ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-3— 2014

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 3

Стадия формирования концепции

ISO 26262-3:2011
Road vehicles — Functional safety — Part 3: Concept phase
(IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 10 июня 2014 г. № 522-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-3:2011 «Дорожные транспортные средства. Функциональная безопасность. Часть 3. Стадия формирования концепции» (ISO 26262-3:2011 «Road vehicles — Functional safety — Part 3: Concept phase»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов и документов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины, определения и сокращения . . . 2
4 Требования соответствия настоящему стандарту . . . 2
4.1 Общие требования . . . 2
4.2 Интерпретация таблиц . . . 2
4.3 Требования и рекомендации, зависимые от значения УПБА . . . 3
5 Определение устройства . . . 3
5.1 Цели . . . 3
5.2 Общие положения . . . 3
5.3 Входная информация . . . 3
5.4 Требования и рекомендации . . . 4
5.5 Результаты работы . . . 4
6 Начальное формирование жизненного цикла системы безопасности . . . 4
6.1 Цели . . . 4
6.2 Общие положения . . . 4
6.3 Входная информация . . . 5
6.4 Требования и рекомендации . . . 5
6.5 Результаты работы . . . 6
7 Анализ опасностей и оценка рисков . . . 6
7.1 Цель . . . 6
7.2 Общие положения . . . 6
7.3 Входная информация . . . 6
7.4 Требования и рекомендации . . . 6
7.5 Результаты работы . . . 11
8 Концепция функциональной безопасности . . . 11
8.1 Цель . . . 11
8.2 Общие положения . . . 11
8.3 Входная информация . . . 12
8.4 Требования и рекомендации . . . 12
8.5 Результаты работы . . . 15
Приложение А (справочное) Обзор и поток документов стадии формирования концепции . . . 16
Приложение В (справочное) Анализ опасностей и оценка рисков . . . 17
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 24
Библиография . . . 25

Введение

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

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

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

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

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

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

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

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

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

e) устанавливает требования к взаимодействию с поставщиками.

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

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

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

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

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

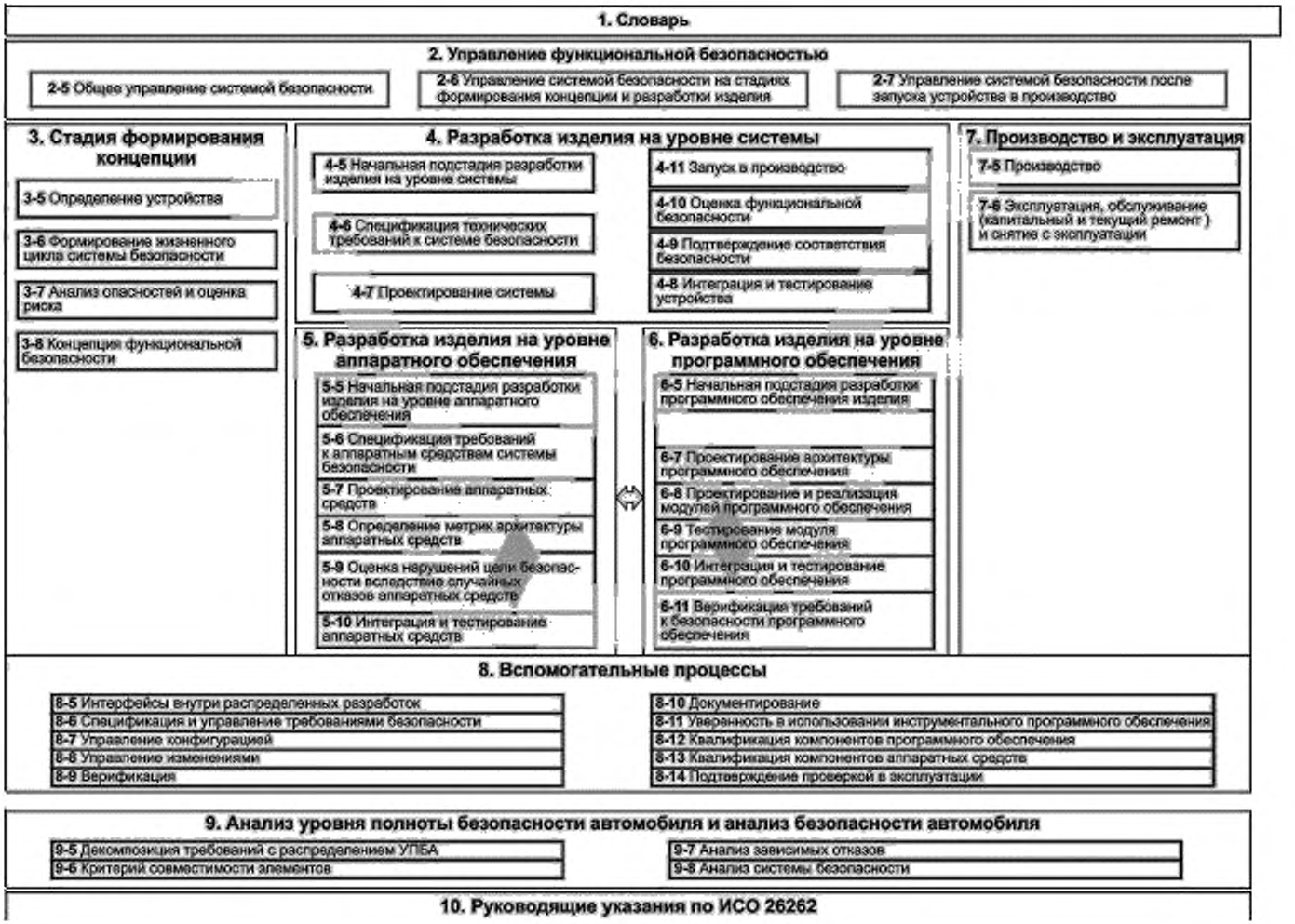


Рисунок 1 — Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 3

Стадия формирования концепции

Road vehicles. Functional safety. Part 3. Concept phase

Дата введения — 2015—05—01

1 Область применения

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

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

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

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

Настоящий стандарт устанавливает требования для стадии формирования концепции изделия для автомобильной промышленности, в том числе к:

- определению устройства;
- подстадии начального формирования жизненного цикла системы безопасности;
- анализу опасностей и оценке рисков;
- концепции функциональной безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

Издание официальное

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

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

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

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

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

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

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

3 Термины, определения и сокращения

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

4 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

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

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

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 Определение устройства

5.1 Цели

Первой целью настоящего раздела является определение и описание устройства, его зависимостей и взаимодействие с внешней средой и другими устройствами.

Второй целью является поддержка адекватного понимания этого устройства, чтобы могли быть выполнены соответствующие действия на последующих стадиях.

5.2 Общие положения

В данном разделе перечислены требования и рекомендации к формированию определения устройства, учитывая его функциональность, интерфейсы, условия внешней среды, правовые требования, опасности и т. д. Это определение позволит обеспечить достаточным объемом информации об устройстве лиц, выполняющих последующие подстадии: «начальное формирование жизненного цикла системы безопасности» (см. раздел 6), «анализ опасностей и оценка рисков» (см. раздел 7) и «концепция функциональной безопасности» (см. раздел 8).

Примечание — Таблица А.1 содержит обзор целей, предварительных требований и результатов работы стадии формирования концепции.

5.3 Входная информация

5.3.1 Предварительные требования

Не задаются.

5.3.2 Дополнительная информация

Следующая информация может быть учтена:

- любая информация, связанная с устройством, которая уже существует, например, идея изделия, эскизный проект, соответствующие патенты, результаты предварительных испытаний, документация от предшествующих устройств, соответствующая информация о других независимых от разрабатываемого устройствах.

5.4 Требования и рекомендации

5.4.1 Должны быть определены функциональные и нефункциональные требования устройства, а также зависимости между устройством и его окружением.

Примечания

1 Требования могут быть классифицированы как связанные с безопасностью после определения целей безопасности и значений их УПБА.

2 Требуемая информации является необходимым вкладом в определение устройства, хотя она не связана с безопасностью. Если такая информация отсутствует, то ее создание может быть инициировано требованиями настоящего пункта.

Эта информация включает в себя:

a) концепцию выполняемой устройством функции, описание цели и функционального назначения, в том числе режимов работы и состояний устройства;

b) эксплуатационные ограничения и ограничения внешней среды;

c) правовые требования (в частности, законы и постановления), национальные и международные стандарты;

d) описание поведения, реализуемое аналогичными функциями, устройствами или элементами, если таковые имеются;

e) предположения об ожидаемом поведении устройства;

f) возможные последствия вследствие некорректного поведения, включая известные отказы и опасности.

Примечание — Могут быть включены известные, связанные с безопасностью инциденты в подобных устройствах.

5.4.2 Должны быть определены габариты устройства, его интерфейсы и предположения о его взаимодействии с другими устройствами и элементами, учитывая:

a) элементы устройства.

Примечание — Элементы могут также быть основаны на других технологиях;

b) предположения о влиянии поведения устройства на другие устройства или элементы, которые окружают устройство;

c) взаимодействия устройств с другими устройствами или элементами;

d) функциональность, необходимую другим устройствам, элементам и окружающей среде;

e) функциональность, необходимую от других устройств, элементов и окружающей среды;

f) выделение и распределение функций между включенными в устройство системами и элементами;

g) сценарии работы, которые влияют на функциональность устройства.

5.5 Результаты работы

Определение устройства формируется в результате выполнения требований 5.4.

6 Начальное формирование жизненного цикла системы безопасности

6.1 Цели

Первая цель начального формирования жизненного цикла системы безопасности — установить различие между разработкой нового устройства и модификацией существующего устройства (см. рисунок 2 ИСО 26262-2).

Вторая цель заключается в определении действий в процессах жизненного цикла системы безопасности (см. рисунок 2 ИСО 26262-2), которые будут выполняться в случае модификации.

6.2 Общие положения

На основании определения устройства выполняется начальное формирование жизненного цикла системы безопасности либо для разработки нового, либо для модификации существующего устройства. В случае модификации существующего устройства происходит настройка связанных с безопасностью действий.

6.3 Входная информация

6.3.1 Предварительные требования

Следующая информация должна быть доступна:

- определение устройства в соответствии с требованиями 5.5.1.

6.3.2 Дополнительная информация

Следующая информация может быть учтена:

- еще не охваченная определением устройства, любая имеющаяся информация, полезная для выполнения анализа влияния.

Пример — Концепция изделия, запросы на изменение, осуществление планирования, подтверждение проверкой эксплуатацией.

6.4 Требования и рекомендации

6.4.1 Определение вида разработки

6.4.1.1 Должно быть установлено, является ли создание устройства новой разработкой или, если это модификация, то существующего устройства или его внешней среды:

a) в случае новой разработки она должна начинаться с анализа опасностей и оценки рисков в соответствии с разделом 7;

b) в случае модификации устройства или его внешней среды, выполняемые подстадии жизненного цикла и действия на них определяются в соответствии с 6.4.2.

Примечание — При модификации может быть использовано подтверждение проверкой в эксплуатации (см. раздел 14 ИСО 26262-8).

6.4.2 Анализ влияния и возможная настройка жизненного цикла системы безопасности при модификации

6.4.2.1 Должен быть проведен анализ влияния для того, чтобы определить и описать предполагаемое изменение, применяемое к устройству или его окружению, и оценить влияние таких модификаций.

Примечания

1 Модификации устройства включают в себя модификации проекта и модификации реализации устройства. Модификации проекта могут возникнуть в результате изменений требований (например, функциональных или связанных с повышением производительности и оптимизацией затрат). Модификации реализации не влияют на спецификацию или производительность устройства, а только на особенности реализации.

Пример — Модификации реализации могут возникнуть в результате корректировки программного обеспечения или в случае новой разработки или новых средств производства.

2 Модификации данных конфигурации или калибровочных данных рассматриваются как модификации устройства, если они влияют на его функциональное поведение.

3 Модификации внешней среды устройства могут возникнуть в результате установки устройства в новую целевую внешнюю среду (например, другой вариант автомобиля) или в результате модернизации других устройств или элементов, взаимодействующих с (или находящихся в непосредственной близости от) данным устройством.

6.4.2.2 Анализ влияния должен выявить и указать области, на которые повлияли модификации устройства и изменения между предыдущими и будущими условиями использования этого устройства, в том числе:

a) эксплуатационные ситуации и режимы работы;

b) интерфейсы с внешней средой;

c) характеристики установки, такие как расположение в транспортном средстве, конфигурации и варианты транспортного средства;

d) диапазоны значений параметров окружающей среды, например, температуры, высоты над уровнем моря, влажности, вибрации, электромагнитных помех, а также видов топлива.

6.4.2.3 Должно быть идентифицировано и описано значение модификации для функциональной безопасности.

6.4.2.4 Должны быть идентифицированы и описаны результаты работы, на которые модификации оказали влияние и которые должны быть обновлены.

6.4.2.5 Должны быть настроены действия по обеспечению безопасности в соответствии с применяемой стадией жизненного цикла.

6.4.2.6 Настройка должна быть основана на результатах анализа влияния.

6.4.2.7 Результаты настройки должны быть включены в план по обеспечению безопасности в соответствии с 6.4.3 ИСО 26262-2.

6.4.2.8 Результаты работы, на которые модификации оказали влияние, должны быть получены повторно.

Примечание — Результатом работы, на который влияют модификации, является план подтверждения соответствия (см. ИСО 26262-4).

6.4.2.9 В случае потери результатов работы или если результаты работы не соответствуют требованиям настоящего стандарта, должны быть определены необходимые действия для достижения такого соответствия.

6.5 Результаты работы

6.5.1 Анализ влияния

В результате выполнения требований 6.4.2.1—6.4.2.4.

6.5.2 План по обеспечению безопасности (уточненный)

В результате выполнения требований 6.4.2.5 – 6.4.2.9.

7 Анализ опасностей и оценка рисков

7.1 Цель

Целью анализа опасностей и оценки рисков является идентификация и классификация опасностей, которые могут привести к неправильному функционированию устройства, а также формулирование целей безопасности, связанных с предотвращением или смягчением последствий опасных событий, чтобы избежать необоснованного риска.

7.2 Общие положения

Анализ опасностей, оценки рисков и определение значения УПБА используются для определения целей безопасности для элемента так, чтобы предотвратить неоправданный риск. С этой целью оцениваются потенциально опасные события устройства. Цели безопасности и их значения УПБА определяются систематической оценкой опасных событий. Значения УПБА определяются с учетом оценки влияющих факторов, таких как тяжесть, вероятность воздействия и управляемость опасного события. Для этого необходимо знать функциональное поведение элемента, поэтому детальное проектирование элемента не обязательно должно быть известно.

7.3 Входная информация

7.3.1 Предварительные требования

Следующая информация должна быть доступна:

- определение устройства в соответствии с 5.5.

7.3.2 Дополнительная информация

Следующая информация может быть учтена:

- результаты анализа влияния, если они применимы (см. 6.5.1), и
- соответствующая информация о других независимых устройствах (из внешнего источника).

7.4 Требования и рекомендации

7.4.1 Запуск процедуры анализа опасностей и оценки рисков

7.4.1.1 Анализ опасностей и оценка рисков должны быть основаны на определении устройства.

7.4.1.2 Анализ опасностей и оценка рисков устройства должны выполняться без его внутренних механизмов безопасности, то есть механизмы безопасности, предназначенные для реализации или которые уже были реализованы в предшественнике устройства, не должны рассматриваться при анализе опасностей и оценке рисков.

Примечания

1 При оценке устройства могут быть полезны доступные и достаточно независимые внешние меры.

Пример — Система динамической стабилизации может смягчить последствия отказов в системах шасси, обеспечивая дополнительное управление, если показано, что она доступна и достаточно независима.

2 Механизмы безопасности устройства, которые предназначены для реализации или уже были реализованы, включены в концепцию функциональной безопасности.

7.4.2 Анализ ситуации и идентификация опасности

7.4.2.1 Анализ ситуации

7.4.2.1.1 Должны быть описаны эксплуатационные ситуации и режимы работы, в которых некорректное поведение устройства приводит к опасному событию, как для случаев, когда транспортное средство используется правильно, так и для предсказуемо неправильного использования.

Примечание — Эксплуатационная ситуация предусматривает пределы, в которых устройство должно вести себя безопасным образом. Например, для обычного пассажирского дорожного транспортного средства не предполагается, что оно должно двигаться по пересеченной местности с большой скоростью.

7.4.2.2 Идентификация опасностей

7.4.2.2.1 Опасности должны определяться систематически при использовании соответствующих методов.

Примечание — Для выявления опасности на уровне устройства могут быть использованы такие методы, как мозговой штурм, контрольные листы, картина изменения качества во времени, FMEA и полевые исследования.

7.4.2.2.2 Опасности должны быть определены в терминах условий или поведения, которые можно наблюдать на уровне автомобиля.

Примечания

1 В общем случае каждая опасность будет иметь несколько возможных причин, связанных с реализацией устройства, но они не должны рассматриваться в ходе анализа опасностей и оценки рисков для определения условий или поведения, которые возникают при рассмотрении функционального поведения устройства.

2 Могут рассматриваться только опасности, связанные с самим устройством, все остальные системы (внешние меры), как предполагается, будут функционировать правильно, если они достаточно независимы.

7.4.2.2.3 Должны быть определены опасные события для соответствующих комбинаций эксплуатационных ситуаций и опасностей.

7.4.2.2.4 Должны быть идентифицированы последствия опасных событий.

Примечание — Если отказы на уровне устройства вызывают потерю нескольких функций устройства, то анализ ситуации и процедура выявления опасности рассматривают результирующие опасные события из-за неправильного поведения всего устройства или транспортного средства.

Пример — Отказ бортовой системы электропитания может привести к одновременной потере ряда функций, в том числе «крутящего момента двигателя», «гидроусилителя рулевого управления» и «переднего освещения».

7.4.2.2.5 Если существуют опасности, идентифицированные в соответствии с 7.4.2.2, которые находятся вне области применения настоящего стандарта (см. раздел 1), то должна быть особо отмечена и доведена до сведения ответственных лиц необходимость соответствующих мер по смягчению или управлению этими опасностями.

Примечание — Для таких опасностей, находящихся вне области применения настоящего стандарта, их классификация не является необходимой.

7.4.3 Классификация опасных событий

7.4.3.1 Все опасные события, идентифицированные в соответствии с 7.4.2.3, должны быть классифицированы, кроме тех, которые находятся вне области применения настоящего стандарта.

Примечание — Если классификацию данной опасности по тяжести последствий, вероятности воздействия или управляемости сделать трудно, то она классифицируется консервативно, то есть всякий раз, когда есть сомнения, ей присваивается более высокое значение УПБА, а не низкое.

7.4.3.2 Тяжесть последствий потенциального вреда должна оцениваться на основе определенного обоснования для каждого опасного события. Тяжесть последствий должна быть отнесена к одному из классов тяжести последствий S0, S1, S2 и S3 в соответствии с таблицей 1.

Примечания

1 Оценка риска опасных событий основывается на возможном причинении вреда каждому человеку, подвергающемуся влиянию опасного события, включая водителя или пассажиров транспортного средства, вызывающего опасное событие, и других лиц, потенциально находящихся в опасности, таких как велосипедисты, пешеходы и пассажиры других транспортных средств. Для характеристики степени тяжести последствий может быть использована Краткая Шкала Повреждений (КШП), представленная в приложении В. Примеры различных типов тяжести последствий и аварий см. в приложении В.

2 Класс тяжести последствий может быть основан на сочетании травм и это может привести к более высокой оценке тяжести последствий, чем результат простого рассмотрения отдельных травм.

3 Оценка учитывает обоснованную последовательность событий для оцениваемой ситуации.

4 Определение тяжести последствий основано на репрезентативной выборке лиц из потенциального круга покупателей.

Таблица 1 — Классы тяжести последствий

	Класс			
	S0	S1	S2	S3
Описание	Нет травм	Легкие и умеренные травмы	Тяжелые и опасные для жизни травмы (вероятное выживание)	Опасные для жизни раны (сомнительное выживание), травмы со смертельным исходом

7.4.3.3 Класс тяжести последствий S0 может быть назначен, если анализ рисков установит, что последствия ошибочного поведения устройства четко ограничены материальным ущербом и не влекут за собой вред людям. Если опасности присваивается класс тяжести последствий S0, то назначение УПБА не требуется.

7.4.3.4 Вероятность воздействия каждой эксплуатационной ситуации должна быть оценена на основе определенного обоснования для каждого опасного события. Вероятность воздействия должна быть отнесена к одному из классов вероятности воздействия E0, E1, E2, E3 и E4 в соответствии с таблицей 2.

Примечания

1 Для классов от E1 до E4 разница в значении вероятности воздействия от одного класса E до следующего составляет один порядок величины.

2 Определение воздействия основано на репрезентативной выборке эксплуатационных ситуаций для рынков сбыта.

3 Для получения дополнительной информации и примеров, связанных с вероятностью воздействия, см. приложение B.

Таблица 2 — Классы вероятности воздействий эксплуатационных ситуаций

	Класс				
	E0	E1	E2	E3	E4
Описание	Невероятное	Очень низкая вероятность	Низкая вероятность	Средняя вероятность	Высокая вероятность

7.4.3.5 Количество транспортных средств, оснащенных устройством, не должно учитываться при оценке вероятности воздействия.

Примечание — При выполнении оценки вероятности воздействия предполагается, что каждый автомобиль оснащен устройством. Это означает, что аргумент «вероятность воздействия может быть уменьшена, потому что устройство не присутствует в каждом транспортном средстве (так как только некоторые автомобили оснащены устройством)», является недопустимым.

7.4.3.6 Класс E0 может быть использован для тех ситуаций, которые определены во время анализа опасности и оценки риска и которые считаются крайне необычными или невероятными, и, следовательно, не рассматриваются. Должно быть документально оформлено обоснование для исключения таких ситуаций. Если опасности присваивается класс воздействия E0, то не требуется назначения УПБА.

Пример — E0 может быть использован в случае «форс-мажорного» риска (см. B.3).

7.4.3.7 Управляемость каждого опасного события водителем или другими лицами, потенциально находящимися в опасности, должна быть оценена на основе определенного обоснования для каждого опасного события. Управляемость должна быть отнесена к одному из классов управляемости C0, C1, C2 и C3 в соответствии с таблицей 3.

Примечания

1 Для классов от С1 до С3 разница в значении вероятности от одного класса С до следующего составляет один порядок величины.

2 Под оценкой управляемости понимается оценка вероятности того, что водитель или другие лица, потенциально находящиеся в опасности, смогут получить достаточный контроль над опасным событием, таким образом, что они могут избежать конкретного вреда. Для этой цели используется параметр С, с классами С1, С2 и С3 для классификации возможности избежать вреда. Предполагается, что водитель находится в надлежащем состоянии для управления (например, он/она не устала), имеет соответствующую водительскую подготовку (он / она имеет водительское удостоверение) и соблюдает все действующие правила дорожного движения, в том числе необходимые требования предосторожности, чтобы избежать рисков для других участников дорожного движения. Некоторые примеры, которые служат интерпретацией данных классов, приведены в таблице В.4. Учитывается разумно предсказуемое неправильное использование.

3 Если опасное событие не связано с направлением и скоростью движения транспортного средства, например, возможный захват ловушкой нижней конечности, управляемость может быть оценена вероятностью того, что находящийся в опасности человек в состоянии вывести себя из опасного состояния, или был выведен из опасной ситуации другими людьми. При рассмотрении управляемости предполагается, что человек, находящийся в опасности, не должен быть знаком с работой устройства.

4 При анализе управляемости в ситуации с несколькими участниками дорожного движения ее оценка может быть основана на управляемости автомобиля с неисправным устройством и вероятных действиях других участников.

Таблица 3 — Классы управляемости

	Класс			
	С0	С1	С2	С3
Описание	Полностью управляемое	Легко управляемое	Обычно управляемое	Трудно управляемое или неконтролируемое

7.4.3.8 Класс С0 может быть использован для опасностей, не охваченных данным устройством, если они не влияют на безопасную эксплуатацию транспортного средства (например, некоторые системы помощи водителю). Класс С0 также может быть назначен, если существуют отдельные специальные документы, определяющие поведение при определенной опасности, и назначение С0 объясняется использованием существующего опыта по достаточной управляемости этой опасностью. Если опасности присваивается класс управляемости С0, то не требуется назначения УПБА.

Пример — Отдельным специальным актом является сертификация системы автомобиля с точным определением значений мощности или ускорения в случае отказа.

7.4.4 Определение значения УПБА и целей безопасности

7.4.4.1 Значение УПБА должно быть определено для каждого опасного события, используя параметры «тяжести последствий», «вероятности воздействия» и «управляемости» в соответствии с таблицей 4.

Примечания

1 Определены четыре значения УПБА: УПБА А, УПБА В, УПБА С и УПБА D, где значение УПБА, равное А, является самым низким значением уровня полноты безопасности автомобиля, а значение УПБА, равное D, — самым высоким.

2 В дополнение к этим четырем значениям УПБА классу QM (управление качеством) не назначается требование соответствия настоящему стандарту.

Таблица 4 — Определение УПБА

Классы тяжести последствий	Класс вероятности воздействия	Класс управляемости		
		С1	С2	С3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B

Окончание таблицы 4

Классы тяжести последствий	Класс вероятности воздействия	Класс управляемости		
		C1	C2	C3
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

7.4.4.2 Должно быть обеспечено, что выбранный уровень детализации списка эксплуатационных ситуаций не приведет к несоответствующему снижению УПБА соответствующих целей безопасности.

Примечание — Подробный список эксплуатационных ситуаций (см. 7.4.2.1.1) для одной опасности, связанных с состоянием автомобиля, дорожными условиями и условиями внешней среды, может привести к подробной классификации опасных событий. Это может облегчить оценку управляемости и тяжести последствий. Однако большое количество различных эксплуатационных ситуаций может привести к логически вытекающему сокращению соответствующих классов воздействия и, таким образом, к несоответствующему снижению значения УПБА соответствующих целей безопасности.

7.4.4.3 Для каждого опасного события должна быть определена цель безопасности со значением УПБА, оцениваемым при анализе рисков. Если определены похожие цели безопасности, то они могут быть объединены в одну цель безопасности.

Примечание — Цели безопасности являются требованиями безопасности самого высокого уровня для данного устройства. Они приводят к требованиям функциональной безопасности, необходимым для предотвращения необоснованного риска для каждого опасного события. Цели безопасности не выражаются через технологические решения, а формулируются в терминах функциональных задач.

7.4.4.4 Значение УПБА, определяемое для опасного события, должно быть назначено соответствующей цели безопасности. Если же цели безопасности объединяются в одну, в соответствии с 7.4.4.3, то такой цели безопасности должно быть назначено наибольшее из значений УПБА, объединяемых целей безопасности.

Примечание — Если объединяемые цели безопасности относятся к одной опасности в различных ситуациях, то значение УПБА, результирующей цели безопасности, должно быть наибольшим среди рассматриваемых целей безопасности любой из ситуаций.

7.4.4.5 Если цель безопасности может быть достигнута путем перехода к одному или нескольким безопасным состояниям или их поддержкой, то соответствующее(ие) безопасное(ые) состояние(я) должно быть специфицировано.

Примечание — Безопасные состояния рассматриваются в разделе 8.

Пример — Безопасными состояниями могут быть: отключено, заблокировано, стоящий автомобиль и поддержка функциональности в случае отказа в течение определенного времени.

7.4.4.6 Цели безопасности вместе с их атрибутами (значениями УПБА) должны быть специфицированы в соответствии с требованиями раздела 6 ИСО 26262-8.

Примечание — Цель безопасности может включать в себя такие параметры, как интервал сбоеустойчивости или физические характеристики (например, максимальный уровень нежелательного крутящего момента рулевого колеса, максимальный уровень нежелательного ускорения), если они имеют отношение к определению значения УПБА.

7.4.5 Верификация

7.4.5.1 Анализ опасностей, оценка рисков и цели безопасности должны быть верифицированы в соответствии с требованиями раздела 9 ИСО 26262-8, чтобы показать их:

а) полноту охвата ситуаций (7.4.2.1) и опасностей (7.4.2.2);

b) соответствие с определением устройства;

c) согласованность с соответствующим анализом опасностей и оценками рисков;

d) полноту охвата опасных событий; а также

e) согласованность назначенных значений УПБА с соответствующими опасными событиями.

Примечание — Верификационная оценка проверяет корректность и полноту результатов анализа опасностей и оценки рисков устройства, т. е. рассматриваемых ситуаций, опасностей и результатов оценки параметров (тяжести последствий, вероятности воздействий и управляемости). С другой стороны, оценка подтверждения результатов анализа опасностей и оценки рисков, выполняемая в соответствии с частью 2 настоящего стандарта, проверяет формально, что процедура анализа опасностей и оценки рисков соответствует требованиям раздела 7. Такая оценка подтверждения выполняется лицом или лицами из других отделов или организаций, которые не участвовали в разработке устройства.

7.5 Результаты работы

7.5.1 Анализ опасностей и оценки рисков

В результате выполнения требований 7.4.1.1—7.4.4.2.

7.5.2 Цели безопасности

В результате выполнения требований 7.4.4.3—7.4.4.6.

7.5.3 Протокол верификационной оценки анализа опасностей и оценки рисков и целей безопасности

В результате выполнения требований 7.4.5.

8 Концепция функциональной безопасности

8.1 Цель

Целью концепции функциональной безопасности является получение требований к функциональной безопасности из целей безопасности и их распределение по элементам предварительной архитектуры устройства или по внешним мерам.

8.2 Общие положения

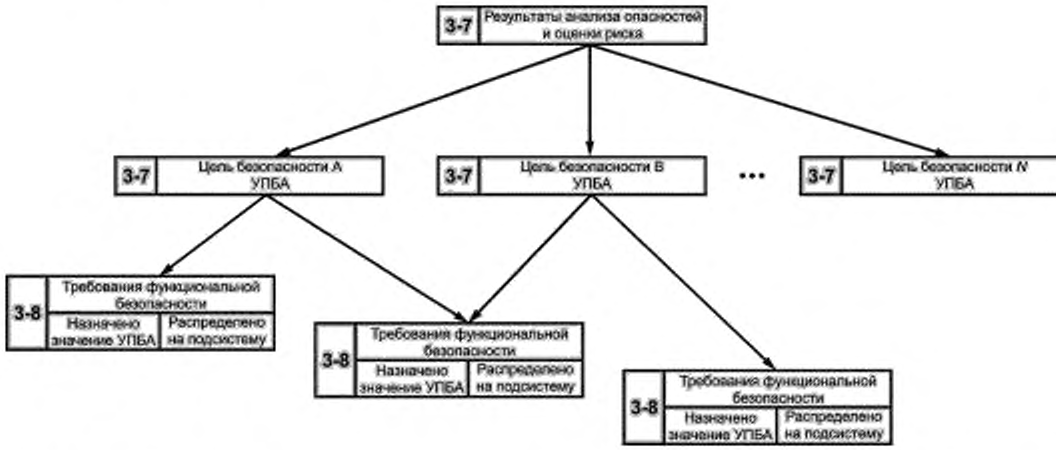
Для выполнения целей безопасности концепция функциональной безопасности должна содержать меры безопасности, в том числе механизмы безопасности, которые должны быть реализованы элементами архитектуры устройства и специфицированы в требованиях функциональной безопасности.

Концепция функциональной безопасности направлена на:

- обнаружение неисправностей и смягчение последствий отказов;
- обеспечение перехода в безопасное состояние;
- создание отказоустойчивых механизмов, в которых неисправность непосредственно не приводит к нарушению цели (целей) безопасности и которые поддерживают устройство в безопасном состоянии (с или без деградации);
- обнаружение неисправностей и предупреждение водителя для того, чтобы сократить время воздействия риска до приемлемого интервала (например, контрольная лампа о неправильной работе двигателя, лампа предупреждения о сбое ABS);
- применение арбитражной логики, чтобы выбрать наиболее подходящий запрос из нескольких запросов, генерируемых одновременно различными функциями.

На рисунке 2 показан иерархический подход, с помощью которого в результате анализа опасностей и оценки рисков определяются цели безопасности. Затем из целей безопасности формируются требования функциональной безопасности.

Структура и распределение требований к системе безопасности между соответствующими частями настоящего стандарта приведены на рисунке 3. Требования функциональной безопасности распределяются элементам предварительной архитектуры.



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

Рисунок 2 — Иерархия целей системы безопасности и требований функциональной безопасности

8.3 Входная информация

8.3.1 Предварительные требования

Следующая информация должна быть доступна:

- определение устройства в соответствии с требованиями 5.5;
- результаты анализа опасностей и оценки рисков в соответствии с требованиями 7.5.1;
- цели безопасности в соответствии с требованиями 7.5.2.

8.3.2 Дополнительная информация

Следующая информация может быть учтена:

- предположения о предварительной архитектуре (из внешнего источника).

8.4 Требования и рекомендации

8.4.1 Общие положения

Требования функциональной безопасности должны быть заданы в соответствии с требованиями раздела 6 ИСО 26262-8.

8.4.2 Вывод требований функциональной безопасности

8.4.2.1 Требования функциональной безопасности должны быть выведены из целей безопасности и безопасных состояний с учетом предположений о предварительной архитектуре.

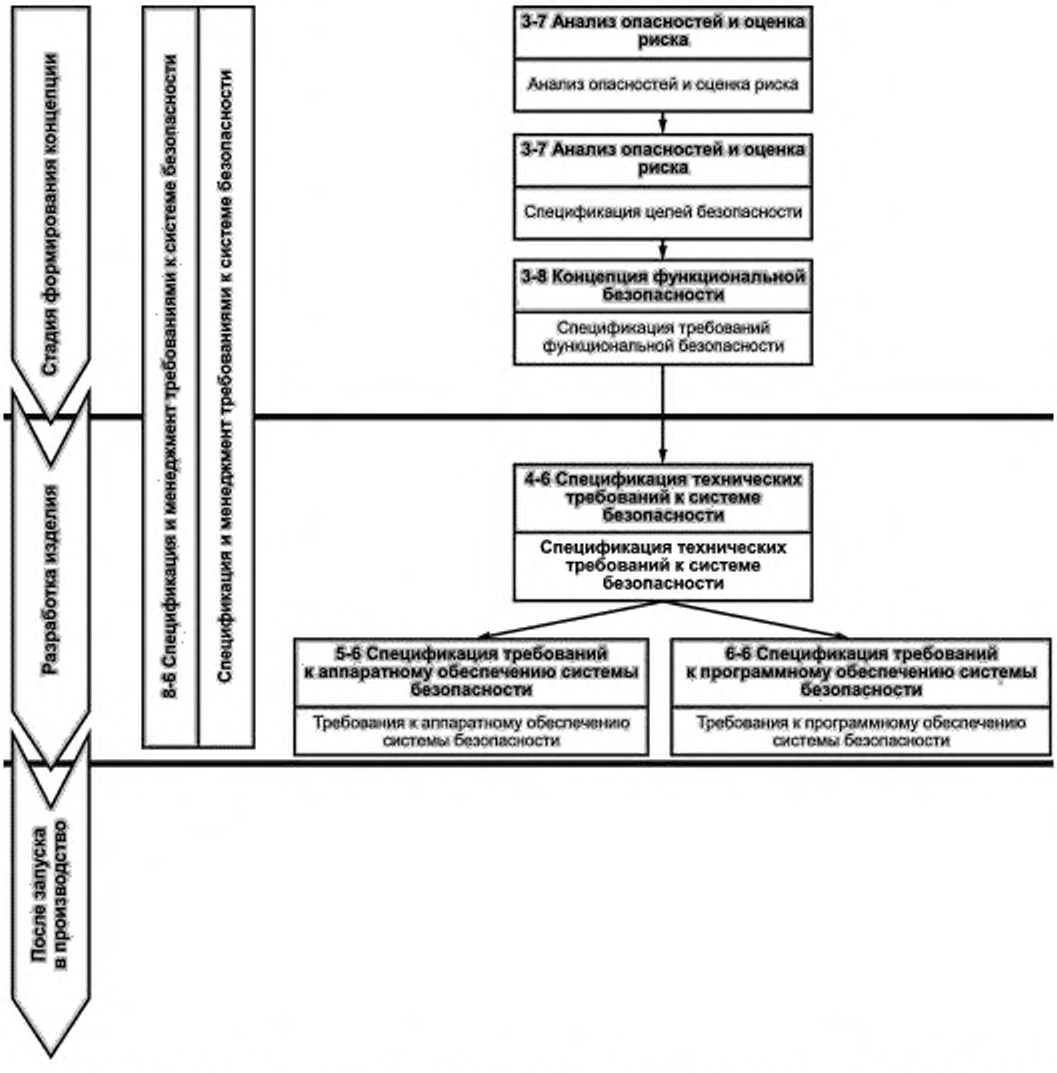
8.4.2.2 По крайней мере одно требование функциональной безопасности должно быть определено для каждой цели безопасности.

Примечание — Одно требование функциональной безопасности может быть применимым для нескольких целей безопасности.

8.4.2.3 Каждое требование функциональной безопасности должно быть определено с учетом следующего (если применимо):

a) режима работы;
b) интервала сбоеустойчивости;
c) безопасных состояний;
d) интервала работы в аварийном режиме;
e) функциональной избыточности (например, сбоеустойчивости).

Примечание — Эта деятельность может быть поддержана анализом безопасности (например, FMEA, FTA, HAZOP) для того, чтобы разработать полный набор эффективных требований функциональной безопасности.



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

Рисунок 3 — Структура требований к системе безопасности

8.4.2.4 Если безопасное состояние не может быть достигнуто путем перехода к нему за приемлемый интервал времени, то должен быть специфицирован аварийный режим.

Пример — Если безопасное состояние не может быть достигнуто путем немедленного отключения системы, то должен быть специфицирован подходящий аварийный режим.

8.4.2.5 Должна быть задана концепция предупреждения и постепенного снижения эффективности в виде требований функциональной безопасности.

Примечание — Переходы в и из безопасного состояния и условия для перехода (переход в безопасное состояние и восстановление из безопасного состояния) описаны в концепции предупреждения и постепенного снижения эффективности.

Примеры

1 При обнаружении неисправности и смягчении последствий отказа выполняется переход в безопасное состояние.

2 При обнаружении неисправности водителю выдается предупреждение для того, чтобы сократить время воздействия риска до приемлемого интервала (например, контрольная лампа о неправильной работе двигателя, лампа предупреждения о сбое ABS)

8.4.2.6 Если в соответствии с целями безопасности водителю или другим лицам, потенциально подвергающимся риску, делаются предложения о необходимых действиях, то следует, чтобы:

a) такие действия были определены в концепции функциональной безопасности и

b) соответствующие средства и элементы управления, доступные водителю или другим лицам, потенциально подвергающимся риску, были определены в концепции функциональной безопасности.

Примечание — Действия включают в себя те, для которых в ходе оценки управляемости было сформировано доверие, а также любые дальнейшие необходимые действия, принятые для выполнения целей безопасности после реализации требований безопасности.

Пример — Адаптивный круиз-контроль: для преодоления торможения водителю предлагается нажать на педаль акселератора.

Примечания

1 Может оказаться полезным анализ задач водителя при рассмотрении предотвращения перегрузки водителя, предотвращения неожиданности / паники / шока (потери возможности управления транспортным средством) водителя, и режима путаницы (неверное предположение о режиме работы).

2 Информация, специфицированная в концепции предупреждения и постепенного снижения эффективности и в необходимых действиях водителя и других лиц, потенциально подвергающихся риску, является исходной для руководства пользователя (см. 6.4.1 ИСО 26262-7).

8.4.3 Распределение требований функциональной безопасности

8.4.3.1 Требования функциональной безопасности должны быть распределены по элементам предположений о предварительной архитектуре.

Примечание — Вопросы резервирования и независимости могут быть проверены путем анализа зависимых отказов (см. раздел 7 ИСО 26262-9).

a) в ходе распределения значение УПБА и информация, приведенная в 8.4.2.3, должны быть унаследованы от соответствующей цели безопасности, или, если значение УПБА декомпозировано, то от более высокого уровня;

b) если несколько требований функциональной безопасности распределены одному элементу архитектуры, то такой элемент архитектуры должен быть разработан в соответствии с самым высоким для этих требований безопасности значением УПБА, если для предварительной архитектуры нельзя обосновать независимость или отсутствие влияния;

c) если устройство состоит более чем из одной системы, то требования функциональной безопасности для отдельных систем и их интерфейсов должны быть заданы с учетом предположений о предварительной архитектуре. Эти требования функциональной безопасности должны быть распределены по системам;

d) если при распределении требований функциональной безопасности выполняется декомпозиция значения УПБА, то она должна применяться в соответствии с требованиями раздела 5 ИСО 26262-9.

8.4.3.2 Если концепция функциональной безопасности предполагает использование элементов, основанных на других технологиях, то применяются следующие положения:

a) требования функциональной безопасности, реализуемые элементами, основанными на других технологиях, должны быть выведены и распределены по соответствующим элементам архитектуры;

b) должны быть заданы требования функциональной безопасности, касающиеся интерфейсов элементов, основанных на других технологиях;

c) реализация требований функциональной безопасности элементами, основанными на других технологиях, должна быть обеспечена путем принятия конкретных мер, требования к которым выходят за область применения настоящего стандарта;

d) для таких элементов не должны назначаться значения УПБА.

Примечание — Адекватность элементов, основанных на других технологиях, показывается в процессе подтверждения соответствия (см. ИСО 26262-4).

8.4.3.3 Если концепция функциональной безопасности предполагает использование внешних мер, то применяются следующие положения:

a) требования функциональной безопасности, реализуемые внешними мерами, должны быть выведены и сообщены;

b) должны быть заданы требования функциональной безопасности для интерфейсов с внешними мерами;

c) если внешние меры реализуются на основе одной или нескольких Э/Э систем, то требования функциональной безопасности должны определяться на основе настоящего стандарта;

d) выполнение требований функциональной безопасности внешними мерами должно быть гарантировано.

Примечание — Адекватность внешних мер показывается в процессе подтверждения соответствия (см. ИСО 26262-4).

8.4.4 Критерии подтверждения соответствия

8.4.4.1 Критерии принятия подтверждения соответствия безопасности устройства должны быть заданы на основе требований функциональной безопасности.

Примечание — О дополнительных требованиях к детализации критериев и список характеристик, необходимых для подтверждения соответствия, см. в пунктах 6.4.6.2 и 9.4.3.2 ИСО 26262-4.

8.4.5 Верификация концепции функциональной безопасности

8.4.5.1 Концепция функциональной безопасности должна быть верифицирована в соответствии с требованиями раздела 9 ИСО 26262-8, чтобы показать ее:

a) согласованность и соответствие целям безопасности и

b) способность смягчать или предотвращать опасные события.

Примечания

1 Верификация способности смягчать или предотвращать опасное событие на стадии формирования концепции может быть основана на тех же методах, которые используются для подтверждения соответствия. Результаты оценки могут указать на улучшение концепции. Однако необходимо иметь в виду, что основной задачей подтверждения соответствия безопасности, осуществляемого в соответствии с требованиями раздела 9 ИСО 26262-8, является создание устройства, разрабатываемого в соответствии с требованиями настоящего стандарта, а не исследования концепции (например, прототипов).

Пример — Способность смягчать или предотвращать опасное событие может быть оценена тестами, испытаниями или экспертом, используя прототипы, исследования, предметные тесты или моделирование.

2 Верификация способности смягчать или предотвращать опасное событие учитывает характеристики сбоя (например, временный или постоянный).

3 Для верификации может быть использовано подтверждение, основанное на прослеживаемости, например, если устройство соответствует требованиям функциональной безопасности, то это устройство соответствует целям безопасности, из которых были получены эти требования.

8.5 Результаты работы

8.5.1 Концепция функциональной безопасности

В результате выполнения требований 8.4.1—8.4.4.

8.5.2 Протокол верификации концепции функциональной безопасности

В результате выполнения требований 8.4.5.

Приложение А
(справочное)

Обзор и поток документов стадии формирования концепции

Таблица А.1 содержит обзор целей, предварительных требований и результатов работы стадии формирования концепции.

Таблица А.1 — Обзор стадии формирования концепции

Раздел	Цели	Предварительные требования	Результаты работы
5 Определение устройства	Первой целью настоящего раздела является определение и описание устройства, его зависимостей от и взаимодействие с внешней средой и другими устройствами. Второй целью является поддержка адекватного понимания этого устройства, чтобы могли быть выполнены соответствующие действия на последующих стадиях	Не задаются	5.5 Определение устройства
6 Начальное формирование жизненного цикла системы безопасности	Первая цель начального формирования жизненного цикла системы безопасности — установить различие между разработкой нового устройства и модификацией существующего устройства (см. рисунок 2 ИСО 26262-2). Вторая цель заключается в определении действий в процессах жизненного цикла системы безопасности (см. рисунок 2 ИСО 26262-2), которые будут выполняться в случае модификации	Определение устройства	6.5.1 Анализ влияния. 6.5.2 План по обеспечению безопасности (уточненный)
7 Анализ опасностей и оценка рисков	Целью анализа опасностей и оценки рисков является идентификация и классификация опасностей, которые могут привести к неправильному функционированию устройства, а также формулирование целей безопасности, связанных с предотвращением или смягчением последствий опасных событий, чтобы избежать необоснованный риск	Определение устройства	7.5.1 Анализ опасностей и оценка рисков. 7.5.2 Цели безопасности. 7.5.3 Протокол верификационной оценки анализа опасностей и оценки рисков и целей безопасности
8 Концепция функциональной безопасности	Целью концепции функциональной безопасности является получение требований к функциональной безопасности из целей безопасности и их распределение по элементам предварительной архитектуры устройства или по внешним мерам	Определение устройства. Анализ опасностей и оценка рисков. Цели безопасности	8.5.1 Концепция функциональной безопасности. 8.5.2 Протокол верификации концепции функциональной безопасности

Приложение В
(справочное)

Анализ опасностей и оценка рисков

В.1 Общие положения

В настоящем приложении представлен общий подход, реализуемый в методе анализа опасностей и оценки рисков. Примеры, приведенные в В.2 (тяжесть последствий), В.3 (вероятность воздействия) и В.4 (управляемость), являются демонстрационными и не являются исчерпывающими.

В рассматриваемом аналитическом подходе риск R описывается как функция F от частоты появления опасного события f, от способности предотвратить конкретный вред или ущерб путем своевременной реакции причастных лиц или управляемости C и от потенциальной тяжести последствий, полученного вреда или ущерба S:

$$R = F(f, C, S).$$

Частота появления опасного события f, в свою очередь, зависит от нескольких факторов. Одними из рассматриваемых факторов являются частота и длительность нахождения людей в ситуации, когда вышеупомянутое опасное событие может произойти. В настоящем стандарте используется более простая мера — вероятность сценария вождения, в котором может произойти опасное событие (называется — воздействие и обозначается E). Еще одним фактором является интенсивность отказов устройства, которые могут привести к опасному событию (частота отказов, λ). Частота отказов характеризуется опасными случайными отказами технических средств и систематическими ошибками, которые остались в системе:

$$f = E \times \lambda.$$

Метод анализа опасностей и оценки рисков используется для установления требований к устройству с целью предотвращения неоправданного риска.

Значения УПБА, полученные в результате анализа опасностей и оценки рисков, определяют минимальный набор требований к устройству, выполнение которых обеспечивает управление или снижение вероятности случайных отказов аппаратных средств, а также предотвращение систематических ошибок. Интенсивность отказов устройства не считается априорной (при оценке риска), поскольку неоправданный остаточный риск можно избежать путем реализации результирующих требований безопасности.

Подстадия анализа опасностей и оценки рисков состоит из трех представленных ниже шагов.

a) Анализ ситуации и идентификация опасности (см. 7.4.2). Целью анализа ситуации и идентификации опасностей является выявление случаев возможного непреднамеренного поведения устройства, которые могут привести к опасному событию. Деятельность, связанная с анализом ситуаций и идентификацией опасностей, требует четкого определения устройства, его функциональности и его границ. Она основана на знании поведения устройства, поэтому информация о детальном проекте устройства не обязательно должна быть известна.

Пример — Факторы, учитываемые при анализе ситуации и идентификации опасности, могут включать в себя:

- сценарии использования транспортного средства, например, вождение с высокой скоростью, вождение в городе, парковка, вождение во внедорожных условиях;

- условия внешней среды, например, сцепление с поверхностью дороги, боковой ветер;

- разумно предсказуемое правильное и неправильное использование водителем автомобиля; а также

- взаимодействие между действующими системами.

b) Классификация опасных событий (см. 7.4.3). Схема классификации опасности включает в себя определение степени тяжести последствий, вероятности воздействия и управляемости, связанных с опасностями событий устройства. Тяжесть последствий представляет собой оценку потенциального вреда в конкретной ситуации вождения, в то время как вероятность воздействия определяется соответствующей ситуацией. Управляемость оценивает, насколько легко или трудно для водителя или других участников дорожного движения избежать конкретный тип аварии в конкретной оперативной обстановке. Для каждой опасности, в зависимости от количества связанных с ней опасных событий, классификация приведет к одной или более комбинации из тяжести последствий, вероятности воздействия и управляемости.

c) Определение значения УПБА (см. 7.4.4). Определение необходимого уровня полноты безопасности автомобиля.

В.2 Примеры тяжести последствий

В.2.1 Общие положения

Возможные травмы в результате опасного события оцениваются для водителя, пассажиров и людей вокруг автомобиля или лиц, находящихся вблизи автомобиля, чтобы определить класс тяжести последствий для данной опасности. Затем, используя эту оценку, определяется соответствующий класс тяжести последствий, например, как показано в таблице В.1.

Таблица В.1 — Примеры классификации тяжести последствий

	Класс тяжести последствий (см. таблицу 1)			
	S0	S1	S2	S3
Ссылка на одиночные травмы (из шкалы УШП)	УШП 0 и с вероятностью менее 10 % УШП 1—6; Повреждения, которые не могут быть классифицированы как связанные с безопасностью	С вероятностью более 10 % УШП 1—6 (и не S2 и S3)	С вероятностью более 10 % УШП 3—6 (и не S3)	С вероятностью более 10 % УШП 5—6
Примеры	- Удары с объектами придорожной инфраструктуры. - Наезд на придорожные столбы, ограждения и т. д - Легкое столкновение. - Легкое повреждение при скользящем ударе. - Повреждение в процессе парковки. - Съезд с дороги без столкновения или опрокидывания	- Боковой удар с узким неподвижным объектом, например, столкновение с деревом (повреждение в зоне пассажира) с очень низкой скоростью. - Боковое столкновение с легковым автомобилем (например, повреждение в зоне салона автомобиля) с очень низкой скоростью. - Заднее/переднее столкновение с другим легковым автомобилем с очень низкой скоростью. - Столкновение с взаимным минимальным проникновением (10 %—20 %) транспортных средств. Переднее столкновение (например, в заднюю часть впереди идущего автомобиля, полуприцепа грузового автомобиля и т. п.) без повреждения пассажирской зоны	- Боковой удар с узким неподвижным объектом, например, столкновение с деревом (повреждение в зоне пассажира) с низкой скоростью. - Боковое столкновение с легковым автомобилем (например, повреждение в зоне салона автомобиля) с низкой скоростью. - Заднее/переднее столкновение с другим легковым автомобилем с низкой скоростью - Наезд на пешехода/велосипедиста при совершении поворота (на перекрестках и улицах города)	- Боковой удар с узким неподвижным объектом, например столкновение с деревом (повреждение в зоне пассажира) со средней скоростью. - Боковое столкновение с легковым автомобилем (например, повреждение в зоне салона автомобиля) со средней скоростью. - Заднее/переднее столкновение с другим легковым автомобилем со средней скоростью. - Наезд на пешехода/велосипедиста (например, на 2-х полосной дороге). - Переднее столкновение (например, в заднюю часть впереди идущего автомобиля полуприцепа грузового автомобиля и т. д.) с повреждением пассажирской зоны

В таблице В.1 приводятся примеры последствий, которые могут возникнуть для данной опасности и соответствующий класс тяжести для каждого последствия.

Из-за сложности аварий и многообразия возможных вариантов аварийных ситуаций примеры, приведенные в таблице В.1, представляют собой лишь приблизительную оценку последствий аварии. Они представляют собой ожидаемые значения, основанные на предыдущих результатах аварий. Поэтому из этих отдельных описаний не могут быть получены общезначимые (общепринятые) заключения.

Для определения распределения травм, которые можно ожидать для различных типов аварий, может быть использована статистика несчастных случаев.

В таблице В.1 упрощенная шкала повреждений (УШП) представляет собой классификацию классов травм, но только для единичных травм. Вместо УШП могут быть использованы другие классификации, такие как максимально упрощенная шкала повреждений (МУШП) и классификация тяжести повреждения (ISS).

Использование конкретной шкалы повреждений зависит от состояния медицинских исследований во время выполняемого анализа. Таким образом, целесообразность использования различных шкал травм, таких как УШП, ISS и NISS, может со временем меняться [2], [4] и [5].

В.2.2 Описание классов УШП

Для оценки тяжести последствий используется УШП, представляющая собой классификацию тяжести травм. Она создана Ассоциацией по развитию автомобильной медицины (AAAM) [2]. Метод, использующий УШП, создан для сопоставления степени повреждения на международном уровне. Шкала разделена на семь классов:

УШП 0. Нет повреждений.

УШП 1. Легкие повреждения, такие как поверхностные раны, боли в мышцах, повреждение мягких тканей шеи и т. д.

УШП 2. Умеренные повреждения, такие как глубокие раны, сотрясение с потерей сознания на 15 минут, переломы трубчатой кости без осложнений, переломы ребра без осложнений и т. д.

УШП 3. Тяжелые повреждения, не угрожающие жизни, такие как перелом основания черепа без травмы головного мозга, вывихи позвонков ниже четвертого шейного позвонка без повреждения спинного мозга, перелом более одного ребра без парадоксального дыхания и т. д.

УШП 4. Тяжелые повреждения (опасные для жизни, вероятное выживание), такие как сотрясение мозга с или без перелома основания черепа с потерей сознания на 12 часов, парадоксальное дыхание.

УШП 5. Критические повреждения (опасные для жизни, сомнительное выживание), такие как переломы позвонков ниже четвертого шейного позвонка с повреждением спинного мозга, разрывы кишечника, кардиальные разрывы, потеря сознания более чем на 12 часов, включая внутримозговое кровоизлияние.

УШП 6. Чрезвычайно критические или смертельные повреждения, такие как переломы шейного отдела позвоночника выше третьего шейного позвонка с повреждением спинного мозга, открытые раны полостей тела (грудная и брюшная полости) и т. д.

В.3 Примеры и объяснения вероятности воздействия

Оценка вероятности воздействия требует оценки сценариев, в которых оказывают влияние соответствующие факторы внешней среды, способствующие возникновению опасности. Сценарии, которые будут оцениваться, включают в себя широкий спектр процессов вождения или эксплуатационных ситуаций.

Эти оценки при обозначении опасных сценариев попадают в одну из пяти классификаций вероятности воздействия, которые составляют следующий набор. E0 (самый низкий уровень воздействия), E1, E2, E3 и E4 (самый высокий уровень воздействия).

Первый из них, E0, присваивается ситуациям, которые, хоть и выявлены в ходе анализа опасностей и рисков, считаются необычными или невероятными. После оценки опасности, связанные исключительно со сценариями уровня E0, могут быть исключены из дальнейшего анализа.

Пример — Типичные примеры сценариев уровня E0 включают в себя:

a) очень необычные или неосуществимые, одновременновозникающие обстоятельства, например,

- транспортное средство, попавшее в ДТП с участием другого транспортного средства, которое перевозит опасные материалы (необходимо заметить, что это не распространяется на транспортное средство, которое предназначено для перевозки такого материала);

- транспортное средство, попавшее в инцидент, в котором участвует самолет, совершающий посадку на шоссе;

b) стихийные бедствия, например, землетрясение, ураган, лесной пожар.

Остальные E1, E2, E3 и E4 уровни предназначены для ситуаций, которые могут стать опасными либо в зависимости от продолжительности ситуации (частичного совпадения во времени) или частоты возникновения ситуации.

Примечание — Классификация может зависеть, например, от географического положения или вида использования (см. 7.4.3.4).

Если воздействие ранжируется на основе продолжительности ситуации, то вероятность воздействия можно оценить с помощью отношения времени нахождения в рассматриваемой ситуации к общему времени работы (когда

включено зажигание). В особых случаях общее время работы может быть сроком службы транспортного средства (в том числе, когда включено зажигание). В таблице В.2 приведены примеры классификаций по длительностям этих ситуаций и ранжирование типичных воздействий в каждой из них.

Примечание — Опасность может быть связана с продолжительностью данного сценария (например, среднее время преодоления транспортных развязок), в то время как другая опасность может быть связана с частотой этого же сценария (например, частота повторного преодоления автомобилем транспортных развязок).

Кроме того, некоторые оценки воздействия могут быть определены более точно, если использовать частоту возникновения ситуации, связанной с вождением. В этих условиях уже существующие сбои системы приводят к опасному событию в течение короткого интервала после возникновения такой ситуации. Примеры таких дорожных ситуаций и ранжирование типичных воздействий на них приведены в таблице В.3.

Таблица В.2 — Классы вероятности воздействия в зависимости от продолжительности эксплуатационной ситуации

		Класс вероятности воздействия в эксплуатационных ситуациях			
		E1	E2	E3	E4
Продолжительность (% от среднего времени работы)		Не задано	< 1 % среднего времени работы	1 % — 10 % среднего времени работы	> 10 % среднего времени работы
Примеры	Дороги	—	- Горный перевал с необустроенным большим уклоном. - Пересечение проселочной дороги. - Шоссейный въезд на эстакаду. - Шоссейный съезд с эстакады	- Улица с односторонним движением	- Шоссе. - Второстепенная дорога. - Проселочная дорога
	Дорожное покрытие	—	- Снег и лед на дороге. - Скользкие листья на дороге	- Мокрая дорога	—
	Близлежащие элементы	- Потерянный груз или препятствие в полосе движения (на шоссе)	- В автомойке. - Приближение к концу пробки (на шоссе)	- В туннеле. - Пробки на дорогах	—
	Автомобиль в стационарном состоянии	- Автомобиль во время запуска от внешнего источника. - В ремонтном гараже (на катковом стенде)	- С трейлером на прицепе. - С багажником на крыше. - Транспортное средство на заправке. - В ремонтном гараже (во время диагностики или ремонта. - На подъемнике	- Автомобиль на уклоне (удержание на уклоне)	—
	Маневр	- Движение под уклон с выключенным двигателем (на перевале)	- Движение задним ходом (с парковки). - Движение задним ходом (по улице города). - Обгон. - Парковка (со спящим человеком в автомобиле). - Парковка (с трейлером на прицепе)	- Интенсивное движение (режим старт стоп)	- Ускорение. - Замедление. - Выполнение поворота (руление). - Парковка (на стоянке). - Перестроение (на улице города). - Остановка у светофора (на улице города). - Перестроение (на шоссе)
	Обзор (Видимость)	—	—	- Неосвещенные ночью дороги	—

Таблица В.3 — Классы вероятности воздействия в зависимости от частоты эксплуатационных ситуаций

		Класс вероятности воздействия в эксплуатационных ситуациях (см. таблицу 2)			
		E1	E2	E3	E4
Частота ситуаций		Происходит реже, чем один раз в год для большинства водителей	Происходит несколько раз в год для большинства водителей	Происходит раз в месяц или чаще для среднестатистического водителя	Происходит во время почти каждой поездки в среднем
Примеры	Дороги	—	- Горный перевал с необустроенным большим уклоном	—	—
	Дорожное покрытие	—	- Снег и лед на дороге	- Мокрая дорога	—
	Близлежащие элементы			- В туннеле. - В автомойке. - Пробки на дорогах	—
	Автомобиль в стационарном состоянии	- Автомобиль остановился и требует перезапуска двигателя (на железнодорожном переезде). - Автомобиль на буксире. - Автомобиль во время запуска от внешнего источника	- С трейлером на прицепе. - С багажником на крыше	- Транспортное средство на заправке. - Автомобиль на уклоне (удержание на уклоне)	—
	Маневр		- Маневр уклонения, с отклонением от желаемого пути	- Обгон	- Трогание с места. - Механическое переключение передачи. - Ускорение. - Замедление. - Выполнение поворота (руление). - Движение по показаниям приборов. - Маневрирование автомобиля в парковочное положение. - Движение задним ходом

Дорожная ситуация характеризуется как продолжительностью, так и частотой, например вождение автомобиля на автостоянке. В таком случае примеры, приведенные в таблицах В.2 и В.3, не могут привести к одинаковой категории воздействия, поэтому выбирается наиболее подходящий класс вероятности воздействия для анализа рассматриваемого сценария вождения.

Если период времени, в котором отказ остается скрытым, сопоставим с периодом времени, в течение которого может произойти опасное событие, то для оценки вероятности воздействия рассматривают этот период времени. Обычно это касается устройств, которые должны действовать по запросу, например, система управления подушками безопасности.

В этом случае вероятность воздействия оценивается как $\sigma \times T$, где σ является частотой возникновения опасных событий и T является длительностью временного периода, в течение которого отказ не воспринимается (возможно, срок службы автомобиля). Это приближение $\sigma \times T$ справедливо, если его значение мало.

Примечание — Что касается продолжительности рассматриваемого отказа, то следует отметить, что анализ опасностей и оценка рисков не учитывает механизмов безопасности, являющихся частью устройства (см. 7.4.1.2).

B.4 Примеры управляемости (возможности избежать вреда)

Для определения класса управляемости для данной опасности необходимо оценить вероятность того, что среднестатистический водитель сможет сохранить или восстановить контроль над транспортным средством при появлении данной опасности.

Такая оценка вероятности включает рассмотрение вероятности того, что среднестатистические водители смогут сохранить или восстановить контроль над транспортным средством, если опасность должна была произойти, или вероятности того, что люди, попавшие в ситуацию или находящиеся в непосредственной близости от нее, будут способствовать тому, чтобы предотвратить опасность в результате своих действий. Это соображение основано на предположениях о необходимости управления своими действиями для лиц, участвующих в опасных сценариях для сохранения или восстановления контроля над ситуацией, а также для поведения среднестатистического водителя, управляющего автомобилем (которое может быть связано с потенциальным кругом покупателей, возрастом физического лица, координацией глаз-рука, опытом вождения, культурой, и т. д.).

Примечание — На оценку управляемости может влиять ряд факторов, в том числе культурный фон аналитиков, потенциальный круг покупателей транспортных средств или профили водителя для потенциального круга покупателей.

В таблице B.4 приведены примеры дорожных ситуаций, в которых введены сбои, и предположения о соответствующем управлении поведением, которое позволило бы избежать вреда. Эти ситуации отображаются в ранжировании управляемости посредством введения уровней 90 % и 99 % для оценки управляемости участников.

Таблица B.4 — Примеры возможной управляемости опасными событиями для водителей или лиц, потенциально подвергающихся риску

Факторы и сценарии вождения		Классы управляемости (см. таблицу 3)			
		C0	C1	C2	C3
		Полная контролируемость	99 % или более всех водителей или других участников дорожного движения, как правило, в состоянии избежать вреда	90 % или более всех водителей или других участников дорожного движения, как правило, в состоянии избежать вреда	Менее 90 % всех водителей или других участников дорожного движения, как правило, в состоянии или едва могут избежать вреда
Примеры	Ситуации, которые считаются отвлекающими	Поддерживать намеченный путь вождения	—	—	—
	Неожиданное увеличение громкости радио	Поддерживать намеченный путь вождения	—	—	—
	Предупреждение — низкий уровень газа	Поддерживать намеченный путь вождения	—	—	—
	Недоступность системы оказания помощи водителю	Поддерживать намеченный путь вождения	—	—	—
	Неисправность регулировки положения сиденья во время движения	—	Торможение для замедления/остановки транспортного средства	—	—
	Заблокированная рулевая колонка при запуске автомобиля	—	Торможение для замедления/остановки транспортного средства	—	—

Продолжение таблицы В.4

Факторы и сценарии вождения		Классы управляемости (см. таблицу 3)			
		C0	C1	C2	C3
		Полная контролируемость	99 % или более всех водителей или других участников дорожного движения, как правило, в состоянии избежать вреда	90 % или более всех водителей или других участников дорожного движения, как правило, в состоянии избежать вреда	Менее 90 % всех водителей или других участников дорожного движения, как правило, в состоянии или едва могут избежать вреда
Примеры	Выход из строя ABS во время экстренного торможения	—	—	Поддерживать намеченный путь вождения	—
	Сбой в фарах при вождении ночью на средней/высокой скорости на неосвещенной дороге	—	—	Свернуть на обочину и/или затормозить, чтобы остановиться	—
	Неисправность двигателя при высоких боковых ускорениях (выезд из автострады)	—	—	Поддерживать намеченный путь вождения	—
	Отказ ABS при торможении на поверхности с низким коэффициентом трения дороги во время выполнения поворота	—	—	—	Поддерживать намеченный путь вождения, остаться в полосе
	Отказ тормозов	—	—	—	Тормозить для замедления/ остановки транспортного средства
	Неправильный угол поворота при высокой угловой скорости на средней или высокой скорости движения автомобиля (изменение угла поворота рулевого колеса не соответствуют намерению водителя)	—	—	—	Поддерживать намеченный путь вождения, остаться в полосе
	Неисправность механизма срабатывания подушки безопасности водителя при движении на высокой скорости	—	—	—	Поддерживать намеченный путь вождения, остаться в полосе. Тормозить для замедления/ остановки транспортного средства

Окончание таблицы В.4

Примечания

1 Для С2 возможный сценарий испытаний, выполненный в соответствии с проектом RESPONSE 3 [3], принят как адекватный: «Практический опыт тестирования показал, что 20 действительных наборов данных на сценарий могут обеспечить базовый показатель обоснованности». Если каждый из 20 наборов данных удовлетворяет критериям прохождения теста, то уровень управляемости со значением 85 % (с уровнем доверия 95 %, который, как правило, принимается для тестирования человеческих факторов) может быть обеспечен. Это является надлежащим доказательством обоснования оценки С2.

2 Для С1 проверка, обеспечивающая обоснование, что 99 % водителей «прошли» тест на конкретном сценарии трафика, может быть невыполнимой, потому что необходимо огромное количество испытуемых для соответствующего доказательства такого обоснования.

3 Поскольку никакая управляемость не принята для категории С3, то нет необходимости иметь соответствующее доказательство обоснования для такой классификации.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 26262-1:2011	—	*
ИСО 26262-2:2011	—	*
ИСО 26262-4:2011	—	*
ИСО 26262-5:2011	—	*
ИСО 26262-6:2011	—	*
ИСО 26262-7:2011	—	*
ИСО 26262-8:2011	—	*
ИСО 26262-9:2011	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Библиография

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

[2] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at gost.e-ecolog.ru gost.e-ecolog.ru

[3] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006

[4] BAKER, S.P., O'NEILL, B., HADDON, W., LONG, W.B., The injury severity score: a method for describing patients with multiple injuries and evaluating emergency care, The Journal of Trauma, Vol. 14, No. 3, 1974

[5] BALOGH, Z., OFFNER, P.J., MOORE, E.E., BIFFL, W.L., NISS predicts post injury multiple organ failure better than ISS, The Journal of Trauma, Vol. 48, No. 4, 2000

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

Ключевые слова: функциональная безопасность; жизненный цикл систем; транспортные средства; концепция функциональной безопасности; стадии жизненного цикла; стадия формирования концепции; определение устройства безопасности; анализ опасностей и оценка рисков

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

Сдано в набор 09.03.2016. Подписано в печать 24.03.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,30. Тираж 32 экз. Зак. 843.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru