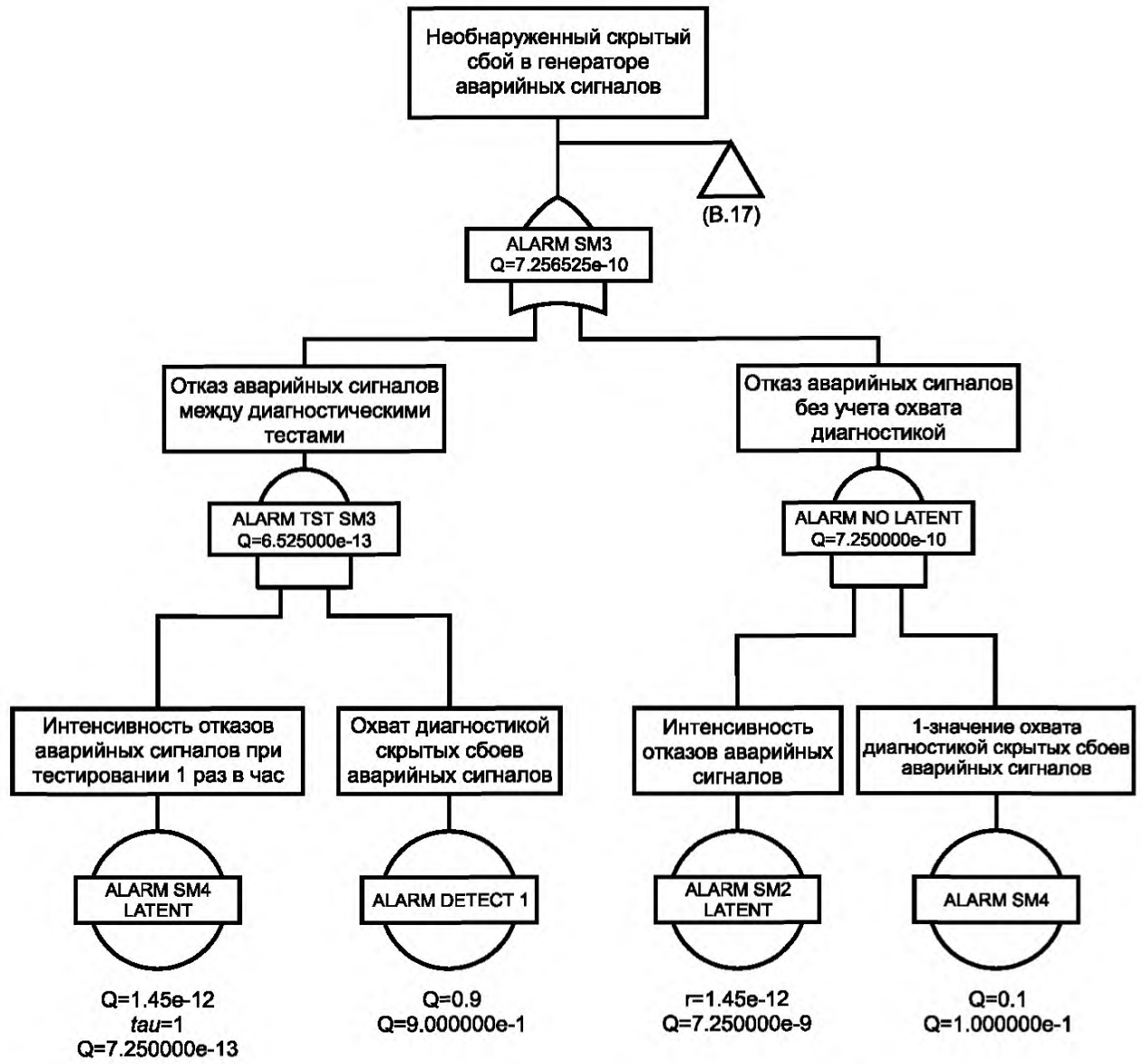


Рисунок B.20 — Ветвь дерева неисправностей, представляющая скрытые сбои в генераторе аварийных сигналов

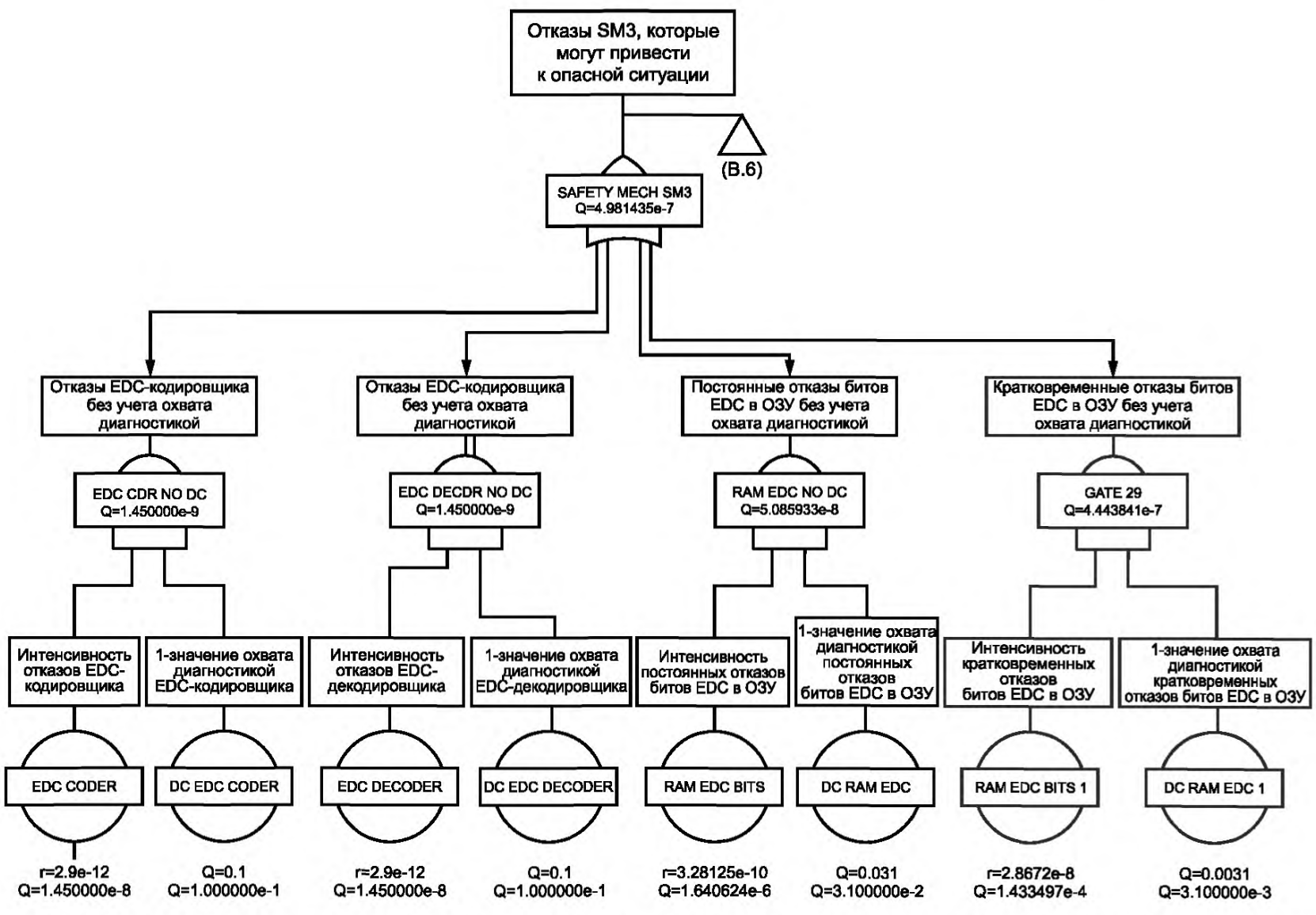


Рисунок B.21 — Ветвь дерева неисправностей SM3, представляющая отказы, которые непосредственно способствуют опасности на высоком уровне

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 26262-5:2011	–	*
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] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[2] Kelly, T. P., Arguing Safety — A Systematic Approach to Safety Case Management, DPhil Thesis, Department of Computer Science, University of York, UK, 1998

[3] Enamul Amyeen, M., et al., "Evaluation of the Quality of N-Detect Scan ATPG Patterns on a Processor", Proceedings of the International Test Conference 2004, ITC'04, p.669-678

[4] Benware, B., et al., "Impact of Multiple-Detect Test Patterns on Product Quality", Proc. of the International Test Conference 2003, ITC'03, pp. 1031-1040

[5] Patel, J. H., "Stuck-At Fault: A Fault Model for the Next Millennium?", Proceedings of the International Test Conference 1998, ITC'98, pp.1166

[6] Siemens AG, "Failure Rates of Components — Expected Values, General", SN 29500 (2004)

[7] Paschalis, A., and Gizopoulos, D., Effective Software-Based Self-Test Strategies for On-Line Periodic Testing of Embedded Processors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 24, 1 (Jan.2005), 88-99

[8] IEC/TR 62380:2004, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment

[9] The International Technology Roadmap For Semiconductors (ITRS), 2009 Edition

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

[11] IEC 61784 (all parts), Industrial communication networks — Profiles

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

Ключевые слова: функциональная безопасность; жизненный цикл систем; транспортные средства; электрические компоненты; электронные компоненты; программируемые электронные компоненты и системы; общие понятия; обзор

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 31.03.2015. Подписано в печать 14.09.2015. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 10,70. Уч.-изд. л. 10,05. Тираж 47 экз. Зак. 2964.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru