ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-4— 2014

ДОРОЖНЫЕ 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 (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. № 523-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-4:2011 «Дорожные 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»)

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

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.

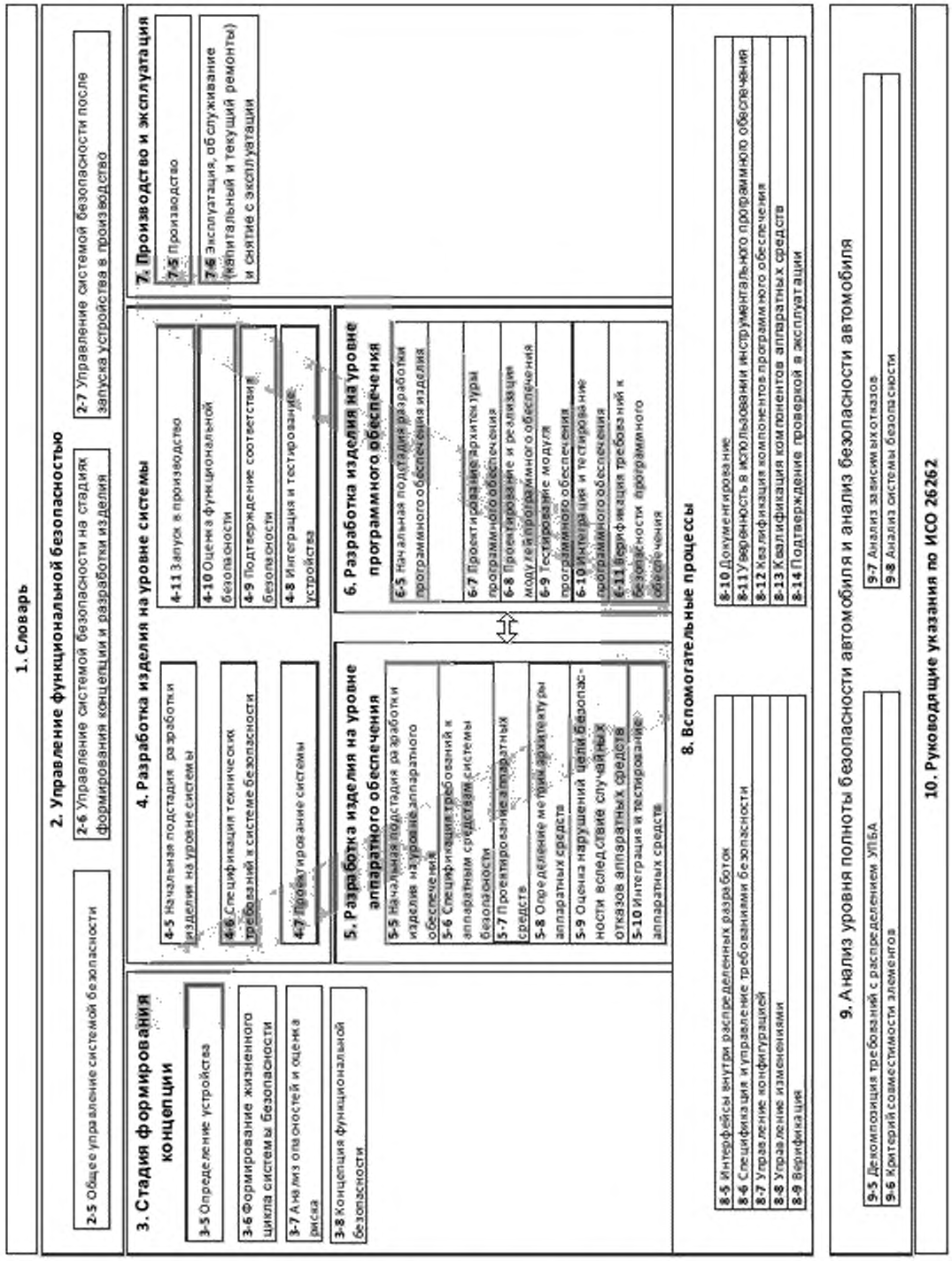


Рисунок 1 – Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 4

Разработка изделия на уровне системы

Road vehicles – Functional safety – Part 4: Product development at the system level

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 область его применения. Если разрабатываемые автомобили или их модификации используют системы и их компоненты, выпущенные до публикации настоящего стандарта, то только модификации этих систем должны быть разработаны в соответствии с настоящим стандартом.

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

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

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

- требования для запуска разработки изделия на уровне системы;
- спецификацию технических требований к системе безопасности;
- техническую концепцию системы безопасности;
- требования к проектированию системы;
- требования к интеграции и тестированию устройства;
- требования к подтверждению соответствия системы безопасности;
- требования к оценке функциональной безопасности;
- требования к запуску изделия в производство.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

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

ИСО 26262-5:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 5.

Издание официальное

Разработка технических средств изделия (ISO 26262-5:2011, Road vehicles – Functional safety – Part 5: Product development at the hardware level)

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

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

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

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

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 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 функциональной безопасности.

4.2 Интерпретация таблиц

В настоящем стандарте используются нормативные или справочные таблицы в зависимости от

их контекста. Перечисленные в таблице различные методы вносят вклад в уровень уверенности в достижении соответствия с рассматриваемым требованием. Каждый метод в таблице включен либо в

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 Начальная подстадия разработки изделия на уровне системы

5.1 Цель

Цель начальной подстадии разработки изделия на уровне системы заключается в определении и планировании действий по обеспечению функциональной безопасности для отдельных подстадий разработки системы. Кроме того, необходимо включить вспомогательные процессы, описанные в ИСО 26262-8.

Эти спланированные действия по обеспечению безопасности на уровне системы будут включены в план по обеспечению безопасности.

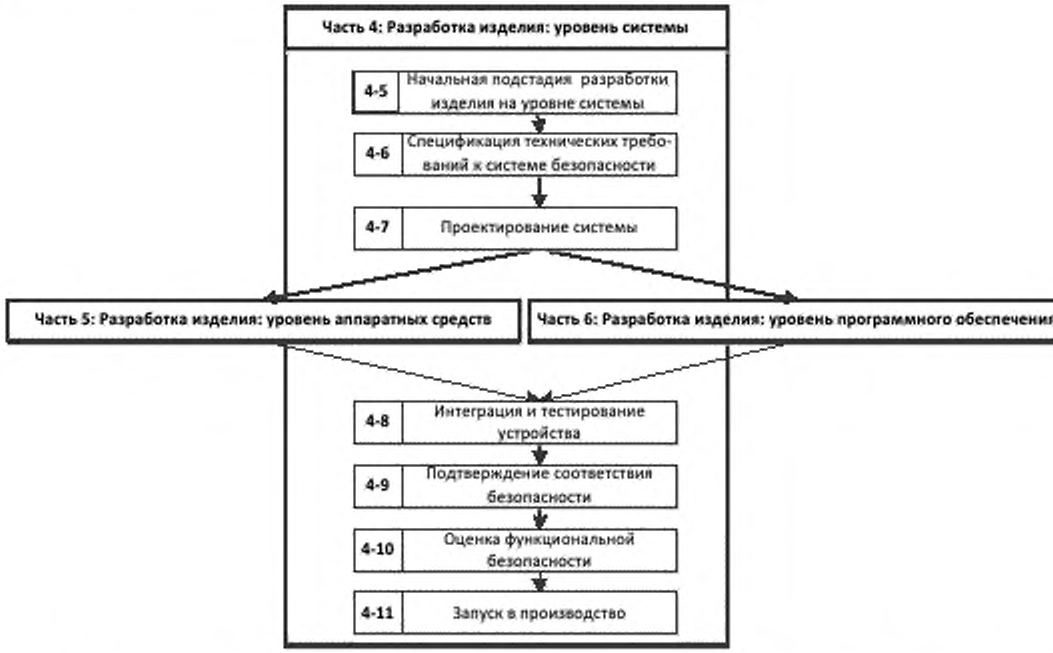
5.2 Общие положения

Необходимые действия при разработке системы приведены на рисунке 2. После начальной подстадии разработки изделия и спецификации технических требований к системе безопасности выполняется проектирование системы. Во время проектирования системы определяется архитектура системы, распределяются технические требования к системе безопасности между аппаратными средствами и программным обеспечением, а также между системами, основанными на других технологиях, если они применяются, Кроме того, технические требования к системе безопасности уточняются и добавляются требования, вытекающие из архитектуры системы, в том числе требования к программно-аппаратному интерфейсу (ПАИ). В зависимости от сложности архитектуры, требования к подсистемам могут быть получены итеративно. После разработки элементов аппаратных средств и программного обеспечения они интегрируются и тестируются, чтобы

сформировать устройство, которое затем устанавливается в транспортное средство. После интеграции устройства на уровне транспортного средства для него выполняется подтверждение соответствия безопасности, чтобы представить доказательства, что все требования функциональной безопасности устройства выполнены и оно соответствует целям безопасности.

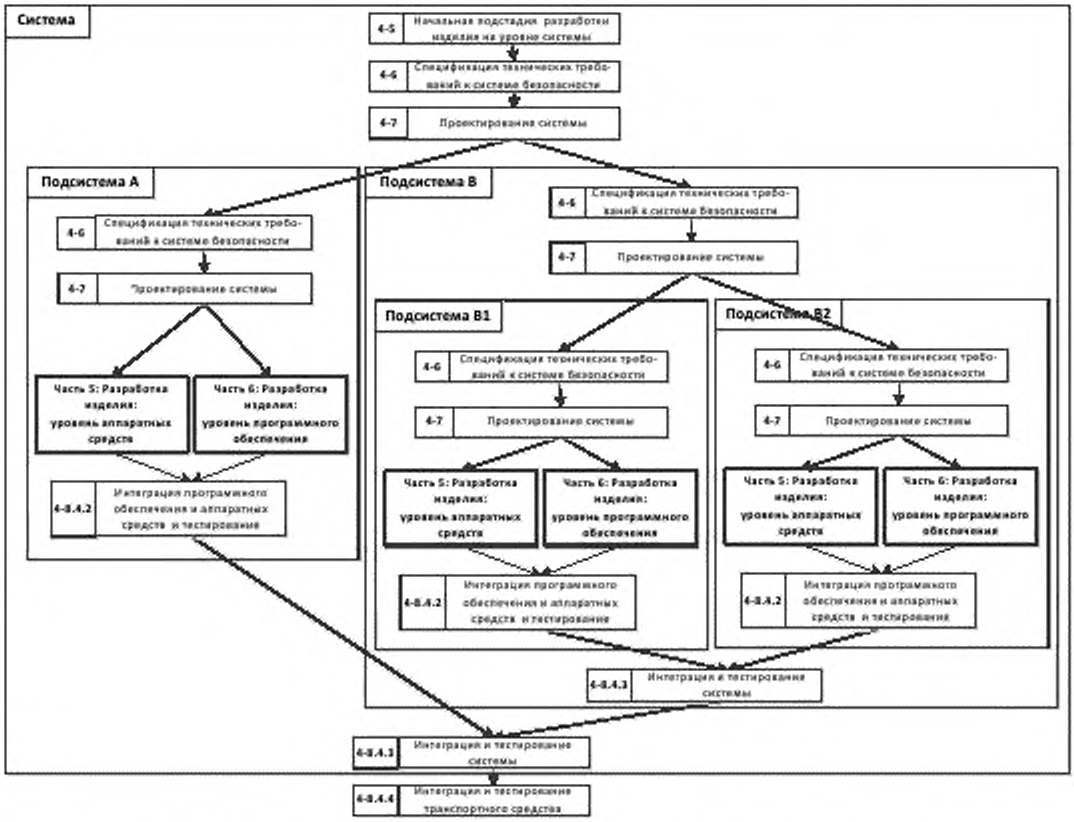
В ИСО 26262-5 и ИСО 26262-6 представлены требования к разработке аппаратных средств и программного обеспечения, соответственно. Настоящий стандарт относится как к разработке систем, так и подсистем. На рисунке 3 представлен пример системы с несколькими уровнями интеграции, иллюстрирующий применение настоящего стандарта, ИСО 26262-5 и ИСО 26262-6.

Примечание – Таблица А.1 содержит обзор целей, предварительных требований и результатов работы рассматриваемых подстадий разработки изделия на уровне системы.



Примечание – На рисунке конкретные разделы каждой части настоящего стандарта указаны следующим образом: «m-n», где «m» представляет собой номер части настоящего стандарта, а «n» указывает на номер ее раздела, например, 4-5 представляет раздел 5 ИСО 26262-4.

Рисунок 2 – Базовая модель стадии разработки устройства, связанного с безопасностью



Примечание – На рисунке конкретные разделы каждой части настоящего стандарта указаны следующим образом: «m-n», где «m» представляет собой номер части настоящего стандарта, а «n» указывает на номер ее раздела, например, 4-5 представляет раздел 5 ИСО 26262-4.

Рисунок 3 – Пример разработки изделия на уровне системы

5.3 Входная информация

5.3.1 Предварительные требования

Необходима следующая информация:

- план проектирования (уточненный) в соответствии с требованиями 6.5.2 ИСО 26262-2;
- план по обеспечению безопасности в соответствии с требованиями 6.5.1 ИСО 26262-3;
- план оценки функциональной безопасности в соответствии с требованиями 6.5.4 ИСО 26262-2;
- концепция функциональной безопасности в соответствии с требованиями 8.5.1 ИСО 26262-3.

5.3.2 Дополнительная информация

Следующая информация может быть учтена:

- предположения о предварительной архитектуре (от внешнего источника);
- определение устройства (см. 5.5 ИСО 26262-3).

5.4 Требования и рекомендации

5.4.1 Для разработки изделия на уровне системы должны быть запланированы действия по обеспечению безопасности, в том числе определение соответствующих методов и мер при проектировании и интеграции.

Примечание – Результаты планирования действий по верификации в процессе проектирования в соответствии с требованиями 6.4.6 (верификация и подтверждение соответствия) и требованиями 7.4.8 (верификация проекта системы) являются частью данного плана по обеспечению безопасности, в то время как планирование интеграции и тестирования устройства, выполняемые в соответствии с требованиями 8.4.2 (аппаратные средства / программное обеспечение), требованиями 8.4.3 (интеграция элементов) и требованиями 8.4.4 (интеграция устройства), представлены в отдельном плане интеграции и тестирования устройства в соответствии с требованиями 8.4.1.3.

5.4.2 Должны быть запланированы действия по выполнению подтверждения соответствия.

5.4.3 Должны быть запланированы действия по выполнению оценки функциональной безопасности при разработке изделия на системном уровне (см. также ИСО 26262-2).

Примечание – Пример программы оценки функциональной безопасности приведен в приложении Е ИСО 26262-2.

5.4.4 Настройка жизненного цикла разработки изделия на уровне системы должна быть выполнена в соответствии с требованиями ИСО 26262-2 на основе базовой модели стадии разработки устройства, приведенной на рисунке 2.

Примечание – План проекта может быть использован для обеспечения связи между отдельными подстадиями разработки изделия на уровне системы и стадиями разработки аппаратных средств и программного обеспечения. Он может включать шаги по интеграции на каждом уровне.

5.5 Результаты работы

5.5.1 План проекта (уточненный)
В результате выполнения требований 5.4.4.
5.5.2 План по обеспечению безопасности (уточненный)
В результате выполнения требований 5.4.1 - 5.4.4.
5.5.3 План интеграции и тестирования устройства
В результате выполнения требований 5.4.1.
5.5.4 План подтверждения соответствия
В результате выполнения требований 5.4.2.
5.5.5 План оценки функциональной безопасности (уточненный)
В результате выполнения требований 5.4.3.

6 Спецификация технических требований к системе безопасности

6.1 Цели

Первой целью данной подстадии является определение технических требований к системе безопасности. Спецификация технических требований к системе безопасности уточняет концепцию функциональной безопасности с учетом как функциональной концепции, так и предположений предварительной архитектуры (см. ИСО 26262-3).

Вторая цель заключается в проверке путем анализа, что технические требования к системе безопасности соответствуют требованиям функциональной безопасности.

6.2 Общие положения

В рамках всего жизненного цикла разработки технические требования к системе безопасности являются техническими требованиями, необходимыми для реализации концепции функциональной безопасности, при этом требования функциональной безопасности на уровне устройства детализируются в технические требования к безопасности на уровне системы (то есть в технические требования к системе безопасности).

Примечание – Что касается предотвращения скрытых сбоев, то выявление требований может быть выполнено после первой итерации подстадии проектирования системы.

6.3 Входная информация

6.3.1 Предварительные требования
Необходима следующая информация:

– концепция функциональной безопасности в соответствии с требованиями 8.5.1 ИСО 26262-3;
– план подтверждения соответствия согласно 5.5.4.

6.3.2 Дополнительная информация

Следующая информация может быть учтена:
– цели безопасности (см. 7.5.2 ИСО 26262-3);
– функциональная концепция (из внешнего источника, см. 5.4.1 ИСО 26262-3);
– предположения предварительной архитектуры (из внешнего источника, см. 8.3.2 ИСО 26262-3).

6.4 Требования и рекомендации

6.4.1 Спецификация технических требований к системе безопасности

6.4.1.1 Технические требования к системе безопасности должны быть специфицированы в соответствии с концепцией функциональной безопасности, предположениями предварительной архитектурны устройства и следующими свойствами системы:

a) внешними интерфейсами, такими как коммуникационные и пользовательские интерфейсы, если применяются;

b) ограничениями, например, условиями внешней среды или функциональными ограничениями;

c) требованиями конфигурации системы.

Примечание – Способность изменить конфигурацию системы для альтернативных применений является стратегией при повторном использовании существующих систем.

Пример – При настройке электронного блока управления двигателем для альтернативных транспортных средств часто используются калибровочные данные (см. приложение С ИСО 26262-6).

6.4.1.2 Должна быть обеспечена согласованность предположений о предварительной архитектуре из 8.3.2 ИСО 26262-3 и предположений о предварительной архитектуре в настоящей подстадии.

6.4.1.3 Если системой или ее элементами реализуются другие функции или требования помимо тех функций, для которых специфицированы технические требования к системе безопасности в соответствии с 6.4.1, то эти функции или требования должны быть специфицированы или должны быть ссылки на их спецификацию.

Пример – Источниками других требований являются правила Европейской Экономической Комиссии (ЕЭК), Федеральный стандарт безопасности автомобилей (FMVSS) или стратегическая платформа компании.

6.4.1.4 Технические требования к системе безопасности должны специфицировать связанные с безопасностью зависимости между системами или элементами устройства и между устройством и другими системами.

6.4.2 Механизмы безопасности

6.4.2.1 Технические требования к системе безопасности должны специфицировать реакцию системы или элементов на входные воздействия, влияющие на достижение целей безопасности и включающие в себя отказы и соответствующие комбинации входных воздействий в сочетании с соответствующим режимом работы и определенным состоянием системы.

Пример – Электронный блок управления адаптивным круиз-контролем (ACC) блокирует функционирование ACC, если из электронного блока управления тормозной системой получена информация о том, что система курсовой устойчивости не функционирует.

6.4.2.2 Технические требования к системе безопасности должны специфицировать необходимые механизмы безопасности (см. раздел 6 ИСО 26262-8), в том числе:

a) меры обнаружения, управления и индикации неисправности в самой системе.

Примечания

1 Они включают в себя самоконтроль системы или элементов для обнаружения случайных сбоев технических средств и, при необходимости, для выявления систематических отказов.

2 Они включают в себя меры по выявлению и управлению режимами отказов каналов связи (например, интерфейсы данных, коммуникационные шины, беспроводная радиосвязь);

b) меры обнаружения, управления и индикации сбоев во внешних устройствах, которые взаимодействуют с системой.

Пример – Внешние устройства включают в себя другие электронные блоки управления, блок питания или средства связи;

c) меры, обеспечивающие достижение или поддержание безопасного состояния системы.

Примечание – Они включают в себя логику установления приоритетов и логику разрешения конфликтов в случае конфликта между механизмами безопасности.

d) меры по детализации и осуществлению концепции предупреждения и постепенного снижения эффективности;

e) меры, предотвращающие скрытые неисправности [см. 6.4.4 (Предотвращение скрытых сбоев)].

Примечание – Данные меры, как правило, связаны с тестами, которые выполняются при включении питания (предварительные проверки автомобиля), как и в случае мер a) - d), в процессе эксплуатации, во время отключения питания (пост-проверки автомобиля), а также при техническом обслуживании.

6.4.2.3 Для каждого механизма безопасности, который позволяет устройству достигнуть или поддерживать безопасное состояние, должны быть специфицированы:

a) переход в безопасное состояние.

Примечание – Такая спецификация включает в себя требования по управлению исполнительными устройствами;

b) интервал сбоеустойчивости.

Примечание – Для определения интервала сбоеустойчивости могут быть использованы испытания и эксперименты, выполненные на автомобиле;

c) интервал аварийного режима, если безопасное состояние не может быть достигнуто сразу.

Примечание – Для определения интервала аварийного режима могут быть использованы испытания и эксперименты, выполненные на автомобиле;

Пример – Отключение может быть действием в аварийном режиме.

d) меры, поддерживающие безопасное состояние.

Пример – Спецификация механизма безопасности для электрической системы управления тормозной системой, который зависит от питания, может включать второй источник питания или устройство хранения данных (емкость, время запуска и работы, и т.д.).

6.4.3 Декомпозиция УПБА

6.4.3.1 Если при спецификации технических требований к системе безопасности применяется декомпозиция УПБА, то она должна применяться в соответствии с требованиями раздела 5 ИСО 26262-9 (Декомпозиция требований с распределением УПБА).

6.4.4 Предотвращение скрытых сбоев

6.4.4.1 Должны быть специфицированы механизмы безопасности по предотвращению скрытых сбоев, если они применимы. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Примечания

1 При случайных сбоях только множественные сбои могут включать скрытые сбои.

Пример – Бортовые тесты являются механизмами безопасности, которые проверяют состояние компонентов при различных режимах работы, таких как включение, выключение, режим эксплуатации или режим дополнительного тестирования для выявления скрытых сбоев. Тесты клапанов, реле или функционирования ламп, которые выполняются стандартной программой при запуске двигателя, являются примерами таких бортовых тестов.

2 Критерии оценки, которые определяют необходимость меры безопасности по предотвращению скрытых сбоев, получают в соответствии с успешной инженерно-технической практикой. Критерии оценки обеспечивает метрика скрытых сбоев, приведенная в раздел 8 ИСО 26262-5.

6.4.4.2 Чтобы предотвратить множественные отказы для каждого механизма безопасности, реализованного в соответствии с 6.4.4 (Предотвращение скрытых сбоев), должен быть определен интервал обнаружения множественного сбоя. Данное требование распространяется на значения

УПБА (A), (B), C и D в соответствии с 4.3.

6.4.4.3 Представленное ниже требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3. Чтобы определить интервал обнаружения множественного сбоя, должны быть рассмотрены следующие параметры:

a) надежность компонента аппаратных средств с учетом его роли в архитектуре;

b) вероятность воздействия соответствующего опасного события(й);

c) заданные количественные целевые значения для максимальной вероятности нарушения каждой цели безопасности из-за случайных отказов аппаратных средств (см. требование 7.4.4.3);

d) назначенное значение УПБА соответствующей цели безопасности.

Примечание – Применение следующих мер зависит от временных ограничений:
- периодическое тестирование системы или элементов в процессе эксплуатации;
- бортовые тесты элементов при включении или выключении двигателя, а также
- тестирование системы или элементов во время технического обслуживания.

6.4.4.4 Представленное ниже требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3. Разработка механизмов безопасности, которые предотвращают двойные скрытые сбои, должна выполняться:

a) со значением УПБА, равным B, если в технических требованиях к системе безопасности назначено значение УПБА, равное D;

b) со значением УПБА, равным A, если в технических требованиях к системе безопасности назначены значения УПБА, равные B и C;

c) с техническим обоснованием, если в технических требованиях к системе безопасности назначено значение УПБА, равное A.

6.4.5 Производство, эксплуатация, техническое обслуживание и вывод из эксплуатации

6.4.5.1 Должны быть специфицированы технические требования к системе безопасности, касающиеся функциональной безопасности устройства или его элементов в процессе производства, эксплуатации, технического обслуживания, ремонта и вывода из эксплуатации, рассматриваемые в ИСО 26262-7.

Примечание – Существует два аспекта, которые обеспечивают безопасность при производстве, эксплуатации, техническом обслуживании, ремонте и выводе из эксплуатации. Первый аспект связан с действиями, выполняемыми на стадии разработки, которые определены в требованиях 6.4.5.1 и 7.4.7 (Требования к производству, эксплуатации, обслуживанию и выводу из эксплуатации), а второй аспект связан с действиями, выполняемыми на стадии производства и эксплуатации, которые рассматриваются в ИСО 26262-7.

6.4.6 Верификация и подтверждение соответствия

6.4.6.1 Технические требования к системе безопасности должны быть верифицированы в соответствии с требованиями раздела 9 ИСО 26262-8, чтобы предоставить доказательства их:

a) соответствия и согласованности с концепцией функциональной безопасности; и

b) соответствия с предварительными предположениями архитектуры проекта.

6.4.6.2 Критерии подтверждения соответствия безопасности для устройства должны быть уточнены на основе технических требований к системе безопасности.

Примечание – Планирование подтверждения соответствия системы и спецификации подтверждения соответствия системы разрабатываются параллельно с техническими требованиями к системе безопасности (см. раздел 9).

6.5 Результаты работы

6.5.1 Спецификация технических требований к системе безопасности

В результате выполнения требований 6.4.1 – 6.4.5.

6.5.2 Отчет о верификации системы

В результате выполнения требований 6.4.6.

6.5.3 План подтверждения соответствия (уточненный)

В результате выполнения требований 6.4.6.2.

7 Проектирование системы

7.1 Цели

Первая цель рассматриваемой подстадии заключается в разработке проекта системы и технической концепции системы безопасности, которые удовлетворяют функциональным требованиям и спецификации технических требований к системе безопасности устройства.

Вторая цель рассматриваемой подстадии заключается в верификации того, что проект системы и техническая концепция системы безопасности соответствуют спецификации технических требований к системе безопасности.

7.2 Общие положения

Разработка проекта системы и технической концепции системы безопасности основана на спецификации технических требований к системе безопасности, полученной из концепции функциональной безопасности. Данная подстадия может выполняться итеративно, если система состоит из подсистем.

Для разработки проекта архитектуры системы необходимы требования функциональной безопасности, технические требования к системе, связанные и не связанные с безопасностью. Следовательно, на данной подстадии связанные и не связанные с безопасностью требования реализуются в рамках одного процесса разработки.

7.3 Входная информация

7.3.1 Предварительные требования

Необходима следующая информация:

- план интеграции и тестирования устройства в соответствии с требованиями 5.5.3;
- спецификации технических требований к системе безопасности в соответствии с требованиями 6.5.1.

7.3.2 Дополнительная информация

Следующая информация может быть учтена:

- предположения предварительной архитектурны (из внешнего источника см. 8.3.2 ИСО 26262-3);
- функциональная концепция (из внешнего источника);
- концепция функциональной безопасности (см. 8.5.1 ИСО 26262-3).

7.4 Требования и рекомендации

7.4.1 Спецификация проекта системы и технической концепции системы безопасности

7.4.1.1 Проект системы должен быть основан на функциональной концепции, предположениях предварительной архитектуры и технических требованиях к системе безопасности. Должна быть обеспечена согласованность предположений о предварительной архитектуре из 8.3.2 ИСО 26262-3 и предположений о предварительной архитектуре в настоящей подстадии.

7.4.1.2 Технические требования к системе безопасности должны быть определены для элементов проекта системы.

7.4.1.3 Проект системы должен реализовать технические требования к системе безопасности.

7.4.1.4 При реализации технических требований к системе безопасности в проекте системы необходимо рассмотреть следующее:

a) возможность проверки проекта системы;

b) технические возможности достижения функциональной безопасности предполагаемым проектом аппаратных средств и программного обеспечения и

c) возможность выполнения тестов во время интеграции системы.

7.4.2 Ограничения проекта архитектуры системы

7.4.2.1 Архитектура системы и подсистемы должна соответствовать техническим требованиям к системе безопасности с соответствующими для них значениями УПБА.

7.4.2.2 Каждый элемент наследуют наивысшее значение УПБА среди технических требований к системе безопасности, которые он реализует.

7.4.2.3 Если элемент включает подэлементы с различными назначенными для них значениями УПБА или связанные и не связанные с безопасностью подэлементы, то каждый из них рассматривается в соответствии с самым высоким значением УПБА, если не выполнены критерии

совместимости в соответствии с требованиями раздела 6 ИСО 26262-9.

7.4.2.4 Чтобы избежать связанные с безопасностью неблагоприятные воздействия других элементов на связанные с безопасностью элементы, должны быть определены внутренние и внешние интерфейсы связанных с безопасностью элементов.

7.4.2.5 Декомпозиция УПБА, выполняемая при проектировании системы в соответствии с требованиями к системе безопасности, должна выполняться в соответствии с требованиями раздела 5 ИСО 26262-9.

7.4.3 Меры предотвращения систематических отказов

7.4.3.1 Для выявления причин систематических отказов и последствий систематических сбоев должен применяться анализ безопасности проекта системы в соответствии с таблицей 1 и требованиями раздела 8 ИСО 26262-9.

Таблица 1 – Анализ проекта системы

Методы		УПБА			
		A	B	C	D
1	Дедуктивный анализ[a)]	o	+	++	++
2	Индуктивный анализ[b)]	++	++	++	++
[a)] Методы дедуктивного анализа включают FTA, блок-диаграммы надежности, диаграмму Ишикава. [b)] Методы индуктивного анализа включают FMEA, ETA, модели Маркова.					

Примечания

1 Цель этого анализа состоит в оказании помощи проектированию. Поэтому на данной стадии, вероятно, можно ограничиться качественным анализом. Количественный анализ можно провести в случае необходимости.

2 Для выявления или исключения причин и последствий систематических отказов необходим более детальный анализ.

7.4.3.2 Выявленные внутренние причины систематических отказов должны быть устранены или их воздействия смягчены.

7.4.3.3 Выявленные внешние причины систематических отказов должны быть устранены или их воздействия смягчены.

7.4.3.4 Для уменьшения систематических отказов должны применяться принципы проектирования автомобильных систем, обладающие высоким доверием. Они могут включать:

a) повторное использование технических концепций систем безопасности, обладающих высоким доверием;

b) повторное использование обладающих высоким доверием проектов для элементов, в том числе компонентов аппаратных средств и программного обеспечения;

c) повторное использование обладающих высоким доверием механизмов для выявления и управления отказами, а также

d) повторное использование обладающих высоким доверием или стандартных интерфейсов.

7.4.3.5 Для обеспечения пригодности обладающих высоким доверием принципов проектирования или элементов для нового устройства должны быть проанализированы результаты их применения, а также проверены основные предположения перед их повторным использованием.

Примечание – Анализ влияния включает в себя определение возможности и целесообразности выполнения заданных диагностик, ограничений внешней среды, временных ограничений, совместимости заданных ресурсов и надежности проекта системы.

7.4.3.6 Данное требование распространяется на значение УПБА, равное D. Решение не использовать обладающие высоким доверием принципы проектирования повторно должно быть обосновано.

7.4.3.7 Представленное ниже требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3. Для предотвращения отказов из-за высокой сложности, проект архитектуры за счет применения принципов, представленных в таблице 2, должен обладать следующими свойствами:

a) модульностью;

b) адекватным уровнем детализации и

c) простотой.

Таблица 2 – Свойства модульного проектирования системы

	Свойства	УПБА			
		A	B	C	D
1	Иерархическое проектирование	+	+	++	++
2	Хорошо определенный интерфейс	+	+	+	+
3	Избегать ненужной сложности компонентов аппаратных средств и программного обеспечения	+	+	+	+
4	Избегать ненужной сложности интерфейсов	+	+	+	+
5	Ремонтопригодность во время сервисного обслуживания	+	+	+	+
6	Тестируемость в процессе разработки и эксплуатации	+	+	++	++

7.4.4 Меры по управлению случайными отказами аппаратных средств в процессе эксплуатации

7.4.4.1 Должны быть специфицированы меры по обнаружению и управлению или смягчению случайных отказов аппаратных средств в соответствии со спецификацией проекта системы, формируемой в соответствии с требованиями 7.4.1 (Спецификация проекта системы и технической концепции системы безопасности).

Примеры

1 Такими мерами могут быть диагностические функции аппаратных средств и их использование программным обеспечением для обнаружения случайных отказов аппаратных средств.

2 Аппаратные средства, которые непосредственно переходят в безопасное состояние при случайном отказе аппаратных средств, управляют отказом даже без выявления.

7.4.4.2 Для окончательной оценки на уровне устройства (см. требование 9.4.3.3) должны быть специфицированы целевые значения метрики одиночного сбоя и метрики скрытого сбоя (см. раздел 8 ИСО 26262-5). Данное требование распространяется на значения УПБА (B), C и D в соответствии с 4.3.

7.4.4.3 Для окончательной оценки на уровне устройства (см. требование 9.4.3.3) должна быть выбрана одна из альтернативных процедур оценки нарушения цели безопасности из-за случайных отказов аппаратных средств (см. раздел 9 ИСО 26262-5) и должны быть специфицированы целевые значения. Данное требование распространяется на значения УПБА (B), C и D в соответствии с 4.3.

7.4.4.4 Представленное ниже требование распространяется на значения УПБА (B), C и D в соответствии с 4.3. Соответствующие целевые значения для интенсивностей отказов и охвата диагностикой должны быть специфицированы на уровне элемента для того, чтобы выполнить:

a) целевые значения метрик в соответствии с требованиями раздела 8 ИСО 26262-5 и

b) процедуры в соответствии с требованиями раздела 9 ИСО 26262-5:2011.

7.4.4.5 При распределенной разработке (см. раздел 5 ИСО 26262-8) полученные целевые значения должны быть доведены до каждого соответствующего участника. Данное требование распространяется на значения УПБА (B), C и D в соответствии с 4.3.

Примечание – Ограничения архитектуры, описанные в разделах 8 и 9 ИСО 26262-5, непосредственно не применимы к коммерчески доступным компонентам и частям, так как поставщики обычно не могут предвидеть использование своей продукции в конечном устройстве и возможные последствия ее применения в системах безопасности. В таком случае основные данные, такие как частота отказов, виды отказов, распределение частоты отказов по видам отказов, встроенная диагностика и т.д. предоставляются поставщиком компоненты или части, чтобы позволить оценить ограничения архитектуры на уровне архитектуры аппаратных средств всей системы.

7.4.5 Распределение требований для аппаратных средств и программного обеспечения

7.4.5.1 Технические требования к системе безопасности должны быть распределены непосредственно или с учетом дальнейшего развития технических средств и (или) программного обеспечения.

7.4.5.2 Если технические требования к системе безопасности распределяются на заказные элементы технических средств, которые включают программируемые средства (например, ASIC, FPGA или другие виды цифрового оборудования), то должен быть определен и реализован подходящий процесс разработки, соответствующий сочетанию требований ИСО 26262-5 и ИСО 26262-6.

Примечание – Доказательство соответствия с распределенным требованием безопасности для некоторых из этих элементов аппаратных средств может быть предоставлено с помощью квалификационных

мер согласно требованиям раздела 13 ИСО 26262-8, если будут выполнены критерии для его применения.

7.4.5.3 Проект системы должен выполнять решения по распределению и разделению.

Примечание – Чтобы добиться независимости и предотвратить распространение отказов, при проектировании системы можно реализовать разделение функций и компонентов.

7.4.6 Спецификация программно-аппаратного интерфейса (ПАИ)

7.4.6.1 Спецификация ПАИ должна определить взаимодействие аппаратных средств и программного обеспечения и быть согласованной с технической концепцией системы безопасности. Спецификация ПАИ должна включать компоненты аппаратных средств устройств, которые находятся под управлением программного обеспечения и ресурсы аппаратных средств, которые поддерживают выполнение программ.

Пример – Аспекты и характеристики, подробно описанные в ПАИ, приводятся в приложении В.

7.4.6.2 Спецификация ПАИ должна включать в себя следующие характеристики:

a) соответствующие режимы работы аппаратных средств приборов и соответствующие параметры конфигурации.

Примеры

1 Режимы работы аппаратных средств приборов: по умолчанию, запуск, тестирование или новые режимы.

2 Параметры конфигурации: регулятор усиления, полоса пропускания частот или тактовый генератор предварительного делителя частоты;

b) функции аппаратных средств, обеспечивающие независимость между элементами и поддерживающие разделение программного обеспечения на части;

c) общее и исключительное использование ресурсов аппаратных средств.

Пример – Распределение памяти, распределение регистров, таймеры, прерывания, порты ввода / вывода;

d) механизм доступа к аппаратным средствам приборов.

Пример – Последовательный, параллельный, ведомый, ведущий - ведомый;

e) ограничения синхронизации, определенные для каждой службы, участвующей в реализации технической концепции системы безопасности.

7.4.6.3 В спецификации ПАИ должно быть указано о соответствующих диагностических возможностях аппаратных средств и об их реализации программным обеспечением:

a) должны быть определены диагностические функции аппаратных средств.

Пример – Обнаружение перегрузки по току, короткого замыкания или перегрева;

б) должны быть определены диагностические функции для аппаратного обеспечения, которые должны быть реализованы программным обеспечением.

7.4.6.4 ПАИ должен быть специфицирован во время проектирования системы и уточняться в ходе разработки аппаратных средств (см. раздел 7 ИСО 26262-5) и при разработке программного обеспечения (см. раздел 7 ИСО 26262-6).

7.4.7 Требования к производству, эксплуатации, обслуживанию и снятию с эксплуатации

7.4.7.1 Должны быть определены диагностические функции и обеспечены необходимыми данными, позволяющими выполнить контроль в процессе эксплуатации устройства или его элементов с учетом результатов анализа безопасности и реализованных механизмов безопасности.

7.4.7.2 Для поддержания функциональной безопасности должны быть определены диагностические функции, которые позволят сотрудникам цеха выявить сбои в процессе необходимого обслуживания.

7.4.7.3 Должны быть определены требования к производству, эксплуатации, обслуживанию и выводу из эксплуатации, выявленные в ходе проектирования системы (см. ИСО 26262-7). Они включают в себя:

a) требования инструкций по сборке;

b) специальные, связанные с безопасностью характеристики;

c) требования, предназначенные обеспечить надлежащую идентификацию систем или элементов;

Пример – Маркировка элементов.

d) методы и средства верификации в производстве;

e) требования к обслуживанию, включая диагностические данные и указания по обслуживанию;

f) требования к выводу из эксплуатации.

Пример – Инструкции по выводу из эксплуатации.

7.4.8 Верификация проекта системы

7.4.8.1 Проект системы должен быть проверен на соответствие и полноту технической концепции системы безопасности, используя методы верификации, перечисленные в таблице 3.

Таблица 3 – Верификация проекта системы

Методы		УПБА			
		A	B	C	D
1a	Осмотр (контроль) проекта системы [a]	+	++	++	++
1b	Сквозной контроль проекта системы [a]	++	+	o	o
2a	Моделирование [b]	+	+	++	++
2b	Системное прототипирование и тестирование автомобиля [b]	+	+	++	++
3	Анализ проекта системы [c]	См. таблицу 1			

[a] Методы 1a и 1b служат для проверка полноты и правильности выполнения технических требований системы безопасности.
[b] Методы 2a и 2b могут с успехом использоваться как метод тестирования с внесением неисправности.
[c] О выполнении анализа безопасности см. раздел 8 ИСО 26262-9.

Примечание – Об аномалиях и неполноте, выявленных при проектировании системы, относящихся к технической концепции системы безопасности, должно быть сообщено в соответствии с требованиями 5.4.2 ИСО 26262-2.

7.4.8.2 Вновь выявленные опасности в проекте системы, не рассмотренные в цели безопасности, должны быть учтены и оценены, применением анализа опасностей и оценки рисков в соответствии с требованиями ИСО 26262-3 и процессов управления изменениями в соответствии с требованиями раздела 8 ИСО 26262-8.

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

7.5 Результаты работы

7.5.1 Техническая концепция системы безопасности

В результате выполнения требований 7.4.1 и 7.4.5.

7.5.2 Спецификация проекта системы

В результате выполнения требований 7.4.1 – 7.4.5.

7.5.3 Спецификация программно-аппаратного интерфейса

В результате выполнения требований 7.4.6.

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

В результате выполнения требований 7.4.7.

7.5.5 Отчет о верификации системы (уточненный)

В результате выполнения требований 7.4.8.

7.5.6 Отчеты по результатам анализа системы безопасности

В результате выполнения требований 7.4.3.

8 Интеграция и тестирование устройства

8.1 Цели

Стадия интеграции и тестирования включает в себя три этапа, реализующие две основные цели. На первом этапе выполняется интеграция аппаратных средств и программного обеспечения каждого элемента устройства. Второй этап заключается в интеграции элементов устройства и создании всей системы. На третьем этапе выполняется интеграция устройства с другими системами в транспортном средстве и с самим транспортным средством.

Первая цель процесса интеграции заключается в проверке соответствия каждого требования безопасности его спецификации и заданному значению УПБА.

Вторая цель заключается в проверке того, что «Проект системы», удовлетворяющий

требованиям безопасности (см. раздел 7 «Проектирование системы»), правильно реализован полностью интегрированным устройством.

8.2 Общие положения

Интеграция элементов устройства осуществляется на систематической основе, начиная с программно-аппаратной интеграции, выполняется системная интеграция и затем интеграция на уровне транспортного средства. Для обеспечения доказательств того, что в результате интеграции элементы взаимодействуют правильно, на каждом этапе интеграции проводятся специфицированные тесты интеграции.

После обоснованного завершения разработки аппаратных средств и программного обеспечения в соответствии с требованиями ИСО 26262-5 и ИСО 26262-6, можно начинать системную интеграцию в соответствии с требованиями настоящего раздела.

8.3 Входная информация

8.3.1 Предварительные требования

Необходима следующая информация:

- цели безопасности в соответствии с 7.5.2.
- концепция функциональной безопасности в соответствии с 8.5.1 ИСО 26262-3;
- план интеграции и тестирования устройства в соответствии с 5.5.3;
- техническая концепция системы безопасности в соответствии с 7.5.1;
- спецификация проекта системы в соответствии с 7.5.2;
- спецификация программно-аппаратного интерфейса в соответствии с 7.5.3.

8.3.2 Дополнительная информация

Следующая информация может быть учтена:

- архитектура транспортного средства (из внешнего источника);
- техническая концепция системы безопасности других систем транспортного средства (из внешнего источника);
- отчет об анализе безопасности (см. 7.5.6).

8.4 Требования и рекомендации

8.4.1 Планирование и спецификация интеграции и тестирования

8.4.1.1 Чтобы продемонстрировать, что проект системы соответствует требованиям функциональной безопасности и техническим требованиям к системе безопасности, действия по тестированию интеграции должны проводиться в соответствии с требованиями раздела 9 ИСО 26262-8.

Примечание – Реализация перечисленных ниже целей тестирования рассматривается в таблицах 4–18:

a) корректная реализация функциональной безопасности и технических требований к системе безопасности;

b) корректное функционирование, точность и синхронизация механизмов безопасности;

c) согласованная и корректная реализация интерфейсов;

d) эффективность диагностики механизма безопасности или его охвата отказов;

e) уровень надежности.

8.4.1.2 Должна быть определена стратегия интеграции и тестирования, которая основана на спецификации проекта системы, концепции функциональной безопасности, технической концепции системы безопасности и плане интеграции и тестирования устройства, а также должны быть предоставлены доказательства, что цели тестирования охвачены полностью. Стратегия интеграции и тестирования должна охватывать как Э/Э элементы, а также элементы, основанные на других технологиях, рассматриваемых в концепциях построения системы безопасности.

Примечание – Обычно применяют следующие уровни интеграции: уровень технических средств / программного обеспечения, уровень системы и уровень автомобиля.

8.4.1.3 На подстадии интеграции системы:

а) должен быть уточнен план интеграции и тестирования для программно-аппаратных средств;

б) должен быть уточнен план интеграции и тестирования устройства включением спецификаций тестов интеграции на уровне системы и уровне автомобиля. Это должно гарантировать, что

рассматриваются нерешенные вопросы, связанные с верификацией программно-аппаратных средств;

c) в плане интеграции и тестирования устройства на уровнях системы и транспортного средства должны быть рассмотрены интерфейсы между подсистемами транспортного средства (внутренние и внешние к устройству) и окружающей средой.

Примечания

1 При планировании интеграции и тестирования на уровне транспортного средства может быть рассмотрено правильное поведение автомобиля при типичных и чрезвычайных ситуациях в транспортном средстве и окружающей среде, но с достаточным подмножеством методов (см. таблицу 4).

2 Планирование интеграции и тестирования, на основе которого выполняется интеграция устройства на программно-аппаратном уровне и уровне системы, рассматривает интерфейсы и взаимодействие между аппаратными средствами и программным обеспечением.

8.4.1.4 Если в системе используются данные о конфигурации или калибровочные данные, то верификация на уровне системы или транспортного средства должна предоставить доказательства соответствия требованиям к системе безопасности для каждой конфигурации на уровне реализации или для каждой конфигурации, предназначенной для серийного производства.

Примечание – Если полная верификация каждой конфигурации на уровне системы или транспортного средства не представляется возможной, то может быть выбрано разумное подмножество.

8.4.1.5 Испытательное оборудование должно быть под управлением системы контроля качества.

8.4.1.6 Каждое функциональное и техническое требование системы безопасности должно быть верифицировано (если это возможно тестированием), по крайней мере, один раз на подстадии интеграции.

Примечания

1 Обычная практика заключается в верификации требования безопасности на более высоком уровне интеграции, на котором оно было специфицировано.

2 Об аномалиях системы безопасности, выявленных в ходе тестирования интеграции, сообщается в соответствии с требованиями 5.4.2 ИСО 26262-2.

8.4.1.7 Чтобы сформировать соответствующую спецификацию тестовых примеров для интеграционных тестов, тестовые примеры должны быть получены на основе соответствующей комбинации методов, перечисленных в таблице 4, а также с учетом уровня интеграции.

Таблица 4 – Методы получения тестовых примеров для тестирования интеграции

Методы		УПБА			
		A	B	C	D
1a	Анализ требований	++	++	++	++
1b	Анализ внешних и внутренних интерфейсов	+	++	++	++
1c	Генерация и анализ классов эквивалентности интеграции аппаратных средств и программного обеспечения	+	+	++	++
1d	Анализ граничных значений	+	+	++	++
1e	Ошибки, предполагаемые на основе знаний и опыта	+	+	++	++
1f	Анализ функциональных зависимостей	+	+	++	++
1g	Анализ общих предельных условий, последователь-ностей и источников зависимых отказов	+	+	++	++
1h	Анализ состояния окружающей среды и прецедентов эксплуатации	+	++	++	++
1i	Анализ опыта эксплуатации	+	++	++	++

8.4.2 Интеграция и тестирование аппаратных средств и программного обеспечения

8.4.2.1 Интеграция аппаратных средств и программного обеспечения

8.4.2.1.1 При интеграции аппаратных средств, разработанных в соответствии с требованиями ИСО 26262-5, и программного обеспечения, разработанного в соответствии с требованиями ИСО 26262-6, должны использоваться методы тестирования интеграции, перечисленные в таблицах 4 – 8.

8.4.2.1.2 Требования программно-аппаратного интерфейса должны быть протестированы с соответствующим охватом с учетом значения УПБА или должно быть дано обоснование, что все вопросы, связанные с программно-аппаратным интерфейсом, решены. Данное требование распространяется на значения УПБА C и D в соответствии с 4.3.

Примечание – Использование предназначенных для применения в изделиях аппаратных средств и программного обеспечения является предпочтительным. В случае необходимости для конкретных методик тестирования могут быть использованы модифицированные аппаратные средства или программное обеспечение.

8.4.2.2 Цели и методы тестирования во время тестирования программно- аппаратных средств

8.4.2.2.1 Для выявления систематических ошибок, присутствующих в проекте системы, в процессе интеграции аппаратных средств и программного обеспечения, цели тестирования, вытекающие из требований 8.4.2.2.2 – 8.4.2.2.6, должны достигаться путем применения адекватных методов тестирования, как указано в соответствующих таблицах.

Примечание – В зависимости от реализованной функции, сложности или распределенного характера системы может быть разумно перенести методы тестирования на другие подстадии интеграции с адекватным обоснованием.

8.4.2.2.2 Корректное выполнение технических требований к системе безопасности на программно-аппаратном уровне должно быть продемонстрировано с помощью обоснованных методов тестирования, приведенных в таблице 5.

Таблица 5 – Корректное выполнение технических требований к системе безопасности на программно-аппаратном уровне

Методы		УПБА			
		A	B	C	D
1a	Тестирование на основе требований [a)]	++	++	++	++
1b	Тестирование с введением неисправности [b)]	+	++	++	++
1c	Тестирование с прямым сравнением [c)]	+	+	++	++

[a)] Тестирование на основе требований выполняет проверку требований на функциональность и нефункциональность.

[b)] Тестирование с введением неисправности использует специальные средства для внедрения неисправностей в тестируемое средство во время его работы. Для программного обеспечения это может быть выполнено через специальный тестовый интерфейс или специально подготовленные аппаратные средства. Этот метод часто используется, чтобы улучшить тестовый охват требований безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[c)] Тестирование с прямым сравнением сопоставляет ответы тестируемого средства с ответами имитационной модели с теми же входными воздействиями для выявления различий между поведением модели и ее реализации.

Примечание – Различие трудоемкости метода 1b из таблицы 5 и таблицы 10 объясняется количеством усилий для выполнения тестирования с введением неисправности на уровне системы.

8.4.2.2.3 Корректное функционирование, точность и синхронизация механизмов безопасности на программно-аппаратном уровне должно быть продемонстрировано с помощью обоснованных методов тестирования, приведенных в таблице 6. Данное требование распространяется на значения УПБА (A), B, C и D в соответствии с 4.3.

Таблица 6 – Корректное функционирование, точность и синхронизация механизмов безопасности на программно-аппаратном уровне

Методы		УПБА			
		A	B	C	D
1a	Тестирование с прямым сравнением [a)]	+	+	++	++
1b	Промышленные испытания [b)]	+	++	++	++

[a)] Тестирование с прямым сравнением сопоставляет ответы тестируемого средства с ответами имитационной модели с теми же входными воздействиями для выявления различий между поведением модели и ее реализации.

[b)] Промышленные испытания могут проверить рабочие характеристики (например, планирование задачи, синхронизацию, выходную мощность) для всего объекта испытаний, а также возможности выполнения целевого управляющего программного обеспечения на аппаратных средствах

8.4.2.2.4 Согласованная и корректная реализация внешних и внутренних интерфейсов на программно-аппаратном уровне должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 7. Данное требование распространяется на значения УПБА (A), B, C и D в соответствии с 4.3.

Таблица 7 – Согласованная и корректная реализация внешних и внутренних интерфейсов на программно-аппаратном уровне

Методы		УПБА			
		A	B	C	D
1a	Тестирование внешних интерфейсов [a]	+	+	++	++
1b	Тестирование внутренних интерфейсов [a]	+	++	++	++
1c	Проверка согласованности интерфейсов [a]	+	++	++	++

[a] Тесты интерфейса проверяемого объекта включают в себя тесты для аналоговых и цифровых входов и выходов, тестирование граничных значений и тестирование на основе классов эквивалентности, чтобы полностью проверить специфицированный интерфейс, совместимость, синхронизацию и другие заданные значения характеристик проверяемого объекта. Внутренние интерфейсы электронного блока управления могут быть проверены с помощью статических испытаний совместимости программного обеспечения и аппаратных средств, а также с помощью динамических испытаний коммуникации последовательных синхронных периферийных интерфейсов или коммуникации между интегральными схемами или любые другие интерфейсы между элементами электронного блока управления.

8.4.2.2.5 Эффективность обнаружения сбоя в аппаратных средствах механизмами охвата диагностикой на программно-аппаратном уровне, по отношению к моделям сбоев, должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 8. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Примечание – О моделях сбоев см. приложение D ИСО 26262-5.

Таблица 8 – Эффективность охвата диагностикой механизма безопасности на программно-аппаратном уровне

Методы		УПБА			
		A	B	C	D
1a	Тестирование с введением неисправности [a]	+	+	++	++
1b	Тестирование предполагаемых ошибок [b]	+	+	++	++

[a] Тестирование с введением неисправности использует специальные средства для внедрения неисправностей в тестируемое средство во время его работы. Для программного обеспечения это может быть выполнено через специальный тестовый интерфейс или специально подготовленные аппаратные средства. Этот метод часто используется, чтобы улучшить тестовый охват требований к безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[b] Тестирование предполагаемых ошибок основано на использовании экспертных знаний и данных, собранных в результате полученного из опыта умения предвидеть ошибки в тестируемом объекте. Затем для проверки этих ошибок проектируется набор тестов наряду с надлежащими средствами тестирования. Предположение ошибок является эффективным методом испытателя, который имеет опыт работы с подобными тестируемыми объектами.

8.4.2.2.6 Уровень надежности элементов на программно-аппаратном уровне должен быть продемонстрирован с помощью обоснованных методов тестирования, приведенных в таблице 9. Данное требование распространяется на значения УПБА (A), (B), (C) и D в соответствии с 4.3.

Таблица 9 – Уровень надежности на программно-аппаратном уровне

Методы		УПБА			
		A	B	C	D
1a	Тестирование используемых ресурсов [a]	+	+	++	++
1b	Стресс-тест [b]	+	+	++	++

[a] Тестирование используемых ресурсов может быть выполнено статически (например, с помощью проверки размеров кода или анализа кода по использованию прерываний, для того, чтобы убедиться, что наихудший сценарий не приведет к использованию всех ресурсов) или динамически во время выполнения мониторинга.

[b] Стресс-тест верифицирует исправность работы тестируемого объекта в условиях высоких эксплуатационных нагрузок или повышенных требований со стороны внешней среды. Таким образом, возможны тесты при высоких нагрузках на тестируемый объект, или с исключительными нагрузками на интерфейс или значениями величин (загрузки шины, поражения электрическим током и т.д.), а также тесты с экстремальными значениями температур, влажности и механических воздействий.

8.4.3 Интеграция и тестирование системы

8.4.3.1 Интеграция системы

8.4.3.1.1 Отдельные элементы, включаемые в систему, должны быть интегрированы в соответствии с проектом системы, испытаны в соответствии с тестами интеграции системы и испытаны в соответствии со специфицированными тестами интеграции системы, указанными в ИСО

26262-5 и ИСО 26262-6.

Примечание – Тесты предназначены для предоставления доказательств того, что каждый элемент системы взаимодействует правильно, соответствует требованиям функциональной безопасности и техническим требованиям к системе безопасности и обеспечивает достаточный уровень уверенности, что отсутствует непреднамеренное поведение, которое может привести к нарушению цели безопасности.

8.4.3.2 Цели тестирования и методы испытаний при тестировании системы

8.4.3.2.1 Для выявления систематических ошибок при интеграции системы цели тестирования, полученные из требований 8.4.3.2.2 – 8.4.3.2.6, должны достигаться применением адекватных методов тестирования, как указано в соответствующих таблицах.

Примечание – В зависимости от реализованной функции, сложности или распределенного характера системы может быть разумно с адекватным обоснованием перенести методы тестирования на другие подстадии интеграции.

8.4.3.2.2 Корректное выполнение требований функциональной безопасности и технических требований к системе безопасности на уровне системы должно быть продемонстрировано с помощью обоснованных методов тестирования, приведенных в таблице 10.

Таблица 10 – Корректное выполнение требований функциональной безопасности и технических требований к системе безопасности на уровне системы

Методы		УПБА			
		A	B	C	D
1a	Тестирование на основе требований [a)]	++	++	++	++
1b	Тестирование с введением неисправности [b)]	+	+	++	++
1c	Тестирование с прямым сравнением [c)]	o	+	+	++

[a)] Тестирование на основе требований выполняет проверку требований на функциональность и нефункциональность.

[b)] Тестирование с введением неисправности использует специальные средства для внедрения неисправностей в тестируемое средство во время его работы. Для программного обеспечения это может быть выполнено через специальный тестовый интерфейс или специально подготовленные аппаратные средства. Этот метод часто используется, чтобы улучшить тестовый охват требований к безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[c)] Тестирование с прямым сравнением сопоставляет ответы тестируемого средства с ответами имитационной модели с теми же входными воздействиями для выявления различий между поведением модели и ее реализации.

8.4.3.2.3 Корректное функционирование, точность и синхронизация механизмов безопасности на уровне системы должны быть продемонстрированы с помощью обоснованных методов тестирования, приведенных в таблице 11. Данное требование распространяется на значения УПБА (A), (B), (C) и D в соответствии с 4.3.

Таблица 11 – Корректное функционирование, точность и синхронизация механизмов безопасности на уровне системы

Методы		УПБА			
		A	B	C	D
1a	Тестирование с прямым сравнением [a)]	o	+	+	++
1b	Промышленные испытания [b)]	o	+	+	++

[a)] Тестирование с прямым сравнением сопоставляет ответы тестируемого средства с ответами имитационной модели с теми же входными воздействиями для выявления различий между поведением модели и ее реализации.

[b)] Промышленные испытания могут проверить рабочие характеристики (например, скорость или прочность привода, полное время реакции системы) механизмов безопасности на уровне системы.

8.4.3.2.4 Согласованная и корректная реализация внешних и внутренних интерфейсов на уровне системы должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 12.

Таблица 12 – Согласованная и корректная реализация внешних и внутренних интерфейсов на уровне системы

Методы		УПБА			
		A	B	C	D
1a	Тестирование внешних интерфейсов [a]	+	++	++	++
1b	Тестирование внутренних интерфейсов [a]	+	++	++	++
1c	Проверка согласованности интерфейсов [a]	o	+	++	++
1d	Проверка взаимодействия / коммуникации [b]	++	++	++	++

[a] Тесты интерфейса проверяемого объекта включают в себя тесты аналоговых и цифровых входов и выходов, тестирование граничных значений и тестирование на основе классов эквивалентности, чтобы полностью проверить специфицированный интерфейс, совместимость, синхронизацию и другие заданные значения характеристик проверяемого объекта. Внутренние интерфейсы системы могут быть проверены с помощью статических испытаний (например на соответствие штепсельных разъемов), а также с помощью динамических испытаний коммуникационных шин или любых других интерфейсов между элементами системы.

[b] Тестирование коммуникации и взаимодействия включает в себя тестирование связей между элементами системы, а также между тестируемой системой и другими системами автомобиля во время его работы, чтобы обеспечить выполнение функциональных и нефункциональных требований.

8.4.3.2.5 Эффективность охвата диагностикой механизмов безопасности на уровне системы должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 13. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Таблица 13 – Эффективность охвата диагностикой механизмов безопасности на уровне системы

Методы		УПБА			
		A	B	C	D
1a	Тестирование с введением неисправности [a]	+	+	++	++
1b	Тестирование предполагаемых ошибок [b]	+	+	++	++
1c	Тесты, полученные из опыта эксплуатации	o	+	++	++

[a] Тестирование с введением неисправности использует специальные средства для внедрения неисправностей в систему. В системе это может быть выполнено через специальный тестовый интерфейс, специально подготовленные элементы или средства коммуникации. Этот метод часто используется для улучшения тестового охвата требований к безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[b] Тестирование предполагаемых ошибок основано на использовании экспертных знаний и данных, собранных в результате полученного из опыта умения предвидеть ошибки в тестируемом объекте. Затем для проверки этих ошибок проектируется набор тестов наряду с надлежащими средствами тестирования. Предположение ошибок является эффективным методом испытателя, который имеет опыт работы с подобными тестируемыми объектами.

8.4.3.2.6 Уровень надежности системы должен быть продемонстрирован с помощью обоснованных методов тестирования, приведенных в таблице 14.

Таблица 14 – Уровень надежности на уровне системы

Методы		УПБА			
		A	B	C	D
1a	Тестирование используемых ресурсов [a]	o	+	++	++
1b	Стресс-тест [b]	o	+	++	++
1c	Тестирование на помехоустойчивость и надежность при определенных условиях окружающей среды [c]	++	++	++	++

[a] На уровне системы тестирование используемых ресурсов обычно проводится в динамических условиях (например, автомобили-лаборатории или автомобили-прототипы). Тестируются также потребление энергии и загрузка коммуникационной шины.

[b] Стресс-тест верифицирует исправность работы системы в условиях высоких эксплуатационных нагрузок или повышенных требований со стороны окружающей среды. Таким образом, возможны тесты при высоких нагрузках на систему или с экстремальным объемом данных, вводимых пользователем, или запросов от других систем, а также тесты с экстремальными значениями температур, влажности и механических воздействий.

[c] Тесты на помехоустойчивость и надежность при определенных условиях окружающей среды, являются частным случаем стресс-тестов. Они включает в себя тестирование влияния электромагнитных помех и устойчивости к электростатическим разрядам [2], [3].

8.4.4 Интеграция и тестирование транспортного средства

8.4.4.1 Интеграция автомобиля

8.4.4.1.1 Устройство должно быть интегрировано в транспортное средство и для автомобиля должны быть выполнены комплексные тесты.

8.4.4.1.2 Должна быть выполнена верификация спецификации интерфейса устройства с коммуникационной сетью автомобиля и с сетью электропитания автомобиля.

8.4.4.2 Цели и методы тестирования во время испытаний транспортного средства

8.4.4.2.1 Для выявления систематических ошибок при интеграции систем автомобиля цели тестирования, полученные из требований 8.4.3.2.2 – 8.4.3.2.6, должны достигаться применением адекватных методов тестирования, как указано в соответствующих таблицах.

Примечание – В зависимости от реализованной функции, сложности или распределенного характера системы может быть разумно при адекватном обосновании перенести методы тестирования на другие подстадии интеграции.

8.4.4.2.2 Корректное выполнение требований функциональной безопасности на уровне транспортного средства должно быть продемонстрировано с помощью обоснованных методов тестирования, приведенных в таблице 15.

Таблица 15 – Корректное выполнение требований функциональной безопасности на уровне транспортного средства

Методы		УПБА			
		A	B	C	D
1a	Тестирование на основе требований [a)]	++	++	++	++
1b	Тестирование с введением неисправности [b)]	++	++	++	++
1c	Долговременное тестирование [c)]	++	++	++	++
1d	Тестирование у заказчика в реальных условиях [c)]	++	++	++	++

[a)] Тестирование на основе требований выполняет проверку требований на функциональность и нефункциональность.

[b)] Тестирование с введением неисправности использует специальные средства для внедрения неисправностей в устройство. В устройстве это может быть выполнено через специальный тестовый интерфейс или специально подготовленные элементы или средства связи. Этот метод часто используется, чтобы улучшить тестовый охват требований к безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[c)] Долговременное тестирование и тестирование у заказчика в реальных условиях похожи на тесты, полученные из опыта эксплуатации, но используют больший объем выборки, обычных пользователей в качестве испытателей и не связаны с предшествующими заданными сценариями тестирования, но выполняются в реальных условиях во время повседневной работы. Эти тесты могут иметь ограничения, если это необходимо для обеспечения безопасности испытателей, например, дополнительные меры безопасности или выполнение тестов с отключенными приводами.

8.4.4.2.3 Корректное функционирование, точность и синхронизация механизмов безопасности на уровне транспортного средства должны быть продемонстрированы с помощью обоснованных методов тестирования, приведенных в таблице 16. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Таблица 16 – Корректное функционирование, точность и синхронизация механизмов безопасности на уровне транспортного средства

Методы		УПБА			
		A	B	C	D
1a	Промышленные испытания [a)]	+	+	++	++
1b	Долговременное тестирование [b)]	+	+	++	++
1c	Тестирование у заказчика в реальных условиях [b)]	+	+	++	++

[a)] Промышленные испытания могут проверять рабочие характеристики (например, время сбоеустойчивости и управляемость транспортного средства в присутствии сбоев) механизмов безопасности устройства.

[b)] Долговременное тестирование и тестирование у заказчика в реальных условиях похожи на тесты, полученные из опыта эксплуатации, но используют больший объем выборки, обычных пользователей в качестве испытателей и не связаны с предшествующими заданными сценариями тестирования, но выполняются в реальных условиях во время повседневной работы. Эти тесты могут иметь ограничения, если это необходимо для обеспечения безопасности испытателей, например, дополнительные меры безопасности или выполнение тестов с отключенными приводами.

8.4.4.2.4 Согласованная и корректная реализация внешних интерфейсов на уровне

транспортного средства должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 17. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Таблица 17 – Согласованная и корректная реализация внешних и внутренних интерфейсов на уровне транспортного средства

Методы		УПБА			
		A	B	C	D
1a	Тестирование внешних интерфейсов [a]	o	+	++	++
1b	Проверка взаимодействия / коммуникации [b]	o	+	++	++

[a] Тесты интерфейса на уровне транспортного средства проверяют интерфейсы систем транспортного средства на совместимость. Они могут быть статическими, выполняющими подтверждение соответствия диапазона допустимых значений, паспортных данных или габаритов, а также динамическими, реализуемыми во время работы всего транспортного средства.

[b] Тестирование коммуникации и взаимодействия включает в себя тестирование связей между системами транспортного средства во время его работы для функциональных и нефункциональных требований.

8.4.4.2.5 Эффективность охвата диагностикой механизмами безопасности на уровне транспортного средства должна быть продемонстрирована с помощью обоснованных методов тестирования, приведенных в таблице 18. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Таблица 18 – Эффективность охвата диагностикой механизмами безопасности на уровне транспортного средства

Методы		УПБА			
		A	B	C	D
1a	Тестирование с введением неисправности [a]	o	+	++	++
1b	Тестирование предполагаемых ошибок [b]	o	+	++	++
1c	Тесты, полученные из опыта эксплуатации [c]	o	+	++	++

[a] Тестирование с введением неисправности использует специальные средства для введения неисправностей в транспортное средство. В транспортном средстве это может быть выполнено через специальный тестовый интерфейс, специально подготовленные аппаратные средства или средства коммуникации. Этот метод часто используется, чтобы улучшить тестовый охват требований к безопасности, так как в процессе обычной эксплуатации механизмы безопасности не вызываются.

[b] Тестирование предполагаемых ошибок основано на использовании экспертных знаний и данных, собранных в результате полученного из опыта умения предвидеть ошибки в транспортном средстве. Затем для проверки этих ошибок проектируется набор тестов наряду с надлежащими средствами тестирования. Предположение ошибок является эффективным методом испытателя, который имеет опыт работы с подобными транспортными средствами.

[c] Тесты, полученные из опыта эксплуатации, используют опыт и данные, собранные при эксплуатации. Анализируются ошибочное поведение транспортного средства или вновь появившиеся эксплуатационные ситуации и разрабатывается набор тестов для проверки транспортного средства по отношению к вновь полученным фактам.

8.4.4.2.6 Уровень надежности транспортного средства должен быть продемонстрирован с помощью обоснованных методов тестирования, приведенных в таблице 19. Данное требование распространяется на значения УПБА (A), (B), C и D в соответствии с 4.3.

Таблица 19 – Уровень надежности транспортного средства

Методы		УПБА			
		A	B	C	D
1a	Тестирование используемых ресурсов [a]	o	+	++	++
1b	Стресс-тест [b]	o	+	++	++
1c	Тестирование на помехоустойчивость и надежность при определенных условиях окружающей среды [c]	o	+	++	++
1d	Долговременное тестирование [d]	o	+	++	++

Окончание таблицы 19

[a] Тестирование используемых ресурсов устройства обычно проводится в динамических условиях (например, на автомобиле-лаборатории или автомобиле-прототипе). Тестируются также внутренние ресурсы устройства, потребление энергии или ограничение ресурсов других систем автомобиля. [b] Стресс-тест верифицирует исправность работы транспортного средства в условиях высоких эксплуатационных нагрузок или повышенных требований со стороны окружающей среды. Таким образом, возможны тесты при высоких нагрузках на транспортное средство или с экстремальным объемом данных, вводимых пользователем, или запросов от других систем, а также тесты с экстремальными значениями температур, влажности и механических воздействий. [c] Тесты на помехоустойчивость и надежность при определенных условиях окружающей среды являются частным случаем стресс-тестов. Они включают в себя тестирование влияния электромагнитных помех и устойчивости к электростатическим разрядам [2], [3]. [d] Долговременное тестирование и тестирование у заказчика в реальных условиях похожи на тесты, полученные из опыта эксплуатации, но используют больший объем выборки, обычных пользователей в качестве испытателей и не связаны с предшествующими заданными сценариями тестирования, но выполняются в реальных условиях во время повседневной работы.

8.5 Результаты работы

8.5.1 План интеграции и тестирования устройства (уточненный)

В результате выполнения требований 8.4.1.

8.5.2 Спецификация(и) тестирования интеграции

В результате выполнения требований 8.4.1.

8.5.3 Отчет(ы) о тестировании интеграции

В результате выполнения требований 8.4.2 – 8.4.4.

9 Подтверждение соответствия безопасности

9.1 Цели

Первая цель заключается в предоставлении доказательств о соответствии целям безопасности, а также о том, что концепция функциональной безопасности предназначена для обеспечения функциональной безопасности устройства.

Вторая цель заключается в предоставлении доказательств того, что цели безопасности корректны, полны и полностью достижимы для транспортного средства.

9.2 Общие положения

Целью предыдущих действий по верификации (например, при верификации проекта, анализе безопасности, тестировании и интеграции аппаратных средств, программного обеспечения и устройства) является предоставление доказательств того, что результаты каждого конкретного вида деятельности соответствуют заданным требованиям.

Подтверждение соответствия интегрированного устройства в типичном транспортном средстве(ах) призвано обеспечить доказательство пригодности его целевого использования и направлено на подтверждение адекватности мер безопасности для класса или множества транспортных средств. Подтверждение соответствия безопасности гарантирует, что цели безопасности являются достаточными и были достигнуты на основе экспертизы и испытаний.

9.3 Входная информация

9.3.1 Предварительные требования

Необходима следующая информация:

- результаты анализа опасностей и оценки рисков в соответствии с 7.5.1 ИСО 26262-3;
- цели безопасности в соответствии с 7.5.2 ИСО 26262-3;
- концепция функциональной безопасности в соответствии с 8.5.1 ИСО 26262-3.

9.3.2 Дополнительная информация

Следующая информация может быть учтена:

- план проекта (уточненный) (см. 5.5.1);
- техническая концепция системы безопасности (см. 7.5.1);
- функциональная концепция (из внешнего источника);
- план интеграции и тестирования устройства (уточненный) (см. 8.5.1);

- отчеты по результатам анализа системы безопасности (см. 7.5.6).

9.4 Требования и рекомендации

9.4.1 Среда подтверждения соответствия

9.4.1.1 Подтверждение соответствия целям безопасности должно быть выполнено для интегрированного устройства в типичном транспортном средстве.

Примечание – Такое интегрированное устройство включает в себя, если они применяются: систему, программное обеспечение, аппаратные средства; элементы, основанные на других технологиях, внешние меры.

9.4.2 Планирование подтверждения соответствия

9.4.2.1 Должен быть уточнен план подтверждения соответствия, включая:

a) выполнение подтверждения соответствия конфигурации устройства, в том числе его данные о калибровке в соответствии с приложением С ИСО 26262-6;

Примечание – Если подтверждение соответствия каждой конфигурации устройства не представляется возможным, то может быть выбрано их разумное подмножество.

b) спецификацию процедур подтверждения соответствия, тестовые примеры, выполняемые маневры и критерии приемки;

c) оборудование и требуемые условия окружающей среды.

9.4.3 Выполнение подтверждения соответствия

9.4.3.1 Если для подтверждения соответствия используется тестирование, то могут быть применены такие же требования, как это предусмотрено для верификации (см. 9.4.2 и 9.4.3 ИСО 26262-8).

9.4.3.2 Для целей безопасности, для которых должно быть выполнено подтверждение соответствия элемента на уровне автомобиля, необходимо оценить следующее:

a) управляемость.

Примечание – Подтверждение соответствия управляемости может быть выполнено, используя сценарии эксплуатации, в том числе при целевом и предсказуемом неправильном использовании;

b) эффективность мер безопасности для управления случайными и систематическими отказами;

c) эффективность внешних мер;

d) эффективность элементов, основанных на других технологиях.

9.4.3.3 Представленное ниже требование распространяется на значения УПБА (B), C и D цели безопасности. На уровне устройства должно быть выполнено подтверждение соответствия метрик для случайных отказов аппаратных средств для:

a) оценки нарушений цели безопасности из-за случайных отказов аппаратных средств, как это определено в разделе 9 ИСО 26262-5 относительно целевых значений, как определено требованием 7.4.4.3, и

b) оценки метрик архитектуры аппаратных средств в соответствии с критериями оценки из раздела 8 ИСО 26262-5 относительно целевых значений, как это определено требованием 7.4.4.2.

Примечание – Количественная оценка для элементов устройства определена в 9.4.2 и 9.4.3 ИСО 26262-5. Все устройство оценивается качественно, если в нем применяются элементы, основанные на других технологиях.

9.4.3.4 В соответствии с планом должно быть выполнено подтверждение соответствия транспортного средства целям безопасности, требованиям функциональной безопасности и предусмотренному применению, используя:

a) процедуры подтверждения соответствия и тесты для каждой цели безопасности, в том числе четко определенные критерии прохождения / непрохождения и

b) информацию об области применения, которая может включать сведения о конфигурации, условиях окружающей среды, дорожных ситуациях, эксплуатационных сценариях и т.д.

Примечание – Для подтверждения соответствия безопасности на уровне автомобиля могут быть созданы специальные эксплуатационные сценарии.

9.4.3.5 Должен применяться соответствующий набор следующих методов:

a) систематические тесты с заданными процедурами испытаний, тестовые примеры и критерии прохождения / непрохождения;

Пример – Положительные тесты функций и требований к безопасности, тестирование методом «черного ящика», моделирование, испытания с граничными значениями, тестирование с введением неисправности, испытания на выносливость, стресс-тесты, ускоренные испытания на долговечность, моделирование внешних воздействий.

b) виды анализа;

Пример – FMEA, FTA, ETA, моделирование.

c) долговременное тестирование, такое как вождение автомобиля по графикам и охваченные тестированием парки автомобилей;

d) тестирование у заказчика в реальных условиях, тестирование на стенде или вслепую, экспертные комиссии;

e) обзоры.

9.4.4 Оценка

9.4.4.1 Результаты подтверждения соответствия должны быть оценены.

9.5 Результаты работы

9.5.1 План подтверждения соответствия (уточненный)

В результате выполнения требований 9.4.2.

9.5.2 Отчет о подтверждении соответствия

В результате выполнения требований 9.4.3 и 9.4.4.

10 Оценка функциональной безопасности

10.1 Цель

Целью требований настоящего раздела является оценка функциональной безопасности, достигаемой устройством.

10.2 Общие положения

Структурное подразделение, отвечающее за функциональную безопасность (например, у производителя транспортного средства или у поставщика, если последний несет ответственность за функциональную безопасность), инициирует ее оценку.

10.3 Входная информация

10.3.1 Предварительные требования

Необходима следующая информация:

- руководство по безопасности в соответствии с 6.5.3 ИСО 26262-2;
- план по обеспечению безопасности (уточненный) в соответствии с 5.5.2 ИСО 26262-5, 5.5.2 ИСО 26262-6 и 5.5.2 настоящего стандарта;
- отчеты о мерах подтверждения в соответствии с 6.5.5 ИСО 26262-2;
- протокол аудита, если имеется, в соответствии с 6.5.4 ИСО 26262-2;
- план оценки функциональной безопасности (уточненный) в соответствии с 5.5.5.

10.3.2 Дополнительная информация

Не задается.

10.4 Требования и рекомендации

10.4.1 Для каждой стадии жизненного цикла системы безопасности, представленного на рисунке 2 ИСО 26262-2, оценка функциональной безопасности должна рассматриваться отдельно. Данное требование распространяется на значения УПБА (B), C и D цели безопасности.

10.4.2 Оценка функциональной безопасности должна проводиться в соответствии с 6.4.9 ИСО 26262-2. Данное требование распространяется на значения УПБА (B), C и D цели безопасности.

10.5 Результаты работы

10.5.1 Отчет по оценке функциональной безопасности

В результате выполнения требований 10.4.1 и 10.4.2.

11 Запуск в производство

11.1 Цель

11.1.1 Целью настоящего раздела является специфицировать критерии запуска в производство при завершении разработки устройства. Запуск в производство подтверждает, что устройство соответствует требованиям функциональной безопасности на уровне транспортного средства.

11.2 Общие положения

11.2.1 Запуск в производство подтверждает, что устройство готово к серийному производству и эксплуатации.

11.2.2 Доказательство соответствия предварительным условиям для серийного производства обеспечивается в результате:

- завершения верификации и подтверждения соответствия в ходе разработки аппаратных средств, программного обеспечения, системы, устройства и автомобиля и
- успешной общей оценки функциональной безопасности.

11.2.3 Такая документация для запуска в производство является основой для изготовления компонентов, систем или транспортных средств и подписывается лицом, ответственным за запуск.

11.3 Входная информация

11.3.1 Предварительные требования

Необходима следующая информация:

- отчет по оценке функциональной безопасности в соответствии с 10.5.1;
- руководство по безопасности в соответствии с 6.5.3 ИСО 26262-2.

11.3.2 Дополнительная информация

Не задается.

11.4 Требования и рекомендации

11.4.1 Запуск в производство

11.4.1.1 Запуск в производство устройства должен быть утвержден только в том случае, если получены результаты работы, перечисленные в 11.3.1, если они необходимы (в зависимости от УПБА), а также обеспечено доверие функциональной безопасности.

11.4.2 Документация для запуска в производство

11.4.2.1 Документация по функциональной безопасности для запуска в производство должна включать следующую информацию:

a) фамилию и подпись лица, ответственного за запуск в производство;
b) версию(и) запускаемого устройства;
c) конфигурацию запускаемого устройства;
d) ссылки на связанные с ней документы;
e) дату запуска.

Примечание – Документация по функциональной безопасности может быть частью документации по запуску устройства в производство или она может представлять собой отдельный документ.

11.4.2.2 При запуске в производство должны быть готовы базовая конфигурация программного обеспечения и базовая конфигурация аппаратных средств, которые должны быть документально оформлены в соответствии с разделом 10 ИСО 26262-8.

11.4.2.3 Все вопросы, связанные с выявленными аномалиями безопасности, должны быть решены в соответствии с требованиями 5.4.2 ИСО 26262-2 и раздела 8 ИСО 26262-8.

11.5 Результаты работы

11.5.1 Отчет о запуске в производство

В результате выполнения требований 11.4.1 и 11.4.2.

Приложение А
(справочное)

Обзор и поток документов подстадии разработки изделия на уровне системы

Таблица А.1 содержит обзор целей, предварительных требований и результатов работы подстадии разработки изделия на уровне системы.

Таблица А.1 – Обзор разработки изделия на уровне системы

Раздел	Цели	Предварительные требования	Результаты работы
5 Начальная подстадия разработки изделия на уровне системы	Цель начальной подстадии разработки изделия на уровне системы заключается в определении и планировании действий по обеспечению функциональной безопасности для отдельных подстадий разработки системы. Кроме того, необходимо включить вспомогательные процессы, описанные в ИСО 26262-8. Эти спланированные действия по обеспечению безопасности на уровне системы будут включены в план по обеспечению безопасности	План проектирования (уточненный) (см. 6.5.2 ИСО 26262-2). План по обеспечению безопасности (см. 6.5.2 ИСО 26262-2). Концепция функциональной безопасности (см. 8.5.1 ИСО 26262-3)	5.5.1 План проекта (уточненный). 5.5.2 План по обеспечению безопасности (уточненный). 5.5.3 План интеграции и тестирования устройства. 5.5.4 План подтверждения соответствия. 5.5.5 План оценки функциональной безопасности (уточненный)
6 Спецификация технических требований к системе безопасности	Первой целью данной подстадии является определение технических требований к системе безопасности. Спецификация технических требований к системе безопасности уточняет концепцию функциональной безопасности с учетом как функциональной концепции, так и предположений предварительной архитектуры (см. ИСО 26262-3). Вторая цель заключается в проверке путем анализа, что технические требования к системе безопасности соответствуют требованиям функциональной безопасности	Концепция функциональной безопасности (см. 8.5.1 ИСО 26262-3). План подтверждения соответствия (см. 5.5.4)	6.5.1 Спецификация технических требований к системе безопасности 6.5.2 Отчет о верификации системы. 6.5.3 План подтверждения соответствия (уточненный)
7 Проектирование системы	Первая цель рассматриваемой подстадии заключается в разработке проекта системы и технической концепции системы безопасности, которые удовлетворяют функциональным требованиям и спецификации технических требований к системе безопасности устройства. Вторая цель рассматриваемой подстадии заключается в проверке того, что проект системы и техническая концепция системы безопасности соответствуют спецификации технических требований к системе безопасности	План интеграции и тестирования устройства (см. 5.5.3). Спецификация технических требований к системе безопасности (см. 6.5.1)	7.5.1 Техническая концепция системы безопасности. 7.5.2 Спецификация проекта системы. 7.5.3 Спецификация программно-аппаратного интерфейса. 7.5.4 Спецификация требований к производству, эксплуатации, обслуживанию и выводу из эксплуатации. 7.5.5 Отчет о верификации системы (уточненный). 7.5.6 Отчеты по результатам анализа системы безопасности, полученный в результате выполнения требований 7.4.3

Окончание таблицы А.1

Раздел	Цели	Предварительные требования	Результаты работы
8 Интеграция и тестирование устройства	Стадия интеграции и тестирования включа-ет в себя три этапа, реализующие две основные цели. На первом этапе выполняется интеграция аппаратных средств и программного обеспечения каждого элемента устройства. Второй этап заключается в интеграции элементов устройства и создании всей системы. На третьем этапе выполняется интеграция устройства с другими системами в транспортном средстве и с самим транспортным средством. Первая цель процесса интеграции заключается в проверке соответствия каждого требования безопасности его специфика-ции и заданному значению УПБА. Вторая цель заключается в проверке того, что «Проект системы», удовлетворяющий требованиям безопасности (см. раздел 7 «Проектирование системы»), правильно реализован полностью интегрированным устройством	Цели безопасности (см. 7.5.2). Концепция функциональной безопасности (см. 8.5.1 ИСО 26262-3). План интеграции и тестирования устройства (см. 5.5.3). Техническая концепция системы безопасности см. 7.5.1). Спецификация проекта системы (см. 7.5.2). Спецификация программно-аппаратного интерфейса (см. 7.5.3)	8.5.1 План интеграции и тестирования устройства (уточненный). 8.5.2 Спецификация(и) тестирования интеграции. 8.5.3 Отчет(ы) о тестировании интеграции
9 Подтверждение соответствия безопасности	Первая цель заключается в предоставлении доказательств о соответствии целям безопасности, а также о том, что концепция функциональной безопасности предназначена для обеспечения функциональной безопасности устройства. Вторая цель заключается в предоставлении доказательств того, что цели безопасности корректны, полны и полностью достижимы для транспортного средства	Результаты анализа опасностей и оценки рисков (см. 7.5.1 ИСО 26262-3). Цели безопасности (см. 7.5.2 ИСО 26262-3). Концепция функциональной безопасности (см. 8.5.1 ИСО 26262-3). План подтверждения соответствия (уточненный) (см. 6.5.3)	9.5.1 План подтверждения соответствия (уточненный), полученный в результате выполнения требования 9.4.2. 9.5.2 Отчет о подтверждении соответствия, полученный в результате выполнения требований 9.4.3 – 9.4.4
10 Оценка функциональной безопасности	Целью требований настоящего раздела является оценка функциональной безопасности, достигаемой устройством	Руководство по безопасности (см. 6.5.3 ИСО 26262-2). План по обеспечению безопасности (уточненный) (см. 5.5.2 ИСО 26262-5, 5.5.2 ИСО 26262-6 и 5.5.2). Отчеты о мерах подтверждения (см. 6.5.5 ИСО 26262-2). Протокол аудита, если имеется, (см. 6.5.4 ИСО 26262-2). План оценки функциональной безопасности (уточненный) (см. 5.5.5)	10.5.1 Отчет по оценке функциональной безопасности, полученный в результате выполнения требований 10.4.1 и 10.4.2
11 Запуск изделия в производство	Целью настоящего раздела является специфицирование критериев запуска в производство при завершении разработки устройства. Запуск в производство подтверждает, что устройство соответствует требованиям функциональной безопасности на уровне транспортного средства	Отчет по оценке функциональной безопасности (см. 10.5.1). Руководство по безопасности (см. 6.5.3 ИСО 26262-2)	11.5.1 Отчет о запуске в производство, полученный в результате выполнения требований 11.4.1 и 11.4.2

Приложение В
(справочнное)

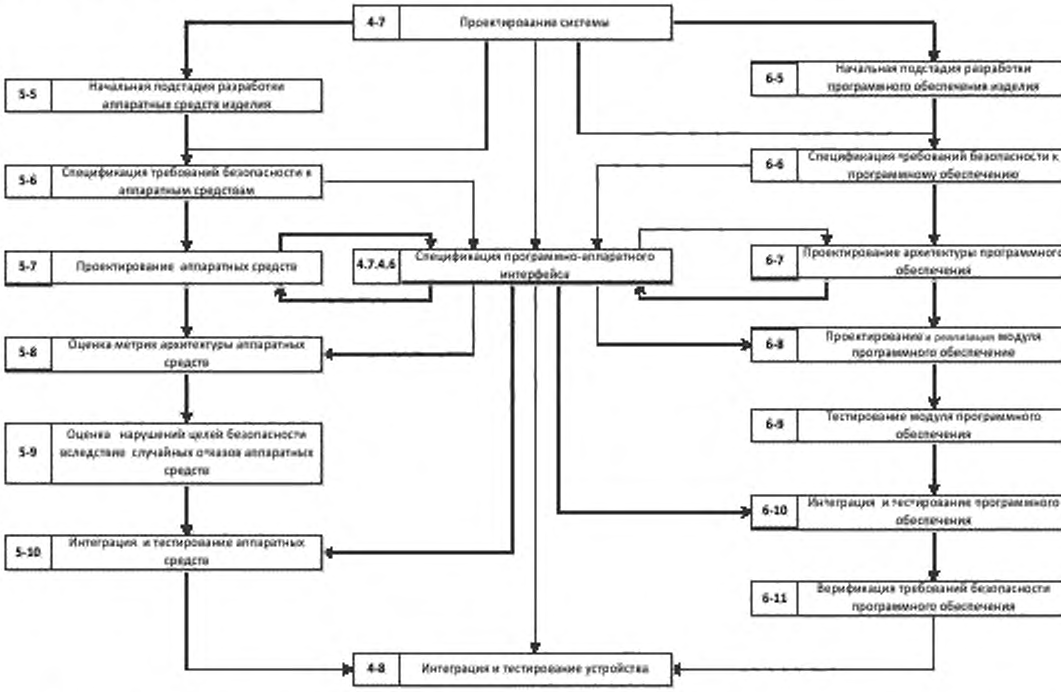
Пример содержания программно-аппаратного интерфейса

В.1 В настоящем приложении представлены дополнительные разъяснения по программно-аппаратному интерфейсу.

Аппаратно-программный интерфейс специфицируется в соответствии с требованиями настоящего стандарта на подстадии «Проектирование системы». Эта спецификация уточняется на соответствующих подстадиях в процессе непрерывно продолжающейся разработки аппаратных средств (ИСО 26262-5) и программного обеспечения (ИСО 26262-6).

Во-первых, на рисунке В.1 приведено общее представление, демонстрирующее связь между разработкой изделия на уровнях системы, аппаратных средств и программного обеспечения, а также роль программно-аппаратного интерфейса. Программно-аппаратный интерфейс связывает между собой различные уровни разработки изделия. Программно-аппаратный интерфейс используется для согласования вопросов взаимодействия при проектировании аппаратных средств и программного обеспечения.

Во-вторых, чтобы упростить спецификацию программно-аппаратного интерфейса, дан перечень типовых программно-аппаратных элементов интерфейса, а также неполный перечень характеристик, реализуемых этими элементами программно-аппаратного интерфейса.



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

Рисунок В.1 – Общее представление о взаимодействии с программно-аппаратным интерфейсом

В.2 При спецификации программно-аппаратного интерфейса могут быть рассмотрены следующие его элементы:

a) память:

1) энергозависимая память (например, ОЗУ);

2) энергонезависимая памяти (например, ПЗУ);

b) интерфейсы шины [например, локальная сеть контроллеров (CAN), коммутируемая локальная сеть (LIN), внутренний высокоскоростной последовательный канал (HSSL)];

c) преобразователь:

1) аналого-цифровой;
2) цифро-аналоговый;
3) широтно-импульсной модуляции;
d) мультиплексор;
e) электрический ввод-вывод;
f) сторожевое устройство:
1) внутреннее;
2) внешнее.

B.3 При спецификации программно-аппаратного интерфейса могут быть рассмотрены следующие его характеристики:

a) прерывание;
b) согласованность синхронизации;
c) целостность данных;
d) инициализация:
1) память и регистры;
2) управление начальной загрузкой;
e) передача сообщений:
1) отправление сообщения;
2) получение сообщения;
f) режимы сети:
1) ждущий;
2) активный;
g) управление памятью:
1) при считывании;
2) при записи;
3) при диагностике;
4) адресного пространства;
5) типов данных;
h) счетчик реального времени:
1) запуск счетчика;
2) остановка счетчика;
3) фиксация значения счетчика;
4) загрузка счетчика.

В таблице B.1 приведен пример, демонстрирующий распределение характеристик программно-аппаратного интерфейса по его элементам.

Таблица B.1 – Пример входных значений внутренних сигналов

Описание	Идентификатор аппаратных средств	Идентификатор программного обеспечения	Канал 1	Канал 2	№ мультиплексора – Канал 1	№ мультиплексора – Канал 2	Тип данных программно-аппаратого интерфейса	Адрес Канала 1	Адрес Канала 2	Модуль	Тип интерфейса	Комментарии	Диапазон значений	Точность от (% диапазона значений
Входы														
Вход 1	IN_1	IN_1	x		4		U16	0x8000		V	Аналоговый внутренний	Аналоговый вход 1	0 - 5	0,50 %

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 26262-5:2011	–	*
ИСО 26262-6:2011	–	*
ИСО 26262-7:2011	–	*
ИСО 26262-8:2011	–	*
ИСО 26262-9:2011	–	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.		

Библиография

[1] ISO 11451 (all parts), Road vehicles — Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy

[2] IEC 61000-6-1, Electromagnetic compatibility (EMC) — Part 6-1: Generic standards — Immunity for residential, commercial and light-industrial environments

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

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

Ключевые слова: функциональная безопасность; жизненный цикл систем; транспортные средства; электрические компоненты; программируемые электронные компоненты и системы; разработка на уровне системы; анализ опасностей и оценка рисков

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

Усл. печ. л. 4.19. Тираж 31 экз. Зак. 83

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