ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 26262-9— 2014

ДОРОЖНЫЕ 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)
(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. № 519-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 26262-9:2011 «Дорожные 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»).

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.

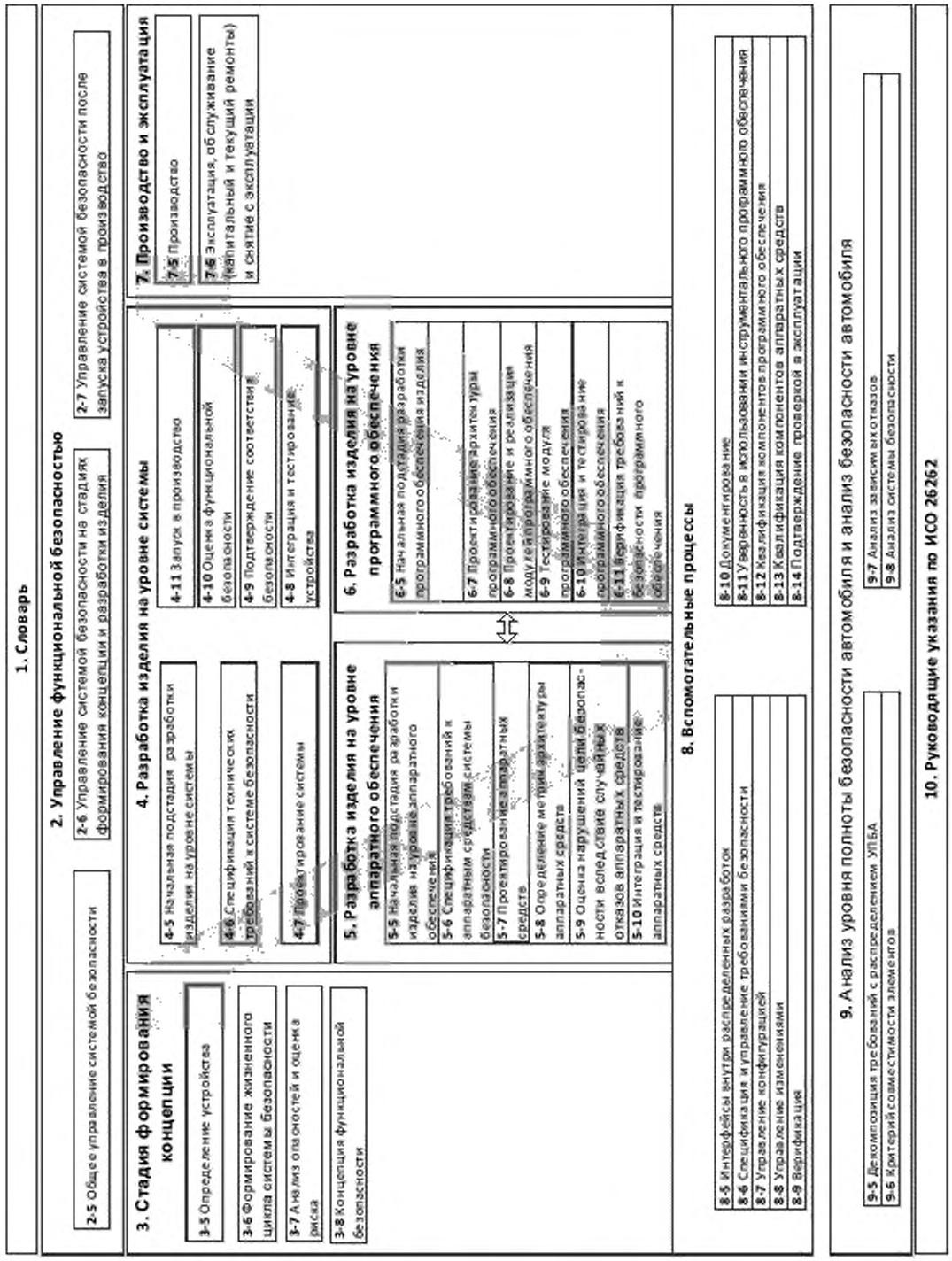


Рисунок 1 – Общая структура ИСО 26262

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Часть 9

Анализ уровня полноты безопасности автомобиля и анализ безопасности автомобиля

Road vehicles – Functional safety – Part 9: Automotive Safety Integrity Level-oriented and safety-oriented analyses

Дата введения — 2015—05—01

1 Область применения

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

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

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

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

Настоящий стандарт устанавливает требования к анализу уровня полноты безопасности автомобиля и анализу безопасности автомобиля, в том числе к:

- декомпозиции требований с распределением УПБА;
- критериям совместимости элементов;
- анализу зависимых отказов;
- анализу 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)

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 26262-4:2011 Дорожно-транспортные средства. Функциональная безопасность. Часть 4. Разработка изделия на уровне системы (ISO 26262-4:2011, Road vehicles – Functional safety – Part 4:

Издание официальное

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

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

3 Термины, определения и сокращения

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

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

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 настоящего стандарта 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 Декомпозиция требований с распределением УПБА

5.1 Цель

В данном разделе установлены правила и руководящие указания для декомпозиции требований к системе безопасности на избыточные требования для обеспечения заданных значений УПБА на следующем уровне детализации.

5.2 Общие положения

Определение значений УПБА целей безопасности разрабатываемого устройства выполняется по всему процессу разработки устройства. Исходя из целей безопасности, требования к системе безопасности распределяются и уточняются в процессе стадий разработки. Значение УПБА как атрибут цели безопасности наследуется каждым последующим требованием безопасности. Функциональные и технические требования безопасности распределяются элементам архитектуры, начиная с предварительных предположений по архитектуре и заканчивая элементами аппаратных средств и программного обеспечения.

Метод обеспечения заданного значения УПБА в процессе проектирования называется «декомпозиция УПБА». В процессе распределения требований можно получить преимущество из архитектурных решений, включающих достаточно независимые архитектурные элементы, которые дают возможность:

- с избыточностью реализовать требования безопасности с помощью этих независимых элементов архитектуры и
- назначить, по возможности, более низкое значение УПБА полученным в результате декомпозиции требованиям безопасности.

Если элементы архитектуры не являются достаточно независимыми, то избыточные требования и элементы архитектуры наследуют исходное значение УПБА.

Примечания

1 Декомпозиция значения УПБА является средством обеспечения заданных значений УПБА, которое может быть применено к функциональным, техническим требованиям безопасности, а также к требованиям безопасности аппаратных средств или программного обеспечения устройства или элемента.

2 Основное правило применения декомпозиции УПБА требует, чтобы требования к безопасности, распределяемые элементам архитектуры, которые являются достаточно независимыми, были избыточными.

3 В случае использования однородной избыточности (например, дублирующее устройство или дублирующее программное обеспечение) и при рассмотрении систематических отказов аппаратных средств и программного обеспечения значение УПБА не может быть уменьшено, пока анализ зависимости отказов не предоставит доказательство того, что они достаточно независимы или, что возможная общая причина приведет к безопасному состоянию. Таким образом, однородная избыточность в общем случае не является достаточной для снижения значения УПБА из-за отсутствия независимости между элементами.

4 В общем случае декомпозиция значения УПБА не распространяется на элементы, обеспечивающие выбор или переключение канала в проектах с многоканальной архитектурой.

В общем случае декомпозиция значения УПБА позволяет распределить значение УПБА требования к системе безопасности между несколькими элементами, которые обеспечивают соответствие этому требованию к безопасности и реализуют ту же цель безопасности. Декомпозиция значения УПБА между заданной функциональностью и ее соответствующим механизмом обеспечения безопасности допускается при определенных условиях (см. 5.4.7).

Конкретные требования к случайным отказам аппаратных средств, в том числе к оценке метрик архитектуры аппаратных средств и оценке нарушения цели безопасности из-за случайных отказов аппаратных средств (см. ИСО 26262-5) остаются неизменными при декомпозиции значения УПБА.

5.3 Входная информация

5.3.1 Предварительные требования

Необходима следующая информация:

- требования к безопасности на уровне, на котором должна применяться декомпозиция УПБА: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 8.5.1 ИСО 26262-3, или 6.5.1 ИСО 26262-4, или 6.5.1 ИСО 26262-5, или 6.5.1 ИСО 26262-6, и
- информация об архитектуре на уровне, на котором должна применяться декомпозиция УПБА: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 7.5.2 ИСО 26262-4, или 7.5.1 ИСО 26262-5, или 7.5.1 ИСО 26262-6.

5.3.2 Дополнительная информация

Следующая информация может быть учтена:

- определение устройства (см. 5.5 ИСО 26262-3);
- цели безопасности (см. 7.5.2 ИСО 26262-3).

5.4 Требования и рекомендации

5.4.1 Если применяется декомпозиция значения УПБА, то должны соблюдаться все требования, содержащиеся в настоящем разделе.

5.4.2 Декомпозиция значения УПБА должна осуществляться отдельно для каждого исходного требования к безопасности.

Примечание – В результате декомпозиций значений УПБА различных исходных требований к безопасности некоторые из этих требований могут быть распределены одним и тем же независимым элементам.

5.4.3 Исходные требования к безопасности должны быть декомпозированы на избыточные требования к безопасности, реализуемые достаточно независимыми элементами.

5.4.4 Каждое полученное в результате декомпозиции требование к безопасности само по себе должно соответствовать исходному требованию безопасности.

Примечание – Данное требование обеспечивает избыточность по определению.

5.4.5 Требования к оценке метрик архитектуры аппаратных средств и оценке нарушений целей безопасности из-за случайных отказов аппаратных средств должны оставаться неизменными при декомпозиции значения УПБА в соответствии с требованиями ИСО 26262-5.

5.4.6 Если декомпозиция значения УПБА применяется для программного обеспечения, то на

уровне системы должна быть проверена достаточная независимость между элементами, реализующими декомпозируемые требования, а также должны быть предприняты соответствующие меры на уровне программного обеспечения, уровне аппаратных средств или уровне системы для достижения такой независимости.

5.4.7 Если декомпозиция значения УПБА исходного требования к безопасности приводит при распределении декомпозируемых требований к целевой функциональности и соответствующему механизму безопасности, то:

а) соответствующему механизму безопасности должно быть назначено наибольшее декомпозируемое значение УПБА.

Примечание – В общем случае механизмы безопасности имеют более низкую сложность и меньший размер, чем механизмы, реализующие целевую функциональность;

б) требование к безопасности должно быть распределено целевой функциональности и реализовано применением соответствующего декомпозируемого значения УПБА.

Примечание – Если выбрана схема декомпозиции УПБА x(x) + QM(x), то QM(x) означает, что системы менеджмента качества может быть достаточно для разработки элемента(ов), которые реализуют требование безопасности, распределенное целевой функциональности. QM(x) также означает, что система менеджмента качества может обеспечить обоснование независимости между целевой функциональностью и механизмом безопасности.

5.4.8 Если нарушение исходного требования безопасности не может быть предотвращено путем отключения элемента, то должна быть показана соответствующая возможность использования достаточно независимых элементов для реализации декомпозируемых требований безопасности.

5.4.9 Если декомпозируется значение УПБА требования безопасности, то:

a) декомпозиция значения УПБА должна применяться в соответствии с требованиями 5.4.10;

b) декомпозиция значения УПБА может быть применена более одного раза;

c) каждое полученное в результате декомпозиции значение УПБА должны быть помечено путем задания в скобках значения УПБА цели безопасности.

Пример – Если требование со значением УПБА, равным D, декомпозируется на одно требование со значением УПБА, равным C, и одно требование со значением УПБА, равным A, то они записываются как УПБА C(D) и УПБА A(D). Если требование со значением УПБА, равным C(D), декомпозируется далее на одно требование со значением УПБА, равным B, и одно требование со значением УПБА, равным A, то они также записываются в соответствии со значением УПБА цели безопасности как УПБА B(D) и УПБА A(D).

5.4.10 Для каждого значения УПБА требования безопасности до его декомпозиции (как показано на рисунке 2) может быть выбрана одна из следующих описанных ниже схем декомпозиции, либо может быть использована схема с наиболее высокими значениями УПБА.

Примечание – Шаг от одного уровня выбранной схемы декомпозиции к следующему, более низкому, уровню определяет одну декомпозицию значения УПБА.

a) Требование со значением УПБА, равным D, может быть декомпозировано по одной из следующих схем:

1) одно требование со значением УПБА, равным C(D), и одно требование со значением УПБА, равным A(D); или

2) одно требование со значением УПБА, равным B(D), и одно требование со значением УПБА, равным B(D); или

3) одно требование со значением УПБА, равным D(D), и одно требование со значением УПБА, равным QM (D).

b) Требование со значением УПБА, равным C, может быть декомпозировано по одной из следующих схем:

1) одно требование со значением УПБА, равным B(C), и одно требование со значением УПБА, равным A(C); или

2) одно требование со значением УПБА, равным C(C), и одно требование со значением УПБА, равным QM(C).

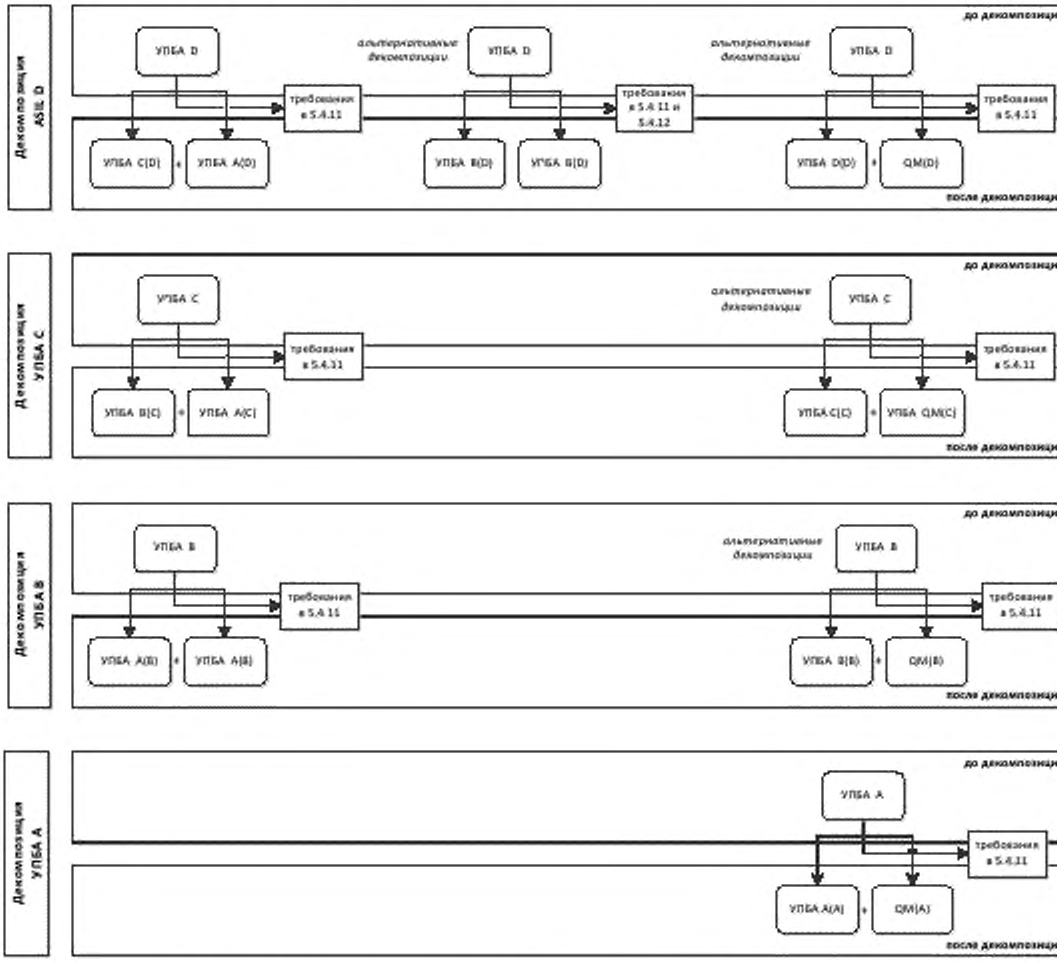
c) Требование со значением УПБА, равным B, может быть декомпозировано по одной из следующих схем:

1) одно требование со значением УПБА, равным A(B), и одно требование со значением УПБА, равным A(B); или

2) одно требование со значением УПБА, равным B(B), и одно требование со значением УПБА,

равным QM(B).

d) Требование со значением УПБА, равным A, не может быть далее декомпозировано, за исключением одного случая, при необходимости: одно требование со значением УПБА, равным A(A), и одно требование со значением УПБА, равным QM(A).



Пример – Случаи, описанные в 5.4.7, где QM назначается целевой функциональности и значение УПБА, равное исходному значению УПБА, назначается связанному с ней механизму безопасности, приведены в правой колонке.

Примечание – Верхние блоки каждого шага декомпозиции содержат значения УПБА до декомпозиции.

Рисунок 2 – Схемы декомпозиции УПБА

5.4.11 При использовании любой схемы декомпозиции, приведенной в 5.4.10:

a) должны применяться меры подтверждения соответствия требованиям 6.4.7 ИСО 26262-2 в соответствии со значением УПБА цели безопасности;

b) должны быть подготовлены доказательства достаточной независимости элементов после декомпозиции.

Примечание – Элементы являются достаточно независимыми, если анализ зависимости отказов (см. раздел 7) не находит причину зависимости отказов, которые могут привести к нарушению требования безопасности до его декомпозиции, или если каждая идентифицируемая причина зависимости отказов

контролируется адекватной мерой безопасности в соответствии со значением УПБА цели безопасности.

5.4.12 Если используется схема декомпозиции требования со значением УПБА, равным D, приведенная в перечислении 2) перечисления а) п. 5.4.10, то:

а) декомпозируемые требования безопасности должны быть специфицированы в соответствии с требованиями раздела 6 ИСО 26262-8 для значения УПБА, равного С.

Примечание – Более формализованная нотация, необходимая для значения УПБА, равного С, по сравнению со значением УПБА, равным В, повышает возможность избежать систематических отказов и уменьшает зависимость между двумя реализациями со значением УПБА, равным B(D);

b) если же для разработки декомпозируемых элементов используется одинаковое инструментальное программное обеспечение, то такое инструментальное программное обеспечение должно рассматриваться как инструментальное программное обеспечение для разработки устройств или элементов со значением УПБА, равным D, в соответствии с уверенностью в использовании инструментального программного обеспечения, рассмотренной в ИСО 26262-8.

5.4.13 Разработка декомпозируемых элементов на уровне системы и на уровне программного обеспечения осуществляется, как минимум, в соответствии с требованиями к УПБА (после декомпозиции), представленными в ИСО 26262-4 и ИСО 26262-6. Разработка декомпозируемых элементов на уровне аппаратных средств осуществляется, как минимум, в соответствии с требованиями к УПБА (после декомпозиции), представленными в ИСО 26262-5, за исключением оценки метрик архитектуры аппаратных средств и оценки нарушений цели безопасности, связанных со случайными отказами аппаратных средств (см. п. 5.4.5).

5.4.14 На каждом уровне процесса проектирования, на котором выполняется декомпозиция, применяются соответствующие действия по интеграции декомпозируемых элементов и последующие действия в соответствии с требованиями к УПБА до декомпозиции.

5.5 Результаты работы

5.5.1 Обновление информации об архитектуре

В результате выполнения требований 5.4.

5.5.2 Обновление значения УПБА как атрибута требований и элементов системы безопасности

В результате выполнения требований 5.4.

6 Критерии совместимости элементов

6.1 Цель

Настоящий раздел устанавливает критерии совместимости внутри одного элемента:

– связанных с безопасностью подэлементов с подэлементами, для которых значение УПБА не назначено, и

– связанных с безопасностью подэлементов, которые имеют различные назначенные значения УПБА.

6.2 Общие положения

По умолчанию, когда элемент состоит из нескольких подэлементов, каждый из них разрабатывается в соответствии с мерами, соответствующими самому высокому значению УПБА, применяемому к элементу, то есть самому высокому значению УПБА требований безопасности, распределенному элементу (см. 7.4.2.3 ИСО 26262-4).

В случае совместимости подэлементов, которые имеют различные назначенные значения УПБА, или совместимости подэлементов, для которых значение УПБА не назначено, со связанными с безопасностью подэлементами, может оказаться выгодно избежать повышения значения УПБА для некоторых из них до значения УПБА элемента. Для этого данный раздел представляет собой руководство по определению значения УПБА подэлементов элемента. Данный раздел основан на анализе влияния подэлемента на другие подэлементы элемента.

Влиянием считается наличие каскадных отказов от подэлемента, для которого значение УПБА не назначено или назначено меньшее значение УПБА, к подэлементу с более высоким назначенным значением УПБА, приводящее к нарушению требования безопасности элемента (см. определения 2.13 и 2.49 ИСО 26262-1).

При определении значения УПБА подэлементов элемента, обоснование отсутствия влияния формируется в результате анализа зависимых отказов, выполненного для каскадных отказов (см. раздел 7).

6.3 Входная информация

6.3.1 Предварительные требования

Необходима следующая информация:

- требования безопасности на уровне, на котором должен быть выполнен анализ: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 8.5.1 ИСО 26262-3, или 6.5.1 ИСО 26262-4, или 6.5.1 ИСО 26262-5, или 6.5.1 ИСО 26262-6; и
- информация об архитектуре элемента на уровне, на котором должен быть выполнен анализ: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 7.5.2 ИСО 26262-4, или 7.5.1 ИСО 26262-5, или 7.5.1 ИСО 26262-6.

6.3.2 Дополнительная информация

Не используется.

6.4 Требования и рекомендации

6.4.1 Требования данного раздела могут быть применены на любом уточняющем шаге в процессе проектирования параллельно с распределением требований безопасности элементам и подэлементам архитектуры, обычно на подстадиях проектирования системы или проектирования аппаратных средств, или проектирования архитектуры программного обеспечения в соответствии с требованиями ИСО 26262-4, или ИСО 26262-5, или ИСО 26262-6.

6.4.2 Требования безопасности должны быть распределены подэлементам элемента до применения требований данного раздела.

Примечание – Распределение требований безопасности по подэлементам приводит к появлению связанных с безопасностью подэлементов и подэлементов, которым значение УПБА не назначено.

6.4.3 При анализе элементов следует учитывать:

a) каждое требование безопасности, распределенное элементу; и

b) каждый подэлемент, который является частью элемента.

6.4.4 Если подэлемент, для которого значение УПБА не назначено, и связанные с безопасностью подэлементы работают вместе в одном элементе, то подэлемент, для которого значение УПБА не назначено, должен рассматриваться только как QM подэлемент, если имеется доказательство, что он не может нарушить прямо или косвенно любое из требований безопасности, распределенных элементу, то есть он не может повлиять на любой связанный с безопасностью подэлемент элемента.

Примечания

1 Это означает, что каскадные отказы от такого подэлемента к связанным с безопасностью элементам отсутствуют.

2 Это может быть достигнуто предупредительными мерами по обеспечению безопасности при проектировании, такими как анализ потока данных и потока управления для программного обеспечения или сигналов ввода / вывода и линий передачи сигналов управления для аппаратных средств.

В противном случае такому подэлементу должно быть назначено самое высокое из значений УПБА вместе работающих связанных с безопасностью подэлементов, у которых обоснование отсутствия влияния не имеется.

6.4.5 Если связанные с безопасностью подэлементы с различными значениями УПБА, в том числе и QM(x) (см. 5.4.10), работают вместе в одном элементе, то подэлемент будет рассматриваться как подэлемент с более низким назначенным ему значением УПБА, только если имеется доказательство, что для каждого требования безопасности, распределенного этому элементу, этот подэлемент не может оказывать влияние на любой подэлемент с более высоким назначенным ему значением УПБА. В противном случае такому подэлементу должно быть назначено самое высокое из значений УПБА, работающих вместе, связанных с безопасностью подэлементов, у которых не имеется обоснование отсутствия влияния.

6.5 Результаты работы

6.5.1 Обновление значения УПБА как атрибута подэлементов элементов

В результате выполнения требований 6.4.

7 Анализ зависимых отказов

7.1 Цель

Анализ зависимых отказов направлен на выявление отдельных событий или отдельных оснований, которые могли бы не учитывать или считать необоснованной требуемую независимость или отсутствие влияния между данными элементами и таким образом нарушить требование безопасности или цель безопасности.

7.2 Общие положения

Анализ зависимых отказов рассматривает следующие характеристики архитектуры:

- схожесть и несхожесть элементов, реализующих резервирование;
- различные функции, реализуемые одинаковыми элементами программного обеспечения или аппаратных средств;
- функции и их соответствующие механизмы безопасности;
- разбиения функций или элементов программного обеспечения;
- физическое расстояние между элементами аппаратных средств с установленными или неустановленными защитными экранами;
- общие внешние ресурсы.

В соответствии с определениями, приведенными в ИСО 26262-1, независимость может быть нарушена отказами по общей причине и каскадными отказами, в то время как отсутствие влияния может быть нарушено только каскадными отказами.

Пример – Электромагнитное поле с высокой напряженностью, которое вызывает отказ различных электронных устройств, что в известном смысле зависит от их конструкции и применения, является примером отказа по общей причине. Необъективная информация о скорости автомобиля, что влияет на поведение одной или нескольких функций автомобиля, является примером каскадных сбоев.

Зависимые отказы могут проявляться одновременно либо в достаточно короткий промежуток времени, что приводит к эффекту одновременных отказов.

Пример – Монитор, предназначенный для обнаружения аномального поведения функции, может быть выведен из строя за некоторое время до отказа контролируемой функции, если и монитор и контролируемая функция подвергаются влиянию одного и того же события или причины.

7.3 Входная информация

7.3.1 Предварительные требования

Необходима следующая информация:

- требования независимости на уровне, на котором они применяются: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 8.5.1 ИСО 26262-3, или 6.5.1 ИСО 26262-4, или 6.5.1 ИСО 26262-5, или 6.5.1 ИСО 26262-6;
- требования отсутствия влияния на уровне, на котором они применяются: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 8.5.1 ИСО 26262-3, или 6.5.1 ИСО 26262-4, или 6.5.1 ИСО 26262-5, или 6.5.1 ИСО 26262-6;
- информация об архитектуре на уровне, на котором независимость и отсутствие влияния должны быть применены: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 7.5.2 ИСО 26262-4, или 7.5.1 ИСО 26262-5, или 7.5.1 ИСО 26262-6.

Примечание – Информация об архитектуре используется для определения границ анализ зависимых отказов.

7.3.2 Дополнительная информация

Не используется.

7.4 Требования и рекомендации

7.4.1 Возможность появления зависимых отказов должна быть определена в результате анализа системы безопасности в соответствии с требованиями раздела 8.

Примечания

1 Как систематические отказы, так и случайные отказы аппаратных средств могут быть зависимыми отказами.

2 Для выявления возможности появления зависимых отказов может быть использован дедуктивный анализ: исследование сечений или повторяющихся идентичных событий в процессе анализа дерева отказов может указывать на возможность появления зависимых отказов.

3 Для выявления возможности появления зависимых отказов может быть также использован индуктивный анализ: подобные части или компоненты с похожими видами отказов, которые появляются несколько раз в процессе анализа видов и последствий отказов, могут дать дополнительную информацию о возможности появления зависимых отказов.

7.4.2 Каждая выявленная возможность появления зависимых отказов должна быть оценена для определения ее достоверности, т.е. существования обоснованно прогнозируемой причины, которая приводит к зависимому отказу и, следовательно, нарушает требуемую независимость или отсутствие влияния между данными элементами.

Примечание – Если в случае оценки нарушений цели безопасности из-за случайных отказов аппаратных средств требуется количественная оценка случайных отказов аппаратных средств (см. ИСО 26262-5), то вклад отказов по общей причине оценивается качественно, так как не существует общих и достаточно надежных методов для количественной оценки таких отказов.

7.4.3 Такая оценка должна учитывать эксплуатационные ситуации, а также различные режимы работы анализируемого устройства или элемента.

7.4.4 Такая оценка, исходя из реальной ситуации, должна выполняться для:

Примечания

1 Такая оценка достоверности возможности появления зависимых отказов может быть выполнена применением соответствующих таблиц контрольных проверок, например, с помощью таблиц контрольных проверок, полученных из практического опыта. Таблицы контрольных проверок обеспечивают аналитикам репрезентативные примеры коренных причин и коэффициентов связи, таких как тот же самый проект, тот же процесс, такой же компонент, тот же интерфейс, близость. МЭК 61508 предоставляет информацию, которая может быть использована для создания таких таблиц контрольных проверок.

2 Такая оценка также может быть также обеспечена строгим соблюдением процессов, описанных в руководящих указаниях, которые предназначены для предотвращения введения исходных причин и коэффициентов связи, которые могут привести к зависимым отказам.

a) случайных отказов аппаратных средств.

Пример – Отказы общих блоков, таких как блок синхронизации, тестовая логика и внутренние регуляторы напряжения в больших интегральных схемах (микроконтроллеры, интегральные схемы и т.п.);

b) ошибок разработки.

Пример – Ошибки в требованиях, ошибки проектирования, ошибки реализации, ошибки, связанные с использованием новых технологий, и ошибки, появляющиеся при выполнении модификаций;

c) сбоев производства.

Пример – Сбои в процессах, процедурах и в подготовке персонала; сбои в планах управления и при мониторинге конкретных характеристик; сбои, связанные с инструментальным программным обеспечением для прошивки контроллеров;

d) сбоев при монтаже.

Пример – Сбои, связанные с укладкой жгута проводов; сбои, связанные с взаимозаменяемостью деталей; отказы смежных устройств или элементов;

e) сбоев ремонта.

Пример – Сбои в процессах, процедурах и подготовке персонала; сбои, связанные с устранением неисправностей; сбои, связанные с взаимозаменяемостью деталей и сбои из-за обратной (сверху-вниз) несовместимости;

f) факторов окружающей среды.

Пример – Температура, вибрация, давление, влажность / конденсация, загрязнение окружающей среды, коррозия, заражение, ЭМС;

g) отказов общих внешних ресурсов.

Пример – Источник питания, входные данные, межсистемная шина данных и связь;

h) воздействий, обусловленных конкретными ситуациями.

Пример – Износ, старение.

7.4.5 Обоснование достоверности зависимых отказов и их воздействие должно быть доступно.

Примечание – Достоверными зависимыми отказами являются те, для которых выполнена оценка обоснованно прогнозируемой причины, как указано в 7.4.2.

7.4.6 Меры по устранению достоверных зависимых отказов должны быть определены на стадии разработки в соответствии с требованиями технологии управления изменениями, представленными в ИСО 26262-8.

7.4.7 Меры по устранению достоверных зависимых отказов должны включать меры по предотвращению их исходных причин или по управлению их последствиями, или для уменьшения коэффициентов связи.

Пример – Разнообразие является мерой, которая может быть использована для предотвращения, сокращения или обнаружения отказов по общей причине.

7.5 Результаты работы

7.5.1 Анализ зависимых отказов

В результате выполнения требований 7.4.

8 Анализ системы безопасности

8.1 Цели

Целью различных видов анализа системы безопасности является изучение последствий сбоев и отказов для функций, поведения и проектов устройств и элементов. Анализ системы безопасности также предоставляет информацию об условиях и причинах, которые могут привести к нарушению цели безопасности или требования безопасности.

Кроме того, выполняемые виды анализа системы безопасности также способствуют выявлению новых функциональных или нефункциональных опасностей, ранее не выявленных в процессе анализа опасностей и оценки рисков.

8.2 Общие положения

В область применения выполняемых анализов системы безопасности входит:

- подтверждение соответствия системы целям безопасности и концепциям безопасности;
- верификация концепций и требований системы безопасности;
- определение условий и причин, в том числе сбоев и отказов, которые могут привести к нарушению цели безопасности или требования безопасности;
- определение дополнительных требований для выявления сбоев и отказов;
- определение требуемых мероприятий (действий / мер) для выявления сбоев и отказов;
- определение дополнительных требований к верификации выполнения целей безопасности или требований безопасности, в том числе связанного с безопасностью тестирования транспортных средств.

На различных уровнях абстракции на стадиях формирования концепции и разработки изделия выполняются соответствующие методы анализа системы безопасности. Количественные методы анализа прогнозируют частоту отказов, а качественные методы анализа идентифицируют отказы, но не предсказывают их частоту. Оба типа методов анализа зависят от знания соответствующих типов и видов моделей.

Качественные методы анализа включают в себя:

- качественный метод анализа вида и последствий отказов на уровне системы, проекта или процесса;
- качественный метод анализа дерева отказов;
- анализ опасности и работоспособности систем;
- качественный анализ дерева событий.

Примечание – Качественные методы анализа, перечисленные выше, могут быть применены к программному обеспечению, если больше никаких соответствующих методов анализа конкретного программного обеспечения не существует.

Количественные методы анализа системы безопасности дополняют качественные методы анализа системы безопасности. Они используются для верификации проекта аппаратных средств с определенными целями – для оценки метрик архитектуры аппаратных средств и оценки нарушений цели безопасности из-за случайных отказов аппаратных средств (см. ИСО 26262-5). Количественный анализ системы безопасности требует дополнительных знаний о количественных значениях интенсивностей отказов элементов аппаратных средств.

Количественные методы анализа включают в себя:

- количественный метод анализа вида и последствий отказов;
- количественный метод анализа дерева отказов;
- количественный метод анализа дерева событий;
- модели Маркова;
- структурные схемы надежности.

Примечание – Количественных методы анализа применяются только для случайных отказов аппаратных средств и в настоящем стандарте для систематических отказов не применяются.

Классифицировать виды анализа системы безопасности можно по другим критериям, например, по способу их выполнения:

- индуктивные методы анализа (реализуются снизу-вверх), которые начинаются с анализа известных причин и прогнозируют неизвестные последствия;
- дедуктивные методы анализа (реализуются сверху-вниз), которые начинаются с анализа известных результатов и выполняют поиск неизвестных причин.

Пример – Анализ вида и последствий отказов, анализ дерева событий и модели Маркова, используемые для моделирования системы, проекта и процесса, являются индуктивными методами анализа. Анализ дерева отказов и структурные схемы надежности являются дедуктивными методами анализа.

8.3 Входная информация

8.3.1 Предварительные требования

Необходима следующая информация:

- требования к безопасности для уровней, на которых должны быть выполнены виды анализа безопасности: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 8.5.1 ИСО 26262-3, или 6.5.1 ИСО 26262-4, или 6.5.1 ИСО 26262-5, или 6.5.1 ИСО 26262-6;
- информация об архитектуре элемента для уровней, на которых должны быть выполнены виды анализа безопасности: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения в соответствии с 7.5.2 ИСО 26262-4, или 7.5.1 ИСО 26262-5, или 7.5.1 ИСО 26262-6.

Примечание – Информация об архитектуре используется для определения границ анализа системы безопасности;

- план обеспечения безопасности в соответствии с 6.5.1 ИСО 26262-2.

Примечание – План обеспечения безопасности содержит цели анализа системы безопасности.

8.3.2 Дополнительная информация

Следующая информация может быть учтена:

- модели сбоев (из внешних источников).

8.4 Требования и рекомендации

8.4.1 Анализ систем безопасности должен выполняться согласно соответствующим стандартам или руководствам.

8.4.2 Результаты анализа систем безопасности должны показать, выполняются или нет соответствующие цели безопасности или требования к системе безопасности.

8.4.3 Если цель безопасности или требование к безопасности не выполняется, то результаты анализа системы безопасности должны использоваться для формирования мер предотвращения или обнаружения или ослабления влияния сбоев или отказов, вызывающих нарушение.

8.4.4 Меры, сформированные по результатам анализа системы безопасности, должны быть реализованы в рамках разработки изделия на уровне системы или на уровне аппаратных средств, или на уровне программного обеспечения, учитывая требования ИСО 26262-4 или ИСО 26262-5, или

ИСО 26262-6 соответственно.

8.4.5 Вновь выявленные опасности при выполнении анализа системы безопасности в процессе разработки изделия, не охваченные целью безопасности, должны быть оценены методом анализа опасностей и оценки рисков и учтены в соответствии с технологией управления изменениями, представленной в ИСО 26262-8.

8.4.6 Модели сбоев, используемые для анализа систем безопасности, должны быть согласованы с соответствующими подстадиями разработки, например, с подстадиями разработки аппаратных средств, оценки метрик архитектуры аппаратных средств и оценки нарушений цели безопасности из-за случайных отказов аппаратных средств, рассмотренными в ИСО 26262-5.

8.4.7 Используя конкретные модели сбоев и результаты анализа системы безопасности, должна быть определена необходимость в дополнительных связанных с безопасностью тестовых примерах.

8.4.8 Результаты анализа системы безопасности должны быть верифицированы в соответствии с требованиями ИСО 26262-8.

8.4.9 Качественные методы анализа системы безопасности включают:

a) систематическое выявление сбоев или отказов, которые могут привести к нарушению целей безопасности или требований безопасности, происходящих:

- в самих устройствах или элементах; или
- при взаимодействии устройства или элемента с другими устройствами или элементами; или
- в применяемых устройствах или элементах;

b) оценку последствий каждого выявленного сбоя для определения возможности нарушения целей безопасности или требований безопасности;

c) выявление причин каждого идентифицированного сбоя;

d) выявление или поддержку выявления возможных слабых сторон концепции обеспечения безопасности, в том числе неэффективности механизмов безопасности при обработке ситуаций с отклонениями от нормы, таких как скрытые сбои, множественные сбои, отказы по общей причине и каскадные отказы.

Примечание – Изучение взаимодействий с другими устройствами или элементами внутри и за пределами устройства делается для того, чтобы оценить степень независимости или влияния.

8.4.10 Если применимы количественные методы анализа системы безопасности, то они должны обеспечить:

a) количественные данные для выполнения оценки метрик архитектуры аппаратных средств и оценки нарушений цели безопасности из-за случайных отказов аппаратных средств (см. ИСО 26262-5);

b) систематическое выявление сбоев или отказов, которые могут привести к нарушению целей безопасности или требований безопасности;

c) оценку и ранжирование возможных слабых сторон концепции обеспечения безопасности, в том числе неэффективности механизмов безопасности;

d) интервал диагностических проверок, интервал аварийного режима, а также время между обнаружением сбоя и его устранением.

8.4.11 Если применяются качественные методы анализа системы безопасности для обеспечения соответствия количественным требованиям, то должны быть выбраны соответствующие уровни детализации выполнения таких видов анализа системы безопасности.

8.5 Результаты работы

8.5.1 Анализ системы безопасности

В результате выполнения требований 8.4.

Приложение А
(справочное)

Обзор и поток документов для анализа уровня полноты безопасности автомобиля и анализа безопасности автомобиля

Таблица А.1 содержит обзор целей, предварительных требований и результатов работы анализа уровня полноты безопасности автомобиля и анализа безопасности автомобиля.

Таблица А.1 – Обзор анализа уровня полноты безопасности автомобиля и анализа безопасности автомобиля

Раздел	Цели	Предварительные требования	Результаты работы
5 Декомпозиция требований с распределением УПБА	В данном разделе установлены правила и руководящие указания для декомпозиции требований к системе безопасности на избыточные требования для обеспечения заданных значений УПБА на следующем уровне детализации	Требования к безопасности на уровне, на котором должна применяться декомпозиция УПБА: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения. Информация об архитектуре на уровне, на котором должна применяться декомпозиция УПБА: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения	5.5.1 Обновление информации об архитектуре. 5.5.2 Обновление значения УПБА как атрибута требований и элементов системы безопасности
6 Критерии совместимости элементов	Настоящий раздел устанавливает критерии совместимости внутри одного элемента: – связанных с безопасностью подэлементов с подэлементами, для которых значение УПБА не назначено; и – связанных с безопасностью подэлементов, которые имеют различные назначенные значения УПБА	Требования безопасности на уровне, на котором должен быть выполнен анализ: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения Информация об архитектуре элемента на уровне, на котором должен быть выполнен анализ: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения	6.5.1 Обновление значения УПБА как атрибута подэлементов элементов
7 Анализ зависимых отказов	Анализ зависимых отказов направлен на выявление отдельных событий или отдельных оснований, которые могли бы не учитывать или считать необоснованной требуемую независимость или отсутствие влияния между данными элементами и, таким образом, нару-шить требование безопасности или цель безопасности	Требования независимости на уровне, на котором они применяются: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения. Требования отсутствия влияния на уровне, на котором они применяются: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения. Информация об архитектуре на уровне, на котором независимость и отсутствие влияния должны быть применены: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения	7.5.1 Анализ зависимых отказов

Окончание таблицы А.1

Раздел	Цели	Предварительные требования	Результаты работы
8 Анализ системы безопасности	Целью различных видов анализа системы безопасности является изучение последствий сбоев и отказов для функций, поведения и проектов устройств и элементов. Анализ системы безопасности также предоставляет информацию об условиях и причинах, которые могут привести к нарушению цели безопасности или требования безопасности. Кроме того, выполняемые виды анализа системы безопасности также способствуют выявлению новых функциональных или нефункциональных опасностей, ранее не выявленных в процессе анализа опасностей и оценки рисков	Требования к безопасности для уровней, на которых должны быть выполнены виды анализа безопасности: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения. Информация об архитектуре элемента для уровней, на которых должны быть выполнены виды анализа безопасности: на уровне системы, на уровне аппаратных средств или на уровне программного обеспечения. План обеспечения безопасности	8.5.1 Анализ системы безопасности

Приложение ДА
(справочное)

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

Таблица ДА

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 26262-1:2011	–	*
ИСО 26262-2:2011	–	*
ИСО 26262-3:2011	–	*
ИСО 26262-4:2011	–	*
ИСО 26262-5:2011	–	*
ИСО 26262-6:2011	–	*
ИСО 26262-8:2011	–	*

* 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

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

Ключевые слова: функциональная безопасность; транспортные средства; электрические компоненты; электронные компоненты; совместимость элементов; зависимые отказы; стадии жизненного цикла системы безопасности; анализ системы безопасности; анализ уровня полноты безопасности автомобиля

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

Усл. печ. л. 2,79. Тираж 31 экз. Зак. 82

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