ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-1— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 1

Термины и определения

ISO 26262-1:2011
Road vehicles – Functional safety – Part 1: Vocabulary
(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 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 «01» августа 2014 г. № 860-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-1:2011 «Дорожные транспортные средства. Функциональная безопасность. Часть 1. Словарь» (ISO 26262-1:2011 «Road vehicles – Functional safety – Part 1: Vocabulary»)

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

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 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.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

Введение

Комплекс стандартов ИСО 26262 является адаптацией комплекса стандартов МЭК 61508[12] и предназначен для применения электрических и/или электронных (Э/Э) систем в дорожно-транспортных средствах.

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

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

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

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

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

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

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

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

e) устанавливает требования к взаимодействию с поставщиками.

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

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

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

- залитая область в виде символа «V» представляет взаимосвязь между ИСО 26262-3[4], ИСО 26262-4[5], ИСО 26262-5[6], ИСО 26262-6[7] и ИСО 26262-7[8];

- 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
- **3-6** 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 1

Термины и определения

Road vehicles – Functional safety – Part 1: Vocabulary

Дата введения — 2015—05—01

1 Область применения

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

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

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

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

Настоящий стандарт определяет термины, определения и сокращения, применяемые во всех частях комплекса ИСО 26262.

2 Термины и определения

В настоящем стандарте применены следующие термины и определения:

2.1 **распределение** (allocation): Присвоение требований **элементу** (2.32) архитектуры.

Примечание – Не подразумевает разделение элементарного требования на несколько требований. Означает прослеживание от элементарного требования на уровне **системы** (2.129) к нескольким элементарным требованиям на ее более низком уровне.

2.2 **аномалия** (anomaly): Условие, отклоняющееся от ожидаемых значений, например, в требованиях, спецификациях, проектной документации, пользовательской документации, стандартах или на практике.

Примечание – Аномалии могут быть обнаружены также в ходе **оценки** (2.98), **тестирования** (2.134), анализа, компиляции или использования **компонентов** (2.15) или соответствующей документации.

2.3 **архитектура** (architecture): Представление структуры из **устройств** (2.69) или функций, или **систем** (2.129), или **элементов** (2.32), которое позволяет идентифицировать блоки, из которых строится архитектура, их границы и интерфейсы, а также включает в себя **распределение** (2.1) функций

Издание официальное

элементам аппаратных средств и программного обеспечения.

2.4 **оценка** (assessment): Проверка характеристики **устройства** (2.69) или **элемента** (2.32).

Примечание – Уровень **независимости** (2.61) стороны или сторон, дающих оценку, касается каждой оценки.

2.5 **аудит** (audit): Экспертиза реализованного процесса.

2.6 **уровень полноты безопасности автомобиля**; УПБА, (Automotive Safety Integrity Level; ASIL): Один из четырех уровней, используемый для задания необходимых для **устройства** (2.69) или **элемента** (2.32) требований настоящего стандарта или **мер безопасности** (2.110), чтобы предотвратить неоправданный **остаточный риск** (2.97), для которого значение УПБА, равное D, является наиболее строгим уровнем, а значение УПБА, равное A, – наименее строгим.

2.7 **декомпозиция УПБА** (ASIL decomposition): Распределение требований безопасности с избыточностью между **элементами** (2.32), которые в достаточной степени являются независимыми, с целью снижения значения **УПБА** (2.6) избыточных требований безопасности, распределяемых между соответствующими элементами.

2.8 **готовность** (availability): Способность изделия выполнять необходимую функцию в заданных условиях, в определенное время или в течение заданного периода при условии, что необходимые внешние ресурсы доступны.

2.9 **базовая конфигурация** (baseline): Версия набора из одного или нескольких готовых изделий, **устройств** (2.69) или **элементов** (2.32), которая поддерживается управлением конфигурацией и используется в качестве основы для дальнейшего развития в процессе управления изменениями.

Примечание – См. раздел 8 ИСО 26262-8.

2.10 **охват ветвей** (branch coverage): Процент ветвей потока управления, которые были выполнены.

Примечания

1 100% охват ветвей предполагает 100% **охват операторов** (2.127).

2 Оператор ЕСЛИ-ТО-ИНАЧЕ всегда имеет две ветви - условие истинно и условие ложно - независимо от наличия оператора в ветви ИНАЧЕ.

2.11 **калибровочные данные** (calibration data): Данные, которые будут использоваться после создания программного обеспечения в процессе разработки.

Пример – Параметры (например, значение низких оборотов холостого хода, диаграммы характеристик двигателя); конкретные параметры транспортного средства (значения настроек, например, ограничителя хода дроссельной заслонки); различные коды (например, код страны, левостороннее или правостороннее рулевое управление).

Примечание – Калибровочные данные не могут содержать исполняемый или интерпретируемый код.

2.12 **кандидат** (candidate): **Устройство** (2.69) или **элемент** (2.32), определение и условия использования которого идентичны или имеют очень высокую степень унификации с устройством или элементом, который уже был выпущен и находится в эксплуатации.

Примечание – Это определение применяется, если кандидат используется для **подтверждения проверкой эксплуатацией** (2.90).

2.13 **каскадный отказ** (cascading failure): **Отказ** (2.39) **элемента** (2.32) или **устройства** (2.69), приводящий к отказу другого элемента или элементов того же устройства.

Примечание – Каскадные отказы являются **зависимыми отказами** (2.22), но не являются **отказами по общей причине** (2.14). См. Отказ A на рисунке 2.

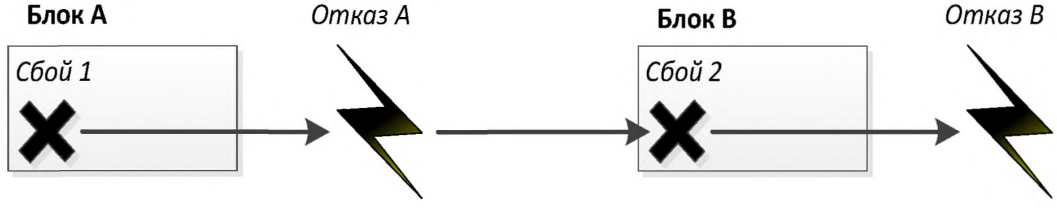


Рисунок 2 – Каскадный отказ

2.14 **отказ по общей причине**; ООП (common cause failure; CCF): **Отказ** (2.39) двух или более **элементов** (2.32) **устройства** (2.69) в результате одного конкретного события или исходной причины.

Примечание – Отказы по общей причине являются **зависимыми отказами** (2.22), но не являются **каскадными отказами** (2.13). См. рисунок 3.

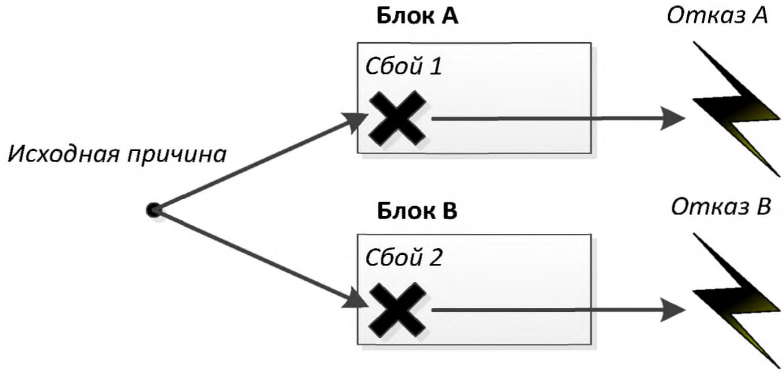


Рисунок 3 – Отказ по общей причине

2.15 **компонент** (component): **Элемент** (2.32) не уровня **системы** (2.129), который логически и технически отделим от другого элемента и состоит из нескольких **частей аппаратных средств** (2.55) или одного или более **модулей программного обеспечения** (2.125).

Примечание – Компонент является частью системы.

2.16 **данные конфигурации** (configuration data): Данные, присвоенные во время создания программного обеспечения и управляющие процессом создания программного обеспечения.

Пример – Команды препроцессора, скрипты создания программного обеспечения (например XML конфигурационные файлы).

Примечания

1 Данные конфигурации не могут содержать исполняемый или интерпретируемый код.

2 Данные конфигурации управляют созданием программного обеспечения. Только код или данные, выбранные данными конфигурации, могут быть включены в исполняемый код.

2.17 **мера подтверждения** (confirmation measure): **Оценка подтверждения** (2.18), **аудит** (2.5) или **оценка** (2.4), касающиеся **функциональной безопасности** (2.51).

2.18 **оценка подтверждения** (confirmation review): Подтверждение того, что результаты работы соответствуют требованиям настоящего стандарта при обеспечении необходимой степени **независимости** (2.61) оценивающего.

Примечания

1 Полный список оценок подтверждения приведен в ИСО 26262-2[3].

2 Целью оценки подтверждения является обеспечение соответствия требованиям настоящего стандарта.

2.19 **управляемость** (controllability): Способность предотвратить конкретный **вред** (2.56) или повреждение путем своевременной реакции заинтересованных лиц, возможно, при поддержке **внешних мер** (2.38).

Примечания

1 Заинтересованными лицами могут быть: водитель, пассажир или лицо, находящееся в непосредственной близости от транспортного средства.

2 Управляемость в **анализе опасности и оценке риска** (2.58) описывается параметром С.

2.20 **предназначенная мера** (dedicated measure): Мера, гарантирующая **интенсивность отказов** (2.41), требуемую при оценке вероятности нарушения **целей безопасности** (2.108).

Пример – Характеристики проектирования [задание с «запасом» параметров проектирования частей аппаратных средств (2.55) (например, диапазона значений электрических

или температурных параметров) или физическое разделение (например, расстояние между контактами на печатной плате)]; специальный выборочный входной контроль материала для снижения риска (2.99) возникновения видов отказов (2.40), которые способствуют нарушению целей безопасности; отбраковочные испытания; специальный план управления.

2.21 **снижение эффективности** (degradation): Заложенная при проектировании стратегия по обеспечению **безопасности** (2.103) после появления **отказов** (2.39).

Примечание – Снижение эффективности может включать в себя ограничение функциональности и/или снижение производительности.

2.22 **зависимые отказы** (dependent failures): **Отказы** (2.39), вероятность одновременного или последовательного возникновения которых не может быть представлена как простое произведение безусловной вероятности каждого из них.

Примечания

1 Зависимые отказы A и B могут быть охарактеризованы как:

$$P_{AB} \neq P_A \times P_B,$$

где P_{AB} – вероятность одновременного возникновения отказа A и отказа B;

P_A – вероятность возникновения отказа A;

P_B – вероятность возникновения отказа B.

2 Зависимые отказы включают **отказы по общей причине** (2.14) и **каскадные отказы** (2.13).

2.23 **обнаруженный сбой** (detected fault): **Сбой** (2.42), наличие которого обнаруживается в течение установленного времени **механизмом безопасности** (2.111), который выявляет этот сбой.

Пример – Сбой может быть обнаружен с помощью специального механизма безопасности (2.111) (например, обнаружив ошибку (2.36) и уведомив об этом водителя с помощью средства оповещения на приборной панели), как определено в концепции функциональной безопасности (2.52).

2.24 **соглашение о взаимодействии при разработке** (development interface agreement; DIA): Соглашение между заказчиком и поставщиком, в котором указывается ответственность за действия, доказательства или результаты работы при взаимодействии между сторонами.

2.25 **охват диагностикой** (diagnostic coverage): Доля **интенсивности отказов** (2.41) **элементов аппаратных средств** (2.32), обнаруженных или находящихся под контролем реализованных **механизмов безопасности** (2.111).

Примечания

1 Охват диагностической может быть оценен с помощью **остаточных сбоев** (2.96) или с помощью невыявленных **множественных сбоев** (2.77), которые могут произойти в элементах аппаратных средств.

2 Данное определение может быть представлено в виде уравнений, приведенных в ИСО 26262-5[6].

3 Механизмы безопасности могут быть реализованы на различных уровнях **архитектуры** (2.3).

2.26 **интервал диагностических проверок** (diagnostic test interval): Интервал между неавтономными проверками, выполняемыми **механизмом безопасности** (2.111).

2.27 **совместная разработка** (distributed development): Разработка **устройства** (2.69) или **элемента** (2.32) с разделением ответственности между заказчиком и поставщиком(и) для всего устройства или элемента или для подсистем.

Примечание – Заказчик и поставщик – это роли сотрудничающих сторон.

2.28 **разнообразие** (diversity): Применение различных подходов с целью получения независимых решений, удовлетворяющих одинаковым требованиям (2.61).

Пример – Различные методы разработки программ, различные технические средства.

Примечание – Разнообразие не гарантирует независимость, но устраняет некоторые типы **отказов по общей причине** (2.14).

2.29 **двойной отказ** (dual-point failure): **Отказ** (2.39), произошедший в результате комбинации двух независимых **сбоев** (2.42), который непосредственно вызывает нарушение **цели безопасности** (2.108).

Примечания

1 Двойной отказ является **множественным отказом** (2.76) второго порядка.

2 Двойные отказы, которые рассматриваются в настоящем стандарте, включают отказы, в которых один сбой влияет на **связанный с безопасностью элемент** (2.113), а другой сбой влияет на соответствующий **механизм безопасности** (2.111), предназначенный для достижения или поддержания **безопасного состояния** (2.102).

3 Чтобы двойной отказ непосредственно привел к нарушению цели безопасности, необходимо наличие двух независимых сбоев, то есть нарушение цели безопасности вследствие сочетания **остаточного сбоя** (2.96) с **безопасным сбоем** (2.101) не является двойным отказом, так как к нарушению цели безопасности приводит остаточный сбой независимо от наличия или отсутствия второго независимого сбоя.

2.30 **двойной сбой** (dual-point fault): **Отдельный сбой** (2.42), который в сочетании с другим независимым сбоем приводит к **двойному отказу** (2.29).

Примечания

1 Двойным сбой может быть признан только после идентификации двойного отказа, например, в результате анализа сечений дерева отказов.

2 См. также **множественный сбой** (2.77).

2.31 **электрическая и/или электронная система**; Э/Э система (electrical and/or electronic system; E/E system): **Система** (2.129), которая состоит из электрических и/или электронных **элементов** (2.32), в том числе программируемых электронных элементов.

Пример – Источник питания, датчик или другое устройство ввода; магистраль данных; исполнительное устройство или другое устройство вывода.

2.32 **элемент** (element): **Система** (2.129) или часть системы, включающая **компоненты** (2.15), аппаратные средства, программное обеспечение, **части аппаратных средств** (2.55), а также **модули программного обеспечения** (2.125).

2.33 **встроенное программное обеспечение** (embedded software): Полностью интегрированное программное обеспечение, выполняемое в **элементе** (2.32) обработки данных.

Примечание – Элементом обработки данных, как правило, является микроконтроллер, программируемая пользователем матрица (FPGA) или специализированная интегральная схема (ASIC), а также более сложный **компонент** (2.15) или подсистема.

2.34 **аварийный режим** (emergency operation): Режим функционирования с ухудшающимися характеристиками во время перехода из состояния, в котором произошел **сбой** (2.42), в **безопасное состояние** (2.102), как определено в **концепции предупреждения и постепенного ограничения характеристик** (2.140).

2.35 **интервал аварийного режима** (emergency operation interval): Установленная длительность **аварийного режима** (2.34), необходимая для поддержки реализации **концепции предупреждения и постепенного ограничения характеристик** (2.140).

Примечание – Аварийный режим является частью **концепции предупреждения и постепенного ограничения характеристик** (2.140).

2.36 **ошибка** (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и истинным, специфицированным или теоретически правильным значением или условием.

Примечания

1 Ошибка может возникнуть в результате непредвиденных условий эксплуатации или из-за **сбоя** (2.42) в рассматриваемой **системе** (2.129), подсистеме или **компоненте** (2.15).

2 Сбой может проявлять себя как ошибка в рассматриваемом **элементе** (2.32), а ошибка в конечном итоге может привести к **отказу** (2.39).

2.37 **воздействие** (exposure): Состояние в **процессе эксплуатации** (2.83), которое может быть **опасным** (2.57), если оно совпадает с опасным состоянием анализируемого **вида отказа** (2.40).

2.38 **внешняя мера** (external measure): Отдельная и отличная от **устройства** (2.69) мера, которая снижает или ослабляет **риски** (2.99), появившиеся в устройстве.

2.39 **отказ** (failure): Прекращение способности **элемента** (2.32) выполнять необходимую функцию.

Примечание – Неверная спецификация является источником отказа.

2.40 **вид отказа** (failure mode): Способ отказа **элемента** (2.32) или **устройства** (2.69).

2.41 **интенсивность отказов** (failure rate): Плотность вероятности **отказа** (2.39), деленная на вероятность сохранения работоспособности **элемента** (2.32) аппаратных средств.

Примечание – Интенсивность отказов предполагается постоянной и ее обычно обозначают как λ.

2.42 **сбой** (fault): Ненормальный режим, который может вызвать отказ **элемента** (2.32) или **устройства** (2.69).

Примечания

1 Различают постоянные, неустойчивые и **кратковременные сбои** (2.135) (в частности исправимые ошибки).

2 Неустойчивым является сбой, который появляется несколько раз, а затем исчезает. Этот тип сбоя может происходить, когда **компонент** (2.15) находится на грани выхода из строя или, например, из-за помехи в коммутаторе. Некоторые **систематические сбои** (2.131) (например, небольшие изменения длительности сигналов синхронизации) могут привести к неустойчивым сбоям.

2.43 **модель сбоя** (fault model): Представление **видов отказов** (2.40), произошедших в результате **сбоев** (2.42).

Примечание – Модели сбоя, как правило, формируются из опыта или используются из справочников по надежности.

2.44 **время реакции на сбой** (fault reaction time): Промежуток времени между обнаружением **сбоя** (2.42) и моментом времени достижения **безопасного состояния** (2.102). См. рисунок 4.

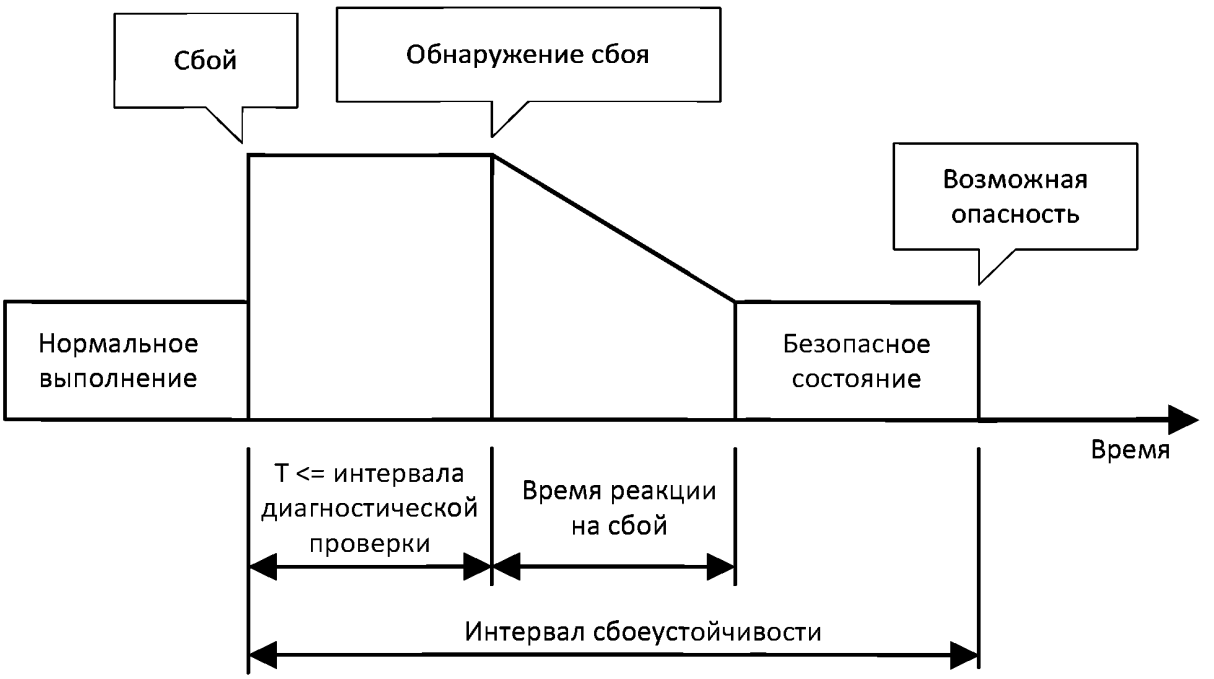


Рисунок 4 – Время реакции на сбой и интервал сбоеустойчивости

2.45 **интервал сбоеустойчивости** (fault tolerant time interval): Промежуток времени, в течение которого **сбой** (2.42) или сбои в **системе** (2.129) могут произойти, но **опасное** (1.57) событие не наступило.

2.46 **полевые данные** (field data): Данные, полученные в результате применения **устройства** (2.69) или **элемента** (2.32), включая накопленное число часов их работы, все **отказы** (2.39) и аномалии в процессе эксплуатации.

Примечание – Полевые данные обычно поступают от потребителя изделия.

2.47 **формальное средство описания** (formal notation): Язык технического описания, синтаксис и семантика которого определены формально.

Пример – Z нотация (Zed), NuSMV (средство проверки символьной модели), Система верификации прототипа (PVS), Венский метод разработки (VDM).

2.48 **формальная верификация** (formal verification): Метод, используемый для доказательства соответствия **системы** (2.129) спецификации ее требуемого поведения, представленной с помощью **формального средства описания** (2.47).

2.49 **отсутствие влияния** (freedom from interference): Отсутствие **каскадных отказов** (2.13) между двумя или более **элементами** (2.32), которые могут привести к нарушению требования безопасности.

Примеры

1 Элемент 2 не влияет на элемент 1, если никакой отказ (2.39) элемента 2 не может нарушить работу элемента 1.

2 Элемент 3 влияет на элемент 4, если существует такой отказ элемента 3, который нарушает работу элемента 4.

2.50 **функциональная концепция** (functional concept): Спецификация целевых функций и их взаимодействий, необходимых для достижения желаемого поведения.

Примечание – Функциональная концепция разрабатывается на **стадии** (2.89) формирования концепции системы.

2.51 **функциональная безопасность** (functional safety): Отсутствие **неоправданного риска** (2.136) вследствие **опасностей** (2.57), вызванных **неправильным поведением** (2.73) **Э/Э систем** (2.31.).

2.52 **концепция функциональной безопасности** (functional safety concept): Спецификация **требований функциональной безопасности** (2.53), связанной с ними информации, их **распределения** (2.1) по **элементам** (2.32) архитектуры и их взаимодействия, что необходимо для достижения **целей безопасности** (2.108).

2.53 **требование функциональной безопасности** (functional safety requirement): Спецификация независимого от реализации **безопасного** (2.103) поведения или независимых от реализации **мер безопасности** (2.110), в том числе связанных с безопасностью атрибутов.

Примечания

1 Требование функциональной безопасности может быть реализовано связанной с безопасностью **Э/Э системой** (2.31) или связанной с безопасностью **системой** (2.129), основанной на **других технологиях** (2.84), с целью достижения или поддержания **безопасного состоянии** (2.102) **устройства** (2.69) для определенного **опасного события** (2.59).

2 Требования функциональной безопасности могут быть заданы независимо от используемой технологии на **стадии** (2.89) формирования концепции разрабатываемого изделия.

3 Связанные с безопасностью атрибуты включают информацию об **УПБА** (2.6).

2.54 **метрики архитектуры аппаратных средств** (hardware architectural metrics): Метрики для **оценки** (2.4) эффективности **архитектуры** (2.3) аппаратных средств, используемой для обеспечения **безопасности** (2.103).

Примечание – Метриками архитектуры аппаратных средств являются метрика **одиночного сбоя** (2.122) и метрика **скрытого сбоя** (2.71).

2.55 **часть аппаратного средства** (hardware part): Аппаратное средство, которое не может быть далее декомпозировано.

2.56 **вред** (harm): Физическое повреждение или ущерб, причиняемый здоровью людей.

2.57 **опасность** (hazard): Потенциальный источник причинения вреда, вызванный **неправильным поведением** (2.73) **устройства** (2.69).

Примечание – Областью применения данного определения является настоящий стандарт. Более общим определением является: потенциальный источник причинения вреда.

2.58 **анализ опасностей и оценка рисков** (hazard analysis and risk assessment): Метод идентификации и классификации **опасных событий** (2.59) **устройств** (2.69), а также определения **целей безопасности** (2.108) и значений **УПБА** (2.6), позволяющий предотвратить или смягчить опасности

для того, чтобы избежать **неоправданный риск** (2.136).

2.59 **опасное событие** (hazardous event): Появление **опасности** (2.57) в **процессе эксплуатации** (2.83).

2.60 **однородная избыточность** (homogeneous redundancy): Несколько идентичных реализаций требования.

2.61 **независимость** (independence): Отсутствие **зависимых отказов** (2.22) между двумя или более **элементами** (2.32), которые могут привести к нарушению требования безопасности, либо разделение частей, выполняющих действие, организационными методами.

Примечание – По определению, **декомпозиция УПБА** (2.7) или **меры подтверждения** (2.17) включают в себя требования независимости.

2.62 **независимые отказы** (independent failures): **Отказы** (2.39), вероятность одновременного или последовательного возникновения которых может быть представлена как простое произведение безусловной вероятности каждого из них.

2.63 **неформальное средство описания** (informal notation): Техническое описание, синтаксис которого полностью не определен.

Пример – Описание в виде рисунка или схемы.

Примечание – Неполное определение синтаксиса влечет за собой неполное определение семантики.

2.64 **неформальная верификация** (informal verification): Методы **верификации** (2.137), не использующие полуформальные или **формальные средства верификации** (2.48).

Пример – Критический обзор (2.98) проекта; анализ модели.

2.65 **наследование** (inheritance): Передача в процессе разработки тех же атрибутов требований на следующий уровень детализации.

2.66 **начальное значение УПБА** (initial ASIL): Значение **УПБА** (2.6), полученное в результате анализа опасностей или **декомпозиции УПБА** (2.7) на предыдущем уровне.

Примечание – Начальное значение УПБА является исходным значением для начальной **декомпозиции УПБА** (2.7) или дальнейшей декомпозиции УПБА.

2.67 **контроль** (inspection): Проверка результатов работы, следуя формальной процедуре, в целях выявления аномалий.

Примечания

1 Контроль является средством верификации (2.137).

2 Контроль отличается от **тестирования** (2.134) тем, что он обычно не рассматривает функционирование соответствующего **устройства** (2.69) или **элемента** (2.32).

3 Обнаруживаемые аномалии, как правило, устраняются доработкой и последующим повторным осмотром доработанного изделия.

4 Формальная процедура обычно включает в себя предварительно установленную процедуру, таблицу контрольных проверок, координатора и результирующую **оценку** (2.98).

2.68 **целевая функциональность** (intended functionality): Поведение, заданное для **устройства** (2.69), **системы** (2.129) или **элемента** (2.32) без учета **механизмов обеспечения безопасности** (2.111).

2.69 **устройство** (item): **Система** (1.129) или несколько систем, реализующие некоторую функцию уровня транспортного средства, находящуюся в области применения настоящего стандарта.

2.70 **разработка устройства** (item development): Полный процесс реализации **устройства** (2.69).

2.71 **скрытый сбой** (latent fault): **Множественный сбой** (2.77), наличие которого не выявляется **механизмом безопасности** (2.111) и не воспринимается водителем в течение **интервала обнаружения множественного сбоя** (2.78).

2.72 **жизненный цикл** (lifecycle): Все стадии **устройства** (2.69) от разработки концепции до его вывода из эксплуатации.

2.73 **неправильное поведение** (malfunctioning behaviour): **Отказ** (2.39) или непреднамеренное поведение **устройства** (2.69), не соответствующее проектируемому.

2.74 **проектирование на основе модели** (model-based development): Проектирование, использующее модели, описывающие функциональное поведение разрабатываемых **элементов** (2.32).

Примечание – В зависимости от уровня абстракции представления такой модели, она может быть

использована для моделирования и/или генерации кода.

2.75 **модификация** (modification): Санкционированное изменение **устройства** (2.69).

Примечания

1 В настоящем стандарте модификация используется при повторном использовании устройства для адаптации его **жизненного цикла** (2.72).

2 Изменение выполняется в течение жизненного цикла устройства, а модификация выполняется для создания нового устройства из существующего.

2.76 **множественный отказ** (multiple-point failure): **Отказ** (2.39), произошедший в результате комбинации нескольких независимых **сбоев** (2.42), который непосредственно приводит к нарушению **цели безопасности** (2.108).

Примечание – Чтобы множественный отказ непосредственно привел к нарушению цели безопасности, необходимо, чтобы все сбои были независимыми. Таким образом, нарушение цели безопасности вследствие комбинации **остаточных сбоев** (2.96) с другими независимыми сбоями не рассматривается как нарушение от множественного отказа.

2.77 **множественный сбой** (multiple-point fault): Отдельный **сбой** (2.42), который в сочетании с другими независимыми сбоями приводит к множественному отказу (2.76).

Примечание – Множественный сбой может быть распознан только после идентификации множественного отказа, например, в результате анализа сечений дерева отказов.

2.78 **интервал обнаружения множественного сбоя** (multiple-point fault detection interval): Промежуток времени, в течение которого может быть обнаружен **множественный сбой** (2.77), прежде чем он может вызвать **множественный отказ** (2.76). См. рисунок 4.

2.79 **новая разработка** (new development): Процесс создания **устройства** (2.69) с новой функциональностью и/или новая реализация существующей функциональности.

2.80 **нефункциональная опасность** (non-functional hazard): **Опасность** (2.57), которая возникает из-за других факторов, отличных от неправильного функционирования **Э/Э систем** (2.31), а также **связанных с безопасностью систем** (2.129), основанных на **других технологиях** (2.84), или **внешних мер** (2.38).

2.81 **режим работы** (operating mode): Воспринимаемое функциональное состояние **устройства** (2.69) или элемента (2.32).

Пример – Система (2.129) выключена; система активна; система пассивна; режим постепенного ограничения характеристик; аварийный режим (2.34).

2.82 **время работы** (operating time): Суммарное время, которое **устройство** (2.69) или **элемент** (2.32) функционирует.

2.83 **эксплуатационная ситуация** (operational situation): Сценарий, который может возникать в течение жизни автомобиля.

Пример – Вождение, парковка, обслуживание.

2.84 **другая технология** (other technology): Используемая в области применения настоящего стандарта технология, отличающаяся от Э/Э технологий.

Пример – Технология, основанная на принципах механики; технология, основанная на принципах гидравлики.

Примечание – Другие технологии могут быть рассмотрены либо при спецификации **концепции функциональной безопасности** (2.52) (см. раздел 8 и рисунок 2 ИСО 26262-3[4]), а также при **распределении** (2.1) требований безопасности (см. ИСО 26262-3[4] и ИСО 26262-4[5]), либо как **внешняя мера** (2.38).

2.85 **разбиение** (partitioning): Разделение функций или **элементов** (2.32) в целях проектирования.

Примечание – Разбиение может быть использовано для локализации **сбоев** (2.42) для предотвращения **каскадных отказов** (2.13). Для достижения **отсутствия влияния** (2.49) между разбиваемыми элементами при проектировании могут быть введены дополнительные нефункциональные требования.

2.86 **легковой автомобиль** (passenger car): Автомобиль, который спроектирован и построен в основном для перевозки пассажиров и их багажа и/или товара, имеющий не более восьми сидячих мест, кроме водительского, и не имеющий мест для стоящих пассажиров.

2.87 **воспринимаемый сбой** (perceived fault): **Сбой** (2.42), наличие которого выявляется водителем в течение установленного интервала времени.

Пример – Сбой может быть непосредственно выявлен в результате очевидного ограничения поведения или производительности системы (2.129).

2.88 **постоянный сбой** (permanent fault): Появившийся **сбой** (2.42), который не исчезает до его устранения или ремонта.

Примечание – Сбои постоянного тока, например, константные неисправности и замыкание являются постоянными сбоями. **Систематические отказы** (2.131) проявляются главным образом как постоянные сбои.

2.89 **стадия** (phase): Этапы **жизненного цикла** (2.72) системы безопасности, рассмотренные в различных частях комплекса ИСО 26262.

Примечание – В настоящем стандарте стадии рассмотрены в отдельных частях, т.е. ИСО 26262-3[4], ИСО 26262-4[5], ИСО 26262-5[6], ИСО 26262-6[7] и ИСО 26262-7[8] посвящены, соответственно, следующим стадиям:

- формированию концепции;
- разработке изделия на уровне системы;
- разработке технических средств изделия;
- разработке программного обеспечения изделия;
- производству и эксплуатации.

2.90 **подтверждение проверкой эксплуатацией** (proven in use argument): Доказательство, основанное на анализе **полевых данных** (2.46), полученных в результате использования **кандидата** (2.12), демонстрирующее, что вероятность любых **сбоев** (2.39) этого кандидата, которые могут ослабить **цель безопасности** (2.108) **устройства** (2.69), которую он реализует, удовлетворяет требованиям соответствующего значения **УПБА** (2.6).

2.91 **доверие проверке эксплуатацией** (proven in use credit): Замена заданного набора **подстадий** (2.128) **жизненного цикла** (2.72) соответствующими результатами работы, прошедшими **подтверждение проверкой в эксплуатации** (2.90).

2.92 **случайный отказ аппаратных средств** (random hardware failure): Отказ, возникающий в случайный момент времени жизни **элемента** (2.32) аппаратных средств в соответствии с распределением вероятности.

Примечание – **Интенсивность отказов** (2.41) элемента, связанная со случайными отказами аппаратных средств, может быть прогнозируема с достаточной степенью точности.

2.93 **разумно предсказуемое событие** (reasonably foreseeable event): Событие, которое технически возможно и имеет заслуживающее доверие и измеряемое значение интенсивности его появления.

2.94 **избыточность** (redundancy): Существование дополнительных средств к тем средствам, которые были бы достаточными для **элемента** (2.32) для выполнения им необходимых функций или для представления информации.

Примечание – Избыточность используется в настоящем стандарте для достижения **цели безопасности** (2.108) или заданного требования безопасности, или для представления связанной с безопасностью информации.

Примеры

1 Дублирование функциональных компонентов (2.15) является примером избыточности с целью повышения готовности (2.8) или обеспечения обнаружения сбоя (2.42).

2 Добавление битов четности для данных, представляющих связанную с безопасностью информацию, реализует избыточность с целью обеспечения обнаружения сбоя.

2.95 **стратегия обеспечения текущего состояния** (regression strategy): Стратегия, проверяющая, что реализуемое изменение не влияет на неизменяемые, существующие и ранее проверенные части или свойства **устройства** (2.69) или **элемента** (2.32).

2.96 **остаточные сбои** (residual fault): Часть **сбоев** (2.42), которые сами по себе приводят к нарушению **цели безопасности** (1.108), происходят в **элементе** (2.32) аппаратных средств и не охвачены **механизмами безопасности** (2.111.)

Примечание – Предполагается, что элемент аппаратных средств охвачен механизмом безопасно-

сти только для части его сбоев.

Пример – Если для вида отказов (2.40) требуется низкий (60%) охват диагностикой, то остальные 40% этого вида отказов являются остаточными сбоями.

2.97 **остаточный риск** (residual risk): Риск, остающийся после принятия мер безопасности (2.110).

2.98 **критический обзор** (review): Рассмотрение результатов работы с целью достижения ими намеченной цели в соответствии с задачей обзора.

Примечание – Критические обзоры могут быть поддержаны таблицами контрольных проверок.

2.99 **риск** (risk): Сочетание вероятности события причинения **вреда** (2,56) и **тяжести** (2.120) этого вреда.

2.100 **проектирование надежных в эксплуатации систем** (robust design): Проектирование, обеспечивающее способность системы правильно функционировать при искаженных входных сигналах или в отклоняющихся от нормы условиях окружающей среды.

Примечание – Под надежностью в эксплуатации понимается:

- для программного обеспечения – это способность реагировать на отклоняющиеся от нормы входные сигналы и условия;
- для технических средств – это способность быть защищенными при отклоняющихся от нормы условиях окружающей среды и стабильно функционировать в течение срока службы во всем диапазоне проектных параметров;
- в контексте настоящего стандарта – это возможность обеспечения безопасного поведения для граничных значений проектных параметров.

2.101 **безопасный сбой** (safe fault): **Сбой** (2.42), появление которого несущественно увеличивает вероятность нарушения **цели безопасности** (2.108).

Примечания

1 Как показано в приложении В ИСО 26262-5[6], безопасные сбои могут происходить как в **связанных с безопасностью элементах** (2.113), так и в не связанных с безопасностью.

2 **Одиночные сбои** (2.122), **остаточные сбои** (2.96) и двойные сбои не являются безопасными сбоями.

3 Если это не указано в концепции безопасности, то **множественные сбои** (2.77) выше второго порядка можно рассматривать как безопасные сбои.

2.102 **безопасное состояние** (safe state): **Режим работы** (2.81) **устройства** (2.69) в отсутствии необоснованного уровня **риска** (2.99).

Пример – Целевой рабочий режим; режим постепенного ограничения характеристик; режим выключенного состояния.

2.103 **безопасность** (safety): Отсутствие неприемлемого риска (2.136).

2.104 **действие по обеспечению безопасности** (safety activity): Действие, осуществляемое на одной или нескольких **подстадиях** (2.128) **жизненного цикла** (2.72) системы безопасности.

2.105 **безопасная архитектура** (safety architecture): Совокупность взаимодействующих **элементов** (2.32), удовлетворяющая требования безопасности.

2.106 **обоснование безопасности** (safety case): Подтверждение того, что требования безопасности **устройства** (2.69) обладают полнотой и удовлетворены доказательством, сформированным в процессе разработки этого устройства из результатов работы, связанной с обеспечением безопасности.

Примечание – Обоснование безопасности может быть распространено на вопросы **безопасности** (2.103), выходящие за область применения настоящего стандарта.

2.107 **культура безопасности** (safety culture): Используемые в организации политика и стратегия поддержки разработки, производства и эксплуатации **систем** (2.129), связанных с безопасностью.

Примечание – См. приложение В ИСО 26262-2.

2.108 **цель безопасности** (safety goal):, Требования к безопасности высокого уровня, полученные в результате анализа опасностей и оценки рисков (2.58).

Примечание – Одна цель безопасности может быть связана с несколькими **опасностями** (2.57) и несколько целей безопасности могут быть связаны с одной опасностью.

2.109 **менеджер по безопасности** (safety manager): Роль, выполняемая лицом, ответственным за управление **функциональной безопасностью** (2.51) в процессе разработки **устройства** (2.69).

2.110 **мера безопасности** (safety measure): Деятельность или техническое решение по предотвращению или управлению **систематическими отказами** (2.130) и по обнаружению **случайных отказов аппаратных средств** (2.92) или по управлению случайными отказами аппаратных средств, или по смягчению их вредного воздействия.

Примечания

1 Примерами мер безопасности является FMEA, а также программное обеспечение без использования глобальных переменных.

2 Меры безопасности включают в себя **механизмы безопасности** (2.111).

2.111 **механизм безопасности** (safety mechanism): Техническое решение, реализованное Э/Э функциями или **элементами** (2.32), или выполненное на основе **других технологий** (2.84) для обнаружения **сбоев** (2.42) или управления **отказами** (2.39) в целях достижения или поддержки **безопасного состояния** (2.102).

Примечания

1 Механизмы безопасности реализуются внутри **устройства** (2.69) для предотвращения сбоев, ведущих к **одиночному отказу** (2.121), или для уменьшения остаточных отказов, или для предотвращения скрытых сбоев.

2 Механизм безопасности обеспечивает либо

а) перевод или поддержку устройства в безопасном состоянии, либо

б) предупреждение водителю о том, чтобы он, как предполагается, контролировал влияние **отказа** (2.39), как это определено в **концепции функциональной безопасности** (2.52).

2.112 **план обеспечения безопасности** (safety plan): План по управлению и руководству выполнением **действий по обеспечению безопасности** (2.104) проекта, включая сроки, этапы, задачи, ожидаемые результаты, ответственности и ресурсы.

2.113 **элемент, связанный с безопасностью** (safety-related element): **Элемент** (2.32), который имеет возможность внести свой вклад в нарушение или достижение **цели безопасности** (2.108).

Примечание – Отказоустойчивые элементы считаются связанными с безопасностью, если они могут внести свой вклад, по крайней мере, в реализацию одной цели безопасности.

2.114 **функция, связанная с безопасностью** (safety-related function): Функция, которая имеет возможность внести вклад в нарушение **цели безопасности** (2.108).

2.115 **связанная с безопасностью специальная характеристика** (safety-related special characteristic): Характеристика **устройства** (2.69) или **элемента** (2.32), либо процесса их изготовления, которая может разумно предсказуемо воздействовать, способствовать или вызвать любое возможное снижение **функциональной безопасности** (2.51).

Примечания

1 Термин «специальные характеристики» определен в ИСО/ТС 16949[2].

2 Связанные с безопасностью специальные характеристики формируются на **стадии** (2.89) разработки устройств или элементов.

Пример – Диапазон температур, срок действия, крутящий момент, допуск на обработку, конфигурация.

2.116 **подтверждение соответствия безопасности** (safety validation): Обеспечение путем обследования и испытаний достаточности **целей безопасности** (2.108) и их достижения.

Примечание – В ИСО 26262-4[5] представлены соответствующие методы подтверждения соответствия.

2.117 **полуформальное средство описания** (semi-formal notation): Язык технического описания, синтаксис которого полностью определен, но определение семантики может быть неполным.

Пример – Язык структурного анализа и проектирования (SADT); универсальный язык моделирования (UML).

2.118 **полуформальная верификация** (semi-formal verification): Метод **верификации** (2.137), использующий **полуформальное средство описания** (2.117).

Пример – Использование тестовых векторов, полученных из полу-формального описания модели, чтобы проверить, что поведение системы (2.129) соответствует модели.

2.119 **указание по сервисному обслуживанию** (service note): Документально оформленная информация по **безопасности** (2.103), которая будет учитываться при выполнении процедур технического обслуживания **устройства** (2.69).

Пример – Связанные с безопасностью специальные характеристики (2.115), работы по безопасности, которые могут быть необходимы.

2.120 **тяжесть** (severity): Оценка степени **вреда** (2.56), причиняемого одному или нескольким лицам, который может возникнуть в потенциально **опасных** (2.57) ситуациях.

Примечание – Параметр "S" в методе анализа опасностей и оценки рисков (2.58) представляет возможную тяжесть вреда.

2.121 **одиночный отказ** (single-point failure): **Отказ** (2.39), происходящий в результате **одиночного сбоя** (2.122), который непосредственно приводит к нарушению **цели безопасности** (2.108).

Примечания

1 Одиночный отказ эквивалентен остаточному отказу для **элемента** (2.32), значение **охвата диагностикой** (2.25) которого равно 0%.

2 Если для элемента аппаратных средств определен по крайней мере один **механизм безопасности** (2.111) (например, сторожевой таймер для микроконтроллера), то никакой **сбой** (2.42) рассматриваемого элемента аппаратных средств не является одиночным сбоем.

2.122 **одиночный сбой** (single-point fault): **Сбой** (2.42) в **элементе** (2.32), не охваченном **механизмом безопасности** (2.111), который непосредственно приводит к нарушению **цели безопасности** (2.108).

Примечание – См. также **одиночный отказ** (2.121).

2.123 **компонент программного обеспечения** (software component): Один или несколько **модулей программного обеспечения** (2.125).

2.124 **инструментальное программное обеспечение** (software tool): Компьютерная программа, используемая при разработке **устройства** (2.69) или **элемента** (2.32).

2.125 **модуль программного обеспечения** (software unit): Представляющий самый низкий уровень **архитектуры** (2.3) программного обеспечения **компонент программного обеспечения** (2.123), который может быть **протестирован** (2.134) автономно.

2.126 **транспортное средство специального назначения** (special-purpose vehicle): Транспортное средство, предназначенное для выполнения функции, которые требуют кузов специальной конструкции и/или специальное оборудование.

Пример – Домик на автомобильном прицепе, бронированный автомобиль, скорая помощь, катафалк, автомобильный трейлер, автокран.

Примечание – ECE TRANS / WP.29 / 78/Rev.1 / Amend.2 являются определениями транс-портных средств специального назначения.

2.127 **охват операторов** (statement coverage): Процент выполненных операторов в программе.

2.128 **подстадия** (subphase): Часть стадии **жизненного цикла** (2.72) системы безопасности, которая рассматривается в отдельном разделе настоящего стандарта.

Пример – Анализ опасностей и оценка рисков (2.58) является подстадией жизненного цикла системы безопасности, которая рассмотрена в разделе 7 ИСО 26262-3[4].

2.129 **система** (system): Набор **элементов** (2.32), содержащий, по крайней мере, связанные между собой датчик, контроллер и исполнительное устройство.

Примечания

1 Датчик или исполнительный механизм могут быть включены в систему или могут быть внешними по отношению к системе.

2 Элементом системы может быть также другая система.

2.130 **систематический отказ** (systematic failure): **Отказ** (2.39), связанный детерминированным образом с некоторой причиной, которая может быть исключена только путем изменения проекта либо производственного процесса, операций, документации, либо других соответствующих факторов.

2.131 **систематический сбой** (systematic fault): **Сбой** (2.42), после которого детерминированным образом появляется **отказ** (2.39), который можно предотвратить только путем применения опре-

деленных мер к процессу производства или проектирования.

2.132 **техническая концепция обеспечения безопасности** (technical safety concept): Спецификация **технических требований к системе безопасности** (2.133) и их **распределение** (2.1) **элементам** (2.32) **системы** (2.129) для реализации проекта системы.

2.133 **техническое требование к системе безопасности** (technical safety requirement): Требование, выведенное для реализации соответствующих **требований функциональной безопасности** (2.53).

Примечание – Выведенное требование включает требования к смягчению.

2.134 **тестирование** (testing): Процесс планирования, подготовки и выполнения или осуществление испытания **устройства** (2.69) или **элемента** (2.32), чтобы убедиться, что они удовлетворяют указанным требованиям, обеспечивающим обнаружение **аномалий** (2.2), и сформировать уверенность в их поведении.

2.135 **кратковременный сбой** (transient fault): **Сбой** (2.42), который происходит один раз, и впоследствии исчезает.

Примечание – Кратковременные сбои могут появиться из-за электромагнитных помех, которые могут привести к изменению значения бита памяти на противоположное. Исправимые ошибки, такие как одиночный сбой и кратковременное одиночное событие, являются кратковременными сбоями.

2.136 **неоправданный риск** (unreasonable risk): **Риск** (1.99), который считается неприемлемым в конкретном контексте в соответствии с действующими социально- нравственными понятиями.

2.137 **верификация** (verification): Определение полноты и корректности спецификации или выполнения требований для **стадий** (2.89) или **подстадий** (2.128).

2.138 **верификационная оценка** (verification review): Деятельность по **верификации** (2.137), гарантирующая, что результат разработки соответствует требованиям проекта и/или техническим требованиям.

Примечания

1 Отдельные требования для верификационных оценок даны в конкретных разделах отдельных частей настоящего стандарта.

2 Целью верификационных оценок является обеспечение технической корректности и полноты **устройства** (2.69) или **элемента** (2.32) для каждого варианта применения и **вида отказов** (2.40).

Пример – Технический критический обзор (2.98), сквозной контроль (2.139), контроль (2.67).

2.139 **сквозной контроль** (walk-through): Систематическая проверка **результатов работы** (2.142) с целью выявления аномалий.

Примечания

1 Сквозной контроль это средство **верификации** (2.137).

2 Сквозной контроль отличается от **тестирования** (2.134) тем, что он обычно не связан с работой соответствующего **устройства** (2.69) или **элемента** (2.32).

3 Любые обнаруженные аномалии, как правило, устраняются доработкой, за которой следует сквозной контроль доработанных результатов.

Пример – В процессе сквозного контроля разработчик подробно объясняет результаты работы одному или нескольким экспертам. Цель заключается в создании общего понимания результатов работы и выявлении в них любых аномалий. Контроль (2.67) и сквозной контроль относятся к виду критического обзора (2.98), выполняемого экспертом, где сквозной контроль является менее строгой формой экспертной оценки, чем контроль.

2.140 **концепция предупреждения и постепенного снижения эффективности** (warning and degradation concept): Спецификация того, как предупредить водителя о возможно ограниченной функциональности и того, как при этой ограниченной функциональности обеспечить достижение **безопасного состояния** (2.102).

2.141 **обладающий высоким уровнем доверия** (well-trusted): Ранее использованный, без известных **аномалий** (2.2) при обеспечении **безопасности** (2.103).

Пример – Принцип проектирования с высоким уровнем доверия, инструментальное средство с высоким уровнем доверия, компонент (2.15) аппаратного средства с высоким уровнем доверия.

2.142 **результат работы** (work product): Результат одного или нескольких взаимосвязанных требований настоящего стандарта.

Примечание – Ссылка может быть независимым документом, содержащим полную информацию о результатах работы или список ссылок на полную информацию о результатах работы.

3 Сокращения

В настоящем стандарте применены следующие сокращения:

Сокращение (англ.)	Сокращение (рус.)	Полное название
ACC	АКК	Адаптивный круиз-контроль
AEC	КАЭ	Совет по автотранспортной электронике
AIS	УШП	Упрощенная шкала повреждений
ASIC	СИС	Специализированная интегральная схема
ASIL	УПБА	Уровень полноты безопасности автомобиля (см. определение 2.6)
BIST	ВСТ	Встроенное самотестирование
CAN	CAN – протокол	CAN – шина (стандарт транспортного средства)
CCF	ООП	Отказ по общей причине (см. определение 2.14)
COTS	КД	Коммерчески доступные (имеющиеся в продаже)
CPU	ЦП	Центральный процессор
CRC	КЦИК	Контроль циклическим избыточным кодом
DC	ОД	Охват диагностикой (см. определение 2.25)
d.c.	Пост. Ток	Постоянный ток
DIA	СИР	Соглашение об интерфейсе разработки (см. определение 2.24)
DSC	СДС	Система динамической стабилизации
ECU	ЭУБ	Электронный блок управления
EDC	ОКО	Обнаружение и коррекция ошибки
E/E system	Э/Э система	Электрическая и/или электронная система; (см определение 2.31)
EMC	ЭМС	Электромагнитная совместимость
EMI	ЭП	Электромагнитные помехи
ESD	УЭР	Устойчивость к электростатическим разрядам
ESC	ЭКУ	Электронный контроль устойчивости
ETA	АДО	Анализ дерева событий
FMEA	ВМПП	Вентильная матрица, программируемая пользователем
FIT		Количество отказов за интервал времени
FMEA	АВПО	Анализ видов и последствий отказов
FTA	АДО	Анализ дерева отказов
HAZOP	АОР	Анализ опасности и работоспособности систем
HSI	ПАИ	Программно-аппаратный интерфейс
HW	ТС	Технические средства
H&R	АОиОР	Анализ опасностей и оценка рисков (см. определение 2.58)
IC	ИС	Интегральная схема
I/O	Вх/Вых	Вход / Выход
MC/DC	ИУ/ПРР	Изменение условий / Покрытие результатов решений
MMU	БУП	Блок управления памятью
MPU	БЗП	Блок защиты памяти
MUX	УКС	Уплотнитель канала связи
OS	ОС	Операционная система
PLD	ПЛУ	Программируемое логическое устройство
PMHF	ВМСОА	Вероятностная метрика для случайных отказов аппаратных средств
QM	УК	Управление качеством
RAM	ППД	Память с произвольным доступом
ROM	ПЗУ	Постоянное запоминающее устройство
RFQ	ЗИР	Запрос на использование ресурсов
SIL	УПБ	Уровень полноты безопасности
SOP	НП	Начало производства
SRS	СТС	Спецификация требований системы
SW	ПО	Программное обеспечение
UML	УЯМ	Унифицированный язык моделирования
V&V	ВиПС	Верификация и подтверждение соответствия
XML	РЯР	Расширяемый язык разметки

Библиография

[1] ISO 3779, Road vehicles — Vehicle identification number (VIN) — Content and structure

[2] ISO/TS 16949, Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations

[3] ISO 26262-2:2011, Road vehicles — Functional safety — Part 2: Management of functional safety

[4] ISO 26262-3:2011, Road vehicles — Functional safety — Part 3: Concept phase

[5] ISO 26262-4:2011, Road vehicles — Functional safety — Part 4: Product development at the system level

[6] ISO 26262-5:2011, Road vehicles — Functional safety — Part 5: Product development at the hardware level

[7] ISO 26262-6:2011, Road vehicles — Functional safety — Part 6: Product development at the software level

[8] ISO 26262-7:2011, Road vehicles — Functional safety — Part 7: Production and operation

[9] ISO 26262-8:2011, Road vehicles — Functional safety — Part 8: Supporting processes

[10] ISO 26262-9:2011, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

[11] ISO 26262-10, Road vehicles — Functional safety — Part 10: Guideline on ISO 26262

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

[13] ECE TRANS/WP.29/78/Rev.1/Amend.2, Consolidated Resolution on the construction of vehicles (R.E.3)

УДК 62-783:614.8:331.454:006.354 ОКС 13.110

Ключевые слова: безопасность функциональная, дорожно-транспортные средства, жизненный цикл систем безопасности автомобиля, системы, связанные с безопасностью, термины, определения, сокращения

Подписано в печать 20.01.2015. Формат 60x84 1/8.

Усл. печ. л. 2.33. Тираж 31 экз. Зак. 79

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»
123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru