ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-2— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 2

Менеджмент функциональной безопасности

ISO 26262-2:2011
Road vehicles — Functional safety — Part 2: Management of functional safety (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 10 июня 2014 г. № 521-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-2:2011 «Дорожные транспортные средства. Функциональная безопасность. Часть 2. Менеджмент функциональной безопасности» (ISO 26262-2:2011 «Road vehicles — Functional safety — Part 2: Management of functional safety»).

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

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов и документов 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 Требования соответствия настоящему стандарту . . . 2
4.1 Общие требования . . . 2
4.2 Интерпретация таблиц . . . 2
4.3 Требования и рекомендации, зависимые от значения УПБА . . . 3
5 Общие требования к управлению созданием системы безопасности . . . 3
5.1 Цель . . . 3
5.2 Общие положения . . . 3
5.3 Входная информация . . . 6
5.4 Требования и рекомендации . . . 7
5.5 Результаты работы . . . 8
6 Управление созданием системы безопасности на стадиях формирования концепции и разработки изделия . . . 8
6.1 Цели . . . 8
6.2 Общие положения . . . 8
6.3 Входная информация . . . 9
6.4 Требования и рекомендации . . . 9
6.5 Результаты работы . . . 15
7 Управление созданием системы безопасности после запуска устройства в производство . . . 16
7.1 Цель . . . 16
7.2 Общие положения . . . 16
7.3 Входная информация . . . 16
7.4 Требования и рекомендации . . . 16
7.5 Результаты работы . . . 16
Приложение А (справочное) Обзор и последовательность выполняемых работ менеджмента функциональной безопасностью . . . 17
Приложение В (справочное) Примеры оценки культуры реализации системы безопасности . . . 18
Приложение С (справочное) Цель мер подтверждения . . . 19
Приложение D (справочное) Обзор верификационных оценок . . . 21
Приложение Е (справочное) Пример программы оценки функциональной безопасности (для устройств, цель системы безопасности которых имеет значение УПБА, равное D) . . . 22
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам Российской Федерации . . . 24
Библиография . . . 25

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
- **3-6** 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 ремонт) 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 2

Менеджмент функциональной безопасности

Road vehicles — Functional safety — Part 2: Management of functional safety

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 подобные опасности, если они непосредственно не вызваны некорректным поведением Э/Э связанных с безопасностью систем.

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

Настоящий стандарт устанавливает требования к управлению функциональной безопасностью для автомобильной промышленности, в том числе следующие:

- независимые от проекта требования к участвующим организациям (общее управление системой безопасности) и
- связанные с проектом требования к управлению действиями в процессе жизненного цикла системы безопасности (т. е. управление на стадиях формирования концепции и разработки изделия, а также после его запуска в производство).

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 26262-3:2011 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 технических 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 применены термины, определения и сокращения по ИСО 26262-1.

4 Требования соответствия настоящему стандарту

4.1 Общие требования

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

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

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

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

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

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

4.2 Интерпретация таблиц

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

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

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

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

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

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

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

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

4.3 Требования и рекомендации, зависимые от значения УПБА

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

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

5 Общие требования к управлению созданием системы безопасности

5.1 Цель

Целью настоящего раздела является определение требований к организациям, которые отвечают за реализацию жизненного цикла системы безопасности или которые выполняют мероприятия по обеспечению безопасности на различных стадиях жизненного цикла системы безопасности.

Полученная в соответствии с настоящим разделом информация служит в качестве предварительных требований к действиям, выполняемым на различных стадиях жизненного цикла системы безопасности.

5.2 Общие положения

5.2.1 Краткое описание жизненного цикла системы безопасности

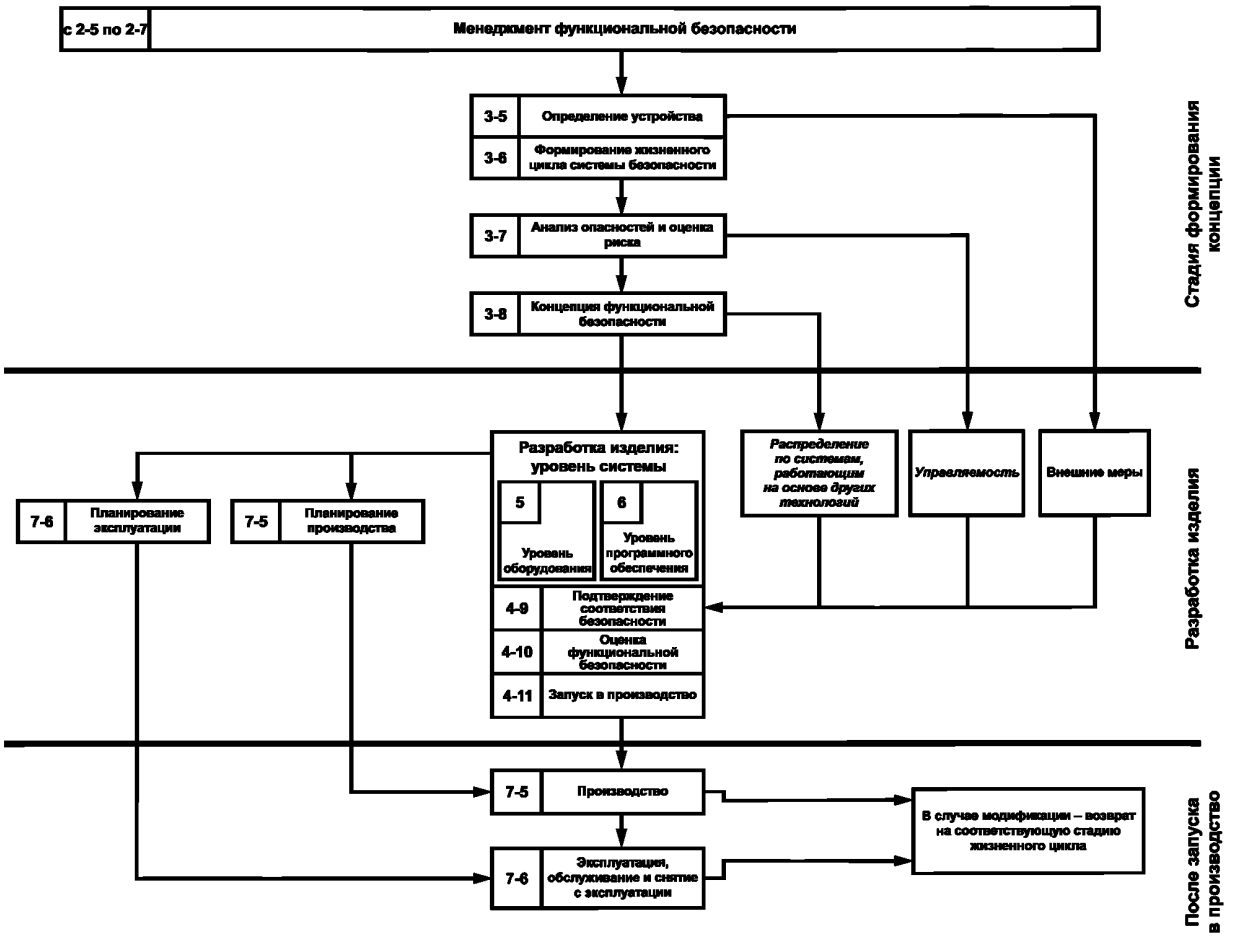
Представленный в настоящем стандарте жизненный цикл системы безопасности (см. рисунок 2) включает в себя основные мероприятия по обеспечению безопасности на стадиях формирования концепции, разработки, производства, эксплуатации, обслуживания и вывода из эксплуатации. Планирование, координация и документирование деятельности по обеспечению безопасности на всех стадиях жизненного цикла систем безопасности являются ключевыми задачами управления.

На рисунке 2 представлена рекомендуемая модель жизненного цикла системы безопасности. Допускается адаптация жизненного цикла системы безопасности, в том числе и итерация между подстадиями.

Примечания

1 Действия на стадиях формирования концепции и разработки изделия, а также после запуска в производство подробно описаны в ИСО 26262-3 (стадия формирования концепции), ИСО 26262-4 (разработка изделия на системном уровне), ИСО 26262-5 (разработка технических средств изделия), ИСО 26262-6 (разработка программного обеспечения изделия) и ИСО 26262-7 (производство и эксплуатация).

2 Таблица А.1 содержит обзор целей, предварительных требований и результатов работы конкретных стадий при реализации управления функциональной безопасностью.



Примечание — На рисунке конкретные разделы каждой части настоящего стандарта указаны следующим образом: «m-n», где «m» представляет собой номер части настоящего стандарта, а «n» указывает на номер ее раздела, например, 3-6 представляет раздел 6 ИСО 26262-3.

Рисунок 2 — Жизненный цикл системы безопасности

5.2.2 Пояснения к жизненному циклу системы безопасности

Настоящий стандарт устанавливает требования для конкретных стадий и подстадий жизненного цикла системы безопасности, а также включает в себя требования, которые применяются к нескольким или ко всем стадиям жизненного цикла систем безопасности, такие как требования к управлению функциональной безопасностью.

Основными задачами управления являются планирование, координация и отслеживание деятельности, связанной с функциональной безопасностью. Эти задачи управления распространяются на все стадии жизненного цикла систем безопасности. В настоящем стандарте приведены требования к управлению функциональной безопасностью, которые можно разделить на:

- общее управление системой безопасности (см. настоящий раздел);
- управление системой безопасности на стадии формирования концепции и разработки изделия (см. раздел 6);
- управление системой безопасности после запуска устройства в производство (см. раздел 7).

Ниже дано объяснение определений различных стадий и подстадий жизненного цикла системы безопасности, а также других ключевых понятий:

а) Подстадия определения устройства.

Для формирования жизненного цикла устройства обеспечения безопасности необходимо разработать описание, включающее его функциональность, интерфейсы, условия окружающей среды, правовые требования, известные опасности и т. д. Кроме того, определяются основные размеры устройства и

его интерфейсы, а также предположения, связанные с другими устройствами, элементами, системами и компонентами (см. раздел 5 ИСО 26262-3).

b) Подстадия формирования жизненного цикла системы безопасности.

На основании определения устройства обеспечения безопасности формируется его жизненный цикл либо для новой разработки такого устройства, либо для модификации существующего устройства.

Если модифицируется существующее устройство, то используются результаты анализа влияния для адаптации жизненного цикла системы безопасности (см. раздел 6 ИСО 26262-3).

c) Подстадия анализа опасностей и оценки рисков.

После формирования жизненного цикла системы безопасности выполняется анализ опасностей и оценка рисков, как указано в разделе 7 ISO 26262-3. Во-первых, с помощью метода анализа опасностей и оценки рисков оценивают вероятность воздействия, управляемости и тяжести опасных событий на устройство. Все вместе эти параметры определяют значения УПБА опасных событий. Во-вторых, с помощью метода анализа опасностей и оценки рисков определяют цели безопасности для устройства, которые становятся для устройства требованиями безопасности верхнего уровня. Определенные для опасных событий значения УПБА назначаются соответствующим целям безопасности.

На последующих стадиях и подстадиях из целей безопасности получают детальные требования безопасности. Эти требования безопасности наследуют значения УПБА соответствующих целей безопасности.

d) Подстадия формирования концепции функциональной безопасности.

На основе целей безопасности специфицируется концепция функциональной безопасности (см. раздел 8 ИСО 26262-3) с учетом рассмотрения предварительных предположений архитектуры. Концепция функциональной безопасности определяется функциональными требованиями к системе безопасности, которые распределяются элементам устройства. Концепция функциональной безопасности может также рассматривать устройства, выполненные на основе других технологий, или интерфейсы с внешними мерами, при условии, что для их предполагаемого поведения может быть выполнено подтверждение соответствия (см. раздел 9 ИСО 26262-4). Реализация устройств, выполненных на основе других технологий, не входит в область применения настоящего стандарта, а осуществление внешних мер не входит в область применения разработки устройства.

e) Стадия разработки изделия на уровне системы.

Как указано в ИСО 26262-4, после появления специфицированной концепции функциональной безопасности устройство разрабатывается на уровне системы. Процесс разработки на уровне системы основан на концепции V-модели со спецификацией технических требований обеспечения безопасности, разработкой архитектуры системы, разработкой и реализацией системы на левой ветви V-модели и с интеграцией, верификацией и подтверждением соответствия на правой ветви V-модели.

На данной стадии также специфицируется аппаратно-программный интерфейс.

На рисунке 1 представлен обзор подстадий разработки изделия на уровне системы.

Разработка изделия на уровне системы включает в себя задачи подтверждения соответствия действий, выполняемых на других стадиях жизненного цикла системы безопасности, в том числе:

- подтверждение соответствия аспектов концепции функциональной безопасности, которые реализуются на основе других технологий;
- подтверждение соответствия предположений об эффективности и производительности внешних мер и
- подтверждение соответствия предположений о реакции человека, включая управляемость и задачи эксплуатации.

Запуск в производство является последней подстадией разработки изделия и обеспечивает запуск устройства в серийное производство (см. раздел 11 ИСО 26262-4).

f) Подстадия разработки аппаратных средств изделия.

На основании спецификации проектирования системы разрабатываются аппаратные средства устройства (см. ИСО 26262-5). Процесс разработки аппаратных средств основан на концепции V-модели, в которой спецификация требований к аппаратным средствам, проектирование аппаратных средств и их реализация принадлежат левой ветви V-модели, а интеграция аппаратных средств и их тестирование — правой ветви V-модели.

На рисунке 1 представлен обзор подстадий разработки аппаратных средств изделия.

g) Подстадия разработки программного обеспечения изделия.

На основании спецификации проектирования системы разрабатывается программное обеспечение устройства (см. ИСО 26262-6). Процесс разработки программного обеспечения основан на концепции V-модели, в которой спецификация требований к программному обеспечению, проектирование

программного обеспечения и его реализация принадлежат левой ветви V-модели, а интеграция программного обеспечения, его тестирование и верификация — правой ветви V-модели.

На рисунке 1 представлен обзор подстадий разработки программного обеспечения изделия.

h) Планирование производства и эксплуатации.

Планирование производства и эксплуатации, а также спецификация соответствующих требований начинается во время разработки изделия на уровне системы (см. ИСО 26262-4). Требования к производству и эксплуатации приведены в разделах 5 и 6 ИСО 26262-7.

i) Стадия производства и эксплуатации, обслуживания и вывода из эксплуатации.

На этой стадии рассматриваются производственные процессы, имеющие значение для целей функциональной безопасности устройства, то есть связанные с безопасностью специальные характеристики, а также разработка и администрирование инструкций по обслуживанию, ремонту и утилизации устройств для обеспечения функциональной безопасности после запуска устройства в производство (см. разделы 5 и 6 ИСО 26262-7).

j) Управляемость.

При анализе опасностей и оценке рисков (см. раздел 7 ИСО 26262-3) может быть учтена способность водителя или других лиц, подвергающихся риску, контролировать опасные ситуации. Предположения, касающиеся управляемости, в анализе опасностей и оценке рисков и в концепции обеспечения функциональной и технической безопасности проходят процедуру подтверждения соответствия во время выполнения для системы подтверждения соответствия безопасности (см. рисунок 2 и раздел 9 ИСО 26262-4).

Примечание — Воздействие и тяжесть являются факторами, которые зависят от сценария. Возможная управляемость в результате вмешательства человека зависит от конструкции устройства и, следовательно, оценивается во время подтверждения соответствия (см. 9.4.3.2 ИСО 26262-4).

k) Внешние меры.

К внешним мерам относятся меры вне устройства, как специфицировано в определении устройства (см. рисунок 2 и раздел 5 ИСО 26262-3), которые снижают или смягчают риски, связанные с устройством. К внешним мерам можно отнести не только другие устройства в автомобиле, такие как контроллеры динамической устойчивости или противопрокольное устройство для шин, но и внешние к автомобилю устройства, такие как оградительные барьеры, системы пожаротушения в туннелях.

Предположения о внешних мерах в определении устройства, в анализе опасностей и оценке рисков и в концепции функциональной и технической безопасности проходят процедуру подтверждения соответствия во время выполнения для системы подтверждения соответствия безопасности (см. рисунок 2 и раздел 9 ИСО 26262-4).

Внешние меры могут быть рассмотрены при анализе опасностей и оценке рисков. Однако, если потенциал внешней меры учтен при анализе опасностей и оценке рисков, то внешняя мера не может рассматриваться для снижения риска в концепции обеспечения функциональной безопасности.

Настоящий стандарт распространяется на те внешние меры, которые находятся в области его применения.

l) Другие технологии.

Применение устройств, основанных на других технологиях, например, механических и гидравлических, которые отличаются от электрических и/или электронных технологий, находится в области применения настоящего стандарта. Они могут быть рассмотрены в спецификации концепции функциональной безопасности (см. рисунок 2 и раздел 8 ИСО 26262-3), при распределении требований безопасности (см. ИСО 26262-3 и ИСО 26262-4) или как внешняя мера.

Примечание — Если устройство, реализованное на другой технологии, определяется как внешняя мера, то может быть полезно повторить анализ опасностей и оценку рисков, чтобы рассмотреть соответствующее снижение риска, которое может привести к снижению значения УПБА соответствующей цели безопасности.

5.3 Входная информация

5.3.1 Предварительные требования

Не задаются.

5.3.2 Дополнительная информация

Может быть рассмотрена следующая информация.

Существующее подтверждение системы менеджмента качества о соответствии стандартам управления качеством, таким как ИСО/ТС 16949, ИСО 9001 или эквивалентным.

5.4 Требования и рекомендации

5.4.1 Общие положения

Организации, участвующие в реализации жизненного цикла системы безопасности, должны соответствовать требованиям 5.4.2—5.4.5.

5.4.2 Культура реализации системы безопасности

5.4.2.1 Организация должна создать, развивать и поддерживать культуру безопасности, которая поощряет эффективное достижение функциональной безопасности.

Пример — Примеры оценки культуры реализации системы безопасности приведены в приложении В.

5.4.2.2 Организация должна устанавливать, выполнять и поддерживать специальные для организации правила и процессы в соответствии с требованиями настоящего стандарта.

Примечание — Такие специальные для организации правила и процессы могут включать в себя создание и поддержку общего плана обеспечения безопасности и описание процесса его выполнения.

5.4.2.3 Организация должна устанавливать, выполнять и поддерживать процессы, гарантирующие, что выявленные аномалии функциональной безопасности напрямую доведены до сведения соответствующего менеджера(ов) по безопасности и других ответственных лиц.

Пример — Менеджер по безопасности клиента и менеджер по безопасности поставщика, менеджер по разработке системы безопасности соответствующего устройства.

5.4.2.4 Организация должна устанавливать, выполнять и поддерживать процесс разрешения аномалий безопасности для того, чтобы анализ, оценка, разрешение и устранение аномалий функциональной безопасности выполнялись своевременно и эффективно.

Примечание — Процесс разрешения аномалии может включать в себя анализ ее основной причины, что в дальнейшем приведет к корректирующему действию.

5.4.2.5 Во время реализации жизненного цикла системы безопасности организация должна выполнять необходимые мероприятия по обеспечению функциональной безопасности, в том числе работы по созданию необходимой документации и управлению ею в соответствии с требованиями раздела 10 ИСО 26262-8.

5.4.2.6 Организация должна предоставлять ресурсы, необходимые для достижения функциональной безопасности.

Примечание — Ресурсы включают в себя человеческие ресурсы, инструментальные средства, базы данных и шаблоны.

5.4.2.7 Организация должна устанавливать, выполнять и поддерживать непрерывный процесс совершенствования, основанный на:

- изучении опыта, накопленного в ходе реализации жизненного цикла систем безопасности других устройств, в том числе практического опыта и
- применении полученных усовершенствований в последующих устройствах.

5.4.2.8 Организация должна гарантировать, чтобы лицам, выполняющим или поддерживающим деятельность по обеспечению безопасности, были даны достаточные полномочия для выполнения своих обязанностей.

5.4.3 Компетентность руководства

5.4.3.1 Организация должна гарантировать, чтобы лица, участвующие в реализации жизненного цикла систем безопасности, имели достаточный уровень навыков, компетенции и квалификации, соответствующих их обязанностям.

Примечания

1 Одним из возможных средств для достижения достаточного уровня навыков и компетенций в разработке является программа подготовки и повышения квалификации, которая охватывает следующие области знаний:

- основные понятия, технологии и методы проектирования систем безопасности;
- настоящий стандарт и, при необходимости, дополнительные стандарты в области безопасности;
- специальные для организации правила по функциональной безопасности;
- установленные в организации процессы по функциональной безопасности.

2 Чтобы оценить навыки, компетенцию и квалификацию для осуществления деятельности в соответствии с настоящим стандартом, можно учесть опыт предыдущей профессиональной деятельности, например:

- знания об устройстве;
- знания об окружающей среде устройства;
- управленческий опыт.

5.4.4 Управление качеством в течение жизненного цикла систем безопасности

5.4.4.1 Организации, участвующие в реализации жизненного цикла системы безопасности, должны иметь действующую систему управления качеством, соответствующую стандартам управления качеством, таким как ИСО/ТС 16949, ИСО 9001 или эквивалентным.

5.4.5 Независимая от проекта настройка жизненного цикла системы безопасности

5.4.5.1 Организация может настраивать жизненный цикл системы безопасности для его применения при разработках устройств, т. е. применять независимую от проекта настройку, но если она ограничивается применением одной или нескольких из следующих процедур настройки:

a) подстадии, действия или задачи могут быть объединены или разделены или

Примечание — Отдельные подстадии могут быть объединены, если используемый метод не обеспечивает четкое разграничение между отдельными подстадиями, например, автоматизированные средства разработки могут поддерживать действия нескольких подстадий на одном шаге процесса;

b) действия или задачи могут быть выполнены на другой стадии или подстадии, или

c) действия или задачи могут быть выполнены на дополнительной стадии или подстадии или

d) стадии или подстадии могут использоваться итеративно.

5.5 Результаты работы

5.5.1 Специальные для организации правила и процедуры для функциональной безопасности

Результат 5.4.2 и 5.4.5.

5.5.2 Подтверждение компетентности

Результат 5.4.3.

5.5.3 Подтверждение менеджмента качества

Результат 5.4.4.

6 Управление созданием системы безопасности на стадиях формирования концепции и разработки изделия

6.1 Цели

Первая цель данного раздела состоит в определении ролей и обязанностей при управлении созданием системы безопасности на стадиях формирования концепции и разработки ее жизненного цикла (см. рисунок 1 и рисунок 2).

Вторая цель данного раздела состоит в определении требований к управлению созданием системы безопасности на стадиях формирования концепции и разработки, в том числе к планированию и координации действий по обеспечению безопасности, к выполнению жизненного цикла системы безопасности, к созданию обоснования безопасности и выполнению мер подтверждения.

6.2 Общие положения

Управление созданием системы безопасности включает в себя ответственность за обеспечение выполнения мер подтверждения. В зависимости от применяемого значения УПБА, некоторые меры подтверждения требуют независимости от ресурсов, управления и определения полномочий (см. 6.4.7).

Меры подтверждения включают в себя оценки подтверждения, аудиты функциональной безопасности и оценки функциональной безопасности:

- оценки подтверждения предназначены для проверки соответствия отдельных результатов работы соответствующим требованиям настоящего стандарта;
- аудит функциональный безопасности оценивает выполнение процессов, необходимых для деятельности в области функциональной безопасности;
- оценка функциональной безопасности оценивает функциональную безопасность, достигаемую устройством.

Кроме мер подтверждения, выполняются верификационные оценки. Они требуются в других частях настоящего стандарта и предназначены для проверки того, что соответствующие результаты работ удовлетворяют требованиям проекта и техническим требованиям для случаев их применения и видов отказов.

В таблице 1 перечислены необходимые меры подтверждения. В приложении D перечислены верификационные оценки и ссылки на соответствующие части настоящего стандарта.

Управление системой безопасности включает в себя ответственность за описание и обоснование любых специальных действий по обеспечению безопасности (см. 6.4.5).

6.3 Входная информация

6.3.1 Предварительные требования

Необходима следующая информация:

- специальные для организации правила и процедуры по функциональной безопасности в соответствии с требованиями 5.5.1;
- подтверждение компетентности в соответствии с требованиями 5.5.2;
- подтверждение реализации менеджмента качества в соответствии с требованиями 5.5.3.

6.3.2 Дополнительная информация

Следующая информация может быть учтена, если она доступна:

- план проекта (из внешнего источника);
- зависимости от других видов деятельности, включая другие мероприятия по обеспечению безопасности.

6.4 Требования и рекомендации

6.4.1 Общие положения

Организации, участвующие в реализации жизненного цикла системы безопасности, должны соответствовать требованиям 6.4.2—6.4.9 для устройств, которые имеют, по крайней мере, одну цель безопасности с УПБА равным A, B, C или D, если не указано иное.

6.4.2 Роли и ответственности при управлении созданием системы безопасности

6.4.2.1 Менеджер проекта должен быть назначен в начале разработки устройства.

6.4.2.2 На менеджера проекта должна быть возложена ответственность и даны полномочия в соответствии с требованиями 5.4.2.8, с тем чтобы:

a) выполнялись связанные с безопасностью мероприятия, необходимые для достижения функциональной безопасности, и

b) было достигнуто соответствие требованиям настоящего стандарта.

6.4.2.3 Менеджер проекта должен убедиться, что организация предоставила необходимые ресурсы для выполнения действий по функциональной безопасности в соответствии с требованиями 5.4.2.6.

Примечание — Оценка, определение и выделение достаточных ресурсов, как правило, выполняются на стадии планирования.

6.4.2.4 Менеджер проекта должен гарантировать, что менеджер по системе безопасности назначен в соответствии с требованиями 5.4.3.

Примечания

1 Роль менеджера по системе безопасности может выполнять менеджер проекта.

2 Термин «менеджер по системе безопасности» определяется как роль (см. ИСО 26262-1), его функции могут быть разделены между различными лицами в организации.

6.4.3 Планирование и координация деятельности по обеспечению безопасности

6.4.3.1 Менеджер по системе безопасности несет ответственность за планирование и координацию деятельности по функциональной безопасности на стадиях разработки жизненного цикла системы безопасности в соответствии с требованиями 5.4.2.8.

Примечания

1 Менеджер по системе безопасности может делегировать полномочия лицам, которые обладают необходимыми навыками, компетенцией и квалификацией (см. 5.4.3).

2 Планирование деятельности по обеспечению безопасности включено в план обеспечения безопасности (см. 6.4.3.5). Некоторые запланированные мероприятия по обеспечению безопасности более подробно представлены в результатах работы других частей настоящего стандарта (см. 6.4.3.3).

3 В зависимости от того, разрабатывается ли новое устройство или оно является модификацией уже существующего устройства (см. раздел 6 ИСО 26262-3), объем работ по обеспечению безопасности и их планирование могут меняться.

6.4.3.2 Менеджер по системе безопасности несет ответственность за выполнение плана по обеспечению безопасности, а также контролирует процесс деятельности по обеспечению безопасности в соответствии с планом по обеспечению безопасности.

6.4.3.3 В соответствии с требованиями 5.4.2.8 и 5.4.3 в перечисленных ниже планах, которые передаются в организации, должны быть определены обязанности, связанные с конкретизацией и координацией деятельности по обеспечению безопасности:

- план интеграции и тестирования устройства в соответствии с требованиями ИСО 26262-4;
- план подтверждения соответствия в соответствии с требованиями ИСО 26262-4;

- план верификации программного обеспечения в соответствии с требованиями ИСО 26262-6;
- план оценки функциональной безопасности в соответствии с требованиями 6.4.9.

Лицо, которому была назначена такая ответственность, должно также нести ответственность за выполнение соответствующего плана и контролировать выполнение работ в соответствии с планом.

6.4.3.4 План по обеспечению безопасности должен быть либо

a) планом, на который имеется ссылка в плане проекта, либо

b) включен в план проекта так, чтобы мероприятия по обеспечению безопасности были представлены в проекте.

Примечание — План по обеспечению безопасности может включать перекрестные ссылки на другую информацию при управлении конфигурацией (см. раздел 7 ИСО 26262-8). Перекрестные ссылки, как правило, предпочтительнее параллельному описанию действий в различных результатах работ или в других документах, управляемых конфигурацией.

6.4.3.5 План по обеспечению безопасности должен включать:

a) планирование действий и процедур для достижения функциональной безопасности;

b) реализацию независимых от проекта действий в области безопасности в соответствии с требованиями раздела 5 в управление созданием системы безопасности конкретного проекта;

c) определение адаптации действий по обеспечению безопасности в соответствии с требованиями 6.4.5, если это применимо;

d) планирование анализа опасностей и оценку рисков в соответствии с требованиями раздела 7 ИСО 26262-3;

e) планирование действий по разработке, включая разработку и реализацию концепции функциональной безопасности в соответствии с требованиями раздела 8 ИСО 26262-3, разработку изделия на системном уровне в соответствии с требованиями ИСО 26262-4, разработку аппаратных средств изделия в соответствии с требованиями ИСО 26262-5 и разработку программного обеспечения изделия в соответствии с требованиями ИСО 26262-6;

f) планирование соглашения об интерфейсе разработки (СИР) в соответствии с требованиями раздела 5 ИСО 26262-8, если применимо;

g) планирование вспомогательных процессов в соответствии с требованиями ИСО 26262-8;

h) планирование действий по верификации в соответствии с требованиями ИСО 26262-3, ИСО 26262-4, ИСО 26262-5, ИСО 26262-6 и раздела 9 ИСО 26262-8:2011, а также планирование мероприятий по подтверждению соответствия безопасности в соответствии с требованиями раздела 9 ИСО 26262-4.

Примечание — Действия по верификации подробно описаны в плане интеграции и тестирования устройства (см. ИСО 26262-4) и в плане верификации программного обеспечения (см. ИСО 26262-6). Действия по подтверждению соответствия подробно описаны в плане подтверждения соответствия (см. ИСО 26262-4). См. также 6.4.3.3;

i) планирование выполнения оценок подтверждения, аудита(ов) функциональной безопасности и оценки функциональной безопасности в соответствии с требованиями 6.4.7 до 6.4.9.

Примечание — Уровень независимости, приведенный в 6.4.7, а также квалификация, приведенная в 5.4.3, лиц, осуществляющих меры подтверждения, указываются в плане по обеспечению безопасности;

j) планирование анализа зависимых отказов в соответствии с требованиями раздела 7 ИСО 26262-9, если это применимо, и анализов системы безопасности в соответствии с требованиями раздела 8 ИСО 26262-9;

k) обеспечение подтверждений проверкой в эксплуатации кандидатов в соответствии с требованиями раздела 14 ИСО 26262-8, если это применимо; и

l) обеспечение уверенности в использовании инструментальных средств программного обеспечения в соответствии с требованиями раздела 11 ИСО 26262-8, если это применимо.

6.4.3.6 Планирование деятельности по обеспечению безопасности должно включать описание:

a) цели;

b) зависимостей от других видов действий или информации;

c) ресурсов, отвечающих за выполнение деятельности;

d) ресурсов, необходимых для осуществления деятельности;

e) даты начала и длительности, а также

f) идентификации соответствующего результата работы.

6.4.3.7 Данное требование должно быть выполнено для устройств, которые имеют, по крайней мере, одну цель безопасности со значением УПБА, равным B, C или D. План обеспечения безопасности в

соответствии с требованиями 6.4.3.1 до 6.4.3.6 должен быть утвержден уполномоченным лицом, которое должно рассмотреть оценку подтверждения плана обеспечения безопасности в соответствии с требованиями 6.4.7.

6.4.3.8 Выявленные аномалии системы безопасности должны быть доведены до сведения менеджера по безопасности и других ответственных лиц в соответствии с требованиями 5.4.2.3.

Примечание — Изменения, появившиеся в результате устранения аномалий в системе безопасности, поступают на вход процесса управления изменениями (см. раздел 8 ИСО 26262-8).

6.4.4 Выполнение жизненного цикла систем безопасности

6.4.4.1 Действия по обеспечению безопасности на следующей подстадии жизненного цикла системы безопасности должно начинаться только при наличии достаточной информации от имеющих отношение к ней подстадий.

Примечание — Информация может рассматриваться как достаточная, если ее отсутствие не вызывает неприемлемый риск достижения устройством цели безопасности.

6.4.4.2 Результаты работы, требуемые планом по обеспечению безопасности, должны быть обеспечены управлением конфигурацией, управлением изменениями и документально оформлены в соответствии с требованиями разделов 7, 8 и 10 ИСО 26262-8, соответственно, не позднее начала стадии «разработки изделия на уровне системы» (см. рисунок 1).

6.4.5 Настройка действий по обеспечению безопасности

6.4.5.1 Деятельность по обеспечению безопасности с учетом специфики разрабатываемого устройства может быть настроена, т. е. что-то может быть исключено или что-то добавлено. Если деятельность по обеспечению безопасности настраивается, то:

a) ее настройка должна быть определена в плане обеспечения безопасности (см. перечисление c) п. 6.4.3.5) и

b) должно быть доступно обоснование того, почему такая настройка является адекватной и достаточной для достижения функциональной безопасности.

Примечания

1 Обоснование учитывает значения УПБА соответствующих требований.

2 Обоснование настройки включается в план обеспечения безопасности и рассматривается в ходе оценки подтверждения плана обеспечения безопасности (см. 6.4.7) или во время оценки функциональной безопасности (см. 6.4.9).

3 Данное требование распространяется на настройку, которая применяется для конкретного устройства. Если выполняется настройка жизненного цикла системы безопасности, применяемого в рамках организации для разработки устройств, то применяются только требования п. 5.4.5.

6.4.5.2 Если деятельность по обеспечению безопасности настраивается в соответствии с 6.4.5.1 в результате изменения существующего устройства, то должны соблюдаться требования раздела 6 ИСО 26262-3.

6.4.5.3 Если деятельность по обеспечению безопасности настраивается в соответствии с 6.4.5.1 в результате имеющегося подтверждения проверкой в эксплуатации, то должны соблюдаться требования раздела 14 ИСО 26262-8.

6.4.5.4 Если деятельность по обеспечению безопасности настраивается в соответствии с 6.4.5.1 в результате декомпозиции УПБА, то должны соблюдаться требования раздела 5 ИСО 26262-9.

6.4.5.5 Если деятельность по обеспечению безопасности настраивается в соответствии с 6.4.5.1 на базе обоснования, которое рассматривает уверенность в использовании инструментального программного обеспечения, то должны соблюдаться требования раздела 11 ИСО 26262-8.

6.4.5.6 Если деятельность по обеспечению безопасности настраивается в соответствии с 6.4.5.1 из-за того, что элемент разработан отдельно от устройства, то:

a) разработка элемента отдельно от устройства должна быть основана на спецификации требований, которая выводится из предположений о целевом применении и контексте элемента, включая его внешние интерфейсы, а также

b) должна быть установлена обоснованность предположений о целевом применении и контексте элемента, разработанного отдельно от устройства.

Примечание — Настоящий стандарт в целом не может быть применен к элементу, разработанному отдельно от устройства, так как функциональная безопасность не является свойством элемента (однако, элемент устройства может быть идентифицирован как связанный с безопасностью). Функциональная безопасность является свойством устройства и может быть оценена средствами оценки функциональной безопасности.

Пример — Микроконтроллер разработан отдельно от устройства.

6.4.6 Обоснование безопасности

6.4.6.1 В соответствии с планом по обеспечению безопасности должно быть разработано обоснование безопасности. Данное требование должно быть выполнено для устройств, которые имеют, по крайней мере, одну цель безопасности со значением УПБА, равным (A), B, C или D.

6.4.6.2 Для формирования обоснования безопасности следует постепенно собирать результаты работы, которые создаются в течение жизненного цикла системы безопасности.

6.4.7 Меры подтверждения: виды, независимость и полномочие

6.4.7.1 Меры подтверждения, указанные в таблице 1, должны быть выполнены в соответствии с требуемым уровнем независимости (см. таблицу 2, перечисление i) 6.4.3.5, 6.4.8 и 6.4.9).

Примечания

1 Оценка подтверждения выполняется для тех результатов работ, которые указаны в таблице 1 и требуются планом обеспечения безопасности.

2 Оценка подтверждения включает в себя проверку правильности соблюдения установленных норм и правил, содержания, адекватности и полноты относительно требований настоящего стандарта.

3 Таблица 1 включает в себя меры подтверждения. Анализ верификационных оценок приводится в приложении D.

4 Отчет, который формируется в результате выполнения меры подтверждения, включает в себя имя и номер версии проанализированных документов о результатах работы или процессах (см. 10.4.5 ИСО 26262-8).

5 Если после завершения выполнения оценки подтверждения или оценки функциональной безопасности следуют изменения в устройстве, то эти процедуры должны быть выполнены повторно или добавлены (см. 8.4.5.2 ИСО 26262-8).

6 Цели каждой меры подтверждения приведены в приложении C.

7 Такие меры подтверждения, как оценки подтверждения и аудиты функциональной безопасности, могут быть объединены и в сочетании с оценкой функциональной безопасности могут быть использованы при создании сопоставимых вариантов устройства.

Таблица 1 — Требуемые меры подтверждения с учетом требуемого уровня независимости

Меры подтверждения	Степень независимости[a)] применятся к УПБА				Область применения
	A	B	C	D	
Оценка подтверждения анализа опасностей и оценки рисков устройства (разделы 5 и 7 ИСО 26262-3 и, если применимо, п. 5 ИСО 26262-8). Выполняется независимо от разработчиков устройства, управления проектом и авторов результатов работы	I3	I3	I3	I3	Область применения данной оценки должна включать правильность определения значений УПБА и правильность определения оценок опасных событий для устройства, выявленных системой менеджмента качества (QM), а также оценку целей безопасности
Оценка подтверждения плана по обеспечению безопасности (6.5.1). Выполняется независимо от разработчиков устройства, управления проектом и авторов результатов работы	—	I1	I2	I3	Применяется к цели безопасности устройства с самым высоким значением УПБА
Оценка подтверждения плана по интеграции и тестированию устройства (ИСО 26262-4). Выполняется независимо от разработчиков устройства, управления проектом и авторов результатов работы	I0	I1	I2	I2	Применяется к цели безопасности устройства с самым высоким значением УПБА
Оценка подтверждения плана подтверждения соответствия (ИСО 26262-4). Выполняется независимо от разработчиков устройства, управления проектом и авторов результатов работы	I0	I1	I2	I2	Применяется к цели безопасности устройства с самым высоким значением УПБА

Окончание таблицы 1

Меры подтверждения	Степень независимости[a] применятся к УПБА				Область применения
	A	B	C	D	
Оценка подтверждения видов анализа системы безопасности (раздел 8 ИСО 26262-9). Выполняется независимо от разработчиков устройства, управления проектом и авторов результатов работы	I1	I1	I2	I3	Применяется к цели безопасности устройства с самым высоким значением УПБА
Оценка подтверждения отчета о критериях оценки инструментального программного обеспечения и отчета о квалификации[b] инструментального программного обеспечения (раздел 11 ИСО 26262-8). Выполняется независимо от персонала, выполняющего квалифицирование инструментального программного обеспечения	—	I0	I1	I1	Применяется к требованиям, имеющим самое высокое значение УПБА, которые могут быть нарушены используемым инструментальным программным обеспечением
Оценка подтверждения проверкой эксплуатацией (видов анализа, данных и доверия) кандидатов (раздел 14 ИСО 26262-8). Выполняется независимо от автора подтверждения	I0	I1	I2	I3	Применяется к УПБА цели безопасности, либо к требованию, относящемуся к рассматриваемому поведению, либо функции кандидата
Оценка подтверждения полноты обоснования безопасности (6.5.3). Выполняется независимо от автора обоснования безопасности	I0	I1	I2	I3	Применяется к цели безопасности устройства с самым высоким значением УПБА
Аудит функциональной безопасности в соответствии с 6.4.8. Выполняется независимо от разработчиков устройств и управления проектом	—	I0	I2	I3	Применяется к цели безопасности устройства с самым высоким значением УПБА
Оценка функциональной безопасности в соответствии с 6.4.9. Выполняется независимо от разработчиков устройств и управления проектом	—	I0	I2	I3	Применяется к цели безопасности устройства с самым высоким значением УПБА

[a] Обозначения определены следующим образом:

— — требования или рекомендации за или против данной меры подтверждения отсутствуют;

I0 — мера подтверждения должна быть выполнена; однако, если данная мера подтверждения осуществляется, то она должна быть выполнена другим лицом;

I1 — мера подтверждения должна быть выполнена другим лицом;

I2 — мера подтверждения выполняется лицом из другой команды, то есть не подчиняющимся тому же самому непосредственному начальнику;

I3 — мера подтверждения выполняется лицом из другого отдела или организации, т. е. лицом, независимым от департамента, отвечающего за рассматриваемые результаты работы, организацию их выполнения, используемые ресурсы и определение полномочий.

[b] Разработка инструментальных средств программного обеспечения выполняется вне рамок жизненного цикла системы безопасности, реализуемой устройством, но квалификация таких инструментальных средств является деятельностью, выполняемой на жизненном цикле разрабатываемой системы безопасности.

Таблица 2 — Требования к процедурам, реализующим меры подтверждения

Тема	Оценка подтверждения	Аудит функциональной безопасности	Оценка функциональной безопасности
Предмет оценки	Результат работы	Осуществление процессов, необходимых для функциональной безопасности	Оценка устройства согласно его определению, представленному в соответствии с требованиями раздела 5 ИСО 26262-3
Результат	Отчет об оценке подтверждения	Отчет[a)] об аудите функциональной безопасности в соответствии с 6.4.8	Отчет об оценке функциональной безопасности в соответствии с 6.4.9
Обязанность людей, выполняющих меру подтверждения	Оценка соответствия результата работы с соответствующими требованиями настоящего стандарта	Оценка выполнения требуемых процессов	Оценка достигнутой функциональной безопасности. Предоставление рекомендаций для принятия, условное принятие или отказ в соответствии с 6.4.9.6
Временная привязка к процессам жизненного цикла системы безопасности	После завершения соответствующей деятельности по обеспечению безопасности. Завершение перед запуском в производство	Во время выполнения необходимых процессов	Постепенно в процессе разработки или для отдельного блока. Завершение перед запуском в производство
Область применения и глубина	В соответствии с планом по обеспечению безопасности	Выполнение процессов соответствующих определениям действий, на которые есть ссылка или которые определены в плане по обеспечению безопасности	Результаты работы, задаваемые планом по обеспечению безопасности, реализация требуемых процессов и оценка реализованных мер безопасности, которые могут быть оценены в ходе разработки устройства
[a)] Данный отчет может быть включен в отчет об оценке функциональной безопасности.			

6.4.7.2 Лица, осуществляющие меры подтверждения, должны иметь доступ к лицам и подразделениям организации (а также должны быть поддержаны ими), которые осуществляют мероприятия по обеспечению безопасности во время разработки устройства.

6.4.7.3 Лица, осуществляющие меры подтверждения, должны иметь доступ к соответствующей информации и инструментальным средствам.

6.4.8 Аудит функциональной безопасности

6.4.8.1 Аудит функциональной безопасности для устройств, у которых наибольшее значение УПБА их целей безопасности равно (B), C или D, должен быть выполнен в соответствии с 6.4.7, перечислением i) 6.4.3.5 и 6.4.8.2.

6.4.8.2 Одно или несколько лиц назначаются для выполнения одного или более аудитов функциональной безопасности в соответствии с 5.4.3. Назначенные лица должны представить отчет, содержащий оценку выполнения процессов, необходимых для функциональной безопасности.

Примечания

1 Если аудит функциональной безопасности осуществляется экспертом SPICE (Software Process Improvement and Capability Determination), то этот аудит функциональной безопасности и оценка SPICE (см. ИСО/МЭК 15504) могут быть выполнены одновременно. Содержательно настоящий стандарт и SPICE имеют достаточно много общего, поэтому можно запланировать их синхронное выполнение. Если синхронизацию удалось запланировать, то эксперт SPICE может обеспечить обратную связь аудитору функциональной безопасности. Однако SPICE-оценка может быть синхронизирована с проверкой некоторого вспомогательного процесса, специфицированного в ИСО 26262-8, но ее недостаточно для выполнения оценки функциональной безопасности (см. 6.4.9).

2 Определения процессов организации можно найти сразу в нескольких стандартах, например, в настоящем стандарте и SPICE-требования к процессу управления конфигурацией. Такая координация процессов может помочь избежать дублирования работ или несоответствий процесса. Для таких скоординированных процессов может быть создан специальный для организации процесс перекрестных ссылок к требованиям настоящего стандарта и SPICE.

6.4.9 Оценка функциональной безопасности

6.4.9.1 Оценка функциональной безопасности для устройств, у которых наибольшее значение УПБА их целей безопасности равно (B), C или D, должна выполняться в соответствии с 6.4.7 и 6.4.9.2—6.4.9.8.

6.4.9.2 Оценка функциональной безопасности должна планироваться в соответствии с 6.4.3.3 и перечислением i) 6.4.3.5.

Пример — Программа для оценки функциональной безопасности приведена в приложении E.

6.4.9.3 В соответствии с 5.4.3 для выполнения оценки функциональной безопасности назначается одно или несколько лиц. Назначенные лица должны представить отчет, содержащий заключение о достижении функциональной безопасности.

6.4.9.4 Область применения оценки функциональной безопасности должна включать:

- результаты работы, требуемые планом по обеспечению безопасности;
- процессы, необходимые для функциональной безопасности.

Примечание — Оценка выполняемых процессов может быть основана на результатах аудита(ов) функциональной безопасности;

- рассмотрение целесообразности и эффективности выполняемых мер безопасности, которые могут быть оценены в ходе разработки устройства.

Примечание — Меры безопасности, которые должны быть реализованы в процессе подстадии производства, но которые не могут быть оценены в ходе разработки устройства, оцениваются в сочетании с возможностями производственного процесса (см. пункт 5.4.2.2 ИСО 26262-7).

6.4.9.5 Оценка функциональной безопасности должна рассматривать следующие вопросы:

a) планирование других мер подтверждения [см. перечисление i) 6.4.3.5];

b) результаты оценок подтверждения и аудита(ов) функциональной безопасности и

c) рекомендацию(и), полученную(ых) в результате предыдущей(их) оценки(ок) функциональной безопасности, если применимо (см. пункты 6.4.9.7, 6.4.9.8 и 8.4.5.2 ИСО 26262-8).

6.4.9.6 Отчет об оценке функциональной безопасности в соответствии с 6.4.9.3 должен включать в себя рекомендации по принятию, условному принятию или отказу в достижении функциональной безопасности устройством. В случае условного принятия:

a) условное принятие должно быть дано только в том случае, если функциональная безопасность устройства считается очевидной, несмотря на выявленные открытые вопросы и

b) рекомендация для условного принятия будет включать отклонения от критериев оценки функциональной безопасности и обоснования, почему эти конкретные отклонения считаются приемлемыми.

6.4.9.7 Если рекомендацией, содержащейся в отчете об оценке функциональной безопасности в соответствии с 6.4.9.6, является условное принятие достигнутой функциональной безопасности, то должны быть выполнены корректирующие действия, предусмотренные в отчете об оценке функциональной безопасности.

6.4.9.8 Если рекомендацией, содержащейся в отчете об оценке функциональной безопасности в соответствии с 6.4.9.6, является отказ в достижении функциональной безопасности, то:

a) должны быть запущены адекватные корректирующие действия и

b) оценка функциональной безопасности должна быть выполнена повторно.

6.5 Результаты работы

6.5.1 План по обеспечению безопасности

Результат 6.4.3—6.4.5.

6.5.2 План проекта (уточненный)

Результат 6.4.3.4.

6.5.3 Обоснование безопасности

Результат 6.4.6.

6.5.4 План оценки Функциональной безопасности

Результат 6.4.9.

6.5.5 Отчеты о мерах подтверждения

Результат 6.4.7—6.4.9.

7 Управление созданием системы безопасности после запуска устройства в производство

7.1 Цель

Целью настоящего раздела является определение ответственности организаций и лиц, ответственных за функциональную безопасность после запуска устройства в производство. Это относится к общим действиям для обеспечения требуемой функциональной безопасности данного устройства в течение подстадий жизненного цикла после запуска его в производство.

7.2 Общие положения

См. 5.2.

7.3 Входная информация

7.3.1 Предварительные требования

Следующая информация должна быть доступна:

- подтверждение менеджмента качества в соответствии с требованиями 5.5.3.

7.3.2 Дополнительная информация

Не задается.

7.4 Требования и рекомендации

7.4.1 Общие положения

Организации, участвующие в выполнении жизненного цикла системы безопасности, должны соответствовать требованиям 7.4.2 для устройств, которые имеют, по крайней мере, одну цель безопасности со значением УПБА, равным A, B, C или D.

7.4.2 Обязанности, планирование и необходимые процессы

7.4.2.1 Организация должна назначить лиц, возлагая на них обязанности и предоставляя им соответствующие полномочия в соответствии с требованиями 5.4.2.8, для обеспечения функциональной безопасности устройства после его запуска в производство.

7.4.2.2 Мероприятия по обеспечению функциональной безопасности устройства после его запуска в производство должны планироваться в соответствии с требованиями ИСО 26262-7 и должны быть инициированы в процессе разработки изделия на уровне системы в соответствии с требованиями ИСО 26262-4.

7.4.2.3 Организация должна устанавливать, выполнять и поддерживать процессы в целях поддержания функциональной безопасности устройства на стадиях его жизненного цикла после запуска в производство.

7.4.2.4 Организация должна устанавливать, выполнять и поддерживать контроль функциональной безопасности устройства в процессе его эксплуатации.

Примечания

1 Процесс контроля системы безопасности за инцидентами в процессе ее эксплуатации включает в себя предоставление отчетов об инцидентах, меры по их исправлению, например, возврат, равно как и другие соответствующие процессы принятия решений.

2 Собранные в результате контроля в процессе эксплуатации данные могут быть использованы для подтверждения проверкой в эксплуатации (см. раздел 14 ИСО 26262-8).

7.4.2.5 Если в устройстве произошли изменения после его запуска в производство, то в соответствии с требованиями раздела 11 ИСО 26262-4 запуск его в производство необходимо повторить.

Примечание — Эти изменения выполняются процедурой управления изменениями (см. раздел 8 ИСО 26262-8).

7.5 Результаты работы

7.5.1 Подтверждение контроля в процессе эксплуатации

Результат 7.4.2.4.

Приложение А
(справочное)

Обзор и последовательность выполняемых работ менеджмента функциональной безопасностью

Таблица А.1 содержит обзор целей, предварительных требований и результатов работы конкретных стадий менеджмента функциональной безопасностью.

Таблица А.1 — Менеджмент функциональной безопасности: обзор

Раздел	Цели	Предварительные требования	Результаты работы
5 Общие требования к управлению созданием системы безопасности	Целью раздела 5 является определение требований к организациям, которые отвечают за реализацию жизненного цикла системы безопасности или которые выполняют мероприятия по обеспечению безопасности на различных стадиях жизненного цикла системы безопасности. Полученная в соответствии с разделом 5 информация служит в качестве предварительных требований к действиям, выполняемым на различных стадиях представленного в настоящем стандарте жизненного цикла системы безопасности	Не задаются	5.5.1 Специальные для организации правила и процедуры для функциональной безопасности. 5.5.2 Подтверждение компетентности. 5.5.3 Подтверждение менеджмента качества
6 Управление созданием системы безопасности на стадиях формирования концепции и разработки изделия	Первая цель раздела 6 состоит в определении ролей и обязанностей при управлении созданием системы безопасности на стадиях формирования концепции и разработки изделия ее жизненного цикла. Вторая цель раздела 6 состоит в определении требований к управлению созданием системы безопасности на стадиях формирования концепции и разработки, в том числе к планированию и координации деятельности по обеспечению безопасности, к выполнению жизненного цикла системы безопасности, к созданию обоснования безопасности и к выполнению мер подтверждения	Специальные для организации правила и процедуры по функциональной безопасности (см. 5.5.1). Подтверждение компетентности (см. 5.5.2). Подтверждение реализации менеджмента качества (см. 5.5.3)	6.5.1 План по обеспечению безопасности. 6.5.2 План проекта (уточненный). 6.5.3 Обоснование безопасности. 6.5.4 План оценки функциональной безопасности. 6.5.5 Отчеты о мерах подтверждения
7 Управление созданием системы безопасности после запуска устройства в производство	Целью раздела 7 является определение ответственности организаций и лиц, ответственных за функциональную безопасность после запуска устройства в производство. Это относится к общим действиям для обеспечения требуемой функциональной безопасности данного устройства в течение подстадий жизненного цикла после запуска его в производство	Подтверждение менеджмента качества (см. 5.5.3)	7.5.1 Подтверждение контроля в процессе эксплуатации

Приложение В
(справочное)

Примеры оценки культуры реализации системы безопасности

Таблица В.1 — Примеры оценки культуры реализации системы безопасности

Примеры, свидетельствующие о низкой культуре реализации системы безопасности	Примеры, свидетельствующие о высокой культуре реализации системы безопасности
Ответственность не прослеживается	Процесс гарантирует, что ответственность за решения, связанные с функциональной безопасностью, прослеживается
Стоимость и график работ всегда имеет преимущество перед безопасностью и качеством	Безопасность является главным приоритетом
Система вознаграждения отдает предпочтение стоимости и графику работ, а не безопасности и качеству	Системы вознаграждения поддерживают и мотивируют эффективное достижение функциональной безопасности. Системы вознаграждения наказывает тех, кто обходит вопросы, которые ставят под угрозу безопасность или качество
Персонал, выполняющий оценку безопасности, качества и управление этими процессами, находится под чрезмерным влиянием лица, ответственного за выполнение процессов	Процесс обеспечивает адекватную систему сдержек и противовесов, например, соответствующий уровень независимости в интегральных процессах (безопасности, качества, подтверждения соответствия, верификации и управления конфигурацией)
Пассивное отношение к безопасности, например: - сильная зависимость от тестирования в конце цикла разработки изделия; - менеджмент реагирует только тогда, когда есть проблемы при эксплуатации	Активное отношение к безопасности, например, проблемы безопасности и качества выявляются и исправляются на самом раннем этапе жизненного цикла изделия
Необходимые ресурсы не планируются или не выделяются своевременно	Необходимые ресурсы распределяются. Квалификация персонала имеет компетенцию, соответствующую порученной деятельности
«Групповое мышление». «Подтасовывание карт» при формировании групп для оценки. Несогласные подвергаются остракизму или помечаются как «некомандный игрок». Инакомыслие негативно отражается на оценках работы. Лицо из «инакомыслящего меньшинства» отмечается или рассматривается как «нарушитель спокойствия», «некомандный игрок» или «осведомитель». Обеспокоенные сотрудники боятся последствий	Процесс использует преимущества разнообразия: - интеллектуальное разнообразие ищут, ценят и включают во все процессы; - поведение, мешающее использованию разнообразия, не приветствуется и наказывается. Существуют каналы поддержки коммуникации и принятия решений и менеджмент поощряет их использование: - рекомендуется свободное общение; - обнародование полученных кем-либо результатов поощряется; - процесс получения результатов и решения проблем продолжается при эксплуатации
Не систематизированы процессы непрерывного совершенствования, учебные циклы или другие формы «извлеченных уроков»	Непрерывное совершенствование является неотъемлемой частью всех процессов
Процессы «для данного случая» или неявные	Определенные, прослеживаемые и управляемые процессы выполняются на всех уровнях, включая процессы: - управления; - технические; - разработки интерфейсов; - верификации; - подтверждения соответствия; - аудита функциональной безопасности; - оценки функциональной безопасности

Приложение С
(справочное)

Цель мер подтверждения

С.1 Оценка плана по обеспечению безопасности

С.1.1 Оценка соответствия плана по обеспечению безопасности жизненному циклу системы безопасности, представленному в настоящем стандарте. Если это применимо, то оценка настройки действий по обеспечению безопасности, т. е. сравнение действий по обеспечению безопасности, которые пропущены или выполнены другим способом, с базовым жизненным циклом системы безопасности, включая соответствующие обоснования (см. 6.4.5).

С.1.2 Оценка соответствия плана по обеспечению безопасности требованиям настоящего стандарта по планированию деятельности по обеспечению безопасности (см. 6.4.3—6.4.5).

С.2 Оценка полноты обоснования безопасности (см. 6.5.3)

С.2.1 Подтверждение того, что результаты работы, указанные в обосновании безопасности, доступны и настолько полны, что достижение устройством функциональной безопасности может быть правильно оценено.

Примечание — Эти указанные результаты работы могут быть результатами работы, которые определены как имеющие отношение к поддержке обоснования безопасности.

С.2.2 Подтверждение того, что результаты работы, указанные в обосновании безопасности:

- прослеживаются от одного к другому;
- не имеют никаких противоречий внутри или между результатами работы;
- либо не имеют нерешенных вопросов, которые могут привести к нарушению цели безопасности, либо имеют только такие нерешенные вопросы, которые находятся под контролем и существует план для их решения.

С.3 Аудит функциональной безопасности (см. 6.4.8 и 6.5.5)

Оценка выполнения процессов, связанных с функциональной безопасностью, во время выполнения этих процессов относительно определений действий, на которые имеется ссылка или которые указаны в плане по обеспечению безопасности.

С.4 Оценка функциональной безопасности (см. 6.4.9 и 6.5.5)

С.4.1 Оценка соответствия результатов работы, задаваемых планом по обеспечению безопасности, требованиям настоящего стандарта, включая (но не ограничиваясь) результаты работы, для которых необходима оценка подтверждения. Для последних результатов работы результаты оценок подтверждения также учитываются.

С.4.2 Оценка выполнения процессов, обеспечивающих функциональную безопасность, с учетом результатов проведенного аудита(ов) функциональной безопасности (см. 6.4.8).

С.4.3 Рассмотрение целесообразности и эффективности реализованных мер безопасности, которые могут быть оценены в ходе разработки устройства.

С.4.4 Следование рекомендациям, вытекающим из результатов предыдущих оценок функциональной безопасности, включая любые выполненные корректирующие действия, если они применимы (см. 6.4.9.7 и 6.4.9.8).

С.5 Оценка результатов анализа опасности и оценки рисков (см. раздел 7 ИСО 26262-3, и, если применим, раздел 5 ИСО 26262-8)

Оценка полноты результатов анализа опасности и оценки рисков, а также правильности определения УПБА (включая оценку качества) и целей безопасности, учитывая процедуру анализа опасности и оценки риска, рассматриваемую в настоящем стандарте.

С.6 Оценка плана интеграции и тестирования устройства (см. ИСО 26262-4)

Оценка соответствия плана интеграции и тестирования устройства требованиям к интеграции и тестированию настоящего стандарта.

С.7 Оценка плана подтверждения соответствия (см. ИСО 26262-4)

Оценка соответствия плана подтверждения соответствия требованиям настоящего стандарта к мероприятиям по подтверждению соответствия безопасности системы.

С.8 Оценка подтверждений проверкой эксплуатацией кандидатов (см. раздел 14 ИСО 26262-8), если это применимо

С.8.1 Оценка, определяющая, обосновываются ли заявленные значения доверия проверке эксплуатацией кандидатов результатами выполненных для них различных видов анализа (с учетом любых действий по обеспечению безопасности, связанных с настройкой).

С.8.2 Оценка эффективности контроля в процессе эксплуатации.

С.8.3 Оценка изменений кандидата, которые рассматриваются при подтверждении проверкой эксплуатацией.

С.9 Оценка доклада по оценке критериев инструментальных средств программного обеспечения и доклада о квалификации инструментальных средств программного обеспечения (см. раздел 11 ИСО 26262-8)

С.9.1 Подтверждение правильной оценки требуемого уровня уверенности в инструментальном(ых) средстве(ах) программного обеспечения, используемых для разработки устройства или связанного с безопасностью элемента.

С.9.2 Оценка квалификации инструментальных(ого) средств(а) программного обеспечения с учетом требуемого уровня уверенности в соответствующих инструментальных средствах программного обеспечения.

С.10 Оценка видов анализа системы безопасности (см. раздел 8 ИСО 26262-9)

Оценка правильности выполнения различных видов анализа системы безопасности, идентифицирующих сбои или неадекватные механизмы системы безопасности, которые могут привести к нарушению цели безопасности.

Приложение D
(справочное)

Обзор верификационных оценок

Таблица D.1 содержит перечень верификационных оценок, которые требуются в других частях ИСО 26262 (см. также раздел 9 ИСО 26262-8).

Таблица D.1 — Необходимые верификационные оценки

Тема верификационной оценки	Наибольшее значение УПБА, характеризующее цели безопасности устройства				Раздел, в котором требуется или рекомендуется отчет
	A	B	C	D	
Анализ опасностей и оценка рисков устройства (см. разделы 5 и 7 ИСО 26262-3, и, если применимо, раздел 5 ИСО 26262-8)	Требуется[a]				Раздел 7 ИСО 26262-3
Цели системы безопасности	Требуется				Раздел 7 ИСО 26262-3
Концепция функциональной безопасности	Требуется				Раздел 8 ИСО 26262-3
Спецификация технических требований системы безопасности	Требуется				Раздел 6 ИСО 26262-4
Проектирование на уровне системы	Требуется				Раздел 7 ИСО 26262-4
Требования к техническим средствам системы безопасности	Требуется				Раздел 6 ИСО 26262-5
Проектирование технических средств	Требуется				Раздел 7 ИСО 26262-5
Результаты прикладных методов для оценки метрик архитектуры аппаратных средств	b)	Рекомендуется	Требуется	Требуется	Раздел 8 ИСО 26262-5
Анализ возможных нарушений цели системы безопасности из-за случайных отказов аппаратных средств, с учетом применяемого метода оценки	b)	Рекомендуется	Требуется	Требуется	Раздел 9 ИСО 26262-5
Требования к программному обеспечению системы безопасности и к уточненному программно-аппаратному интерфейсу	Требуется				Разделы 6 и 11 ИСО 26262-6
Проектирование архитектуры программного обеспечения	Требуется				Раздел 7 ИСО 26262-6
Проектирование и реализация модуля программного обеспечения	Требуется				Раздел 8 ИСО 26262-6
Протокол о квалификации компонента программного обеспечения	Требуется для квалифицируемых компонентов программного обеспечения				Раздел 12 ИСО 26262-8
Протокол о квалификации компонента технических средств	Требуется для квалифицируемых компонентов технических средств				Раздел 13 ИСО 26262-8
Различные виды анализа системы безопасности	Требуется				Раздел 8 ИСО 26262-9

[a] Область применения данного отчета включает также опасные события, оцененные как QM.
[b] Никаких требований и рекомендаций ни за, ни против.

Приложение Е
(справочное)

Пример программы оценки функциональной безопасности (для устройств, цель системы безопасности которых имеет значение УПБА, равное D)

Е.1 Менеджмент системы безопасности

Е.1.1 Применение в организации культуры безопасности и вспомогательных процессов при оценке проекта.

Е.1.2 Применение управления компетенцией и практикой непрерывного совершенствования при оценке проекта.

Е.1.3 Роли и ответственность при оценке проекта.

Е.1.4 План по обеспечению безопасности оцениваемого проекта и планирование распределенной разработки.

Е.1.5 Настройка жизненного цикла системы безопасности, в том числе подтверждение проверкой в эксплуатации кандидатов оцениваемого проекта.

Е.1.6 Аудиты функциональной безопасности, обоснование безопасности и доступные документы.

Е.2 Действия по обеспечению безопасности на стадии формирования концепции

Е.2.1 Определение устройства.

Е.2.2 Анализ опасностей и оценка рисков.

Е.2.3 Концепция функциональной безопасности.

Е.2.4 Зависимости устройства и его концепции безопасности от других систем или функций.

Е.2.5 Распределение требований функциональной безопасности между:

- Э/Э элементами;
- элементами, основанными на других технологиях;
- интерфейсами с внешними мерами.

Е.2.6 Верификация концепции функциональной безопасности.

Е.3 Действия по обеспечению безопасности на стадии разработки системы

Е.3.1 Планирование разработки, интеграции и подтверждение соответствия системы.

Е.3.2 Техническая концепция системы безопасности и ее верификация.

Е.3.3 Проектирование системы и предотвращение систематических отказов.

Е.3.4 Распределение технических требований к безопасности элементов аппаратных средств и программного обеспечения и оценка программно-аппаратного интерфейса.

Е.3.5 Верификация проекта системы.

Е.4 Разработка аппаратных средств

Е.4.1 Планирование разработки, квалификации и интеграции аппаратных средств.

Е.4.2 Требования к безопасности аппаратных средств, проектирование и верификация аппаратных средств.

Е.4.3 Ограничения архитектуры аппаратных средств.

Е.4.4 Оценка вероятности нарушения целей безопасности случайными отказами аппаратных средств.

Е.4.5 Интеграция и тестирование аппаратных средств.

Е.5 Разработка программного обеспечения

Е.5.1 Планирование разработки, квалификации и интеграции программного обеспечения.

Е.5.2 Требования к безопасности программного обеспечения, проектирование архитектуры программного обеспечения, разработка и реализация модулей программного обеспечения.

Е.5.3 Тестирование модулей программного обеспечения.

Е.5.4 Тестирование и интеграция программного обеспечения.

Е.5.5 Верификация требований к безопасности программного обеспечения.

Е.6 Интеграция устройства

Е.6.1 Планирование интеграционных тестов.

Е.6.2 Интеграция аппаратных средств и программного обеспечения и их тестирование.

Е.6.3 Интеграция системы/устройства.

Е.6.4 Интеграция в автотранспортное средство.

Е.7 Подтверждение соответствия безопасности системы и запуск в производство

Е.7.1 Действия по подтверждению соответствия.

E.7.2 Документация по подтверждению соответствия и запуск в производство.

E.8 Планирование производства и обслуживания

E.8.1 Связанные с безопасностью специальные характеристики производства.

E.8.2 Связанные с безопасностью специальные характеристики эксплуатации, обслуживания и вывода из эксплуатации.

E.9 Результат

Документация по оценке функциональной безопасности, рекомендации и действия, которые должны быть выполнены после оценки функциональной безопасности.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 26262-1:2011	—	*
ИСО 26262-3:2011	—	*
ИСО 26262-4:2011	—	*
ИСО 26262-5:2011	—	*
ИСО 26262-6:2011	—	*
ИСО 26262-7:2011	—	*
ИСО 26262-8:2011	—	*
ИСО 26262-9:2011	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.		

Библиография

[1] ISO 9001, Quality management systems — Requirements
[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/IEC 15504 (all parts), Information technology — Process assessment
[4] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

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; менеджмент функциональной безопасности; требования к жизненному циклу; оценка функциональной безопасности

Редактор *Т.С. Никифорова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 04.09.2015. Подписано в печать 05.10.2015. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,35. Тираж 30 экз. Зак. 3196.

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

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

gost.e-ecolog.ru