ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-8— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 8

Вспомогательные процессы

ISO 26262-8:2011
Road vehicles – Functional safety – Part 8: Supporting processes
(IDT)

Издание официальное

Москва
Стандартинформ
2015

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 10 июня 2014 г. № 526-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-8:2011 «Дорожные транспортные средства. Функциональная безопасность. Часть 8. Вспомогательные процессы» (ISO 26262-8:2011 «Road vehicles – Functional safety – Part 8: Supporting processes»)

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 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

Содержание

1 Область применения ... 01
2 Нормативные ссылки ... 01
3 Термины, определения и сокращения ... 02
4 Требования соответствия настоящему стандарту ... 02
4.1 Общие требования ... 02
4.2 Интерпретация таблиц ... 03
4.3 Требования и рекомендации, зависимые от значения УПБА ... 03
5 Взаимодействие в совместных разработках ... 03
5.1 Цель ... 03
5.2 Общие положения ... 03
5.3 Входная информация ... 04
5.4 Требования и рекомендации ... 04
5.5 Результаты работы ... 06
6 Спецификация и менеджмент требований к системе безопасности ... 07
6.1 Цели ... 07
6.2 Общие положения ... 07
6.3 Входная информация ... 07
6.4 Требования и рекомендации ... 07
6.5 Результаты работы ... 11
7 Управление конфигурацией ... 11
7.1 Цели ... 11
7.2 Общие положения ... 11
7.3 Входная информация ... 12
7.4 Требования и рекомендации ... 12
7.5 Результаты работы ... 12
8 Управление изменениями ... 12
8.1 Цель ... 12
8.2 Общие положения ... 12
8.3 Входная информация ... 12
8.4 Требования и рекомендации ... 13
8.5 Результаты работы ... 14
9 Верификация ... 14
9.1 Цель ... 14
9.2 Общие положения ... 14
9.3 Входная информация ... 15
9.4 Требования и рекомендации ... 15
9.5 Результаты работы ... 16
10 Документирование ... 16
10.1 Цель ... 16
10.2 Общие положения ... 17
10.3 Входная информация ... 17
10.4 Требования и рекомендации ... 17
10.5 Результаты работы ... 18
11 Уверенность в использовании инструментального программного обеспечения ... 18
11.1 Цели ... 18
11.2 Общие положения ... 18
11.3 Входная информация ... 19
11.4 Требования и рекомендации ... 19
11.5 Результаты работы ... 24
12 Квалификация компонентов программного обеспечения ... 24
12.1 Цель ... 24
12.2 Общие положения ... 24
12.3 Входная информация ... 25
12.4 Требования и рекомендации ... 25
12.5 Результаты работы ... 26
13 Квалификация компонентов аппаратных средств ... 27
13.1 Цели ... 27
13.2 Общие положения ... 27
13.3 Входная информация ... 28

13.4 Требования и рекомендации 29
13.5 Результаты работы 30
14 Подтверждение проверкой эксплуатацией 30
14.1 Цель 30
14.2 Общие положения 31
14.3 Входная информация 31
14.4 Требования и рекомендации 32
14.5 Результаты работы 34
Приложение А (справочное) Обзор и поток документов вспомогательных процессов 35
Приложение В (справочное) Пример соглашения о взаимодействии при разработке (СВР) 38
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам Российской Федерации 43
Библиография 44

Введение

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

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

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

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

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

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

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

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

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

e) устанавливает требования к взаимодействию с поставщиками.

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

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

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

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

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

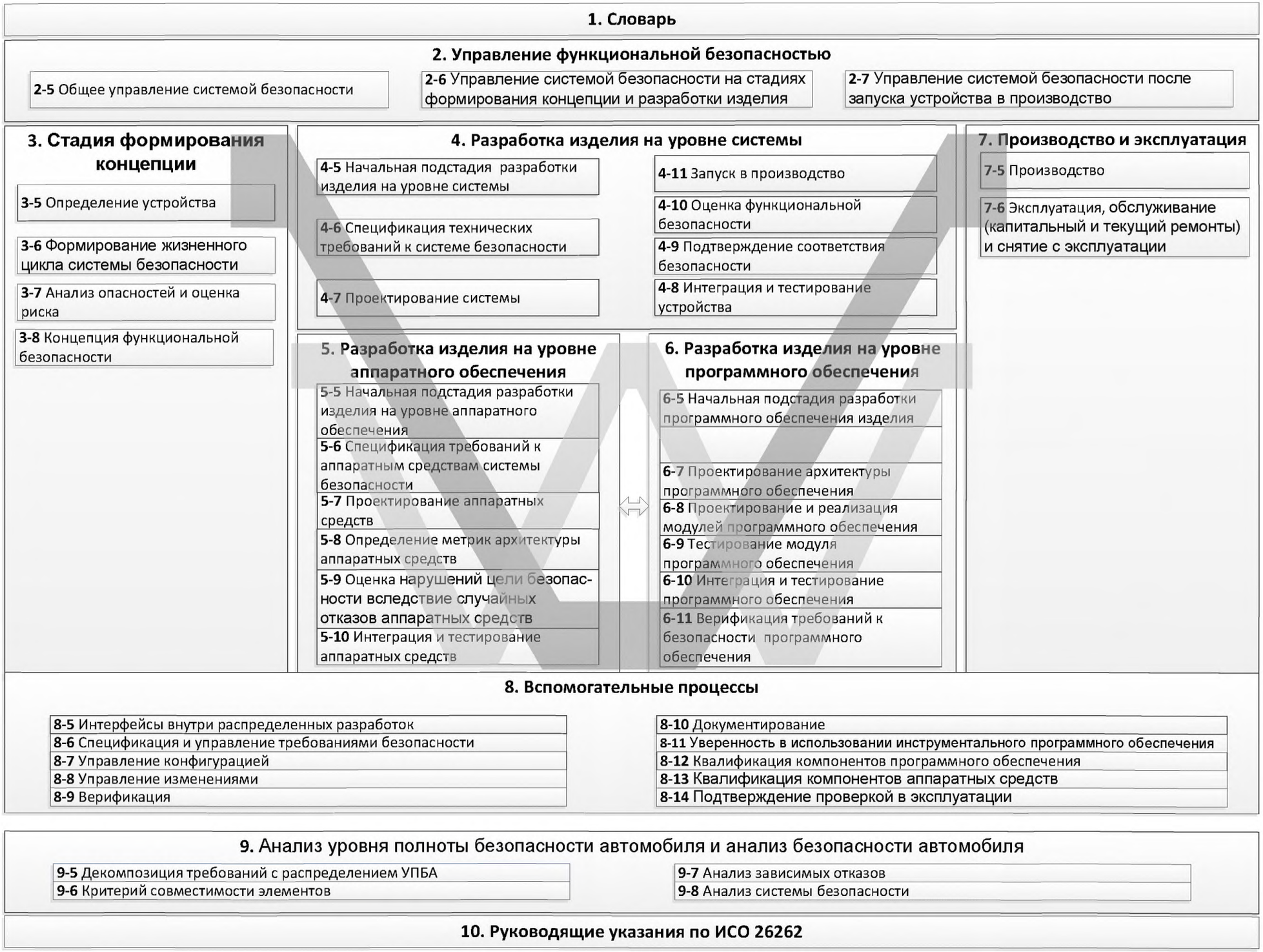


Рисунок 1 – Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 8

Вспомогательные процессы

Road vehicles – Functional safety – Part 8: Supporting processes

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 вспомогательным процессам, в том числе:

- взаимодействие в совместных разработках;
- менеджмент требований к системе безопасности на всех этапах ее жизненного цикла;
- управление конфигурацией;
- управление изменениями;
- верификация
- документирование;
- обеспечение уверенности в использовании инструментального программного обеспечения;
- квалификация компонентов программного обеспечения;
- квалификация компонентов технических средств;
- подтверждение проверкой эксплуатацией.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ИСО 26262-3:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 3.

Издание официальное

Стадия формирования концепции (ISO 26262-3:2011, Road vehicles – Functional safety – Part 3: Concept phase)

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

ИСО 26262-5:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 5. Разработка аппаратных средств изделия (ISO 26262-5:2011, Road vehicles – Functional safety – Part 5: Product development at the hardware level)

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

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

ИСО 26262-9:2011 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)

ИСО/МЭК 12207 Информационная технология. Процессы жизненного цикла программных средств (ISO/IEC 12207, Systems and software engineering — Software life cycle processes)

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

В настоящем стандарте применимы 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 для 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 функциональ-

ной 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 достижение соответствия с рассматриваемым требованием. Каждый метод в таблице включен либо в

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

б) 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 Взаимодействие в совместных разработках

5.1 Цель

Цель данного раздела заключается в описании процедур и распределении соответствующих сфер ответственности в рамках совместной разработки устройств и элементов.

5.2 Общие положения

Заказчик (например, изготовитель транспортного средства) и поставщики при разработках устройств совместно выполняют требования, заданные в настоящем стандарте. Между заказчиком и поставщиками согласовываются сферы ответственности. Допускаются также отношения с субподрядчиками. Заказчик для реализации своих связанных с безопасностью технических требований при планировании, исполнении и оформлении документации для разработок собственных устройств использует набор процедур. Аналогичные процедуры должны быть согласованы для взаимодействия с поставщиком при совместных разработках устройства или при разработках устройства, где поставщик полностью несет ответственность за обеспечение безопасности.

Примечание – Данный раздел не имеет отношения к закупке стандартных компонентов и частей или к комиссиям по разработке, которые не возлагают какую-либо ответственность за обеспечение безопасности на поставщика.

5.3 Входная информация

5.3.1 Предварительные требования

См. применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, на которых планируется и осуществляется совместная разработка.

5.3.2 Дополнительная информация

Следующая информация может быть учтена:

– предварительная версия соглашения о взаимодействии при разработке (из внешнего источника);

– о тендере поставщика на основе запроса котировок (из внешнего источника).

5.4 Требования и рекомендации

5.4.1 Область применения требований

5.4.1.1 Требования раздела 5 должны применяться к каждому устройству и элементу, разработанному в соответствии с требованиями настоящего стандарта, за исключением готовых частей аппаратных средств, при выполнении одного из следующих условий:

a) нет конкретных требований к аппаратным средствам системы безопасности, распределяемых частям аппаратных средств или

b) готовые части аппаратных средств квалифицированы в соответствии с процедурами, основанными на международных стандартах качества (например, AEC стандарты для электронных компонентов), а также квалификация готовых частей аппаратных средств охватывает диапазон параметров, связанный с целевым применением.

5.4.1.2 Требования к отношению заказчик-поставщик (интерфейсам и взаимодействиям) должны применяться к каждому уровню отношений заказчик-поставщик.

Примечания

1 Они включает субподряды, сформированные поставщиком верхнего уровня, субподряды, сформированные этими субпоставщиками и т.д.

2 Управление внутренними поставщиками может быть таким же, как внешними поставщиками.

5.4.2 Критерии выбора поставщика

5.4.2.1 Критерии выбора поставщика должны включать оценку возможностей поставщика по разработке и производству устройств и элементов сравнимой сложности с одинаковыми значениями УПБА в соответствии с требованиями настоящего стандарта.

Примечание – Критерии выбора поставщика включают в себя:

- доказательство существования у поставщика системы менеджмента качества;
- характеристики производства и качество продукции поставщика в прошлом;
- подтверждение в тендерной документации поставщика способности выполнять проекты в области функциональной безопасности;
- результаты предыдущих оценок безопасности в соответствии с требованиями 6.4.9 ИСО 26262-2;
- рекомендации отделов разработки, производства, качества и логистики изготовителя транспортного средства о влиянии результатов их работы на функциональную безопасность.

5.4.2.2 Запрос предложения от заказчика к поставщику-кандидату должен содержать:

a) официальный запрос в соответствии с требованиями настоящего стандарта;

b) определение устройства или функциональные характеристики элемента;

c) цели безопасности, требования функциональной безопасности или технические требования системы безопасности, в том числе их соответствующие значения УПБА, если они уже имеются, в зависимости от того, что указывается поставщиком.

Примечание – Если значение УПБА не известно во время выбора поставщика, то делается консервативное допущение.

5.4.3 Инициирование и планирование совместной разработки

5.4.3.1 Заказчик и поставщик должны определить соглашение о взаимодействии при разработке, включающее следующее:

Примечание – Пример соглашения о взаимодействии при разработке приведен в приложении В.

a) назначение заказчиком и поставщиком менеджеров по безопасности;

b) совместную настройку жизненного цикла системы безопасности в соответствии с требованиями 6.4.5 ИСО 26262-2;

c) описания действий и процессов, выполняемых заказчиком, и действий и процессов, выполняемых поставщиком;

d) информацию и результаты работы, подлежащие обмену.

Примечания

1 Они включают в себя соглашение о документации, которая будет предоставлена при завершении заказчиком и поставщиком отчетов об оценке безопасности.

2 В обмениваемой информации содержится информация о специальных, связанных с безопасностью характеристиках.

3 В случае совместной разработки соответствующие части результатов работы, необходимые для разработки, заинтересованные стороны могут определить и ими обменяться;

e) перечень сторон или лиц, ответственных за выполняемые действия;

f) целевые значения, полученные из целей на уровне системы, переданные каждой соответствующей стороне с тем, чтобы ими были выполнены целевые значения для метрики одиночных сбоев и метрики скрытых сбоев при оценке метрик архитектуры аппаратных средств и оценке нарушений цели безопасности из-за случайных отказов аппаратных средств (см. ИСО 26262-5);

g) описание вспомогательных процессов и инструментальных средств, включая интерфейсы, для обеспечения совместимости между заказчиком и поставщиком.

5.4.3.2 Если поставщик выполняет анализ опасностей и оценку рисков, то результаты анализа опасностей и оценки рисков должны быть предоставлены заказчику для верификации.

5.4.3.3 Сторона, ответственная за разработку устройства, формирует концепцию функциональной безопасности в соответствии с требованиями ИСО 26262-3. Требования функциональной безопасности должны быть согласованы между заказчиком и поставщиком.

5.4.4 Выполнение совместной разработки

5.4.4.1 Поставщик должен сообщить заказчику о каждой проблеме, которая увеличивает риск несоответствия плану проекта, плану обеспечения безопасности, плану интеграции и тестирования согласно требованиям ИСО 26262-4, или плану верификации программного обеспечения в соответствии с требованиями ИСО 26262 – 6, или другим положениям соглашения о взаимодействии при разработке.

5.4.4.2 Поставщик должен сообщить заказчику о каждом отклонении от нормы, которое происходит во время действий по разработке в его зоне ответственности или у его субподрядчиков.

5.4.4.3 Поставщик должен определить, может ли быть выполнено каждое из требований безопасности. Если это не удается реализовать, то должна быть пересмотрена концепция обеспечения безопасности и, при необходимости, она должна быть модифицирована, чтобы получить требования безопасности, которые будут выполнены.

5.4.4.4 Каждое изменение, потенциально влияющее на безопасность устройства, или планируемые действия для демонстрации соответствия требованиям настоящего стандарта доводятся до сведения другой стороны для выполнения анализа влияния в соответствии с требованиями раздела 8.

5.4.4.5 Обе стороны при формировании требований безопасности для текущей разработки должны учитывать уже накопленный опыт в аналогичных разработках в соответствии с требованиями 5.4.2.7 ИСО 26262-2:2011.

5.4.4.6 Поставщик должен предоставить менеджеру по безопасности заказчика информацию об основных результатах, достигнутых при решении задач на основных стадиях, определенных в плане обеспечения безопасности. Формат отчета и сроки предоставления должны быть согласованы между поставщиком и заказчиком.

Пример – Через равные промежутки времени или по выполнении основных стадий указанных в графике работ заказчик проверяет составленные поставщиком отчеты по менеджменту качества.

5.4.4.7 Должно быть достигнуто соглашение, на основе которого сторона (поставщик или заказчик) осуществляет подтверждение соответствия системы безопасности требованиям ИСО 26262-4.

Примечание – Если поставщик выполняет интеграцию и подтверждение соответствия, то поставщику важно иметь соглашение об имеющихся возможностях и необходимых ресурсах, так как подтверждение соответствия системы безопасности требует интегрированного транспортного средства (см. ИСО 26262-4).

5.4.4.8 Данное требование распространяется на значение УПБА, равное D, в соответствии с 4.3. Заказчик должен иметь возможность проводить дополнительные аудиты функциональной безопасности на предприятии поставщика в любое подходящее время.

5.4.5 Оценка функциональной безопасности на предприятии поставщика

5.4.5.1 Данное требование распространяется на значения УПБА (B), C, D в соответствии с 4.3. При достижении определенных точек должна выполняться оценка функциональный безопасности устройства. Эти оценки должны выполняться на каждой стадии разработки устройства. Такие оценки функциональной безопасности должны выполняться на соответствующих уровнях детализации для сложного устройства и для значений УПБА его целей безопасности. Оценка функциональной безопасности должна быть выполнена в соответствии с требованиями 6.4.9 ИСО 26262-2.

5.4.5.2 Данное требование распространяется на значение УПБА, равное B, в соответствии с 4.3. Оценка функциональной безопасности должна быть выполнена.

Примечание – Данное требование может быть выполнено заказчиком, другой организацией или самим поставщиком.

5.4.5.3 Данное требование распространяется на значения УПБА C и D в соответствии с 4.3. Оценку функциональной безопасности в соответствии с требованиями 6.4.9 ИСО 26262-2 должен проводить на предприятии поставщика заказчик либо организация или лицо, которых назначил заказчик.

Примечание – Данное требование может быть выполнено самим поставщиком.

5.4.5.4 Данное требование распространяется на значения УПБА (B), C и D в соответствии с 4.3. Отчет по оценке функциональной безопасности должен быть доступен на предприятиях поставщика и заказчика.

5.4.5.5 Данное требование распространяется на значения УПБА (B), C и D в соответствии с 4.3. Каждое выявленное отклонение от нормы, которое может повлиять на результаты работы поставщика, должно быть проанализировано и должны быть выполнены действия по устранению таких отклонений. Между обеими сторонами должно быть достигнуто соглашение о том, кто выполняет необходимые действия.

5.4.6 После запуска в производство

5.4.6.1 Поставщик должен предоставить заказчику доказательства, что возможности технологического процесса выполнены и поддерживаются в соответствии с требованиями раздела 7 ИСО 26262-2 и раздела 5 ИСО 26262-7.

5.4.6.2 Договор поставки между заказчиком и поставщиком должен определить ответственность за обеспечение функциональной безопасности в соответствии с требованиями 7.4.2.1 ИСОО 26262-2 и определить мероприятия по обеспечению безопасности для каждой из сторон.

5.4.6.3 Договор поставки должен установить правила доступа и обмена между сторонами учетной производственной информацией о специальных, связанных с безопасностью характеристиках.

5.4.6.4 Каждая сторона, которой становится известно о связанном с безопасностью событием, в соответствии с договором поставки должна своевременно известить об этом другую сторону. Если происходит связанное с безопасностью событие, то должен быть выполнен анализ этого события. Проанализированы должны быть аналогичные устройства и связанные с ними части, на которые может повлиять аналогичное событие.

5.5 Результаты работы

5.5.1 Отчет о выборе поставщика

В результате выполнения требований 5.4.2.1 – 5.4.2.2.

5.5.2 Соглашения о взаимодействии при разработке

В результате выполнения требований 5.4.3.

5.5.3 План работы поставщика

В результате выполнения требований 5.4.3.

5.5.4 План обеспечения безопасности поставщика

В результате выполнения требований 5.4.3.

5.5.5 Отчет по оценке функциональной безопасности

В результате выполнения требований 5.4.5.1 – 5.4.5.5.

5.5.6 Договор поставки

В результате выполнения требований 5.4.6.2 – 5.4.6.3.

6 Спецификация и менеджмент требований к системе безопасности

6.1 Цели

Первая цель заключается в обеспечении корректной спецификации требований к системе безопасности, их атрибутов и характеристик.

Вторая цель заключается в обеспечении согласованного менеджмента требований к системе безопасности на протяжении всего ее жизненного цикла.

6.2 Общие положения

Требованиями к системе безопасности являются все требования, направленные на достижение и обеспечение необходимых значений УПБА.

В процессе жизненного цикла системы безопасности, требования к системе безопасности специфицируются и подробно описываются в виде иерархической структуры. На рисунке 2 показаны структура и зависимости требований к системе безопасности, используемые в настоящем стандарте. Требования к системе безопасности выделяются элементам или распределяются между ними.

Менеджмент требований к системе безопасности включает управление требованиями, получение согласия по требованиям, получение обязательств со стороны тех, кто реализует требования, поддержка прослеживаемости.

Для того, чтобы поддерживать менеджмент требований к системе безопасности, рекомендуется применять соответствующие инструменты менеджмента требований.

Данный раздел включает в себя требования к спецификации и менеджменту требований к системе безопасности (см. рисунок 3).

Конкретные требования, включающие содержание требований к системе безопасности на различных иерархических уровнях, перечислены в ИСО 26262-3, ИСО 26262-4, ИСО 26262-5 и ИСО 26262-6.

6.3 Входная информация

6.3.1 Предварительные требования

См. применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, на которых специфицируется или выполняется менеджмент требований к системе безопасности.

6.3.2 Дополнительная информация

См. применимую дополнительную информацию поддержки соответствующих стадий жизненного цикла систем безопасности, на которых специфицируются или выполняется менеджмент требований к системе безопасности.

6.4 Требования и рекомендации

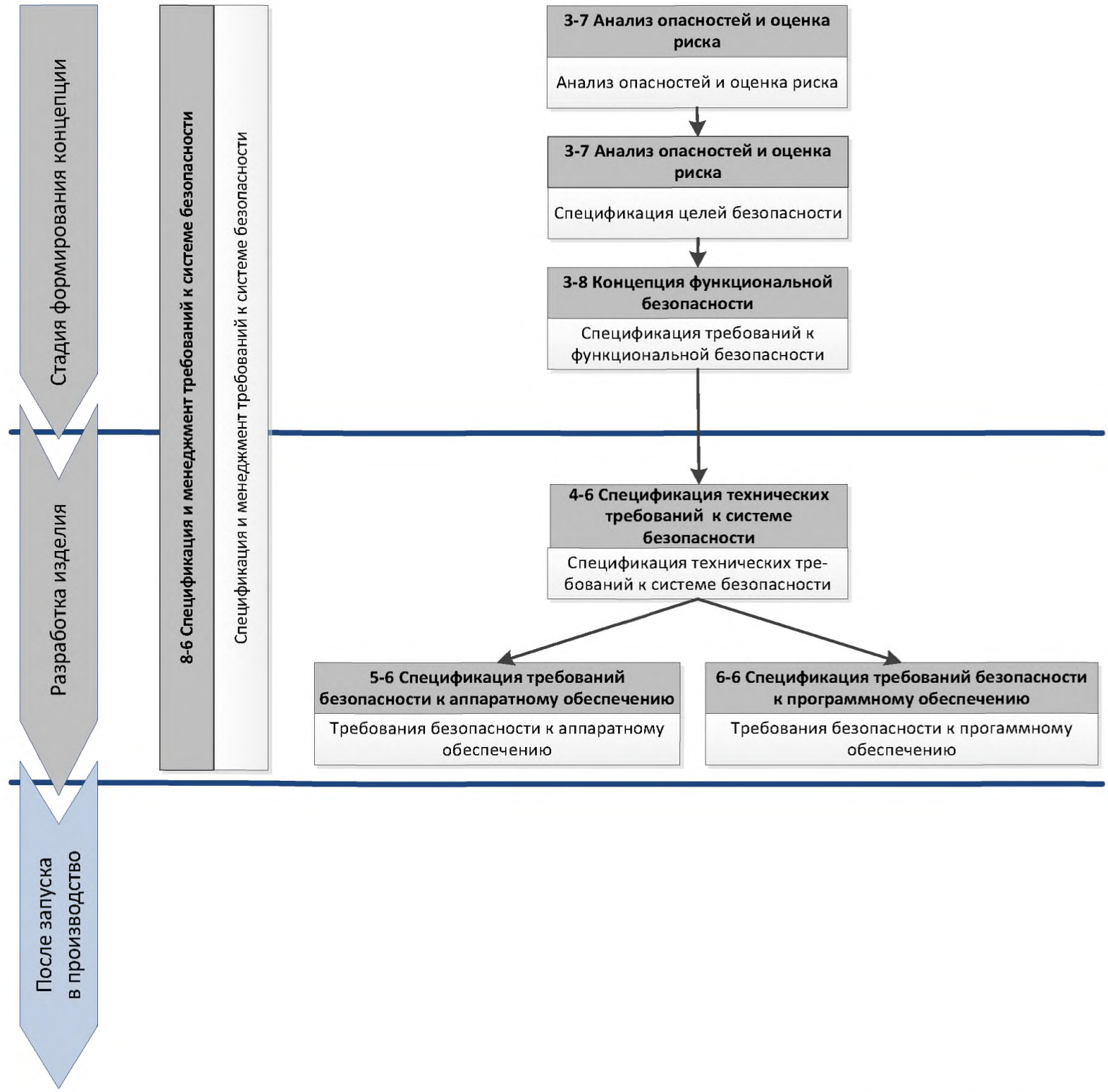
6.4.1 Спецификация требований к системе безопасности

6.4.1.1 Для достижения характеристик требований к системе безопасности, перечисленных в 6.4.2.4, требования к системе безопасности должны быть определены с помощью соответствующей комбинации:

a) естественного языка и

b) методов, перечисленных в таблице 1.

Примечание – Использование естественного языка является наиболее целесообразным средством для представления требований к системе безопасности на более высоком уровне (например, функциональные и технические требования к системе безопасности), а требования к системе безопасности на более низком уровне (например, требования к программному обеспечению и аппаратным средствам системы безопасности) наиболее удобно описывать методами, перечисленными в таблице 1.



Примечание – На рисунке конкретный раздел каждой части настоящего стандарта указан следующим образом: «m-n», где «m» представляет собой номер части, а «n» указывает на номер раздела, например, 3-7 представляет раздел 7 ИСО 26262-3.

Рисунок 2 – Структура требований к системе безопасности

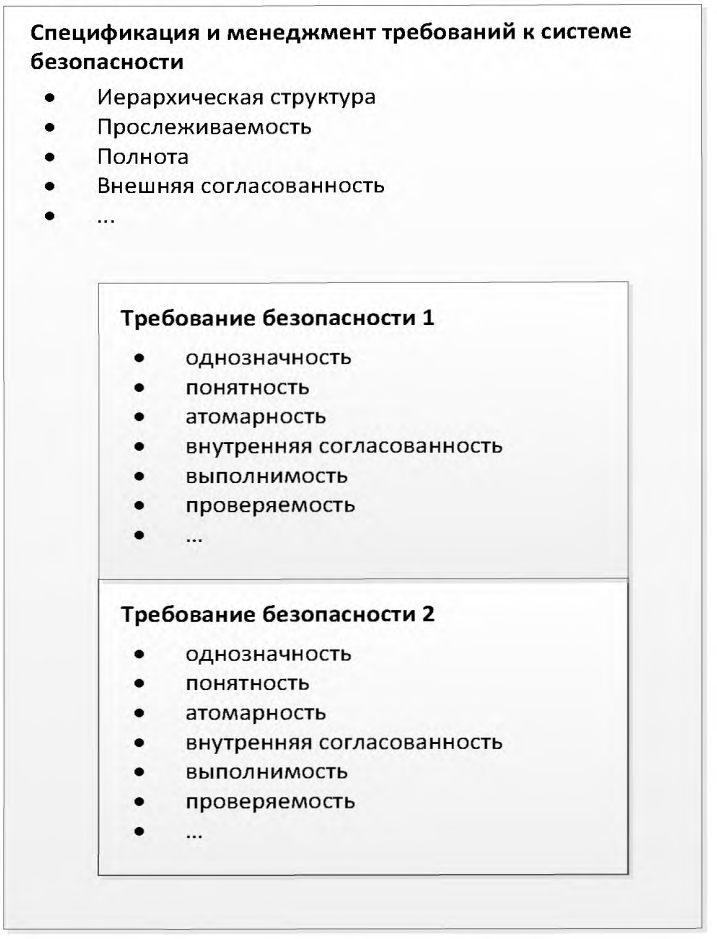


Рисунок 3 – Связь между менеджментом требований к системе безопасности и определенными требованиями к системе безопасности

Таблица 1 – Спецификация требований к системе безопасности

Методы		УПБА			
		A	B	C	D
1a	Неформальные нотации для спецификации требований	++	++	+	+
1b	Полуформальные нотации для спецификации требований	+	+	++	++
1c	Формальные нотации для спецификации требований	+	+	+	+

6.4.2 Атрибуты и характеристики требований к системе безопасности

6.4.2.1 Требования к системе безопасности должны быть однозначно идентифицированы как требования к системе безопасности.

Примечание – Для того, чтобы выполнить это требование, требования к системе безопасности могут быть перечислены в отдельном документе. Если требования к системе безопасности и другие требования вводятся одним и тем же документом, то требования к системе безопасности могут быть выделены явно с помощью специального атрибута, как описано в 6.4.2.5.

6.4.2.2 Требования к системе безопасности наследуют значения УПБА от требований к системе безопасности, из которых они получены, за исключением случаев применения декомпозиции УПБА, выполненной в соответствии с требованиями ИСО 26262-9.

Примечание – Так как цели безопасности являются требованиями к системе безопасности наивысшего уровня, то наследование значений УПБА начинается с уровня цели безопасности (см. определение 2.108 ИСО 26262-1).

6.4.2.3 Требования к системе безопасности должны быть распределены устройству или элементу.

6.4.2.4 Требования к системе безопасности должны быть:

a) однозначными и понятными.

Примечания

1 Требование является однозначным, если есть общее понимание смысла этого требования.

2 Требование понятно, если читатель соседнего уровня абстракции (т.е. либо заинтересованное лицо, либо потребитель этого требования) понимает его смысл;

b) атомарными.

Примечание – Требования к системе безопасности на одном иерархическом уровне являются атомарными, если они сформулированы таким образом, что не могут быть разделены на более простые требования к системе безопасности на рассматриваемом уровне;

c) внутренне согласованными.

Примечание – В отличие от внешней согласованности, при которой множество требований к системе безопасности не противоречат друг другу, внутренняя согласованность означает, что каждое отдельное требование безопасности не содержит в себе противоречия;

d) выполнимыми.

Примечание – Требование выполнимо, если оно может быть реализовано в рамках ограничений разрабатываемого устройства (ресурсов, современного уровня и т.д.);

e) проверяемыми.

6.4.2.5 Требования к системе безопасности должны иметь следующие атрибуты:

a) уникальный идентификатор, остающийся неизменным на протяжении жизненного цикла системы безопасности.

Пример – Уникальная идентификация требования может быть достигнута различными способами, например, индексацией каждого экземпляра слова «должен», например, «Система должна$_{9782}$ проверить ...», или последовательной нумерацией каждого предложения, содержащего слово «должен», например, «$_{9782}$ В случае ... система должна проверить ...»;

b) статус.

Пример – Статус требования к системе безопасности может быть «предложенное», «предполагаемое», «принятое» или «рассмотренное»;

c) УПБА.

6.4.3 Менеджмент требований к системе безопасности

6.4.3.1 Набор требований к системе безопасности должен обладать следующими свойствами:

a) иметь иерархическую структуру.

Примечание – Иерархическая структура означает, что требования к системе безопасности структурированы на нескольких последовательных уровнях, представленных на рисунке 2. Эти уровни всегда совпадают с соответствующими стадиями проекта;

b) быть организационно структурированным согласно соответствующей схеме группирования.

Примечание – Организация требований к системе безопасности означает, что требования к системе безопасности на каждом уровне группируются вместе, как правило, в соответствии с архитектурой;

c) обладать полнотой.

Примечание – Полнота означает, что требования к системе безопасности на одном уровне в полном объеме реализуют все требования к системе безопасности на предыдущем уровне;

d) быть внешне согласованным.

Примечание – В отличие от внутренней согласованности, в которой индивидуальное требование к системе безопасности не противоречит само себе, внешняя согласованность означает, что несколько требований к системе безопасности не противоречат друг другу;

e) не иметь дублирование информации на любом уровне иерархической структуры.

Примечание – Отсутствие дублирования информации означает, что содержание требований к системе безопасности не повторяется в любом другом требовании к безопасности на одном отдельном уровне иерархической структуры, и это верно на каждом иерархическом уровне;

f) быть сопровождаемым.

Примечание – Сопровождаемость означает, что набор требований может быть изменен или расширен, например, при введении новых версий требований или путем добавления (удаления) требования к (из) набору(а) требований.

6.4.3.2 Требования безопасности должны быть прослеживаемыми со ссылками на:

a) каждый источник требований к системе безопасности на верхнем уровне иерархии;

b) каждое выведенное требование к системе безопасности на более низком уровне иерархии, или к его реализации в проекте;

c) спецификацию верификации в соответствии с требованиями 9.4.2.

Примечание – Кроме того, прослеживание поддерживает:

- анализ последствий, если изменения вносятся в конкретные требования к системе безопасности;
- оценку функциональной безопасности.

6.4.3.3 Должна применяться соответствующая комбинация методов верификации, приведенная в таблице 2, для верификации соблюдения требований к системе безопасности соответствия требованиям настоящего пункта, и что комбинация методов удовлетворяет конкретным требованиям к верификации требований к системе безопасности в соответствующих частях настоящего стандарта, где выводятся требования к системе безопасности

Таблица 2 – Методы верификации требований к системе безопасности

Методы		УПБА			
		A	B	C	D
1a	Верификация с помощью сквозного контроля	++	+	o	o
1b	Верификация с помощью контроля	+	++	++	++
1c	Полуформальная верификация [a)]				
1d	Формальная верификация				
[a)] Метод 1c может быть реализован исполняемыми моделями.					

6.4.3.4 Для требований к системе безопасности должна быть применена технология управления конфигурацией в соответствии с требованиями раздела 7.

Пример – Если требования к системе безопасности на более низком уровне соответствуют требованиям к системе безопасности более высокого уровня, то с помощью технологии управления конфигурацией можно определить базовую конфигурацию в качестве основы для последующих стадий жизненного цикла системы безопасности.

6.5 Результаты работы

Не формируются.

7 Управление конфигурацией

7.1 Цели

Первая цель – обеспечить, чтобы результаты работы, а также принципы и общие условия их создания могли быть однозначно определены и воспроизведены в управляемом режиме в любое время.

Вторая цель – обеспечить, чтобы отношения и различия между ранней и текущей версиями можно было проследить.

7.2 Общие положения

Управление конфигурацией является устоявшейся технологией в автомобильной промышлен-

ности и может быть применено в соответствии с ИСО/ТС 16949, ИСО 10007 и ИСО/МЭК 12207.

Каждый результат работы настоящего стандарта охвачен технологией управления конфигурацией.

7.3 Входная информация

7.3.1 Предварительные требования

Необходима следующая информация:

- план обеспечения безопасности в соответствии с 6.5.1 ИСО 26262-2;
- применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, где планируется или реализуется управление конфигурацией.

7.3.2 Дополнительная информация

Отсутствует.

7.4 Требования и рекомендации

7.4.1 Управление конфигурацией должно планироваться.

7.4.2 Процесс управления конфигурацией должен соответствовать:

a) соответствующим требованиям к системе менеджмента качества (например, ИСО/ТС 16949 или ИСО 9001);

b) конкретным требованиям к разработке программного обеспечения, относящимся к разделу, посвященному управлению конфигурацией, в ИСО/МЭК 12207.

7.4.3 Результаты работы, требуемые планом обеспечения безопасности в соответствии с ИСО 26262-2, должны быть охвачены технологией управления конфигурацией и получены в соответствии со стратегией управления конфигурацией.

7.4.4 Результаты работы, охваченные технологией управления конфигурацией, должны быть документально оформлены в плане управления конфигурацией.

7.4.5 Управление конфигурацией должно выполняться на протяжении всего жизненного цикла системы безопасности.

7.5 Результаты работы

7.5.1 План управления конфигурацией

В результате выполнения требований 7.4.1, 7.4.2 и 7.4.5.

8 Управление изменениями

8.1 Цель

Целью управления изменениями является анализ и контроль изменений, связанных с безопасностью результатов работы на протяжении всего жизненного цикла системы безопасности.

8.2 Общие положения

Управление изменениями обеспечивает систематическое планирование, контроль, мониторинг, реализацию и документирование изменений, сохраняя согласованность каждого результата работы. Перед внесением изменений оценивается возможное влияние этих изменений на функциональную безопасность. Для этой цели вводятся и устанавливаются процессы принятия решений об изменениях, а ответственность возлагается на участвующие стороны.

Примечание – Здесь изменение понимается как модификация из-за: отклонений от нормы, удалений, добавлений, расширений, устаревания компонентов или частей и т. д.

8.3 Входная информация

8.3.1 Предварительные требования

Необходима следующая информация:

- план управления конфигурацией в соответствии с 7.5.1;
- план обеспечения безопасности в соответствии с 6.5.2 ИСО 26262-2.

8.3.2 Дополнительная информация

Не предполагается.

8.4 Требования и рекомендации

8.4.1 Планирование и запуск управления изменениями

8.4.1.1 Процесс управления изменениями должен планироваться и запускаться до внесения изменений в результаты работы.

Примечание – Управление конфигурацией и управление изменениями запускаются одновременно. Между двумя процессами определяются и поддерживаются интерфейсы для того, чтобы прослеживать изменения.

8.4.1.2 Должны быть определены результаты работы, для которых выполняется управление изменением, и они должны включать результаты работы, требуемые настоящим стандартом, для которых выполняется управление конфигурацией.

8.4.1.3 Для каждого результата работы должен быть определен график применения процесса управления изменениями.

8.4.1.4 Процесс управления изменениями должен включать:

a) формирование запросов на изменение в соответствии с требованиями 8.4.2;

b) анализ запросов на изменение в соответствии с требованиями 8.4.3;

c) принятие решений с обоснованием по рассматриваемым запросам на изменение в соответствии с требованиями 8.4.4;

d) осуществление принятых изменений в соответствии с требованиями 8.4.5;

e) документальное оформление в соответствии с требованиями 8.4.5.

8.4.2 Запросы на изменение

8.4.2.1 Каждому запросу на изменение должен быть присвоен уникальный идентификатор.

8.4.2.2 Каждый запрос на изменение, по меньшей мере, должен включать следующую информацию:

a) дату;

b) причину запрашиваемого изменения;

c) подробное описание запрашиваемого изменения;

d) конфигурацию, для которой запрашивается изменение.

8.4.3 Анализ запроса на изменение

8.4.3.1 Для каждого запроса на изменение должен быть выполнен анализ его влияния на изменяемое устройство, его интерфейсы и подключенные к нему устройства. Должно быть выполнено следующее:

a) определен тип запроса на изменение.

Примечание – Возможные типы изменений включают в себя: устранение ошибок, адаптацию, усовершенствование, предотвращение;

b) определены изменяемые результаты работы и результаты работы, на которые это изменение повлияет;

c) выявлены и привлечены стороны, на которые это изменение повлияет в случае распределенной разработки;

d) определено возможное влияние изменения на функциональную безопасность;

e) сформирован график реализации и верификации изменения.

8.4.3.2 Каждое изменение результата работы должно запускать возвращение на соответствующую стадию жизненного цикла системы безопасности. При этом последующие стадии должны выполняться в соответствии с требованиями настоящего стандарта.

8.4.4 Оценка запроса на изменение

8.4.4.1 Запрос на изменение должен оцениваться с учетом результатов анализа влияния, выполненного в соответствии с требованиями 8.4.3.1, а решение о принятии, отказе или отсрочке изменения принимается уполномоченными лицами.

Пример – Обычно уполномоченными лицами являются:

- ***руководитель проекта;***
- ***менеджер по обеспечению безопасности;***
- ***лицо, ответственное за обеспечение качества;***
- ***участвующие разработчики.***

Примечание – Принятые запросы на изменения могут быть расположены по приоритету и объединены со связанными принятыми запросами на изменение.

8.4.4.2 Для каждого принятого запроса на изменение должен быть решен вопрос о том, кто и когда выполняет изменения. Это решение должно учитывать интерфейсы, участвующие в выполнении запроса на изменение.

8.4.5 Выполнение и документальное оформление изменения

8.4.5.1 Изменения должны быть выполнены и верифицированы в соответствии с планом.

8.4.5.2 Если изменение оказывает влияние на функции, связанные с безопасностью, то оценка функциональной безопасности и применимые оценки подтверждения, выполняемые в соответствии с требованиями 6.4.7 и 6.4.9 ИСО 26262-2, должны быть обновлены перед выпуском устройства.

8.4.5.3 Документальное оформление изменения должно содержать следующую информацию:

a) список измененных результатов работы на соответствующем уровне, в том числе их конфигурации и версии в соответствии с требованиями раздела 7 (управление конфигурацией);

b) подробное описание выполняемого изменения;

c) планируемый срок ввода в действие изменения.

Примечание – В случае отклонения запроса на изменение, запрос на изменение и обоснование отклонения также документально оформляются.

8.5 Результаты работы

8.5.1 План управления изменением

В результате выполнения требований 8.4.1.1 – 8.4.1.3

8.5.2 Запрос на изменение

В результате выполнения требований 8.4.2.

8.5.3 Анализ влияния и план запроса на изменение

В результате выполнения требований 8.4.3.1, 8.4.4.1 и 8.4.4.2.

8.5.4 Отчет об изменении

В результате выполнения требований 8.4.5.3.

9 Верификация

9.1 Цель

Целью верификации является обеспечение соответствия результатов работы их требованиям.

9.2 Общие положения

Верификация выполняется на следующих стадиях жизненного цикла системы безопасности.

a) На стадии формирования концепции верификация гарантирует, что концепция верна, обладает полнотой и согласована с граничными условиями данного устройства, и что определяемые граничные условия сами являются достоверными, полными и согласованными настолько, что концепция может быть реализована.

b) На стадии разработки изделия верификация выполняется в различных описанных ниже формах.

1) На стадиях проектирования верификация оценивает результаты работы, такие как спецификация требований, проект архитектуры, модели, программный код, гарантируя, тем самым, что они соответствуют ранее установленным требованиям к правильности, полноте и согласованности. Оценка может быть сделана в результате осмотра, моделирования, с применением методов анализа. Выполнение оценки планируется, специфицируется, осуществляется и документально оформляется на систематической основе.

Примечание – Стадии проектирования представлены: в разделе 7 ИСО 26262-4, (Проектирование системы), в разделе 7 ИСО 26262-5 (Проектирование аппаратных средств), в разделе 7 ИСО 26262-6 (Проектирование архитектуры программного обеспечения) и в разделе 8 ИСО 26262 - 6 (Проектирование и реализация программного обеспечения устройства).

2) На стадиях тестирования верификация оценивает результаты работы в тестовой среде, чтобы убедиться, что они соответствуют своим требованиям. Такие тесты планируются, специфицируются, осуществляются и документально оформляются на систематической основе.

c) На стадиях производства и эксплуатации верификация гарантирует, что:

1) требования к системе безопасности реализуются надлежащим образом в процессе производства, руководствах пользователей и руководствах по ремонту и техническому обслуживанию;

2) выполнение связанных с безопасностью свойств устройства обеспечивается применением

средств управления производственным процессом.

Примечание – Этот общий процесс верификации формируется на стадиях жизненного цикла системы безопасности в ИСО 26262-3, ИСО 26262-4, ИСО 26262-5, ИСО 26262-6 и ИСО 26262-7. Данный процесс не охватывает подтверждение соответствия безопасности. См. раздел 9 ИСО 26262-4 (Подтверждение соответствия безопасности) для уточнения деталей.

9.3 Входная информация

9.3.1 Предварительные требования

См. применимые предварительные требования соответствующих стадий жизненного цикла системы безопасности, на которых планируется или выполняется верификация.

9.3.2 Дополнительная информация

См. применимую дополнительную информацию соответствующих стадий жизненного цикла системы безопасности, на которых планируется или выполняется верификация.

9.4 Требования и рекомендации

9.4.1 Планирование верификации

9.4.1.1 Верификация должна быть запланирована для каждой стадии и подстадии жизненного цикла системы безопасности В этом плане должно быть отражено следующее:

a) содержание верифицируемых результатов работы;

b) методы, используемые для верификации.

Примечание – Методы верификации включают: осмотр, сквозной контроль, инспекцию, проверку моделей, моделирование, инженерный анализ, демонстрацию и тестирование. Обычно при верификации применяется сочетание этих и других методов;

c) критерии прохождения и непрохождения верификации;

d) верификация окружающей среды, если это необходимо.

Примечание – Верификация окружающей среды может быть выполнена тестированием или моделированием окружающей среды;

e) инструментальные средства, используемые для верификации, если это необходимо;

f) действия, которые необходимо предпринять, если фиксируются отклонения от нормы;

g) стратегия регрессии.

Примечание – Стратегия регрессии определяет, как повторяется верификация после внесения изменений в устройство или элемент. Верификация может быть выполнена полностью или частично и может охватывать другие устройства или элементы, которые могут повлиять на результаты проверки.

9.4.1.2 Планирование верификации должно учитывать следующее:

a) адекватность применяемых методов верификации;

b) сложность верифицируемых результатов работы;

c) предыдущий опыт, связанный с верификацией.

Примечание – Он включает в себя историю технического обслуживания, а также уровень, который был достигнут при подтверждении проверкой эксплуатацией;

d) уровень зрелости используемых технологий, или риски, связанные с использованием этих технологий.

9.4.2 Спецификация верификации

9.4.2.1 Спецификация верификации должна содержать выбранные и определенные методы, которые будут использоваться для верификации, а также должна включать:

a) критический обзор или анализ таблиц контрольных проверок или

b) описание сценариев моделирования или

c) описание тестовых примеров, тестовых данных и объектов испытаний.

9.4.2.2 Для испытаний спецификация каждого тестового примера должна включать следующее:

a) уникальную идентификацию;

b) ссылку на версию соответствующего верифицируемого результата работы;

c) предварительные требования и конфигурации.

Примечание – Если полная верификация возможных конфигураций результата работы (например, вариантов системы) не представляется возможной, то выбирается разумное подмножество (например, конфигурации системы с минимальной или максимальной функциональностью);

d) условия окружающей среды, при необходимости.

Примечание – Условия окружающей среды связаны с физическими свойствами (например, температурой) окружения, в котором проводится тест или выполняется моделирование как часть процедуры тестирования;

e) входные данные, их временная последовательность и их значения;

f) ожидаемое поведение, которое включает выходные данные, приемлемые диапазоны выходных величин, поведение во времени и допустимое поведение.

Примечания

1 При определении ожидаемого поведения необходимо указать начальные выходные данные для того, чтобы выявить изменения.

2 Чтобы избежать избыточность спецификации и не хранить предварительные требования, параметры конфигурации и условия окружающей среды, необходимые для различных тестовых примеров, рекомендуется использовать однозначно идентифицируемые ссылки на эти данные.

9.4.2.3 Для испытаний тестовые примеры должны быть сгруппированы в соответствии с применяемыми методами тестирования. Для каждого метода тестирования, помимо тестовых примеров, должны быть указаны:

a) среда тестирования;

b) логические и временные зависимости;

c) ресурсы.

9.4.3 Выполнение и оценка верификации

9.4.3.1 Верификация должна быть выполнена согласно плану, сформированному в соответствии с требованиями 9.4.1, и специфицирована в соответствии с требованиями 9.4.2.

9.4.3.2 Оценка результатов верификации должна содержать следующую информацию:

a) однозначную идентификацию верифицируемого результата работы;

b) ссылку на соответствующий план верификации и спецификацию верификации;

c) параметры конфигурации среды верификации и используемые инструменты верификации, а также данные о калибровке, используемые в процессе оценки, если они применяются;

d) уровень соответствия результатов верификации с ожидаемыми результатами;

e) однозначное заявление о том, пройдена верификация или нет, и если верификация не пройдена, то заявление должно включать объяснение непрохождения и предложения по выполнению изменений в верифицируемом результате работы.

Примечание – Верификация оценивается при использовании критериев для завершения и прекращения верификации [см. перечисление c) 9.4.1.1] в соответствии с ожидаемыми результатами верификации;

f) причины, по которым шаги верификации не выполняются.

9.5 Результаты работы

9.5.1 План верификации

В результате выполнения требований 9.4.1.1 и 9.4.1.2.

9.5.2 Спецификация верификации

В результате выполнения требований 9.4.2.1 – 9.4.2.3.

9.5.3 Отчет о верификации

В результате выполнения требований 9.4.3.1 и 9.4.3.2.

10 Документирование

10.1 Цель

Основная цель заключается в разработке стратегии управления документированием в течение всего жизненного цикла системы безопасности в целях обеспечения эффективности и воспроизводимости процесса управления документацией.

10.2 Общие положения

Требования к документации в настоящем стандарте сосредоточены главным образом на информации, а не на ее размещении и внешнем виде.

Информация не обязательно должна быть доступна в форме физического документа, если это явно не указано в настоящем стандарте. Документация может иметь различные формы и структуры, а также различные инструменты могут быть использованы для автоматического создания документов.

Пример – Возможными формами являются: бумажный носитель, электронный носитель, базы данных.

Достоверность информации зависит от целого ряда факторов, включая сложность, масштаб связанных с безопасностью систем/подсистем и требования, относящиеся к конкретному применению.

Дублирования информации в документе, а также между документами, следует избегать, чтобы обеспечить сопровождаемость.

Примечание – Альтернативой дублированию информации является использование перекрестных ссылок в одном документе, направляющих читателя к документу, который является первоисточником информации.

10.3 Входная информация

10.3.1 Предварительные требования

Необходима следующая информация:

– план по обеспечению безопасности в соответствии с 6.5.1 ИСО 26262-2.

10.3.2 Дополнительная информация

Не предполагается.

10.4 Требования и рекомендации

10.4.1 Чтобы сделать документацию доступной, процесс ее подготовки должен быть спланирован:

a) на каждой стадии всего жизненного цикла системы безопасности для эффективного завершения стадий и действий по верификации;

b) для управления функциональной безопасностью;

c) в качестве источника исходной информации для оценки функциональной безопасности.

10.4.2 Идентификация результата работы в настоящем стандарте должна быть интерпретирована как требование к документации, содержащей информацию о результатах соответствующих требований.

Примечание – Документация может быть представлена в виде отдельного документа, содержащего полную информацию о результате работы, или набора документов, которые вместе содержат полную информацию о результате работы.

10.4.3 Документы должны быть:

a) точными и краткими;

b) понятно структурированными;

c) понятными для предполагаемых пользователей;

d) сопровождаемыми.

10.4.4 Структура всей документации должна учитывать внутренние процедуры и практику работы. Документирование должно быть организовано для упрощения поиска необходимой информации.

Пример – Древовидная структура документации.

10.4.5 С каждым результатом работы или документом должны быть связаны следующие формальные элементы:

a) название, указывающее на область применения;

b) автор и утверждающее лицо;

c) уникальная идентификация каждой отдельной ревизии (версии) документа;

d) история изменений.

Примечание – История изменений содержит для каждого изменения имя автора, дату и его краткое описание;

e) статус.

Пример – «Проект», «Выпущен».

10.4.6 Должна быть обеспечена возможность определить актуальную версию документа или информацию об устройстве в соответствии с требованиями раздела 7.

10.5 Результаты работы

10.5.1 План управления документацией

В результате выполнения требований 10.4.1.

10.5.2 Руководящие указания по документированию

В результате выполнения требований 10.4.3 – 10.4.6.

11 Уверенность в использовании инструментального программного обеспечения

11.1 Цели

Первая цель данного раздела заключается в предоставлении критериев для определения необходимого уровня доверия инструментального программного обеспечения, если они применяются.

Второй целью данного раздела является обеспечение средств для квалификации инструментального программного обеспечения, если они применяются, в целях формирования доказательств того, что инструментальное программное обеспечение может быть использовано для настройки действий или задач, предусмотренной настоящим стандартом (т. е. пользователь может рассчитывать на правильное функционирование инструментального программного обеспечения для этих действий или задач, предусмотренное настоящим стандартом).

11.2 Общие положения

Инструментальное программное обеспечение, используемое при разработке системы или элементов ее программного обеспечения или аппаратных средств, может поддержать или адаптировать жизненный цикл системы безопасности, посредством настройки действий и задач, предусмотренных настоящим стандартом. В таких случаях необходима уверенность, что инструментальное программное обеспечение эффективно достигает следующих целей:

a) риск систематических сбоев в разрабатываемых изделиях из-за ошибок в инструментальном программном обеспечении, приводящих к неправильным результатам на его выходе, сведен до минимума;

b) процесс разработки соответствует требованиям настоящего стандарта, если действия или задачи, предусмотренные настоящим стандартом, полагаются на правильное функционирование используемого инструментального программного обеспечения.

Примечание – Понятие «инструментальное программное средство» может варьироваться от отдельно используемого автономного инструментального программного средства до набора инструментальных программных средств, интегрированных в цепочку инструментов.

Пример – Такие инструментальные программные средства могут быть коммерческими, с открытым исходным кодом, бесплатными, со свободным доступом или разработаны самими пользователями.

Для определения требуемого уровня доверия инструментальному программному обеспечению, используемому при разработке в условиях, указанных выше, оцениваются следующие критерии:

– возможность того, что содержащее ошибку инструментальное программное обеспечение и соответствующий неверный результат его работы может ввести или не обнаружить ошибки в связанном с безопасностью разрабатываемом устройстве или элементе и

– уверенность в предотвращении или обнаружении таких ошибок на его соответствующем выходе.

Для оценки доверия к мерам предотвращения или выявления ошибок рассматриваются и могут быть оценены внутренние для инструментального программного обеспечения меры (например, мониторинг), а также внешние для инструментального программного обеспечения меры (например, руководства, тесты, критические обзоры), выполняемые в процессе разработки связанного с безопасностью устройства или элемента.

Если для инструмента указан определенный уровень доверия, то применяются соответствующие методы квалификации, обеспечивающие соблюдение как этого уровня доверия инструмента, так и максимального значения УПБА среди всех требований к системе безопасности, распределенных

устройству или элементу, которые должны быть разработаны с использованием данного инструментального программного обеспечения. В противном случае нет необходимости применять такие методы квалификации.

11.3 Входная информация

11.3.1 Предварительные требования

Необходима следующая информация:

– план по обеспечению безопасности в соответствии с 5.5.2 ИСО 26262-4;

– применимые предварительные требования стадий жизненного цикла системы безопасности, на которых используется инструментальное программное обеспечение.

11.3.2 Дополнительная информация

Следующая информация может быть учтена:

– предварительно определенное максимальное значение УПБА;

– руководство пользователя инструментального программного обеспечения (из внешнего источника);

– внешняя среда и ограничения инструментального программного обеспечения (из внешнего источника).

11.4 Требования и рекомендации

11.4.1 Общее требование

11.4.1.1 Если жизненный цикл системы безопасности предусматривает использование инструментального программного обеспечения для разработки системы или элементов ее аппаратных средств или программного обеспечения и выполнение таких действий или задач, предусмотренных настоящим стандартом, которые полагаются на правильное функционирование инструментального программного обеспечения, а соответствующие результаты этого инструмента не проверяются или не верифицируются на соответствующей(их) стадии(ях) его применения, то такое инструментальное программное обеспечение должно соответствовать требованиям настоящего раздела.

11.4.2 Обоснованность уровня доверия или квалификации заданного инструмента

11.4.2.1 Если оценка уровня доверия или квалификация инструментального программного обеспечения осуществляется независимо от разработки конкретного связанного с безопасностью устройства или элемента, то обоснованность этого уровня доверия или квалификации заданного инструмента должна быть подтверждена в соответствии с требованиями таблицы 1 ИСО 26262-2 до использования этого инструментального программного обеспечения для разработки конкретного связанного с безопасностью устройства или элемента.

Примечание – Сбор информации об инструментальном программном обеспечении может быть общей для организаций деятельностью, способствуя тем самым действиям по классификации или квалификации.

11.4.3 Соответствие инструментального программного обеспечения его критериям оценки или его квалификации

11.4.3.1 При использовании инструментального программного обеспечения должно быть обеспечено, чтобы его применение, определенные для него ограничения внешней среды и функциональные ограничения, а также его основные условия эксплуатации соответствовали его критериям оценки или его квалификации.

Пример – Использование для идентичных версий и параметров конфигурации для таких же случаев применения вместе с теми же принятыми мерами для предотвращения или обнаружения неисправностей и их соответствующих ошибок на выходе, как описано в отчете о квалификации для этого инструментального программного обеспечения.

11.4.4 Планирование использования инструментального программного обеспечения

11.4.4.1 Использование инструментального программного обеспечения должно планироваться, включая определение:

a) обозначения и номера версии инструментального программного обеспечения;

b) конфигурации инструментального программного обеспечения.

Пример – Конфигурация компилятора определяется установкой ключей компилятора и предложениями «#pragma» в исходном файле С;

c) случаев использования инструментального программного обеспечения.

Примечания

1 Случаи использования могут описывать взаимодействия пользователя с инструментальным программным обеспечением или применяемое подмножество функциональности инструментального программного обеспечения.

2 Случаи использования могут включать в себя требования к конфигурации инструмента и к окружающей среде, в которой выполняется инструментальное программное обеспечение;

d) окружающей среды, в которой выполняется инструментальное программное обеспечение;

e) максимального значения УПБА из всех требований к системе безопасности, распределенных устройству или элементу, которые могут быть нарушены, если инструментальное программное обеспечение содержит ошибку и реализует соответствующий неверный выходной результат.

Примечание – Максимальное значение УПБА может быть определено в условиях конкретной разработки или его можно предположить, учитывая общее использование инструментального программного обеспечения. Если значение УПБА предполагается определить заранее, то такое предположение верифицируется;

f) методов квалификации инструментального программного обеспечения, в случае необходимости, на основании определенного уровня доверия.

11.4.4.2 Для обеспечения надлежащей оценки или применения инструментального программного обеспечения необходима следующая информация:

a) описание характеристик, функций и технических свойств инструментального программного обеспечения;

b) руководство пользователя или другие руководства по применению, если они применяются;

c) описание внешней среды, необходимой для его эксплуатации;

d) описание предполагаемого поведения инструментального программного обеспечения при аномальных условиях эксплуатации, в случае необходимости.

Примеры

1 Аномальными условиями эксплуатации могут быть запрещенные комбинации ключей компилятора, среда, не соответствующая руководству пользователя, или неправильная установка.

2 Предполагаемым поведением при аномальном условии эксплуатации может быть подавление сгенерированного выхода, указание пользователю или отчет пользователю;

e) описание известных ошибок инструментального программного обеспечения и соответствующих мер защиты, мер предотвращения или мер «обхода» проблемы, если они применимы.

Примеры

1 Руководства по применению или «обходные» пути, устраняющие известные неисправности, ограничение оптимизации кода компиляторами или использование ограниченного набора средств для моделирования.

2 Для выполнения соответствующей деятельности меры защиты включают предотвращение с помощью ограничения, обнаружения и учета всех известных сбоев и проблем, а также использование безопасных альтернативных методов;

f) меры для обнаружения ошибок и соответствующих неверных результатов работы инструментального программного обеспечения, идентифицированные в ходе определения необходимого уровня доверия для этого инструментального программного обеспечения.

Примечание – Меры по обнаружению соответствующих неверных результатов работы могут устранить как известные, так и возможные неверные результаты на выходе инструментального программного обеспечения.

Пример – Сравнения результатов работы резервного инструментального программного обеспечения, выполненных тестов, результатов статического анализа или критических обзоров, результатов анализа записей журнала регистрации событий для инструментального программного обеспечения.

11.4.5 Оценка инструментального программного обеспечения на основе анализа

11.4.5.1 Описание применения инструментального программного обеспечения должно содержать следующую информацию:

a) намеченную цель.

Пример – Моделирование функции, генерация исходного кода или тестирование встроенного программного обеспечения, настройка или упрощение жизненного цикла системы безопасности или автоматизация действий и задач, предусмотренных настоящим стандартом;

b) входы и предполагаемые выходы.

Пример – Необходимые данные на входе для последующей деятельности по разработке, исходный код, результаты моделирования, результаты теста или другие результаты работы в рамках настоящего стандарта;

c) ограничения внешней среды и функциональные ограничения, если они применимы.

Пример – Встраивание инструментального программного обеспечения в процессы разработки, использование общих данных различным инструментальным программным обеспечением и других используемых условий, меры для предотвращения или обнаружения неисправностей, возникающих вокруг инструментального программного обеспечения.

11.4.5.2 Предназначенное использование инструментального программного обеспечения должно быть проанализировано и оценено, чтобы определить:

a) может ли ошибка конкретного инструментального программного обеспечения внести ошибку или не обнаружить ее в разрабатываемом связанном с безопасностью устройстве или элементе. Это представляется классами влияния инструмента (ВИ):

1) класс ВИ 1 выбирается в том случае, если существует объяснение, что подобное произойти не может;

2) во всех остальных случаях выбирается класс ВИ 2;

b) доверие к мерам, которые предотвращают ошибки инструментального программного обеспечения и формирование им соответствующих неверных выходных результатов, или к мерам, которые обнаруживают, что инструментальное программное обеспечение содержит ошибку и сформировало соответствующий неверный выходной результат. Это представляется классами обнаруживающих ошибки инструментов (ООИ):

1) ООИ 1 выбирается в том случае, если существует высокая степень уверенности, что ошибка и соответствующий неверный выходной результат из-за нее будут предотвращены или обнаружены;

2) ООИ 2 выбирается в том случае, если существует средняя степень уверенности, что ошибка и соответствующий неверный выходной результат из-за нее будут предотвращены или обнаружены;

3) ООИ 3 выбирается во всех остальных случаях.

Примечания

1 Предотвращение или обнаружение может быть достигнуто с помощью разделения процесса на этапы, используя избыточность в задачах или в инструментальном программном обеспечении, или путем проверок «рациональности» инструментальным программным обеспечением самим в себе.

2 Класс ООИ 3 обычно выбирается, если никакие систематические меры не применяются в используемом процессе разработки, поэтому ошибки и соответствующие неверные выходные результаты инструментального программного обеспечения могут быть обнаружены только случайно.

3 Если инструментальное программное обеспечение используется для верификации выходных результатов другого инструментального программного обеспечения, то при оценке последнего инструментального программного обеспечения и выборе адекватного класса ООИ для этого последовательно используемого инструментального программного обеспечения учитывается взаимозависимость между этими системами инструментального программного обеспечения.

4 При таком анализе использования для правильного определения обоих классов ВИ и ООИ необходим только определенный уровень детализации.

Примеры

1 Для генератора кода может быть выбран класс ООИ 1, если сгенерированный им исходный код верифицируется в соответствии с требованиями настоящего стандарта.

2 Используя руководства по применению, можно предотвратить ошибки, такие как неправильное или неоднозначное толкование кода, созданного компилятором.

11.4.5.3 Если правильный выбор классов ВИ и ООИ непонятен или вызывает сомнения, то ВИ и ООИ следует оценивать консервативно.

11.4.5.4 Если в результате использования инструментального программного обеспечения для настройки процесса разработки оказалось, что действия или задачи, предусмотренные настоящим стандартом, пропущены, то класс ООИ 2 не может быть выбран.

11.4.5.5 На основе значений, определенных для классов ВИ и ООИ (в соответствии с требованиями 11.4.5.2, 11.4.5.3 или 11.4.5.4), необходимый уровень доверия к инструментальному программному обеспечению будет определяться в соответствии с таблицей 3.

Таблица 3 – Определение уровня доверия к инструменту (УДИ)

		Инструменты, обнаруживающие ошибки		
		ООИ 1	ООИ 2	ООИ 3
Влияние инструмента	ВИ 1	УДИ 1	УДИ 1	УДИ 1
	ВИ 2	УДИ 1	УДИ 2	УДИ 3

11.4.6 Квалификация инструментального программного обеспечения

11.4.6.1 Для квалификации инструментального программного обеспечения с УДИ 3 должны быть применены методы, перечисленные в таблице 4. Для квалификации инструментального программного обеспечения с УДИ 2 должны быть применены методы, перечисленные в таблице 5. Инструментальное программное обеспечение с УДИ1 не нуждается в методах квалификации.

Таблица 4 – Квалификация инструментального программного обеспечения с УДИ 3

Методы		УПБА			
		A	B	C	D
1a	Рост доверия в результате использования в соответствии с 11.4.7	++	++	+	+
1b	Оценка процесса разработки инструмента в соответствии с требованиями 11.4.8	++	++	+	+
1c	Подтверждение соответствия инструментального программного обеспечения в соответствии с требованиями 11.4.8	+	+	++	++
1d	Разработка в соответствии со стандартом для системы безопасности [a)]	+	+	++	++

[a)] Не существует стандарта для системы безопасности, который в полной мере относится к разработке инструментального программного обеспечения. Вместо этого может быть выбрано соответствующее подмножество требований в стандарте для системы безопасности.

Пример – Разработка инструментального программного обеспечения в соответствии с требованиями ИСО 26262, МЭК 61508 или RTCA DO-178.

Таблица 5 – Квалификация инструментального программного обеспечения с УДИ 2

Методы		УПБА			
		A	B	C	D
1a	Рост доверия в результате использования в соответствии с 11.4.7	++	++	++	+
1b	Оценка процесса разработки инструмента в соответствии с требованиями 11.4.8	++	++	++	+
1c	Подтверждение соответствия инструментального программного обеспечения в соответствии с требованиями 11.4.8	+	+	+	++
1d	Разработка в соответствии со стандартом для системы безопасности [a)]	+	+	+	++

[a)] Не существует стандарта для системы безопасности, который в полной мере относится к разработке инструментального программного обеспечения. Вместо этого может быть выбрано соответствующее подмножество требований в стандарте для системы безопасности.

Пример – Разработка инструментального программного обеспечения в соответствии с требованиями ИСО 26262, МЭК 61508 или RTCA DO-178.

11.4.6.2 Квалификация инструментального программного обеспечения должна быть документально оформлена, включая следующее:

a) уникальный идентификатор и номер версии инструментального программного обеспечения;

b) максимальное значение УДИ, для которого классифицировано инструментальное программное обеспечение вместе со ссылкой на его анализ оценки;

c) заранее определенное максимальное значение УПБА или конкретное значение УПБА любого требования системы безопасности, которое может быть нарушено, если в инструментальном программном обеспечении происходит сбой и на его выходе формируется неправильный результат.

d) конфигурация и внешняя среда, для которых инструментальное программное обеспечение квалифицировано;

e) лицо или организация, которые выполнили квалификацию;

f) методы, применяемые для его квалификации в соответствии с требованиями 11.4.6.1;

g) результаты принятых мер при квалификации инструментального программного обеспечения;

h) используемые ограничения и неисправности, выявленные во время квалификации, если это применимо.

11.4.7 Рост доверия в результате использования

11.4.7.1 Если в соответствии с таблицей 4 или 5 применяется метод «Рост доверия в результате использования» для квалификации инструментального программного обеспечения, то должны соблюдаться требованиям данного пункта.

11.4.7.2 Можно утверждать о росте доверия в результате использования инструментального программного обеспечения, если только представлены следующие доказательства:

Примечание – Требования раздела 14 «Подтверждение проверкой в эксплуатации» на настоящий пункт не распространяются.

a) инструментальное программное обеспечение было использовано ранее для той же цели, в сопоставимых случаях использования, в сопоставимой определенной среде эксплуатации и с аналогичными функциональными ограничениями;

b) обоснование роста доверия в результате использования основано на достаточности и адекватности данных.

Примечание – Данные могут быть получены из накопленного объема использования (например, из продолжительного или частого).

c) спецификация инструментального программного обеспечения не меняется;

d) возникающие ошибки и соответствующие неверные выходные результаты инструментального программного обеспечения, полученные в течение предыдущих разработок, накапливаются систематически.

11.4.7.3 Опыт предыдущего применения инструментального программного обеспечения, полученный в процессе конкретных действий по разработке, должен быть проанализирован и оценен с учетом следующей информации:

a) уникального идентификатора и номера версии инструментального программного обеспечения;

b) параметров конфигурации инструментального программного обеспечения;

c) подробностей периода применения и соответствующих данных по их использованию.

Пример – Используемые функции инструментального программного обеспечения и частота их использования для соответствующих вариантов применения инструментального программного обеспечения;

d) документально оформленных ошибок и соответствующих неверных выходных результатов инструментального программного обеспечения с подробными приводящими к ним условиями;

e) списка предыдущих проверенных версий, в котором перечислены неисправности, зафиксированные для каждой соответствующей версии;

f) мер защиты, мер предотвращения или мер «обхода» известных ошибок или мер обнаружения соответствующих неверных выходных результатов, если они применимы.

Пример – Источниками для отчета о применении могут быть: журнал регистрации событий; история версий, предоставляемая поставщиком инструментального программного обеспечения; опубликованные листы корректировок (уточняющая документация).

11.4.7.4 Обоснование роста доверия от использования будет действительным только для рассматриваемой версии инструментального программного обеспечения.

11.4.8 Оценка процесса разработки инструмента

11.4.8.1 Если в соответствии с таблицей 4 или 5 применяется метод «Оценка процесса разработки инструмента» для квалификации инструментального программного обеспечения, то должны соблюдаться требования данного пункта.

11.4.8.2 Процесс разработки инструментального программного обеспечения должен выполняться в соответствии с подходящим стандартом.

Примечание – Для разработок с открытым исходным кодом могут подходить некоторые из стандартов, используемые этими сообществами разработчиков.

11.4.8.3 Оценка процесса разработки, применяемая для разработки инструментального программного обеспечения, должна быть выполнена на основе подходящего национального или международного стандарта, а также должно быть продемонстрировано надлежащее применение оцененного процесса разработки.

Примечание – Данная оценка охватывает разработку адекватного и соответствующего подмножества функций инструментального программного обеспечения.

Пример – Использование метода оценки на основе автомобильной SPICE, CMMI, ИСО 15504.

11.4.9 Подтверждение соответствия инструментального программного обеспечения

11.4.9.1 Если в соответствии с таблицей 4 или 5 применяется метод «Подтверждение соответствия инструментального программного обеспечения» для квалификации инструментального программного обеспечения, то должны соблюдаться требования данного пункта.

11.4.9.2 Подтверждение соответствия инструментального программного обеспечения должно отвечать следующим критериям:

a) средства подтверждения соответствия должны продемонстрировать, что инструментальное программное обеспечение соответствует заданным для него требованиям.

Примечание – Для подтверждения соответствия могут быть использованы тесты, предназначенные для оценки функциональных и нефункциональных качественных аспектов инструментального программного обеспечения.

Пример – Стандарт для языка программирования помогает определить требования для подтверждения соответствия соответствующего компилятора;

b) должны быть проанализированы ошибки и соответствующие неверные выходные результаты инструментального программного обеспечения, происходящие во время подтверждения соответствия, вместе с информацией об их возможных последствиях и мерах по их предотвращению или обнаружению;

c) должна быть проверена реакция инструментального программного обеспечения при не соответствующих норме условиях эксплуатации.

Пример – Возможное предсказуемое неправильное использование, неполные входные данные, неполное обновление инструментального программного обеспечения, использование запрещенных комбинаций параметров конфигурации.

11.4.10 Оценка подтверждения квалификации инструментального программного обеспечения

Требования данного пункта распространяется на значения УПБА (B), C, D в соответствии с 4.3.

Доверие в использовании инструментального программного обеспечения должно быть оценено в соответствии с требованиями таблицы 1 ИСО 26262-2, чтобы обеспечить:

a) корректную оценку необходимого уровня доверия в инструментальном программном обеспечении;

b) соответствующую квалификацию инструментального программного обеспечения в соответствии с необходимым для него уровнем доверия.

11.5 Результаты работы

11.5.1 Отчет о критериях оценки инструментального программного обеспечения

В результате выполнения требований 11.4.1 – 11.4.5 и 11.4.10.

11.5.2 Отчет о квалификации инструментального программного обеспечения

В результате выполнения требований 11.4.1 – 11.4.10.

12 Квалификация компонентов программного обеспечения

12.1 Цель

Целью квалификации компонентов программного обеспечения является предоставление доказательств о возможности их повторного использования в устройствах, разрабатываемых в соответствии с требованиями настоящего стандарта.

12.2 Общие положения

Повторное использование квалифицированных компонентов программного обеспечения позволяет избежать повторной разработки компонентов программного обеспечения с аналогичной или идентичной функциональностью.

Примечание – Под компонентами программного обеспечения понимают исходные коды, модели, предварительно скомпилированные коды или скомпилированное и связанное программное обеспечение.

Пример – Компоненты программного обеспечения, рассматриваемые в настоящем пункте, включают в себя:

- ***программные библиотеки от сторонних поставщиков (коммерческое готовое программное обеспечение);***
- ***внутренние уже использующиеся в электронных блоках управления компоненты.***

12.3 Входная информация

12.3.1 Предварительные требования

Необходима следующая информация:

– требования к компоненту программного обеспечения (из внешнего источника).

12.3.2 Дополнительная информация

Следующая информация может быть учтена:

– проектная спецификация компонента программного обеспечения (из внешнего источника);

– результаты предыдущих мер верификации компонента программного обеспечения (из внешнего источника).

12.4 Требования и рекомендации

12.4.1 Общие положения

Для квалификации компонента программного обеспечения необходимо наличие:

a) спецификации компонента программного обеспечения в соответствии с требованиями 12.4.3.1;

b) доказательства того, что компонент программного обеспечения выполняет свои требования в соответствии с 12.4.3.2, 12.4.3.3, 12.4.3.4;

c) доказательства того, что компонент программного обеспечения подходит для его целевого использования в соответствии с требованиями 12.4.4;

d) доказательства того, что процесс разработки программного обеспечения для компонента основан на соответствующем национальном или международном стандарте.

Примечание – В целях соблюдения требований данного пункта для ранее разработанных компонентов программного обеспечения могут быть выполнены некоторые действия по реинжинирингу.

12.4.2 Планирование квалификации компонента программного обеспечения

12.4.2.1 При планировании квалификации компонента программного обеспечения должны быть определены:

a) однозначная идентификация компонента программного обеспечения;

b) максимальное целевое значение УПБ, характеризующее любое из всех требований к системе безопасности, которые могут быть нарушены, если этот программный компонент выполняется неправильно;

c) действия, которые должны быть выполнены, чтобы квалифицировать компонент программного обеспечения.

12.4.3 Квалификация компонента программного обеспечения

12.4.3.1 Спецификация компонента программного обеспечения должна включать:

a) требования к компоненту программного обеспечения.

Пример – Требования к компоненту программного обеспечения:

– ***функциональные требования;***

– ***точность алгоритма или численная точность, где точность алгоритма рассматривает ошибки процедуры, которые позволяют получать только приближенное решение, а численная точность рассматривает ошибки округления, в результате которых возникают неточности вычислений и ошибки усечения, вызванные приближенным представлением многих функций в электронном блоке управления;***

– ***поведение в случае отказа;***

– ***время отклика;***

– ***используемый ресурс;***

– ***требования к среде реализации;***

– ***поведение в ситуации перегрузки (устойчивость к ошибкам);***

b) описание конфигурации.

Примечание – Для компонентов программного обеспечения, которые содержат более одного модуля программного обеспечения, описание конфигурации включает в себя уникальный идентификатор и конфигурацию каждого модуля программного обеспечения;

c) описание интерфейсов;

d) руководство по применению, при необходимости;

e) описание интеграции компонента программного обеспечения.

Примечание – Описание может включать в себя средства разработки, необходимые для интеграции и использования компонента программного обеспечения;

f) реакции функций при не соответствующих норме условиях эксплуатации.

Пример – Повторный вызов компонента программного обеспечения, не обладающего повторной входимостью;

g) зависимости от других компонентов программного обеспечения;

h) описание известных отклонений от нормы с соответствующими мерами для их «обхода».

12.4.3.2 Чтобы представить доказательства того, что компонент программного обеспечения выполняет свои требования, верификация этого компонента программного обеспечения должна:

a) показать охват требования в соответствии с требованиями раздела 9 26262-6.

Примечание – Эта верификация основывается, прежде всего, на тестировании на основе требований. Могут быть использованы результаты тестирования на основе требований компонента программного обеспечения, выполненного во время его разработки или во время предыдущих тестов интеграции.

Пример – Применение специального квалификационного набора тестов, анализ всех тестов, уже выполненных в ходе реализации и интеграции любого компонента программного обеспечения;

b) охватывать как нормальные условиях эксплуатации, так и поведение в случае отказа;

c) привести к отсутствию известных ошибок, которые ведут к нарушению требований к системе безопасности.

12.4.3.3 Требование данного подпункта распространяется на значения УПБА, равное D, в соответствии с 4.3. Чтобы оценить полноту набора тестов, должно быть измерено структурное покрытие в соответствии с требованиями раздела 9 ИСО 26262-6. При необходимости должны быть специфицированы дополнительные наборы тестов или должно быть предусмотрено обоснование.

12.4.3.4 Верификация в соответствии с требованиями 12.4.3.2 будет допустима только для реализации неизменяемого компонента программного обеспечения.

12.4.3.5 Квалификация компонента программного обеспечения должна быть документально оформлена, включая следующее:

a) уникальный идентификатор компонента программного обеспечения;

b) уникальную конфигурацию компонента программного обеспечения;

c) лицо или организацию, которые выполнили квалификацию;

d) описание внешней среды, используемой для квалификации;

e) результаты верификации мер, применяемых для квалификации компонента программного обеспечения;

f) максимальное целевое значение УПБ, характеризующее любое из всех требований к системе безопасности, которые могут быть нарушены, если этот программный компонент выполняется неправильно.

12.4.4 Верификация квалификации компонента программного обеспечения

12.4.4.1 Должны быть верифицированы результаты квалификации компонента программного обеспечения вместе с обоснованностью этих результатов относительно целевого использования компонента программного обеспечения. При необходимости должны быть применены дополнительные меры.

Примечание – Обоснованность квалификации может измениться, если квалификация выполняется для другой промышленной области или другого автомобильного применения.

Пример – Контроль двигателя, контроль кузова и контроль шасси – разные применения контроля в автомобиле. Железные дороги и гражданская бортовая радиоэлектроника – различные промышленные области.

12.4.4.2 Спецификация компонента программного обеспечения должна соответствовать требованиям целевого использования этого компонента программного обеспечения.

12.5 Результаты работы

12.5.1 Документация на компонент программного обеспечения

В результате выполнения требований 12.4.3.1.

12.5.2 Отчет о результатах квалификации компонента программного обеспечения

В результате выполнения требований 12.4.3.5.

12.5.3 План по обеспечению безопасности (уточненный)

В результате выполнения требований 12.4.2.

13 Квалификация комонентов аппаратных средств

13.1 Цели

Первой целью квалификации компонентов аппаратных средств является предоставление доказательств того, что компоненты и части аппаратных средств промежуточного уровня могут быть использованы в качестве части устройств, систем или элементов, разрабатываемых в соответствии с требованиями настоящего стандарта, касающихся их функционального поведения и их эксплуатационных ограничений для реализации целей концепции обеспечения безопасности.

Вторая цель квалификации компонентов аппаратных средств заключается в предоставлении соответствующей информации:

- об их видах отказов;
- о распределении их видов отказов;
- об их диагностических средствах, соответствующих концепции обеспечения безопасности для данного устройства.

13.2 Общие положения

Каждый связанный с безопасностью компонент или часть аппаратного средства, который используются в рамках области применения настоящего стандарта, подлежит стандартной квалификации, где рассматриваются общие функциональные характеристики, соответствие производству, срок службы во внешней среде и надежность.

Пример – Квалификация электронных компонент выполняется в соответствии со стандартами ИСО 16750 или с AEC-Q100 или AEC-Q200 или эквивалентными стандартами компании.

Для базовых частей (пассивный компонент, дискретный полупроводник) достаточно выполнить квалификацию в соответствии со стандартом на них, чтобы эти базовые части могли быть использованы в аппаратных средствах в соответствии с требованиями ИСО 26262-5.

Требования данного раздела распространяются на компоненты или части аппаратных средств промежуточного уровня, которые обеспечивают заданные функциональные возможности системы.

Пример – Датчики, приводы, интегральные схемы с заданной функциональностью (например, адаптер протокола).

Если компонент или часть аппаратных средств промежуточного уровня связаны с безопасностью, то в зависимости от их уровня они интегрируются и тестируются в соответствии с требованиями ИСО 26262-4 и/или ИСО 26262-5 и, кроме того, выполняется квалификация этих компонентов в соответствии с требованиями настоящего раздела.

Обычно квалификация, описанная в данном разделе, применяется к компонентам или частям, виды отказов или неисправности которых известны и которые являются в достаточной мере тестируемыми для выявления их возможных отказов.

Пример – В ходе разработки датчика давления топлива было определено, что датчик должен функционировать корректно в пределах границ диапазона его эксплуатационных параметров: для давления топлива до значения, равного 200 бар, и для температуры до значения, равного 140 °С. Квалификация этого датчика давления топлива позволяет использовать его для реализации конкретного, связанного с безопасностью устройства, учитывая функциональные характеристики датчика и его сбои при условии, что диапазон значений эксплуатационных параметров устройства такой же или уже. В такой ситуации можно не выполнять анализ проекта, а также интеграцию и тестирование базовых аппаратных средств датчика в соответствии с требованиями ИСО 26262-5, а действия по интеграции могут быть выполнены сразу после того, как в соответствии с требованиями ИСО 26262-4 датчику распределены технические требования к безопасности.

Краткое изложение квалификации и интеграции базовых частей, частей аппаратных средств и компонентов показаны в таблице 6.

Таблица 6 – Квалификация, интеграции и тестовые задачи, которые будут проводиться в зависимости от уровня части или компонента аппаратного средства

Действие	Часть или компонент аппаратного средства			
	Связанная с безопасностью базовая часть аппаратного средства	Связанная с безопасностью промежуточная часть аппаратного средства	Связанный с безопасностью промежуточный компонент аппаратного средства	Связанный с безопасностью сложный компонент аппаратного средства
	(например, резистор, транзистор)	(например, декодер кода Грея)	(например, датчик давления топлива)	(например, электронный блок управления)
Квалификация в соответствии со стандартом	Применимо	Применимо	–	–
Квалификация в соответствии с требованиями раздела 13	–	Применимо	Применимо	–
Интеграция / тестирование в соответствии с требованиями ИСО 26262-5	–	Применимо [a]	Применимо [a]	Применимо
Интеграция / тестирование в соответствии с требованиями ИСО 26262-4	–			Применимо

[a] Часть или компонент аппаратного средства будут интегрированы в соответствии с ИСО 26262-4 и/или ИСО 26262-5 в зависимости от их уровня

Квалификация компонентов или частей аппаратных средств может быть выполнена с помощью двух различных методов: тестирование или анализ. Эти методы могут быть использованы отдельно или вместе в зависимости от компонент или частей аппаратного средства.

- При тестировании компонент или часть аппаратного средства подвергается воздействию целевой окружающей среды и условий эксплуатации и при этом оценивается соблюдение их функциональных требований. Воспроизведение точных условий окружающей среды является трудной задачей, а любые экстраполяции также подвержены ошибкам, поэтому при интерпретации результатов тестирования учитываются ограничения таких условий тестирования.
- В основе выполнения квалификации с помощью анализа лежит обоснование аналитических методов и используемых допущений. В общем случае высокая сложность компонента аппаратного средства не позволят выполнить его квалификацию только с помощью анализа. Тем не менее, анализ может быть эффективно использован для экстраполяции результатов тестирования, чтобы определить влияние небольших изменений в уже протестированном компоненте аппаратных средств.

Даже если используются различные методы квалификации, окончательные результаты оформляются в виде отчета о квалификации (который может состоять из набора документов, содержащих отчеты о результатах, замечания по их интерпретации и т.д.), содержащем предположения, условия, а также тестовые примеры и их результаты, и который в соответствии с результатами используется для квалификации компонентов или частей аппаратных средств. Если это возможно, его лучше сформировать как объединение документов таким образом, чтобы была возможна независимая проверка. Такое объединение обычно включает в себя технические параметры, процесс квалификации, результаты и обоснования.

Указания, представленные в ИСО 16750, являются полезными для определения типа и последовательности квалификационных тестов.

13.3 Входная информация

13.3.1 Предварительные требования

Необходима следующая информация:

- требования, связанные с безопасностью;

– критерии (анализа и тестов) квалификации в соответствии с требованиями раздела 6 ИСО 26262-5;

– спецификация производителя для компонента или части аппаратного средства, или, если она недоступна, то предположения о спецификации для компонента или части аппаратного средства (из внешнего источника).

13.3.2 Дополнительная информация

Следующая информация может быть учтена:

– критерии тестирования в соответствии с требованиями раздела 6 ИСО 26262-5;

– дополнительная информация для стадий жизненного цикла системы безопасности, на которых применяется квалификация компонентов аппаратных средств.

13.4 Требования и рекомендации

13.4.1 Общие положения

13.4.1.1 Критериями для применения данного раздела являются:

a) квалифицируемый компонент или часть должны иметь промежуточную сложность, исключая сложные компоненты аппаратных средств и основные части аппаратных средств;

b) предполагается, что соответствующие виды отказов квалифицируемого компонента или части должны быть верифицируемыми путем тестирования и/или анализа.

13.4.2 Цели квалификации компонента или части аппаратного средства

13.4.2.1 Квалификацией компонента или части аппаратного средства должны быть достигнуты следующие цели:

a) адекватные эксплуатационные качества компонентов или частей, удовлетворяющие целям концепции обеспечения безопасности;

b) идентификацию видов отказов и их моделей (количественное выражение их распределения) с помощью соответствующих тестов (например, проверкой выхода за пределы заданного диапазона, ускоренным испытанием) или анализа;

c) достаточную надежность;

d) определение ограничений использования для компонентов или частей.

13.4.3 Методы квалификации компонента или части аппаратного средства

13.4.3.1 Квалификации компонента или части аппаратного средства выполняется соответствующим выбором из следующих методов:

a) анализ;

b) тестирование.

13.4.4 План квалификации

13.4.4.1 План квалификации должен быть разработан и должен описывать:

a) точное обозначение и номер версии компонента или части аппаратного средства;

b) спецификацию внешней среды, в которой предполагается применять компонент или часть аппаратного средства;

c) стратегию квалификации и ее обоснование.

Примечание – Стратегия включает в себя: анализ, необходимые тесты и пошаговое описание;

d) необходимые инструменты и оборудование, реализующие эту стратегию;

e) сторону, ответственную за выполнение этой стратегии;

f) критерии, используемые для оценки квалификации (прошел / не прошел) компонента или части аппаратного средства.

13.4.5 Подтверждение квалификации

13.4.5.1 Должно быть выполнено исчерпывающее обоснование, что функционирование компонента или части аппаратного средства соответствует его спецификации.

Примечание – Требуемое функционирование охватывает его поведение при установленных нормальных условиях внешней среды и в условиях внешней среды в сочетании с предполагаемым событием возникающего отказа.

13.4.5.2 Исчерпывающее обоснование (см. 13.4.5.1) должно быть основано на объединении следующей информации:

a) аналитические методы и используемые допущения или

b) данные из опыта эксплуатации или

c) существующие результаты тестирования.

13.4.5.3 Должно быть дано обоснование для каждого предположения, включая экстраполяции.

13.4.6 Квалификация с помощью анализа

13.4.6.1 Результаты анализа должны быть представлены в форме, которая может быть легко понята и проверена лицами, квалифицированными в соответствующих инженерных или научных дисциплинах.

Примечание – Аналитические методы, которые могут быть использованы, включают экстраполяции, математическое моделирование, анализ ущерба или подобные методы.

13.4.6.2 Анализ должен учитывать все условия внешней среды, которые влияют на компонент или часть аппаратного средства, предельные значения этих условий и другие дополнительные нагрузки на них в процессе работы (например, предполагаемые циклы переключения, заряд-разряд аккумуляторной батареи, длительные времена выключения).

13.4.7 Квалификация с помощью тестирования

13.4.7.1 Должен быть разработан план тестирования, который должен содержать следующую информацию:

a) описание функций компонента или части аппаратного средства;

b) количество и последовательность тестов, которые будут проводиться;

c) требования к сборке и соединениям;

d) процедуру ускоренного старения с учетом условий эксплуатации компонента или части аппаратного средства;

e) условия эксплуатации и окружающей среды для моделирования;

f) должны быть установлены критерии прошел / не прошел;

g) должны быть измерены параметры внешней среды;

h) требования к испытательному оборудованию, включая точность;

i) разрешенные во время тестирования процессы технического обслуживания и замены.

13.4.7.2 Должна использоваться стандартизированная спецификация теста.

Примечание – Такая спецификации может быть основана на серии стандартов ИСО 16750 или эквивалентных стандартах компании.

13.4.7.3 Тестирование должно проводиться в соответствии с планом и данные результатов испытаний должны быть доступны.

13.4.8 Отчет о квалификации

13.4.8.1 В отчете о квалификации должно быть установлено, прошел или не прошел квалификацию компонент или часть аппаратного средства по отношению к рабочему диапазону значений параметров эксплуатации.

Примечание – Отчет о квалификации может состоять из набора документов, который включает в себя отчеты о результатах и замечания по их интерпретации.

13.4.8.2 Отчет о квалификации должен быть верифицирован в соответствии с требованиями раздела 9.

13.5 Результаты работы

13.5.1 План квалификации

В результате выполнения требований 13.4.4.

13.5.2 План тестирования компонента технического средства

В результате выполнения требований 13.4.7.1, если они применимы.

13.5.3 Отчет о квалификации

В результате выполнения требований 13.4.8.1.

14 Подтверждение проверкой эксплуатацией

14.1 Цель

Данный раздел содержит указания по подтверждению проверкой эксплуатацией. Подтверждение проверкой эксплуатацией является альтернативным средством обеспечения соответствия требованиям настоящего стандарта, которое может быть использовано в случае повторного использования существующих элементов или элементов, для которых известны эксплуатационные данные.

14.2 Общие положения

Подтверждение проверкой эксплуатацией может быть применено к любому типу изделия, определение и условия использования которого являются идентичными или очень похожи для изделия, которое уже выпущено и находится в эксплуатации. Оно также может быть применено к любому результату работы, связанному с такими изделиями.

Примечание – Подтверждение проверкой эксплуатацией не является взаимозаменяемостью: одно изделие, спроектированное или реализованное альтернативным способом, которое предназначено, чтобы заменить проверенное эксплуатацией изделие, не может считаться проверенным в эксплуатации, потому что оно удовлетворяет исходным функциональным требованиям, но не соответствует критериям, указанным в настоящем разделе.

Устройство или элемент, такой как система, функция, аппаратное средство или программный продукт, могут быть кандидатами на подтверждение проверкой эксплуатацией.

Кандидатами на подтверждение проверкой эксплуатацией могут быть также результаты работы на уровне системы, на уровне разработки аппаратных средств или программного обеспечения, такие как техническая концепция безопасности, алгоритмы, модели, исходный код, объектный код, компоненты программного обеспечения, набор данных о конфигурации или калибровке.

Мотивацией использования подтверждения проверкой эксплуатацией является:

a) намерение использовать коммерческие решения в автомобилестроении частично или полностью для реализации другой цели; или

b) намерение в эксплуатируемом электронном блоке управления реализовать дополнительную функцию; или

c) кандидат на подтверждение проверкой эксплуатацией находился в эксплуатации до выпуска настоящего стандарта; или

d) кандидат на подтверждение проверкой эксплуатацией используется в других связанных с безопасностью областях; или

e) кандидат на подтверждение проверкой эксплуатацией является коммерческим коробочным программным продуктом, предназначенным не только для автомобильных применений.

Подтверждение проверкой эксплуатацией обосновывается соответствующими документами о кандидате, отчетами об управлении конфигурацией и управлении изменениями и эксплуатационными данными о связанных с безопасностью инцидентах.

Как только определен кандидат (см. 14.4.3) с предполагаемым доверием проверке эксплуатацией (см. 14.4.2), при подготовке подтверждения проверкой эксплуатацией необходимо учитывать два важных критерия:

- предназначение эксплуатационных данных в течение срока службы кандидата (см. 14.4.5) и
- изменения, если таковые имеются, которые могут повлиять на кандидата во время его срока службы (см. 14.4.4).

Примечание – Что касается предназначения эксплуатационных данных, то подтверждение проверкой эксплуатацией направлено на устранение систематических и случайных отказов кандидата и не устраняет отказы, связанные со старением кандидата.

Использование проверенных эксплуатацией устройств или элементов не освобождает эти устройства или элементы от последующих зависимых от проекта действий, связанных с менеджментом системы безопасности, так как:

- доверие проверке эксплуатацией зафиксировано в плане по обеспечению безопасности и
- данные и результаты подтверждения проверкой эксплуатацией являются частью обоснования безопасности и на них распространяются действия средств подтверждения.

14.3 Входная информация

14.3.1 Предварительные требования

Необходима следующая информация:

– связанная с целевым использованием одного из кандидатов:

– спецификация кандидата,

– установленные цель(и) безопасности или требование(я) безопасности с соответствующим(и) УПБА,

– предсказуемая эксплуатационная ситуация и целевые режимы работы и интерфейсы;

- связанная с предыдущим использованием кандидата:
- эксплуатационные данные в течение срока службы (из внешнего источника).

14.3.2 Дополнительная информация

Следующая информация может быть учтена:

- связанная с предыдущим использованием кандидата:
- обоснование безопасности в соответствии с 6.5.3 ИСО 26262-2.

Примечание – Для кандидата, разработанного не в соответствии с требованиями настоящего стандарта (например, коммерческий коробочный программный продукт; кандидаты, разработанные в соответствии с требованиями стандартов по безопасности, отличных от настоящего стандарта, таких как МЭК 61508 или RTCA DO-178), некоторые результаты обоснования безопасности могут быть недоступны. В таком случае они заменяются имеющимися данными, полученными при разработке кандидата.

14.4 Требования и рекомендации

14.4.1 Общие положения

14.4.1.1 Требования следующих пунктов определяют значения УПБА для будущего кандидата.

14.4.2 Доверие проверке эксплуатацией

14.4.2.1 Доверие проверке эксплуатацией должно использоваться только тогда, когда кандидат соответствует требованиям 14.4.2 – 14.4.5.

14.4.2.2 Доверие проверке эксплуатацией, получаемое в результате подтверждения проверкой эксплуатацией должно планироваться в соответствии с требованиями 6.4.3.5 ИСО 26262-2.

14.4.2.3 Доверие проверке эксплуатацией должно распространяться на подстадии жизненного цикла системы безопасности и на действия, охваченные подтверждением проверкой эксплуатацией кандидата.

14.4.2.4 Интеграция средств проверки эксплуатацией в устройстве или элементе должна выполняться на соответствующем уровне в соответствии с требованиями раздела 8 ИСО 26262-4.

Пример – Аппаратные средства электронного блока управления имеют удовлетворительную историю обслуживания и на 100% могут быть перенесены в новое применение. Доверие проверке эксплуатацией может быть применено к подстадиям и действиям по разработке этого элемента аппаратного средства. Аналогично, если программное обеспечение на 100% переносится с удовлетворительной историей обслуживания, то доверие проверке эксплуатацией также можно применять и к подстадиям и действиям по разработке программного обеспечения.

14.4.2.5 Подтверждение соответствия безопасности для устройства, в которое встроены проверенные эксплуатацией элементы, должно выполняться в соответствии с требованиями раздела 9 ИСО 26262-4.

14.4.2.6 Меры подтверждения устройства, в которое встроены проверенные эксплуатацией элементы, должны рассматривать подтверждения проверкой эксплуатацией и соответствующие данные согласно требованиям 6.4.7 ИСО 26262-2.

14.4.2.7 Любое изменение проверенного эксплуатацией устройства или элемента должны соответствовать требованиям 14.4.4 для обеспечения соответствующего доверия проверке эксплуатацией.

Примечание – Настоящий подпункт применяется к любому типу модификации, в том числе и к модификации, инициированной связанным с безопасностью инцидентом.

14.4.3 Минимальная информация, необходимая кандидату

14.4.3.1 Описание кандидата и его предыдущего использования должно быть доступно и включать в себя:

a) идентификацию и прослеживаемость кандидата в каталоге внутренних элементов или компонентов, если такой имеется,

b) соответствующие требования к установке, форме и функции, которые описывают, если это применимо, интерфейс и окружающую среду, физические и размерные, функциональные и эксплуатационные характеристики кандидата;

c) требования к безопасности кандидата в предыдущей эксплуатации и соответствующие значения УПБА, если таковые имеются.

14.4.4 Анализ изменений кандидата

14.4.4.1 Кандидаты, проверенные эксплуатацией

Изменения кандидатов и их окружение должны быть определены в соответствии с требованиями 14.4.4.2 и 14.4.4.3.

Примечания

1 Изменения кандидатов ведут к изменениям в разработке и к изменениям в реализации. Изменения в разработке могут возникнуть в результате модификации требований, функциональных усовершенствований, либо с целью повышения эффективности. Изменения в реализации не влияют на спецификацию или эффективность кандидата, а только на его особенности реализации. Изменениями в реализации могут быть исправления программного обеспечения или использование новой разработки или новых инструментальных средств.

2 Изменения данных конфигурации или данных калибровки рассматриваются как изменения кандидата, если они влияют на его поведение, что приводит к нарушению целей безопасности.

3 Изменения в окружающей среде кандидата могут возникнуть в результате использования этого кандидата в новом типе применения, с другими целями безопасности или требованиями, в результате его установки в новой целевой окружающей среде (например вариант транспортного средства и диапазона условий окружающей среды) или в результате модернизации компонент взаимодействующих с ним или расположенных вблизи от него.

14.4.4.2 Изменения устройств, выполняемые для будущего применения

Изменения устройств и их окружения, выполняемые с целью дальнейшего применения, должны соответствовать требованиям 6.4.2 ИСО 26262-3.

14.4.4.3 Изменения элементов, выполняемые для будущего применения

Изменения элементов и их окружения, выполняемые с целью дальнейшего применения в другом устройстве, должны соответствовать требованиям раздела 8.

14.4.4.4 Изменения кандидата, независимые от дальнейшего применения

Изменения кандидата, выполненные после его срока службы и независимые от дальнейшего применения, должны быть подтверждены доказательством того, что статус кандидата, проверенного эксплуатацией, не изменился.

14.4.5 Анализ эксплуатационных данных

14.4.5.1 Управление конфигурацией и управление изменениями

Должно быть предоставлено доказательство, что во время и после срока службы кандидата для него были реализованы технологии управления конфигурацией и управление изменениями так, что текущий статус кандидата может быть установлен.

14.4.5.2 Целевые значения для проверки эксплуатацией

Примечание – Если для кандидата не определено значение УПБА, то для него выбирается целевое значение УПБА с большим запасом, равное D.

14.4.5.2.1 Должно быть предоставлено обоснование для расчета срока службы кандидата.

14.4.5.2.2 Срок службы кандидата будет определяться сложением периода наблюдения для всех образцов в соответствии с рекомендацией из 14.4.5.2.3.

14.4.5.2.3 Перед тем как проводить анализ срока службы кандидата, необходимо, чтобы период наблюдений каждого образца с одинаковой спецификацией и реализацией в качестве кандидата и время работы в транспортном средстве превышали среднегодовое время работы транспортного средства.

14.4.5.2.4 Чтобы кандидат получил статус «проверен эксплуатацией», его срок службы должен продемонстрировать соответствие с каждой целью безопасности, которая может быть нарушена кандидатом, в соответствии с таблицей 7 с односторонним нижним уровнем доверия 70 % (используя распределение хи-квадрат).

Примечания

1 Для целей подтверждения проверкой эксплуатацией наблюдаемый инцидент означает отказ, о котором сообщается производителю, и который вызван кандидатом и может привести к нарушению цели безопасности.

Таблица 7 – Пределы наблюдаемой интенсивности инцидентов

УПБА	Наблюдаемая интенсивность инцидентов
D	$< 10^{-9}$/час
C	$< 10^{-8}$/час
B	$< 10^{-8}$/час
A	$< 10^{-7}$/час

2 Характер и интенсивность наблюдаемых инцидентов интерпретируются при анализе возможного нарушения целей безопасности в процессе эксплуатации.

3 Таблица 8 представляет пример требуемого минимального срока службы без наблюдаемого инцидента, который необходим для достижения 70%-ой уверенности:

Таблица 8 – Целевые значения минимального срока службы кандидата

УПБА	Минимальное значение срока службы без наблюдаемого инцидента
D	$1,2 \times 10^{9}$ час
C	$1,2 \times 10^{8}$ час
B	$1,2 \times 10^{8}$ час
A	$1,2 \times 10^{7}$ час

4 Если в собранных данных для образцов находятся наблюдаемые инциденты, то необходимый минимальный срок службы $t_{\text{службы}}$, может быть скорректирован следующим образом:

$$t_{\text{службы}} = t_{MTTF} \times \frac{(\chi_{CL;2f+2})}{2},$$

где CL - уровень доверия как абсолютное значение (например, 0,7 для 70%);

t_{MTTF} - наработка на отказ (1 / интенсивность отказов);

f - число связанных с безопасностью инцидентов;

$(\chi_{\alpha,\nu})^2$ - распределение хи-квадрат с вероятностью ошибки α и ν степеней свободы.

14.4.5.2.5 Доверие проверке эксплуатацией можно предварительно предсказать до получения статуса «проверен эксплуатацией» (в соответствии с 14.4.5.2.4). В этом случае срок службы кандидата должен демонстрировать соответствие с каждой целью безопасности, которая может быть нарушена кандидатом в соответствии с таблицей 9 с односторонним нижним доверительным уровнем 70% (используя распределение хи-квадрат).

Таблица 9 – Пределы наблюдаемой интенсивности инцидентов (промежуточный период)

УПБА	Наблюдаемая интенсивность инцидентов
D	$< 3 \times 10^{-9}$ / час
C	$< 3 \times 10^{-8}$ / час
B	$< 3 \times 10^{-8}$ / час
A	$< 3 \times 10^{-7}$ / час

14.4.5.2.6 В случае любого наблюдаемого инцидента при эксплуатации в течение промежуточного периода, описанного в 14.4.5.2.5, должно быть выполнено следующее:

- прекратить использование таблицы 9 для наблюдаемой интенсивности инцидентов и использовать для кандидата таблицу 7; или
- предоставить доказательства того, что причина наблюдаемого инцидента полностью выявлена и устранена в соответствии с настоящим стандартом, и продолжить считать общее количество часов для кандидата, сбросив счетчик общего количества часов для данной конкретной причины, и документально оформить это доказательство в обосновании безопасности.

14.4.5.2.7 Если интенсивность отказов кандидата является непостоянной величиной, то для подтверждения проверкой эксплуатацией должны применяться дополнительные меры, например, в случае повреждения в результате усталости.

Примечание – Меры, применяемые к кандидатам с различной интенсивностью отказов, в значительной степени зависят от таких факторов, как износ, старение или количества часов работы за время срока службы устройства. Они могут включать специальные испытания на долговечность или применять более длительный период наблюдения.

14.4.5.3 Проблемы эксплуатации

Система отчетов о проблемах должна обеспечить, чтобы любой наблюдаемый инцидент с возможным воздействием на безопасность, вызванный кандидатом при эксплуатации, был документально оформлен и устранен в период работы кандидата (см. 6.4.2.1 ИСО 26262-7).

14.5 Результаты работы

14.5.1 План по обеспечению безопасности (уточненный)

В результате выполнения требований 14.4.2.1 – 14.4.2.7.

14.5.2 Описание кандидата для подтверждения проверкой эксплуатацией

В результате выполнения требований 14.4.3.

14.5.1 Отчеты анализа проверок эксплуатацией

В результате выполнения требований 14.4.4 – 14.4.5.

Приложение А
(справочное)

Обзор и поток документов вспомогательных процессов

Таблица А.1 содержит обзор целей, предварительных требований и результатов работы вспомогательных процессов.

Таблица А.1 – Обзор вспомогательных процессов

Раздел	Цели	Предварительные требования	Результаты работы
5 Взаимодействие в совместных разработках	Цель данного раздела заключается в описании процедур и распределении соответствующих сфер ответственностей в рамках совместной разработки устройств и элементов	См. применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, на которых планируется и осуществляется совместная разработка	5.5.1 Отчет о выборе поставщика. 5.5.2 Соглашения о взаимодействии при разработке. 5.5.3 План работы поставщика. 5.5.4 План обеспечения безопасности поставщика. 5.5.5 Отчет по оценке функциональной безопасности. 5.5.6 Договор поставки
6 Спецификация и менеджмент требований к системе безопасности	Первая цель заключается в обеспечении корректной спецификации требований к системе безопасности, их атрибутов и характеристик. Вторая цель заключается в обеспечении согласованного менеджмента требований к системе безопасности на протяжении всего ее жизненного цикла	См. применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, на которых специфицируется или выполняется менеджмент требований к системе безопасности	Не формируются
7 Управление конфигурацией	Первая цель – обеспечить, чтобы результаты работы, а также принципы и общие условия их создания моли быть однозначно определены и воспроизведены в любое время. Вторая цель – обеспечить, чтобы отношения и различия между ранней и текущей версиями можно было проследить	План обеспечения безопасности в соответствии с 6.5.1 ИСО 26262-2. Применимые предварительные требования соответствующих стадий жизненного цикла систем безопасности, где планируется или реализуется управление конфигурацией	7.5.1 План управления конфигурацией
8 Управление изменениями	Целью управления изменениями является анализ и контроль изменений, связанных с безопасностью результатов работы на протяжении всего жизненного цикла системы безопасности	План управления конфигурацией (см. 7.5.1). План обеспечения безопасности в соответствии с 6.5.2 ИСО 26262-2	8.5.1 План управления изменением. 8.5.2 Запрос на изменение. 8.5.3 Анализ влияния и план запроса на изменения. 8.5.4 Отчет об изменении
9 Верификация	Целью верификации является обеспечение соответствия результатов работы их требованиям	См. применимые предварительные требования соответствующих стадий жизненного цикла системы безопасности, на которых планируется или выполняется верификация	9.5.1 План верификации. 9.5.2 Спецификация верификации. 9.5.3 Отчет о верификации

Продолжение таблицы А.1

Раздел	Цели	Предварительные требования	Результаты работы
10 Документирование	Основная цель заключается в разработке стратегии управления документированием в течение всего жизненного цикла системы безопасности в целях обеспечения эффективности и воспроизводи-мости процесса управления документацией	План по обеспечению безопасности в соответствии с 6.5.1 ИСО 26262-2	10.5.1 План управления документацией. 10.5.2 Руководящие указания по документированию
11 Уверенность в использовании инструментального программного обеспечения	Первая цель данного раздела заключается в предоставлении критериев для определения необходимого уровня доверия инструментального программного обеспечения, если они применяются. Второй целью данного раздела является обеспечение средств для квалификации инструментального программного обеспечения, если они применяются, в целях формирования доказательств того, что инструментальное программное обеспечение может быть использовано для настройки действий или задач, предусмотренной настоящим стандартом (т. е. пользователь может рассчитывать на правильное функционирование инструментального программного обеспечения для этих действий или задач, предусмотренное настоящим стандартом)	План по обеспечению безопасности в соответствии с 5.5.2 ИСО 26262-4. Применимые предварительные условия стадий жизненного цикла системы безопасности, на которых используется инструментальное программное обеспечение	11.5.1 Отчет о критериях оценки инструментального программного обеспечения. 11.5.2 Отчет о квалификации инструментального программного обеспечения
12 Квалификация компонентов программного обеспечения	Целью квалификации компонентов программного обеспечения является предоставление доказательств о возможности их повторного использования в устройствах, разрабатываемых в соответствии с требованиями настоящего стандарта	Требования к компоненту программного обеспечения (из внешнего источника)	12.5.1 Документация на компонент программного обеспечения. 12.5.2 Отчет о результатах квалификации компонента программного обеспечения. 12.5.3 План по обеспечению безопасности (уточненный)
13 Квалификация компонентов аппаратных средств	Первой целью квалификации компонентов аппаратных средств является предоставление доказательств того, что компоненты и части аппаратных средств промежуточного уровня могут быть использованы в качестве части устройств, систем или элементов, разрабатываемых в соответствии с требованиями настоящего стандарта, касающихся их функционального поведения и их эксплуатационных ограничений для реализации целей концепции обеспечения безопасности. Вторая цель квалификации компонентов аппаратных средств заключается в предоставлении соответствующей информации: об их видах отказов; о распределении их видов отказов; об их диагностических средствах, соответствующих концепции обеспечения безопасности для данного устройства	Требования, связанные с безопасностью. Критерии (анализа и тестов) квалификации в соответствии с требованиями раздела 6 ИСО 26262-5. Спецификация производителя для компонента или части аппаратного средства, или, если она недоступна, то предположения о спецификации для компонента или части аппаратного средства (из внешнего источника)	13.5.1 План квалификации. 13.5.2 План тестирования компонента технического средства. 13.5.3 Отчет о квалификации

Окончание таблицы А.1

Раздел	Цели	Предварительные требования	Результаты работы
14 Подтверждение проверкой эксплуатацией	Данный раздел содержит указания по подтверждению проверкой эксплуатацией. Подтверждение проверкой эксплуатацией является альтернативным средством обеспечения соответствия требованиям настоящего стандарта, которое может быть использовано в случае повторного использования существующих элементов или элементов, для которых известны эксплуатациионные данные	Информация, связанная с целе-вым использованием одного из кандидатов: – спецификация кандидата; – применимые цель(и) безопасности или требование(я) безопасности с соответствующим(и) УПБА; – предсказуемая эксплуатационная ситуация и целевые режимы работы и интерфейсы. Информация, связанная с предыдущим использованием кандидата: – эксплуатационные данные в течение срока службы (из внешнего источника)	14.5.1 План по обеспечению безопасности (уточненный). 14.5.2 Описание кандидата для подтверждения проверкой эксплуатацией. 14.5.1 Отчеты по анали-зу проверок эксплуата-цией

Приложение В
(справочнное)

Пример соглашения о взаимодействии при разработке (СВР)

В.1 Цели

В настоящем приложении приводится иллюстративный пример соглашения о взаимодействии при разработке (СВР) в соответствии с требованиями раздела 5 [перечисления c) – g) 5.4.3.1], с адаптацией под конкретную организацию в соответствии с требованиями и рекомендациями 5.4.5 и 5.5.1 ИСО 26262-2, если необходимо. Также может быть выполнена настройка действий по обеспечению безопасности для конкретного проекта в соответствии с требованиями 6.4.5 ИСО 26262-2.

В.2 Общие положения

На вид и объем взаимодействий заказчик–поставщик будет влиять много факторов; данный пример упрощен и основан на применении сценария взаимодействия, описанного в В.3, и наборе исходных условий, перечисленных в В.4.

В таблицах В.1 – В.3 представлен пример СВР:

- таблица В.1 примерно соответствует требованиям 5.4.2 с некоторыми дополнениями для конкретной организации, предназначенными для предотвращения или устранения риска от поставщика с не отвечающими требованиям возможностями;
- таблица В.2 примерно соответствует требованиям 5.4.3 с некоторыми дополнениями для конкретной организации, предназначенными для предотвращения или устранения риска от неправильного понимания или определения границы компонента С и его взаимодействий с его окружением;
- таблица В.3 примерно соответствует требованиям 5.4.4 применительно к компоненту С аппаратных средств.

Примечание – В каждой таблице соответствующий раздел настоящего стандарта указан в скобках.

В.3 Сценарий применения

Примеры СВР, представленные в таблицах В.1 – В.3, основаны на следующем сценарии применения:

a) Заказчик несет ответственность за проектирование и производство транспортного средства.

b) Заказчик несет ответственность за проектирование системы, состоящей из большого количества компонентов аппаратных средств и программного обеспечения, среди которых один компонент аппаратных средств С должен быть поставлен другим поставщиком.

c) Для компонента С будут определены требования, соответствующие значению УПБА, равному D.

d) Компонент С не был ранее разработан, т. е. он не является коммерческим продаваемым изделием. Он включает в себя новые технологии, для которых нет достаточного пула проверенных поставщиков.

e) Множество поставщиков заинтересованы в поставке компонента С, но их возможности, отвечающие требованиям для поддержки проекта, не очевидны.

f) Используется процесс разработки, основанный на модели.

В.4 Исходные условия

Данный пример разработан на основе следующих исходных условий:

a) Ресурсы, необходимые для управления проектом и раработки, доступны в случае необходимости.

b) Оценки команд, которые квалифицируются как «независимые», доступны для каждой участвующей организации и используются там, где это необходимо.

c) При выполнении независимой оценки для всех участвующих организаций, претендующих на самый высокий уровень полноты, используется одинаковый процесс и общая архитектура.

1) Чтобы квалифицировать на требуемый уровень полноты, повторно используемые средства согласовывают с процессом и общей архитектурой и независимо оценивают.

2) Чтобы квалифицировать на требуемый уровень полноты другие ресурсы, например, инструментальные средства, согласовывают с процессом и общей архитектурой и независимо оценивают.

3) Участвующие организации выбирают конкретные процессы и инструменталь-ные средства, которые совместимы и выполняются в той же архитектуре.

4) Явные мета-модели или спецификации однозначно определяют семантики инструментов, языков моделирования, языков программирования, а также создаваемых моделей.

5) Модели внешне наблюдаемого поведения, рабочие характеристики (в том числе в наихудших условиях) и виды отказов и их влияние доступны для компонентов аппаратных средств, включая устройства ввода / вывода. Модели представлены в форме, которая может обеспечить корректную интеграцию для создания моделей (суб)системы.

d) Обеспечено высококачественное выполнение других взаимодействий заказчик-поставщик, реализуемых не только для проектирования, обеспечивающего высокий уровень полноты, которые не включены в данный пример, например, взаимодействие бизнес-процессов, управление проектами и управление качеством.

Если исходные условия, перечисленные выше, не выполняются, то потребуются дополнительные взаимодействия заказчик-поставщик и последующие усилия, которые не определены в данном примере.

Таблица В.1 – Обмен данными заказчик-поставщик для квалификации и выбора поставщика

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
A.1	Предварительный выбор поставщиков. Проект независимых критериев. См. 5.4.2	Анкета оценки [a]: - культуры безопасности (5.4.2 ИСО 26262-2); - свидетельства компетентно-сти (5.4.3 ИСО 26262-2); - доказательства наличия управления качеством (5.4.4 ИСО 26262-2); - требования настоящего стандарт.. Согласие на, например: - независимую оценку (5.4.5); - шаблон СВР	–
A.2		–	Принятие условий [a]
A.3		–	Возможность оценки [a] (раздел 5 ИСО 26262-2). Сообщаемая информация [a] Предложенные корректирующие действия [a]
A.4		Оценка: Значения УПБА компонента, для которого квалификация не выполнена [a]	–
A.5	Квалификация поставщиков (короткий лист) 5.4.2	Конкретный для организации заказчика процесс настройки согласно 5.4.5 ИСО 26262-2, включая методы, языки, инструменты и применяемые ограничения / руководства	–
		–	Оценка соответствия 1-й стороной. Сообщаемая информация [a]. Достижения по критериям выбора (5.4.2.1). Предложенные корректирующие действия [a]. Альтернативный подход или предложения для достижения целей [a]
		Повторяющиеся оценка и запросы о проблемах и альтернативах [a]	Повторяющиеся изменения к планам и альтернативам [a]
		Оценка: Значения УПБА компонента, для которого квалификация не выполнена [a]	–
A.6	Приглашение к выбору поставщика 5.4.2.2	Запрос на ресурсы / запрос предложений, включая процесс настройки под конкретный проект [перечисление b) 5.4.3.1], концепцию изделия, то есть определение устройства (5.5 ИСО 26262-3) и целей безопасности (7.5.2 ИСО 26262-3)	–
A.7	–	–	Предложение. Декларация о соответствии. Обновления предварительно подписанной информации [a]
A.8	Выбор поставщика 5.4.2	Предлагаемое СВР (для конкретного проекта) 5.4.3	–
A.9		–	Ресурсы выбранного проекта и возможность их оценки, например навыки, компетентность и квалификация членов команды по безопасности (5.5.2 ИСО 26262-2). Правила и процессы конкретной организации (5.5.1 ИСО 26262-2), включая инструменты, библиотеки. Предварительные планы, например план по обеспечению безопасности (6.5.1 ИСО 26262-2)
A10		Повторяющиеся оценка и запросы, например при нехватке квалифицированных кадров [a]	Повторяющиеся изменения решения проблем заказчика [a]

Окончание таблицы В.1

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
A.11	Выбор поставщика 5.4.2	Принятие СВР. (5.5.2) Отчет о выборе поставщика (5.5.1)	Принятие СВР (5.5.2)
A.12		Договор на разработку концепции (ИСО 26262-3, ИСО 26262-4) и стадии планирования (раздел 5 ИСО 26262-4), включая формулировку задания на опытно-конструкторскую разработку	Принятие
[a] Деятельность или данные конкретной организации, которые не регламентируются настоящим стандартом.			

Таблица В.2 – Обмен данными заказчик-поставщик при инициировании и формировании концепции проекта

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
B.1	Инициирование проекта (5.4.3). Формироание концепции функциональной безопасности (разделы 5 – 8 ИСО 26262-3)	Планы на уровне системы. Определение устройства (5.5 ИСО 26262-3) и его жизненного цикла (рис. 1, 5.2.2 ИСО 26262-2, рисунок 2 ИСО 26262-2 и 6.4.5 ИСО 26262-2) Концепция функциональной безопасно-сти (раздел 8 ИСО 26262-3)	–
B.2	–	–	План проекта (5.5.3). План обеспечения безопасности (5.5.4). Анализ опасностей и оценка рисков (5.4.3.2), модели поведения компонент аппаратных средств, включая метрики неисправностей [перечисление f) 5.4.3.1, приложение В ИСО 26262-5, и 9.4.3.1 ИСО 26262-5]. Независимые оценки планов, включающие гарантии того, что процессы и ресурсы, которые сконфигурированы и выделены в соответствии с требуемыми результатами работы, а также профессиональными навыками [перечисления c) e) и g) 5.4.3 и 5.4.5]
B.3	–	Принятие	–
B.4	Рассмотрение опыта, накопленного для компонентов проверенных эксплуатацией, инструментов, библиотек, используемых в подобных проектах (5.4.4.5), а так-же данных о проверке эксплуатацией и анализа возможных кандидатов (раздел 14 ИСО 26262-8)	Первоначальный план обеспечения безопасности (раздел 5 ИСО 26262-2), включая структуру отчета об оценке безопасности системы	–
B.5	–	–	Предложены проверенные эксплуатацией элементы (раздел 14) с независимой оценкой пригодности для данного проекта (5.4.5 и таблица 1 ИСО 26262-2)
B.6	–	Принятие	

Окончание таблицы В.2

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
B.7	Жизненный цикл разработки системы [перечисление в) 5.4.3] –	Техническая концепция системы безопасности (7.5.1 ИСО 26262-4), соответствующие части спецификации проекта системы, спецификации аппаратных средств, ограничения проектирования и реализации, спецификации программно-аппаратного интерфейса (7.5.3 ИСО 26262-4)	Повторные оценки, разъяснения запросов, и отзывы о конфликтах, полноте, согласованности и т. д.; технологические ограничения, если таковые имеются; запросы на изменения, если таковые имеются (5.4.4). Обновленные модели поведения, включая модели неисправностей
B.8		Повторно получаемые разъяснения, ответы и изменения, в том числе спецификации проектирования и верификации архитектуры системы (7.5.2 ИСО 26262-4, 7.5.5 ИСО 26262-4), спецификации аппаратных средств (7.5.1 ИСО 26262-5), относящиеся к компоненту С, программно-аппаратному интерфейсу, распределению и т.д.	Отзыв о границе между компонентом С и его окружением
B.9	–	–	Принятие

Таблица В.3 – Обмен данными заказчик-поставщик о жизненном цикле разработки аппаратных средств

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
C.1	План (5.4.3)	Разрешение для разработки аппаратных средств	–
C.2		–	Планы: план обеспечения безопасности (5.5.4 и 5.5. ИСО 26262-5), план проекта (5.5.3 и 5.5.2 ИСО 26262-5), план интеграции и тестирования устройства (5.5.3 ИСО 26262-4), планирование СВР (5.4.3) и др. Независимые отчеты о соответствии планированию (5.4.4.8 и 5.4.5)
C.3		Принятие спецификации требований и разрешение начать по ним работать	–
C.4	Требования (5.4.5 и ИСО 26262-5)	–	Спецификации аппаратных средств – вы-веденных; уточненных, учитывающих ограничения разработки и реализации (7.5.1 ИСО 26262-5). Расширение плана верификации [a]. Запросы на изменение программно-аппаратного интерфейса, если таковые имеются (10.5 ИСО 26262-5). Независимый аудит системы безопасности (5.4.4.8). Независимое подтверждение (5.4.5 и 5.5.5)
C.5	–	Принятие и разрешение начать проектирование	–
C.6	Проект (5.4.5 и ИСО 26262-5)	–	Спецификации проекта (7.5.1 ИСО 26262-5), ограничения реализации, включая архитектурные (раздел 8 ИСО 26262-5). Расширение или модификация анализа опасностей и оценки рисков (раздел 7 ИСО 26262-3), если необходимо. Дополнение к плану интеграции и тестирования устройства (10.5 ИСО 26262-5). Запросы на изменение программно-аппаратного интерфейса, если таковые имеются (10.5 ИСО 26262-5). Независимый аудит системы безопасности (5.4.4.8, 5.4.5)

Окончание таблицы В.3

ID	Деятельность	Данные от заказчика поставщику	Данные от поставщика заказчику
C.7	5.4.4 и 5.4.5	Повторные оценки и отзывы о конфликтах, обнаруженных на уровне системы	Повторные разъяснения, изменения и другие ответы на получаемые от заказчика отзывы и запросы. Независимая оценка (5.4.5 и 5.5.5)
C.8	5.4.4 и 5.4.5	Принятие проекта компонента. Разрешение на реализацию	Реализация Требования окружающей среды. Независимая оценка (5.4.5 и 5.5.5)
C.9	–	Принятие	–
C.10	–	–	Прототип части. Комплексная верификация (10.5 ИСО26262-5) Независимая оценка (5.4.5)
C.11	–	Комплексная оценка (раздел 8 ИСО 26262-4). Запросы на изменение, если таковые имеются	–
C.12	–	–	Отчеты и аудиты выполненных изменений. Независимая оценка (5.4.5, 5.5.5)
C.13	–	Принятие	–
C.14	–	–	Образец для серийного производства. Независимая оценка (5.4.5, 5.5.5)
C.15	–	Комплексная оценка (раздел 8 ИСО 26262-4). Запросы на изменение, если таковые имеются	–
C.16	–	–	Отчеты и аудиты выполненных изменений. Независимая оценка (5.4.4, 5.4.5 и 5.5.5)
C.17	–	Разрешение на запуск стадии производства	–
C.18	–	–	Отчеты после начала производ-ства (5.4.6, а также 5.5.6 и 7.5 ИСО 26262-2)

[a] Деятельность или данные конкретной организации, которые не регламентируются настоящим стандартом.

Приложение ДА
(справочное)

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

Таблица ДА

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 26262-1:2011	–	*
ИСО 26262-2:2011	–	
ИСО 26262-3:2011	–	*
ИСО 26262-4:2011	–	*
ИСО 26262-5:2011	–	
ИСО 26262-6:2011	–	
ИСО 26262-7:2011	–	*
ИСО 26262-9:2011	–	*
ISO/IEC 12207	IDT	ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств

* 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.

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT – идентичные стандарты.

Библиография

[1] ISO 10007, Quality management systems — Guidelines for configuration management

[2] ISO 16750 (all parts), Road vehicles — Environmental conditions and testing for electrical and electronic equipment

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

[4] ISO/IEC 15504 (all parts), Information technology — Process assessment

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

[6] RTCA DO-178 B, Software Considerations in Airborne Systems and Equipment Certification

[7] CMMI, gost.e-ecolog.ru /

[8] German V-Model, gost.e-ecolog.ru

[9] AEC-Q100, Stress Qualification For Integrated Circuits

[10] AEC-Q200, Stress Test Qualification For Passive Components

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 Группа Т51

Ключевые слова: функциональная безопасность; жизненный цикл систем; транспортные средства; электрические компоненты; электронные компоненты; вспомогательные процессы; стадии жизненного цикла системы безопасности

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

Усл. печ. л. 6,05. Тираж 31 экз. Зак. 80

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