ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 21448— 2025

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА

Безопасность заданной функциональности

(ISO 21448:2022, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 сентября 2025 г. № 1106-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 21448:2022 «Дорожные транспортные средства. Безопасность заданной функциональности» (ISO 21448:2022 «Road vehicles — Safety of the intended functionality», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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 (www.rst.gov.ru)

Содержание

Введение

Безопасность дорожных транспортных средств имеет первостепенное значение для автомобильной отрасли. Количество функций автоматического вождения, включенных в транспортные средства, увеличивается. Они основаны на распознавании, обработке сложных алгоритмов и их реализации, выполняемой электрическими и/или электронными (Э/Э) системами.

Для соблюдения приемлемого уровня безопасности дорожных транспортных средств требуется отсутствие неоправданного риска, который вызывается любой опасностью, связанной с заданной функциональностью и ее реализацией, в том числе опасностями, которые связаны с отказами, недостаточностями спецификации или производительности.

Для достижения функциональной безопасности в ИСО 26262-1 функциональная безопасность определяется как отсутствие неоправданного риска из-за опасностей, вызываемых некорректным функционированием Э/Э-системы. В ИСО 26262-3 описано, как проводить анализ опасностей и оценку рисков (HARA) для определения опасностей на уровне транспортного средства и связанных с ними целей безопасности. Другие стандарты серии ИСО 26262 устанавливают требования и рекомендации по предотвращению и управлению случайными сбоями аппаратных средств и систематическими отказами, которые могут нарушать цели безопасности.

Для некоторых Э/Э-систем (например, систем, которые формируют осведомленность о ситуации путем определения состояния внешней или внутренней среды транспортного средства) заданная функциональность и ее реализация могут приводить к опасному поведению, несмотря на отсутствие в этих системах сбоев, которые описаны в стандартах серии ИСО 26262. Примеры причин такого потенциально опасного поведения:

- неспособность функции правильно воспринимать внешнюю среду;
- недостаточная устойчивость функции, системы или алгоритма к изменениям входных сигналов датчиков, эвристикам, используемым системами ориентации, или различным условиям внешней среды;
- неожиданное поведение из-за алгоритма принятия решений и/или противоречивых ожиданий человека.

В частности, перечисленные факторы актуальны для функций, систем или алгоритмов, в которых используется машинное обучение.

Отсутствие неоправданного риска, который возникает в результате опасного поведения, связанного с функциональными недостаточностями, определяется как безопасность заданной функциональности (SOTIF). Функциональная безопасность (которая рассматривается в стандартах серии ИСО 26262) и SOTIF являются взаимодополняющими аспектами безопасности (более подробную информацию о соответствующих областях применения стандартов серии ИСО 26262 и настоящего стандарта см. в А.2).

Для обеспечения SOTIF меры по устранению опасностей или снижению рисков реализуются на следующих этапах:

- этап спецификации и проектирования.

Пример 1 — Изменение требований к функциональным возможностям транспортного средства или характеристикам датчиков в связи с обнаруженными недостатками системы или опасными сценариями, выявленными в ходе мероприятий SOTIF;

- этап верификации и валидации.

Пример 2 — Технические экспертизы, тестовые примеры с высокой степенью охвата соответствующих сценариев, введение потенциальных триггерных условий при тестировании в контуре (например, SIL: программное обеспечение в контуре/HIL: аппаратное средство в контуре/MIL: модель в контуре) выбранных сценариев, соответствующих SOTIF.

Пример 3 — Долгосрочные испытания транспортных средств, испытания транспортных средств на полигоне, имитационные испытания;

- этап эксплуатации.

Пример 4 — Мониторинг инцидентов SOTIF при эксплуатации.

Эти опасности могут вызываться конкретными условиями сценария, определяемыми как триггерные условия, к которым может относиться обоснованно предсказуемое неправильное использование заданной функциональности. Кроме того, взаимодействие с другими функциями на уровне транспортного средства может приводить к возникновению опасностей (например, включению стояночного тормоза при активной функции автоматического вождения).

Таким образом, правильное понимание пользователем функциональности, ее поведения и ограничений (это относится, в том числе, к человеко-машинному интерфейсу) имеет важное значение для обеспечения безопасности.

Пример 5 — Невнимание водителя при использовании автоматизированной системы вождения 2-го уровня.

Пример 6 — Некорректное определение режима (например, водитель полагает, что функция активирована, когда она деактивирована) может напрямую приводить к опасности.

Примечание 1 — К обоснованно предсказуемому неправильному использованию не относятся изменения, которые преднамеренно внесены в работу системы.

Информация, предоставляемая инфраструктурой (например, связь V2X — Vehicle2Everything, карты), также участвует в оценке функциональных недостаточностей, если она может влиять на SOTIF (руководство по функциям V2X см. в D.4, приложение D).

Пример 7 — Для систем автоматизированной парковки функциональные возможности планирования маршрута и обнаружения объектов могут совместно реализовываться инфраструктурой и транспортным средством.

Примечание 2 — В зависимости от конкретной прикладной системы при оценке SOTIF могут приниматься во внимание элементы других технологий.

Пример 8 — Расположение и крепление датчика на транспортном средстве могут быть важны для избежания помех на выходе датчика вследствие вибрации.

Пример 9 — Оптические свойства лобового стекла могут иметь значение при оценке SOTIF датчика камеры.

Предполагается, что реагирование на случайные сбои аппаратных средств и систематические сбои (в том числе сбои аппаратных средств и программного обеспечения) Э/Э-системы осуществляется с использованием стандартов серии ИСО 26262.

Функциональные недостаточности, рассматриваемые в настоящем стандарте, можно интерпретировать как систематические сбои, однако предложенные меры по их устранению специфичны и дополняют меры, описанные в стандартах серии ИСО 26262, в котором, в частности, предполагается, что заданная функциональность безопасна, и учитываются сбои Э/Э-системы, которые могут вызывать опасности из-за отклонения от заданной функциональности. Процесс формирования требований к системе и ее элементам может включать аспекты из обоих стандартов.

В таблице 1 показано, как возможные причины опасных событий отражены в существующих стандартах.

Таблица 1 — Обзор тем, связанных с безопасностью, рассматриваемых в различных стандартах

Источник опасности	Причина опасного события	Стандарт(ы)
Система	Сбои Э/Э-системы	Стандарты серии ИСО 26262
	Функциональные недостаточности	Настоящий стандарт
	Неправильный и неадекватный проект человеко-машинного интерфейса (ЧМИ) (ненадлежащая осведомленность пользователя о ситуации — например, замешательство пользователя, перегруженность пользователя информацией, недостаточный контроль внимания пользователя)	Настоящий стандарт. Европейское положение о принципах ЧМИ
	Функциональные недостаточности алгоритмов на основе искусственного интеллекта	Настоящий стандарт
Внешний фактор	Обоснованно предсказуемое неправильное использование пользователем или другими участниками дорожного движения	Настоящий стандарт. Стандарты серии ИСО 26262

Окончание таблицы 1

Источник опасности	Причина опасного события	Стандарт(ы)
Внешний фактор	Атака с использованием уязвимостей в системе безопасности транспортного средства	ISO/SAE 21434
	Влияние активной инфраструктуры и/или связи между транспортными средствами и внешних систем	Настоящий стандарт. ИСО 20077, стандарты серии ИСО 26262, стандарты серии МЭК 61508
	Воздействие внешней среды на транспортное средство (например, других пользователей, пассивной инфраструктуры, погоды, электромагнитных помех)	Настоящий стандарт. Стандарты серии ИСО 26262, ИСО 7637-2, ИСО 7537-3, ИСО 11452-2, ИСО 11452-4, ИСО 10605 и другие применимые стандарты

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОРОЖНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА

Безопасность заданной функциональности

Road vehicles. Safety of the intended functionality

Дата введения — 2026— 01— 01

1 Область применения

В настоящем стандарте представлены общие обоснования и рекомендации в отношении мер обеспечения безопасности заданной функциональности (SOTIF), т. е. отсутствия неоправданного риска вследствие опасности, вызванной функциональными недостаточностями, а именно:

a) недостаточностями спецификации заданной функциональности на уровне транспортного средства;

b) недостаточностями спецификации или недостаточностями производительности электрических и/или электронных (Э/Э) элементов системы.

В настоящем стандарте представлены рекомендации по применению мер на этапах проектирования, верификации и валидации, а также действиям на этапе эксплуатации, которые необходимы для достижения и поддержания SOTIF.

Настоящий стандарт применим к заданным функциям, в которых надлежащая осведомленность о ситуации важна для безопасности и основана на сложных датчиках и алгоритмах обработки (в особенности к функциям систем экстренного вмешательства и систем с уровнями автоматизации вождения от 1 до 5 [2]).

Настоящий стандарт применим к заданным функциям, которые включают в себя одну или несколько Э/Э-систем, установленных на серийных дорожных транспортных средствах, за исключением мопедов.

Обоснованно предсказуемое неправильное использование входит в область применения настоящего стандарта. В нее также входят управление или помощь транспортному средству, которые оказываются удаленным пользователем или посредством связи с бэк-офисом в случае, если они могут повлиять на управление транспортным средством и создавать угрозы безопасности.

Настоящий стандарт не распространяется:

- на сбои, описанные в стандартах серии ИСО 26262;
- угрозы кибербезопасности;
- опасности, непосредственно вызываемые технологией системы (например, повреждение глаз лучом лидара);
- опасности, связанные с поражением электрическим током, пожаром, задымлением, нагревом, радиацией, токсичностью, воспламеняемостью, реактивностью, выделением энергии и аналогичными опасностями, если они не вызваны непосредственно заданными функциями Э/Э-систем;
- умышленные действия, которые явно не соответствуют назначению системы и считаются некорректным использованием функций.

Настоящий стандарт не применяется к функциям существующих систем, для которых существуют хорошо зарекомендовавшие себя и заслуживающие доверия меры проектирования, верификации и валидации (например, системы курсовой устойчивости, подушки безопасности).

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

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

3 Термины и определения

В настоящем стандарте применены термины по ИСО 26262-1, а также следующие термины с соответствующими определениями.

ИСО и МЭК ведут терминологические базы данных для использования в стандартизации по следующим адресам:

- платформа онлайн-просмотра ИСО, доступная на http://www.iso.org/obp;
- Электропедия МЭК, доступная на http://www.electropedia.org/.

3.1 **критерий приемлемости** (acceptance criterion): Критерий, отражающий отсутствие неоправданного уровня риска (3.23).

Примечание 1 — Критерий приемлемости может иметь как качественный, так и количественный характер, например: физические параметры, которые определяют, когда конкретное поведение считается опасным, максимальное количество аварийных событий в час, практически целесообразный низкий уровень (ALARP).

Пример 1 — Из статистики дорожного движения выведен разумный уровень риска: одно происшествие на X км.

Пример 2 — Сравнение с эквивалентным результатом на уровне транспортного средства, которое, как доказано в процессе эксплуатации, контролируется водителем, может способствовать определению критерия приемлемости. Например, нарушение траектории из-за нежелательного вмешательства функции помощи для удержания полосы движения можно сравнивать с боковым порывом ветра для определения приемлемого уровня полномочий этой функции.

3.2 **действие** (action): Отдельная операция или поведение любого участника сцены (3.27).

Примечание 1 — Временная последовательность действий/событий (3.7) и сцен является частью определения сценария (3.26).

Пример — Целевое транспортное средство (3.6) активирует аварийную световую сигнализацию.

Примечание 2 — В контексте данного определения участником может быть человек, другой объект, другая система или любой элемент, взаимодействующий с рассматриваемой функцией.

3.3 **политика вождения** (driving policy): Стратегия и правила, определяющие приемлемые действия (3.2) на уровне транспортного средства.

3.4 **динамическая задача управления;** DDT (dynamic driving task, DDT): Оперативные и тактические функции в режиме реального времени, необходимые для управления транспортным средством в условиях дорожного движения.

Примечание 1 — В состав DDT входят следующие функции:

- управление боковым движением транспортного средства (оперативная);
- управление продольным движением транспортного средства (оперативная);
- мониторинг условий вождения (оперативная и тактическая) и реакция на объекты и события (3.7) (оперативная и тактическая), см. обнаружение и реагирование на объекты и события (OEDR) (3.20);
- планирование маневра (тактическая);
- повышение заметности посредством освещения, подачи сигналов или жестов и т. д. (тактическая).

Примечание 2 — Первоначально эта концепция была определена в SAE J3016 [2].

3.5 **резервный вариант динамической задачи управления** (DDT fallback): Реакция водителя или автоматизированной системы на выполнение динамической задачи управления (DDT) (3.4) или переход в состояние минимального риска (MRC) (3.16) после возникновения отказа(ов) или обнаружения функциональной недостаточности (3.8), либо при обнаружении потенциально опасного поведения.

Пример — Выход из проектной области эксплуатации (ODD) (3.21) или датчик, заблокированный льдом, могут приводить к опасному поведению, на которое должен реагировать водитель.

Примечание 1 — Первоначально эта концепция была определена в SAE J3016 [2].

3.6 **целевое транспортное средство** (ego vehicle): Транспортное средство, оснащенное функциональностью, которая анализируется для SOTIF (3.25).

3.7 **событие** (event): Явление, которое происходит в определенный момент времени.

Примечание 1 — Временная последовательность действий (3.2)/событий и сцен (3.27) входит в определение сценария (3.26).

Примечание 2 — Несмотря на то, что каждое действие также является событием, не каждое событие является действием, т. е. множество всех действий является подмножеством всех событий.

Пример 1 — Дерево, упавшее на проезжую часть в 50 м перед транспортным средством.

Пример 2 — Зеленый свет светофора включается в определенный момент времени.

3.8 **функциональная недостаточность** (functional insufficiency): Недостаточность спецификации (3.12) или недостаточность производительности (3.22).

Примечание 1 — Функциональные недостаточности включают в себя недостаточности спецификации или характеристик на уровне транспортного средства или элементов Э/Э-системы.

Примечание 2 — Деятельность по обеспечению SOTIF (3.25) включает выявление функциональных недостаточностей и оценку их последствий. Функциональные недостаточности по определению (см. 3.12 и 3.22) приводят к опасному поведению или неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неправильное использование (3.17). Термин «потенциальная функциональная недостаточность» может использоваться, когда еще не установлена способность содействия опасному поведению или неспособность предотвратить или обнаружить и смягчить обоснованно предсказуемое неправильное использование.

Примечание 3 — Рисунки 1—3 описывают причинно-следственную модель SOTIF, в которой описана взаимосвязь триггерных условий (3.30), функциональных недостаточностей, нарушений выходных данных, опасного поведения, неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование, а также опасности (3.11), опасные события (3.7) и вред.

Примечание 4 — В случае неявного неправильного использования, способствующего причинению вреда, как правило, возникают две функциональные недостаточности. Одной из них является функциональная недостаточность, приводящая к опасному поведению системы в сочетании с триггерными условиями, а другой — функциональная недостаточность, приводящая к неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование (см. рисунки 1, 2 и 3).

Пример — Транспортное средство оснащено функцией помощи при вождении на шоссе уровня 2. В состав системы входит камера наблюдения за водителем, позволяющая выявить невнимательность водителя. Для простоты предположим, что верны следующие утверждения:

- чувствительный элемент имеет функциональную недостаточность, которая, если она активируется триггерным условием 1, приводит к опасному поведению — выполнению неправильной траектории движения транспортного средства;

- камера наблюдения за вождением имеет функциональную недостаточность, которая, если она активирована триггерным условием 2, приводит к неспособности системы обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование.

Для возникновения вреда сценарий (3.26) должен содержать следующее:

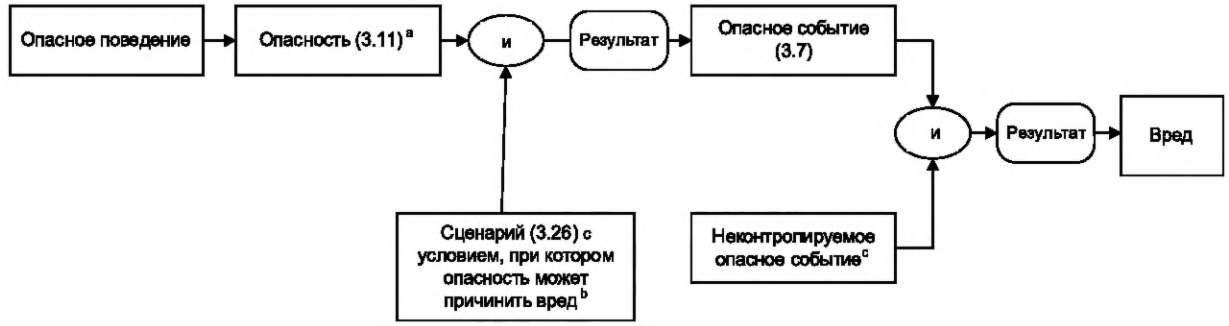
- наличие неявного неправильного использования со стороны водителя: водитель невнимателен и своевременно не обнаруживает опасное поведение системы, чтобы иметь возможность контролировать его;

- наличие триггерного условия 2, приводящего к неспособности системы вовремя обнаружить и смягчить нынешнее обоснованно предсказуемое неявное неправильное использование; и

- наличие триггерного условия 1, приводящего к опасному поведению системы.

Примечание 5 — Если функциональная недостаточность на уровне транспортного средства активируется триггерным условием, то это приводит к опасному поведению либо к неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование [см. рисунок 3 (A)].

Примечание 6 — Если функциональная недостаточность на уровне элемента активируется триггерным условием, то это приводит к нарушению выхода [см. рисунок 3 (B)]. Нарушение выхода само по себе или в сочетании с одним или несколькими нарушениями выхода других элементов способствует опасному поведению на уровне транспортного средства либо неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование [см. рисунок 3 (B)].



[a] Опасность — возможный источник вреда, вызываемый опасным поведением на уровне транспортного средства.

[b] Сценарий, содержащий условия, при которых опасность может привести к причинению вреда, является фактором, способствующим возникновению вреда, а не его источником.

[c] Неспособность получить достаточный контроль над опасным событием является фактором, способствующим возникновению вреда, но не его источником.

Рисунок 1 — Корреляция между опасностью и возникновением вреда

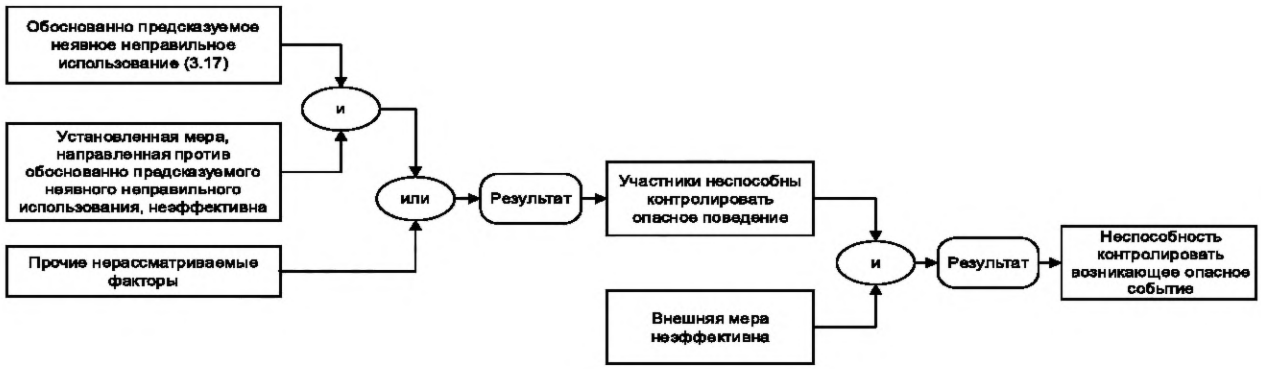
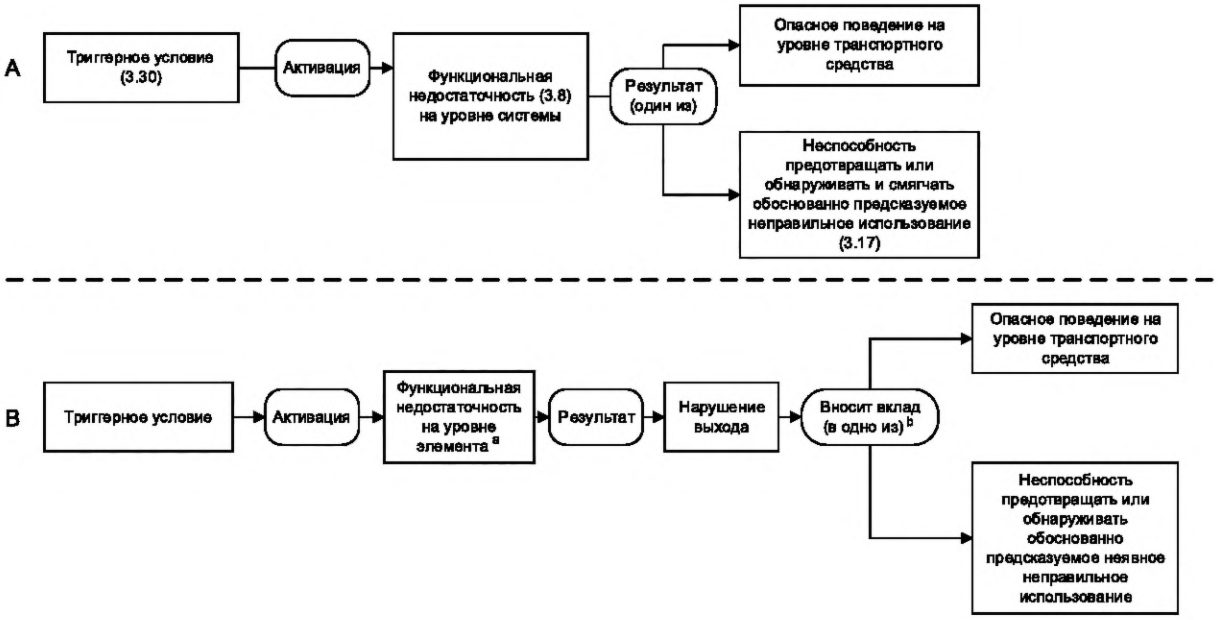


Рисунок 2 — Причины неконтролируемого опасного события



[a] В зависимости от архитектуры системы эту функциональную недостаточность на уровне элемента можно распознать как единичную функциональную недостаточность (3.28) либо множественную функциональную недостаточность (3.19).

[b] Нарушение выхода само по себе или в сочетании с одним или несколькими нарушениями выходов других элементов способствует опасному поведению на уровне транспортного средства либо неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование.

Рисунок 3 — Причинно-следственная модель SOTIF

3.9 **функциональная модификация** (functional modification): Изменение функциональной спецификации.

Примечание 1 — Функциональная модификация не совпадает с модификацией в терминах ИСО 26262-1:2018. Термин «функциональная модификация» в настоящем стандарте соответствует термину «изменение» в серии стандартов ИСО 26262.

3.10 **пользователь, готовый к резервному варианту** (fallback-ready user): Пользователь, который может управлять транспортным средством и способен подключиться к выполнению резервного варианта динамической задачи управления (3.5) по мере необходимости в течение периода времени, соответствующего определенной профессии, не связанной с вождением автомобиля.

Примечание 1 — Первоначально эта концепция была определена в SAE J3016 [2].

3.11 **опасность** (hazard): Потенциальный источник вреда, вызванный опасным поведением на уровне транспортного средства.

[ИСО 26262-1:2018, 3.75, изменено — словосочетание «неправильным поведением» заменено на «опасным поведением», слово «устройства» заменено на словосочетание «на уровне транспортного средства», примечание удалено]

3.12 **недостаточность спецификации** (insufficiency of specification): Спецификация (возможно, неполная), которая способствует опасному поведению либо неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование (3.17), когда оно активируется одним или несколькими триггерными условиями (3.30).

Пример 1 — Неполная спецификация дистанции движения адаптивного круиз-контроля приводит к тому, что транспортное средство, оснащенное датчиком (3.6), не поддерживает безопасную дистанцию до впереди идущего транспортного средства.

Пример 2 — Неспособность системы обрабатывать необычные дорожные знаки из-за их отсутствия в спецификации, т. е. если необычный дорожный знак отсутствует в спецификации, система не может корректно обработать его.

Примечание 1 — Недостаточность спецификации может быть как выявлена, так и не выявлена в конкретный момент жизненного цикла системы.

Примечание 2 — Деятельность по обеспечению SOTIF (3.25) включает выявление недостаточностей спецификации и оценку их последствий. Термин «потенциальная недостаточность спецификации» может использоваться, когда еще не установлена его способность приводить к опасному поведению или неспособность предотвращать или обнаруживать и смягчать обоснованно предсказуемое неправильное использование.

Примечание 3 — Требования, вытекающие из спецификации, допущений о других системах или элементах или из систематического анализа (например, включенного в раздел 6, или других видов анализа, которые определяют требования к проектированию и реализации SOTIF), могут быть включены в формальные базы данных для поддержки степени доверия верификации. Во многих организациях эти требования могут не обозначаться как «спецификации», однако они необходимы для обеспечения SOTIF. Термин «недостаточность (недостаточности) спецификации» в настоящем стандарте включает в себя недостаточности таких производных требований.

3.13 **заданное поведение** (intended behaviour): Поведение заданной функциональности (3.14).

Примечание 1 — Заданное поведение — это поведение, которое разработчик считает номинальной функциональностью с учетом ограничений возможностей, обусловленных внутренними характеристиками используемых компонентов и технологий.

Примечание 2 — Несмотря на то, что заданное поведение, определенное разработчиком, не представляет неоправданного риска (3.31), оно может не соответствовать ожиданиям водителя в отношении поведения системы.

3.14 **заданная функциональность** (intended functionality): Функциональность, которая указана в спецификации.

Примечание 1 — Заданная функциональность определяется на уровне транспортного средства.

3.15 **уровни автоматизации вождения** (levels of driving automation): Взаимоисключающий набор уровней автоматизации вождения от уровня 0 (без автоматизации) до уровня 5 (полная автоматизация), определяющий роли водителя или пользователя и системы автоматизации по отношению друг к другу.

Примечание 1 — См. таблицу 2.

Примечание 2 — Первоначально эта концепция была определена в SAE J3016 [2].

Таблица 2 — Уровни автоматизации вождения

		DDT (3.4)			
Уровень	Название	Управление поперечным и продольным движением транспортного средства	OEDR (3.20)	Резервный вариант динамической задачи управления (3.5)	ODD (3.21)
0	Автоматизация вождения отсутствует	Водитель	Водитель	Водитель	Не применимо
1	Помощь водителю	Водитель и система	Водитель	Водитель	Ограниченное
2	Частичная автоматизация вождения	Система	Водитель	Водитель	Ограниченное
3	Условная автоматизация вождения	Система	Система	Пользователь, готовый к резервному варианту (3.10)	Ограниченное
4	Высокая автоматизация вождения	Система	Система	Система	Ограниченное
5	Полная автоматизация вождения	Система	Система	Система	Неограниченное

3.16 **состояние минимального риска**; MRS (minimal risk condition, MRC): Состояние транспортного средства, снижающее риск (3.23), когда невозможно завершить конкретную поездку.

Примечание 1 — Это один из ожидаемых результатов резервного варианта динамической задачи управления (3.5).

Примечание 2 — Аналогом функциональной безопасности в серии ИСО 26262 будет безопасное состояние.

Примечание 3 — Первоначально эта концепция была определена в SAE J3016 [2].

3.17 **неправильное использование** (misuse): Использование способом, не предусмотренным изготовителем или поставщиком услуг.

Примечание 1 — Неправильное использование включает в себя непреднамеренное поведение человека, но не включает в себя преднамеренное изменение системы или использование системы с намерением причинить вред.

Примечание 2 — Неправильное использование может быть результатом чрезмерной уверенности в работе системы.

Примечание 3 — В зависимости от причинно-следственной связи с опасным поведением различают два вида неправильного использования: явное и неявное.

Примечание 4 — Явное неправильное использование, которое может являться причиной возникновения опасного поведения системы, считается возможным триггерным условием (3.30). Если установлена его способность содействовать возникновению опасного поведения, оно считается триггерным условием. Также возможно, что явное неправильное использование является частью триггерного условия, т. е. для того, чтобы возникло опасное поведение системы, помимо явного неправильного использования должны присутствовать дополнительные конкретные условия сценария.

Пример 1 — Явное неправильное использование: активация функции, предназначенной для шоссе в городских условиях, приводит к сценарию (3.26), в котором транспортное средство не обнаруживает знак СТОП и не реагирует на него.

Пример 2 — Явное неправильное использование: водитель активирует автоматизированную систему вне проектируемой области эксплуатации (ODD) (3.21), указанной в руководстве пользователя. Это считается явным неправильным использованием независимо от того, включает ли система компонент локализации целевого транспортного средства (3.6), который предотвращает активацию за пределами указанной ODD.

Примечание 5 — Неявное неправильное использование приводит к снижению управляемости опасным поведением и/или потенциальному увеличению серьезности происходящего инцидента. Это не считается потенциальным триггерным условием, поскольку не может способствовать опасному поведению самой системы.

Пример 3 — Неявное неправильное использование: помощник на дороге без участия человека уровня 2 с выявленными проблемами восприятия требует от водителя постоянно контролировать правильность выполнения системой динамической задачи управления (3.4) и вмешиваться при необходимости. Неявное неправильное использование — водитель засыпает и не следит за выполнением динамической задачи управления. Эта ситуация считается неявным неправильным использованием независимо от того, обнаружена ли она и устранена системой мониторинга водителя.

Пример 4 — Неявное неправильное использование: пассажир расстегивает ремень безопасности целевого транспортного средства во время движения и автономного вождения. Это неявное неправильное использование, поскольку оно может увеличить серьезность инцидента, при этом не являясь триггерным условием.

Примечание 6 — См. рисунки 1—3.

3.18 **сценарий неправильного использования** (misuse scenario): Сценарий (3.26), в котором происходит неправильное использование (3.17).

3.19 **множественная функциональная недостаточность** (multiple-point functional insufficiency): Функциональная недостаточность (3.8) элемента, приводящая к опасному поведению или неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование (3.17) только в сочетании с функциональными недостаточностями других элементов при активации одним или несколькими триггерными условиями (3.30).

3.20 **обнаружение и реакция на объекты и события**; OEDR (object and event detection and response, OEDR): Динамические задачи управления (3.4), которые включают в себя мониторинг условий вождения и выполнение соответствующей реакции на объекты и события (3.7) и обеспечивают выполнение динамической задачи управления и/или резервного варианта динамической задачи управления (3.5).

[SAE J3016:2021, 3.19 [2], изменено — словосочетание «обнаружение, распознавание и классификация объектов и событий, а также подготовка к реагированию по мере необходимости», расположенное после слова «внешняя среда», удалена]

3.21 **домен штатной эксплуатации**; ODD (operational design domain, ODD): Конкретные условия функционирования, которые предусмотрены проектом для данной системы автоматизации вождения.

Примечание 1 — Условия могут быть пространственными, временными, внутренними или относящимися к внешней среде.

Примечание 2 — Термин «предусмотрены проектом» взят из определения в SAE J3016 [2]. В настоящем стандарте это означает «специфицированы».

Примечание 3 — Условия самой автоматизированной системы вождения (например, скорость транспортного средства, вычислительные возможности и возможности восприятия сигналов датчиков) также входят в область ODD.

Примечание 4 — Первоначально эта концепция была определена в SAE J3016 [2].

3.22 **недостаточность производительности** (performance insufficiency): Ограничение технических возможностей, вносящее вклад в возникновение опасного поведения или в неспособность предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование (3.17), когда оно активируется одним или несколькими триггерными условиями (3.30).

Примечание 1 — Недостаточности производительности могут быть как выявлены, так и не выявлены в конкретный момент жизненного цикла системы.

Примечание 2 — Недостаточности производительности рассматриваются для элементов Э/Э-системы и для основанных на других технологиях элементов, которые считаются значимыми для достижения SOTIF (3.25) (см. 3.8, примечание 1).

Примечание 3 — Деятельность по обеспечению SOTIF включает выявление недостаточностей производительности и оценку их последствий. Термин «возможная недостаточность производительности» может использоваться, когда еще не установлена способность, вносящая вклад в возникновение опасного поведения, или неспособность предотвратить или обнаружить и смягчить обоснованно предсказуемое неправильное использование.

Пример — Ограничениями технических возможностей являются ограниченная производительность вычислений, ограниченная дальность восприятия датчика, ограниченное срабатывание и т. д.

3.23 **риск** (risk): Сочетание вероятности события причинения вреда и тяжести последствий этого вреда.

[ИСО 26262-1:2018, 3.128]

3.24 **реакция** (reaction): Отклик на действие (3.2) любого участника сцены (3.27).

3.25 **безопасность заданной функциональности** (safety of the intended functionality; SOTIF): Отсутствие неоправданного риска (3.31) из-за опасностей (3.11), возникающих в результате функциональных недостаточностей (3.8) заданной функциональности (3.14) или их реализации.

Примечание 1 — Опасное поведение системы, которое может привести к опасности (см. рисунок 1), инициируется триггерным условием (3.30) сценария (3.26). Обоснованно предсказуемое явное неправильное использование (3.17) рассматривается как возможное триггерное условие.

Примечание 2 — При обнаружении опасных событий (3.7) также учитываются заданное использование и обоснованно предсказуемое неявное неправильное использование в сочетании с опасным поведением, возникающим из-за недостаточности спецификации (3.12) или недостаточности производительности (3.22).

3.26 **сценарий** (scenario): Описание временных отношений между несколькими сценами (3.27) в последовательности сцен, а также целей и ценностных установок для каждой конкретной ситуации, на которую влияют действия (3.2) и события (3.7).

Примечание 1 — Каждый сценарий начинается с начальной сцены. Действия и события, а также цели и ценностные установки могут указываться для характеристики этих временных отношений в сценарии. В отличие от сцены, сценарий охватывает определенный промежуток времени.

Примечание 2 — Определение адаптировано из [3].

Примечание 3 — Указанные цели и ценностные установки являются условными параметрами заданной функциональности (3.14). Пример цели — оставаться между разметкой полосы движения. Пример ценностной установки — ставить безопасность пешеходов выше предотвращения финансового ущерба.

3.27 **сцена** (scene): Состояние внешней среды в конкретный момент времени, которое включает в себя окружающую обстановку, динамические элементы, все собственные представления участников и наблюдателей, а также отношения между перечисленными сущностями.

Примечание 1 — Сцена может включать в себя элементы окружающей среды (состояние, время, погоду, освещение и другие внешние условия), дорожную инфраструктуру или внутренние элементы (геометрические параметры дороги, внутренние геометрические параметры, топологию, качество, дорожные знаки, ограждения и т. д.), объектов/участников (статические, динамические, подвижные), а также взаимодействия и маневры (если применимо).

Примечание 2 — Всеохватывающая сцена (т. е. объективная сцена или реальная ситуация), которая включает в себя все объекты (например, декорации, динамические элементы, актеров), может быть смоделирована только в среде имитационного моделирования. В реальном мире сцены воспринимаются датчиками. Сцена, которая воспринимается автономным транспортным средством (3.6) или водителем-человеком, является неполным, неточным, неопределенным и потенциально ошибочным представлением реальной ситуации.

Примечание 3 — Сцена также может включать в себя аспекты целевого транспортного средства и системы, реализующей заданную функциональность (3.14) — например, давление в шинах, род деятельности пользователя и наличие отказов компонентов системы.

Примечание 4 — Определение адаптировано из [3].

3.28 **одиночная функциональная недостаточность** (single-point functional insufficiency): Функциональная недостаточность (3.8) элемента, которая непосредственно приводит к опасному поведению или неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неправильное использование (3.17) при активации одним или несколькими триггерными условиями (3.30).

3.29 **осведомленность о ситуации** (situational awareness): Понимание ситуации.

3.30 **триггерное условие** (triggering condition): Конкретное состояние сценария (3.26), которое служит инициатором последующей реакции системы, способной привести к опасному поведению либо неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неявное неправильное использование (3.17).

Примечание 1 — Понятие «возникновение» включает в себя возможность последовательного возникновения множества условий, приводящих к опасному поведению или неспособности предотвратить или обнаружить и смягчить обоснованно предсказуемое неправильное использование.

Примечание 2 — Триггерное условие сценария (3.26) активирует функциональную недостаточность (3.8), что приводит к последующей реакции системы (см. рисунки 1—3).

Пример — При движении по шоссе автоматизированная система экстренного торможения (AEB) транспортного средства ошибочно определяет дорожный знак как ведущее транспортное средство, что приводит к торможению со значением отрицательного ускорения X·g в течение Y секунд. В данном примере триггерным условием является обстоятельство, которое приводит к ошибочному распознаванию дорожного знака при движении по шоссе, тогда как AEB имеет соответствующую недостаточность производительности (3.22) (например, низкую точность восприятия или неправильную классификацию алгоритмов).

Примечание 3 — К действиям по обеспечению SOTIF (3.25) относятся идентификация триггерных условий и оценка реакции системы. Термин «потенциальное триггерное условие» можно использовать, когда способность инициировать соответствующую реакцию еще не установлена.

Примечание 4 — Обоснованно предсказуемое явное неправильное использование, которое может непосредственно инициировать опасное поведение системы, рассматривается как возможное триггерное условие.

Примечание 5 — См. рисунки 1—3.

3.31 **неоправданный риск** (unreasonable risk): Риск (3.23), который считается неприемлемым в определенном контексте в соответствии с действующими социально-нравственными понятиями.

[ИСО 26262-1:2018, 3.176]

3.32 **вариант использования** (use case): Описание набора связанных сценариев (3.26).

Примечание 1 — Вариант использования может включать следующую информацию о системе:

- один или несколько сценариев;
- функциональный диапазон (например, максимально допустимая скорость, максимально допустимое замедление);

- желаемое поведение;
- границы системы;
- допущения о внешней среде и действиях человека.

Примечание 2 — Описание варианта использования, как правило, не включает в себя подробный список всех соответствующих сценариев. Вместо этого используется более абстрактное описание этих сценариев.

Примечание 3 — Определение адаптировано из [3].

3.33 **цель валидации** (**целевой показатель валидации**) (validation target): Значение характеристики, которое подтверждает соблюдение критерия приемлемости (3.1).

Примечание 1 — Определение цели валидации зависит от области применения и планов применения.

Примечание 2 — В контексте SOTIF (3.25) валидация — это обеспечение достижения критериев приемлемости (идентифицированных опасностей) с достаточным доверительным уровнем посредством проверок и испытаний.

Пример — Отсутствие опасного поведения во время Y-часового пробега при испытаниях на надежность или однократное опасное поведение определенного уровня серьезности при X-кратном выполнении парковки.

Примечание 3 — Для полного соблюдения данного критерия приемлемости может требоваться достижение нескольких целей валидации.

3.34 **стратегия SOTIF на уровне транспортного средства**; VLSS (vehicle-level SOTIF strategy, VLSS); Набор требований на уровне транспортного средства для заданной функциональности (3.14), который используется для поддержки действий по проектированию, верификации и валидации с целью достижения SOTIF (3.25).

Примечание 1 — Стратегия SOTIF на уровне транспортного средства может определяться для каждой системы, связанной с SOTIF.

4 Обзор и организация деятельности по обеспечению SOTIF

4.1 Общие положения

В разделе 4 представлены:

a) обзор принципов SOTIF;

b) руководство по рабочему процессу обеспечения SOTIF и использованию настоящего стандарта;

c) руководство по управлению обеспечением SOTIF и вспомогательными процессами.

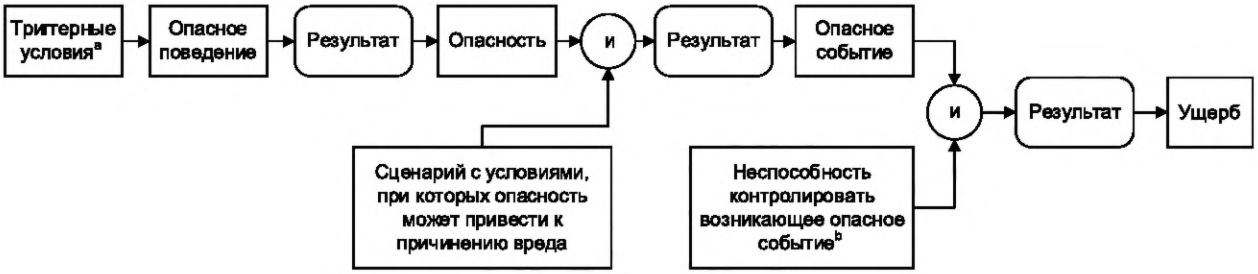
Деятельность, представленная в настоящем стандарте, применима к уровню транспортного средства, системы и компонентов.

4.2 Принципы SOTIF

4.2.1 Модель опасных событий, связанных с SOTIF

Основная цель настоящего стандарта — описать действия и представить обоснования достаточно низкого уровня риска, который связан со всеми выявленными опасными событиями, относящимися к SOTIF.

Функция, спецификация системы и проект включают в себя соответствующие варианты использования, которые, в свою очередь, имеют несколько сценариев. Эти сценарии могут содержать триггерные условия, которые приводят к нанесению вреда (упрощенную версию см. на рисунке 4, более подробную версию — на рисунках 1—3). Во избежание вреда необходима надлежащая осведомленность о ситуации.



[a] Триггерные условия включают в себя обоснованно предсказуемое явное неправильное использование.

[b] Неспособность контролировать опасное событие также может являться результатом обоснованно предсказуемого неявного неправильного использования (пример: водитель не контролирует систему должным образом).

Рисунок 4 — Визуализация модели опасных событий, связанных с SOTIF

Пример 1 — При активации в городских условиях функция, предназначенная только для использования на автомагистралях, имеет ограничения в распознавании и интерпретации движения уязвимых участников дорожного движения.

Пример 2 — Неверное понимание режима работы системы водителем, который полагает, что система активна, хотя она деактивирована. В такой ситуации потенциальная неспособность ЧМИ системы предотвращать это непонимание или отсутствие соответствующей реакции системы (если поведение водителя можно контролировать) также можно рассматривать как опасное поведение системы.

Примечание 1 — Надлежащая осведомленность о ситуации зависит:

- от достаточно полного и точного восприятия соответствующих условий внешней среды, правильного понимания сцены (например, обнаружения соответствующего знака остановки) и модели прогнозирования состояния каждого участника дорожного движения (например, направления движения, скорости). Осведомленность о ситуации может дополнительно поддерживаться такой информацией, как локализация, движение по заданному маршруту или связь с другими транспортными средствами или о внешней среде;
- соответствующих действий или реакций во время вождения (например, соблюдения правил, связанных со знаками остановки).

В течение срока эксплуатации транспортного средства могут меняться:

- внешняя среда (например, новые типы дорожных знаков, дорожной разметки, транспортные средства);
- соответствующие реакции (например, новые действия при вождении, которые требуется выполнять в связи с появлением нового дорожного знака; изменения в сценариях вождения, правилах вождения).

Примечание 2 — Мониторинг таких изменений описан в разделе 13.

Примечание 3 — Эту проблему можно решить с помощью требований, вытекающих из политики вождения (см. пример в D.1).

Такие соображения учитываются при спецификации проектируемой области эксплуатации (ODD) и разработке системы (идентификации рисков, определении соответствующих мер) для обеспечения SOTIF во время эксплуатации.

4.2.2 Четыре области сценариев

В настоящем стандарте под опасными сценариями понимаются сценарии, вызывающие опасное поведение. Сценарии, которые являются частью соответствующих вариантов использования, подразделяются на четыре области (см. рисунки 5 и 6).

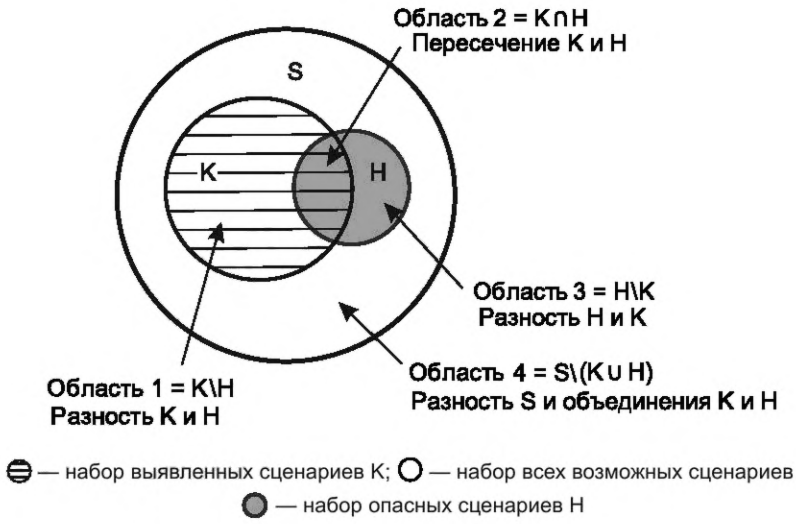
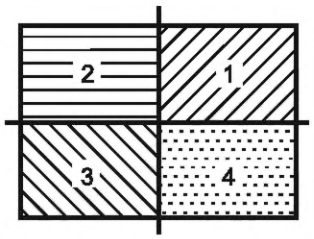


Рисунок 5 — Визуализация категорий сценариев



1 — выявленные безопасные сценарии (область 1); 2 — выявленные опасные сценарии (область 2);
3 — невыявленные опасные сценарии (область 3); 4 — невыявленные безопасные сценарии (область 4)

Рисунок 6 — Альтернативная визуализация категорий сценариев

Для структурирования и разъяснения этого стандарта определены области 1, 2, 3 и 4:

- выявленные безопасные сценарии (область 1);
- выявленные опасные сценарии (область 2);
- невыявленные опасные сценарии (область 3);
- невыявленные безопасные сценарии (область 4).

Пример — К невыявленным областям относятся сценарии, у которых:

- определены возможные триггерные условия (например, экстремально низкая температура, особое сочетание сценариев движения), однако поведение системы неизвестно;

- существуют неизвестные триггерные условия (например, события «черного лебедя»);

- известные параметры сценариев могут объединяться в неизвестные возможные триггерные условия (например, сочетание погодных условий и условий дорожного движения).

Примечание 1 — Сценарии в области 4, которые являются невыявленными, но не опасными, не создают риск причинения вреда. Как только сценарий в области 4 обнаруживается (т. е. становится известным), он перемещается в область 1.

Эта модель представляет собой концептуальную абстракцию цели деятельности по обеспечению SOTIF, которая заключается в следующем:

- выполнение оценки приемлемости риска области 2 на основе анализа заданной функциональности;
- снижение до приемлемого уровня вероятности выявленных опасных сценариев, вызывающих опасное поведение в области 2, путем функциональной модификации (см. раздел 8);
- снижение до приемлемого уровня вероятности невыявленных сценариев, вызывающих потенциально опасное поведение, в области 3 посредством адекватной стратегии верификации и валидации (см. разделы 9 и 11).

Примечание 2 — Это лишь концептуальный подход к одному аспекту задачи, поскольку размеры областей не поддаются измерению.

Примечание 3 — Размер зон отражает количество сценариев, а не риск, связанный с этими сценариями. Однако это лишь концептуальный подход к одному из аспектов задачи, поскольку размеры площадей на самом деле не поддаются измерению. Задача SOTIF — предоставить обоснование достаточно низкого риска заданной функциональности, для которой количество сценариев является одним, но не единственным аспектом. Тяжесть причиненного вреда и вероятность возникновения опасного сценария влияют на риск заданной функциональности, но не представлены в вышеуказанных областях.

Примечание 4 — Если использование сценариев для определенных действий, связанных с SOTIF, не запланировано в подходе к разработке прикладной системы, это не меняет цели SOTIF (избежать неоправданного риска).

Конкретный вариант использования может включать выявленные и невыявленные сценарии. Исследование сценариев каждого варианта использования может привести к выявлению ранее невыявленных сценариев.

Конечной целью деятельности SOTIF является оценка потенциально опасного поведения, присутствующего в областях 2 и 3, и предоставление аргументов в пользу того, что остаточный риск, вызванный этими сценариями, достаточно низок, т. е. находится на уровне или ниже критериев приемлемости. Если риск, возникающий в результате выявленных сценариев в области 2, оценивается явно, то риск, возникающий в результате невыявленных сценариев в области 3 согласно статистическим тестам, считается достаточно малым.

Ожидается, что остаточный риск, связанный с областями 2 и 3, будет снижен. Уверенность в достижении SOTIF будет увеличиваться благодаря росту количества сценариев в области 1 (см. рисунки 7 и 8).

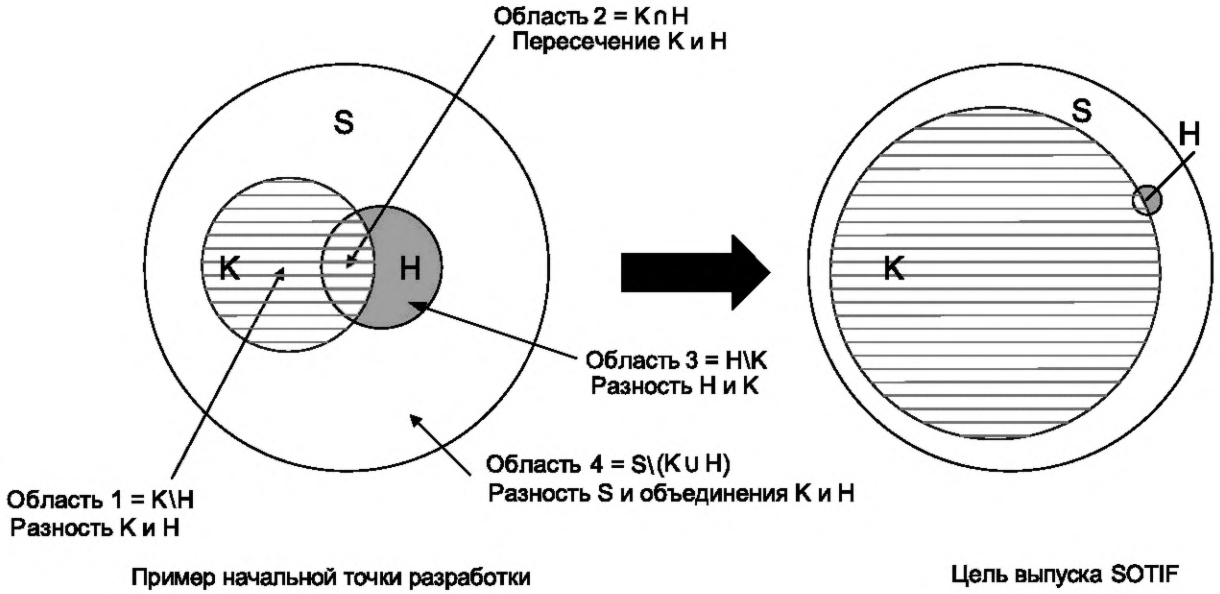
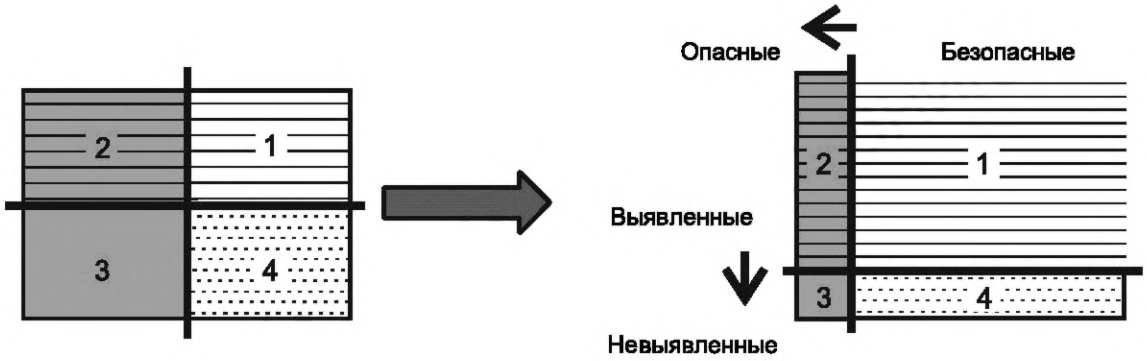


Рисунок 7 — Эволюция категорий сценариев
в результате реализации настоящего стандарта



Пример начальной точки разработки — Цель выпуска SOTIF

1 — выявленные безопасные сценарии (область 1); 2 — выявленные опасные сценарии (область 2); 3 — невыявленные опасные сценарии (область 3); 4 — невыявленные безопасные сценарии (область 4)

Рисунок 8 — Альтернативная эволюция категорий сценариев в результате деятельности по настоящему стандарту

4.2.3 Модель «Восприятие — План — Выполнение»

Возможные причины опасного поведения, рассматриваемые в настоящем стандарте, тесно связаны со способностью системы создавать достаточно точную модель внешней среды, принимать правильные решения, формировать корректные управляющие действия на основе модели внешней среды и выполнять их.

Ключевые элементы системы и их взаимодействие представлены в виде модели «Восприятие — План — Выполнение» (см. рисунок 9). Элемент «Восприятие» выполняет часть представления (в том числе локализацию), т. е. создает модель внешней среды на основе информации, полученной в результате зондирования внешней и внутренней сред транспортного средства, а также состояний транспортного средства и систем. Элемент «План» применяет свои цели и стратегии к модели внешней среды, формируемой элементом «Восприятие», для генерации управляющих действий. Наконец, элемент «Выполнение» выполняет эти действия.

Примечание — Алгоритмы принятия решений включены во все элементы модели «Восприятие — План — Выполнение» (например, классификация данных датчиков, объединение элементов, анализ ситуации, принятие решения о действии).

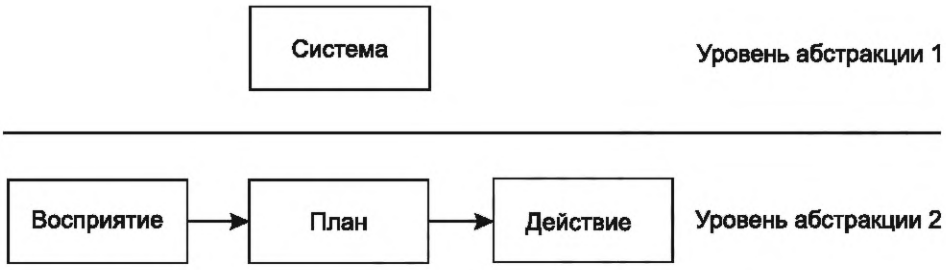


Рисунок 9 — Визуализация модели «Восприятие — План — Выполнение»

Выбор пригодной комплексной системной архитектуры на основе модели «Восприятие — План — Действие» может являться важным фактором в достижении эффективного процесса обеспечения SOTIF, чтобы общие возможности и соответствующие действия могли осуществляться как на ранних стадиях функциональной разработки, так и на протяжении всего ее жизненного цикла. Поскольку выбор подходящей системной архитектуры имеет решающее значение для обеспечения SOTIF, мероприятия по определению архитектуры системы можно начинать на ранней стадии разработки системы. Кроме того, архитектура системы регулярно пересматривается на протяжении всего жизненного цикла системы и обновляется при необходимости.

4.3 Использование настоящего стандарта

4.3.1 Блок-схема и структура настоящего стандарта

Действия по обеспечению SOTIF (см. рисунок 10) начинаются с определения спецификации и проекта (см. раздел 5). Спецификация и проект включают в себя функциональные недостаточности, которые становятся известными до выполнения последующих действий и циклов обеспечения SOTIF. Итерации действий по обеспечению SOTIF могут приводить к обновлениям спецификации и проекта, а также к обнаружению новых, ранее неизвестных функциональных недостаточностей. Каждая итерация, начиная со спецификации и проекта, требует, чтобы спецификация и проект были актуальными.

Для потенциально опасного поведения заданной функциональности выполняется идентификация опасности и оценка риска (см. раздел 6). Для выявленных опасных событий оценивается их риск и соответствующим образом определяются критерии его приемлемости. Если показано, что опасные события не приводят к неоправданному риску, то дополнительные проектные мероприятия не выполняются. В разделе 6 рассматриваются не причины опасного поведения заданной функциональности, а только их последствия для безопасности. Таким образом, основное внимание уделяется оценке опасных событий, которые могут возникать в результате опасного поведения, и определению критериев приемлемости, которые должны быть удовлетворены.

В разделе 7 определяются возможные первопричины опасного поведения заданной функциональности (см. рисунок 1) и оценивается оправданность риска, возникающего в результате выявленных возможных функциональных недостаточностей и триггерных условий.

В функциональность вносятся изменения (примеры — улучшение возможностей датчика, дальнейшее ограничение проектируемой области эксплуатации) для улучшения SOTIF, если это признается необходимым в результате действий, предусмотренных разделами 6, 7, 9, 10, 11, 12 и 13 (см. раздел 8).

Разрабатывается стратегия верификации и валидации для предоставления доказательств того, что остаточный риск на уровне транспортного средства, связанный с SOTIF, находится ниже приемлемого уровня, а элементы соответствуют своим функциональным требованиям (см. раздел 9). Для подтверждения достаточно низкого риска на основе этой стратегии могут создаваться соответствующие тестовые примеры верификации и валидации (см. разделы 10 и 11).

Оценивается достаточность результатов действий по обеспечению SOTIF для обоснования достижения SOTIF (раздел 12).

Процесс оценки и решения возможных проблем SOTIF, возникающих при реальной эксплуатации, определяется на этапе эксплуатации (см. раздел 13).

На рисунке 10 показана последовательность действий по обеспечению безопасности заданной функциональности, которые требуются в настоящем стандарте; цифры в кружках обозначают его соответствующие разделы.

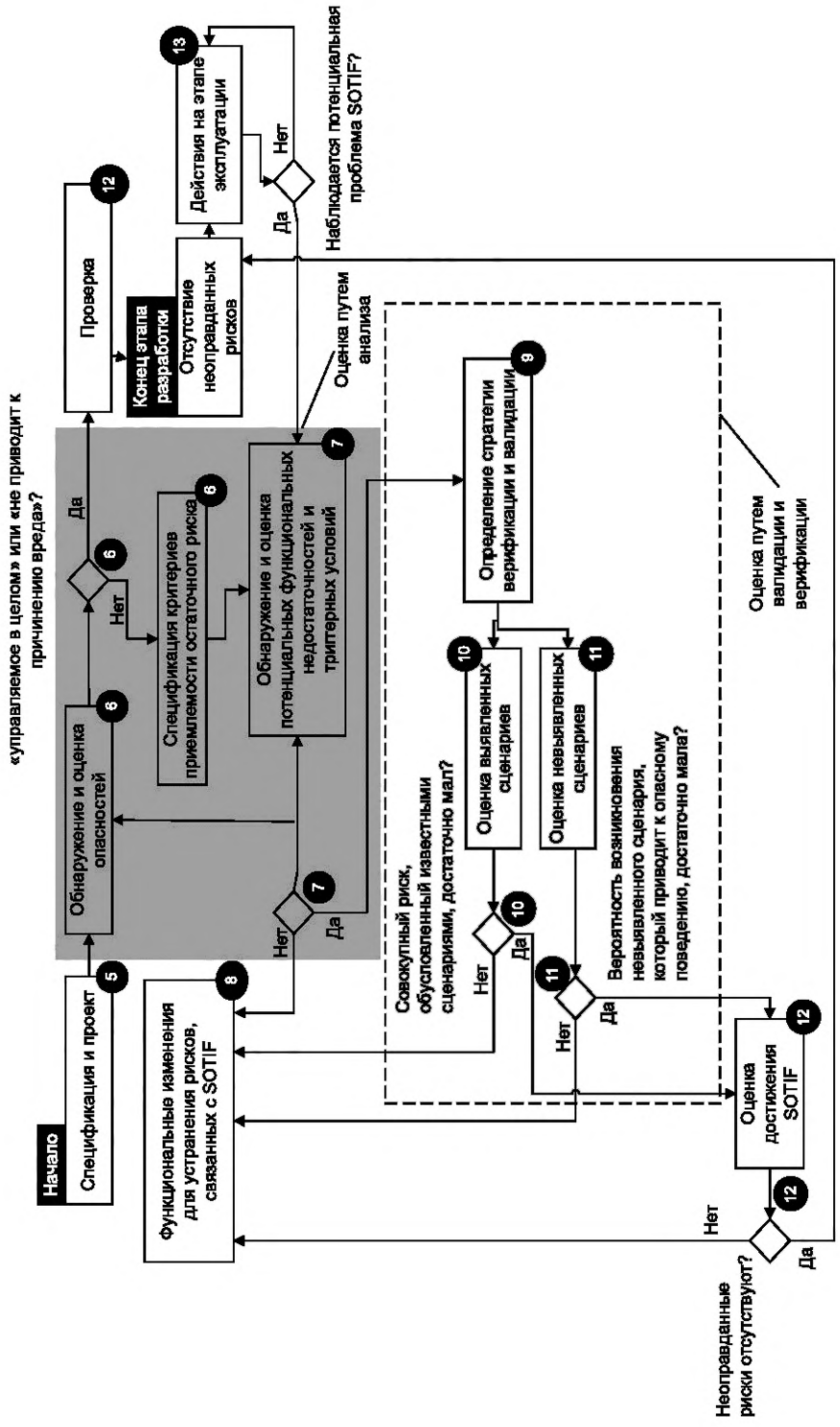


Рисунок 10 — Зависимости между действиями в настоящем стандарте

Примечание — В приложении А.3 описано упрощенное применение SOTIF на всех уровнях автоматизации.

Приложение А содержит общие рекомендации по SOTIF.

Приложение В содержит рекомендации по анализу сценариев и системы.

Приложение С содержит рекомендации по верификации и валидации SOTIF.

Приложение D содержит рекомендации по конкретным аспектам SOTIF, таким как спецификация политики вождения, влияние на машинное обучение и аспекты, которые касаются карт и V2X.

4.3.2 Нормативные положения

Соответствие настоящему стандарту подтверждается достижением целей, перечисленных в начале разделов, и предоставлением доказательств их достижения, документированных в соответствующих результатах работ. Нормативный характер целей выражается использованием ключевого слова «должен», которое указывается для требования.

Примечание — В А.1 приведены примеры таких доказательств, основанных на нотации структурирования цели (GSN).

4.3.3 Интерпретация таблиц

В некоторых таблицах настоящего стандарта перечислены методы и меры достижения определенной цели разработки. Данные таблиц, которые иллюстрируют возможные методы и меры, не являются исчерпывающими — допускается применение других эквивалентных методов и мер. Назначение таблиц — помочь команде разработчиков выбрать одну или несколько подходящих мер и методов.

Примечание — Выбор подходящего набора методов может зависеть от различных факторов, таких как сложность или уровень воздействия опасного события.

4.4 Менеджмент действий по обеспечению SOTIF и вспомогательных процессов

4.4.1 Менеджмент качества, системная инженерия и функциональная безопасность

Для разработки безопасного изделия необходимы строгие процессы проектирования и управления качеством. Они уже описаны в других стандартах, таких как IATF 16949, стандарты серии ИСО 26262 и ISO/IEC/IEEE 15288. В настоящем стандарте основное внимание уделено только тем аспектам этих процессов, которые специфичны для SOTIF.

Примечание 1 — В ходе разработки изделий действия, указанные в настоящем стандарте и стандартах серии ИСО 26262, могут выполняться параллельно. В целом реализованные меры могут влиять как на SOTIF, так и на функциональную безопасность, и оцениваются в обеих дисциплинах. В 6.1 представлено практическое руководство по параллельному внедрению стандартов серии ИСО 26262 и SOTIF.

Что касается деятельности в области менеджмента и вспомогательных процессов, то ИСО 26262-2, ИСО 26262-7 и ИСО 26262-8 можно распространять на деятельность по обеспечению SOTIF. Особое внимание в 5.3 и 10.2 уделяется каскадированию и прослеживаемости требований.

Для деятельности, связанной с SOTIF, выбираются следующие методы и меры:

- процесс SOTIF (см. рисунок 10) начинается с определения спецификации, проекта системы и ее архитектуры (см. раздел 5);
- для каждого потенциально опасного поведения заданной функциональности идентифицируются опасности и выполняется оценка риска (см. раздел 6), в ходе которой определяются опасности и соответствующие им опасные события. Если демонстрируется, что данные опасные события не приводят к неприемлемому риску причинения вреда, дополнительные проектные мероприятия не проводятся.

Примечание 2 — В разделе 6 рассматриваются не причины опасного поведения заданной функциональности, а только их последствия для безопасности. Таким образом, основное внимание уделяется оценке опасных событий, которые могут возникать в результате опасного поведения, и определению критериев приемлемости, которые должны быть удовлетворены;

- в разделе 7 определяются возможные первопричины опасного поведения заданной функциональности (см. рисунок 1) и оценивается приемлемость риска, возникающего в результате выявленных возможных функциональных недостаточностей и триггерных условий;
- в функциональность вносятся изменения (например, усовершенствование возможностей датчиков, дополнительные ограничения ODD) для улучшения SOTIF, если это считается необходимым по результатам действий, предусмотренных разделами 6, 7, 10, 11, 12 и 13 (см. раздел 8);
- разрабатывается стратегия верификации и валидации для предоставления доказательств того, что остаточный риск, связанный с SOTIF, на уровне транспортного средства находится ниже приемлемого уровня, и компоненты соответствуют своим функциональным требованиям (см. раздел 9). На основе этой стратегии можно создавать соответствующие тестовые примеры верификации и валидации для проверки, является ли результирующий риск достаточно малым (см. разделы 10 и 11);
- оценивается остаточный риск (см. раздел 12) с учетом результатов предыдущей деятельности;

- процесс выявления и решения возможных проблем SOTIF, возникающих при реальной эксплуатации, определяется на этапе разработки и реализуется на этапе эксплуатации (см. раздел 13).

Примечание 3 — Дополнительные пояснения по взаимному отношению между функциональной безопасностью в соответствии со стандартами серии ИСО 26262 и настоящим стандартом (см. А.2).

4.4.2 Деятельность по совместной разработке SOTIF

В случае совместной разработки изделия формируется соглашение о разработке (DIA) между всеми участвующими сторонами. Целью DIA является подтверждение всей ответственности за выполняемые действия в области SOTIF на ранних стадиях проекта, а также обязательства сторон, занимающихся разработкой, обмениваться надлежащей технической информацией.

В IATF 16949 представлена структура базового процесса, которую также можно рассматривать в этом контексте. В настоящем подразделе основное внимание уделяется расширению DIA для совместной разработки и эксплуатации SOTIF. В ИСО 26262:2018 описывается основа для DIA и договора поставки с точки зрения аспектов функциональной безопасности. Эту структуру можно адаптировать к SOTIF, добавляя ответственность каждой из сторон в рамках разработки и функционирования SOTIF. Ответственность каждой стороны за планирование и выполнение всех необходимых действий в области SOTIF, указанных в разделах 5—13, подлежит рассмотрению и согласованию. Указываются информация и результаты работ, которыми стороны будут обмениваться друг с другом. Эти действия могут быть выполнены с использованием процессов, описанных в 5.4.1—5.4.4 и 5.4.6 ИСО 26262-8:2018 и адаптированных к деятельности в области SOTIF. Формат документации согласовывается в начале проекта разработки.

4.4.3 Универсальный элемент, связанный с SOTIF

Для достижения SOTIF важно описать интерфейсы между различными системами [аппаратными средствами и программным обеспечением (ПО)]. Чтобы гарантировать безопасность интегрированной системы в пределах указанной ODD, границы каждой системы (например, автономной системы датчиков) подлежат тщательной оценке. Поскольку факторы внешней среды (например, ODD, сценарий) являются важными аспектами разработки SOTIF, системы и их элементы имеют разные проблемы в зависимости от иерархических уровней, на которых они находятся. С точки зрения развития эти системы и элементы можно относить к одному из следующих трех типов:

a) разработка с учетом контекста: полнокомплектная система разрабатывается с использованием всех мероприятий SOTIF согласно V-модели. В случае совместной разработки для сторон, разрабатывающих систему и ее элементы, определяются требования к спецификации и проектированию (см. раздел 5) и другим действиям (см. разделы 6—13) в зависимости от распределения ролей. В терминах стандартов серии ИСО 26262 такая разработка рассматривается как разработка «с учетом контекста»;

b) связанный с SOTIF универсальный элемент: для этих элементов можно делать допущения об их использовании во всей системе и их вкладе в заданную функциональность. Таким образом, можно делать предположения о недостатках выходных данных, связанных с SOTIF, и допустимой целевой частоте их возникновения. Эти допущения документируются и используются в качестве исходных данных для последующей разработки этих элементов. Деятельность, связанная с SOTIF, обеспечивает доказательства достижения соответствующих целевых показателей. Для связанного с SOTIF универсального элемента документируются обнаруженные триггерные условия, обусловленные ими нарушения на выходах, а также допущения об их использовании. При интеграции такого связанного с SOTIF универсального элемента достоверность допущений устанавливается в ходе действий по обеспечению SOTIF в контексте всех функциональных возможностей на уровне транспортного средства (см. ИСО 26262-10:2018, раздел 9);

c) разработка, специально не связанная с SOTIF: функциональность этих элементов может входить в состав заданной функциональности в настолько различных формах, что практически невозможно заранее оценить требования, связанные с SOTIF, без контекста, в котором эти элементы будут использоваться.

Пример — Требования, предъявляемые к графическим процессорам (GPU), зависят от системного контекста и программного обеспечения, работающего на этих графических процессорах.

5 Спецификация и проект

5.1 Цели

Целью настоящего раздела является решение следующих задач:

a) спецификация и проект должны содержать информацию, достаточную для осуществления деятельности, связанной с SOTIF;

b) спецификация и проект должны обновляться по мере необходимости после каждой итерации действий, связанных с SOTIF (см. рисунок 10).

5.2 Спецификация функциональности и факторы, которые необходимо учитывать в проекте

Спецификация и проект могут включать в себя различные аспекты, перечисленные в настоящем подразделе. Некоторые аспекты актуальны только для определенного уровня автоматизации или конкретной реализации. Кроме того, одни аспекты важны для спецификации функциональности на уровне транспортного средства, а другие — на уровне элемента.

К аспектам анализа (где применимо) относятся, в том числе:

- описание заданной функциональности, функциональности вспомогательных подсистем и компонентов, в том числе:
  - ODD;
  - уровень и особенности функции автоматического вождения, контролирующей динамику транспортного средства;
  - стратегия SOTIF на уровне транспортного средства;
  - варианты использования, в которых функция может быть активной или неактивной, и переходы между ними;
  - описание логики принятия решений (например, планирование маршрута, политика вождения — см. D.1);
- проектирование соответствующей системы и ее элементов, реализующих заданную функциональность;
- целевые характеристики установленных датчиков, контроллеров, исполнительных устройств или других входных устройств и компонентов (например, карты — см. D.3), обеспечивающих заданную функциональность.

Примечание 1 — Примерами целевых показателей автоматизированной системы вождения являются обнаружение и реагирование на критические объекты и события (например, пешеходов, транспортные средства, велосипеды, мотоциклы и дорожные знаки) в пределах ODD;

- зависимость заданной функциональности от нижеперечисленных сущностей, а также взаимодействия или интерфейсы с ними:
  - водитель;
  - интерфейс водителя (например, ЧМИ) и методов его применения для предотвращения выявленного обоснованно предсказуемого неправильного использования;
  - оператор удаленного/служебного офиса;
  - пассажиры, пешеходы, велосипедисты и другие участники дорожного движения;
  - соответствующие условия внешней среды;
  - дорожная инфраструктура и оборудование;
  - средства обмена данными с облаком, между транспортными средствами или другими коммуникационными инфраструктурами (например, V2X/X2V — см. D.4) и телематическими средствами, осуществляющими диагностику и обновление параметров во время эксплуатации;
  - средства удаленной прошивки обновлений ПО;
  - другие функции транспортного средства, которые могут препятствовать выполнению заданной функциональности, в том числе обмен информацией и соответствующие допущения об использовании;
  - обоснованно предсказуемое неправильное использование (явное и неявное);
  - возможные недостаточности производительности, выявленные триггерные условия и контрмеры системы и ее элементов.

Примечание 2 — Некоторые возможные недостаточности производительности и риски, выявленные в ходе деятельности SOTIF, могут приниматься и не иметь соответствующих «контрмер». В таких случаях их можно документировать в составе спецификации и проекта;

- архитектура системы и транспортного средства, реализующая заданную функциональность;
- концепция предупреждения и постепенного снижения эффективности:
  - стратегии предупреждения;
  - резервный вариант динамической задачи управления: условия и схемы перехода управления от автоматизированной системы вождения к водителю или другой системе в рамках соответствующих вариантов использования;
  - схемы условий минимального риска (например, автономный выезд с полосы движения и парковка, остановка в пути, пользователь, готовый к резервному варианту);
  - система мониторинга водителя и ее оперативное влияние на стратегию переключения на резервный вариант;
- процедуры, поддерживающие сбор и мониторинг данных во время и после разработки заданной функциональности:
  - цели и требования к сбору данных;
  - архитектура, реализация и механизмы, поддерживающие сбор необходимых данных перед выпуском SOTIF;
  - требования, проект и механизмы, которые поддерживают сбор данных на этапе эксплуатации для анализа SOTIF (см. 13.5), в том числе облачные, «эфирные» технологии и технологии радиосвязи;
- механизм, проект и требования, которые поддерживают возможности снижения риска во время эксплуатации.

5.3 Проект системы и факторы архитектуры

Спецификация и проект создают адекватное представление о системе, ее элементах, функциях и целевых показателях, которое позволяет выполнять действия на последующих этапах. Сюда входит исчерпывающий список выявленных функциональных недостаточностей, связанных с ними триггерных условий и, где применимо, мер противодействия им. Одни потенциальные функциональные недостаточности, триггерные условия и контрмеры выявлены и документально оформлены до начала процесса, связанного с SOTIF, в то время как другие выявляются в результате деятельности SOTIF. Система проектируется таким образом, что контрмеры для смягчения влияния выявленных функциональных недостаточностей реализуются для всей системы.

Каждая итерация деятельности, связанной с SOTIF (см. рисунок 10), может инициировать проведение инженерных работ, а они, в свою очередь, приводить к обновлениям спецификаций и проектов на любом соответствующем уровне. На каждой итерации должны использоваться спецификация и проект, которые обновлены на всех соответствующих уровнях и отражают всю информацию, обнаруженную на предыдущих итерациях.

Сотрудничество между сторонами разработки (OEM, уровень 1, уровень N) необходимо для обнаружения возможных функциональных недостаточностей интегрированной системы, компонента или элемента и разработки мер противодействия этим недостаткам на этапах разработки (см. 4.4). Соответствующие части проекта и спецификации передаются разработчикам систем и компонентов нижнего уровня. Допущения об использовании, прогнозируемом неправильном использовании и возможных недостаточностях производительности передаются с одного уровня иерархии на следующие до OEM-изготовителя включительно после каждого цикла/итерации разработки.

По мере того как в ходе действий по обеспечению SOTIF обнаруживаются новые функциональные недостаточности и триггерные условия (см. раздел 7), а также определяются меры по улучшению SOTIF (см. раздел 8), спецификация и проект обновляются в рамках каждого цикла разработки, как показано на рисунке 10.

Результаты работы по обеспечению SOTIF связаны со спецификацией и проектом, если они влияют на спецификацию и проект (как определено в 5.2), в том числе на соответствующие ранее существовавшие материалы. Это гарантирует, что к следующему циклу итерации вся информация из предыдущих итераций будет собрана и спецификация будет готова.

Примечание — Можно демонстрировать прослеживаемость и полноту спецификации и проекта (результаты работы по 5.5) путем привязки к мерам SOTIF (результаты работы по 8.5), которые можно дополнительно связывать:

- с соответствующей проектной документацией;
- результатами работы:
  - из раздела 6 — оценка риска опасного поведения (например, для достижения S=0, C=0 или получения менее строгих критериев приемлемости);
  - раздела 7 — оценка реакции системы на выявленные триггерные условия (например, ссылка на анализ триггерного условия, указывающего на неприемлемый риск);
  - разделов 9 и 10 — результаты верификации и валидации для выявленных опасных сценариев (например, ссылка на отчет о верификационных испытаниях, который демонстрирует значения характеристик, неприемлемые с точки зрения требований);
  - разделов 9 и 11 — результаты валидации для невыявленных опасных сценариев (например, ссылка на отчет о валидационных испытаниях, который демонстрирует значения характеристик, неприемлемые с точки зрения опасного сценария или целей валидации);
  - раздела 12 — заключение о выпуске SOTIF (например, ссылка на отчет, в котором документированы причины отклонения запроса на выпуск);
  - раздела 13 — процесс мониторинга в процессе эксплуатации (например, ссылка на отчет, в котором документирован новый опасный сценарий, обнаруженный при мониторинге в процессе эксплуатации).

Технические допущения о SOTIF, которые относятся к оценке риска в 6.4 и 7.4, не обязательно связаны с мерами SOTIF в 8.3, но, тем не менее, могут быть отнесены к спецификации и проекту. Этот процесс могут поддерживать инструментальные средства, которые обеспечивают проектирование на основе моделей и поддерживают прослеживаемость между различными артефактами модели (требованиями, компонентами, интерфейсами, анализом, тестовыми примерами и результатами).

5.4 Недостаточности производительности и меры противодействия

Проект включает в себя результаты анализа возможных недостаточностей производительности, которые обусловлены выходным значением элемента и могут приводить к опасному поведению на уровне транспортного средства. Неисчерпывающий список возможных недостаточностей производительности:

- недостаточность классификации;
- недостаточность измерения;
- недостаточность отслеживания;
- недостаточность выбора цели;
- недостаточность в оценке кинематики;
- обнаружение ложноположительных результатов (например, призраков, фантомных объектов);
- обнаружение ложноотрицательных результатов;
- ограничения на уровне политики вождения, такие как учет «закрытых» областей.

Руководство по возможным методам выявления функциональных недостаточностей и соответствующего опасного поведения на уровне транспортного средства можно найти в В.3, приложение В. Функциональные недостаточности наиболее актуальны, когда система работает в пределах заданной проектируемой области эксплуатации. То, как система обнаруживает выход из заданной проектируемой области эксплуатации и работает во время таких переходов, имеет значение для полноты анализа.

Разработка системы основана на допущениях о недостаточностях производительности в проекте. Принимаются меры по устранению этих недостаточностей для обеспечения SOTIF. Проект и меры, которые интегрированы в спецификацию и проект, снижают остаточный риск и повышают общую надежность (см. рисунки 5 и 6).

Примечание 1 — Методы и меры обнаружения возможных функциональных недостаточностей и их триггерных условий подробно описаны в разделе 7.

Примечание 2 — Методы и меры устранения функциональных недостаточностей, в том числе резервирование, разнообразие и дополнительные элементы, описаны в разделе 8.

Примечание 3 — Содержание спецификации и проекта обеспечения SOTIF проверяется в соответствии с разделом 10.

Ниже приведены примеры недостаточностей производительности и возможные меры противодействия. Эта информация включается в документ(ы) по спецификации и проектированию:

Пример 1 — Алгоритм определения границ полосы движения на шоссе для таких функций, как удержание полосы движения, может неправильно определять полосу из-за мусора на проезжей части, однако можно уменьшать отклонения от полосы движения, которые приводят к столкновению,

с помощью других функций автоматического вождения, таких как использование карты высокой четкости и локализация для подтверждения полосы движения, координация траектории транспортного средства с траекториями предшествующих транспортных средств, алгоритмы предотвращения столкновений, поддерживающие интервал с другими транспортными средствами, даже если это предполагает выезд из воспринимаемой полосы движения, и т. д.

Пример 2 — Алгоритм обнаружения объекта идентифицирует человека на скейтборде как пешехода, но отклоняет объект, поскольку его скорость неправдоподобна. В этом случае можно смягчить столкновение со скейтбордистом с помощью системы с разделением алгоритма обнаружения объекта и алгоритмов восприятия и обработки, а также других различных проверок достоверности.

Пример 3 — Иногда для предупреждения водителей используется пешеходный переход, нарисованный в виде трехмерной оптической иллюзии (см. рисунок 11). Изображение специально нанесено на дорогу так, чтобы обмануть восприятие человека, однако оно может обманывать систему технического зрения и заставлять ее обнаруживать несуществующий объект. В этом случае механизм анализа оптического потока может предотвращать ложное торможение. Анализ оптического потока, а также радиолокационное распознавание окружающей среды являются альтернативными контрмерами в таких случаях, которые возникают из-за ограничений классификации.

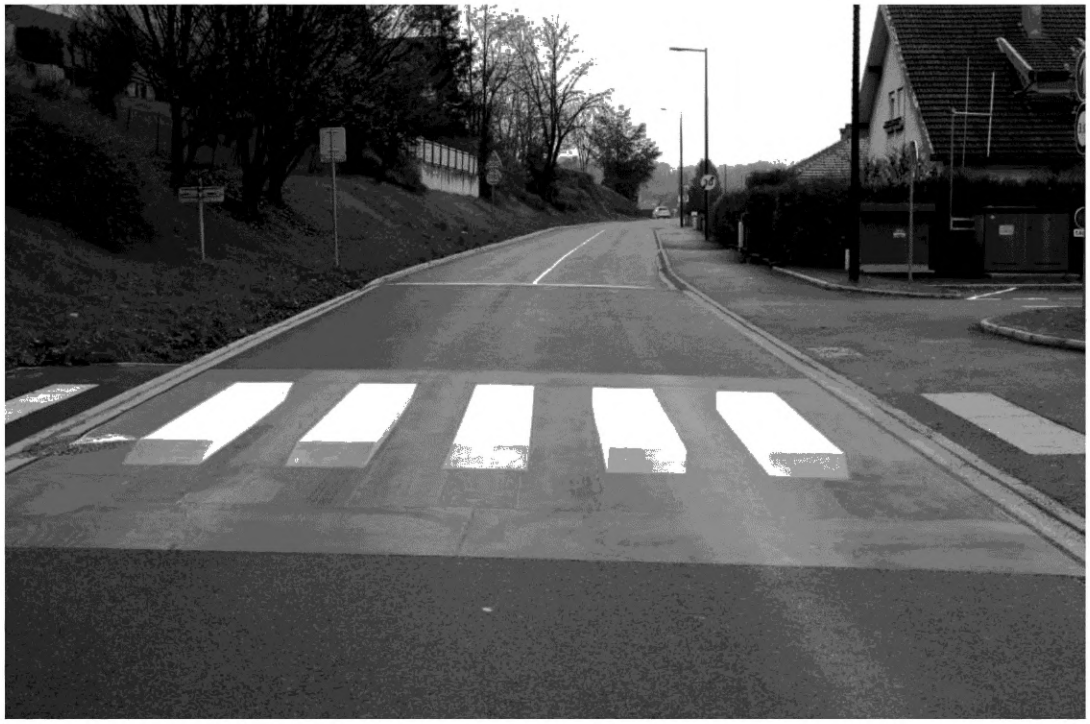


Рисунок 11 — Пример рисунка с оптической иллюзией, которая может обмануть систему технического зрения

Пример 4 — Использование автоматизированной системы парковки, когда из открытого багажника выступает предмет, может приводить к опасному событию. Пример контрмеры в проекте системы — разрешение на автоматическую парковку только при закрытом багажнике.

5.5 Результаты работы

Результатом работы являются спецификация и проект, отвечающие целям 5.1 a) и 5.1 b).

Примечание 1 — Можно разделять спецификацию и проект на несколько документов или связывать их с несколькими документами. Например, спецификации требований, функциональные спецификации и проектные спецификации систем, связанных с SOTIF.

Примечание 2 — Можно интегрировать спецификацию мер по смягчению последствий обеспечения SOTIF в существующую проектную документацию по функциональной безопасности, например в концепцию функциональной безопасности и/или концепцию технической безопасности.

6 Идентификация и оценка опасностей

6.1 Цели

Целью настоящего раздела является достижение следующих результатов:

a) опасности, которые возникают из-за заданной функциональности, определенной на уровне транспортного средства, должны систематически идентифицироваться;

b) риск, который возникает в результате опасного поведения заданной функциональности, и соответствующие сценарии, в которых опасное поведение может приводить к причинению вреда, должны систематически выявляться и оцениваться. Должны указываться параметры, определяющие обстоятельства, при которых поведение заданной функциональности считается опасным.

Пример — Такими параметрами могут являться отклонение скорости или минимальные расстояния до других объектов;

c) должны быть указаны критерии приемлемости остаточного риска.

6.2 Общие положения

Для достижения целей настоящего раздела можно рассматривать следующую информацию:

- спецификация и проект в соответствии с 5.5;
- доступные данные для определения критериев приемлемости.

6.3 Идентификация опасностей

Опасности, которые возникают в результате недостаточностей производительности, систематически определяются на уровне транспортного средства. Эта систематическая идентификация основана прежде всего на знаниях о функции и ее возможных отклонениях, которые возникают в результате функциональных недостаточностей. Этого можно достичь, применяя методы, которые указаны в ИСО 26262-3. Общие элементы анализа опасностей, соответствующие требованиям стандартов серии ИСО 26262 и настоящего раздела, представлены на рисунке 12. На рисунке 13 показана система автономного экстренного торможения (AEB), которая иллюстрирует использование элементов рисунка 12. В примере показаны две опасности, возникающие в результате одного и того же опасного поведения. Применение анализа опасностей подробнее описано в A.2.5, приложение A, на примере AEB.

Пример 1 — Система AEB может создавать опасности, которые возникают как из-за опасного поведения заданной функциональности, так и из-за неисправности. Опасность, которая возникает в результате непреднамеренного торможения в пределах и за пределами функциональных ограничений, можно анализировать с точки зрения функциональной безопасности при анализе опасностей и оценке рисков. Та же опасность, связанная с непреднамеренным торможением в пределах функциональных ограничений, также подлежит анализу SOTIF.

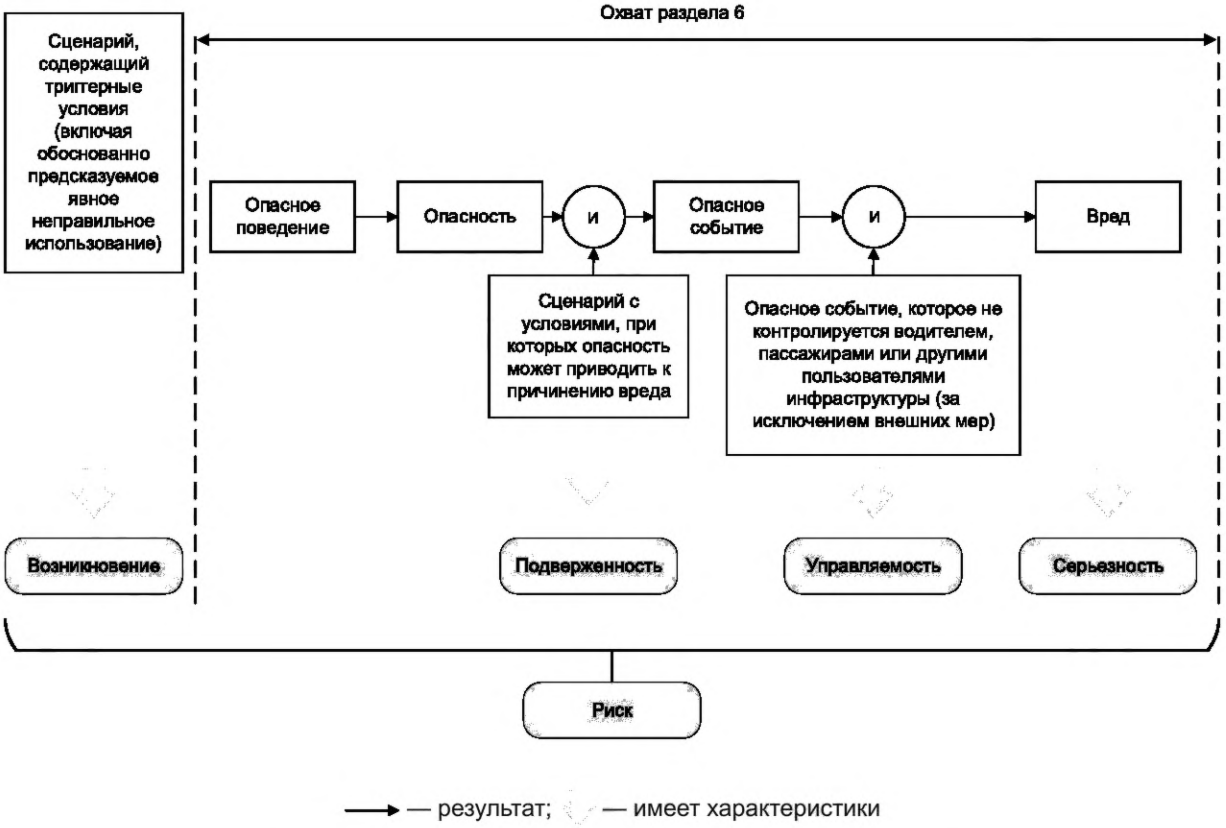


Рисунок 12 — Иллюстрация общих элементов анализа опасностей в стандартах серии ИСО 26262 и настоящем стандарте

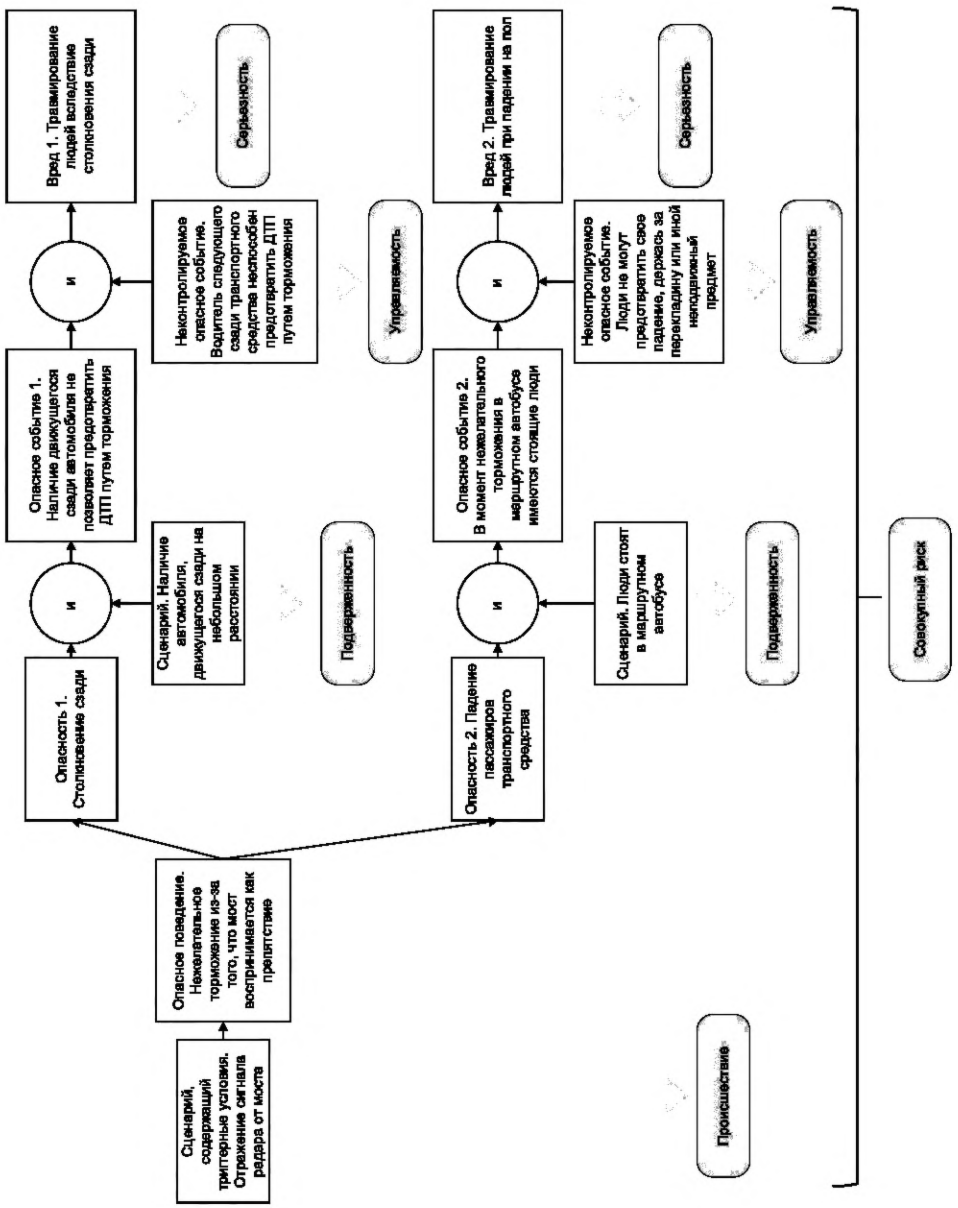
Примечание 1 — В отличие от ИСО 26262-3, при анализе опасности, связанной с SOTIF, для опасного события не определяется уровень полноты безопасности транспортного средства (ASIL). Однако параметры серьезности (S), воздействия (E) и управляемости (C) можно использовать для корректировки действий по валидации.

Примечание 2 — Происшествие отражает вероятность возникновения триггерных условий на этапе эксплуатации функции.

Существует важное различие между возникновением триггерного условия и воздействием сценария, при котором опасность может привести к причинению вреда. В целом триггерные условия не являются независимыми от сценариев, поэтому, чтобы использовать воздействие сценария в качестве обоснования для снижения риска, при оценке учитывается статистическая зависимость между вероятностями нахождения в сценарии и возникновения триггерного условия.

Пример 2 — Невозможно предполагать какую-либо статистическую независимость для триггерного условия функции Highway pilot, когда сценарием является движение по шоссе.

В некоторых конкретных случаях можно допускать статистическую независимость, как показано на рисунке 13.



→ — результат; ⋯ — имеет характеристики

Рисунок 13 — Пример AEB с использованием элементов рисунка 12

Параметр C можно использовать для оценки возможности управлять опасностями, связанными с SOTIF (см. 10.6 и таблицу 10). Для подтверждения оценок управляемости можно использовать исследования или допущения о реакции участников дорожного движения.

Примечание 3 — Пример на рисунке 13 показывает, что результирующий риск может быть оценен на двух уровнях: во-первых, риск, связанный с конкретной опасностью в данном сценарии, и, во-вторых, общий риск, связанный с опасным поведением и включающий оценку нескольких опасностей и соответствующих сценариев.

Помимо систематической идентификации возможных функциональных отклонений можно выявлять дополнительные опасности (в том числе обоснованно предсказуемое неправильное использование) путем рассмотрения взаимодействия водителя или пользователя с системой. Обоснованно

предсказуемое неправильное использование имеет иную причинную связь с опасностью. Явное неправильное использование заданной функциональности приводит к возникновению триггерного условия, а неявное неправильное использование заданной функциональности — к снижению управляемости или повышению серьезности опасного события в результате опасного поведения (например, невнимательный водитель или водитель, который неправильно понимает ограничения функции).

Обнаружение обоснованно предсказуемого неявного неправильного использования и анализ его последствий рассматриваются в разделе 7.

Примечание 4 — Общие рекомендации по анализу обоснованно предсказуемого неправильного использования содержатся в 7.3.4 и В.1, приложение В.

6.4 Оценка рисков

Оценка риска направлена на определение количественной характеристики риска, связанного с опасным поведением в определенных сценариях; это помогает определять критерии приемлемости риска, связанного с SOTIF.

Примечание 1 — В этой оценке участвует опасное поведение, возникающее в результате функциональной недостаточности на уровне транспортного средства (если таковая имеется).

Тяжесть вреда и управляемость опасными событиями можно оценивать с помощью метода, описанного в ИСО 26262-3:2018 (раздел 6). Несмотря на использование одного и того же метода анализа, наблюдаемый результат и расчетные параметры для конкретной опасности при анализе SOTIF могут различаться.

Примечание 2 — В ИСО 26262-3 вводятся классы управляемости, серьезности и воздействия. В контексте раздела 6 имеет значение только то, является ли опасное событие в целом управляемым и приводит ли к нанесению вреда. Воздействие не является определяющим параметром для оценки риска в разделе 6. Поскольку риск оценивается в сценариях, их выбор уже подразумевает, что воздействие на них связано с SOTIF, иначе они не рассматриваются в анализе.

Примечание 3 — Воздействие на конкретные сценарии может учитываться при определении целей валидации (см. раздел 9).

Пример 1 — Можно уменьшить тяжесть удара в заднюю часть впереди идущего транспортного средства, вызванного его автоматическим экстренным торможением, ограничивая степень воздействия тормозной системы. Ее предельную величину можно рассматривать как меру безопасности, направленную на повышение управляемости, или функциональную модификацию заданного поведения. При анализе опасности этот предел рассматривается как часть заданного поведения; напротив, отказы, связанные с соблюдением предела, рассматриваются в других стандартах безопасности — например, в стандартах серии ИСО 26262.

Серьезность и управляемость опасного события учитываются при определении, является ли возникающий риск неоправданным в конкретном сценарии. Оценка серьезности и управляемости учитывает функциональную спецификацию (соответствующую спецификации и проекту, приведенным в разделе 5). Отсутствие неоправданного риска устанавливается, если управляемость оценивается как «в целом управляемая» (т. е. C = 0) или степень тяжести оценивается как «отсутствие причиненного вреда» (т. е. S = 0). Во всех остальных случаях опасное событие считается связанным с SOTIF. Соответствующее опасное поведение описывается с использованием измеряемых параметров, таких как отклонения скорости и минимальные расстояния до других объектов. Оценка управляемости включает в себя «отсутствие реакции» или «замедленную реакцию» участвующих лиц при управлении опасностью, например в результате обоснованно предсказуемого неявного неправильного использования. Эта оценка также может учитывать внешние меры.

Пример 2 — При классификации опасных событий может учитываться состояние внешней среды, которое не обрабатывается усовершенствованной системой помощи водителю (ADAS) безопасным образом и, следовательно, требует от водителя возобновить управление.

Запоздалая или неадекватная реакция водителя, в том числе время, необходимое водителю для достижения достаточной осведомленности о ситуации и восстановления работоспособного состояния, может влиять на оценку управляемости и является предметом анализа, связанного с SOTIF.

Если после функциональной модификации (см. рисунок 10) опасное событие оценивается как S = 0 или C = 0, опасность устранена в достаточной степени.

Пример 3 — В таблице 3 приведен пример оценки возможных последствий опасного события, связанного с SOTIF, для системы AEB.

Таблица 3 — Пример опасного события

Опасное поведение	Возможные последствия	Серьезность		Контролируемость		Неоправданный риск?
		Рейтинг	Примечание	Рейтинг	Примечание	
Непреднамеренная активация AEB на скорости *x* м/с^2 в течение *y* секунд при движении по шоссе	Столкновение сзади со следующим автомобилем	C > 0	Эффективная скорость удара: *v* ≥ *x* км/ч	C > 0	Следующее транспортное средство может оказаться не в состоянии затормозить, чтобы избежать столкновения	Да

6.5 Спецификация критериев приемлемости остаточного риска

Если параметры риска не оцениваются как S = 0 или C = 0, то для рисков, связанных с опасным поведением, указываются критерии приемлемости и действия продолжаются в соответствии с разделом 7.

Обоснования для классификации S = 0 или C = 0 рассматриваются в рамках процесса SOTIF и включают в себя рассмотрение доказательств классификации (например, результатов испытаний или анализа).

В критериях приемлемости учитывают:

- применимые государственные и отраслевые правила;
- является ли функция новой или занимающей устойчивое положение на рынке;
- является ли неоправданным риск для людей, которые могут подвергаться ему (например, для владельца транспортного средства, оператора, пешехода или пассажира в автоматизированной системе общественного транспорта);
- критерии приемлемости уже установленных функций;
- характеристики безупречно действующего водителя.

Пример 1 — Таким критерием приемлемости может являться максимальное количество несчастных случаев в час. Соответствующая стратегия верификации и валидации определена в разделе 9 и основана на установленных критериях приемлемости.

К подходам, которые можно рассматривать при определении критериев приемлемости, относятся:

- имеющиеся данные о дорожном движении для целевого рынка (например, статистика аварий, анализ дорожного движения) (см. С.2.2.4); и
- ранее существовавшие критерии аналогичных функций, действующих в данной области.

Пример 2 — Количество ложноположительных срабатываний на x км аналогичной системы предупреждения о столкновениях, которая находится в серийном производстве (распределение аналогичных испытаний).

Соответствующие количественные критерии приемлемости можно выбирать при наличии достоверного обоснования. Общее обоснование может включать в себя одно или несколько следующих отдельных обоснований:

- принцип толерантности к риску, такой как GAMAB (Globalement au moins aussi bon) или GAME (Globalement au moins équivant); оба французских термина имеют значение «в целом, как минимум, не хуже». По этому принципу остаточный риск (в отношении безопасности) любой новой системы не выше, чем у существующих систем, имеющих сопоставимые функциональные возможности или опасности;
- положительный баланс рисков. Применение такого принципа толерантности к общему остаточному риску, который учитывает все опасности новой системы, позволяет находить надлежащие компромиссы между рисками. Система может быть выпущена, даже если остаточный риск для конкретной

опасности увеличивается, при условии, что это компенсируется снижением одного или нескольких других остаточных рисков;

- принцип ALARP. Система управления рисками ALARP может обеспечивать полезный принцип снижения рисков, особенно в отношении разработки и внедрения новых технологий там, где в настоящее время не существует надлежащей практики. В принципе ALARP достижение нулевого риска признается невозможным, и этот принцип направлен на снижение риска до уровня, который считается практически достижимым, путем сопоставления риска с усилиями, необходимыми для его дальнейшего снижения;
- принцип MEM (минимальной эндогенной смертности). Принцип MEM основан на идее о том, что внедрение технической системы не должно существенно увеличивать уровень смертности в обществе. Количественные критерии приемлемости вероятности летального исхода, вызываемого технологической системой, выводятся из минимальной вероятности летального исхода от естественных причин.

Примечание 1 — Обоснование в контексте настоящего стандарта может включать только риски, связанные с SOTIF, и не включает риски из других областей безопасности (например, электробезопасности).

Примечание 2 — В С.2 и С.6 приведены примеры определения и оценки критериев приемлемости и целей валидации.

Примечание 3 — Описание GAMAB, ALARP и MEM можно найти в EH 50126-2:2017, A.1 (RAMS) [4].

Примечание 4 — В качестве надежного обоснования может использоваться риск для всего парка или риск, связанный с отдельным транспортным средством. Даже если у автопарка очень низкая вероятность возникновения триггерного условия в рамках сценария, реакция системы может быть неприемлемой, если вероятность возникновения такого сценария высока для конкретного транспортного средства.

6.6 Результаты работы

6.6.1 Опасности на уровне транспортного средства, соответствующие цели по 6.1, перечисление a).
6.6.2 Оценка риска опасного поведения для достижения цели по 6.1, перечисление b).
6.6.3 Критерии приемлемости, соответствующие цели по 6.1, перечисление c).

7 Идентификация и оценка потенциальных функциональных недостаточностей и их триггерных условий

7.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

a) должны быть идентифицированы потенциальные недостаточности спецификации, недостаточности производительности и их триггерные условия, в том числе обоснованно предсказуемое явное неправильное использование, а также определены те из них, которые приводят к опасному поведению;

b) ответ системы должен быть оценен на соответствие приемлемости SOTIF.

Примечание 1 — Сюда входит выявление функциональных недостаточностей и их триггерных условий, относящихся к контексту обоснованно предсказуемых случаев явного и неявного неправильного использования.

Примечание 2 — В этой деятельности рассматриваются потенциальные недостаточности спецификации заданной функциональности на уровне транспортного средства, а также потенциальные недостаточности спецификации или недостаточности производительности элементов Э/Э-системы.

7.2 Общие положения

Для достижения целей настоящего раздела может быть рассмотрена следующая информация:

- спецификация и проект в соответствии с 5.5;
- опасности на уровне транспортного средства в соответствии с 6.6.1;
- оценка риска опасного поведения, в том числе выявленные обоснованно предсказуемые случаи явного и неявного неправильного использования, в соответствии с 6.6.2;
- критерии приемлемости в соответствии с 6.6.3;
- выявленные потенциальные функциональные недостаточности системы и ее элементов, а также их выявленные потенциальные триггерные условия (в том числе обоснованно предсказуемое явное неправильное использование), которые могут привести к опасному поведению, на основе внешней информации или приобретенного опыта (например, 13.5).

7.3 Анализ потенциальных функциональных недостаточностей и их триггерных условий

7.3.1 Общие положения

Потенциальные функциональные недостаточности и их триггерные условия систематически анализируются. В этом анализе могут учитываться практический опыт и знания, полученные из аналогичных проектов или от экспертов.

Этот анализ может выполняться параллельно, начиная:

- с выявленных потенциальных недостаточностей спецификаций и производительности для определения сценариев (содержащих их триггерные условия), приводящих к выявленному опасному поведению;
- выявленных внешних условий и обоснованно предсказуемого неправильного использования для определения потенциальных недостаточностей спецификации и недостаточностей производительности.

Примечание 1 — Более подробная информация о методах анализа SOTIF приведена в приложении В. Также см. ИСО 34502 [5].

Примечание 2 — Можно подкреплять анализ индуктивными, дедуктивными или эвристическими методами.

Примечание 3 — Можно выполнять количественный и/или качественный анализ.

Примечание 4 — Можно определять количественные целевые показатели вплоть до уровня элементов, исходя из критериев приемлемости или целевых показателей валидации на уровне транспортного средства.

Примечание 5 — Подходящая абстракция (например, создание и использование классов эквивалентности или подмножеств) всех соответствующих параметров вариантов использования может являться полезной для обработки большого количества сочетаний вариантов использования.

Примечание 6 — Для концентрации на правдоподобных случаях использования, которые могут приводить к потенциально опасному поведению, можно использовать статистику дорожного движения.

Примечание 7 — Этот анализ можно подкреплять моделированием, например с использованием методов Монте-Карло.

Для выявления и оценки потенциальных недостаточностей спецификации, недостаточностей производительности, недостаточностей выхода и их триггерных условий может применяться подходящее сочетание методов, представленных в таблице 4.

Таблица 4 — Методы анализа потенциальных функциональных недостаточностей и их триггерных условий

Методы	
A	Анализ требований
B	Анализ ODD, вариантов использования и сценариев [a]
C	Анализ статистики аварий [b]
D	Анализ граничных значений
E	Анализ классов эквивалентности
F	Анализ функциональных зависимостей
G	Анализ общих триггерных условий [c]
H	Анализ возможных триггерных условий на основе практического и приобретенного опыта [d]
I	Анализ архитектуры системы (в том числе резервирования)
J	Анализ конструкции датчиков потенциальных технологических ограничений [e]
K	Анализ алгоритмов и их результатов или решений
L	Анализ старения системы [f]
M	Анализ возможных изменений внешней среды в течение срока службы транспортного средства (например, помехи)
N	Анализ внешних и внутренних интерфейсов [g]

Окончание таблицы 4

Методы	
O	Анализ конструкции приводов и возможных ограничений
P	Анализ сценариев аварий [h]
Q	Анализ обоснованно прогнозируемого неправильного использования [i]

[a] Он включает анализ границ ODD.

[b] Например, STATS19 (Великобритания) (см. [6]), GIDAS (Германия) (см. [7]), GES (США) (см. [8]), CARE (см. [9]), IGLAD (см. [10]).

[c] Множественные недостаточности производительности или недостаточности спецификации могут активироваться одним триггерным условием (например, сильный дождь может повлиять на работу различных датчиков, таких как радар и камера).

[d] При этом учитывается анализ сопоставимых систем на рынке, предшествующих систем и проектов, а также претензий клиентов.

[e] При этом учитываются технологические ограничения (например, угловое разрешение из-за формирователя изображения, ограничения конструкции антенны радара или отсутствие изоляции от внешней среды, такой как гидроизоляция и вибрация), а также технические ограничения из-за монтажа (например, слепые зоны, возникающие из-за того, что датчик не охватывает 360° поля зрения вокруг автомобиля).

[f] Например, объектив камеры, который тускнеет из-за эффекта старения в указанных пределах.

[g] Например, карты «транспортное средство транспортное средство», «транспортное средство инфраструктура», беспроводные карты.

[h] Например, на основе анализа записей, поступающих из системы хранения данных для автоматизированного вождения/регистратора данных о событиях (DSSAD/EDR).

[i] Методы анализа перечислены в таблице 5.

Примечание 8 — Можно адаптировать методы анализа безопасности для выявления и оценки потенциальных функциональных недостаточностей, их триггерных условий и их влияния на опасности [например, анализ опасностей с помощью дерева причин, анализ дерева событий (ETA), индуктивный анализ SOTIF или анализ опасностей и работоспособности (HAZOP)]. Примеры адаптации методов анализа безопасности приведены в B.3.

В зависимости от архитектуры системы возможные функциональные недостаточности элемента можно разделить:

- на единичные функциональные недостаточности;
- множественные функциональные недостаточности.

Эта классификация может помочь в определении адекватной функциональной модификации для достижения SOTIF (см. раздел 8). С ее помощью можно получать требования на уровне элемента, необходимые для достижения SOTIF на уровне транспортного средства (см. раздел 5).

Пример 1 — Учитывая критерии приемлемости, определенные SOTIF, которые должны быть достигнуты на уровне транспортного средства, можно распределять целевые показатели между различными участвующими элементами, например, как показано на рисунке 14. Каждому датчику можно назначать менее строгие целевые показатели (например, уровень ложноположительного обнаружения) по сравнению с системой с одним датчиком.

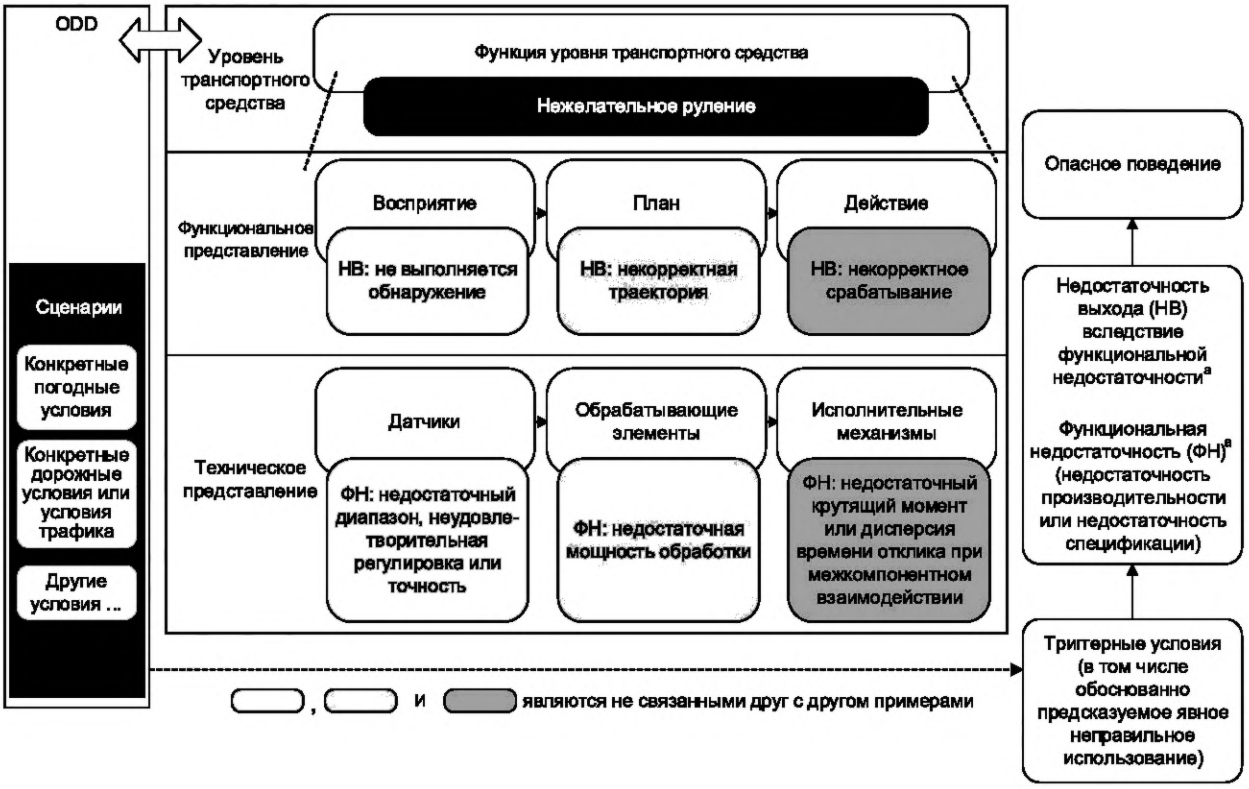
Рисунок 14 — Пример архитектуры системы с объединением двух разнородных датчиков

Эту классификацию также можно использовать при определении стратегии валидации, где можно уменьшать целевые показатели валидации для множественных функциональных недостаточностей с учетом их независимости (см. раздел 9 и С.6.3, приложение С).

Могут существовать различные триггерные условия для недостаточностей производительности или недостаточностей спецификации, которые приводят к опасному поведению. Кроме того, выявленные условия внешней среды и обоснованно прогнозируемое неправильное использование могут вызвать некоторые недостаточности производительности или недостаточности спецификации на уровне транспортного средства или элемента. На уровне транспортного средства или элемента между опасным поведением, его триггерными условиями и потенциальными недостаточностями производительности или недостаточностями спецификации устанавливается и поддерживается прослеживаемость.

На рисунке 15 приведена иллюстрация с примером связи между опасностями, их триггерными условиями и потенциальными недостаточностями производительности или недостаточностями спецификации на уровне транспортного средства или элемента.

Для структурированного представления материала в следующих подразделах стандарта отдельно рассматриваются алгоритмы планирования, датчики и исполнительные механизмы. При необходимости также можно использовать возможные недостаточности производительности и их триггерные условия в списке датчиков и исполнительных механизмов для анализа алгоритма планирования и наоборот.



[a] Функциональные недостаточности (как свойства проекта) могут существовать во всех представлениях и на всех уровнях абстракции.

Рисунок 15 — Иллюстрация связи между возможными функциональными недостаточностями и их триггерными условиями

7.3.2 Возможные функциональные недостаточности и их триггерные условия, связанные с алгоритмами планирования

В процессе анализа могут рассматриваться, среди прочих, следующие категории:

- внешняя среда и местоположение;
- дорожная инфраструктура;
- городская или сельская инфраструктура;

- автомагистральная инфраструктура;
- поведение водителя или пользователя (включая обоснованно предсказуемое неправильное использование);
- возможное поведение других водителей или участников дорожного движения;
- сценарий вождения (например, строительная площадка, авария, пробка с аварийным коридором, движение транспортного средства по встречной полосе);
- известные ограничения алгоритма планирования (например, неспособность обрабатывать возможные сценарии или недетерминированное поведение);
- известные недостаточности спецификации машинного обучения;
- известные недостаточности данных измерений для машинного обучения;
- известные функциональные недостаточности и функциональные улучшения.

7.3.3 Возможные функциональные недостаточности и их триггерные условия, связанные с датчиками и исполнительными устройствами

В процессе анализа могут быть рассмотрены, среди прочего, следующие категории:

- домен штатной эксплуатации (ODD);
- погодные условия;
- механические неисправности (например, шум на выходе датчика из-за вибрации вследствие расположения датчика на транспортном средстве);
- грязь на датчиках;
- электромагнитные помехи (ЭМИ);
- помехи от других транспортных средств или источников (например, радаров или лидаров);
- акустические помехи;
- блики;
- некачественное отражение;
- точность;
- диапазон;
- время отклика;
- влияние прочности, износа, старения на характеристики;
- документально обоснованные возможности (применимо к исполнительным механизмам — например, максимально допустимое тормозное давление в гидравлической тормозной системе при заданной функциональности);
- объединение данных от нескольких датчиков; и
- относительное расположение и установка датчиков.

Пример 1 — Дождь и снег могут влиять на работу радара.

Пример 2 — Восходящее солнце впереди автомобиля может влиять на работу видеокамеры.

Пример 3 — Плотное шерстяное пальто на пешеходе может влиять на работу ультразвуковых датчиков.

Пример 4 — Неправильное относительное расположение может влиять на многие типы датчиков.

Примечание 1 — Возможно, опасное поведение может возникать в результате сочетания известных потенциальных функциональных недостаточностей и триггерных условий.

Примечание 2 — Конкретные категории анализа см. в приложении В. Для каждой категории список подробных недостаточностей определяется на основе знаний и опыта (в том числе знаний, полученных в ходе аналогичных проектов и на практическом опыте).

Примечание 3 — Если входной сигнал датчика, обеспечиваемый элементами инфраструктуры, важен для функций автоматического вождения (AD) или ADAS, настоящий пункт также применим в данном случае для анализа функциональных недостаточностей.

Кроме того, можно выполнять систематический анализ каждого воздействия внешней среды в диапазоне возможных значений (как в возможных, так и в наблюдаемых сценариях).

7.3.4 Анализ обоснованно предсказуемого явного или неявного неправильного использования

Обоснованно предсказуемое явное или неявное неправильное использование заданной функциональности может приводить к неоправданному уровню риска.

С одной стороны, анализ явного неправильного использования рассматривается в разделе 7 как часть анализа его возможных триггерных условий. С другой стороны, возможные функциональные недостаточности, которые могут приводить к неэффективности мер против неявного неправильного использования, также относятся к области применения раздела 7.

Причинами обоснованно предсказуемого явного или неявного неправильного использования могут являться:

- непонимание системы пользователями; например, водителя вводит в заблуждение схожая система на рынке с другими правилами эксплуатации;
- неправильные ожидания пользователя от системы; например, недостаточная, неуместная или неверная информация, предоставляемая водителю;
- потеря концентрации;
- чрезмерная зависимость от системы;
- неверное предположение о взаимодействии пользователя при проектировании системы.

Анализ обоснованно предсказуемого неправильного использования можно поддерживать с помощью методов, описанных в таблице 5. Кроме того, в приложении В.1 описан метод получения сценариев неправильного использования SOTIF.

Таблица 5 — Методы выявления обоснованно предсказуемого неправильного использования

Методы	
A	Анализ выявленных сценариев неправильного использования на основе практического опыта и опыта из других источников [a]
B	Исследования испытуемых объектов
C	Анализ вариантов использования и сценариев
D	Анализ взаимодействия пользователей с системой [b]
E	Анализ ЧМИ
F	Анализ выявленных склонностей человека к неиспользованию, неправильному использованию и излишнему доверию к автоматизации
G	Анализ способности человека выполнять определенные задачи или переключаться между ними [c]
H	Применение соответствующих стандартов, правил и руководств [d]

[a] Например, пользовательские видеоролики в Интернете, демонстрирующие, как система или другие подобные ей системы могут использоваться не по назначению обоснованно предсказуемым образом.

[b] Например, бдительность водителя, понимание системы или ошибочное определение режима работы.

[c] Например, анализ способности человека восстанавливать свою осведомленность о ситуации.

[d] Например, свод правил проектирования и оценки ADAS (см. [11]), Европейские правила о принципах ЧМИ (см. [1]).

Примечание 1 — Подход подробно описан в В.1.

Примечание 2 — Использование транспортного средства водителем, неспособным при необходимости выполнять задачу управления им, считается злоупотреблением и не входит в область применения настоящего стандарта.

Пример 1 — Водитель находится под воздействием ограниченных в обращении веществ.

Пример 2 — Движение на неоправданно высокой скорости, превышающей возможности динамического управления транспортным средством на снегу.

Необходимость дополнительных мер, направленных на предотвращение или смягчение обоснованно предсказуемого (явного или неявного) неправильного использования, а также эффективность этих мер можно оценивать при оценке приемлемости реакции системы на его возможные триггерные условия. Эффективность этих мер можно демонстрировать на этапах верификации и валидации.

7.4 Оценка приемлемости реакции системы на триггерные условия недостаточности

Чтобы определить, считается ли SOTIF достижимой, оцениваются сценарии, содержащие идентифицированные триггерные условия.

Примечание 1 — Окончательная оценка приемлемости этих выявленных сценариев предусмотрена в действиях по верификации, указанных в разделе 10.

Примечание 2 — Конкретные допущения, которые использованы для этой оценки или вытекают из нее и имеют отношение к достижению SOTIF, продемонстрированы в разделе 10.

Примечание 3 — Допущения, которые рассматриваются во время этой оценки, могут включать ожидаемое поведение системы и ее элементов или предполагаемые действия пользователя.

SOTIF считается достижимой без необходимости дальнейшей функциональной модификации (согласно разделу 8), если:

- показано, что остаточный риск системы, вызывающей опасное событие, ниже критериев приемлемости, указанных в 6.5.

Примечание 4 — Доказательства, которые будут использоваться для оценки риска, будут получены в ходе мероприятий по верификации и валидации (разделы 9—11);

- не существует известного сценария, который мог бы привести к неоправданному риску для конкретных участников дорожного движения.

Примечание 5 — Даже если автопарк имеет очень низкую вероятность триггерного условия в рамках сценария, реакция системы может являться неприемлемой, если вероятность возникновения такого сценария высока для конкретного транспортного средства.

Пример — Специфическая конструкция, встроенная в кольцевую развязку или опору моста, которая систематически вынуждает систему AEB тормозить так, что торможение может приводить к недопустимым случаям столкновения сзади со следующим транспортным средством.

Реакция системы на триггерные условия недостаточности, которая не считается приемлемой в соответствии с вышеуказанными условиями, инициирует дальнейшую функциональную модификацию (как описано в разделе 8).

7.5 Результаты работы

7.5.1 Выявленные возможные недостаточности спецификации, недостаточности производительности и их триггерные условия (в том числе обоснованно предсказуемое прямое неправильное использование), обеспечивающие достижение цели 7.1, перечисление a).

Примечание — В 7.5.1 включены отчеты об анализах, выполненных для достижения цели 7.1, перечисление a).

7.5.2 Оценка приемлемости реакции системы на обнаруженные триггерные условия с точки зрения SOTIF, обеспечивающая достижение цели по 7.1, перечисление b).

8 Функциональные модификации, направленные на устранение рисков, связанных с SOTIF

8.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

a) должны быть определены и применены меры по устранению рисков, связанных с SOTIF;

b) должна обновляться входная информация для спецификации и проекта (5.5).

8.2 Общие положения

Для достижения целей настоящего раздела может рассматриваться следующая информация:

- спецификация и проект (в соответствии с 5.5);
- оценка риска опасного поведения (в соответствии с 6.6.2);
- выявленные возможные недостаточности спецификации, недостаточности производительности и их триггерные условия (в соответствии с 7.5.1);

- результаты верификации и валидации для выявленных сценариев (в соответствии с 10.8), если таковые имеются;
- результаты валидации невыявленных опасных сценариев (в соответствии с 11.4.1), если таковые имеются;
- обоснование выпуска SOTIF в соответствии с 12.5, если таковое имеется.

8.3 Меры по улучшению SOTIF

8.3.1 Введение

Меры по снижению рисков, связанных с SOTIF (далее — меры SOTIF), описанные в разделе 8, могут разрабатываться при выполнении следующих условий:

- установлено, что в заданной функциональности текущей спецификации и проекта (см. раздел 5) имеется опасный сценарий, который требует дальнейшего анализа (оценивается как способный причинить вред при оценке риска опасного события) (см. раздел 6);
- реакция системы на выявленное триггерное условие, вызывающее опасное поведение, оценивается как неприемлемая (известен сценарий, когда остаточный риск возникновения опасного события не соответствует критериям приемлемости и приводит к неоправданному риску) (см. раздел 7).

Система совершенствуется путем итерации рассмотрения мер SOTIF, рассмотренных в разделе 8, и обновления спецификации и проекта (см. раздел 5) с учетом этих мер SOTIF; выполняется оценка рисков заданной функциональности (см. разделы 6 и 7) с использованием обновленной спецификации и проекта.

Затем усовершенствованная система (в том числе эффективность мер по обеспечению SOTIF) оценивается на этапе верификации и валидации, и итеративная доработка системы на этапе проектирования может осуществляться в соответствии с разделом 8, если выполняется любое из следующих условий:

- остаточный риск известного опасного сценария признан неприемлемым (см. раздел 10);
- возникает невыявленный и опасный сценарий, при котором остаточный риск неприемлем (см. раздел 11);
- остаточный риск признается неприемлемым (см. раздел 12).

В приведенном выше случае разделы 5—8 выполняются повторно для усовершенствования системы.

Для достижения снижения риска, связанного с SOTIF, выбирается соответствующее сочетание мер предотвращения или смягчения.

Примечание — Меры предотвращения представляют собой меры по разработке безопасной конструкции самой машины, которые нацелены в первую очередь на устранение рисков (с целью достижения S = 0 или C = 0 при оценке рисков согласно разделу 6), и функциональные изменения (особенно добавление новых функций) являются типичным подходом для них. Тем не менее эти меры не гарантируют достижение S = 0 или C = 0.

«Меры смягчения» направлены на максимальное снижение риска, когда известно, что избежать риска сложно, или его можно признать приемлемым. Предполагается, что эти меры увеличивают эффект снижения риска в сочетании с мерами по предотвращению или другими мерами смягчения.

При реализации мер SOTIF можно учитывать:

- отсутствие негативного воздействия на другие элементы;
- отсутствие взаимодействия с другими опасными сценариями.

Кроме того, даже тщательно разработанные и реализованные меры SOTIF могут не давать ожидаемых результатов и приводить к непредвиденным последствиям. Следовательно, выполнение мероприятий по мониторингу и рецензированию, как описано в разделе 13, является важной частью реализации мер SOTIF, обеспечивающих сохранение их эффективности.

Возможные меры SOTIF описаны в 8.3.2—8.3.5.

8.3.2 Модификация системы

Мероприятия по модификации системы направлены на максимальное сохранение заданной функциональности и могут включать в себя, в том числе:

1) повышение производительности и/или точности датчиков за счет:
- улучшенных технологий датчиков.

Пример 1 — Повышение разрешающей способности измерения датчика.

Пример 2 — Переход на новый улучшенный датчик, в котором устранены выявленные ограничения;

- улучшенного обнаружения недостаточностей работы датчиков, запускающего соответствующую стратегию предупреждения о постепенном ухудшении производительности;
- разнообразных типов датчиков.

Пример 3 — Добавление дополнительных сенсорных устройств для увеличения охвата с помощью соответствующих методов;

- улучшения калибровки и установки датчиков.

Пример 4 — Расположение датчиков для лучшего охвата определенных случаев (например, при превышении нескольких показателей в системе), которые могут приводить к нарушению производительности.

Пример 5 — Размещение датчика(ов) в корпусе для предотвращения или сведения к минимуму помех до приемлемого уровня.

Пример 6 — Анализ охвата и оптимизация выбора датчиков (тип, технология, количество) и их взаимного расположения в транспортном средстве;

- методов обнаружения загрязнения и очистки датчиков.

Пример 7 — Обнаружение грязи на камере посредством обнаружения границ и ее очистка с помощью жидкости и скребков;

2) повышение производительности и/или точности исполнительных механизмов за счет совершенствования их технологий (например, повышение точности, расширение или ограничение диапазона выходов, уменьшение времени отклика, повторяемость измерений, полномочия по принятию решений, использование других вспомогательных функций или добавление нового вспомогательного исполнительного механизма);

3) повышение производительности и/или точности алгоритмов распознавания и принятия решения путем их модификаций.

Пример 8 — Улучшенный алгоритм распознавания датчиков [например, улучшение дескриптора функции для обнаружения объектов на изображениях камеры, такого как HOG (гистограммы ориентированных градиентов)].

Пример 9 — Рассмотрение дополнительной входной информации в модели.

Пример 10 — Улучшение алгоритма с целью повышения надежности и точности (например, переход от линейной модели к нелинейной или использование машинного обучения) (см. D.2).

Пример 11 — Ускорение обработки изображений за счет увеличения вычислительной мощности (например, с помощью ускорителя машинного обучения или высокопроизводительного оборудования).

Пример 12 — Распознавание выезда в проектируемой области эксплуатации [2] (например, приближение к съезду на автомагистрали).

Пример 13 — Распознавание известного неподдерживаемого состояния внешней среды (например, прогнозирование ослепления солнечным светом с учетом географического положения, времени суток, сезона и т. д.).

Примечание — Можно рассматривать повышение производительности оборудования при реализации усовершенствованных алгоритмов;

4) повышение заметности целевого ТС для улучшения управляемости других участников дорожного движения при опасном поведении целевого ТС.

Пример 14 — Установка светоотражателей, включение противотуманных фар, указателей поворота, активных звуковых сигналов и т. д., если это разрешено местными правилами.

8.3.3 Функциональные ограничения

Меры функционального ограничения направлены на поддержание частичной функциональности путем ухудшения (или ограничения) заданной функциональности. К этим мерам относятся, в том числе:

1) ограничение заданной функциональности для конкретных вариантов использования.

Пример 1 — Когда устройства обнаружения полосы движения не могут четко обнаруживать полосу движения, функция помощи при удержании полосы движения ограничивает крутящий момент рулевой рейки во избежание нежелательного вмешательства в рулевое управление.

Пример 2 — Введение ограничений (экологических, географических или временных) проектируемой области эксплуатации.

Пример 3 — Ужесточение или ограничение политики вождения (см. D.1) для обеспечения безопасности принятия решений.

Пример 4 — Камера ослеплена отраженным окружающим светом послеполуденного солнца; функционирование продолжается в ограниченном режиме (например, снижается разрешенная максимальная скорость ТС, ограничивается максимальный крутящий момент рулевого управления вспомогательной функции удержания полосы движения) с использованием радара и других датчиков;

2) лишение полномочий на заданную функциональность для конкретных вариантов использования.

Пример 5 — Все датчики восприятия ослеплены метелью; водителю предлагается взять управление на себя.

Пример 6 — Автоматизированное транспортное средство не может взаимодействовать с пунктами взимания платы за проезд или немаркированными зонами проведения строительных работ; водителю предлагается взять управление на себя.

8.3.4 Передача полномочий

Меры по передаче полномочий от системы водителю нацелены на повышение управляемости на нижних уровнях автоматизации вождения. К этим мерам могут относиться, в том числе:

1) модификация ЧМИ.

Пример 1 — ЧМИ явно передает водителю запрос на передачу управления и предоставляет необходимую информацию, которая помогает ему достичь соответствующей осведомленности о ситуации и выполнить эту задачу;

2) изменение уведомления пользователя и стратегии возврата к динамической задаче управления.

Пример 2 — Когда система обнаруживает ограничение обзора (например, уменьшение дальности действия датчика расстояния из-за грязи), скорость снижается и соответствующий ЧМИ предлагает водителю взять управление на себя. Если переход на ручное управление не выполняется в течение заданного периода времени, система снижает скорость до нуля.

Примечание 1 — На некоторых уровнях автоматизации вождения такой переход невозможен.

Примечание 2 — Улучшение управляемости может достигаться только в случае, если сам переход управляем и не представляет дополнительный риск для водителя.

Примечание 3 — Можно учитывать рекомендации, получаемые в результате исследований ЧМИ.

Пример 3 — См. правила и нормы проектирования и оценки ADAS [11].

8.3.5 Решение проблем обоснованно предсказуемого неправильного использования

К мерам по устранению обоснованно предсказуемого неправильного использования могут относиться, в том числе:

1) обучение клиентов (информирование и подготовка).

Пример 1 — Руководство пользователя, учебные курсы, маркетинг, презентация при продаже;

2) улучшение ЧМИ.

Пример 2 — Поддержка водителя путем предоставления ему информации о правильной эксплуатации;

3) внедрение системы мониторинга и оповещения водителей.

Примечание — Система обнаружения и предупреждения водителя о его отвлечении и т. п. может являться полезным методом предотвращения обоснованно предсказуемого неправильного использования водителем автоматизированной системы транспортного средства. Выбор и внедрение эффективной системы мониторинга водителя зависят от рассматриваемого неправильного использования.

Пример 3 — Предупреждение водителя о том, что он отпустил рулевое колесо.

Пример 4 — Игнорирование водителем входных сигналов/команд, которые могут приводить к опасному поведению, и информирование водителя о причинах их появления;

4) реализация мер по предотвращению неправильного использования.

Пример 5 — Если мониторинг водителя выявляет непрерывное неправильное использование несмотря на предупреждение, можно принимать меры по пресечению опасного поведения — например, отключить функцию помощи движения по полосе после нескольких предупреждений об отсутствии ручного управления или ограничить ее на оставшуюся часть поездки до следующего цикла включения зажигания с отображением соответствующей предупреждающей информации.

Пример 6 — Обоснованно предсказуемое неправильное включение функции, например можно предотвращать включение системы помощи при парковке на слишком высокой скорости, добавляя ограничение скорости в условие включения функции.

8.3.6 Поддержка реализации мер SOTIF

Для поддержания эффективности мер SOTIF после их реализации важно выполнять их мониторинг и анализ в зависимости от уровня автоматизации вождения. Для этой цели можно учитывать некоторые аспекты при разработке системы, в том числе:

- возможность тестирования поведения системы, связанной с SOTIF;
- возможность диагностики поведения системы, связанной с SOTIF;
- возможность мониторинга данных о поведении системы, связанной с SOTIF.

8.4 Обновление входной информации для «спецификации и проектирования»

Входная информация для «Спецификации и проектирования» обновляется на основе спецификации выявленных и примененных мер SOTIF согласно 8.3.

8.5 Результаты работы

Результатом работы является спецификация мер SOTIF, отвечающих целям по 8.1, перечисления a) и b).

9 Определение стратегии верификации и валидации

9.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

a) должна быть определена стратегия верификации и валидации для SOTIF (в том числе цели валидации), которая включает в себя:

1) необходимую оценку потенциально опасных сценариев;
2) достаточный охват соответствующего сценарного пространства;
3) необходимые доказательства (например, результаты анализа, протоколы испытаний, материалы специальных исследований);
4) процедуры получения доказательств;

b) должно быть предоставлено обоснование пригодности выбранных методов верификации и валидации, а также целей валидации.

9.2 Общие положения

Для достижения целей настоящего раздела можно учитывать следующую информацию:

- способность датчиков или внешних источников данных (например, от инфраструктуры) предоставлять достаточно точную информацию о внешней среде для соблюдения требований к характеристикам;
- достаточная надежность предполагаемых внешних источников данных (например, внезапное отключение сети связи или временное отсутствие возможности обновления);
- способность алгоритмов обработки данных датчиков точно моделировать внешнюю среду;
- способность алгоритмов принятия решений:
  - безопасно устранять возможные функциональные недостаточности;
  - принимать соответствующие решения в соответствии с моделью внешней среды, политикой вождения и текущими целями (например, целевым пунктом назначения);
- надежность системы или функциональности, например:
  - устойчивость системы к неблагоприятным условиям окружающей среды;
  - адекватность реакции автоматизированной системы на выявленные триггерные условия;

- чувствительность заданной функциональности и ее мониторинга в различных сценарных условиях;
- отсутствие неоправданного риска, связанного с опасным поведением заданной функциональности;
- способность системы (например, ЧМИ) предотвращать обоснованно предсказуемое неправильное использование;
- способность системы безопасно обрабатывать варианты использования вне проектируемой области эксплуатации (ODD) (например, активацию системы вне ODD, выход из ODD и т. д.);
- пригодность обнаружения и реакции на объекты и события (OEDR), надежность реализации политики (или поведения) вождения в ODD;
- пригодность резервного варианта динамической задачи управления (DDT); пригодность состояния с условием минимального риска (MRC);
- достаточно достоверное соответствие критериям приемлемости на уровне транспортного средства на этапе эксплуатации.

Для достижения целей настоящего раздела можно рассматривать следующую информацию:
- спецификацию и проект в соответствии с 5.4;
- оценку риска опасного поведения в соответствии с 6.6.2;
- критерии приемлемости в соответствии с 6.6.3;
- выявленные возможные недостаточности спецификации, недостаточности производительности и их триггерные условия (включая обоснованно предсказуемое явное неправильное использование) в соответствии с 7.5.1;
- спецификация мер SOTIF в соответствии с 8.5;
- план системной интеграции и тестирования (из внешнего источника);
- опыт, приобретенный в ходе контроля в процессе эксплуатации, в соответствии с 13.5;
- опыт, приобретенный в ходе эксплуатации датчиков и, возможно, в других предметных областях (например, ураганы, которые вызывают задержки сигнала GNSS и могут приводить к опасному событию).

Стратегия верификации и валидации нацелена на оценку характеристик и выявление рисков не только в пределах ODD, но также на ее границах и за пределами. Одним из аспектов стратегии является проверка недоступности системы извне ODD.

Еще одним аспектом является верификация того, что выход за пределы ODD сопровождается передачей управления водителю или резервной системе для достижения состояния с минимальным риском.

Примечание — Эти аспекты важны для обоснования достаточного охвата соответствующего пространства сценариев.

9.3 Спецификация интеграции и тестирования

Стратегия верификации и валидации формируется для подтверждения выполнения требований и описания методов достижения целей валидации. Эта стратегия охватывает всю заданную функциональность транспортного средства, в том числе Э/Э-элементы и компоненты других технологий, которые считаются значимыми для достижения SOTIF. Стратегия верификации и валидации также поддерживает мониторинг данных из внешних источников, которые имеют отношение к SOTIF.

Цели валидации определяются для подтверждения выполнения критериев приемлемости и могут определяться разными способами в зависимости от выбранных методов валидации.

Для каждого метода, выбранного из таблиц 6—11 или другого источника, определяются соответствующие подходы к его реализации (например, совокупная длина теста, глубина анализа) и приводится обоснование для каждого подхода, которое может включать количество или распределение сценариев, количество экспериментов или продолжительность имитационного моделирования.

Примечание 1 — Критерии приемлемости рассматривают риск, возникающий в результате выявленных и невыявленных опасных сценариев. Они учитываются при определении целей валидации, которые могут различаться для областей 2 и 3.

Примечание 2 — В В.2 и С.6 приведены примеры определения и оценки критериев приемлемости и целей валидации.

Пример 1 — Рассмотрим поиск ранее неизвестных триггерных условий, которые имеют отношение к функциональности. Цели валидации определяются для обоснования гипотезы о том, что остальные неизвестные триггерные условия не создают неоправданный риск.

Пример 2 — Цель валидации можно задавать с использованием заранее определенных частот ложноположительных и ложноотрицательных заключений для тестируемой функции.

Если с конкретной опасностью связано только подмножество сценариев, то воздействие этого подмножества можно учитывать при определении целевых значений и продолжительности валидации.

Примечание 3 — В таблице B.5 приведен пример генерации подмножества сценариев.

Примечание 4 — При оценке вероятности того, что триггерное условие нарушит количественный целевой показатель, можно учитывать подверженность воздействию, управляемость и серьезность результирующего поведения. Это может облегчить демонстрацию воздействия триггерного условия. В C.2.1 описана методология упрощения валидации за счет учета воздействия, управляемости и серьезности.

Пример 3 — В примере на рисунке 13 непреднамеренное торможение приводит к столкновению сзади только при наличии следующего за ним транспортного средства. Воздействие следующего транспортного средства можно учитывать при определении цели валидации.

Примечание 5 — Изменчивость параметров триггерных условий учитывается при определении и разработке стратегии верификации и валидации.

Примечание 6 — Поскольку функциональные изменения выполняются посредством итерации действий по обеспечению SOTIF (см. рисунок 10), система анализируется для обнаружения воздействий на существующие функции, и эти функции повторно тестируются с помощью регрессионных тестов. Это гарантирует, что функциональные изменения не приводят к потенциально опасному поведению в существующих функциях. Можно выбирать объем регрессионного тестирования при наличии надлежащего обоснования.

Примечание 7 — Чтобы гарантировать правильность функционального поведения, все действия по верификации и верификации документируются для каждой версии, которая предназначена для выпуска. Сюда входит документирование элементов, которые не были изменены, и повторно протестированных модифицированных элементов.

Примечание 8 — В D.2.4 рассматриваются действия по верификации и валидации для автономного обучения (например, действия, которые применяются к машинному обучению).

Спецификацию стратегии верификации и валидации (например, тестовые примеры для интеграционного тестирования, анализ) можно формировать с использованием соответствующего сочетания методов с учетом уровня интеграции, как показано в таблице 6.

Таблица 6 — Действия по верификации и валидации

Методы	
A	Анализ требований
B	Анализ внешних и внутренних интерфейсов [a]
C	Генерация и анализ классов эквивалентности
D	Анализ граничных значений
E	Предположение об ошибке на основе знаний или опыта
F	Анализ функциональных зависимостей
G	Анализ общих предельных условий и последовательностей
H	Анализ условий внешней среды и вариантов оперативного использования [b]
I	Анализ практического и приобретенного опыта [c]
J	Анализ архитектуры системы (включая резервирование)
K	Анализ конструкций датчиков и их известные потенциальные ограничения
L	Анализ алгоритмов, их путей принятия решений и соответствующих выявленных ограничений
M	Анализ старения системы и компонентов [d]
N	Анализ триггерных условий
O	Анализ целевых показателей эффективности [e]

Окончание таблицы 6

Методы	
P	Анализ измеряемых параметров из анализа опасностей
Q	Анализ внештатных и экстремальных случаев для граничных значений [f]
R	Анализ обновлений существующих систем, связанных с SOTIF
S	Использование баз данных с собранными тестовыми примерами и сценариями
T	Анализ критериев приемлемости
U	Анализ данных аварийных сценариев
V	Анализ известных потенциальных ограничений при срабатывании

[a] Сюда также входят V2X и карты (при наличии).

[b] Сюда входят выявленные источники потенциально опасного поведения системы или ее элементов.

[c] При этом учитываются различные условия, стили, среды вождения и претензии конечных потребителей.

[d] Эффекты старения полупроводников, которые приводят к отказам, как правило, рассматриваются в стандартах серии ИСО 26262. Эффекты старения полупроводников, связанные с SOTIF, т. е. эффекты, влияющие на номинальные характеристики, относятся к области применения настоящего стандарта.

[e] Целевые показатели характеристик могут указываться на разных уровнях абстракции: например, на уровне датчика (дальность действия радара, угловое разрешение камер), а также на уровне системы (например, частота ложных срабатываний при обнаружении объекта).

[f] Внештатный случай — это сценарий, в котором два или более значения параметров находятся в пределах, допустимых для системы, но в совокупности представляют собой редкое состояние, которое препятствует ее возможностям. Экстремальный случай — это сценарий, в котором экстремальные значения или само наличие одного или нескольких параметров приводят к условию, которое препятствует возможностям системы (см. [12]).

Примечание 9 — Информация о дальнейших методах верификации и валидации автомобильных систем восприятия указана в С.4.

9.4 Результаты работы

Результатом работы является определение стратегии верификации и валидации, отвечающей целям по 9.1, перечисления a) и b).

10 Оценка выявленных сценариев

10.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

a) выявленные потенциально опасные сценарии должны быть оценены на предмет опасности;

b) функциональность системы и ее элементов должна быть такой, как определено для выявленных опасных сценариев и обоснованно предсказуемого неправильного использования;

c) должна быть оценена приемлемость потенциально опасного поведения, обусловленного конкретным поведением на уровне транспортного средства;

d) охват выявленных сценариев должен быть достаточным в соответствии со стратегией верификации и валидации;

e) результаты верификации должны демонстрировать, что цели валидации достигнуты.

Примечание — Сюда входит оценка приемлемости резервного варианта динамической задачи управления (DDT) и состояние минимального риска (MRC).

10.2 Общие положения

Для достижения целей настоящего раздела может рассматриваться следующая информация:

- спецификация и проект в соответствии с 5.4;

- выявленные возможные недостаточности спецификации, недостаточности производительности и триггерные условия (в том числе обоснованно предсказуемое явное неправильное использование) в соответствии с 7.5.1;
- меры по устранению рисков, связанных с SOTIF, в соответствии с 8.5;
- определение стратегии верификации и валидации в соответствии с 9.4.

Примечание — Для прослеживания обнаруженных ранее существовавших материалов спецификации и проекта, связанных с SOTIF, а также функциональных модификаций, возникающих в результате итераций деятельности SOTIF, в 5.3 приведены рекомендации.

Структура по 10.3—10.5 соответствует модели: восприятие (см. 10.3), план (см. 10.4) и выполнение (см. 10.5), представленной в 4.2.3. В 10.6 рассмотрены вопросы интеграции.

10.3 Верификация датчиков

Для демонстрации корректных функциональных характеристик, синхронизации, точности и надежности датчиков при их заданном использовании и обоснованно предсказуемом неправильном использовании рекомендуется применять методы, представленные в таблице 7.

Примечание 1 — Некоторые задачи могут быть отнесены к различным действиям по верификации: например, классификацию объектов можно рассматривать как часть алгоритма планирования (см. 10.4). В этом случае можно применять методы верификации из нескольких подразделов.

Таблица 7 — Верификация датчиков

Методы	
A	Верификация достаточности технических характеристик датчика (например, достаточность диапазона, точности, разрешения, временных ограничений, полосы пропускания, отношения сигнал/шум, отношения сигнал/помеха) [a]
B	Испытание на основе требований (например, классификация, объединение данных датчиков)
C	Внесение факторов, вызывающих функциональную недостаточность [b]
D	При тестировании в контуре (например, SIL, HIL, MIL) на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий [c]
E	Тестирование на уровне транспортного средства на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий
F	Испытание датчика при различных условиях окружающей среды (например, холод, влажность, свет, условия видимости, условия помех)
G	Верификация воздействия старения датчика (например, ускоренное испытание на долговечность и т. д.) [d]
H	Оценка опыта эксплуатации этого датчика или датчика этого типа, в том числе мониторинг на месте эксплуатации
I	Повторное моделирование выявленных опасных сценариев для проверки влияния реализованного механизма снижения риска
J	Верификация свойств архитектуры, в том числе независимости от триггерных условий (если применимо)

[a] Сюда также входит выходной контроль во время сборки датчика (например, сопоставление антенны и обтекателя радара или выравнивание формирователя изображения камеры по отношению к ее объективу).

[b] В некоторых случаях можно имитировать потенциально опасное поведение датчика посредством введения ошибки на уровне моделирования. Приводится обоснование того, почему такие модели ошибок способны представлять тестируемые явления. Результаты моделирования можно объединять с результатами анализа триггерных условий.

[c] Используются выявленные ограничения модели датчика для выбора среды испытания (HIL/SIL/MIL или транспортное средство).

[d] В случае хорошо известных моделей сбоев из-за старения для конкретного датчика можно частично верифицировать влияние старения датчика посредством моделирования.

Примечание 2 — Для построения тестовых примеров можно использовать принципы комбинаторного тестирования с соответствующим обоснованием (см. [13]).

Примечание 3 — В С.4 приведены примеры верификации датчиков восприятия.

10.4 Верификация алгоритма планирования

Согласно 4.2.3 алгоритм планирования формирует управляющие воздействия на основе модели внешней среды, предоставляемой подсистемой восприятия. Для верификации способности алгоритма планирования реагировать должным образом и избегать нежелательных действий могут применяться методы, представленные в таблице 8.

Таблица 8 — Верификация алгоритма планирования

	Методы
A	Верификация устойчивости входных данных к помехам из других источников, таким как белый шум, звуковые частоты, ухудшение отношения сигнал/шум (например, путем тестирования чувствительности с помощью шумового сигнала)
B	Испытание на основе требований (например, анализ ситуации, функция, непостоянство данных датчика) [a]
C	Верификация свойств архитектуры, в том числе независимость от триггерных условий (если применимо)
D	При тестировании в контуре (например, SIL, HIL, MIL) на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных условий возникновения
E	Тестирование на уровне транспортного средства на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных условий возникновения
F	Ввод входных воздействий, в результате которых возникает потенциально опасное поведение
G	Верификация надлежащего соблюдения политики вождения [например, достижение MRC и эксплуатация после выхода из проектируемой области эксплуатации (ODD)] [a, b]
H	Повторное моделирование выявленных опасных сценариев для проверки влияния реализованного механизма снижения риска
[a] Также включает в себя верификацию того, что транспортное средство выбирает и достигает соответствующего MRC. [b] Руководство по политике вождения представлено в D.1.	

Примечание — Для формирования тестовых примеров можно обоснованно использовать принципы комбинаторного тестирования [13].

10.5 Верификация исполнительных механизмов

Для проверки исполнительных механизмов с целью их использования по назначению и в случае обоснованно предсказуемого неправильного использования могут применяться методы, представленные в таблице 9.

Таблица 9 — Верификация исполнительных механизмов

	Методы
A	Испытание на основе требований (например, точность, разрешение, ограничения по времени, полоса пропускания)
B	Верификация характеристик исполнительного механизма, когда он интегрирован в транспортное средство или в испытательный стенд системы
C	Испытание исполнительного механизма в различных условиях окружающей среды (например, в условиях холода или повышенной влажности)
D	Испытание исполнительного механизма при различных условиях нагрузки (например, переход от средней нагрузки к максимальной)

Окончание таблицы 9

Методы	
E	Верификация влияния старения исполнительного механизма (например, ускоренное испытание на долговечность) [a]
F	При тестировании в контуре (например, SIL, HIL, MIL) на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий
G	Тестирование на уровне транспортного средства на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий
H	Верификация свойств архитектуры, в том числе независимость от триггерных условий, если применимо
I	Повторное моделирование выявленных опасных сценариев для проверки влияния реализованного механизма снижения риска
[a] При наличии хорошо известных моделей сбоев из-за старения конкретного исполнительного механизма можно частично выполнять верификацию влияния его старения посредством моделирования.	

Примечание — Если можно доказать, что в системах выполнения отсутствуют какие-либо функциональные недостаточности или триггерные условия, могут быть достаточными испытания в соответствии со стандартами серии ИСО 26262 или другими соответствующими отраслевыми стандартами.

10.6 Верификация интегрированной системы

Для верификации надежности и управляемости системы, интегрированной в транспортное средство, а также правильности взаимодействия компонентов системы внутри транспортного средства рекомендуется применять методы, представленные в таблице 10.

Таблица 10 — Верификация интегрированной системы

Методы	
A	Верификация надежности системы (например, путем тестирования чувствительности к шумовому сигналу) [a]
B	Испытание на основе требований при интеграции в среду транспортного средства или на испытательном стенде системы (например, диапазона, точности, разрешения, временных ограничений, полосы пропускания)
C	При тестировании в контуре (например, SIL, HIL, MIL) на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий
D	Испытание системы в различных условиях окружающей среды (например, холода, сырости, в условиях различной видимости, помех)
E	Верификация влияния старения системы (например, ускоренное испытание на долговечность)
F	Направленный рандомизированный входной тест [b]
G	Тестирование на уровне транспортного средства на выбранных вариантах использования и сценариях, соответствующих SOTIF, с учетом выявленных триггерных условий
H	Испытания на управляемость (в том числе обоснованно предсказуемое неправильное использование)
I	Верификация внутренних и внешних интерфейсов
J	Верификация характеристик системы датчиков, установленной на транспортном средстве [c]
K	Верификация свойств архитектуры, в том числе независимости от триггерных условий (если применимо)
L	Повторное моделирование выявленных опасных сценариев для проверки влияния реализованного механизма снижения риска

Окончание таблицы 10

[a] Также включает в себя верификацию надежности характеристик в ODD и OEDR и верификацию надежности выполнения стратегии MRC, в том числе выхода за пределы ODD.

[b] Поскольку ожидаемые реальные ситуации часто бывает трудно воспроизвести, вместо них можно использовать рандомизированные входные тесты, например, в следующих случаях:

- когда датчики изображения добавляют перевернутые изображения или измененные фрагменты изображения;
- радиолокационные датчики добавляют ложные цели при имитации многолучевых отраженных сигналов;
- радиолокационные датчики добавляют ложные цели или пропускают обнаруживаемые цели из-за радиолокационных помех, создаваемых несколькими транспортными средствами.

[c] Сюда входит эксплуатация различных датчиков в различных условиях эксплуатации (например, когда возможности одной сенсорной технологии недостаточны — туман или отражающая способность лобового стекла влияют на камеру или форма и тип краски на бампере/логотипе влияют на радар) и допуски положения датчика.

Примечание 1 — Для верификации недетерминированных систем оценка выявленных опасных сценариев может выполняться с использованием статистических методов или методов управления рисками.

Пример — Стратегия поведения при вождении основана на предположениях участников дорожного движения, в частности, при наличии препятствий, когда выявленное неопасное поведение при определенных обстоятельствах может приводить к столкновению.

Примечание 2 — В В.4 приведены примеры верификации интегрированных систем.

10.7 Оценка остаточного риска для выявленных опасных сценариев

Цели валидации, определенные в разделе 9, являются обоснованием достаточной достоверности выполнения критериев приемлемости на этапе эксплуатации. Таким образом, результаты верификации показывают, что цели валидации для выявленных опасных сценариев достигнуты, а остаточный риск известных опасных сценариев не является неоправданным.

Выявленные опасные сценарии не являются недопустимыми, если:

- вероятность выявленных сценариев, вызывающих опасное поведение, соответствует целям валидации;
- не существует выявленного сценария, который мог бы приводить к неоправданному риску для конкретных участников дорожного движения.

Пример — Местные географические объекты (например, туннель или мост) не могут приводить к неоправданному увеличению риска.

10.8 Результаты работы

Результатами работы являются результаты верификации и валидации, которые демонстрируют, что поведение заданной функциональности в выявленных сценариях соответствует ожиданиям согласно целям, указанным в 10.1.

11 Оценка невыявленных сценариев

11.1 Цели

Цель настоящего раздела заключается в том, чтобы результаты валидации демонстрировали, что остаточный риск от невыявленных опасных сценариев с достаточной уверенностью соответствует критериям приемлемости.

Примечание — Одним из аспектов является способность совокупного набора мероприятий по верификации и валидации обеспечивать репрезентативный охват пространства возможных сценариев.

11.2 Общие положения

Для достижения целей настоящего раздела может рассматриваться следующая информация:

- спецификация и проект в соответствии с 5.4;

- выявленные возможные недостаточности спецификации, недостаточности производительности и их триггерные условия (в том числе обоснованно предсказуемое явное неправильное использование) в соответствии с 7.5.1;
- меры по устранению рисков, связанных с SOTIF, в соответствии с 8.5;
- определение стратегии верификации и валидации в соответствии с 9.4;
- результаты верификации и валидации, которые показывают, что поведение заданной функциональности соответствует ожиданиям в выявленных сценариях в соответствии с 10.8.

11.3 Оценка остаточного риска для невыявленных опасных сценариев

В реальных ситуациях могут возникать невыявленные сценарии. Для оценки остаточного риска в реальных ситуациях, которые могут вызывать опасное поведение системы при ее интеграции в транспортное средство, рекомендуется применять методы, представленные в таблице 11.

Таблица 11 — Оценка остаточного риска

Методы	
A	Валидация устойчивости к ухудшению отношения сигнал/шум (например, путем тестирования чувствительности к шумовому сигналу) [a]
B	Валидация различных факторов и свойств, обеспечиваемых архитектурой, в том числе независимость от триггерных условий (если применимо)
C	При тестировании в контуре на случайных тестовых примерах (полученных на основе технического анализа и предположений об ошибках)
D	Рандомизированный входной тест [a]
E	Тестирование на уровне транспортного средства на выбранных тестовых сценариях (полученных на основе технического анализа и предположений об ошибках) с учетом выявленных триггерных условий
F	Долговременное испытание транспортного средства
G	Эксплуатационное испытание
H	Тест, основанный на практическом опыте
I	Тестирование «внештатных» и экстремальных случаев [b]
J	Сравнение с существующими системами
K	Моделирование на основе случайной последовательности сценариев
L	Тестирование возможных случаев неправильного использования при случайном использовании и неопытных пользователях
M	Анализ чувствительности функциональности для конкретных условий сценария [c]
N	Анализ/имитационное моделирование соответствующих параметров [d]
O	Исследование сценариев в реальном мире [e]
P	Функциональная декомпозиция и вероятностное моделирование (с учетом, что состояние нарушения элемента включает в себя множество нарушений выходов его подэлементов; см. С.6.3.3)
Q	Валидация относительно реальных данных
[a] Поскольку ожидаемые реальные ситуации часто бывает трудно воспроизвести, вместо них можно использовать рандомизированные входные тесты — например, в следующих случаях: - когда датчики изображения добавляют перевернутые изображения или измененные фрагменты изображения; - когда радиолокационные датчики добавляют ложные цели при имитации многолучевых отраженных сигналов; - когда радиолокационные датчики добавляют ложные цели или пропускают обнаруживаемые цели из-за радиолокационных помех, создаваемых несколькими транспортными средствами.	

Окончание таблицы 11

[b] «Внештатный случай» — это сценарий, в котором два или более значения параметров находятся в пределах допустимых для системы, но в совокупности представляют собой редкое состояние, которое препятствует ее возможностям. Экстремальный случай — это сценарий, в котором экстремальные значения или само наличие одного или нескольких параметров приводят к условию, которое препятствует возможностям системы» [12].

[c] Функциональность считается чувствительной к конкретному состоянию сценария, если небольшие изменения этого условия могут приводить к значительному изменению поведения на уровне транспортного средства.

[d] См. примечания 5, 6 и 7 к 7.3.1. Список триггерных условий, полученный в соответствии с 7.3, может использоваться для идентификации соответствующих параметров варианта использования.

[e] Исследование означает поиск невыявленных сценариев путем охвата широкого набора сценариев реального мира. Оно может включать систематическое или случайное изменение соответствующих параметров сценариев.

Примечание — Релевантность выбранных параметров обосновывается, например, анализом чувствительности или статистическим анализом.

При испытаниях в общественных местах в целях предотвращения или смягчения потенциального риска для населения, связанного с испытываемыми транспортными средствами, могут требоваться дополнительные меры безопасности (например, механизм аварийной остановки).

Примечание 1 — Новые невыявленные опасные сценарии могут возникать при каждом внесении изменений в алгоритм, ODD и OEDR, появлении новых типов транспортных средств во внешней среде и изменении политики вождения. Методы, представленные в таблице 11, также можно применять для повторной оценки остаточного риска после внесения этих изменений.

Набор выбранных методов пригоден для выявления потенциально опасных сценариев в области 3, например при использовании входных данных, которые являются репрезентативными для варианта использования, а также рассмотрении сложных или редких сред эксплуатации, конкретных вариантов использования, сцен или сценариев. Приводится обоснование адекватности выбранных методов.

При определении длительности испытаний транспортных средств (например, для долгосрочных и эксплуатационных испытаний) можно учитывать информацию, полученную из предыдущих программ транспортных средств, управляемость водителя или важность выбранных испытательных маршрутов. При использовании рандомизированных входных тестов с внесением ошибок можно выбирать количество моделируемых сценариев в соответствии с требуемой длиной теста и содержанием, которое является репрезентативным для целевого географического рынка.

При рассмотрении таких методов испытаний, как полигон, моделирование или открытая дорога, каждому методу испытаний назначается соответствующее количество километров или часов работы. Можно привести обоснование такого распределения.

Примечание 2 — Непрерывный рандомизированный цикл моделирования алгоритмов принятия решений может имитировать работу на протяжении миллионов километров, но может не соответствовать реальным условиям, поскольку моделирование всегда является неполной моделью реального мира.

Примечание 3 — В С.4 представлены примеры валидации систем, связанных с SOTIF.

В соответствии с разделом 9, цели валидации выбираются таким образом, что их выполнение влечет за собой выполнение критериев приемлемости. В этих условиях остаточный риск, связанный с невыявленными опасными сценариями, является приемлемым.

Пример — Целью валидации может являться максимальное количество встречавшихся ранее невыявленных опасных сценариев в наборе тестовых сценариев. Если после выполнения этих тестовых сценариев количество встречавшихся ранее невыявленных опасных сценариев менее заданного целевого значения, то цель валидации достигнута.

11.4 Результаты работы

11.4.1 Результаты валидации невыявленных опасных сценариев, соответствующие цели по 11.1

11.4.2 Оценка остаточного риска, соответствующая цели по 11.1

12 Оценка результатов реализации SOTIF

12.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

a) результаты работы, полученные в процессе деятельности по обеспечению SOTIF, должны быть проанализированы на полноту, корректность и согласованность;

b) должны быть представлены обоснование достижения SOTIF с учетом выполнения целей разделов настоящего стандарта и соответствующие результаты работы;

c) должно быть оценено обоснование достижения SOTIF и даны рекомендации по утверждению или отклонению версии, обеспечивающей SOTIF.

12.2 Общие положения

Для достижения целей настоящего раздела может рассматриваться следующая информация:

- спецификация и проект (в соответствии с 5.5);
- опасности на уровне транспортного средства (в соответствии с 6.6.1);
- оценка риска опасного поведения (в соответствии с 6.6.2);
- критерии приемлемости (в соответствии с 6.6.3);
- выявленные недостаточности спецификации, недостаточности производительности и их триггерные условия (в соответствии с 7.5.1);
- оценка реакции системы на триггерные условия (в соответствии с 7.5.2);
- спецификация мер обеспечения SOTIF (в соответствии с 8.5);
- определение стратегии верификации и валидации (в соответствии с 9.4);
- результаты верификации и валидации, которые подтверждают, что заданная функциональность демонстрирует ожидаемое поведение в выявленных сценариях (в соответствии с 10.8);
- результаты валидации для невыявленных опасных сценариев (в соответствии с 11.4.1);
- оценка остаточного риска (в соответствии с 11.4.2);
- контроль в процессе эксплуатации (в соответствии с 13.5).

12.3 Методы и критерии оценки SOTIF

Каждый результат работы проверяется на полноту, корректность и согласованность.

Приводится обоснование, которое демонстрирует достижение SOTIF посредством достигнутых целей по разделам 5—11 и мер контроля в процессе эксплуатации (например, процессов и необходимых аппаратных ресурсов), которые определены в разделе 13.

Примечание 1 — Пример возможной структуры обоснования с использованием GSN см. в А.1.

Оценка этого обоснования может включать, помимо прочего, ответы на следующие вопросы:

a) Проанализированы ли опасности, возможные функциональные недостаточности и их триггерные условия, а также реализованы и оценены ли все необходимые модификации проекта для достижения SOTIF, чтобы гарантировать, что эти модификации проекта в достаточной степени снизили риск в соответствии с критериями приемлемости во всех указанных вариантах использования?

b) Достигает ли заданная функциональность состояния минимального риска, когда это необходимо, обеспечивая для пассажиров или других участников дорожного движения состояние без неоправданного риска, учитывая:

1) указанное вмешательство водителя;

2) обоснованно предсказуемое неправильное использование;

3) указанное предупреждение пассажирам транспортного средства и/или другим участникам дорожного движения;

4) указанное ухудшение функциональности;

5) запасной вариант DDT (для достижения состояния минимального риска)?

c) Обеспечивает ли стратегия верификации и валидации охват всех выявленных опасных сценариев и обосновывает ли, что остаточный риск от невыявленных опасных сценариев с достаточной уверенностью соответствует критериям приемлемости?

1) Охватывают ли результаты испытаний выявленные триггерные условия, условия окружающей среды, а также явное и неявное неправильное использование?

2) Включены ли в стратегию верификации и валидации действия по валидации, достаточные для ограничения риска, связанного с выявленными и невыявленными сценариями?

d) Выполнены ли надлежащие верификация и валидация? Достигнуты ли цели валидации, которые обеспечивают уверенность, что остаточный риск не является неоправданным?

1) Была ли заданная функциональность проверена в достаточной степени, чтобы оценить как номинальное, так и потенциально опасное поведение?

2) Были ли предоставлены доказательства отсутствия неоправданного риска в случае опасного поведения?

3) Получены ли в результате тестирования обоснования того, что охват достаточен для подтверждения надежности политики вождения во всех случаях использования и/или ODD, OEDR?

e) Имеются ли необходимые средства для реализации мероприятий этапа эксплуатации (согласно разделу 13)?

Примечание 2 — Если действия на этапе эксплуатации, описанные в разделе 13, привели к принятию мер SOTIF, эти меры рассматриваются в разделе 12.

Пример — См. С.2.2.

Примечание 3 — Анализ результатов деятельности по обеспечению SOTIF может рассматриваться совместно с оценкой функциональной безопасности по ИСО 26262-2.

12.4 Рекомендации по версии обеспечения SOTIF

На основании доказательств методологии, приведенной в 12.3, можно определять рекомендации приемки, условной приемки или отклонения версии. В случае условной приемки условия документально оформляются и их выполнение проверяется перед окончательным выпуском.

Примечание — Условная приемка является промежуточным результатом. В этом случае условия документируются и их выполнение проверяется перед окончательным выпуском, т. е. окончательная версия принимается только после выполнения условий.

Пример — Промежуточное целевое значение пробега в километрах в рамках испытания на долговечность может устанавливаться на приемлемом обосновании в соответствии с 6.5. Соблюдение всех условий может являться основанием для приемки. Если выполнены предыдущие условия, кроме завершения регрессионного тестирования улучшения проекта для устранения аномалии SOTIF, допускается условная приемка. Выпуск возможен после успешного завершения регрессионного тестирования.

Оценка достижений SOTIF оформляется документально.

12.5 Результаты работы

Результатом работы является обоснование приемки версии, обеспечивающей SOTIF, в соответствии с целью по 12.1.

13 Действия на этапе эксплуатации

13.1 Цели

В настоящем разделе рассмотрено достижение следующих целей:

1) перед выпуском версии должен быть определен контроль в процессе эксплуатации для обеспечения SOTIF во время эксплуатации;

2) контроль в процессе эксплуатации должен выполняться для поддержания достижения SOTIF на этапе эксплуатации.

13.2 Общие положения

Действия SOTIF, описанные в разделах 5—12, направлены на снижение риска до приемлемого уровня на момент выпуска версии SOTIF. Тем не менее, эта оценка риска может пересматриваться, например, в следующих случаях:

- если в процессе эксплуатации функций обнаруживается не выявленная ранее опасность;
- если в процессе эксплуатации функций обнаруживается не выявленная ранее функциональная недостаточность и/или ее триггерное условие;

- если допущения, такие как условия окружающей среды или правила дорожного движения, изменяются по сравнению с допущениями, которые были определены во время разработки функциональности.

Для достижения целей настоящего раздела может рассматриваться следующая информация:

- спецификация и проект согласно разделу 5;
- критерии приемлемости согласно разделу 6;
- выявленные потенциальные недостаточности спецификации, недостаточности производительности и их триггерные условия (в том числе обоснованно предсказуемое неправильное использование) согласно разделу 7;
- результаты действий по верификации согласно разделу 10;
- результаты действий по валидации и оценка остаточного риска согласно разделу 11.

На рисунке 16 показаны виды деятельности на этапе эксплуатации.

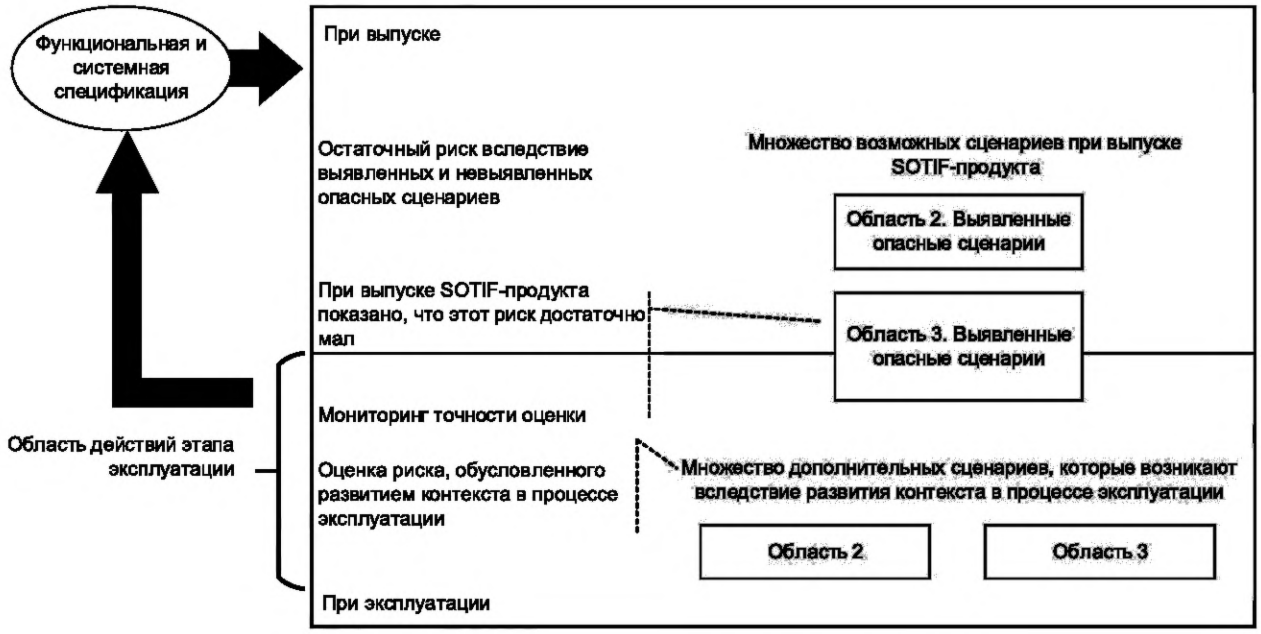


Рисунок 16 — Виды деятельности на этапе эксплуатации

Примечание — В настоящем разделе не рассматриваются действия, которые обеспечивают необходимое соответствие спецификации и проекту для достижения SOTIF в течение жизненного цикла, в том числе производство, эксплуатацию и обслуживание, предусмотренные ИСО 26262-7.

13.3 Сбор необходимых данных

Ожидания от процесса мониторинга при эксплуатации зависят от уровня автоматизации вождения, сложности заданной функциональности и серьезности опасностей. Для более низких уровней автоматизации вождения может быть достаточно обычного наблюдения за рынком. Для более высоких уровней автоматизации вождения могут требоваться дополнительные средства, такие как «Система хранения данных для автоматизированного вождения»/«Регистратор событий» (DSSAD/EDR).

К необходимым данным могут относиться, в том числе:

а) описание инцидентов, в которых функциональность являлась или могла являться причиной причинения вреда, или становилась причиной превышения заданных значений, которые могли привести к причинению вреда в другой ситуации.

Пример 1 — Такое описание инцидентов может содержаться:

- ***в отчетах об авариях или инцидентах;***
- ***сообщениях водителей о проблемах;***
- ***отчетах об обоснованно предсказуемом неправильном использовании;***
- ***бортовом механизме, сигнализирующем о возможных недостатках, таких как:***

- нарушение минимального расстояния до препятствия;
- сценарии, в которых система была близка к запуску определенной системной реакции.

Примечание 1 — Для более высоких уровней автоматизации вождения может являться целесообразным внедрение механизмов мониторинга (например, бортового). Они могут обнаружить возможные функциональные недостаточности до возникновения аварий (например, функциональные недостаточности, приводящие к предаварийной ситуации, условия, которые приводят к нарушениям выходов элементов). В этом случае требования к бортовым механизмам мониторинга SOTIF уточняются на этапе разработки.

Пример 2 — Бортовые механизмы мониторинга могут:
- сохранять данные о сценариях, вызвавших аварийную реакцию системы;
- сохранять данные о сценариях, в которых водитель неожиданно взял на себя управление;
- сохранять данные о сценариях, ведущих к состоянию минимального риска;

b) совокупность знаний.

Пример 3 — Совокупность знаний может включать в себя:
- информацию, исходящую от органов общественной безопасности (в том числе от других изготовителей транспортных средств), общедоступных инцидентах на рынке, которые могут иметь отношение к функциональности;
- опыт полученных в проектах аналогичных систем или функциональных возможностей;

c) развитие контекста, которое может влиять на SOTIF и приводить к пересмотру оценки SOTIF.

Примечание 2 — Развитие контекста описывает возможные изменения в сценариях, в том числе домен эксплуатации и взаимодействие пользователя с системой.

Пример 4 — Развитие контекста может включать в себя:
- развитие дорог и дорожного движения;
- модификацию регламента;
- модификацию инфраструктуры;
- новые виды правильного и неправильного использования;
- развитие характеристик участников дорожного движения;
- изменение привычек пользователей в силу общих причин или в результате использования системы.

13.4 Процесс оценки и разрешения проблем SOTIF

В рамках процесса оценки и разрешения проблем SOTIF определяются роли и обязанности:
- для передачи соответствующих данных в разработку;
- оценки собранных данных с целью определить, продолжает ли риск оставаться оправданным;
- определения и внедрения мер по обеспечению SOTIF при необходимости.

Деятельность на этапе эксплуатации включает в себя, в том числе:

1) мониторинг и анализ

На этапе мониторинга выполняется непрерывный сбор необходимых данных, определенных в 13.3. Допускается выполнять мониторинг с обратной связью [см. 13.3, перечисление а)] и упреждающий мониторинг [см. 13.3, перечисление б) и 13.3, перечисление в)]. Кроме того, в ходе мониторинга могут выявляться потенциально опасные сценарии, которые не были обнаружены на этапе разработки.

Если поступают какие-либо данные, имеющие отношение к SOTIF, анализируется их влияние на обоснование SOTIF и повторно оценивается его достоверность.

Примечание 1 — Цели мониторинга могут определяться на этапе разработки.

Примечание 2 — С помощью собранных данных, относящихся к SOTIF, можно обновлять или расширять базы данных, которые используются для поддержки анализа SOTIF, в целях дальнейшего развития (приобретенный опыт).

Примечание 3 — Примеры обоснования SOTIF см. в приложении А.

Примечание 4 — При необходимости можно обновлять обоснование SOTIF;

2) оценку риска и снижение опасности

Если обоснование SOTIF больше не действительно, выполняется оценка риска. В зависимости от риска, связанного с соответствующими собранными данными о SOTIF, принимается решение

о средствах его снижения. Для снижения неоправданного риска может требоваться немедленное реагирование. Это, в свою очередь, может приводить к принятию мер, которые не требуют выполнения каких-либо дополнительных действий SOTIF [например, частичное или полное запрещение функции беспроводной передачи данных (OTA)] до создания окончательного исправления, к которому применяются соответствующие действия SOTIF. Для добавления новых мер SOTIF и обновления системы может быть необходимым принятие долгосрочных мер, требующих выполнения дополнительных действий SOTIF, которые приводят к созданию новой версии SOTIF. Изменения системы и функций, которые считаются необходимыми после выпуска новой версии SOTIF, рассматриваются с учетом разделов 5—12.

Примечание 5 — Обновления OTA могут являться гибким и удобным методом внесения изменений для своевременного устранения выявленных функциональных недостаточностей на этапе эксплуатации.

13.5 Результаты работы

Результатом работы является контроль в процессе эксплуатации, соответствующий цели по 13.1.

Приложение А
(справочное)

Общее руководство по обеспечению SOTIF

А.1 Примеры структурирования обоснования SOTIF с помощью GSN

А.1.1 Общие положения

В А.1 приведены два примера, которые демонстрируют описание обоснования SOTIF с помощью нотации структурирования цели (GSN) (см. [14]). В таблицах А.1 и А.2 описаны элементы, использованные в примерах GSN. Структура обоснования может быть различной; некоторые ее варианты описаны в А.1.2 и А.1.3.

GSN — это метод, который широко используется в сфере безопасности. Целью GSN является документирование обоснования главной цели, которая заключается в достижении отсутствия неоправданного риска. Для этого цели декомпозируются на подцели и, в конечном счете, подкрепляются фактическими данными (решениями); одновременно поясняются принятые стратегии и контекст, в котором сформулированы цели.

Примечание — GSN может использоваться для достижения целей и задач, которые также вытекают из других стандартов (например, стандарты серии ИСО 26262).

Таблица А.1 — Описание используемых элементов GSN

Символ	Имя	Описание
{Идентификатор цели}	Цель	Цель в виде прямоугольника представляет собой определение, которое входит в состав обоснования
{Идентификатор стратегии} <Определение стратегии>	Стратегия	Стратегия в виде параллелограмма описывает характер логической связи между целью и поддерживающими ее целями
{Идентификатор решения} <Определение решения>	Решение или доказательства	Решение или доказательство в виде круга представляет собой ссылку на элемент доказательства
{Идентификатор контекста} <Определение контекста>	Контекст	Контекст представляет собой контекстный артефакт — ссылку на контекстную информацию или утверждение. Иногда он используется для определения терминов в рамках целей или стратегий
{Идентификатор допущения} <Определение допущения> A	Допущение	Допущение в виде овала с буквой «А» в правом нижнем углу представляет собой преднамеренно необоснованное утверждение
	Поддерживается	Поддержка, отображается в виде линии со сплошной стрелкой и позволяет документировать логические или доказательные связи
	В контексте	В контексте, отображаемом в виде линии с пустотелым наконечником стрелки, объявляется контекстная связь
n	Множественность	Это средство указания на то, что при создании экземпляра могут существовать несколько экземпляров соответствующего отношения. Сплошной шар является символом множественности (что означает ноль или более). Метка рядом с шаром указывает на мощность отношения

Таблица А.2 — Описание используемых элементов нотации, которые отсутствуют в официальном стандарте GSN

Символ	Имя	Описание
ACP:(x) ACP:(x)	Точка требования достоверности	Это способ ссылки на обоснование, которое касается отношения между двумя элементами. Примечание — Обоснование безопасности включает в себя ссылки на информацию, которая: - обеспечивает контекст; - определяет допущения; - содержит доказательства. Достаточность и правомерность этих ссылок может подвергаться сомнению. Ответом на это сомнение является подтверждение того, что эта информация достаточна и правомерна. Использование точки требования достоверности (ACP) является удобным синтаксическим средством указания на присутствие или необходимость обоснования, которое не загромождает основную диаграмму обоснования. Обоснование, связанное с ACP, указывается далее на отдельной диаграмме
+ Рисунок A.X	Ссылка на рисунок	Это ссылка на рисунок A.X, на котором продолжается обоснование
См. таблицу A.X	Ссылка на таблицу	Ссылка на таблицу A.X

A.1.2 GSN. Пример 1

В примере 1 обоснование (см. рисунки А.1— А.7) основано на отсутствии неоправданных рисков из-за выявленных (т. е. относящихся к области 2) и невыявленных (т. е. относящихся к области 3) потенциально опасных сценариев.

Примечание — В этом примере сокращение AD означает «автоматическое вождение», а сокращение DA — «помощь водителю».

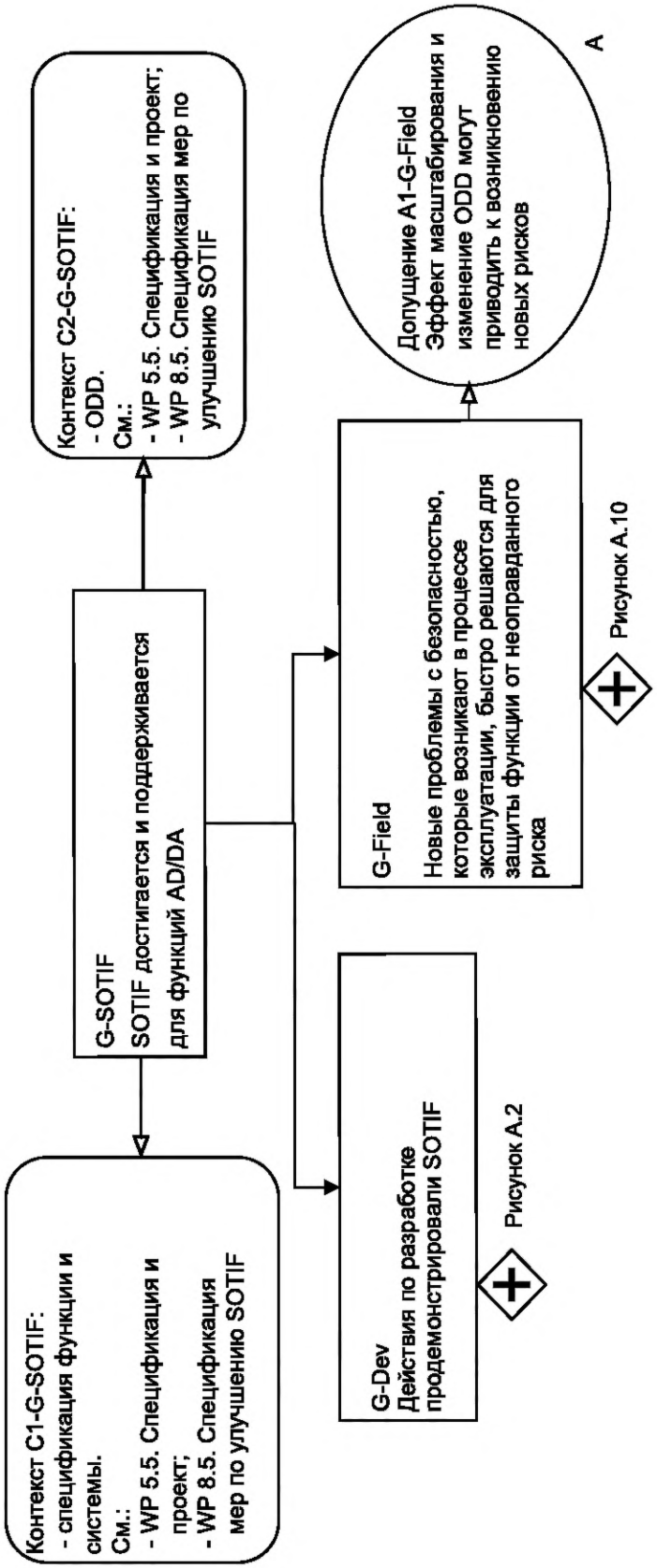


Рисунок A.1 — G-SOTIF: SOTIF достигается и поддерживается для функций AD/DA

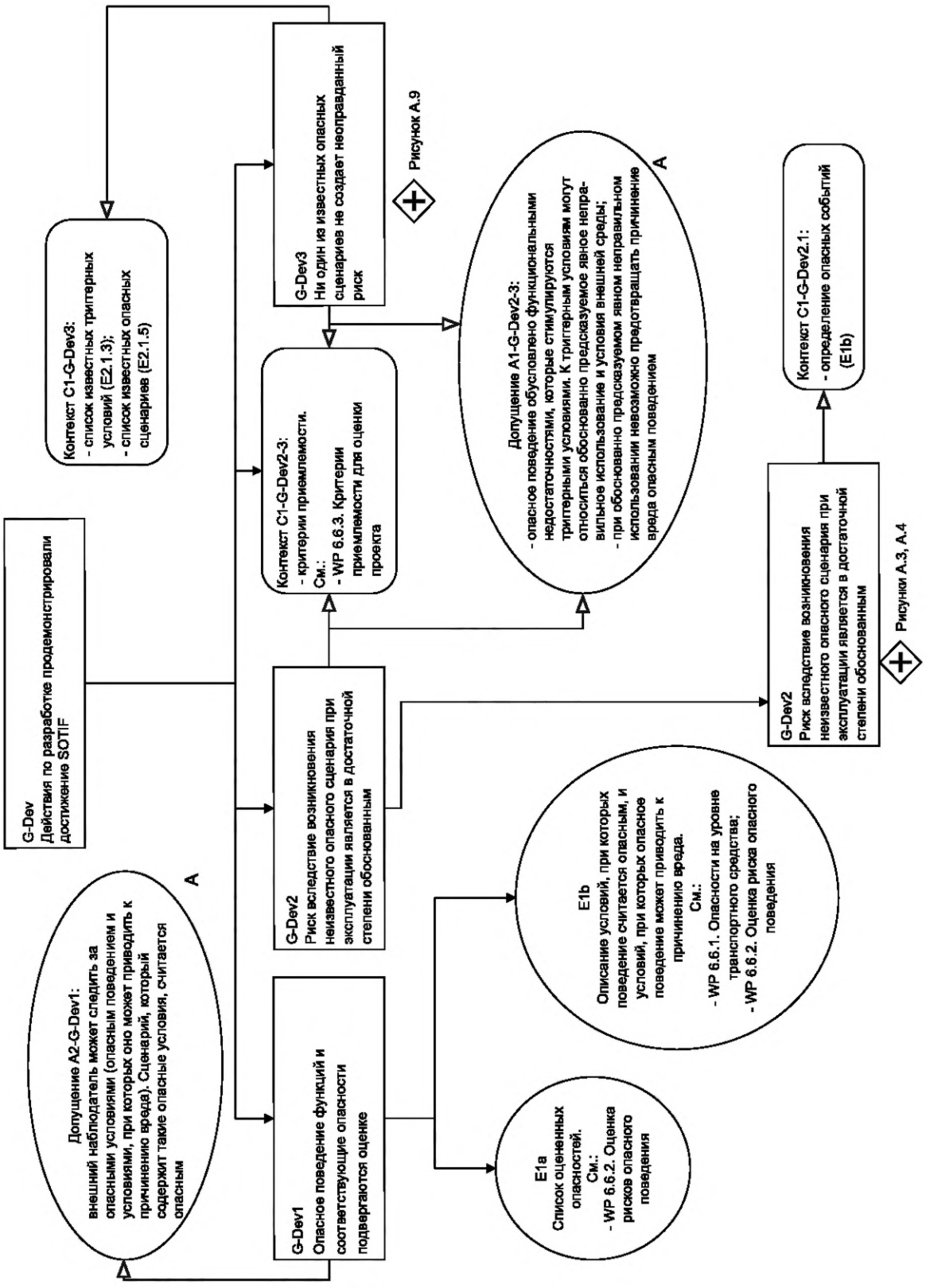


Рисунок А.2 — G-Dev: деятельность по разработке продемонстрировала достижение SOTIF

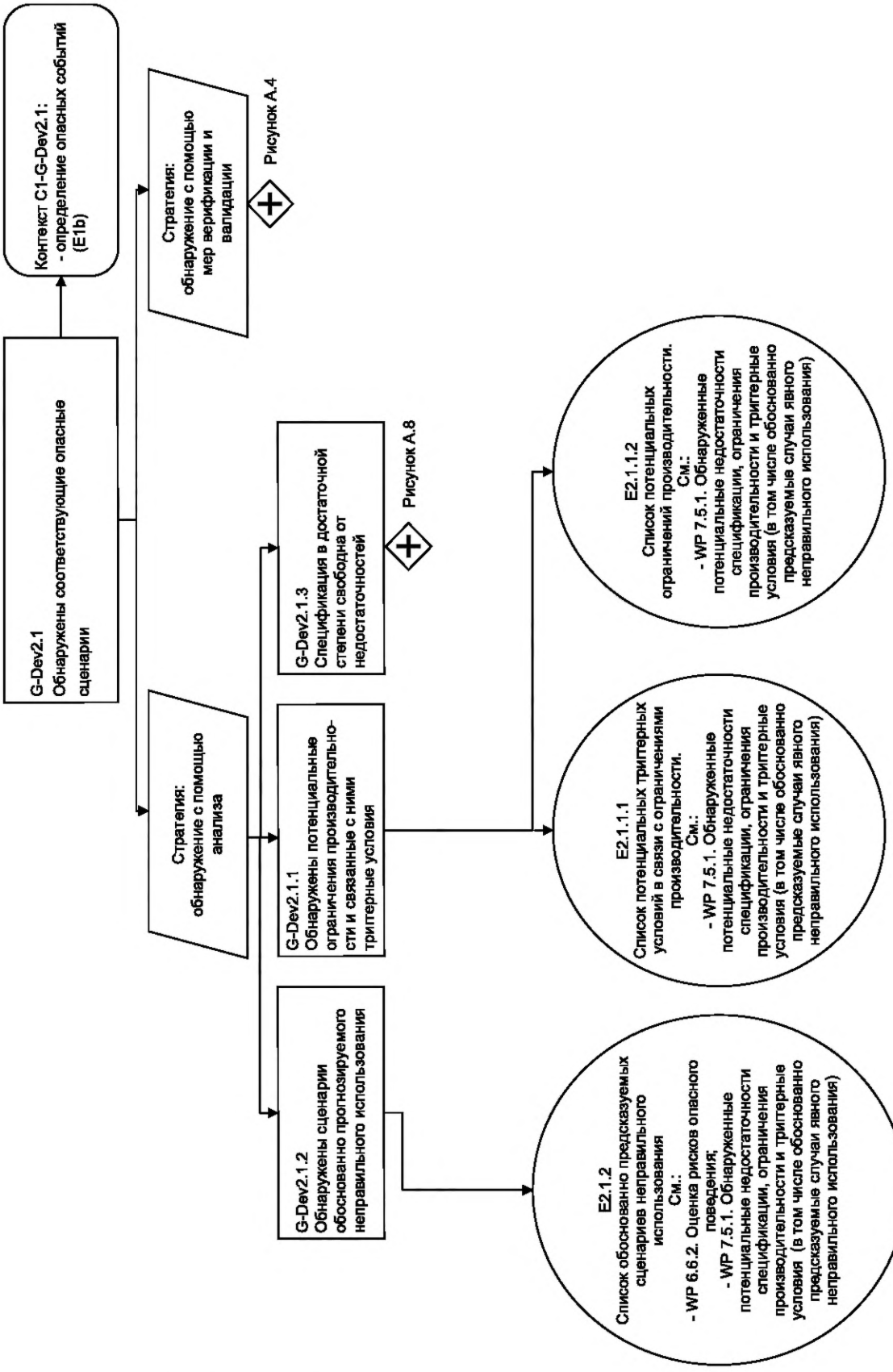


Рисунок А.3 — G-Dev2.1: обнаружены применимые потенциально опасные сценарии. Часть 1

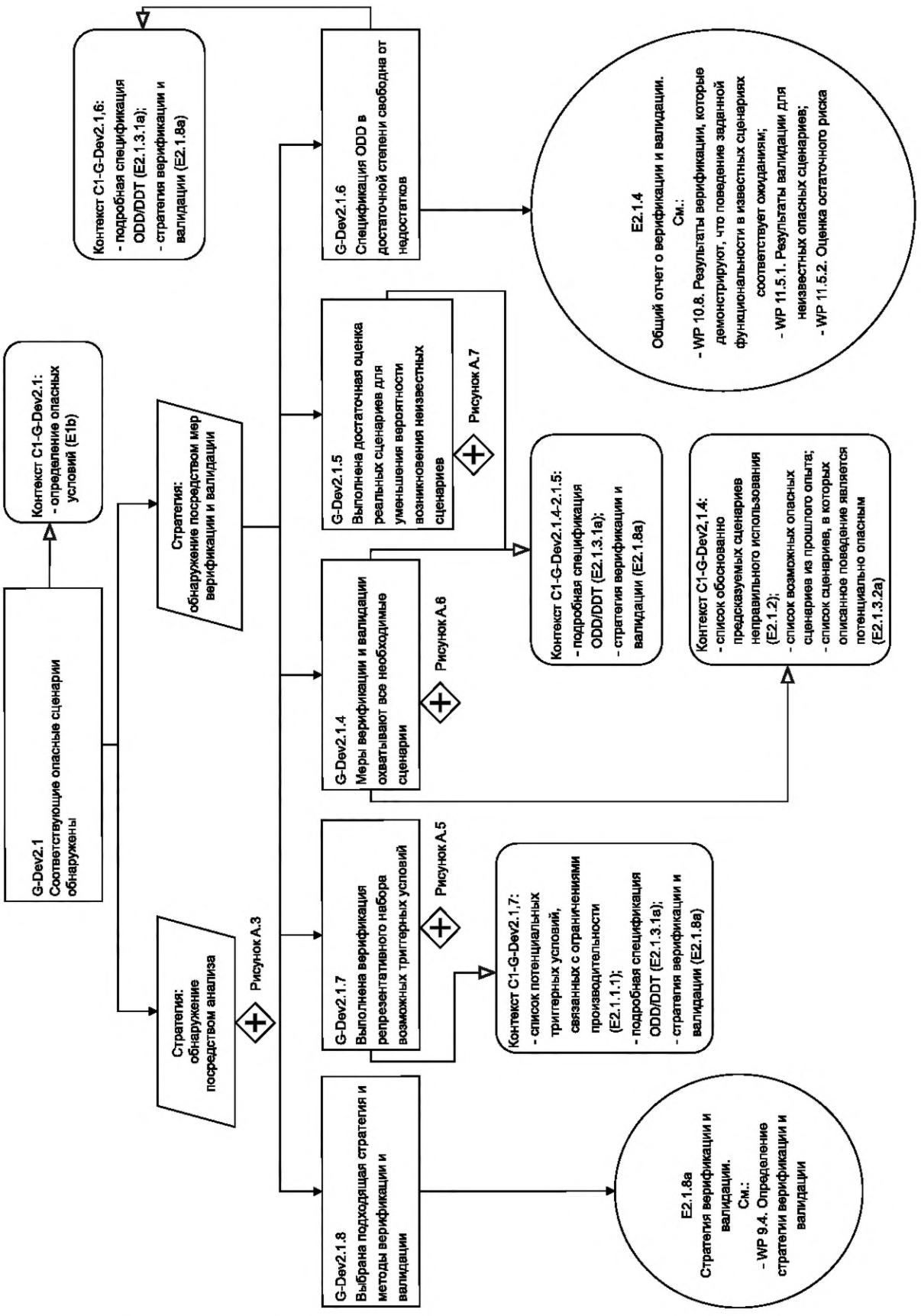


Рисунок A.4 — G-Dev2.1: обнаружены применимые опасные сценарии. Часть 2

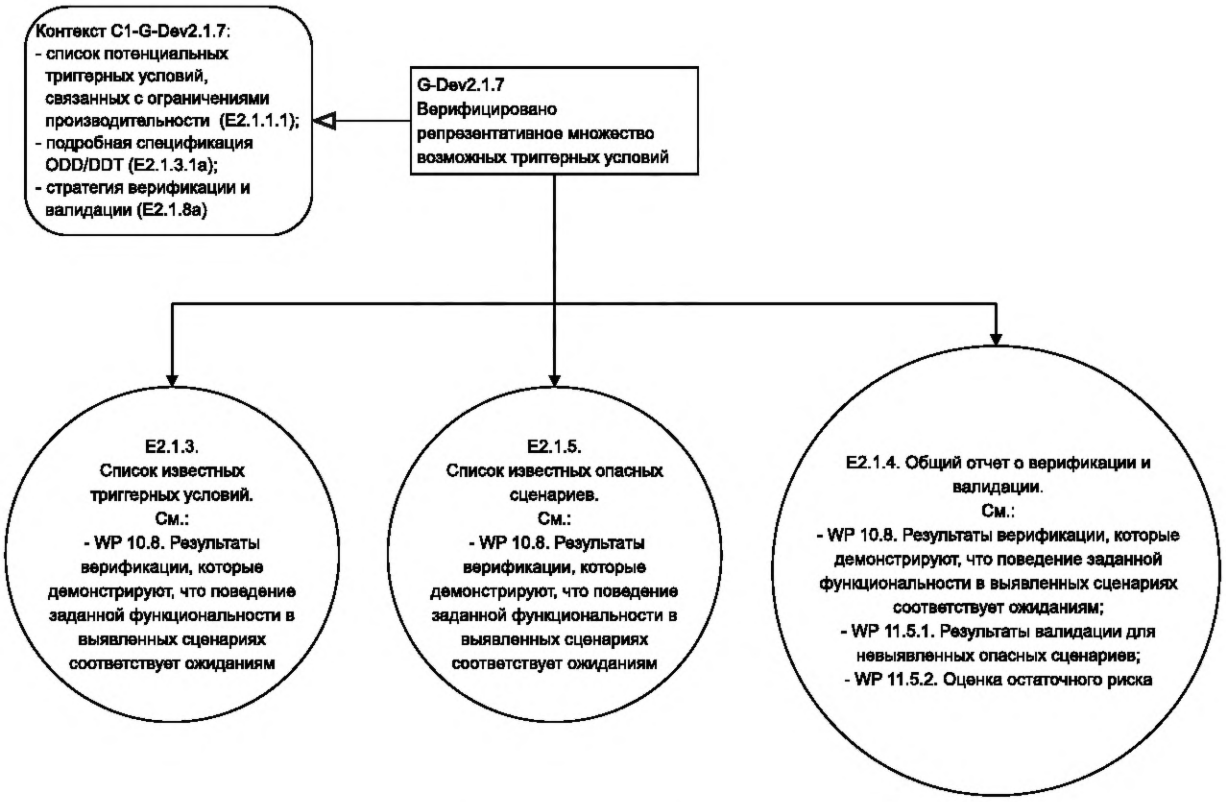


Рисунок А.5 — G-Dev2.1.7

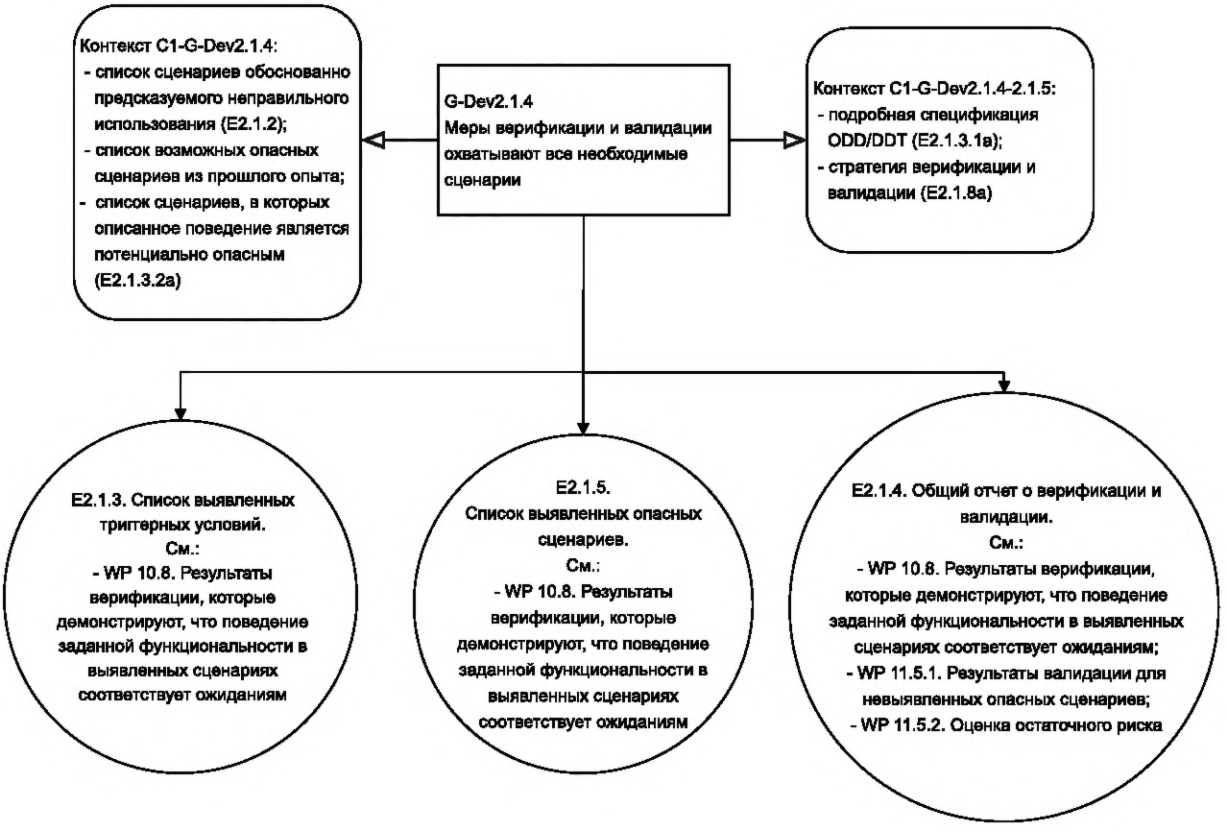


Рисунок А.6 — G-Dev2.1.4

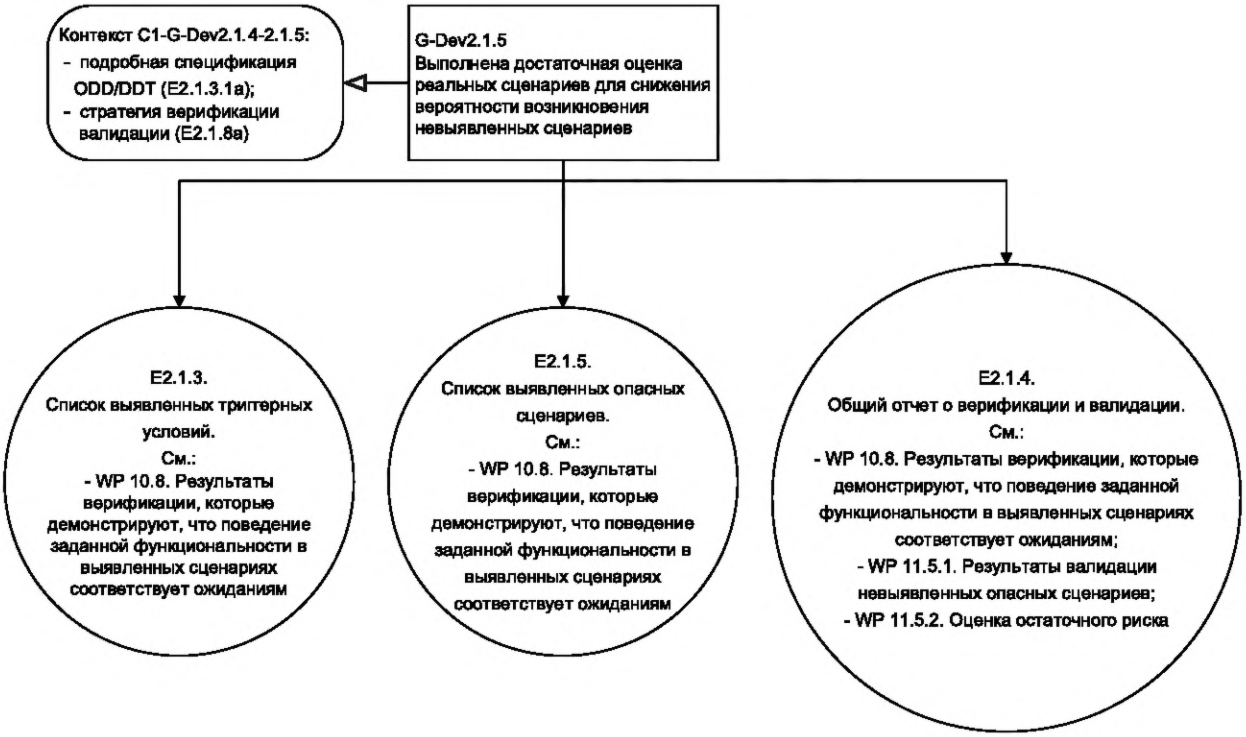


Рисунок А.7 — G-Dev2.1.5

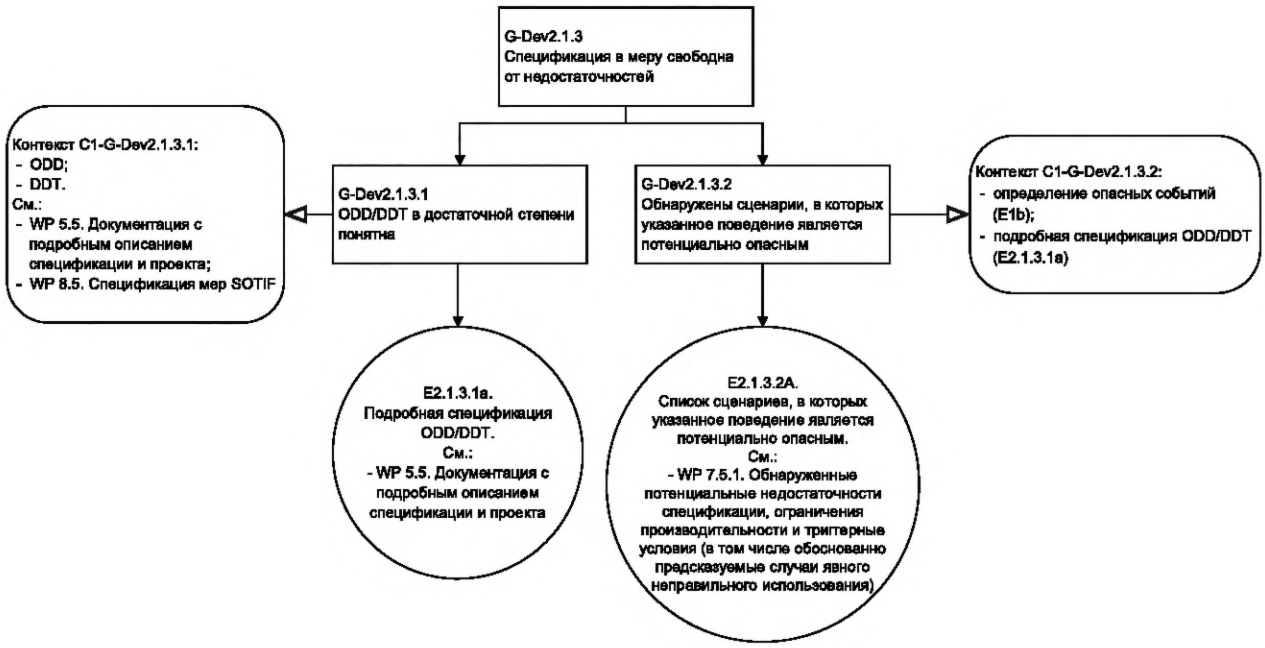


Рисунок А.8 — G-Dev2.1.3: спецификация в меру свободна от недостаточностей

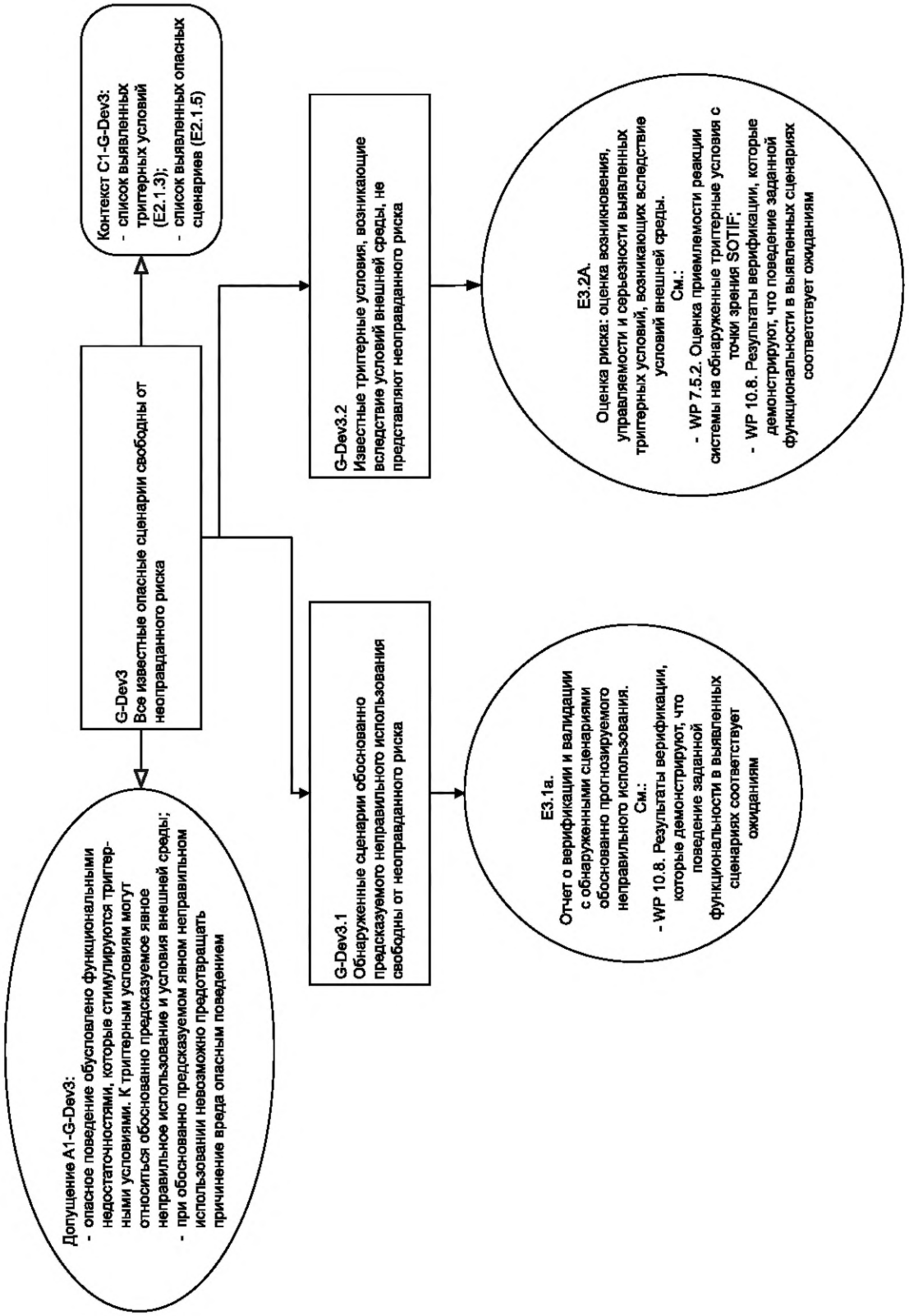


Рисунок А.9 — G-Dev3: все выявленные потенциально опасные сценарии свободны от неоправданного риска

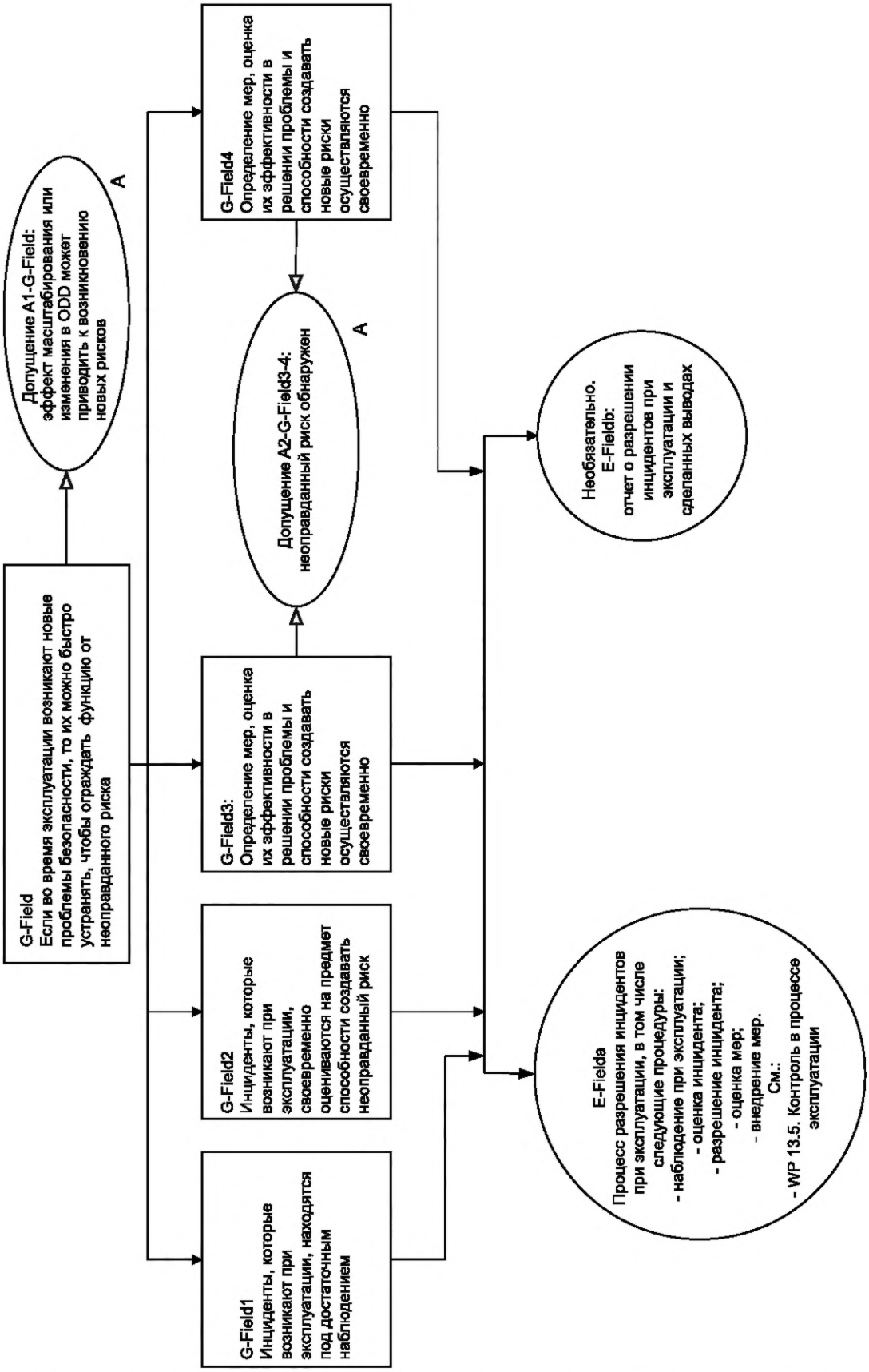


Рисунок А.10 — G-Field: если во время эксплуатации на объекте возникают новые проблемы, то их можно быстро устранять, чтобы ограждать функцию от неоправданного риска

А.1.3 GSN. Пример 2

В примере 2 (см. рисунки А.11— А.16) демонстрируется структура обоснования для поддержки приоритетной цели: «достигнуто отсутствие неоправданного риска из-за опасностей, связанных с заданной функциональностью системы или с ее обоснованно предсказуемым неправильным использованием».

Представленная структура обоснования имеет общий характер и применима ко всем системам. Она разрабатывается до подцели, где дальнейшая разработка становится зависимой от системы. На этом этапе делается ссылка на темы, упомянутые в настоящем стандарте, которые допускается использовать для дальнейшей разработки каждой подцели и предоставления необходимых доказательств.

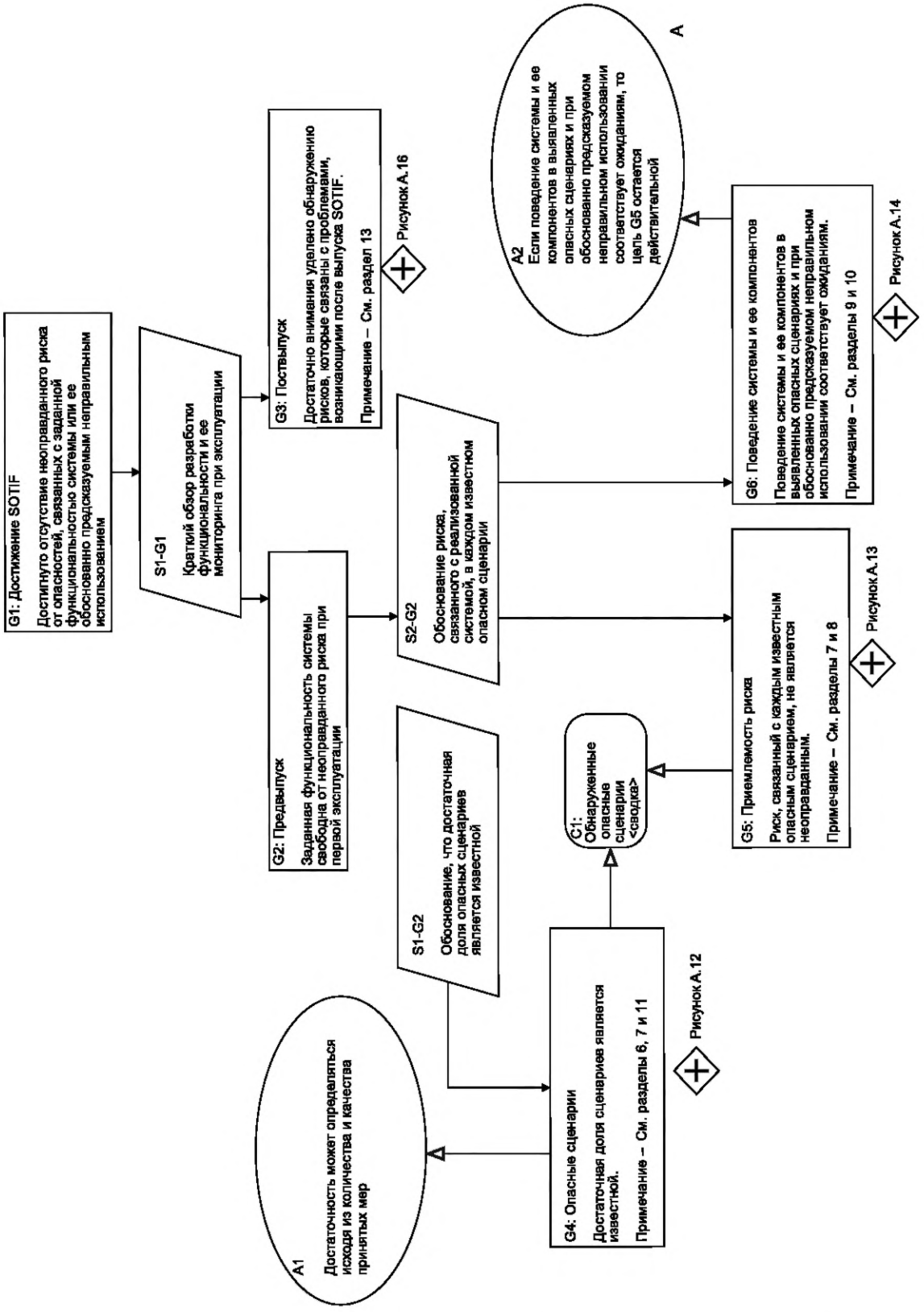


Рисунок А.11 — Достигнуто отсутствие неоправданного риска, который обусловлен опасностями, связанными с заданной функциональностью системы или ее обоснованно предсказуемым неправильным использованием

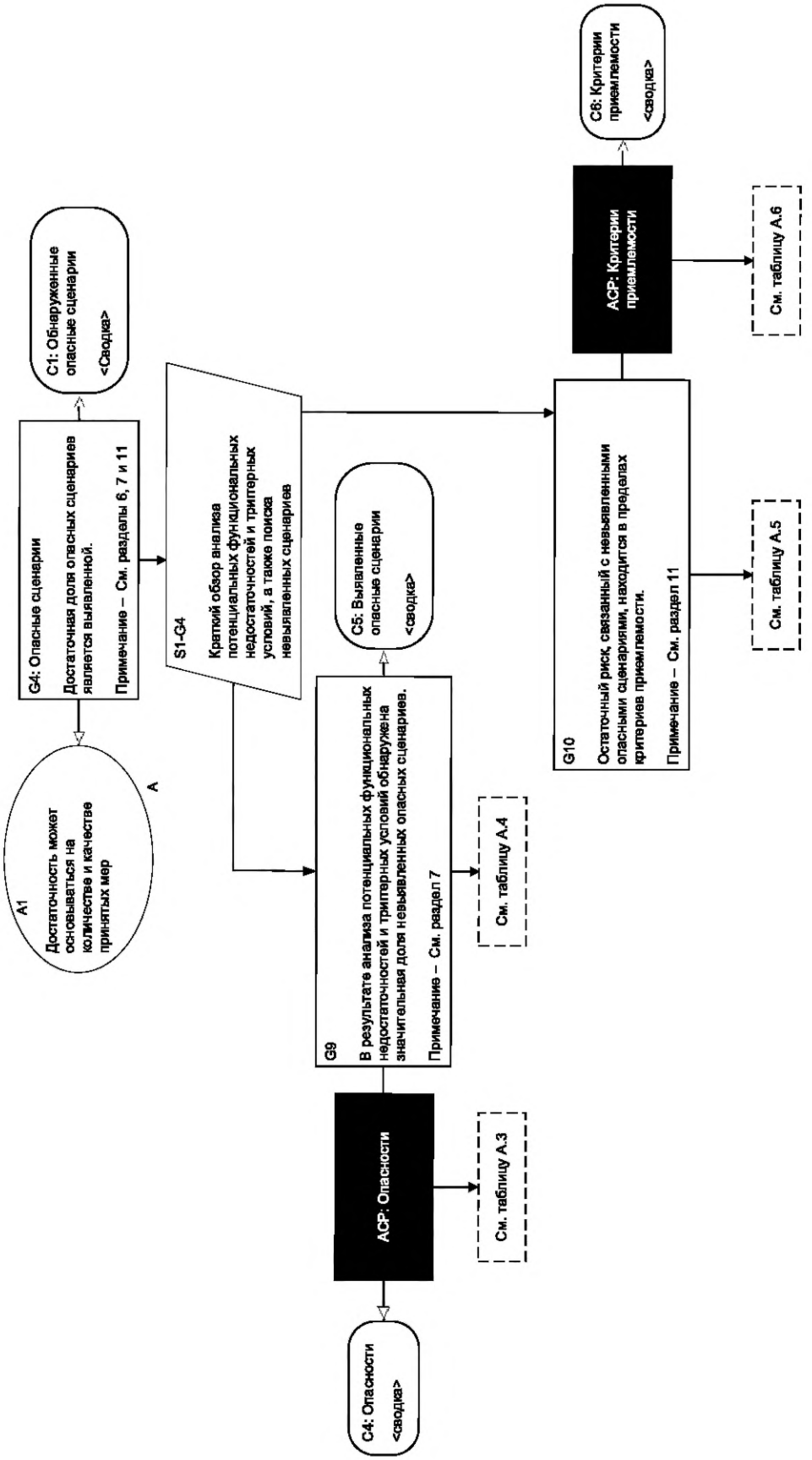


Рисунок A.12 — G4: потенциально опасные сценарии

Таблица А.3 — Темы, относящиеся к ACP: декларация об опасностях (все опасности правильно идентифицированы)

Достаточность одного или нескольких методов выявления всех опасностей, которые возникают в результате функциональных недостаточностей
Определение метода
Ресурс, затраченный на внедрение метода
Полнота и правильность оценки рисков
Возможность проверки (в соответствии с разделом 12) доказательств, полученных в результате деятельности SOTIF, для выявления возможных проблем с достижением SOTIF

Таблица А.4 — Темы, относящиеся к развитию G9 (анализ возможных функциональных недостаточностей и их триггерных условий выявил достаточную долю выявленных потенциально опасных сценариев)

Знания, полученные в ходе аналогичных проектов
Знания, полученные из опыта эксплуатации
Выявленные возможные недостаточности спецификации и производительности
Ранее выявленные внешние условия и обоснованно предсказуемое неправильное использование
Достаточность методов, которые совместно используются для выявления всех возможных функциональных недостаточностей и их триггерных условий (см. таблицу 4)
Способность каждого метода выявлять конкретные возможные функциональные недостаточности и их триггерные условия (см. таблицу 4)
Определение метода (см. таблицу 4)
Ресурс, затраченный на внедрение метода (см. таблицу 4)
Идентификация возможных функциональных недостаточностей и их триггерных условий, связанных с алгоритмами
Идентификация возможных функциональных недостаточностей и их триггерных условий, связанных с датчиками и исполнительными механизмами
Анализ обоснованно предсказуемого неправильного использования (см. таблицу 5)
Возможность проверки (в соответствии с разделом 12) доказательств, полученных в результате деятельности SOTIF, для выявления возможных проблем с достижением SOTIF

Таблица А.5 — Темы, относящиеся к разработке G10 (остаточный риск, связанный с невыявленными опасными сценариями, находится в пределах критериев приемлемости)

Конструкция транспортного средства (например, монтажное положение)
Достаточность используемых методов для выявления ранее не выявленных сценариев (таблица 11)
Способность каждого метода выявлять конкретные возможные недостаточности производительности и их триггерные условия (см. таблицу 11)
Определение метода (см. таблицу 11)
Рассмотрение новых выявленных сценариев

Таблица А.6 — Темы, относящиеся к ACP: заявление об опасности (критерии приемлемости определены правильно)

Соответствие установленным критериям приемлемости
Усилия считаются достаточными
Применимые государственные и отраслевые правила
Определение доверия, которое должно быть продемонстрировано для SOTIF
Использование имеющихся данных о дорожном движении для целевого рынка (см. С.2.2.4)
Использование ранее существовавших критериев для аналогичных функций, используемых в этой области
Обоснование выбранной цели — например GAMAB, ALARP, MEM

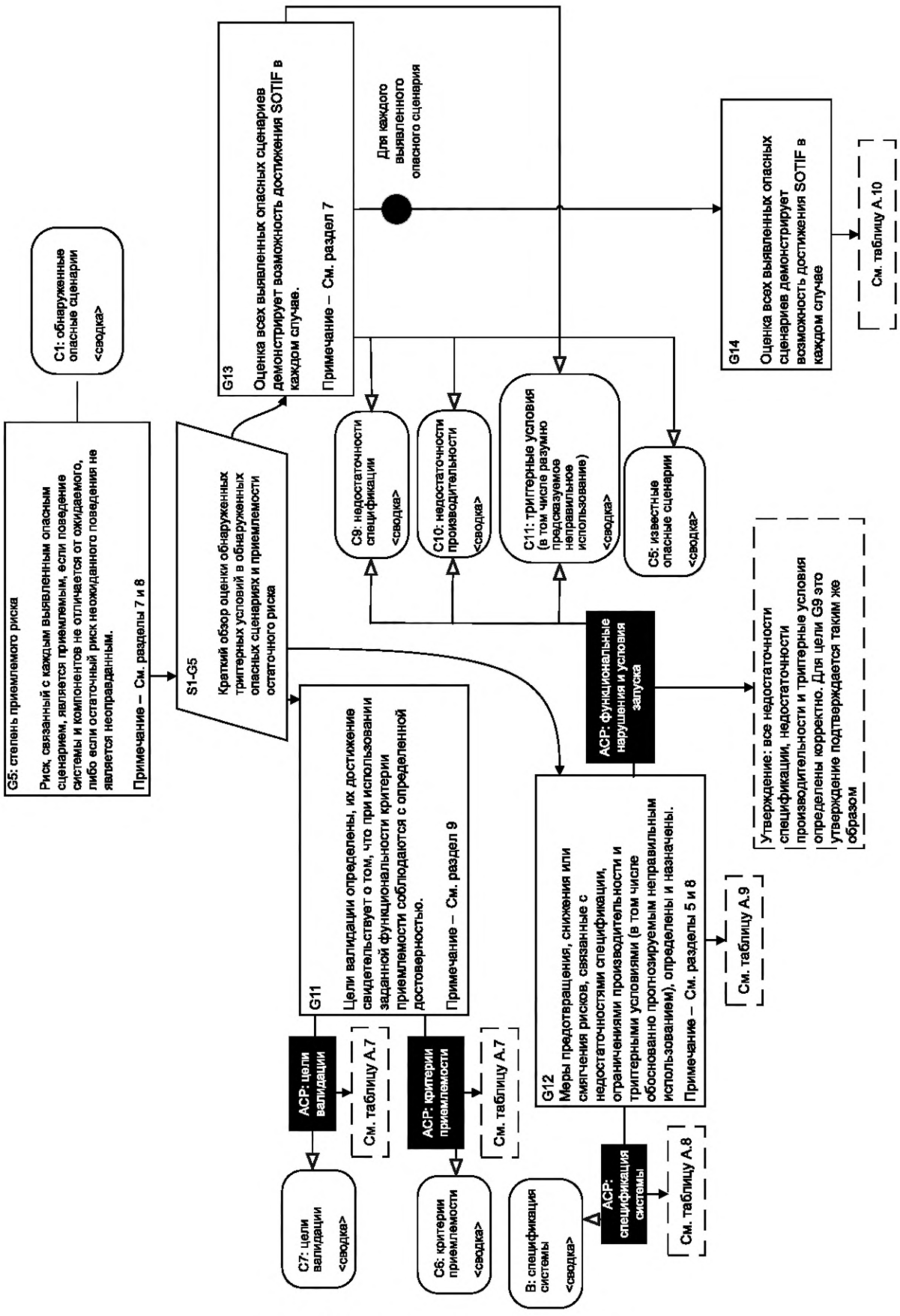


Рисунок A.13 — G5: степень приемлемого риска

Таблица А.7 — Темы, относящиеся к ACP: подтверждение целевых показателей валидации (целевые показатели валидации установлены корректно)

Воздействие подмножества сценариев
Учет воздействия, управляемости и серьезности при оценке триггерных условий

Таблица А.8 — Темы, относящиеся к ACP: заявление о спецификации системы (спецификация системы определена полностью и корректно)

Полнота и корректность определения ODD
Полнота и корректность описания логики принятия решений промежуточного уровня
Полнота и корректность описания транспортного средства, а также элементов, которые могут включать в себя систему, подсистему, компоненты и т. п., реализующие заданную функциональность
Полнота и корректность описания деталей полномочий и уровней автоматизации управления функцией управления динамикой транспортного средства
Пригодность целевых характеристик
Полнота и корректность описания сценариев обоснованно предсказуемого неправильного использования
Полнота и корректность описания интерфейсов и взаимодействий
Полнота и обоснованность предположений
Полнота и корректность описания ограничений системы, подсистем и их контрмер
Полнота и корректность описания архитектуры системы, поддерживающей контрмеры
Полнота и корректность описания концепции предупреждения об ухудшении характеристик
Полнота и корректность описания сбора данных для поддержки заданной функциональности
Полнота и корректность описания целевых показателей
Полнота и корректность описания выявленных возможных недостаточностей производительности и их контрмер
Полнота и корректность описания эффективности итерационного процесса актуализации спецификации
Полнота и корректность описания эффективности процесса управления распределенной разработкой
Полнота и корректность описания ограничений системы
Полнота и корректность описания устойчивости, обеспечиваемой конечной архитектурой системы
Возможность проверки (в соответствии с разделом 12) доказательств, полученных в результате деятельности SOTIF, для выявления возможных проблем с достижением SOTIF

Таблица А.9 — Темы, относящиеся к разработке G12

Использование мер «предотвращения»
Использование мер «сокращения»
Использование мер «снижения»
Предотвращение или снижение рисков, связанных с SOTIF, посредством модификаций системы
Использование мер по ограничению заданной функциональности
Использование мер по передаче полномочий от системы водителю
Использование мер для сокращения или ослабления последствий обоснованно предсказуемого неправильного использования
Адекватность процесса обновления спецификации системы с учетом модификаций

Таблица А.10 — Темы, относящиеся к разработке G14

Использование экспертного заключения
Сравнение остаточного риска с критериями приемлемости, указанными в 6.5
Отсутствие выявленных сценариев, которые могут привести к неоправданному риску для конкретного транспортного средства

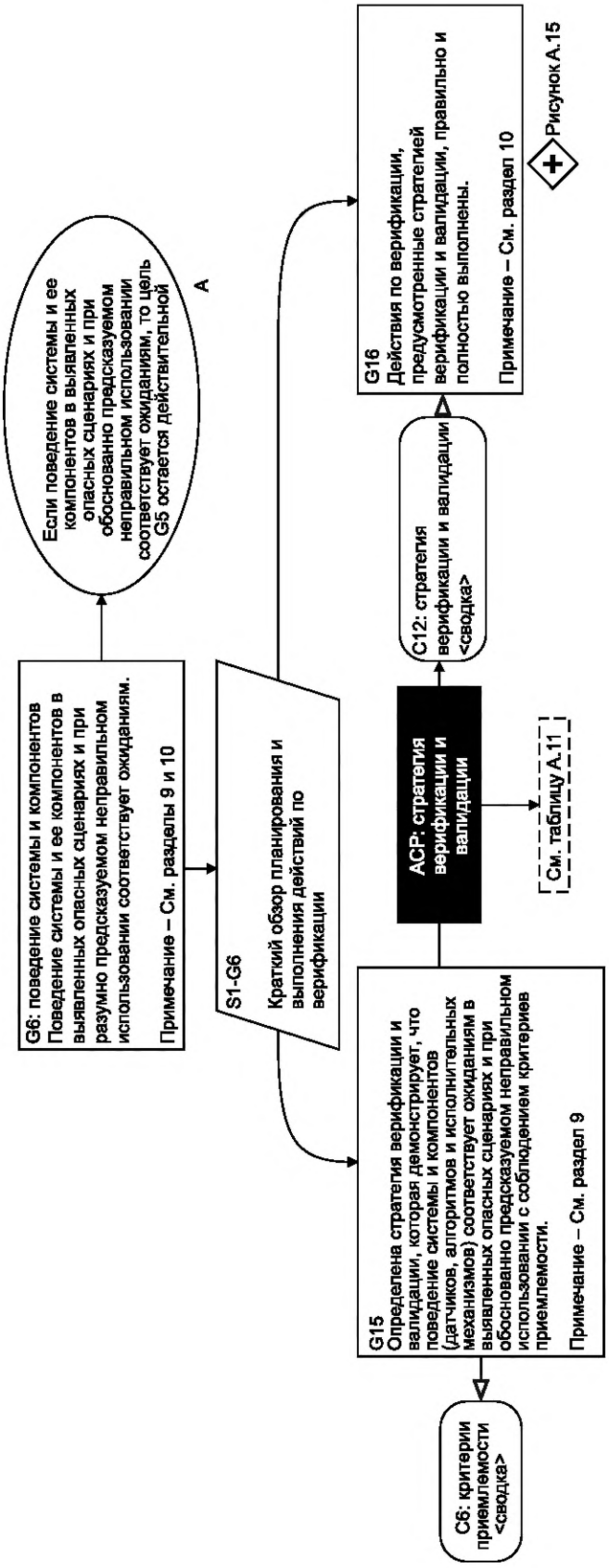


Рисунок А.14 — G6: поведение системы и компонентов

Таблица А.11 — Темы, относящиеся к ACP: стратегия верификации и валидации (стратегия верификации и валидации определена корректно)

Охват выявленных сценариев
Воздействие подмножества сценариев
Учет воздействия, управляемости и серьезности при оценке сценария с опасным поведением
Обоснование методов, используемых для определения действий по верификации и валидации (см. таблицу 6)
Способность стратегии верифицировать возможность датчиков предоставлять точную информацию о внешней среде
Способность стратегии верифицировать возможность алгоритмов обработки данных датчиков точно моделировать внешнюю среду
Способность стратегии верифицировать возможность алгоритмов принятия решений безопасно реагировать на ограничения технических возможностей элементов
Способность стратегии верифицировать возможность алгоритмов принятия решений принимать соответствующие решения в соответствии с моделью внешней среды и архитектурой системы
Способность стратегии верифицировать устойчивость системы или функции
Способность стратегии верифицировать отсутствие неоправданного риска из-за опасного поведения заданной функциональности
Способность стратегии верифицировать возможность ЧМИ предотвращать обоснованно предсказуемое неправильное использование
Способность стратегии верифицировать эффективность сценария перехода на резервный вариант
Обоснование выбранных методов (см. таблицы 7—10)
Адекватность выбранных методов (см. таблицы 7—10)
Возможность проверки (в соответствии с разделом 12) доказательств, полученных в результате деятельности SOTIF, для выявления возможных проблем с достижением SOTIF

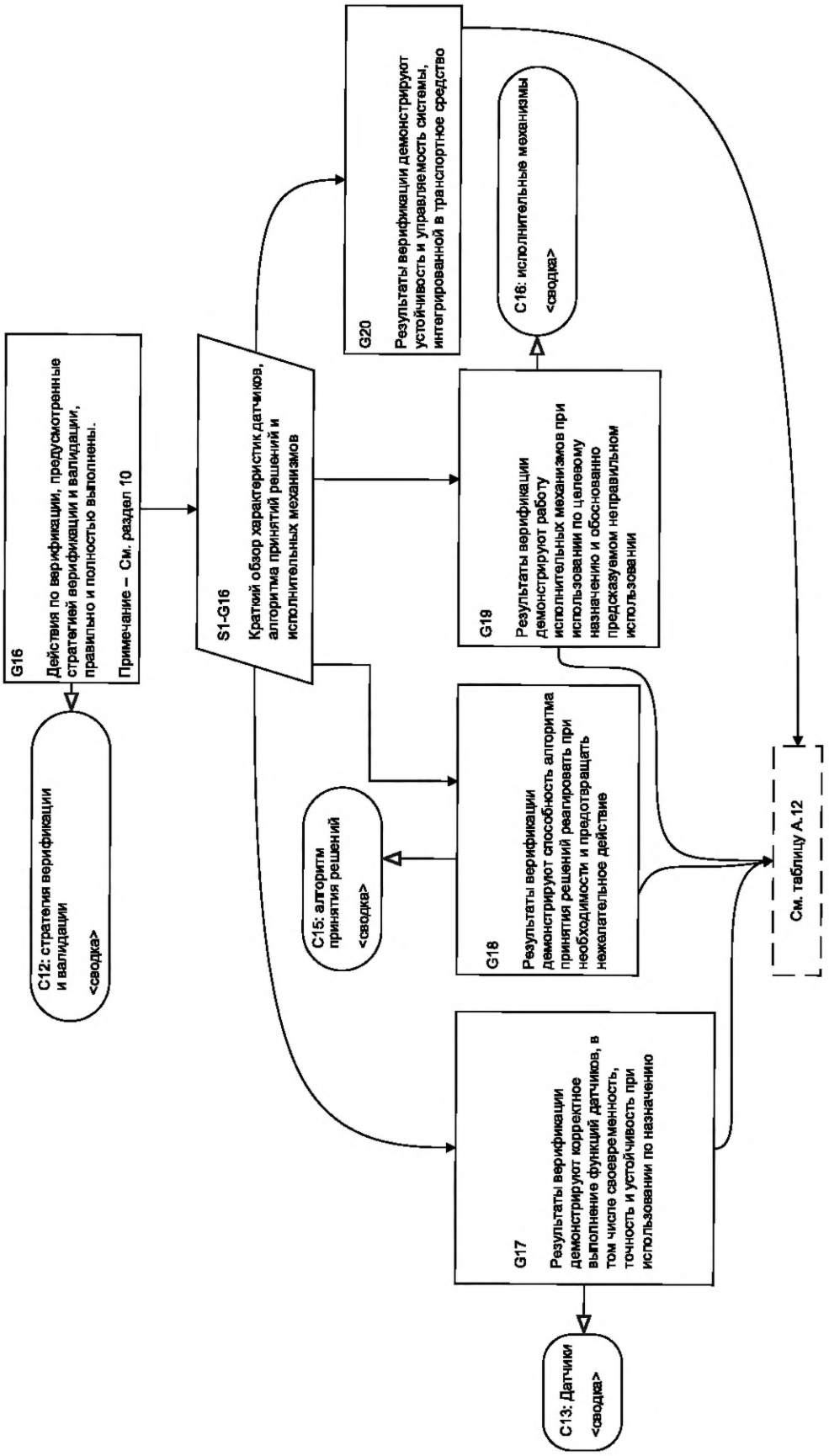


Рисунок А.15 — G16

Таблица А.12 — Задачи, связанные с реализацией целей G17, G18, G19, G20

Конструкция транспортного средства (например, монтажное положение)
Охват выявленных сценариев
Соответствие критериям приемлемости
Охват триггерных условий
Обоснование выбранных методов (см. таблицы 7—10)
Адекватность выбранных методов (см. таблицы 7—10)
Определение метода (см. таблицы 7—10)
Ресурс, затраченный на внедрение метода (см. таблицы 7—10)
Возможность проверки (в соответствии с разделом 12) доказательств, полученных в результате деятельности SOTIF, для выявления возможных проблем с достижением SOTIF

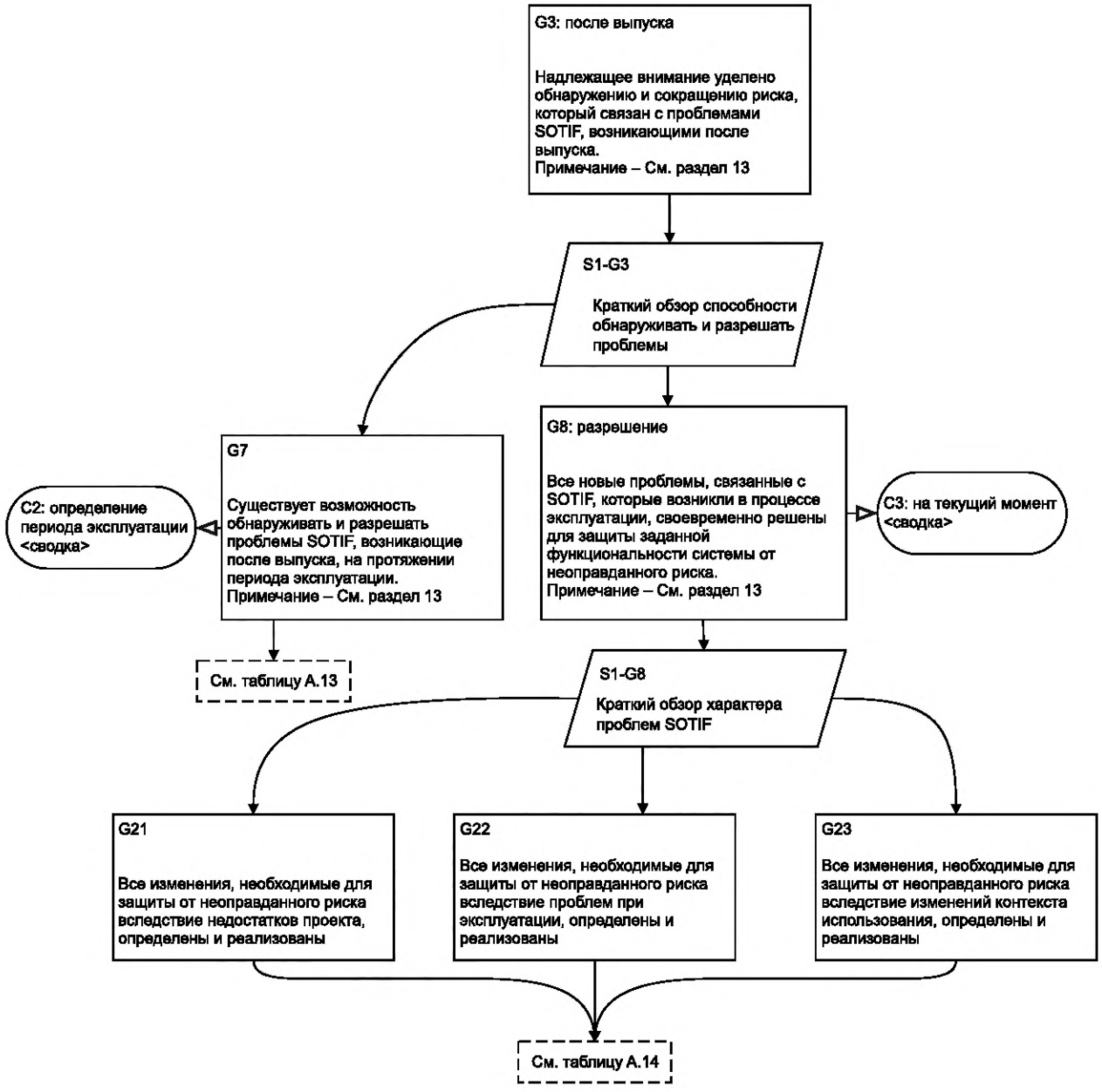


Рисунок А.16 — G3: после выпуска

Таблица А.13 — Темы, относящиеся к разработке G7

Адекватность бортовой и внешней инфраструктуры для мониторинга функциональных недостаточностей при эксплуатации
Способность выявлять возможные недостатки системы и реагировать на них
Способность выявлять и исправлять недостатки проекта
Способность выявлять изменения режимов работы и реагировать на них
Способность собирать данные в процессе эксплуатации
Способность выполнять мониторинг проблем, связанных с SOTIF, в том числе неправильного использования системы
Способность выявлять проблемы с помощью данных об эксплуатации
Способность отслеживать изменения в контексте применения
Способность анализировать и оценивать выявленные риски
Способность снижать выявленные риски

Таблица А.14 — Задачи, связанные с реализацией целей G21, G22, G23

Выявление возможных недостатков системы и реагирование на них
Выявление и исправление недостатков проекта
Выявление и реакция на изменения в процессе эксплуатации
Использование сбора данных контроля в процессе эксплуатации для расширения баз данных деятельности SOTIF
Мониторинг проблем, связанных с SOTIF, в том числе неправильного использования системы
Выявление возможных недостатков посредством контроля в процессе эксплуатации
Мониторинг уровня знаний для выявления возможных недостатков
Мониторинг изменений контекста применения для выявления возможных недостатков
Анализ и оценка выявленных рисков
Снижение рисков

А.2 О соотношении функциональной безопасности в стандартах серии ИСО 26262 и настоящем стандарте

А.2.1 Общие положения

В настоящем подразделе описано соотношение функциональной безопасности в стандартах серии ИСО 26262 и настоящем стандарте, чтобы показать возможности для взаимодействия между ними, а также приведены соответствующие примеры.

Для простоты некоторые аспекты деятельности или результатов работы рассматриваются не полностью; настоящий подраздел не претендует на полноту изложения.

А.2.2 Сравнение областей применения стандартов серии ИСО 26262 и настоящего стандарта

А.2.2.1 Общие положения

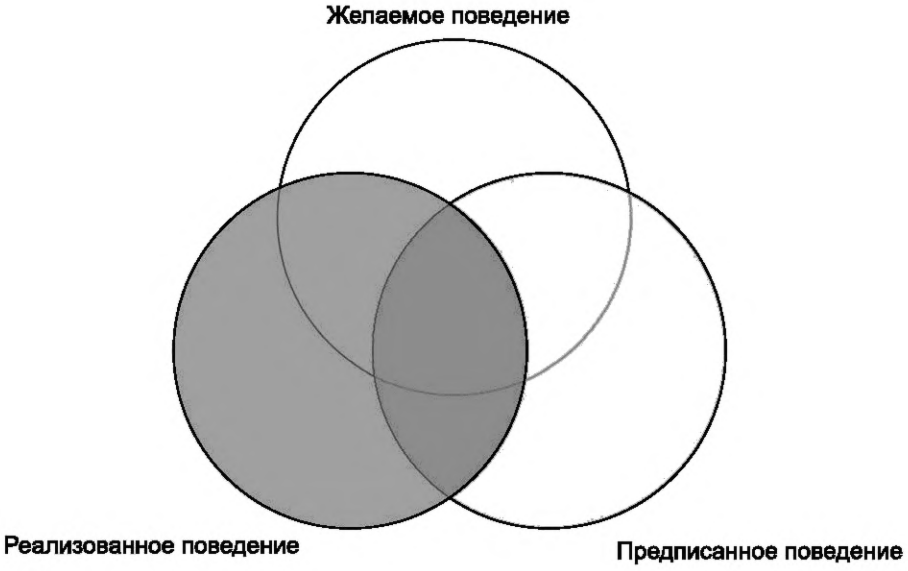
Различия и сходства указанных стандартов рассматриваются с помощью двух различных подходов:

трехкруговая модель поведения;

причинно-следственная классификация проблем безопасности.

А.2.2.2 Трехкруговая модель поведения

Различия и совпадения областей применения стандартов серии ИСО 26262 и настоящего стандарта проиллюстрированы с помощью трехкруговой модели поведения на рисунке А.13 в [15].



Примечание 1 — Пересечение между тремя кругами имеет небольшую площадь только в иллюстративных целях и не отражает реальную ситуацию.

Рисунок А.17 — Трехкруговая модель поведения

На рисунке А.17 каждый круг представляет отдельный аспект поведения:

- желаемое поведение — идеальное (а иногда и мотивирующее) поведение с точки зрения безопасности, в котором не учитываются никакие технические ограничения. Оно отражает ожидания пользователя и общества от поведения системы.

Пример 1 — Функция автоматического вождения, которая всегда работает исправно и не приводит к авариям.

Пример 2 — Желаемым поведением AEB является 100 % истинно-положительных торможений и 0 % ложноположительных торможений.

Примечание 2 — Желаемое поведение не всегда документируется со всеми возможными аспектами;

- предписанное поведение — представление желаемого поведения с учетом различных аспектов (например, юридических, технических, коммерческих, приемлемости для клиентов).

Примечание 3 — В соответствии с разделом 3 заданная функциональность определяется как предписанная функциональность. Следовательно, заданное поведение, определяемое как поведение заданной функциональности, является синонимом предписанного поведения;

- реализованное поведение — поведение реальной системы.

Сравнивая области применения стандартов серии ИСО 26262 и настоящего стандарта, можно сделать следующие выводы:

- стандарты серии ИСО 26262 исключают из рассмотрения аспект безопасности номинального поведения, а в настоящий стандарт явно включена безопасность предписанного поведения на уровне транспортного средства, что соответствует номинальному поведению;
- стандарты серии ИСО 26262, в отличие от настоящего стандарта, рассматривают проблему случайных сбоев Э/Э аппаратных средств, однако реакция на случайный сбой аппаратного компонента, т. е. работа в аварийном режиме, может быть связана с обеспечением SOTIF;
- обоснование соответствия реализованного поведения спецификациям является задачей стандартов серии ИСО 26262, а для некоторых сложных систем (например, ADAS, AD-систем) — задачей настоящего стандарта. Для таких систем стандарты серии ИСО 26262 не дают достаточных указаний об указанном обосновании. Это связано с проблемой открытого контекста — невозможно описать реальный мир со 100 %-ной точностью или подтвердить правильность его восприятия со 100 %-ной достоверностью. В область применения настоящего стандарта входят системы, в которых для восприятия и классификации внешней среды и получения управляющих действий на основе этой информации используются сложные алгоритмы и датчики, такие как видео, радары или лидары.

Пример 3 — Система, оснащенная камерами, реализует функцию обнаружения людей. Алгоритм может ошибаться при классификации людей, когда они носят одежду определенного цвета; задать и протестировать все возможные цвета одежды не представляется возможным. В настоящем стандарте описываются дополнительные требования к стандартам серии 26262. Э/Э-элементы, относящиеся к SOTIF, рассматриваются как элементы, связанные с безопасностью, согласно стандартам серии ИСО 26262.

Пример 4 — Если реализованный в программном обеспечении алгоритм обнаружения объектов может способствовать нарушению цели безопасности или ее достижению, он считается элементом, связанным с безопасностью, в терминах стандартов серии ИСО 26262-1.

А.2.2.3 Классификации причин проблем безопасности

Причинно-следственная классификация проблем безопасности и пересечение областей применения стандартов серии ИСО 26262 и настоящего стандарта показаны на рисунке А.18.

Рисунок А.18 — Причинно-следственная классификация проблем безопасности

Примечание 1 — Эта классификационная схема фокусируется только на проблемах безопасности, связанных с Э/Э-системами, которые рассматриваются в стандартах серии 26262 и настоящем стандарте. Для простоты другие вопросы безопасности (например, связанные с опасностью поражения электрическим током) исключены из рассмотрения.

Схема включает в себя следующие классификации:

Класс причин 1: систематические проблемы.

Этот класс содержит аспекты безопасности, которые могут быть связаны с систематическими проблемами. Этот класс можно разделить на следующие классы:

- класс причин 1.1: проблемы предписанного поведения на уровне транспортного средства;
- класс причин 1.2: проблемы с реализацией предписанного поведения.

Класс причин 2: случайные сбои аппаратных средств.

Этот класс содержит проблемы безопасности, вызванные случайными сбоями аппаратных средств, которые рассматриваются в стандартах серии ИСО 26262.

Класс причин 1.1: проблемы предписанного поведения на уровне транспортного средства.

Этот класс содержит проблемы безопасности, вызываемые предписанным поведением на уровне транспортного средства. В настоящем стандарте рассматривается риск, возникающий в результате предписанного поведения на уровне функциональных возможностей транспортного средства, при котором для обеспечения безопасности необходима достаточная ситуационная осведомленность. Ситуационная осведомленность достигается за счет сложных датчиков и алгоритмов обработки (например, обнаружение объектов с помощью камеры, лидара или

радара). В настоящем стандарте причины этого класса обозначены как недостаточности спецификации на уровне транспортного средства.

Примечание 2 — Аспекты безопасности номинального поведения исключены из области применения стандартов серии ИСО 26262.

Класс причин 1.2: проблемы с реализацией предписанного поведения.

Проблемы этого класса вызваны недостаточностями производительности, спецификации на уровне элемента и другими проблемами проектирования и реализации.

Эти три типа систематических проблем класса причин 1.2 входят в область применения стандартов серии ИСО 26262, поскольку связаны с возможными систематическими отказами Э/Э-систем, подсистем, компонентов или других элементов, в том числе вытекающими из требований, связанных с SOTIF.

На уровне элементов в область применения настоящего стандарта входят только недостаточности производительности и недостаточности спецификации, которые связаны с заданной функциональностью, если для ее безопасности необходима надлежащая ситуационная осведомленность. Функции в области применения элемента включают в себя:

- восприятие: получение информации об окружающей среде [например, обнаружение окружающих статических и динамических объектов, определение плана улиц или местоположения целевого транспортного средства с использованием внутренних и внешних данных транспортного средства (например, V2X)];
- план: алгоритмы принятия решений (т. е. алгоритмы управления, которые вырабатывают управляющие воздействия на основе восприятия);
- действие: выполнение управляющих запросов, полученных с помощью алгоритмов принятия решений.

Примечание 3 — Если конкретную проблему безопасности невозможно однозначно классифицировать как проблему SOTIF или функциональной безопасности, для ее решения можно применять оба стандарта.

А.2.3 Согласование настоящего стандарта и стандартов серии ИСО 26262

Соответствие действий по разработке изделия в настоящем стандарте и стандартах серии ИСО 26262 показано на рисунке А.19. Поскольку в этих стандартах рассматриваются разные аспекты безопасности, оба процесса считаются убедительным обоснованием безопасности изделия. Согласованность действий, предусмотренных стандартами, важна при внесении изменений в проект транспортного средства и элементов, которые могут включать в себя систему, подсистему, компоненты и т. д., на ранних стадиях их жизненного цикла.

В начале процесса разработки спецификация и проект (см. раздел 5) могут приводиться в соответствие с определением устройства согласно ИСО 26262-3 (см. А.2.4).

Примечание — Раздел 5 содержит функциональные и проектные спецификации на всех уровнях абстракции. Это не относится к определению устройства, которое описывает функциональность на верхнем уровне.

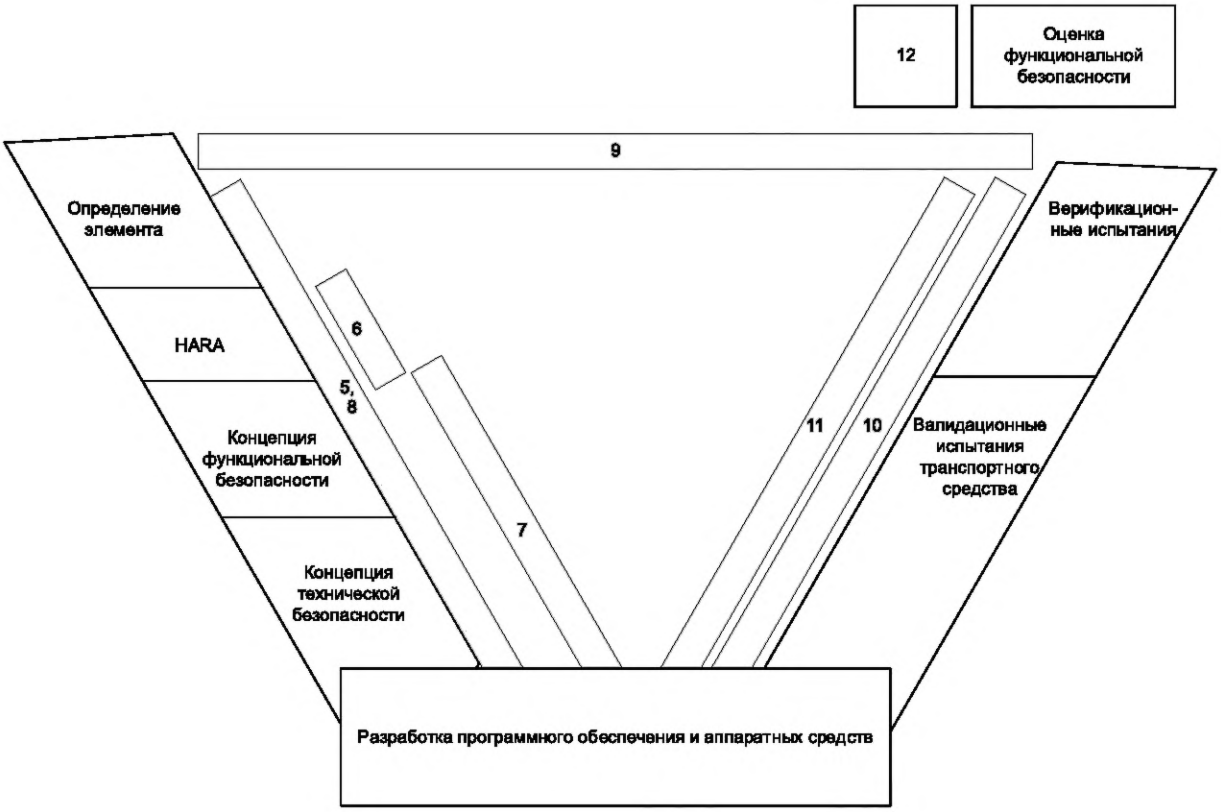
Идентификация и оценка опасностей, вызванных заданной функциональностью, согласуется с анализом опасностей и оценкой рисков (HARA) по ИСО 26262-3 (см. А.2.5). При идентификации и оценке недостаточностей производительности и их возможных триггерных условий рассматриваются ограничения системы, а их приемлемость оценивают с точки зрения SOTIF (см. А.2.7). Этот этап может соответствовать определению функциональной концепции и концепции технической безопасности стандартов серии ИСО 26262 (см. А.2.6 и А.2.7).

Функциональные модификации для снижения рисков SOTIF (в соответствии с разделом 8) можно приводить в соответствие с левой частью V-модели стандартов серии ИСО 26262.

Деятельность по оценке недостаточностей производительности и их возможных триггерных условий на уровне компонентов аппаратных средств (HW) и программного обеспечения (SW) может приводиться в соответствие с деятельностью по разработке аппаратных средств и программного обеспечения стандартов серии ИСО 26262. Руководство по совместной разработке SOTIF и процедур с универсальными элементами безопасности (SEooC) приведено в 4.4.2. Тема вспомогательных процессов ИСО 26262-8 рассмотрена в А.2.9.

Верификация и валидация SOTIF согласуется с соответствующими видами деятельности стандартов серии ИСО 26262 в правой части V-модели (см. А.2.10). Определение стратегии верификации и валидации SOTIF составляется на основе информации, полученной на предыдущих этапах разработки SOTIF.

Разработка завершается оценкой достижения SOTIF и оценкой функциональной безопасности версии всей системы. Мониторинг действий по эксплуатации соответствует требованиям процессов контроля при эксплуатации согласно ИСО 26262-7.



— этап процесса серии стандартов ИСО 26262;

x — этап процесса настоящего стандарта (число X указывает на соответствующий раздел)

Рисунок А.19 — Возможные взаимодействия при разработке изделия между настоящим стандартом и стандартами серии ИСО 26262

А.2.4 Определение и спецификация функциональности устройства на уровне транспортного средства

Начальной точкой в настоящем стандарте является спецификация функциональности на уровне транспортного средства. Для стандартов серии ИСО 26262 — это определение устройства.

Примечание 1 — Устройством является система или комбинация систем, реализующих функцию транспортного средства или ее часть. Функция транспортного средства может реализовываться несколькими устройствами; в этом случае различают функцию транспортного средства и функции отдельных устройств.

Примечание 2 — Устройство может вносить вклад в реализацию нескольких функций транспортного средства, что требует создавать их спецификации (или спецификации их подмножества) в составе определения устройства.

Примечание 3 — Функциональность, определенная на уровне транспортного средства в терминах настоящего стандарта, совпадает с функциями транспортного средства, реализуемыми одним или несколькими элементами в соответствии с серией стандартов ИСО 26262.

Пример 1 — В этом примере функция транспортного средства «автономное экстренное торможение (AEB)» реализована с помощью радиолокационного датчика, контроллера домена и тормозной системы [например, системы курсовой устойчивости (ESC)] (рисунок А.20).

Рисунок А.20 — Пример архитектуры системы

В стандартах серии ИСО 26262 допускаются различные способы определения устройств. Например, функцию транспортного средства можно реализовать в виде двух устройств (одно устройство включает в себя радарный датчик и контроллер домена, а другое — ESC) или одного устройства (которое включает в себя радарный датчик, контроллер домена и ESC).

В А.2.4—А.2.10 устройство определяется таким образом, что оно реализует всю функцию транспортного средства, т. е. функция устройства тождественна функции транспортного средства.

Примечание 4 — Для простоты в этом примере не учитываются другие функции, реализуемые данным устройством.

Пример 2 — Спецификация функциональности AEB на уровне транспортного средства: функция AEB запускает максимальное тормозное усилие:

- если препятствие обнаружено и столкновение неизбежно (т. е. невозможно предотвратить столкновение, но можно уменьшить тяжесть последствий);

- со снижением максимальной скорости на x км/ч.

Примечание 5 — Изменения, направленные на улучшение SOTIF (например, функциональные модификации, введение новых элементов), также могут влиять на определение устройства.

А.2.5 HARA, идентификация и оценка опасностей, вызванных заданной функциональностью

А.2.5.1 Общие положения

В стандартах серии ИСО 26262 основное внимание уделяется Э/Э-функциям, а в HARA некорректное поведение анализируется исходя из возникающих опасностей на уровне транспортного средства. На этом уровне поведение, которое приводит к опасности, не зависит от причины возникновения — Э/Э-отказа или небезопасной заданной функциональности (или даже проблемы безопасности). Однако степени этих опасностей могут различаться, поскольку при опасном поведении заданной функциональности может учитываться влияние ограничений (например, ограничения максимального замедления AEB). Следовательно, опасности и неполадки, которые обнаруживаются в процессе HARA, могут быть такими же или схожими с теми, которые рассматриваются для SOTIF.

А.2.5.2 Анализ опасностей и оценка рисков (HARA) по ИСО 26262-3

HARA позволяет выявлять функциональные недостаточности устройства и оценивать возникающий риск.

Пример 1 — Поведение неисправного устройства AEB:

- НЕЖЕЛАТЕЛЬНОЕ автономное торможение:

- в пределах установленных пределов снижения скорости: УПБА X в результате оценки E, C и S опасных событий;

- за пределами установленных пределов снижения скорости: УПБА Y в результате оценки E, C и S опасных событий (при Y ≥ X);

- СЛИШКОМ ПОЗДНЕЕ или НЕВЫПОЛНЕННОЕ автономное торможение:

- из-за высокой управляемости (задача торможения регулярно выполняется водителем) и низкой вероятности (экстренное торможение — редкое событие) опасные события могут быть оценены как QM.

Примечание (к примеру 1) — В других системах с более высокими уровнями автоматизации вождения система может брать на себя ответственность за торможение при вождении в целом, а не только в аварийных режимах. В этом случае приведенное выше утверждение неприменимо.

На параметры HARA могут влиять функциональные модификации, обусловленные SOTIF.

Пример 2 — Функция AEB ограничивает максимальное снижение скорости при автономном торможении, что повышает управляемость следующих за ним транспортных средств во избежание наезда сзади и снижает тяжесть последствий при столкновении.

А.2.5.3 Идентификация и оценка опасностей, вызванных заданной функциональностью

В этом случае функция транспортного средства оценивается по следующим аспектам:

- Безопасно ли заданное поведение функции транспортного средства?
- Каково нежелательное поведение функции транспортного средства и является ли оно возможным источником вреда?
- Каковы риски, связанные с обоснованно предсказуемым неправильным использованием?

Пример — Идентификация и оценка рисков для AEB.

- Является ли заданное поведение на уровне транспортного средства безопасным в определенных случаях использования?
- Если заданное поведение может являться причиной аварии, то следует оценить наличие более подходящего поведения в данном контексте.

Согласно спецификации, система AEB вмешивается только если столкновение неизбежно. В этом случае водитель может тормозить с максимальным усилием; в противном случае эту задачу берет на себя система AEB. Это наилучшее возможное поведение, если водитель не желает предотвращать аварию путем бокового уклонения. В этом случае торможение может быть даже контрпродуктивным, поскольку уменьшает существующую силу, вызываемую боковым ускорением. Благодаря этому заданное поведение на уровне транспортного средства изменяется: вмешательство AEB подавляется или прерывается при крутящем моменте рулевого управления, равном *y* Н·м. При такой модификации определенное поведение на уровне транспортного средства считается безопасным.

Для простоты в данном примере не приведена дальнейшая оценка этого дополнения.

- Каково нежелательное поведение функции транспортного средства? Являются ли оно потенциальным источником вреда?
- Ложноположительное срабатывание: нежелательное торможение в пределах заданных пределов снижения скорости.
- Последующие транспортные средства не смогли отреагировать вовремя, что привело к столкновению сзади. Здесь система создает новый риск. Такое нежелательное поведение является потенциальным источником вреда и, следовательно, связано с SOTIF.
- Ложноотрицательное срабатывание: отсутствие торможения в случае неизбежного столкновения.
- Система действует исключительно как помощник, т. е. не освобождает водителя от задачи торможения и не создает впечатления, что водитель освобожден от этой задачи, поскольку система тормозит только в случае неизбежной аварии. С точки зрения SOTIF такое нежелательное поведение не создает никаких новых рисков для системы и не рассматривается как источник возможного вреда. Следовательно, это нежелательное поведение не связано с SOTIF.

Существуют системы, которые принимают на себя ответственность за задачу торможения. В этом случае вышеуказанное утверждение неприменимо и нежелательное поведение связано с SOTIF.

- Торможение вне предела снижения скорости.
- Возможность торможения в заданных пределах снижения скорости зависит от точности измерения скорости автомобиля и работы исполнительных механизмов.
- Внешние триггерные условия могут привести к торможению вне установленных пределов снижения скорости (например, порыв ветра спереди, быстрое увеличение градиента подъема), однако предполагается, что контур управления устройством быстро адаптируется к ним и поддерживает недопустимо быстрое торможение.
- Тщательно отлаженные системы эффективно реагируют на недостаточности производительности измерения скорости транспортного средства, контура управления торможением и срабатывания торможения. Им не требуется процедура SOTIF, которая описана в настоящем стандарте. Это нежелательное поведение не относится к настоящему стандарту.
- Каковы риски, связанные с обоснованно предсказуемым неправильным использованием?
- Сценарий неправильного использования: водитель делегирует задачу «торможение на объекте» системе AEB.
- В руководстве пользователя четко указано, что система лишь помогает водителю и не предотвращает столкновение, а лишь смягчает его последствия.
- Система вызывает сильный дискомфорт при торможении.

Таким образом, риск того, что водитель полностью делегирует задачу торможения системе, не является неоправданным.

Как правило, для снижения вероятности неправильного использования водитель информируется об ограничениях системы (например, с помощью руководства пользователя).

Необходимо заботиться о том, чтобы коммерческие материалы, в том числе реклама и названия изделий, не приводили к неверным ожиданиям пользователя.

A.2.5.4 Заключение

Необходимо принимать меры по согласованию результатов идентификации и оценки опасностей, вызванных заданной функциональностью, с HARA. В примере, который был использован в A.2.5, это относится к поведению при неисправности и к нежелательному поведению: «нежелательное торможение» и «отсутствие торможения при неизбежном столкновении». Нежелательное поведение, выявленное при идентификации и оценки опасностей, вызванных заданной функциональностью, и поведение в случае неисправности, выявленное в рамках HARA, могут приводить к одним и тем же опасностям.

Идентификация и оценка опасностей, вызванных заданной функциональностью и HARA, не всегда охватывают одни и те же темы. Оценка заданного поведения с точки зрения его безопасности является типичной темой SOTIF.

В рамках HARA серии стандартов ИСО 26262 только обоснованно предсказуемое неявное неправильное использование рассматривается как возможная причина снижения управляемости или повышенной серьезности при оценке опасного события, вызванного поведением неисправного устройства.

Обоснованно предсказуемое неявное неправильное использование рассматривается аналогичным образом в настоящем стандарте при оценке опасного события, вызванного опасным поведением системы. Однако

в настоящем стандарте в качестве его возможного триггерного условия также рассматривается обоснованно предсказуемое явное неправильное использование.

Некоторые аспекты этой деятельности (например, оценка управляемости) можно рассматривать как в рамках SOTIF, так и в рамках функциональной безопасности.

А.2.6 Концепция функциональной безопасности и функциональная спецификация SOTIF

Концепция функциональной безопасности определяет реакцию на сбой (например, аварийный режим, переход в безопасное состояние и т. д.). Для ADAS и систем автоматического вождения эта реакция на ошибку также может являться проблемой SOTIF. Для этих систем SOTIF определяет необходимую функциональность для безопасного выполнения указанной реакции на сбой. Задачей функциональной безопасности является обеспечение доступности определенных необходимых функций при сбое (например, посредством отказоустойчивости) или обеспечение достаточно малой вероятности возникновения сбоя (например, путем предотвращения сбоя).

Само определение безопасной реакции на сбой можно рассматривать как задачу SOTIF и как задачу функциональной безопасности.

Пример — Варианты реакции на сбой функции автоматического вождения:
- безопасная остановка на текущей полосе движения;
- движение к следующему парковочному месту.

Примечание — Соответствие функциональных модификаций раздела 8 требованиям концепции функциональной безопасности стандартов серии ИСО 26262 может достигаться путем надлежащего обмена информацией и/или анализа.

А.2.7 Концепция технической безопасности и SOTIF

В результате деятельности SOTIF проект системы может изменяться (например, из-за внедрения новых датчиков), а это, в свою очередь — влиять на концепцию технической безопасности.

Кроме того, в результате мероприятий по функциональной безопасности проект системы может подвергаться изменениям (например, путем внедрения новых датчиков), что, в свою очередь, может влиять на SOTIF.

А.2.8 Анализ безопасности

Аналитические мероприятия по обеспечению функциональной безопасности и SOTIF сосредоточены на функциональной цепочке и используют в качестве отправной точки один и тот же проект, но рассматривают его с разных точек зрения. Анализ функциональной безопасности направлен на устранение систематических проблем с реализацией определенного поведения и случайных сбоев аппаратных средств Э/Э-элементов.

Анализ SOTIF (см. раздел 7) фокусируется на функциональных недостатках, их потенциальных триггерных условиях и влиянии на поведение транспортного средства. Кроме того, в этом контексте также рассматривается обоснованно предсказуемое неявное неправильное использование (см. разделы 6 и 7).

Анализ безопасности согласно стандартам серии ИСО 26262 может использоваться в качестве входных данных для анализа SOTIF и наоборот.

Аспекты безопасности заданного поведения на уровне транспортного средства и риск, возникающий в результате обоснованно предсказуемого неправильного использования, являются уникальными для анализа SOTIF.

А.2.9 Вспомогательные процессы

В настоящем стандарте непосредственно не сформулированы требования, которые касаются собственно процесса разработки. Пригодность процесса разработки важна для достижения безопасности и рассматривается в существующих стандартах, таких как IATF 16949 и стандарты серии ИСО 26262. Например, предполагается, что вспомогательные процессы, описанные в ИСО 26262-8, при необходимости адаптируются и применяются для поддержки достижения SOTIF, например:

- аспекты SOTIF отражены в соглашении о разработке (DIA) в соответствии со стандартом ИСО 26262-8:2018, раздел 5 (см. 4.4.2);
- уверенность в использовании программных средств в соответствии с ИСО 26262-8:2018, раздел 11, может применяться к инструментальным средствам, необходимым для достижения SOTIF, с некоторыми изменениями.

Примечание 1 — Помимо явных ошибок инструментальных средств, погрешность представления реального мира инструментальными средствами моделирования может иметь особое значение в контексте SOTIF.

Примечание 2 — Точность измерения реальных данных сама по себе может иметь особое значение в контексте SOTIF.

А.2.10 Верификация и валидация

Требования функциональной безопасности и указанные тестовые примеры (см. разделы 10 и 11), относящиеся к требованиям, связанным с SOTIF, также могут учитываться в стратегии верификации и валидации (см. раздел 9).

Поскольку тестовые сценарии могут обнаруживать проблемы как SOTIF, так и функциональной безопасности, некоторые тестовые сценарии затрагивают аспекты функциональной безопасности (например, способность механизма безопасности обнаруживать случайные аппаратные сбои и сигнализировать о них) или SOTIF (например, тесты для оценки достаточности определенного поведения на уровне транспортного средства) в отдельности.

А.3 Упрощенные примеры применения SOTIF

В таблице А.15 приведено сравнение упрощенных примеров опасностей из предметной области, рассматриваемых для обеспечения SOTIF, и мер по их снижению в зависимости от увеличения автономности транспортного средства для сравнения различных видов функциональных возможностей.

Таблица А.15 — Упрощенные примеры опасностей из предметной области, рассматриваемых для обеспечения SOTIF, и мер по их снижению

	Помощь водителю (L1, см. раздел 3, таблица 2)	Частичная автоматизация вождения (L2, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Высокая автоматизация вождения (L4, см. раздел 3, таблица 2)
Пример системы	Адаптивный круиз-контроль	Адаптивный круиз-контроль в сочетании с функцией удержания на полосе движения	Автоматизация для удобства движения в пробках	Второй водитель на трассе	Роботакси
Описание системы	Эта функция расширяет возможности стандартного автомобильного круиз-контроля, используя датчик для обнаружения идущего впереди транспортного средства. Если ведущее транспортное средство приближается слишком близко, функция замедляет транспортное средство до скорости ведущего автомобиля	Эта функция использует датчики для удержания транспортного средства в центре полосы движения и обнаружения впереди идущего транспортного средства для регулирования скорости транспортного средства и поддержания заданного интервала движения	Эта функция использует датчики для поддержания безопасного продольного расстояния от впереди идущего транспортного средства в пробке на шоссе. Она включает в себя рулевое управление для удержания транспортного средства на полосе движения	Эта функция использует множество различных датчиков для автономной навигации в пробке и выполняет все необходимые маневры при движении по шоссе	Эта функция использует различные датчики для автономной навигации в потоке из точки А в точку Б внутри определенной геозоны
DDT — управление боковым и продольным движением транспортного средства	Водитель и система	Система	Система	Система	Система
DDT — OEDR	Водитель	Водитель	Система	Система	Система
DDT — резервный вариант	Водитель	Водитель	Пользователь, готовый к резервному варианту [a]	Пользователь, готовый к резервному варианту [a]	Система

Продолжение таблицы А.15

	Помощь водителю (L1, см. раздел 3, таблица 2)	Частичная автоматизация вождения (L2, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Высокая автоматизация вождения (L4, см. раздел 3, таблица 2)
Варианты использования	1) Выбор скорости для поддержания расстояния до ведущего транспортного средства. 2) Поддержание желаемой скорости целевого транспортного средства в отсутствие ведущего автомобиля	1) Следование за ведущим транспортным средством по полосе движения с заданными скоростью и расстоянием между двумя автомобилями. 2) Поддержание заданной скорости и движение по полосе в отсутствие ведущего автомобиля	1) Следование за ведущим транспортным средством, движущимся со скоростью *x* км/ч или ниже, на расстоянии не более *y* м. 2) Если ведущий автомобиль меняет полосы движения, продолжается движение непосредственно за следующим ведущим транспортным средством, или водителю предлагается взять на себя управление транспортным средством в отсутствие ведущего автомобиля	Все варианты использования, связанные с шоссе (следование, удержание полосы движения, въезд в поток, обгон и т. д.)	Все варианты использования, связанные с городскими и шоссейными дорогами (следование, обгон, въезд в поток, остановка при регулировании дорожного движения и т. д.)
Рабочие условия	Система работает, когда автомобиль движется со скоростью *x* км/ч или выше	Система работает, когда автомобиль находится на обнаруженной полосе движения и движется со скоростью не менее *x* км/ч	Система работает, когда транспортное средство находится в пределах геозоны (нанесенной на карту области), на допустимой полосе движения и движется со скоростью ниже *x* км/ч при различных условиях внешней среды (предполагается, что эта функция отключается при неблагоприятных условиях внешней среды, таких как густой туман, сильный дождь и т. д.)	Система работает на нанесенных на карту автомагистралях при различных условиях внешней среды (предполагается, что эта функция отключается при неблагоприятных условиях внешней среды, таких как густой туман, сильный дождь и т. д.)	Система работает в геозоне, объединяющей автомагистраль и городскую зону, при любых условиях внешней среды, кроме экстремальных погодных условий (в соответствии со спецификацией)

Продолжение таблицы А.15

	Помощь водителю (L1, см. раздел 3, таблица 2)	Частичная автоматизация вождения (L2, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Высокая автоматизация вождения (L4, см. раздел 3, таблица 2)
Пример заданного поведения/функциональности	Поддержка безопасного движения вместе с ведущим автомобилем. Если ведущий автомобиль приближается на слишком короткое расстояние, функция применяет соответствующее тормозное усилие для поддержания безопасного движения. Если обнаруживается, что ведущий автомобиль находится далеко, функция выполняет ускорение до тех пор, пока не достигается заданная пользователем скорость	Поддержка границы полосы движения и поддержка безопасного движения вместе с ведущим автомобилем.Если ведущий автомобиль приближается на слишком короткое расстояние, функция применяет соответствующее тормозное усилие для поддержания безопасного движения. Если обнаруживается, что ведущий автомобиль находится далеко, функция выполняет ускорение до тех пор, пока не будет достигнута заданная пользователем скорость. Управление боковым движением применяется для удержания в полосе движения	Система предлагает пользователю взять на себя управление при неблагоприятных условиях внешней среды, таких как густой туман (предполагается, что пользователь возьмет на себя управление перед выходом из ODD)	Объезд зоны ремонтных работ с использованием поперечных маневров и предоставлением достаточного времени и пространства другим участникам дорожного движения	Проявление осторожности в «закрытых» областях
Пример опасности SOTIF, которую необходимо снижать	Система тормозит при подъезде к мосту, ошибочно воспринимая его как неподвижный металлический объект на проезжей части	Автономный и ведущий автомобили едут по объединяемой полосе движения. Ведущий автомобиль выезжает на заданную полосу; сопровождающий его автомобиль больше не обнаруживает ведущий автомобиль и начинает ускоряться до ранее установленной круиз-контролем скорости. Водитель целевого автомобиля не может выехать на заданную полосу движения до окончания объединяемой полосы и съезжает с дороги	Готовый к резервному варианту пользователь не берет на себя управление по запросу, поскольку не замечает визуального оповещения, и система попадает в зону сильного тумана, где она не способна воспринимать объекты с приемлемой точностью	Транспортному средству не удалось успешно выполнить проезд по сужению из-за невозможности обнаружить транспортное средство с освещением и окраской, из-за которых автоматическая система ошибочно классифицировала его как номинальный горизонт	Крупногабаритное транспортное средство на соседней полосе загораживает светофор, роботакси не воспринимает его сигнал и выезжает на перекресток, когда загорается красный свет

Окончание таблицы А.15

	Помощь водителю (L1, см. раздел 3, таблица 2)	Частичная автоматизация вождения (L2, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Условная автоматизация вождения (L3, см. раздел 3, таблица 2)	Высокая автоматизация вождения (L4, см. раздел 3, таблица 2)
Пример алгоритма уменьшения последствий SOTIF	Программное обеспечение усовершенствовано, чтобы различать транспортные средства и дорожную инфраструктуру (например, стальной мост, стальное покрытие)	Эта функция имеет ограниченные полномочия на ускорение	Транспортное средство спроектировано так, чтобы иметь возможность обнаруживать мешающий сильный туман и предоставлять визуальное предупреждение пользователю, готовому к резервному использованию. Если такой пользователь не принимает на себя управление, система использует другие методы для уведомления водителя, такие как звук, прикосновение, кинематика (например, короткие тормозные импульсы)	Ортогональный и независимый алгоритм предотвращения столкновений, который по отдельности оценивает необработанные данные датчиков и проверяет, что сгенерированный путь не имеет коллизий, прежде чем его принимают контроллеры нижнего уровня	Транспортное средство анализирует данные карты совместно с данными восприятия, чтобы определить состояние светофора перед выездом на перекресток, и обнаруживает, что присутствие большого транспортного средства перекрывает светофор. Выбирается подходящее поведение

[a] Разница между водителем и пользователем, готовым к резервному варианту, заключается в том, что водитель должен постоянно контролировать ситуацию. Пользователь, готовый к резервному варианту, может не контролировать OEDR, но должен брать на себя управление по запросу в течение надлежащего периода времени.

У верификации и валидации существует множество общих аспектов независимо от уровня автоматизации вождения.

Оценка мер смягчения проблем SOTIF для выявленных потенциально опасных сценариев:

1) аналитические усилия по выявлению их новых возможных триггерных условий;

2) реализация этих мер в контексте выявленного сценария, в котором демонстрируется смягчение последствий.

Этого можно достичь, используя комбинацию испытаний на уровне подсистемы и системы на закрытой трассе, при моделировании или на открытой дороге.

Оценка мер по смягчению последствий SOTIF в отношении невыявленных потенциально опасных сценариев:

a) аналитические усилия, влияющие на стратегию верификации и валидации, с целью выявления их необнаруженных потенциальных триггерных условий;

b) рассмотрение всей области ODD на закрытой трассе, при моделировании и на открытой дороге способствует достижению цели валидации, чтобы продемонстрировать, что остаточный риск невыявленных потенциально опасных сценариев является приемлемым.

При расширении ODD (в других городах или странах) выявляются и оцениваются изменения внутри ODD и OEDR. Это может вызывать необходимость повторения мероприятий по тестированию и моделированию.

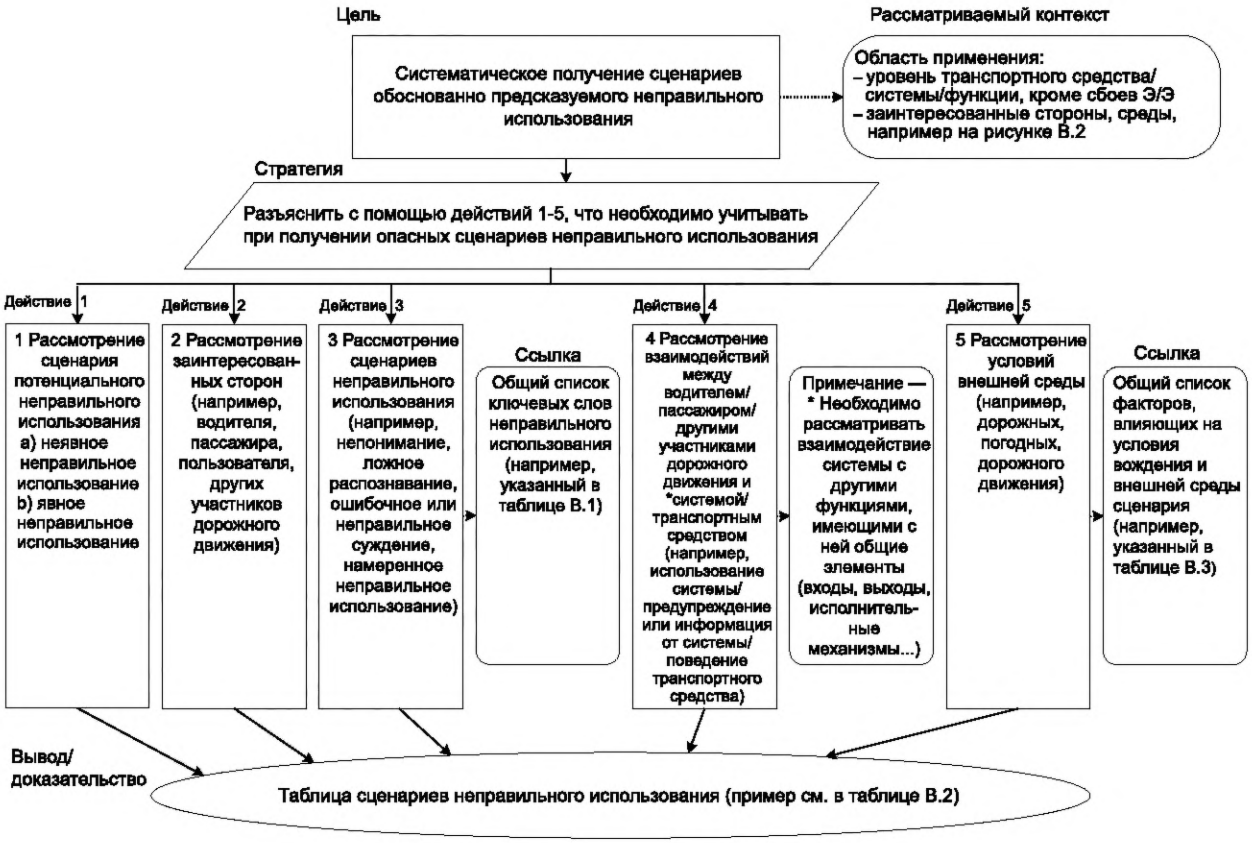
Приложение В
(справочное)

Руководство по анализу сценария и системы

В.1 Метод получения сценариев неправильного использования SOTIF

В.1.1 Общие положения

При анализе безопасности систем, связанных с SOTIF, важно учитывать их возможное обоснованно предсказуемое неправильное использование. Сценарии неправильного использования систем, связанных с SOTIF, можно получать из различных источников, в том числе приобретенного опыта, экспертных знаний, мозгового штурма с участием проектировщиков и т. д. В В.1 представлен пример методологии систематического получения сценариев неправильного использования, связанного с SOTIF, для анализа безопасности SOTIF. Обзор концепции этой методологии представлен на рисунке В.1; далее приведен пример неправильного использования, связанного с SOTIF. Подход к анализу человеческого фактора описан в [16].



Примечание — Пояснение символов каждого элемента, приведенного на рисунке В.1, см. в таблице А.1.

Рисунок В.1 — Систематическое получение сценариев неправильного использования, связанных с SOTIF (пример)

Аспекты, которые следует учитывать, и пример таблицы факторов сценариев для сценариев, содержащих неправильное использование SOTIF, представлены в В.1.2.

В.1.2 Схема метода анализа безопасности при неправильном использовании

Далее описаны аспекты, которые можно учитывать при получении сценариев неправильного использования, связанных с SOTIF.

1) Возможный сценарий неправильного использования

Рассматривают два типа случаев неправильного использования:

- обоснованно предсказуемое неявное неправильное использование в сочетании с потенциально опасным поведением системы при выявлении опасных событий;

- обоснованно предсказуемое явное неправильное использование, которое может являться триггерным условием, непосредственно инициирующим опасное поведение.

2) Заинтересованные стороны

Следует определять, кто инициирует неправильное использование систем, связанных с SOTIF, которое приводит к возникновению опасности (например, водитель, пассажир, пользователь, другие участники дорожного движения).

3) Причины неправильного использования

При рассмотрении причин неправильного использования, связанных с SOTIF, могут быть полезны общие ключевые слова из типичного процесса неправильного использования человеком (распознавание, оценка и действие).

Примеры возможных ключевых слов описаны в таблице В.1.

Таблица В.1 — Ключевые слова для обозначения человеческой ошибки

Процесс	Ключевое слово	Пример
Распознавание	1 Не понимает	Не может действовать правильно из-за сложности использования или недостатка информации
	2 Ложное распознавание	Не может правильно распознавать из-за перегруженности информацией
Суждение	3 Ошибка в суждении или неправильное суждение	Неправильное суждение из-за ошибочного представления или недопонимания (например, изменение условий размещения антенны GNSS из-за установки велосипедной стойки)
Действие	4 Упущение/ошибка	Ошибка из-за потери концентрации внимания (отвлечение, сонливость, расчет на средства автоматизации вождения и т. д.)
	5 Преднамеренный	Нарушение социальных правил, общепринятого поведения, надлежащей эксплуатации (согласно руководству пользователя)
	6 Невозможный	Трудный для выполнения

4) Взаимодействие между водителем/пользователем, системой и транспортным средством

Возможная причина неправильного использования может заключаться в непонимании или ограниченном времени взаимодействия между водителем/пользователем и интерфейсами системы/транспортного средства (см. рисунок В.2).

Например, можно получить следующие субъекты интерфейса:

- эксплуатация системы водителем (использование): интерфейс от водителя к системе/транспортному средству.

Пример 1 — Система, которая должна активироваться голосовой инструкцией водителя, также может неожиданно активироваться ключевыми словами, которые пассажиры произносят во время разговора;

- предупреждение системы: интерфейс от системы/автомобиля к водителю;
- поведение системы/транспортного средства: интерфейс от системы/транспортного средства к водителю.

Рисунок В.2 — Пример взаимодействия между водителем/пользователем, системой и транспортным средством

Примечание 1 — Прямоугольники и стрелки на рисунке В.2 имеют следующее значение:
- четырехугольники: возможные внешние факторы, взаимодействующие с системой;
- стрелка: возможное взаимодействие.

5) Учет внешних условий в вариантах использования и сценариях

Влияние внешней среды, включая дорожные условия, можно учитывать при определении неправильного использования SOTIF.

Пример 2 — Некоторые условия внешней среды, которые следует учитывать в сценариях вариантов использования, описаны в таблице В.3 или В.4.

Примечание 2 — Таблицу В.3 или В.4 можно использовать как для анализа сценариев с функциональными недостаточностями, так и для анализа сценариев, которые содержат факторы, связанные с SOTIF. В качестве альтернативы можно связывать случаи неправильного использования с действиями по выявлению опасностей (см. раздел 6) и каталогом ситуаций вождения, который используется при их выполнении.

Сценарии, которые содержат неправильное использование, связанное с SOTIF, определяют с учетом перечислений 1)— 5); в этом случае можно использовать таблицу сценариев, например, В.2.

Примечание 3 — При разработке сценариев неправильного использования, связанных с SOTIF, могут быть полезны такие методы, как HAZOP и STPA (системно-теоретический анализ процессов, пример применения которого показан в В.4).

Примечание 4 — Метод на рисунке В.1 не предназначен для всестороннего анализа всех возможных сочетаний. Методы, которые представлены на рисунке В.1, могут служить в качестве примера и использоваться в начале выполнения анализа, необходимого для конкретной разработки SOTIF. Для анализа выбираются только факторы, которые влияют на опасные события. Факторы, которые влияют на опасные события, можно регистрировать как неприменимые.

Таблица В.2 — Пример таблицы сценариев неправильного использования с ключевыми словами, аналогичной HAZOP

1) Возможный сценарий неправильного использования, связанный с SOTIF	2) Заинтересованные стороны	3) Причины неправильного использования		4) Взаимодействие между водителем и системой/автомобилем	5) Условия внешней среды (см. таблицу Б.3)	Производный сценарий опасного неправильного использования
		Процесс	Ключевые слова			
При использовании DDT уровня 2 (например, системы удержания полосы движения и адаптивного круиз-контроля на шоссе) транспортное средство не может оценить местоположение границы полосы движения из-за недостаточностей производительности. Водитель получает уведомление, если информация о границах полосы движения потеряна, поскольку система не может определить, будет ли транспортное средство покидать полосу движения	Водитель	Распознавание	1 Не понимает	Эксплуатация (использование)	…	…
				Поведение автомобиля	…	…
				Предупреждение/информация	Белая линия шоссе, поворота, полосы движения внезапно становятся нечеткой	Водитель не принимает на себя управление транспортным средством, и транспортное средство съезжает с полосы движения, т. к. водитель не понимает смысл предупреждения
			2 Ложное распознавание	Эксплуатация (использование)	…	…
				Поведение автомобиля	…	…
				Предупреждение/информация	…	…
		Суждение	3 Ошибка в суждении или неправильное суждение	…	…	…
		Действие	4 Упущение/ошибка	…	…	…
			5 Преднамеренное освобождение места водителя	…	…	…
			6 Невозможность, водитель не обращает внимание, водитель спит	…	…	…
…	…	…		…	…	…

В.2 Пример построения сценарных факторов для метода анализа безопасности SOTIF

В настоящем подразделе приведен пример методологии разработки сценариев для поддержки обнаружения опасностей (см. раздел 6), анализа безопасности (см. раздел 7) и создания сценариев верификации/валидации для выявленных и невыявленных триггерных условий (см. разделы 10 и 11).

Для выявления и оценки возможных триггерных условий, которые влияют на характеристики системы из-за характеристик ее деталей, процесса использования, физических явлений и условий внешней среды, предпринимают следующие шаги:

1 В целях выполнения данного анализа можно разделять функции системы на следующие элементы: восприятие, план, действие.

2 Создают сценарии с возможными функциональными недостатками на основе влияющих факторов (см. таблицу В.3 или В.4) для каждого элемента триггерного условия.

Примечание 1 — Для генерации сценариев, связанных с SOTIF, можно использовать таблицы генерации ситуаций HARA в контексте стандартов серии ИСО 26262.

Примечание 2 — Предложение о том, как получить репрезентативный набор конкретных сценариев испытаний для рассматриваемого маневра, также можно найти в [17].

Таблица В.3 — Примеры сценарных факторов (неисчерпывающие). Случай 1

Категория	Фактор
Погода	Отличная
	Пасмурная
	Дождливая (легкий дождь, сильный дождь)
	Мокрый снег
	Снег (накопление снега); легкий снег, сильный снег
	Град
	Туман; плотный туман, легкий туман
	Ветер
Время суток	Раннее утро
	День
	Вечер
	Ночь
Форма дороги/полосы	Прямая
	Изгиб
	Скоростной спуск
	В гору
	Дорога с насыпью
	Резкий перепад
	Неровное место (неровная дорога)
	Бельгийская кирпичная дорога
	Узкая дорога, широкая дорога
	Наличие разделительных полос
	Крышка люка
	Слияние на проезжей части
	Развилка
	Выбоина

Продолжение таблицы В.3

Категория	Фактор
Характеристика дороги	Туннель
	Подземный переход
	Мосты
	Эстакадная дорога
	Дорожная развязка типа клеверный лист
	Ромбовидная развязка
	пункт взимания дорожных сборов
	Ворота
Состояние дороги	Сухая
	Влажная
	Поверхность с низким μ
	Дорога, пересекающая на верхнем уровне другую дорогу
	Желоб для отвода воды
	Гравийная дорога
Освещение	Прямой солнечный свет (блики)
	Безлунная ночь
	Лунная ночь
	Уличный фонарь
	Подсветка
	Сумерки
Состояние целевого транспортного средства	Нерегулярное нарушение работы датчика (например, удар вызывает изменение поля обзора датчика)
	Изменения в датчике (например, люфт при сборке)
	Датчик запотел
	Датчик загрязнен (пыль, грязь, снег, лед и т. д.)
	Положение транспортного средства (например, угол обзора датчика меняется при крене транспортного средства из-за внезапного торможения)
	Ситуация с транспортным средством (например, поле зрения датчика закрыто, когда транспортное средство с датчиком буксирует большой прицеп)
	Реальная масса транспортного средства (например, с буксировкой)
	Распределение веса
	Шина (например, температура, протектор или твердость резины)
	Тормозная колодка (например, обледенение или температура)

Продолжение таблицы В.3

Категория	Фактор
Эксплуатация целевого транспортного средства	Транспортное средство ускоряется
	Транспортное средство замедляется
	Транспортное средство движется с постоянной скоростью
	Транспортное средство останавливается
	Езда на высокой скорости
	Езда на низкой скорости
	Транспортное средство делает поворот
	Транспортное средство резко отклоняется от траектории
	Обгон
	Правый или левый поворот
	Объезд зоны строительства по существующей разметке
	Приближается к перекрестку
	Кольцевая развязка
	Въезд и съезд
	Пересечение железнодорожных путей
Окружающее транспортное средство: - идущее впереди транспортное средство; - движущееся рядом транспортное средство; - встречное транспортное средство	Положение окружающего транспортного средства
	Идущее впереди транспортное средство замедляет ход
	Идущее впереди транспортное средство внезапно тормозит
	Идущее впереди транспортное средство ускоряется
	Идущее впереди транспортное средство резко ускоряется
	Блокирующее транспортное средство
	Прицепной автомобиль в транспортном потоке с частыми остановками
	Справа от целевого транспортного средства находится транспортное средство, движущееся в том же направлении
	Слева от целевого транспортного средства находится транспортное средство, движущееся в том же направлении
	Присутствует встречное транспортное средство
	Дальний свет встречного транспортного средства
	Обгон мотоцикла
	Велосипед
	Сильные помехи от окружающих транспортных средств (например, их радаров)
Другие участники дорожного движения	Пешеход
	Грузовое транспортное средство
	Мотоцикл
	Личное транспортное средство

Окончание таблицы В.3

Категория	Фактор
Внедорожные объекты (окружение)	Боковая стенка (кузова)
	Знак (различная ориентация расположения)
	Фонарный столб
	Туннель
	Парковочное место
	Под путепроводом
	Бордюр
	Ограждение
	Пилон
	Транспортное средство остановилось на обочине дороги
	Животное выпрыгивает
	Железнодорожный переезд
	Строительная площадка
	Отмеченный пешеходный переход
	Вода вдоль дороги
Объекты на проезжей части: разметка полосы движения	Цветные ретрорефлекторы «боттс-дотс» в дорожной разметке рядов, катафоты, стимсонитовые (встраиваемые) отражатели
	Сплошные линии — белые, желтые
	Пунктирные линии — белые
	Пешеходный переход
	Предохранительные полосы
	Лежачие полицейские
	информационные (стрелка, ограничение скорости, уступи дорогу, замедление и т. д.)
	Нет разметки полосы движения
	Поверхность с углублениями или насечкой
	Испорченная разметка полос движения
	Несколько полос разметки
Грязь на проезжей части	Трупы животных (в результате дорожно-транспортных происшествий)
	Мусор, следы шин и т. д.
	Твердые частицы, пыль, земля, песок и грязь
	Строительные материалы, асфальт, бетон, гвозди, шурупы и другие часто острые предметы
	Твердые предметы, выпавшие или выброшенные из движущегося транспортного средства
	Разбитое стекло, пластик и другие твердые материалы, которые остаются от транспортных средств в результате дорожно-транспортных происшествий

Таблица В.4 — Примеры структуры сценарных факторов (неполный список). Случай 2

Фактор уровня 1	Фактор уровня 2	Фактор уровня 3	Фактор уровня 4
Геометрия и топология дороги	Тип дороги	Шоссе	
		Загородная	
		Городская	
	Геометрия дороги	Прямая	
		Поворот	
	Подъем дороги	Ровная	
		В гору	
		Под гору	
	Профиль дороги	Количество полос	
		Разметка полос	
	Дорожное покрытие	Шероховатость	Асфальт
			Бетон
			Мостовая
			Гравий
		Повреждение	Трещина
			Выбоина
	Перекрестки дороги	Расходящаяся	
		Слияние	
		Пересечение двух дорог под острым углом	
		Пересечение	
Обустройство автомобильных дорог и ограничения	Граница дороги	Фонарный столб	
		Дорожное ограждение	
		Бетонный барьер	
		Шумозащитное ограждение	
		Туннель	Верхний просвет
		Мост	Верхний просвет
			Субъекты, движущиеся под мостом
	Дорожные знаки	Светофоры	
		Предупреждения	
		Ограничения	

Продолжение таблицы В.4

Фактор уровня 1	Фактор уровня 2	Фактор уровня 3	Фактор уровня 4
Временные физические ограничения	Переназначение полосы движения		
	Разметка полос движения		
	Знаки дорожных работ		
	Заграждения дорожных работ		
Движимые объекты	Типы объектов	Транспортные средства	Легковые автомобили
			Грузовики
			Автобусы
			Скоростной трамвай
			Мотоциклы
			Машины скорой помощи
			Сельскохозяйственная техника
			Самокаты
			Велосипеды
		Пешеходы	Младенцы
			Малыши
			Взрослые
		Животные	
		Объекты	
	Маневры	Средняя скорость	Высокая скорость
			Низкая скорость
		Изменение скорости	Замедление
			Ускорение
		Следование	
		Подъезд	
		Проезд	
		Смена полосы движения	Слева
			Справа
		Поворот	Налево
			Направо
		Разворот	
		Безопасная остановка	
	Относительное расположение	Слева	
		Справа	
		Перед	
		Позади	

Окончание таблицы В.4

Фактор уровня 1	Фактор уровня 2	Фактор уровня 3	Фактор уровня 4
Фактор уровня 5			
Условия окружающей среды	Время суток	Раннее утро	
		Дневное время	
		Вечер	
		Ночное время	
	Атмосферные условия	Температура	
		Видимость	
		Ветер	
		Облака	
		Осадки	Дождь
			Град
			Мокрый снег
			Снег
	Условия освещения	Солнечный свет	
		Лунный свет	
	Состояние дорожного покрытия	Сухое	
		Влажное	
		Заснеженное	
		Обледеневшее	
Фактор уровня 6			
Цифровая информация	Информация V2X		
	Данные цифровой карты		

Примечание — Определения уровней в данной таблице следующие:

уровень 1 — планировка улиц и состояние поверхности;

уровень 2 — инфраструктура управления дорожным движением (например, знаки, ограждения и разметка);

уровень 3 — наружный слой, топология и геометрия временных строительных площадок;

уровень 4 — участники дорожного движения и объекты, в том числе взаимодействия с использованием маневров;

уровень 5 — условия окружающей среды (например, погода и время суток), в том числе их влияние на уровни 1—4;

уровень 6 — цифровая информация, в том числе ее влияние на уровни 1—5.

Пример 1 — Построение варианта использования: погода — дождливо, время суток — дневное время, форма дороги — прямая, под гору, дорожные условия — влажная погода, эксплуатация целевого транспортного средства — транспортное средство останавливается, другие транспортные средства — встречные и на правой стороне, пешеход — нет, внедорожные объекты — нет.

Примечание 1 — Данные таблиц В.3 и В.4 не являются исчерпывающими; при построении сценариев можно учитывать и другие факторы, такие как местные правила вождения и инфраструктура.

Примечание 2 — При запуске анализа SOTIF для выявления возможных опасных сценариев и их триггерных условий могут быть полезны следующие категории a), b), c) функциональных недостаточностей/триггерных условий:

a) ограничение восприятия

Например, возможными триггерными условиями могут являться климат, время суток, форма дороги/полосы, состояние целевого транспортного средства, окружение транспортного средства, другие участники дорожного движения и объекты за пределами дорожного полотна;

b) условия дорожного движения

Например, триггерными условиями могут являться форма дороги/полосы, состояние дороги, окружающие транспортные средства, эксплуатация этого транспортного средства, аварии, другие участники дорожного движения и объекты за пределами дорожного полотна;

c) проблемы, связанные с автономным транспортным средством (влияющие на его характеристики или поведение).

Например, места установки датчика в целевом транспортном средстве подвержены скоплению мусора или пыли, что ограничивает его эффективность.

Примечание 3 — Триггерное условие может включать в себя не только один фактор, но и их сочетание.

Примечание 4 — Во время построения сценария сочетания факторов могут формально описываться как подмножества на основе связи этих сценарных факторов с конкретной функцией, системой/компонентом или действием SOTIF (определение ODD, планирование верификации и валидации, …). В таблице B.5 показан пример подмножества, которое можно применять при планировании валидации функции радара.

Если рассматривать в этом примере исключительно радарную систему, ночь и день не являются значимыми факторами и могут быть исключены из подмножества.

Таблица B.5 — Пример подмножества факторов (например, рассматриваемых при валидации функции радара)

Категория	Фактор	Подмножество
Климат	Дождь	Подмножество 1
Характеристика дороги	Туннель	
Время суток	Любое/безразлично	
Объекты за пределами дорожного полотна	Знак (слишком высокое расположение)	
…	…	
…	…	Подмножество *n*

Примечание 5 — Могут приниматься во внимание другие стандарты, обеспечивающие соответствующую таксономию (например, см. [18]).

B.3 Примеры применения анализа безопасности для выявления и оценки возможных функциональных недостаточностей и их триггерных условий

B.3.1 Методы анализа для систематического выявления триггерных условий

С ростом уровня автоматизации вождения триггерные условия становятся все более сложными и трудными для выявления, что требует применения различных методов анализа в сочетании с дорожными испытаниями для адекватного исследования выявленных и невыявленных опасных сценариев. При проведении анализа для выявления триггерных условий можно рассматривать следующие методы: индуктивный анализ, дедуктивный анализ, исследовательский анализ, исследовательское моделирование (с использованием передовых комбинаторных методов, используемых в этом примере, или других методов, которые считаются подходящими) и исследовательское вождение (с адекватными мерами безопасности).

Индуктивный и дедуктивный виды анализа полезны для выявления факторов, которые способствуют опасным событиям вследствие функциональных недостаточностей, недостаточностей выходов и триггерных условий, а также для изучения причинно-следственных связей между ними. Однако при использовании новых технологий (например, машинного обучения) или наличии обширного пространства сценариев в ODD нельзя утверждать, что этих видов анализов достаточно для обнаружения всех соответствующих недостаточностей и триггерных условий.

С ростом уровня автоматизации вождения может быть полезным дополнительное использование методов исследовательского анализа, если система достигает некорректного доверительного состояния, причина которого

неочевидна. Например, высокоавтоматизированная система вождения ошибочно полагает, что она находится на маршруте без столкновений или может избежать/избежала столкновения. Источником этого некорректного состояния доверия могут являться один или несколько элементов. Например, объект с высокой угрозой был ошибочно классифицирован как объект с низкой угрозой из-за близости к другим объектам с низкой угрозой либо транспортное средство не смогло пройти по маршруту из-за каких-либо физических ограничений. В этом случае можно воспользоваться, например, теоретико-системным анализом процессов (STPA), поскольку в нем рассматривается взаимодействие между системой, сценарием и человеком как источником опасности.

Наконец, исследовательское моделирование и исследовательское вождение являются полезными восходящими инструментами для выявления триггерных условий, однако у каждого из них есть свои ограничения, которые могут учитываться при применении методологии и критериев оценки достижений SOTIF.

B.3.2 Пример анализа дерева причин

На основе опасных событий, указанных в разделе 6, можно определять возможные недостаточности спецификации, недостаточности производительности и триггерные условия, используя соответствующий дедуктивный метод оценки риска (аналогично классическому методу анализа дерева отказов, который используется для обеспечения функциональной безопасности).

Примечание — Анализ дерева причин является подходящим методом определения первопричин события и может использоваться для идентификации и изучения триггерных условий конкретного опасного события.

После обнаружения недостаточностей системы и их триггерных условий можно определять сочетание событий, которые способствуют опасности, и минимальные сечения, достаточные для ее возникновения. Результат можно использовать для выявления важных потенциальных зависимостей и наиболее существенных недостаточностей, а также для определения достаточности принятых мер для снижения риска (см. 7.4). Кроме того, результаты можно использовать для задания приоритетов или даже валидации кластера.

Пример — Опасное событие внезапного нежелательного замедления анализируется в рамках системы ACC. Система состоит из регулятора, который может управлять мощностью двигателя и активировать торможение в зависимости от заданной водителем скорости, а также стереокамеры для обнаружения препятствий и измерения расстояния до объектов впереди автомобиля. Модель дерева функциональных недостаточностей представлена на рисунке B.3. На основе анализа функциональных недостаточностей минимальные сечения для события верхнего уровня G0 можно выразить следующей эквивалентной функцией булевой алгебры:

$$TOP = B01 + B02 + (B03 \cdot B04) + (B05 \cdot B06).$$

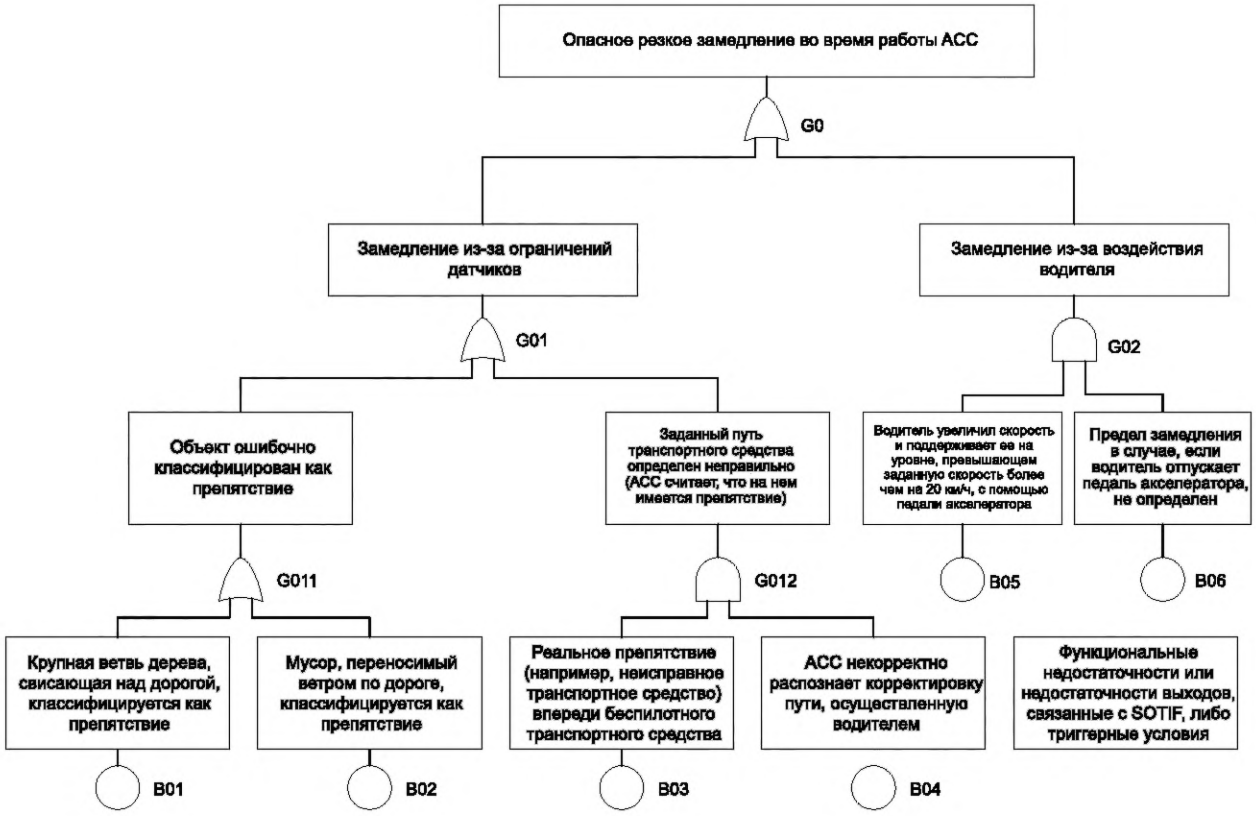


Рисунок В.3 — Анализ дерева причин

В дополнение к дедуктивному анализу, как правило, проводится индуктивный анализ для повышения полноты анализа безопасности путем анализа функционального, архитектурного и детального проектирования, а также оценки вновь выявленных опасностей, внесенных при реализации системы.

В.3.3 Пример индуктивного анализа SOTIF

В.3.3.1 Рабочий процесс индуктивного анализа SOTIF

Рабочий процесс анализа SOTIF, который показан на рисунке В.4, описывает действия, поддерживающие:

- выявление и оценку возможных функциональных недостаточностей, которые могут приводить к опасному поведению, инициируемому выявленными конкретными условиями сценариев вождения;
- выявление и оценку возможных триггерных условий, которые могут инициировать опасное поведение вследствие выявленных возможных функциональных недостаточностей;
- определение мер по модификации, позволяющих избегать рисков, связанных с SOTIF, или уменьшать их.

Порядок рассмотрения различных аспектов (от потенциальных функциональных недостаточностей до их возможных триггерных условий или от конкретных условий сценариев вождения до возможных функциональных недостаточностей) зависит от предпочтений аналитика.

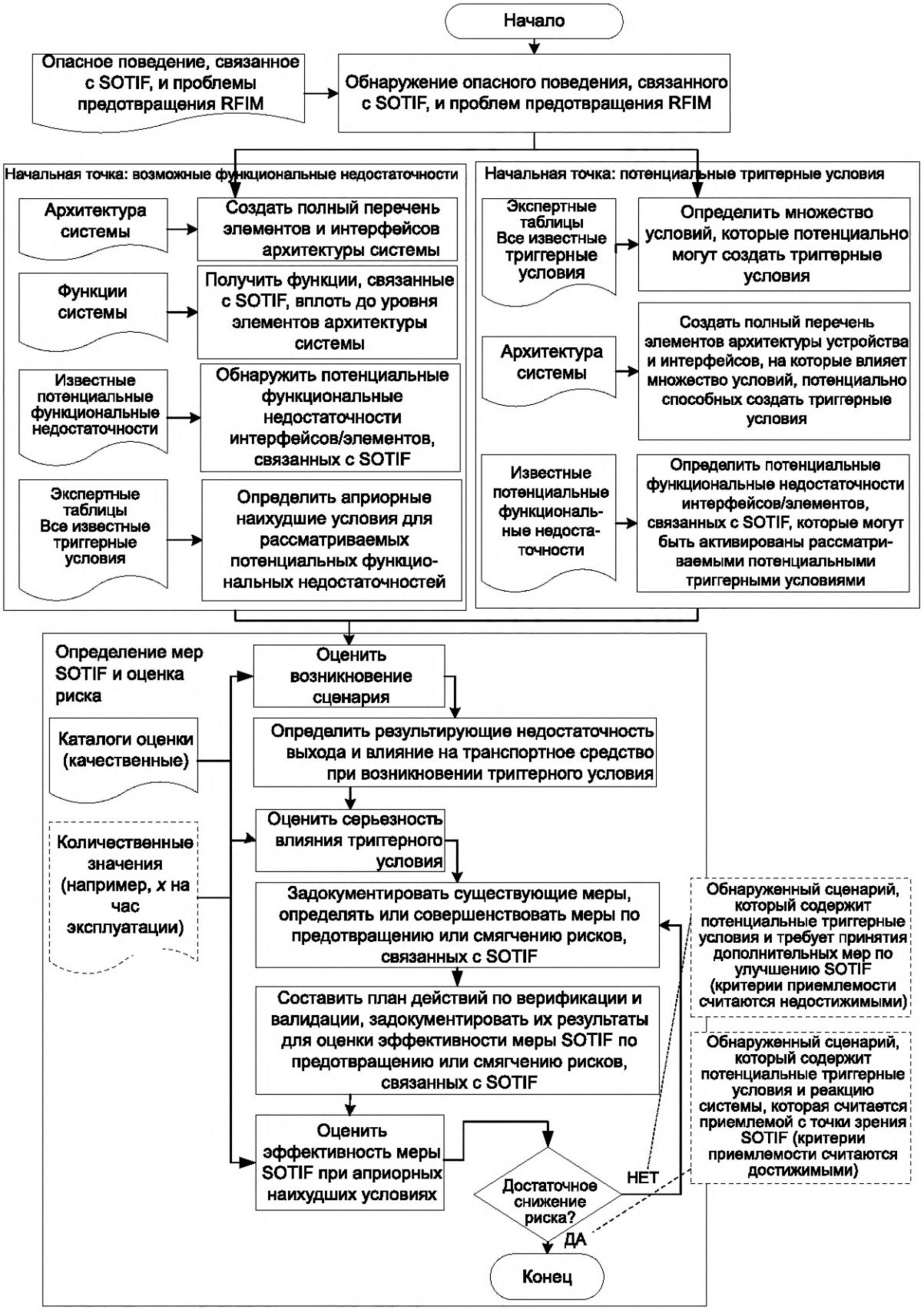


Рисунок В.4 — Рабочий процесс индуктивного анализа SOTIF

Анализ рисков, связанных с SOTIF, может основываться на качественных шкалах оценки вероятности и воздействия или на количественных значениях (например, частоте ложных срабатываний или количестве триггерных условий за час работы). Эти результаты можно использовать для определения приоритета оценки определенных сценариев или элементов над другими.

Примечание 1 — Как указано в 7.4, для поддержки определения приемлемости триггерных условий могут использоваться статистический анализ и диаграммы — например, анализ Парето, матрицы риска с учетом качественных оценок. Однако использование заранее определенных рейтингов для определения приемлемости в этом качественном анализе нецелесообразно из-за изменчивости критериев оценки.

B.3.3.2 Пример анализа SOTIF от возможных функциональных недостаточностей до триггерных условий (системный анализ)

Целью этого индуктивного анализа является выявление возможных функциональных недостаточностей элементов системы и условий сценария, которые могут активировать эти недостаточности и приводить к нарушению выходного сигнала, опасному поведению или проблеме предотвращения обоснованно предсказуемого неявного неправильного использования (RFIM).

Примечание 1 — Термин «проблема предотвращения RFIM» используется в данном пункте для обозначения неспособности системы избежать или смягчить обоснованно предсказуемое неявное неправильное использование.

В следующем примере показан индуктивный анализ различных элементов системы экстренного торможения. Анализ, представленный в таблицах B.6, B.7 и на рисунке B.5, не претендует на полноту, а только иллюстрирует анализ SOTIF различных видов элементов системы, которые включены в модель «Восприятие — План — Действие»:

- аппаратное устройство формирования изображения сенсора камеры (аппаратный блок HW43);
- аппаратный ускоритель камеры или IP (аппаратный блок HW32);
- ПО функции классификации камеры (модуль ПО SW11);
- система активации тормозного момента (система SYS12).

Эти элементы системы участвуют в функции системы «Тормозить при встречном или пересекающемся объекте» (SYS23.1). Экстренное торможение активируется, если обнаруженный объект входит в указанный список объектов (ссылка #RRR) и выполняются определенные аварийные условия (ссылка #CDNXX).

Каждый элемент системы имеет свои возможные функциональные недостаточности, которые в сочетании с априорными наихудшими условиями могут приводить к опасному поведению, проблемам с предотвращением RFIM или недостаточности выхода.

Примечание 2 — Функциональная недостаточность является свойством элемента системы, а априорные наихудшие условия — свойством рассматриваемого сценария.

Для каждого набора (элемент системы, связанная с ним потенциальная функциональная недостаточность и соответствующее потенциальное триггерное условие) выполняется анализ рисков, связанных с SOTIF, с целью определения мер по улучшению SOTIF, верификации их эффективности и оценки остаточного риска с соответствующим обоснованием.

Таблица B.6 анализа SOTIF организована в четыре группы граф, в которых документируются и анализируются:

1) элементы системы, которые могут приводить к недостаточностям выходов (т. е., возможно, все элементы, которые описаны на соответствующем уровне абстракции, вплоть до нижнего уровня архитектуры системы);

2) возможные триггерные условия, которые связаны с элементами системы, перечисленными в 1, и описаны на уровне внешней или внутренней среды;

3) влияние этих триггерных условий при отсутствии каких-либо мер SOTIF, описанное на верхнем уровне абстракции (например, на уровне транспортного средства);

4) существующие и планируемые меры по устранению недостаточностей выходов, перечисленных в 1), описанные на соответствующем уровне абстракции (например, на уровне реализации).

Таблица В.6 — Пример анализа SOTIF от потенциальных функциональных недостаточностей до их триггерных условий

ID	Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальные триггерные условия. Априорные наихудшие условия для выявленных потенциальных функциональных недостаточностей				Влияние потенциальных триггерных условий		Меры по устранению недостаточностей выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Функция архитектуры системы	Распределение по программным/аппаратным элементам системы	Интерфейсы/элементы, связанные с SOTIF	Выявленные возможные функциональные недостаточности в проекте системы	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения	Возникновение	Влияние на уровне транспортного средства, если нарушение выходной мощности не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
ID1.1		Блок HW32: камера с аппаратным ускорителем	Аппаратный ускоритель — результат	Ограничение разрешения изображения, влияющее на оценку расстояния	Дневное время, сухая дорога	Движение прямо со скоростью 90 км/ч	Предшествующий автомобиль слегка выехал на полосу встречного движения целевого автомобиля (> 100 м)	*Выполнено в соответствии с установленным правилом*			Использование датчиков на основе разных технологий: лидар, радар	Протокол испытаний ТС#225 ПРОЙДЕН. Представитель: команда А	*Выполнено в соответствии с установленным правилом*	См. таблицу В.7
ID1.2		Блок HW43: аппаратный датчик камеры	Результат датчика	Плохая визуализация предметов в условиях низкой освещенности	Вечернее время, сухая дорога	Все маневры в условиях низкой освещенности и на сухой дороге	Никаких дополнительных условий	*Выполнено в соответствии с установленным правилом*			Использование датчиков на основе разных технологий: лидар, радар	Протокол испытаний ТС#226, ПРОЙДЕН. Представитель: команда В	*Выполнено в соответствии с установленным правилом*	См. таблицу В.7

Продолжение таблицы В.6

ID	Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальные триггерные условия. Априорные наихудшие условия для выявленных потенциальных функциональных недостаточностей				Влияние потенциальных триггерных условий		Меры по устранению недостаточностей выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Функция архитектуры системы	Распределение по программным/аппаратным элементам системы	Интерфейсы/элементы, связанные с SOTIF	Выявленные возможные функциональные недостаточности в проекте системы	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения	Возникновение	Влияние на уровне транспортного средства, если нарушение выходной мощности не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
ID1.3	Элемент системы, реализующий функцию SYS23.1: тормозить при встречных/пересекающихся объектах (список объектов: артикул #RRR) в аварийных условиях (артикул #CDNXX)	Модуль SW11: классификация объектов	Результат классификации объектов	Низкая производительность во внештатном случае CC#52	Условия CC#52: включают очень большое количество перемещений объектов в обрабатываемой сцене	Час пик, высокая интенсивность движения, оживленный перекресток, группа велосипедистов, группа мотоциклов, пейзаж с множеством флагов. Движущиеся объекты находятся перед автомобилем, но не на его траектории (например, при повороте)	Никаких дополнительных условий	*Выполнено в соответствии с установленным правилом*	Ложное срабатывание: обнаружение встречного объекта, приводящее к непреднамеренному замедлению транспортного средства $<-X$ м/с^2	*Выполнено в соответствии с установленным правилом*	Новая архитектура. Новые алгоритмы. Действие: OPL#227, команда C		*Выполнено в соответствии с установленным правилом*	См. таблицу В.7

Продолжение таблицы В.6

ID	Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальные триггерные условия. Априорные наихудшие условия для выявленных потенциальных функциональных недостаточностей				Влияние потенциальных триггерных условий		Меры по устранению недостаточностей выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Функция архитектуры системы	Распределение по программным/аппаратным элементам системы	Интерфейсы/ элементы, связанные с SOTIF	Выявленные возможные функциональные недостаточности в проекте системы	Характеристики сцены (условия окружающей среды, дорожная/ городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения	Возникновение	Влияние на уровне транспортного средства, если нарушение выходной мощности не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
ID1.4		Система СИС 12: система активации тормозного момента	Тормозной момент	Медленный отклик привода при температуре < –10 °С и низком напряжении < 9,5 В	Зима, снег, T < –15 °С	Низкий заряд аккумулятора. Вмешательство АЕВ из-за медленно приближающегося автомобиля	Никаких дополнительных условий	*Выполнено в соответствии с установленным правилом*	Непреднамеренная потеря замедления <–Z м/с^2. В случае вмешательства АЕВ замедление уменьшается	*Выполнено в соответствии с установленным правилом*	Новый исполнительный механизм. Действие: OPL#228, команда D		*Выполнено в соответствии с установленным правилом*	См. таблицу В.7

Окончание таблицы В.6

ID	Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальные триггерные условия. Априорные наихудшие условия для выявленных потенциальных функциональных недостаточностей				Влияние потенциальных триггерных условий		Меры по устранению недостаточностей выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Функция архитектуры системы	Распределение по программным/аппаратным элементам системы	Интерфейсы/элементы, связанные с SOTIF	Выявленные возможные функциональные недостаточности в проекте системы	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения	Возникновение	Влияние на уровне транспортного средства, если нарушение выходной мощности не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
ID1.5		Модуль SW11: классификация объектов	Результат классификации объектов	Неправильная классификация неожиданных/неизвестных системе объектов	Редкие объекты, необычные объекты	Вождение автомобиля во время определенных мероприятий (например, футбольного матча, парада), праздников (например, Рождества, карнавала), когда украшен автомобиль, при погрузке автомобиля	Водитель установил на багажнике на крыше выступающий объект, который попадает в кадр камеры (например, лестницу или спортивное снаряжение со свисающим текстильным материалом или веревкой)	*Выполнено в соответствии с установленным правилом*	Ложное срабатывание: обнаружение встречного объекта, приводящее к непреднамеренному замедлению транспортного средства $<-X$ м/с^2	*Выполнено в соответствии с установленным правилом*	Проверить наличие необычных объектов, обнаруженных камерой в начале цикла вождения. Непрерывная проверка достоверности обнаруженных объектов. Запись в инструкцию по эксплуатации автомобиля, предписывающая водителю не допускать попадания чего-либо в поле зрения камеры	Моделирование или валидационное испытание	*Выполнено в соответствии с установленным правилом*	См. таблицу В.7

Таблица B.7 — Пример анализа SOTIF от возможных функциональных недостаточностей до их триггерных условий (продолжение)

ID	Обоснование приемлемости
ID1.1	Направленные испытания *на многочисленных и разнообразных узких дорогах* и испытания на долговечность (<Дорога> отмечена тегом «Узкая», <Скорость>—>90 км/ч, <Время суток> — светлое время суток во всем наборе данных о вождении) показывают, что: - подтверждена достаточно низкая вероятность возникновения ситуаций, в которых ограничение разрешения изображения камеры с аппаратным ускорителем HW32 влияет на оценку расстояния таким образом, что может приводить к непреднамеренному замедлению транспортного средства из-за ложного обнаружения объекта при отсутствии мер SOTIF (при отключении радара и лидара): 0 событий привели к непреднамеренному замедлению транспортного средства; 0 инцидентов привели к обнаружению возможных объектов; - совместное использование радара и лидара признано эффективной мерой, если она активирована: повторные испытания в тех же условиях, когда ограничение разрешения изображения влияет на ограничение расстояния, показывают лучшее время реакции (–*x* %) и более высокую оценку достоверности для подтверждения отсутствия объектов, когда в объединенном алгоритме доступна информация радара и лидара. Доказательства: TC#225 пройден. Тему можно закрыть
ID1.2	Направленные испытания и испытания на долговечность в вечернее/ночное время (<Время суток > — «Ночь» или «Сумерки» во всем наборе данных о вождении) демонстрируют, что: - подтверждена достаточно низкая вероятность возникновения ситуаций, когда визуализация изображения в результате ограничений датчика камеры HW43 в условиях низкой освещенности влияет на изображение таким образом, что это может приводить к непреднамеренному замедлению транспортного средства из-за ложного срабатывания обнаружения объекта при отсутствии мер SOTIF (при отключении радара и лидара): 0 событий привели к непреднамеренному замедлению транспортного средства; 6 инцидентов привели к обнаружению «возможных объектов», однако они не были подтверждены алгоритмом принятия решения из-за неправдоподобных условий; - совместное использование радара и лидара признано эффективной мерой, если она активирована: повторные испытания в тех же условиях показывают лучшее время реакции (–*x* %) и достоверность подтверждения отсутствия объектов, когда в объединенном алгоритме доступна информация радара и лидара. Тему можно закрыть
ID1.3	Внештатный случай CC#52 представляет собой набор особых условий, которые не возникали во время испытаний на долговечность и длящихся на текущий момент эксплуатационных испытаний. Тем не менее, поскольку внештатный случай CC#52 нельзя отнести к категории «маловероятной», он был воспроизведен в среде имитатора дорожного движения. Альтернативные алгоритмы команды C демонстрируют небольшое увеличение производительности (более высокую оценку достоверности), хотя и незначительное в этой имитационной среде. Вопрос о том, требуется ли новая архитектура или новые алгоритмы, еще не решен.
ID1.4	В ходе недавних испытаний, проведенных командой D, была выявлена недостаточность спецификации действующего исполнительного механизма тормозного момента (вариант A). При низком значении напряжения (при этом в пределах указанного диапазона) и низких температурах окружающей среды (от –30 °C до –15 °C) в Северной Швеции подтверждается непреднамеренная потеря замедления <–*Z* м/с^2. В этих же испытаниях продемонстрирована эффективность прототипа надежного тормозного привода (вариант B) для достижения целей валидации. Спецификация требований обновлена. По-прежнему открыт вопрос повторения тех же тестов с выпущенной версией варианта B
ID1.5	Рассмотрение результатов моделирования ожидается

Рисунок В.5 — Дерево причинно-следственных связей SOTIF, начиная с потенциальной функциональной недостаточности, иллюстрирующее таблицы В.6 и В.7

В.3.3.3 Пример анализа SOTIF от триггерного условия до возможных функциональных недостаточностей (анализ на основе сценариев)

Этот индуктивный анализ SOTIF направлен на выявление условий сценариев вождения, которые могут приводить к нарушению выходов, опасному поведению или проблемам с предотвращением RFIM, и функций или элемента архитектуры системы, на которые воздействуют эти триггерные условия.

В следующем примере представлен индуктивный анализ элементов системы экстренного торможения, в сценарии с которой состояние «Пешеходы нарисованы на дороге» может приводить к опасному поведению. Анализ, представленный в таблицах В.8, В.9 и на рисунке В.6, не претендует на полноту, а лишь иллюстрирует анализ SOTIF различных видов системных элементов, включенных в модель «Восприятие — План — Действие», а именно:

- аппаратный радиолокационный элемент (аппаратный блок HW53);
- аппаратный ускоритель камеры или IP (аппаратный блок HW52);
- ПО функции классификации камеры (модуль ПО SW11);
- система активации тормозного момента (система SYS12).

Эти элементы участвуют в функции системы «Тормозить при встречном или пересекающемся объекте» (SYS23.1). Экстренное торможение запускается, если обнаруженный объект входит в указанный список объектов (ссылка #RRR) и выполняются определенные аварийные условия (ссылка #CDNXX).

Цель анализа — выявлять функциональные недостаточности элементов системы, на которые может влиять одно триггерное условие. Например, в приведенном ниже примере алгоритм камеры с аппаратным ускорителем (аппаратный блок HW52) может вызывать ложное срабатывание при обнаружении объекта «Пешеходы нарисованы на дороге», несмотря на то что это происходит только в конкретных внештатных случаях (СС № 536).

Примечание — Функциональная недостаточность является свойством элемента системы, тогда как возможные триггерные условия являются свойством рассматриваемого сценария.

Для каждого набора (потенциальное триггерное условие, связанная с ним потенциальная функциональная недостаточность элемента системы) выполняется анализ рисков, связанных с SOTIF, с целью выявления мер по улучшению SOTIF и оценки остаточного риска с надлежащим обоснованием.

Таблица В.8 — Пример анализа SOTIF от триггерных условий до возможных функциональных недостаточностей

ID	Потенциальные триггерные условия				Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальное влияние триггерных условий		Меры по устранению недостаточности выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Выявленный опасный вариант использования из экспертной таблицы			Возникновение	Функция архитектуры системы, на которую влияют триггерные условия	Элементы архитектуры системы, на которые влияют триггерные условия	Интерфейсы/элементы, связанные с SOTIF	Возможные функциональные недостаточности в проекте системы	Влияние на уровне транспортного средства, если нарушение выхода не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения											
ID1.1	Инфраструктура дорожного движения «Пешеходы нарисованы на дороге». Погода: отличная. Страна: ВСЕ. Время суток: вечер, слабая освещенность. Дорога: сухая. Температура: 25 °C	Движение по прямой со скоростью 50 км/ч (городская местность)	Следующее транспортное средство находится рядом с целевым автомобилем (< 5 м)	Выполнено в соответствии с установленным правилом	Элемент системы, реализующий функцию SYS23.1: торможение при встречных/пересекающихся объектах	Блок HW52 IP-камера	Результат IP		Ложное срабатывание: обнаружение пешехода приводит к непреднамеренному замедлению автомобиля <–*X* м/с^2, что приводит к столкновению сзади со следующим транспортным средством	Выполнено в соответствии с установленным правилом	Использование датчиков на основе разных технологий: лидар, радар	ТС#234 ПРОЙДЕН. Представитель: команда А	Выполнено в соответствии с установленным правилом	См. таблицу В.9
ID1.2						Аппаратный блок HW63: радарный элемент	Результат радара	Не для этого сценария			Никакие		Не эффективно	См. таблицу В.9

Продолжение таблицы В.8

ID	Потенциальные триггерные условия				Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальное влияние триггерных условий		Меры по устранению недостаточности выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Выявленный опасный вариант использования из экспертной таблицы			Возникновение	Функция архитектуры системы, на которую влияют триггерные условия	Элементы архитектуры системы, на которые влияют триггерные условия	Интерфейсы/элементы, связанные с SOTIF	Возможные функциональные недостаточности в проекте системы	Влияние на уровне транспортного средства, если нарушение выхода не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения											
ID1.3						Программный модуль SW11: классификация объектов	Результат классификации объектов	Не для этого сценария (сравнение/голосование входных данных с архитектурой 1oo2 обеспечивает отсутствие недостаточностей)			Голосование на основе полностью резервированных и использующих разнообразие алгоритмов (HW52, HW63, SW11)	Протокол испытаний VC2 ПРОЙДЕН	Выполнено в соответствии с установленным правилом	См. таблицу Б.9

Окончание таблицы В.8

ID	Потенциальные триггерные условия				Элементы системы, которые могут приводить к опасным событиям, связанным с SOTIF				Потенциальное влияние триггерных условий		Меры по устранению недостаточности выхода (включая ранее существовавшие, а также вновь предложенные)			Обоснование приемлемости
	Выявленный опасный вариант использования из экспертной таблицы			Возникновение	Функция архитектуры системы, на которую влияют триггерные условия	Элементы архитектуры системы, на которые влияют триггерные условия	Интерфейсы/элементы, связанные с SOTIF	Возможные функциональные недостаточности в проекте системы	Влияние на уровне транспортного средства, если нарушение выхода не устраняется никакими мерами	Серьезность опасного события	Меры в проекте для улучшения SOTIF	Меры верификации для обеспечения доказательств реакции системы или эффективности проектных мер	Эффективность меры	
	Характеристики сцены (условия окружающей среды, дорожная/городская инфраструктура)	Сценарий вождения (действия, события, цели и ценности)	Поведение водителя, других водителей, участников дорожного движения											
ID1.4						Система СИС 12: система активации тормозного момента	Тормозной момент	Не для этого сценария			Никакие		Не эффективно	См. таблицу Б.9

Таблица B.8 анализа SOTIF состоит из четырех макрограф, в которых задокументированы и проанализированы:

1) потенциальные триггерные условия — например, выявленные или случайные потенциальные триггерные условия, которые описаны на уровне внешней или внутренней среды;

2) элементы системы, которые могут приводить к нарушению выходного сигнала, если на них воздействуют потенциальные триггерные условия, перечисленные в 1) и описанные на соответствующем уровне абстракции вплоть до самого нижнего уровня архитектуры системы;

3) влияние этих потенциальных триггерных условий при отсутствии каких-либо мер SOTIF, описанное на верхнем уровне абстракции (например, на уровне транспортного средства);

4) существующие и планируемые меры по устранению нарушений выходов, перечисленные в 2), описанные на соответствующем уровне абстракции (например, на уровне реализации).

Таблица B.9 — Пример анализа SOTIF от триггерного условия до потенциальных функциональных недостаточностей (продолжение)

ID	Обоснование приемлемости
IDA.1	Направленные эксплуатационные испытания по Дельта-авеню в Бернаби, Британская Колумбия, Канада, между Брентвуд-парком и начальной школой Святого Креста: - подтверждена достаточно низкая вероятность возникновения ситуаций, когда камера с аппаратным ускорителем HW52 распознает объекты-призраки, приводящие к непреднамеренному торможению автомобиля, при отсутствии мер SOTIF (при отключении радара, лидара и механизмов на основе оптического потока): 0 событий привели к непреднамеренному торможению автомобиля; 1 случай привел к обнаружению «возможных объектов», однако не подтвержден алгоритмом принятия решения из-за недостаточного времени подтверждения. Действительно, даже при низкой скорости движения изображение не искажается лишь в течение очень короткого периода времени, которого недостаточно для обнаружения пешехода на дороге; - совместное использование радара и лидара признано эффективной мерой, если она активирована: - повторные испытания в тех же условиях показывают более высокую достоверность подтверждения отсутствия объектов, когда в объединенном алгоритме доступна информация радара и лидара. Доказательства: TC#234 пройден
IDA.2	Не эффективно. Радиолокационный элемент не подвержен неправильной трактовке дорожной разметки
IDA.3	Для этого сценария в программном блоке SW11 не выявлено никаких недостатков в проекте системы. Тем не менее, алгоритм принятия решения, основанный на нескольких различных алгоритмах, способных подтверждать присутствие объекта, считается очень эффективной мерой, которая позволяет устранять функциональные недостатки блока SW11 при их наличии
IDA.4	Не эффективно. Привод тормозного момента не связан с неправильной трактовкой дорожной разметки

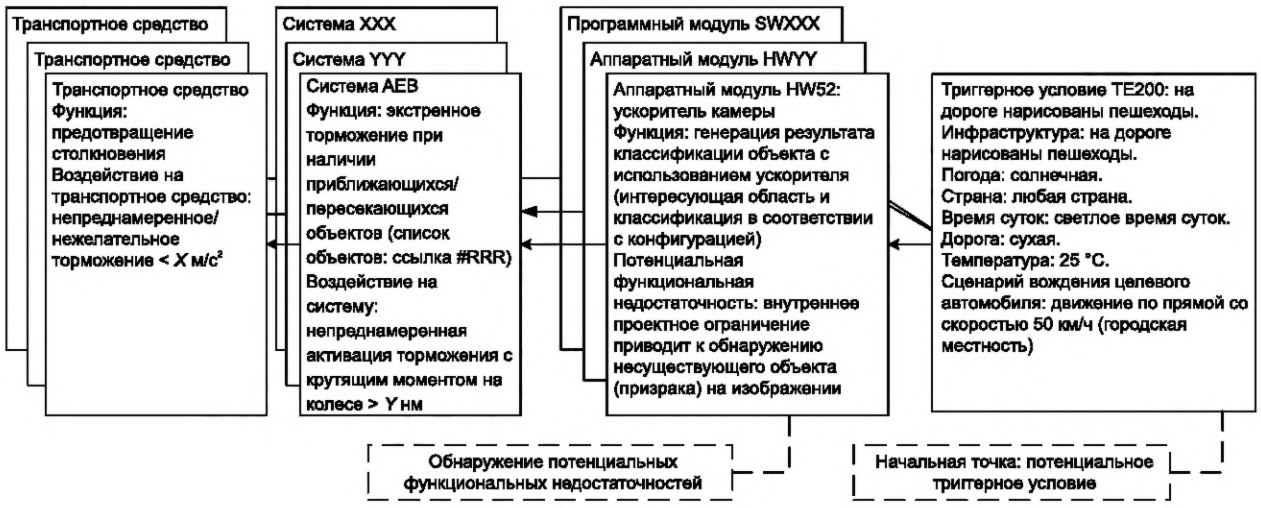


Рисунок B.6 — Дерево причинно-следственных связей SOTIF, начиная с потенциального триггерного условия, иллюстрирующее таблицы B.8 и B.9

B.4 Применение STPA в контексте SOTIF для ADAS и автоматизированных транспортных средств

B.4.1 Введение

STPA (системно-теоретический анализ процессов) (см. [19] и [20]) — это подход к анализу безопасности, который предназначен для оценки безопасности сложных систем, определения ограничений и требований к безопасности. Опубликовано множество статей, в которых описывается применение STPA к автомобильным системам, ADAS и автоматизации (см. [21], [22], [23] и [24]). STPA полезен для SOTIF, поскольку может устранять функциональные недостаточности, решать проблемы использования системы в неподходящей среде, неправильного использования людьми и т. д.

В настоящем подразделе представлен упрощенный пример системы шоссейного пилотного проекта SAE J3016 уровня 3, демонстрирующий использование STPA для анализа SOTIF в соответствии с требованиями разделов 6 (идентификация опасностей) и 7 (идентификация и оценка триггерных условий). Шоссейный пилотный проект полностью управляет динамикой транспортного средства в ограниченной среде без непосредственного контроля со стороны водителя. Водитель-человек присутствует и может возвращать себе управление в течение определенного периода времени — как правило, от нескольких секунд до некоторого максимального предела.

B.4.2 STPA. Шаг 1. Определение цели и области анализа

На первом этапе STPA определяется ущерб участников, который необходимо предотвратить. После ущерба STPA определяет опасности на уровне транспортного средства — состояния или условия, которые вместе с определенным набором наихудших условий внешней среды приводят к ущербу. В таблице B.10 приведен пример потерь и опасностей на уровне транспортного средства, выявленных в результате STPA, для системы шоссейного пилотного проекта.

Таблица B.10 — Пример идентификации ущерба и опасностей

Ситуация/сценарий (выдержка из HARA)	Ущерб	Возможные последствия (вред)	Опасности на уровне транспортного средства (из HARA)
Движение по шоссе ночью с плохой видимостью на высокой скорости. Приближение сзади к более медленному мотоциклисту	[L1] Гибель людей или причинение им вреда	Тяжелые или смертельные травмы	[VH1] Целевое транспортное средство нарушает порог/требование минимального расстояния от/с другими транспортными средствами
....	[L2] ...	...	[VH1] ...

Примечание — Остальная часть B.4 содержит примеры спецификаций. В этом контексте используются слова «должен». В B.4 слова «должен» используются лишь в примерах требований и не предназначены для соответствия настоящему стандарту.

На последующих этапах с помощью STPA систематически анализируются управляющие действия каждого системного контроллера, в том числе людей, для выявления конкретного поведения и причин, которые могут приводить к опасностям на уровне транспортного средства в конкретном сценарии. Набор требований SOTIF на уровне транспортного средства определяется как часть HARA (см. таблицу B.11) с учетом опасностей на уровне транспортного средства.

Таблица B.11 — Опасности и соответствующие ограничения безопасности на уровне транспортного средства

Опасность	Требование SOTIF на уровне транспортного средства (ограничение безопасности на уровне транспортного средства)
[VH1] Каждое транспортное средство нарушает порог/требование минимального расстояния от/с другими транспортными средствами	[SC-1] Каждое транспортное средство должно выдерживать безопасную дистанцию относительно других транспортных средств
...	

B.4.3 STPA. Шаг 2. Моделирование структуры управления

Системная и функциональная спецификация анализируются для определения иерархии управления системой и ее интерфейсного окружения. Это называется структурой управления. Для анализа фиксируются команды контроллера, которые называются управляющими действиями, а также обратная связь от управляемого процесса и внешней среды.

На рисунке B.7 представлен пример структуры управления для функции Highway pilot.

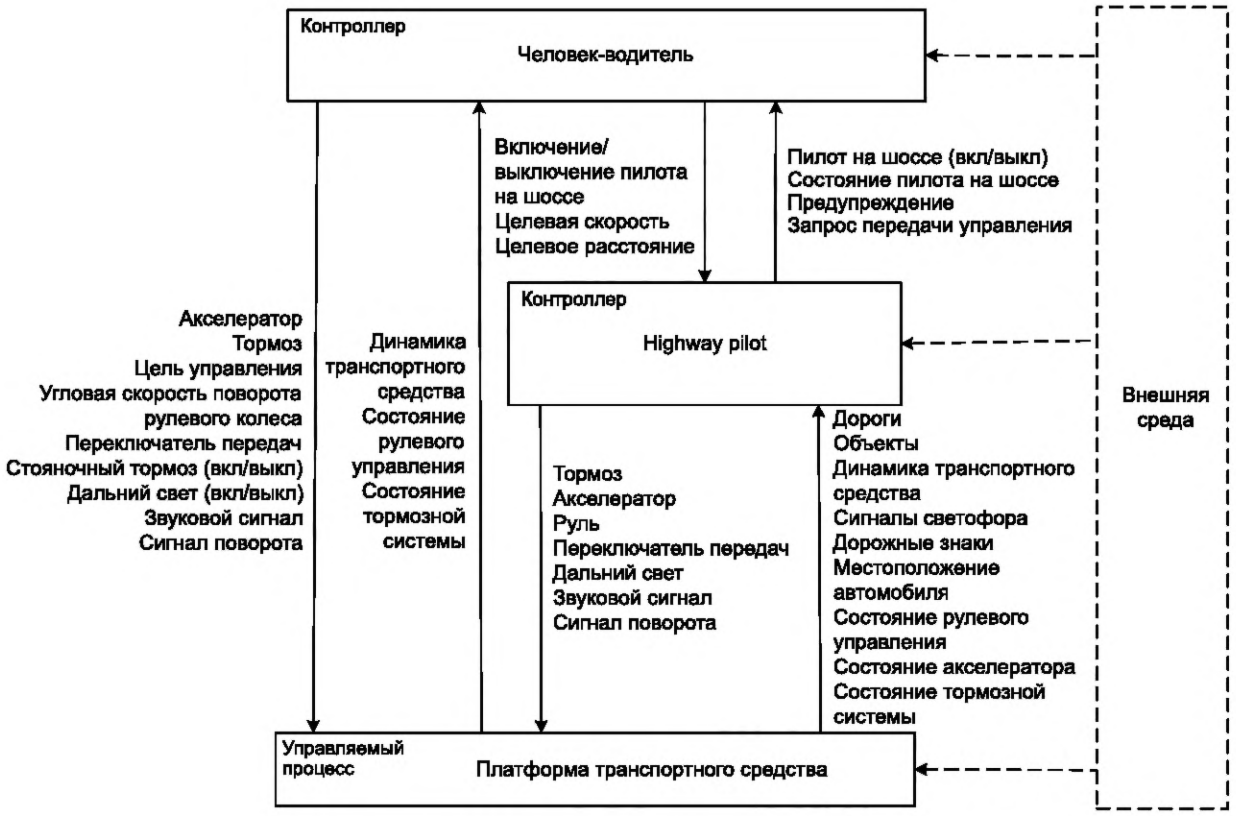


Рисунок В.7 — Высокоуровневая структура управления для функции Highway pilot

Из-за ограниченного объема STPA не рассматривается подробнее в В.4, однако более подробный пример модели контура управления для этого типа функций показан на рисунке 5 в [25].

В.4.4 STPA. Шаг 3. Идентификация опасных управляющих действий

На следующем шаге процедуры STPA определяются опасные управляющие действия (UCA) — действия, которые в определенном контексте и в наихудшем случае приводят к возникновению опасности на уровне транспортного средства. UCA, связанные с ними опасности, и HARA используются для идентификации опасностей и оценки рисков (см. раздел 6). Опасное управляющее действие состоит из пяти элементов, которые показаны на рисунке В.8.

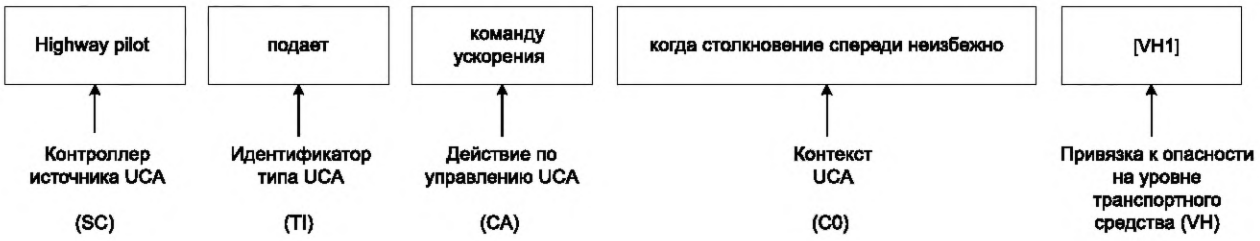


Рисунок В.8 — Пять элементов опасного управляющего действия

Несколько примеров опасных управляющих действий для команды торможения для функции Highway pilot показано в таблице В.12.

Таблица В.12 — Примеры опасных управляющих действий для команды управления торможением контроллера Highway pilot

Управляющее действие	Не формируется	Формируется	Формируется слишком рано, слишком поздно или в неправильном порядке	Формируется слишком долго или прекращается слишком рано
Команда торможения	UCA-1: Highway pilot не подает команду торможения, когда столкновение впереди неизбежно. [VH1]	UCA-2: Highway pilot подает команду торможения при недостаточной степени торможения, когда столкновение впереди неизбежно. [VH1]. UCA-3: Highway pilot подает команду торможения, когда водитель нажимает на акселератор. [VH2]	UCA-4: Highway pilot подает команду торможения слишком поздно, когда столкновение впереди становится неизбежным. [VH1]	UCA-5: Highway pilot перестает подавать команду торможения слишком рано после столкновения (т. е. прекращает подавать команду торможения до того, как водитель возобновляет ручное управление). [VH1]

Каждое опасное управляющее действие может приводить как минимум к одной опасности на уровне транспортного средства (в противном случае оно не было бы опасным), но также может приводить к нескольким опасностям на уровне транспортного средства.

Можно определять ограничения безопасности контроллера, чтобы гарантировать предотвращение определенных UCA. Ограничение безопасности контроллера определяет операторы контроля или инварианты поведения контроллера, которые должны соблюдаться для предотвращения UCA.

Ограничения безопасности контроллера для некоторых UCA, связанных с торможением, показаны в таблице В.13.

Таблица В.13 — Преобразование UCA в требования (ограничения безопасности)

Опасное управляющее действие	Ограничение безопасности
UCA-1: Highway pilot не подает команду торможения, когда столкновение впереди неизбежно. [VH-1]	SC-1: Функция Highway pilot должна подать команду торможения, когда лобовое столкновение неизбежно. [UCA-1]
UCA-2: Highway pilot подает команду торможения с недостаточной степенью торможения, когда столкновение впереди неизбежно. [VH-1]	SC-2: Функция Highway pilot должна подать команду торможения с достаточной степенью торможения, превышающей минимальную величину, необходимую для предотвращения лобового столкновения. [UCA-2]
UCA-3: Highway pilot подает команду торможения, когда водитель нажимает на акселератор. [VH2]	SC-3: Функция Highway pilot не должна подавать команду торможения, когда водитель нажимает на акселератор. [UCA-3]
UCA-4: Highway pilot подает команду торможения слишком поздно после того, как лобовое столкновение стало неизбежным. [VH-1]	SC-4: Функция Highway pilot должна подать команду торможения по крайней мере (подлежит уточнению) за несколько секунд до того, как столкновение впереди станет неизбежным. [UCA-4]
UCA-5: Highway pilot перестает подавать команду торможения слишком рано после того, как произошло столкновение, и водитель не возобновил ручное управление. [VH1]	SC-5: Функция Highway pilot должна подавать команду торможения до тех пор, пока водитель не возобновит ручное управление. [UCA-5]

В.4.5 STPA. Шаг 4. Выявление причин сценариев

Последний основной этап STPA определяет причины сценариев, которые приводят к опасностям, и соответствующие причинные факторы (т. е. триггерные условия, см. 7.3). В таблице В.14 представлены причины сценариев для пилота UCA-1 на шоссе с целью выявления причинных факторов.

В качестве первого шага этого анализа выявляются сочетания одного или нескольких нарушений выходов других элементов или элементов самого системного контроллера, которые могут приводить к рассматриваемым UCA. Это сочетание одного или нескольких нарушений выходного сигнала в таблице В.14 называется состоянием нарушения. На следующем этапе выявляются причинные факторы, приводящие к выявленным состояниям нарушения. Это могут быть недостаточности выходов, функциональные недостаточности и триггерные условия.

Таблица В.14 — Идентификация причинных факторов

Причина сценария	UCA (опасное поведение)	Состояние нарушения	Причинные факторы (триггерное условие, функциональные недостаточности, недостаточности выходов)
CS-1	UCA-1: Highway pilot не подает команду торможения, когда столкновение впереди неизбежно	IC-1: Highway pilot ошибочно полагает, что столкновение не произойдет из-за некорректной оценки ситуации: относительного положения, скорости, ускорения, направленности на препятствие	CF-1: Датчики установлены неправильно, фокус или положение датчика нарушены, датчик заблокирован и т. д. CF-2: Обратная связь задерживается и не получена вовремя из-за занятости шины, недостаточного приоритета сообщения или нерациональной организации доступа к общей шине, электромагнитных помех и т. д. CF-3: Обратная связь считается некорректной (игнорируется функцией Highway pilot), поскольку противоречит другой обратной связи (которая, например, указывает, что скорость колеса равна нулю)
CS-2	UCA-1: Highway pilot не подает команду торможения, когда столкновение впереди неизбежно	IC-2: Highway pilot ошибочно полагает, что столкновение не произойдет из-за не соответствующей оценки ситуации: торможение включено	CF-4: Highway pilot получает неправильный сигнал о том, что функции торможения или рулевого управления уже применены в достаточной степени
CS-3	UCA-1: Highway pilot не подает команду торможения, когда столкновение впереди неизбежно	IC-3: Highway pilot ошибочно полагает, что столкновение не является неизбежным из-за неадекватной оценки ситуации: размера или типа препятствия	CF-5: Highway pilot получает неправильный сигнал, указывающий, что тип препятствия не представляет опасности при столкновении. CF-6: Highway pilot получает неправильный сигнал об отсутствии препятствий для столкновения [например, из-за забрызганного датчика, датчика, установленного в неправильном положении/ориентации, отключенного датчика, препятствия за пределами поля зрения датчика, неблагоприятных погодных условий, определенных некорректно (отсутствует функциональность алгоритма), не откалиброван и т. д.]
CS-4…	UCA-2: Highway pilot…	IC-4: Highway pilot …	CF-7: Highway pilot …

Примечание — В этом примере рассмотрены проблемы, связанные с STPA SOTIF и функциональной безопасностью.

В.4.6 Определение средств контроля и смягчения последствий, улучшение проекта системы и определение требований

После завершения основных действий STPA в контексте настоящего стандарта можно делегировать оставшиеся действия STPA соответствующим этапам процесса для функциональных модификаций, которые направлены на устранение рисков, связанных с SOTIF (см. раздел 8), или причин, связанных с отказами (см. ИСО 26262-4:2018, раздел 6). К этим действиям относятся формулирования реализуемых требований, которые подходят для выполнения ограничений безопасности из STPA.

Приложение С
(справочное)

Руководство по верификации и валидации SOTIF

С.1 Цель стратегии верификации и валидации

Функциональные недостаточности системы являются источником проблем SOTIF. Стратегия верификации и валидации разрабатывается так, чтобы показать, что остаточный риск в выявленных и невыявленных сценариях является достаточно низким и соответствует количественному целевому показателю, который определен в 6.5. В эту стратегию включаются концепции получения и тестирования целей валидации.

После определения цели валидации можно разрабатывать план валидационных испытаний в соответствии с разделами 9 и 11, чтобы продемонстрировать отсутствие неоправданного риска из-за выявленных и невыявленных опасных сценариев (области 2 и 3). Валидация, как правило, сочетает в себе физические испытания (полигон, реальные условия) и испытания методом моделирования. В рамках стратегии валидации, которая определена в разделе 9, количественная цель часто распределяется между физическими испытаниями и испытаниями посредством моделирования.

Валидация может включать в себя испытания транспортного средства в широком диапазоне эксплуатационных условий — например, сочетании SIL, HIL и реальных условий эксплуатации. Валидация может включать в себя некоторое структурированное тестирование (например, тесты, разработанные и реализованные на испытательном полигоне), специальный анализ и моделирование, однако ключевым аспектом, особенно для области 3, является выполнение достаточно тщательного тестирования в достаточно широком диапазоне эксплуатационных условий, чтобы выявить максимальное количество невыявленных потенциально опасных сценариев в соответствии с требованиями стратегии валидации.

Тестовые сценарии, относящиеся к области 3, могут включать в себя:

1) случайные сочетания выявленных параметров выявленных вариантов использования (например, сочетание неблагоприятных погодных условий с конкретными условиями дорожного движения);

2) случайные сочетания выявленных сценариев;

3) неустановленные конкретные сценарии, которые могут вызывать опасное поведение системы при испытаниях на дороге общего пользования.

Моделирование позволяет быстро изучать широкий спектр соответствующих сценариев, однако оно может ограничиваться базовыми допущениями о внешней среде, датчиках и модели транспортного средства. Точность соответствия модели реальному миру указывается в обосновании безопасности. Более того, моделирование может основываться только на определенных параметрах [С.1, перечисление 1)] или сценариях [С.1, перечисление 2)].

Тестирование системы в реальных условиях позволяет использовать реалистичные входные данные, но при ограниченном количестве километров, часов и сценариев, а также в условиях случайных реальных сцен, которые возникают во время тестирования [С.1, перечисление 3)]. С помощью испытаний в реальных условиях можно обнаруживать невыявленные ранее параметры.

Для адаптации стратегии валидации можно использовать существующие знания о подобных функциях и соответствующих потенциально опасных сценариях — например, полученные из опыта применения подобных систем. С помощью таких стратегий валидации можно сокращать объем необходимого тестирования с сохранением целей валидации.

Настоящее приложение имеет следующую структуру:

- в С.2 рассматривается соответствие критериям приемлемости с использованием интенсивности опасного поведения и приводится пример определения и оценки критериев приемлемости и целей валидации;
- в С.3 иллюстрируется, как можно использовать статистические данные и резерв безопасности;
- в С.4 приводится пример использования различных типов испытаний при верификации и валидации датчиков;
- в С.5 рассматривается использование ограниченного испытания методом случайной выборки и выборки по значимости для уменьшения объема испытаний посредством имитационного моделирования;
- в С.6 рассматривается использование физической архитектуры системы для обоснования сокращения объема тестирования.

С.2 Вывод целей валидации

С.2.1 Достижение критериев приемлемости с использованием частоты опасного поведения

Значения критериев приемлемости, как правило, очень малы (например, 10^{-8}/ч); для их валидации часто необходимы значительные усилия. По этой причине важно найти метод, который позволяет снизить валидацию цели и при этом продемонстрировать соблюдение критерия приемлемости. Одним из таких методов является рассмотрение частоты соответствующего опасного поведения $R_{НВ}$.

Целью настоящего подраздела является не определение критерия приемлемости, а получение приемлемой частоты опасного поведения на основе критериев приемлемости, которую, в свою очередь, можно использовать для определения цели валидации.

В разделе 6 определяются и оцениваются возможные опасные события, вызванные опасным поведением заданной функциональности, и их последствия. Как указано в разделе 6, с каждым выявленным опасным поведением связан критерий его приемлемости, из которого выводится цель валидации для каждого опасного поведения.

Примечание 1 — В настоящем подразделе не рассматривается метод получения или обоснование критерия приемлемости. Предполагается, что критерием приемлемости является частота опасного поведения, которая определяется надежным общепринятым методом.

Значение R_{HB}, которое соответствует определенному критерию приемлемости, можно получать в результате следующих шагов:

- выявление происшествий/инцидентов, повлекших за собой вред *H* вследствие проанализированного опасного поведения (например, столкновение сзади из-за нежелательного торможения);
- определение критерия приемлемости для этих аварий/инцидентов A_H (его значение получено из исходных критериев приемлемости в сочетании с резервом безопасности);
- обнаружение потенциально опасных сценариев, в которых выявленные дорожно-транспортные происшествия могут происходить вследствие рассматриваемого опасного поведения (например, вождение транспортного средства на высокой скорости при наличии автомобиля, следующего за ним на близком расстоянии). Условная вероятность возникновения таких обстоятельств в предположении, что рассматриваемое опасное поведение реализуется в этом сценарии, равна $P_{E|HB}$.

Примечание 2 — Потенциально опасные сценарии включают в себя триггерные условия опасного поведения;

- определение вероятности того, что опасное поведение не контролируется в этих сценариях $P_{C|E}$, в предположении, что оно произошло в них;
- определение распределения серьезности выявленных аварий/инцидентов A_H в предположении, что действие по обеспечению управляемости не было успешным. Это распределение описывает вероятность $P_{S|C}$ определенной степени серьезности этих аварий.

Примечание 3 — В зависимости от используемых критериев приемлемости $P_{S|C}$ может использоваться для определенной степени серьезности (например, X % участников получили тяжелые травмы), а также вероятности того, что серьезность находится не ниже определенного уровня (например, Y % участников получили, как минимум, легкие травмы).

Примечание 4 — Полученные параметры $P_{E|HB}$, $P_{C|E}$ и $P_{S|C}$ можно проверять на соответствие параметрам E, C и S HARA функциональной безопасности согласно стандартам серии ИСО 26262 для аналогичного опасного события. Положения ИСО 26262-3 о частоте и продолжительности воздействия также могут применяться к опасному поведению SOTIF.

Предполагая, что опасное поведение не всегда приводит к причинению вреда, критерий приемлемости A_H можно вычислить по формуле

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}. \quad (C.1)$$

Частоту опасного поведения R_{HB} можно рассматривать как вероятность возникновения этого опасного поведения в течение заданного периода времени. R_{HB} непосредственно зависит от частоты его триггерного условия, которое могут активировать функциональные недостаточности, ведущие к опасному поведению. Следовательно, ее можно использовать для получения применимой цели валидации по формуле

$$R_{HB} = A_H / (P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}). \quad (C.2)$$

Примечание 5 — Если триггерные условия не зависят от воздействия обстоятельств, при которых опасное поведение приводит к причинению вреда, эти условные вероятности можно считать равными простому произведению вероятностей.

Пример — При определении и оценке риска был выявлен вред H, связанный с критерием приемлемости $A_H = 10^{-8}$/ ч. Из эксплуатационных данных известно, что опасное поведение, которое приводит к такому вреду, не поддается контролю в $P_{C|E} = 10$ % случаев. Серьезность, к которой относится критерий приемлемости, достигается в $P_{S|C} = 1$ % случаев. Вероятность того, что пользователь окажется в сценарии, в котором возникновение опасного поведения может привести к причинению (выявленного) вреда, оценивается как $P_{E|HB} = 5$ % времени вождения. С учетом этих значений интенсивность

опасного поведения, которая будет использоваться для расчета целевого показателя валидации, соответствует формуле

$$R_{HB} = A_H / (P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}) = 10^{-8}/\text{ч} /(0{,}05 \cdot 0{,}1 \cdot 0{,}01) = 2 \cdot 10^{-4}/\text{ч}. \quad \text{(С.3)}$$

Использование $R_{HB} = 2 \cdot 10^{-4}$/ч в качестве нового исходного значения для определения цели валидации позволяет уменьшить трудоемкость валидации. Используя формулу (С.7) и связанные с ней допущения, можно показать, что критерий приемлемости выполнен с достоверностью 63 %, если за 5000 ч испытаний не обнаружено ни одного случая опасного поведения.

С.2.2 Пример определения и валидации приемлемой интенсивности ложноположительных срабатываний в системах AEB

С.2.2.1 Цель

В настоящем подразделе приведен пример расчета минимального расстояния (в километрах), рекомендованного SOTIF, которое необходимо проехать для выполнения валидации, на основе опубликованной статистики дорожно-транспортных происшествий. В качестве метода валидации было выбрано испытание транспортного средства с длительным пробегом/эксплуатационные испытания. Целевой пробег рассчитывался с применением статистических методов и четырехэтапного анализа. Последовательность этапов приведена ниже; для каждого из них сформулирована следующая частная цель.

1 Возможные причины опасных событий (см. С.2.2.2):

- выявить опасные для целевой системы события, вызванные функциональными недостаточностями;
- уточнить выявленные параметры сценариев реализации опасных событий и соответствующее сочетание этих параметров.

2 Моделирование опасных событий (см. С.2.2.3):

- рассмотреть репрезентативные параметры, которые могут активировать функциональные недостаточности системы;
- смоделировать сценарии опасных событий (аварий).

3 Анализ статистики дорожного движения (см. С.2.2.4):

- определить распределения основных статистических переменных, соответствующих сценариям, полученным на предыдущем этапе;
- рассчитать контрольные показатели пробега на основе имеющейся статистики.

4 Определение сценариев тестирования (см. С.2.2.5):

- выбрать сценарии тестирования, предназначенные для валидации целевого применения, в соответствии с профилем миссии и рассматриваемыми опасными сценариями;
- определить минимальный объем валидации для этих сценариев. В С.2.2.5 определен минимальный объем валидации в виде расстояния (в километрах), которое необходимо проехать.

Примечание 1 — С.2.2 относится как к области 2, так и к области 3. Предполагается, что анализ SOTIF (разделы 6 и 7) и верификация SOTIF выполняются до запуска серийного производства транспортного средства.

Примечание 2 — С.2.2 основан на [30].

С.2.2.2 Возможные причины опасных событий

Системы управления транспортным средством, которые имеют определенные полномочия по использованию тормозной системы (например, AEB), могут в некоторых случаях подвергать риску водителя или других участников дорожного движения из-за ошибочного срабатывания. Ложное срабатывание экстренного торможения, вызванное, например, функциональной недостаточностью распознавания объектов, резко замедляет автомобиль до полной остановки, когда в этом нет необходимости.

В соответствии с настоящим стандартом определяются и оцениваются триггерные условия, которые стимулируют опасное поведение (см. раздел 4, рисунок 4), например: «Столкновение со следующим автомобилем из-за непреднамеренного срабатывания AEB». Указанная недостаточность производительности может быть вызвана множеством внешних факторов.

В этом примере критерием приемлемости является вероятность того, что вероятность опасного события, вызванного функциональностью AEB, менее или равна вероятности того же опасного события, вызванного человеком (см. С.4).

$$P_{\text{ha,AEB}} \le P_{\text{ha,hu}}, \quad \text{(С.4)}$$

где $P_{\text{ha,AEB}}$ — вероятность опасных событий, вызванных функциональностью AEB;

$P_{\text{ha,hu}}$ — вероятность опасных событий, вызванных человеком.

Примечание — В С.2.2.2 не рассмотрен вопрос о достаточности этого критерия для обоснования публикации продукта.

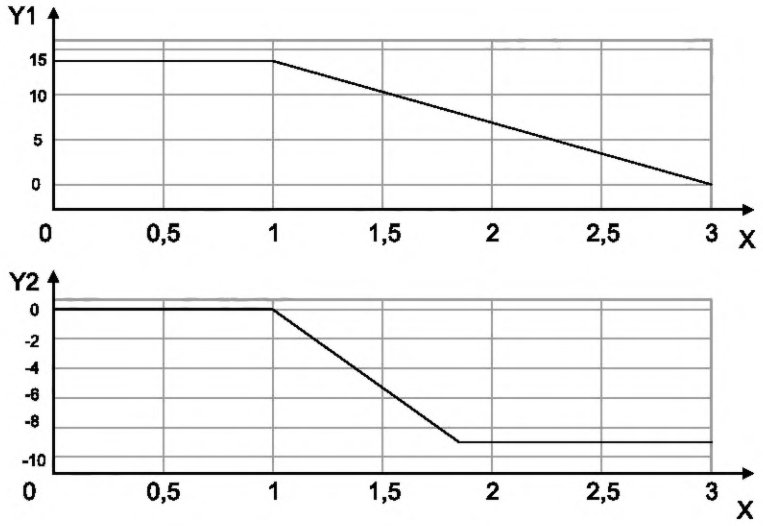
Вероятность опасности зависит от сценария и, в частности, от значений параметров (например, триггерных условий), которые критически важны для безопасности в рамках сценария. Примерами таких параметров являются условия освещенности для систем, оснащенных камерами, наличие материалов, отражающих луч радара для систем с радарами и т. д. Однако в области 3 («невыявленные опасные сценарии») известны не все параметры, которые влияют на безопасность и их значения. Сценарии определяются и их риск оценивается на основе известных зависимостей.

С.2.2.3 Моделирование опасного события

В примерах С.2.2.3—С.2.2.5 рассмотрена система, которая способна выполнять AEB с профилем замедления, показанным на рисунке С.1, в пределах следующих потенциальных проектных ограничений:

- система AEB подает команду торможения с максимальным замедлением 9 м/с^2 в качестве реакции на движущийся объект;
- время нарастания тормозного усилия зависит от предварительного нагнетания жидкости тормозной системы и ограничивается 15 м/с^3;
- функция AEB доступна на скорости выше 5 км/ч;
- максимальное разрешенное снижение скорости составляет 50 км/ч;
- механизмы безопасности в датчике и тормозной системе блокируют выполнение команды AEB за пределами установленного диапазона скоростей.

На рисунке С.1 показано идеальное замедление ведущего транспортного средства системой AEB при начальной скорости 50 км/ч (13,9 м/с).



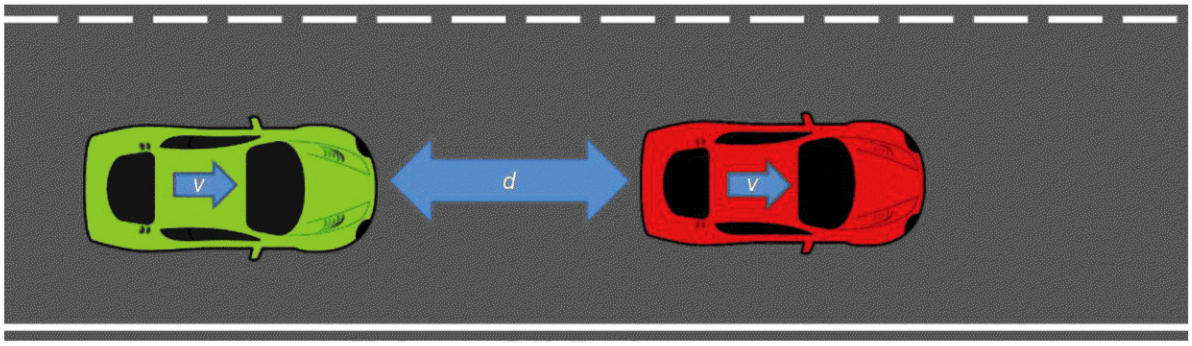
X — время, с; Y1 — скорость транспортного средства, м/с;
Y2 — замедление ведущего транспортного средства, м/с^2

Рисунок С.1 — Профиль замедления AEB

Опасность, связанная с SOTIF, и соответствующий опасный сценарий:

- опасное поведение: непредусмотренное торможение системой AEB в рамках проектных требований в течение более 340 мс;
- опасный сценарий: нежелательное торможение AEB в течение более 340 мс одновременно с близко идущим за ним транспортным средством. В таких условиях нежелательное торможение может привести к наезду сзади.

Это опасное событие можно смоделировать как сценарий следования транспортного средства по прямой дороге с эффектами первого порядка (см. рисунок С.2) [30].



1 — движущееся сзади транспортное средство; *2* — ведущее транспортное средство

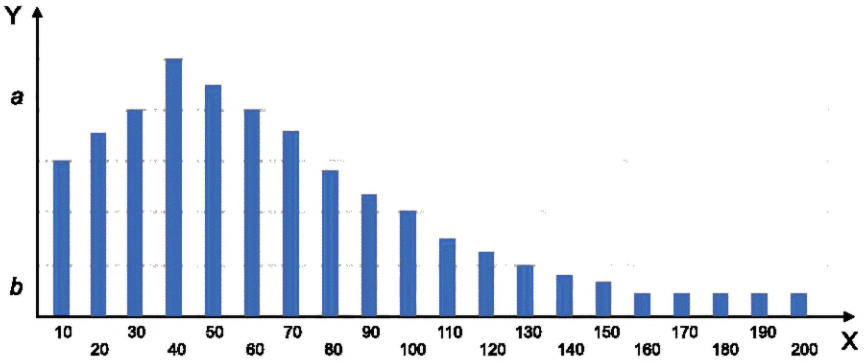
Рисунок С.2 — Сценарий следования транспортных средств, используемый в модели опасного события

Сценарий основан на следующих допущениях:

- вначале оба транспортных средства движутся с одинаковой скоростью *v*;
- расстояние *d*, зависящее от скорости движения, имеет известное распределение вероятностей (см. [27], [28], [30]);
- AEB головного транспортного средства активирует экстренное торможение несмотря на то, что дорожная ситуация не требует этого;
- все события торможения AEB соответствуют профилю торможения, которое изображено на рисунке С.1;
- водитель следующего транспортного средства замечает опасную ситуацию и реагирует на нее торможением. Время реакции имеет известное распределение вероятностей.

Сценарий, который изображен на рисунке С.2 (сценарий 1), был проанализирован с использованием моделирования методом Монте-Карло, где входными переменными являлись расстояние между транспортными средствами и время реакции следующего транспортного средства, для оценки вероятности опасного события (наезда сзади). Было установлено, что исход сценария во многом зависит от скорости транспортных средств в момент непредусмотренного срабатывания AEB. В качестве входных данных при моделировании принимается начальная скорость *v*, а на выходе формируется процент имитационных экспериментов, которые приводят к столкновению.

На рисунке С.3 показано, что вероятность столкновения выше на относительно низких скоростях из-за короткого расстояния следования. Интенсивность столкновения падает при скоростях выше 50 км/ч из-за увеличения дистанции следования и наличия максимального порога снижения скорости. Без порога снижения скорости рисунок С.3 выглядел бы иначе (монотонно увеличивался).



X — начальная скорость, км/ч; Y — вероятность столкновения; *a* — высший порог; *b* — низший порог

Рисунок С.3 — Вероятность вынужденного наезда сзади в сценарии 1 в зависимости от скорости

С.2.2.4 Анализ статистики дорожного движения

Предполагается, что самая распространенная авария, которая приводит к травмам и связана с AEB, происходит в результате столкновения двух автомобилей сзади в сценарии следования за автомобилем («сценарий 1»,

изображенный на рисунке С.2). Был проведен анализ для определения максимально допустимой (приемлемой) частоты возникновения наездов сзади, т. е. $P_{ha,hu}$ в формуле (С.4).

Статистика национальных органов по безопасности дорожного движения [примером являются данные NHTSA GES для США [8], классифицированные по скорости на месте дорожно-транспортного происшествия (ДТП)], дает представление о существующей частоте столкновений при реальной эксплуатации транспортных средств.

Статистика трафика, как правило, включает в себя следующие данные:

- количество легковых автомобилей, которые находятся в эксплуатации (N);
- среднее расстояние, пройденное каждым легковым автомобилем за год (К);
- в качестве альтернативы может указываться общее количество километров, пройденных транспортными средствами за год (М). Если параметр не указан, его можно оценить по формуле: $M = N \cdot K$;
- количество соответствующих несчастных случаев (наездов сзади) в год в реальных условиях (А).

Доверие к оценке, полученной в результате дальнейшего анализа, повышается за счет принятия статистической модели для рассматриваемых переменных. На основе этой информации можно рассчитывать среднее расстояние, пройденное водителями-людьми между столкновениями (контрольный показатель *B*), по формуле

$$B = \frac{M}{A}, \tag{С.5}$$

где B — среднее расстояние, пройденное водителями-людьми между столкновениями (контрольный показатель, В);

M — общее количество километров, пройденных транспортными средствами за год;

A — количество соответствующих несчастных случаев (наездов сзади) за год при реальной эксплуатации.

Чтобы получить оценку наихудшего случая, следует использовать верхнюю границу значения *M* и нижнюю границу значения *A*.

Обоснование безопасности требует доказательств того, что транспортное средство, оснащенное АЕВ, может безаварийно проехать не менее *B* километров, или вероятность аварии, вызванной функциональными недостаточностями системы АЕВ, составляет менее 1/*B* на километр при сравнении с формулой (С.4).

Примечание 1 — Представленный выше критерий является лишь вероятностным теоретическим измерением для оценки риска, который допустим при принятии решения о выпуске продукта на рынок. Следовательно, даже если эта цель достигнута при валидации, а в реальной ситуации происходит нежелательное срабатывание АЕВ, решение о необходимости принятия контрмер требует дополнительного анализа и учета аспектов, связанных, например, с архитектурой, спецификацией системы и ODD.

Примечание 2 — Контрольный показатель в формуле (С.5) можно рассматривать как нижнюю границу при валидации системы. В зависимости от степени достоверности статистики трафика этот показатель можно увеличивать или уменьшать, умножая *B* на коэффициенты $\kappa_1\kappa_2$. Тогда определение контрольного показателя будет следующим: $B = \kappa_1\kappa_2 (M/A)$.

Пример 1 — Умножение контрольного показателя B на коэффициент $\kappa_1 > 1$ можно использовать для консервативной оценки того, что функция АЕВ не приведет к увеличению количества аварий, регистрируемых статистикой дорожного движения.

Пример 2 — Статистика дорожного движения включает обоснованные и необоснованные случаи торможения. Для ложноположительного торможения АЕВ при определении контрольного показателя имеет значение только необоснованное торможение, приводящее к опасному событию (наезду сзади). Коэффициент κ_2 определяется как вероятность опасного события, а $\kappa_2 = 1/n$ может использоваться для корректировки случая, когда только одно из n реальных событий торможения приводит к опасному событию из-за необоснованного торможения.

Примечание 3 — Моделирование, описанное в С.2.2.3, может использоваться для оценки вероятности опасного события из-за необоснованного торможения κ_2.

С.2.2.5 Определение сценариев тестирования

Если критерий приемлемости соблюдается с необходимой достоверностью, может отсутствовать необходимость проезжать расстояние не менее *B*, чтобы продемонстрировать достижение приемлемого уровня остаточного риска. Для уточнения стратегии сбора и валидации данных можно использовать профиль миссии транспортного средства (см. таблицу С.1) и данные о поведении системы.

Моделирование (см. В.2.2.3) показывает, что наибольший риск АЕВ достигается при скорости 50 км/ч.

Сценарий 1 (см. рисунок С.2) делится на три сценария:

- сценарий 1.1: v = 0—40 км/ч;
- сценарий 1.2: v = 40—80 км/ч;
- сценарий 1.3: v > 80 км/ч.

В таблице С.1 представлен анализ распределения вероятности серьезности наездов сзади в США в период с 2010 по 2017 годы с использованием общедоступных данных (см. [30]). В этих данных доступна вероятность столкновения и соответствующие уровни серьезности для каждого установленного ограничения скорости:

- городские дороги (ограничения скорости 0—25 миль/ч или 0—40 км/ч);
- проселочные дороги (ограничение скорости в пределах 25—60 миль/ч или 40—100 км/ч); и
- автомагистрали и автомагистрали между штатами (ограничение скорости выше 60 миль в час — 100 км/ч).

Сравнивая области с наибольшей вероятностью столкновения, изображенные на рисунке С.3, с распределением серьезности в таблице С.1, можно определить, что эти области совпадают для столкновений сзади, вызванных человеком и системой АЕВ. Область наибольшего риска соответствует сценарию 1.2.

Примечание — Возможная активация АЕВ на скорости более 80 км/ч нарушает ограничения системы. Это может быть реализовано, например, с помощью внешних мер, предложенных в стандартах серии ИСО 26262, и поэтому не относится области применения С.2.2.

Таблица С.1 — Распределение вероятности серьезности риска наезда движущегося сзади автомобиля в зависимости от установленного ограничения скорости в США

Установленное ограничение скорости, км/ч	0—40	40—80	80—100	> 100	Все скорости
Процент столкновений сзади (в том числе при движении задним ходом)	9,4 %	69,9 %	12,8 %	7,9 %	100,0 %
Без травм	80,0 %	73,3 %	74,6 %	72,9 %	74,1 %
Травма без потери трудоспособности	18,9 %	24,7 %	22,7 %	25,0 %	24,0 %
Травма с потерей трудоспособности	1,1 %	1,8 %	2,3 %	1,6 %	1,8 %
Травма с летальным исходом	0,055 %	0,52 %	0,33 %	0,55 %	0,13 %

При наличии статистических данных контрольный показатель можно пересчитать для сценария 1.2 по формуле

$$B_{40...80} = \frac{M_{40...80}}{A_{40...80}}, \quad \text{(С.6)}$$

где $B_{40...80}$ — среднее расстояние, пройденное водителями-людьми между столкновениями (контрольный показатель B) при движении со скоростью от 40 до 80 км/ч;

$M_{40...80}$ — общее количество километров, пройденных транспортными средствами за год при движении со скоростью от 40 до 80 км/ч;

$A_{40...80}$ — количество соответствующих аварий (наездов сзади) за год при реальной эксплуатации при движении со скоростью от 40 до 80 км/ч.

Для параметров, влияние которых на риск неизвестно, сбор данных может включать в себя широкий спектр условий вождения, например:

- погодные условия: систему АЕВ можно испытывать в репрезентативном наборе погодных условий. Сюда входят сухая погода, туман, снег, дождь, пасмурная погода и т. д.;
- время суток: в зависимости от типа датчика сбор данных может включать в себя различное время суток — например, ночь, сумерки и т. д.

Кроме того, сбор данных может включать в себя соответствующие ситуации вождения, полученные на основе анализа ограничений датчиков и ограничений конкретных функций.

Пример профиля миссии транспортного средства приведен в таблице С.2. Спецификация основана на реальных профилях погоды, скорости и других параметров. Он также может основываться на данных о частоте возникновения сценариев, полученных в результате моделирования либо путем оценки.

Таблица С.2 — Пример профиля миссии транспортного средства

Время суток	
Тип	Процент
День	50 %

Окончание таблицы С.2

Ночь	35 %
Сумерки	15 %
Скорость транспортного средства	
Скорость (км/ч)	Процент
0—50	60 %
50—80	40 %
> 80	0 %
Погодные условия	
Тип	Процент
Сухое/ясное небо	65 %
Дождь	7 %
Туман	5 %
Снег	5 %
Пасмурно	10 %
Сильный дождь	5 %
Другие погодные условия	3 %

С.2.2.6 Особенности метода определения контрольного показателя

Подход, основанный на статистике дорожного движения, который описан в п. С.2.2, может использоваться для определения целевого контрольного показателя среднего времени между столкновениями (mean time between collisions, MTBC) для валидации надежности системы автоматизации вождения перед массовым производством или эксплуатацией в реальных условиях. Тем не менее, при использовании этого метода учитываются следующие факторы:

- масштабируемость: применение метода к полностью автоматизированному транспортному средству может оказаться практически нецелесообразным, если не приняты во внимание особенности архитектуры конкретной системы. Например, для системы AEB в С.2.2 расширение диапазона скоростей, применимое к функции AEB, до скоростей шоссе (например, 130 км/ч) увеличило пробег для валидации контрольного показателя из-за более низкой частоты наездов сзади на таких скоростях;
- независимость от архитектуры системы: особенности архитектуры системы могут быть использованы для оптимизации пробега при целевой валидации. Для сложных функций, в которых для избыточной валидации конкретного управляющего действия используется более одной подсистемы, можно оптимизировать MTBC, полученное на основе статистики дорожного движения, с учетом отдельных метрик, которые влияют на MTBC на уровне транспортного средства (например, частоты ложных срабатываний камеры или ложного обнаружения объектов радаром каждой подсистемы);
- зависимость от валидации маршрута: конкретные маршруты вождения, выбранные после анализа ограничений системы, могут давать более точное определение MTBC, что позволяет сокращать необходимый объем сбора данных.

С.3 Валидация применяемых систем SOTIF

На рисунке С.4 показано возможное применение итераций верификации и валидации в сочетании с целями охвата и ограниченным случайным тестированием для обнаружения невыявленных опасных сценариев или функциональных недостаточностей (т. е. уменьшения области 3) с целью поддержки разработки SOTIF (см. рисунок 7). В исходном состоянии (крайний левый круг), которое предшествует началу верификации и валидации, в ходе анализа безопасности был выявлен ряд потенциальных функциональных недостаточностей (темно-серые кружки, обозначающие область 2). Могут существовать и другие функциональные недостаточности, однако они не выявляются на данном этапе [черные кружки, невыявленные опасные сценарии (область 3)]. Пунктирный квадрат представляет собой использованную функциональность из полного набора функций (например, функциональность, использованную в ODD).

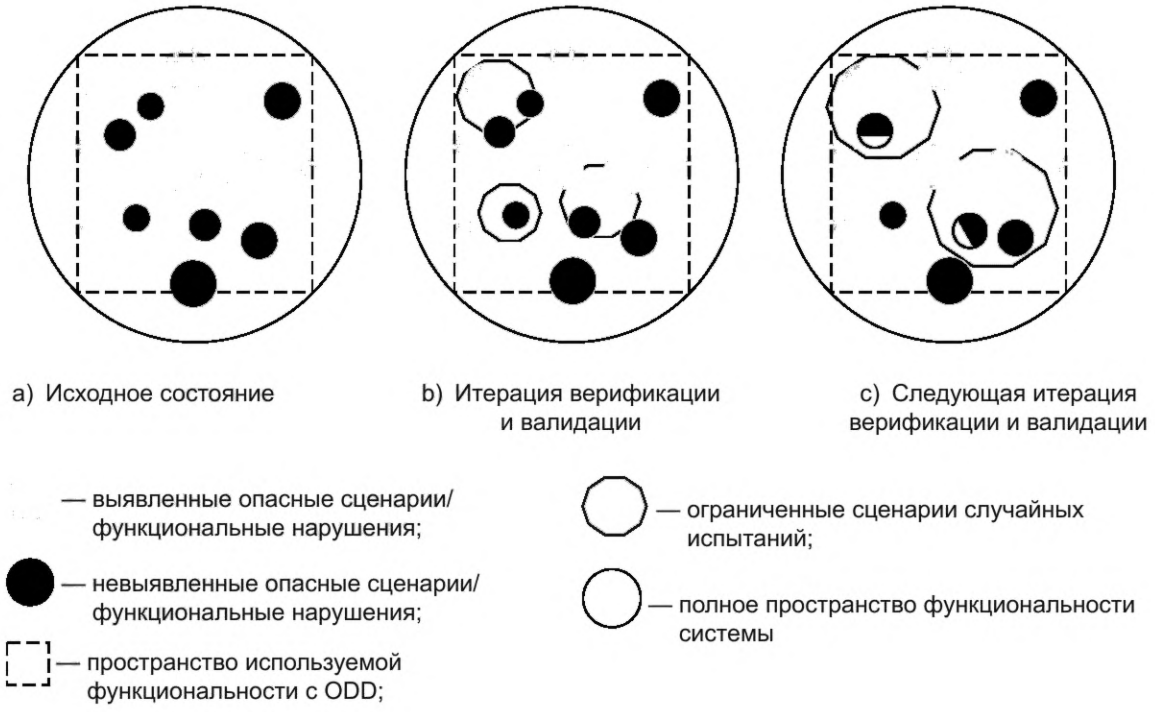


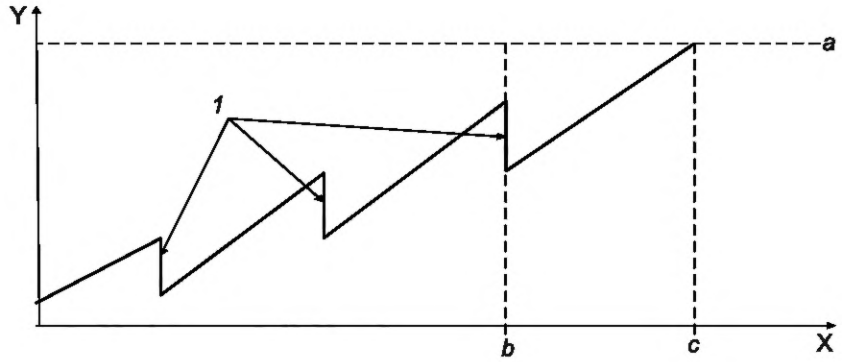
Рисунок С.4 — Итерации тестирования разработки SOTIF

Общая цель верификации и валидации — свести к минимуму возникновение невыявленных опасных сценариев с учетом границ ODD. Одним из методов является использование выявленных сценариев в качестве основы для ограниченной случайной генерации тестов новых сценариев, что позволяет постепенно увеличивать охват тестирования. Эти новые сценарии/тесты могут разрабатываться с целью выявления невыявленных опасных сценариев [см. рисунок С.4 b)] путем увеличения охвата тестирования.

Последующая итерация верификации и валидации основывается на предыдущей. Обнаруженные невыявленные сценарии, которые становятся известными, служат дополнительной основой для увеличения охвата за счет расширения охватываемого случайного пространства. Ранее выявленные сценарии также можно использовать в качестве основы для создания большего количества случайных тестов и сценариев.

Этот итеративный процесс продолжается до тех пор, пока не достигается достаточный охват используемого функционального пространства. Результатом является обнаружение сценариев области 3, которые затем преобразуются в сценарии области 2 [см. рисунок С.4 c)]. Некоторые обнаруженные опасные сценарии можно смягчать благодаря сокращению ODD.

Модель, показанная на рисунке С.4, также может использоваться в типичной стратегии разработки программного обеспечения транспортного средства для систем, к которым применима SOTIF. Следует ожидать, что по мере тестирования программного обеспечения и устранения потенциально опасного поведения средний пробег между его случаями увеличится. Тем не менее, по мере добавления или включения новых возможностей/функций среднее количество часов или километров на один случай потенциально опасного поведения может уменьшаться, а затем увеличиваться по мере устранения ошибок, возникающих при появлении новых возможностей/функций. В конечном счете достигается порог цели валидации для указанного варианта использования и функциональности, и действие по валидации можно считать выполненным. Эта концепция проиллюстрирована на рисунке С.5.



X — время разработки; Y — средний пробег на один случай нежелательного поведения;
1 — реализована новая возможность/функция; *a* — цель валидации;
b — возможность/функция готова (кандидат на выпуск);
c — критерии валидации выполнены

Рисунок С.5 — Ожидаемый профиль интенсивности потенциально опасного поведения во время разработки

Например, перед тестированием разработчик/заказчик системы указывает:

1) цель валидации (условие завершения);
2) распределение задач между режимами тестирования, реальными тестами, HIL, SIL и т. д.;
3) определение потенциально опасного поведения, критерий перезапуска счетчика расстояния.

Процесс валидации систем, к которым применима SOTIF, начинается с выбора критерия приемлемости (см. 6.5), на основании которого определяется цель валидации. Целевое значение может рассчитываться исходя из варианта использования системы (например, помощь при парковке, автоматическое экстренное торможение, удержание полосы движения, автоматическая параллельная парковка, низкоскоростной автоматизированный трансфер/маршрутный транспорт, автопилот на шоссе, автоматическое такси), статистики аварий для данного варианта использования и резерва безопасности.

Для формирования цели можно использовать:

- статистику.

Пример 1 — Сообщения о столкновениях;

- характеристики человеческого фактора в статистике.

Пример 2 — Одно столкновение на 500 000 миль, статистика аварий NHTSA за 2015 г. [29];

- резерв безопасности;
- предел статистической достоверности.

Пример 3 — Для конкретного варианта использования водители-люди проезжают в среднем x километров между происшествиями. Из соображений безопасности указан дополнительный резерв y > 1. Критерием приемлемости выбранной системы, к которой применима SOTIF, является среднее количество километров B · y между случаями потенциально опасных видов поведения или целевая интенсивность инцидентов $A_H = 1 / (B \cdot y)$. Условие завершения предполагает, что инциденты имеют распределение Пуассона. Используя цель валидации τ, можно показать, что интенсивность инцидентов в системе составляет не более A_H с достоверностью α, если количество поездок без возможно опасного поведения равно τ, где τ вычисляют по формуле (см. [31])

$$\tau = -\ln(1-\alpha) / A_H. \qquad \text{(С.7)}$$

Примечание 1 — Значение τ может быть выражено в единицах времени или расстояния в зависимости от единиц интенсивности инцидентов.

Примечание 2 — Для $\alpha \approx 0{,}63$ $\tau = 1/A_H = B \cdot y$.

Примечание 3 — Распределение может изменяться с течением времени. Например, может возникнуть необходимость контролировать наличие в статистике существующей системы ADAS, такой как AEB, путем сравнения интенсивности событий до и после широкого внедрения системы.

На практике τ (пробег в километрах или часах, необходимый для валидации) может быть довольно большим и иногда непрактичным. Можно снижать реальные требования к нему, используя экспертные знания о схожих системах и пробег, получаемый в результате моделирования, MIL, SIL и HIL. Приемлемое соотношение между реальными и модельными испытаниями может быть определено исходя из возможностей моделирования (например, моделирование является реалистичным только в определенных сценариях). Реальные и полученные путем моделирования условия валидационных испытаний разумно варьируются (например, различные погодные условия, время суток, состояние дороги, условия дорожного и пешеходного движения, и т. д.) с целью обнаружения ситуаций, которые редко возникают при эксплуатации.

С.4 Верификация и валидация системы восприятия

С.4.1 Структура верификации и валидации системы восприятия

С.4.1.1 Общие положения

В настоящем подразделе представлен пример метода, который можно использовать для поэтапной верификации и валидации эффективности конкретной системы восприятия. Системы восприятия играют значительную роль в обеспечении SOTIF автоматизированного транспортного средства на любом уровне автоматизации вождения. Метод, который представлен в этом примере, можно применять к любому типу технологии восприятия, используемой в транспортном средстве с ADS (например, радару, камере, лидару, ультразвуковому устройству).

Характеристики системы восприятия находятся под влиянием различных проблем, которые могут возникать на любом этапе разработки. Следовательно, важно, чтобы система восприятия подвергалась поэтапной верификации и валидации, как показано на рисунке С.6.

Примечание 1 — На рисунке представлена восходящая последовательность этапов, однако порядок их выполнения не регламентирован.

Примечание 2 — Этапы могут быть выполняться несколькими компаниями (см. 4.4.2).

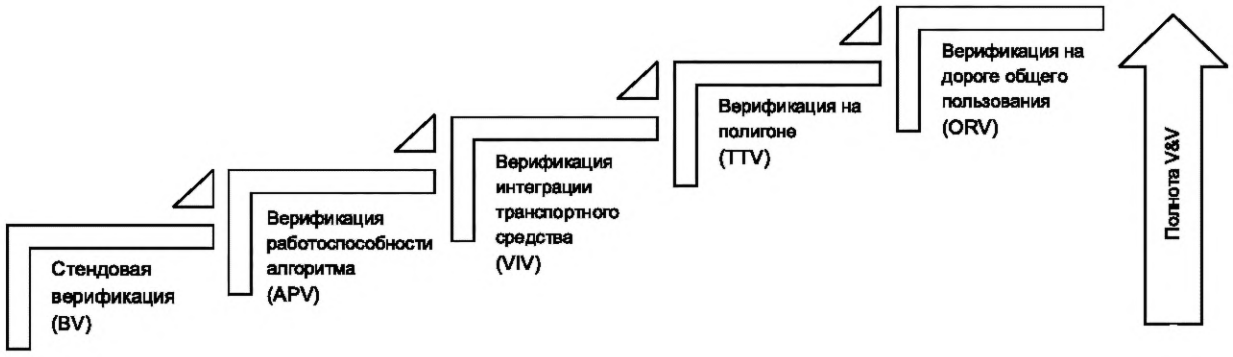


Рисунок С.6 — Примеры этапов верификации и валидации системы восприятия

Процесс верификации и валидации системы восприятия может включать в себя несколько этапов:

- верификация на стенде (BV): первоначальная верификация чувствительности системы восприятия в контролируемой среде;
- верификация работоспособности алгоритма (APV): работоспособность системы восприятия проверяется с использованием более масштабных данных;
- верификация интеграции транспортного средства (VIV): работоспособность системы восприятия верифицируется после интеграции в целевое транспортное средство;
- верификация на полигоне (TTV): работоспособность системы восприятия верифицируется на полигоне по нескольким эталонным сценариям использования;
- валидация на дороге общего пользования (ORV): работоспособность системы восприятия валидируется на дороге общего пользования по всем надлежащим сценариям.

В С.4.1.2—С.4.1.6 представлены примеры анализа с использованием SIPOC (поставщик, вход, процесс, выход, заказчик). SIPOC — это инструмент, который объединяет входные и выходные данные одного или нескольких процессов в табличной форме и используется для определения процесса от начала до конца (см. [32]). SIPOC — это метод анализа, который используется для управления качеством и улучшения процессов, но при анализе процессов верификации и валидации системы восприятия также можно использовать другие методы.

С.4.1.2 Верификация на стенде

Для верификации чувствительности собранной системы восприятия в эталонной среде (стендовые испытания) можно определять действия стендовой верификации. Это испытание полезно для верификации устойчивости

системы восприятия с конкретными производственным допусками в контролируемой среде (например, разная допустимая чувствительность антенны радара или разное расстояние фокусировки камеры). Примеры испытаний такого типа приведены в таблице С.3.

Таблица С.3 — Верификация на стенде

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Заказчик (C)
Определение	Проектирование	Требования к обнаружению (например, способность к различению и разделению, точность)	Верификация чувствительности системы восприятия в контролируемой среде в соответствии со спецификацией изделия	Верификация пройдена: система восприятия с верифицированной чувствительностью в контролируемой среде. Верификация не пройдена: система восприятия отбракована (для доработки или утилизации)	Группа проектирования (для дальнейшего испытания) OEM/ поставщик уровня X
	Производство	Система в сборе (после SMV)			
Пример 1	Проектирование	Требования к радиолокационному обнаружению (KPI)	Верификация требуемой чувствительности в безэховой камере с помощью генератора радиолокационных целей	Верификация пройдена: радар с верифицированной чувствительностью по эталонным данным. Верификация не пройдена: радар отбракован (для доработки или утилизации)	Группа проектирования для дальнейшего испытания OEM/ поставщик уровня X
	Производство	Радар в сборе (после SMV)			
Пример 2	Проектирование	Требования к чувствительности камеры (KPI)	Верификация требуемой чувствительности перед экраном, воспроизводящим ранее записанные данные или искусственные клипы	Верификация пройдена: камера с верифицированной чувствительностью по эталонным данным. Верификация не пройдена: камера отбракована (для доработки или утилизации)	Группа проектирования (для дальнейшего испытания) OEM/ поставщик уровня X
	Производство	Камера в сборе (после SMV)			

С.4.1.3 Верификация работоспособности алгоритма

Для верификации чувствительности алгоритма системы восприятия на наборе эталонных данных можно определять действия по верификации работоспособности алгоритма (например, повторное использование моделирования или собранные ранее данные). Это испытание может быть полезно для проверки отсутствия ухудшения характеристик в последующих версиях ПО, использующих одни и те же аппаратные средства:

- код на различных этапах проявляет поведение системы и возможные функциональные недостаточности;
- повышается устойчивость за счет повторения процесса;
- предотвращается повторное возникновение проблем в процессе разработки;
- формируется стабильная база для анализа первопричин.

Этап верификации работоспособности алгоритма может выполняться на целевых аппаратных средствах (пример теста HIL) либо на эмуляторе (пример теста SIL) с использованием ранее записанных или моделируемых данных. Из-за различий между этими двумя методами в таблице С.4 не приводятся примеры применения этого этапа верификации к различным системам восприятия. Описание метода, который можно использовать для верификации работоспособности алгоритма, приведено в С.4.1.4.

Таблица С.4 — Верификация работоспособности алгоритма

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Клиент (C)
Определение	Проектирование	Эталонные данные (заранее собранные данные или данные, полученные в результате моделирования). Требования к обнаружению/KPI	Верифицировать правильность работы алгоритма на основе набора эталонных данных (внесенных данных или данных, полученных в результате моделирования)	Верификация пройдена: алгоритмы системы восприятия верифицированы. Верификация не пройдена: пересмотр или доработка алгоритма(ов) системы восприятия	Группа проектирования (для дальнейшегоиспытания) OEM/ поставщик уровня X
		Алгоритмы и эмуляция ПО (при ПО в контуре)			
	Производство	Система в сборе (при наличии аппаратных средств в контуре)			

С.4.1.4 Верификация интеграции транспортного средства

Для верификации работоспособности системы восприятия в целевом транспортном средстве и отсутствии внеплановых снижений/изменений характеристик можно определять действия по верификации интеграции транспортного средства. Этот этап верификации может быть полезен для лучшего подтверждения того, что:

- система восприятия способна использовать информацию, предоставляемую целевым транспортным средством (сигналы динамики транспортного средства и т. д.);
- система восприятия может работать без ухудшения характеристик из-за недостаточностей спецификации, связанных с целевой реализацией (например, отражательной способности лобового стекла для камеры, типа и толщины краски для радара, встроенного за бампером, или ненадлежащего диэлектрического материала, размещенного перед радаром).

В таблице С.5 представлен пример верификации интеграции транспортного средства.

Таблица С.5 — Верификация интеграции транспортного средства

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Клиент (C)
Определение	Проектирование	Технические характеристики транспортного средства	Верифицировать, что система восприятия работает в соответствии со спецификацией при использовании в целевом транспортном средстве	Верификация пройдена: система восприятия для интеграции в транспортное средство верифицирована. Верификация не пройдена 1: пересмотр или переработка системы восприятия. Верификация не пройдена 2: пересмотр или переработка системы восприятия	Группа проектирования (для дальнейшего испытания) OEM/ поставщик уровня X
	Производство	Система восприятия в сборе. Транспортное средство (репрезентативная целевая среда)			
Пример 1	Проектирование	Коммуникационный протокол транспортного средства	Верифицировать, что система восприятия может использовать сигналы транспортного средства: - динамические характеристики транспортного средства передаются с правильной задержкой. Электрические сигналы находятся в пределах технических характеристик	Система восприятия интегрирована в транспортное средство. Верификация не пройдена 1: пересмотр или переработка системы восприятия. Верификация не пройдена 2: пересмотр или переработка системы восприятия или интерфейса транспортного средства	Группа проектирования (для дальнейшего испытания) OEM/ поставщик уровня X
	Производство	Система восприятия в сборе. Транспортное средство (репрезентативная целевая среда)			

Окончание таблицы С.5

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Клиент (C)
Пример 2	Проектирование	Ожидаемое ухудшение характеристик радара	Тестируется ухудшение характеристик радара: - из-за неправильно определенной формы/кривизны бампера (радар за бампером или логотипом); - из-за неправильно определенной краски (радар за бампером или логотипом с неправильной толщиной или типом краски). Ухудшение характеристик из-за неправильных диэлектрических характеристик (неверно определен материал бампера, неправильный проект логотипа…)	Верификация пройдена: интеграция радара за бампером транспортного средства. Верификация не пройдена 1: пересмотр или переработка системы восприятия. Верификация не пройдена 2: пересмотр или переработка системы восприятия или бампера транспортного средства	Группа проектирования для дальнейшего испытания OEM/ поставщик уровня X
	Производство	Система восприятия в сборе. Транспортное средство (репрезентативная целевая среда)/ часть транспортного средства (репрезентативный целевой проект)			
Пример 3	Проектирование	Ожидаемое снижение производительности камеры	Тестируется ухудшение характеристик камеры: - интеграция камеры за лобовым стеклом. Верификация сборки камера — кронштейн — лобовое стекло	Верификация пройдена: интеграция камеры за лобовым стеклом. Верификация не пройдена 1: система восприятия отбракована (для доработки или утилизации). Пересмотр или переработка системы восприятия. Верификация не пройдена 2: пересмотр или переработка системы восприятия или бампера транспортного средства	Группа проектирования для дальнейшего испытания OEM/ поставщик уровня X
	Производство	Система восприятия в сборе. Транспортное средство (репрезентативная целевая среда)/ часть транспортного средства (репрезентативный целевой проект)			

С.4.1.5 Верификация на полигоне

Для верификации чувствительности системы восприятия на конкретном наборе эталонных вариантов использования (сценариев, включая конкретные триггерные условия) можно определять действия по верификации на полигоне. Несмотря на то, что сами варианты использования (сценарии), как правило, не зависят от технологии (природы) системы восприятия, можно выбирать специфичный для технологии набор вариантов использования (сценариев, в том числе конкретные триггерные условия) или распределять его по приоритетам для верификации следующих аспектов:

- характеристики системы восприятия в конкретных вариантах использования (обнаружение объектов на определенных расстояниях; сценарии испытаний, аналогичные протоколам, которые разработаны программами оценки показателей безопасности автомобилей: Euro NCAP, JNCAP, NHTSA, KNCAP, C-NCAP, Latin NCAP и т. п.);
- верификация системы восприятия в конкретных сценариях, направленная на использование ограничений системы восприятия (например, угловой точности радара);
- взаимодействие датчика целевого транспортного средства с датчиками этого или других транспортных средств (например, взаимное наведение радиолокационных помех).

В таблице С.6 описан пример верификации на полигоне.

Таблица С.6 — Верификация на полигоне

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Клиент (C)
Определение	Проектирование	Список вариантов использования. Выявленные недостаточности производительности системы восприятия	Верификация работы системы восприятия в конкретных вариантах использования, имеющих отношение к конечной функции	Верификация пройдена: верифицирована работа системы восприятия. Верификация не пройдена: пересмотр или переработка системы восприятия	Группа проектирования (для дальнейшего испытания). OEM/поставщик уровня X
	Производство	Собранная (в транспортном средстве) система восприятия (после VIV)			
Пример 1	Проектирование	Список вариантов использования. Выявленные недостаточности производительности системы восприятия	Верификация способности системы восприятия отличать пешехода от припаркованного автомобиля за заданное время в рамках AEB Euro NCAP. Сценарий скрытого уязвимого участника дорожного движения (VRU), предложенный программами оценки показателей безопасности автомобилей	Верификация пройдена: верифицирована работоспособность системы восприятия. Верификация не пройдена: пересмотр или переработка системы восприятия	Группа проектирования для дальнейшего испытания OEM/поставщик уровня X
	Производство	Собранная (в транспортном средстве) система восприятия (после VIV)			
Пример 2	Проектирование	Радарная система восприятия частотных помех	Верификация возможностей радарной системы с защитой от помех	Верификация пройдена: отсутствие помех в радарной системе восприятия. Верификация не пройдена: пересмотр или переработка системы восприятия	Группа проектирования для дальнейшего испытания OEM/поставщик уровня X
	Производство	Собранная (в транспортном средстве) система восприятия (после VIV)			

С.4.1.6 Валидация на дороге общего пользования

Для валидации характеристик системы восприятия в целевой среде можно определять действия по валидации на дороге общего пользования. Целями этапа валидации могут являться:

- непрерывный сбор репрезентативных данных на нескольких рынках в различных условиях внешней среды;
- сбор конкретных данных в условиях, которые редки и маловероятны при обычном вождении, но могут влиять на восприятие, например:
  - зрительное восприятие: данные в сумерках или на рассвете;
  - восприятие радара: дождь и брызги, дороги с солеными брызгами;
  - восприятие лидара: неблагоприятные погодные условия;
  - все виды восприятия: вход/выход из туннеля;
- сбор конкретных данных в необычных сценариях, которые могут увеличивать вероятность опасного поведения, например:
  - движение по дорогам с низкоинтенсивным движением транспорта и отсутствием головных автомобилей может повышать вероятность неправильного выбора цели в пути и обнаружения целей-призраков;
  - обгон ряда грузовиков с длинной тенью, закрывающей полосу(ы) обгона;
  - разбрызгиваемый снег при проезде снегоочистителя может приводить к внезапному ослеплению одной или нескольких систем восприятия;
- сбор конкретных данных об ограничениях системы, например:
  - о технологических ограничениях (радары на металлических мостах);

- функциональных/алгоритмических ограничениях (регулировка луча при отсутствии дорожного движения);
- различные манеры вождения;
- специальные испытания в неблагоприятных условиях, например:
  - погода;
  - качество инфраструктуры;
  - характер дорожного движения (хаотичный или организованный);
  - динамика вождения (поперечная и продольная);
  - помехи в придорожном пространстве (наличие нескольких источников света или сложные дорожные сооружения);
  - условия дорожного движения (дорога с большим количеством уязвимых участников дорожного движения или шоссе).

В таблице С.7 описан пример валидации на дороге общего пользования.

Таблица С.7 — Валидация на дороге общего пользования

Тип	Поставщик (S)	Вход (I)	Процесс (P)	Выход (O)	Клиент (C)
Определение	Проектирование	Список вариантов использования. Выявленные недостаточности производительности системы восприятия (после TTV или APV или при постоянном обновлении после нескольких сеансов TTV или APV)	Валидация характеристик системы восприятия в целевых вариантах использования с учетом целевого рынка, целевых функций и ограничений системы восприятия	Валидация пройдена: характеристика системы восприятия валидирована для всех надлежащих условий. Валидация не пройдена: пересмотр или переработка системы восприятия	Группа проектирования для дальнейшего испытания) OEM/ поставщик уровня X
	Производство	Собранная (в транспортном средстве) система восприятия (после VIV)			

С.4.2 Стохастические модели датчиков

Сложные системы автоматизации вождения могут требовать столь многочисленных испытаний, что их невозможно осуществить на практике. Моделирование в виртуальной среде может охватывать значительную часть такого тестирования в дополнение к физическим испытаниям. Моделирование датчиков является одним из важнейших аспектов, поскольку современные датчики сложны и подвержены сложным, часто случайным, явлениям.

Высокоточные модели датчиков, учитывающие физические процессы, которые протекают в них, требуют трудоемкого моделирования и очень большого количества вычислительных ресурсов. Стохастические модели датчиков обладают следующими преимуществами:

- не требуется подробная информация о реализации датчика;
- простота применения метода Монте-Карло для различных параметров и ситуаций;
- необходим средний/низкий уровень вычислительных мощностей.

Этот подход может быть как параметрическим, так и непараметрическим: параметрическая статистика — это раздел статистики, где предполагается, что выборка принадлежит совокупности, которая может быть достаточно точно и адекватно смоделирована вероятностным распределением с определенным набором параметров. Большинство известных элементарных статистических методов являются параметрическими. Непараметрическая модель отличается от них тем, что набор параметров не фиксирован и может увеличиваться или даже уменьшаться при сборе новой полезной информации. Поскольку параметрическая модель опирается на фиксированный набор параметров, в ней делается больше допущений о конкретной совокупности, чем в непараметрических методах. Если такие предположения верны, параметрические методы дают более достоверные и точные оценки, чем непараметрические методы, т. е. имеют большую статистическую мощность. Однако, когда предположения неверны, параметрические методы более подвержены ошибкам и, следовательно, ненадежны.

При параметрическом подходе модель датчика, как правило, отражает функциональную структуру датчика:

- датчик декомпозирован на функциональные модули;
- каждый модуль отвечает за моделирование конкретного результата процесса обнаружения/измерения;
- каждый модуль моделируется независимо;
- каждый модуль характеризуется набором настраиваемых параметров;
- выходные данные системы моделирования представляют собой сочетание всех смоделированных этапов.

Непараметрический подход основан на статистическом представлении результата измерения без детального моделирования внутренней структуры датчика, которая моделируется как черный ящик (см. [33]).

Типичная функциональная архитектура статистических экспериментов для оценки параметров датчиков показана на рисунке С.7 для модели датчика с видеокамерой. В качестве входных данных используется база реальных данных. Этот входной сигнал одновременно подается в камеру на испытательном стенде и на вход стохастической модели датчика. Реакция модели сравнивается с реакцией камеры на испытательном стенде. Модель формирует ключевой показатель результата работы датчика, а функция оптимизации обновляет параметры модели до тех пор, пока разница не становится минимальной.

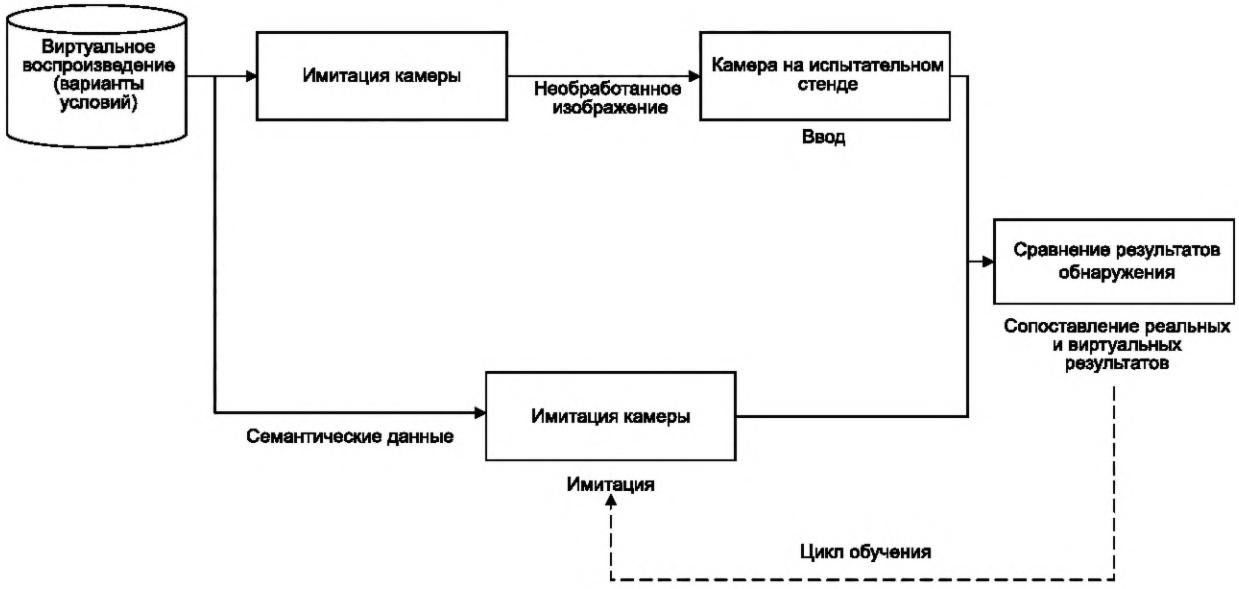


Рисунок С.7 — Пример архитектуры. Калибровка модели датчика с видеокамерой

После калибровки модель датчика валидируется с помощью данных, которые не использовались для калибровки или обучения имитационной модели. После успешной валидации модели ее можно использовать как для анализа отдельного датчика, так и при моделировании транспортного средства. Параметры можно улучшать по мере накопления реальных данных.

С.5 Руководство по параметризации сценариев и выборке

Настоящий раздел включает в себя справочное руководство по моделированию, верификации и валидации на основе сценариев для поддержки целей согласно разделам 10 и 11.

Имитационное испытание может играть важную роль в процессе валидации. После создания точной модели системы и внешней среды можно выполнять валидацию системы, используя заранее записанные или сформированные выявленные сценарии.

Кроме того, можно генерировать новые тестовые примеры на основе записанных сценариев и моделирования для тестирования невыявленных сценариев. На рисунке С.8 показан пример создания новых тестовых вариантов на основе случайного тестирования посредством изменения одного или нескольких аспектов номинального сценария.

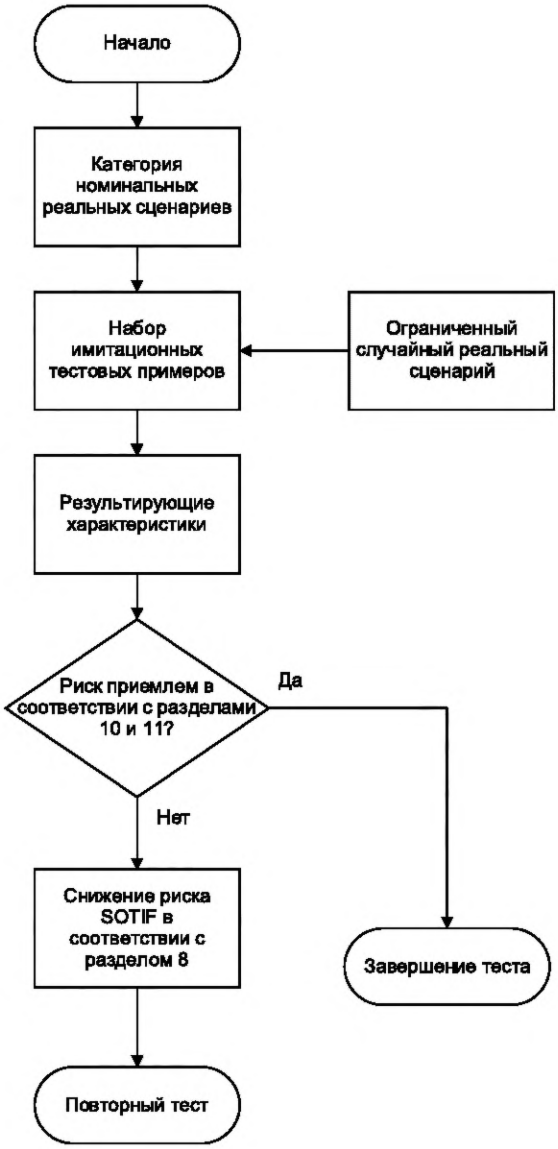
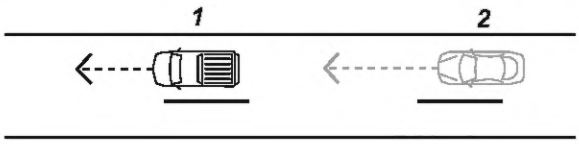


Рисунок С.8 — Ограниченное выборочное тестирование SOTIF

Это тестирование может быть случайным, структурированным (например, с фиксированным шагом увеличения параметра) или сочетать свойства обоих типов (например, последовательную или параллельную композицию подсценариев).

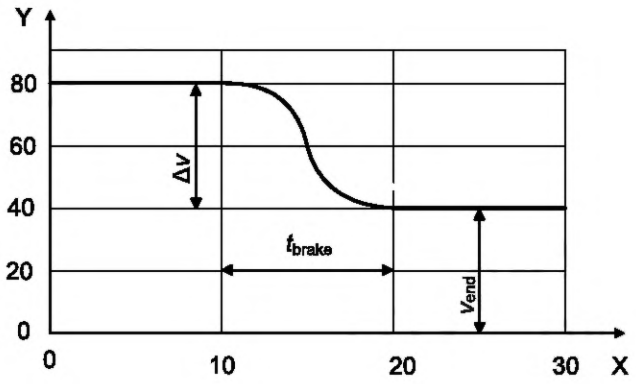
Можно повышать точность процесса моделирования, если известны распределения изменяемых параметров. Часто можно определять распределения параметров на основе реальных данных вождения. Рассмотрим следующий пример, приведенный в [34]. Целевое транспортное средство следует за другим транспортным средством по прямой дороге на заданном расстоянии. ACC осуществляет продольное управление целевым транспортным средством. Предполагается, что оба автомобиля движутся прямо в одном направлении. Ведущий автомобиль выполняет торможение, и целевое транспортное средство тормозит, чтобы предотвратить столкновение с ним. Схема этого сценария показана на рисунке С.9, где седан является целевым транспортным средством.



1 — пикап; *2* — седан

Рисунок С.9 — Схематический сценарий движения

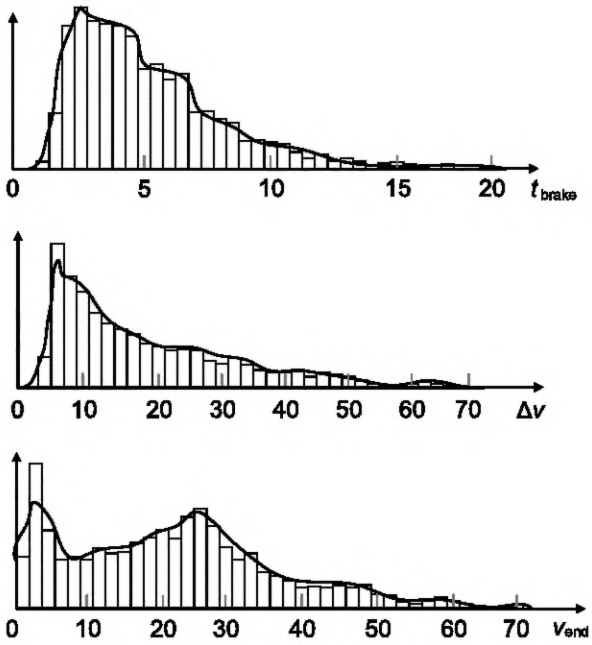
Этот сценарий можно описать тремя параметрами, которые показаны на рисунке С.10:
- v_{end} — скорость после торможения;
- t_{brake} — общее время торможения до заданной скорости v_{end};
- Δv — суммарное снижение скорости ведущего транспортного средства.



X — время, с; Y — скорость, км/ч

Рисунок С.10 — Профиль торможения ведущего транспортного средства в сценарии

Частные распределения вероятностей, которые получены из результата совместного распределения, показаны на рисунке С.11 жирными линиями. В этом случае для оценки основного распределения используется ядерная оценка плотности (KDE), но допускается использовать и другие методы. На гистограммах показаны исходные данные, а жирные линии представляют частные распределения вероятностей параметров, полученные методом KDE.



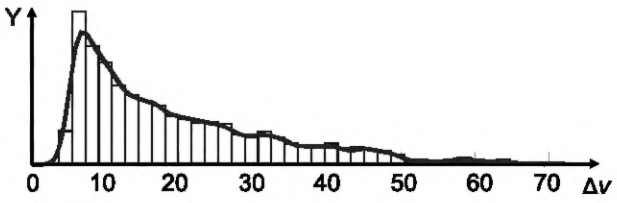
Y — вероятность; t_{brake} — общее время торможения до заданной скорости v_{end}; v_{end} — скорость после торможения; Δv — суммарное снижение скорости ведущего транспортного средства

Рисунок С.11 — Гистограмма для трех параметров сценария тестирования

После получения распределений параметров на основе информации о реальных сценариях можно уточнить процесс, показанный на рисунке С.8 (см. рисунок С.12).

Рисунок С.12 — Сценарное тестирование на основе распределения параметров

При генерации сценариев тестирования с использованием предполагаемого распределения параметров могут возникать многочисленные не представляющие интерес тестовые варианты, поскольку интересующие тесты с более высокой вероятностью попадают в конкретные области распределения. Во избежание расхода вычислительного ресурса на обработку неинтересных тестов можно смещать выбор параметров теста так, чтобы чаще осуществлять выборку из этих областей (этот механизм называется выборкой по значимости [34]). На рисунке С.13 используется усредненный пример из рисунка С.11, где очевидно, что относительно большое снижение скорости ведущего транспортного средства является более рискованным, и выборка смещена в сторону более высоких значений.



a

b

c

Y – вероятность Δ*v*, км/ч; *a* – более легкая выборка;
***b* – более рискованные сценарии; *c* – тяжелая выборка**

Рисунок С.13 — Пример выборки по значимости

Далее можно расширить процесс, который показан на рисунке С.12 (см. рисунок С.14).

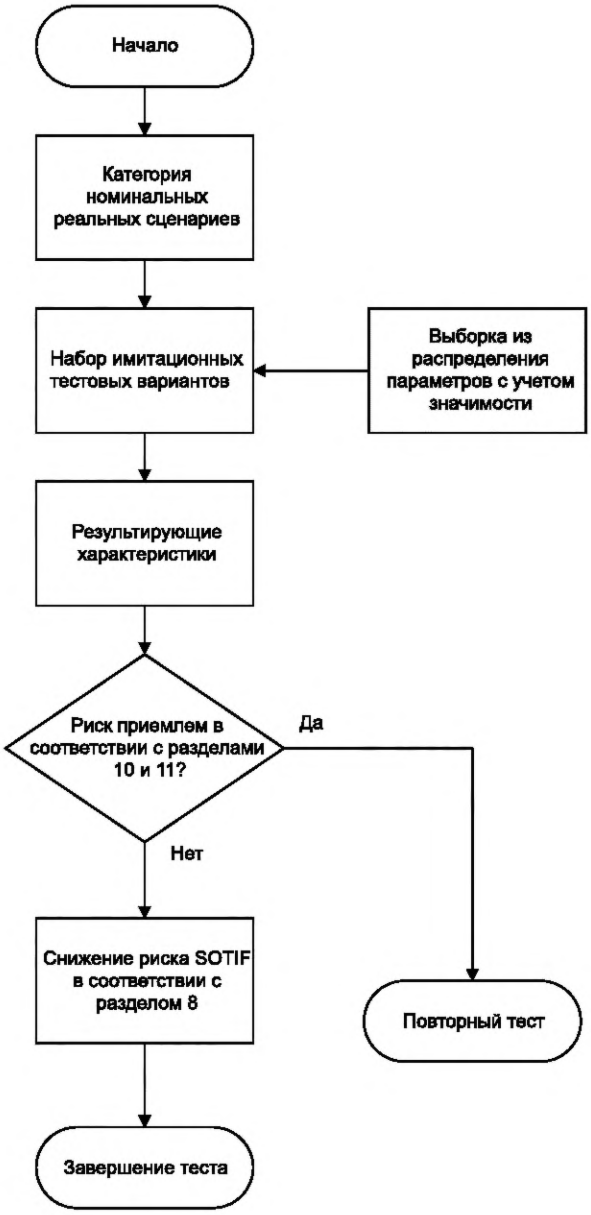


Рисунок С.14 — Тестирование сценариев на основе распределения параметров с выборкой по значимости

Таким образом, тестирование начинается с выбора соответствующей категории сценария для тестируемой функции. В зависимости от типа теста (случайный с ограничениями, выборка по распределению или выборка по значимости) для моделирования создается набор тестовых вариантов. Результат теста оценивается на основе метрики, подходящей для выбранной категории сценария. В зависимости от этапа тестирования и связанного с ним риска для тестируемой функции выбирается соответствующий тип генерации тестовых примеров. Например, для увеличения надежности после метода выборки распределения можно выполнять выборку по значимости. Наконец, риск оценивается по результатам моделирования с учетом критериев приемлемости. Для снижения риска рекомендуется использовать раздел 8. На рисунке С.15 показана блок-схема, которая объединяет все три типа тестирования.

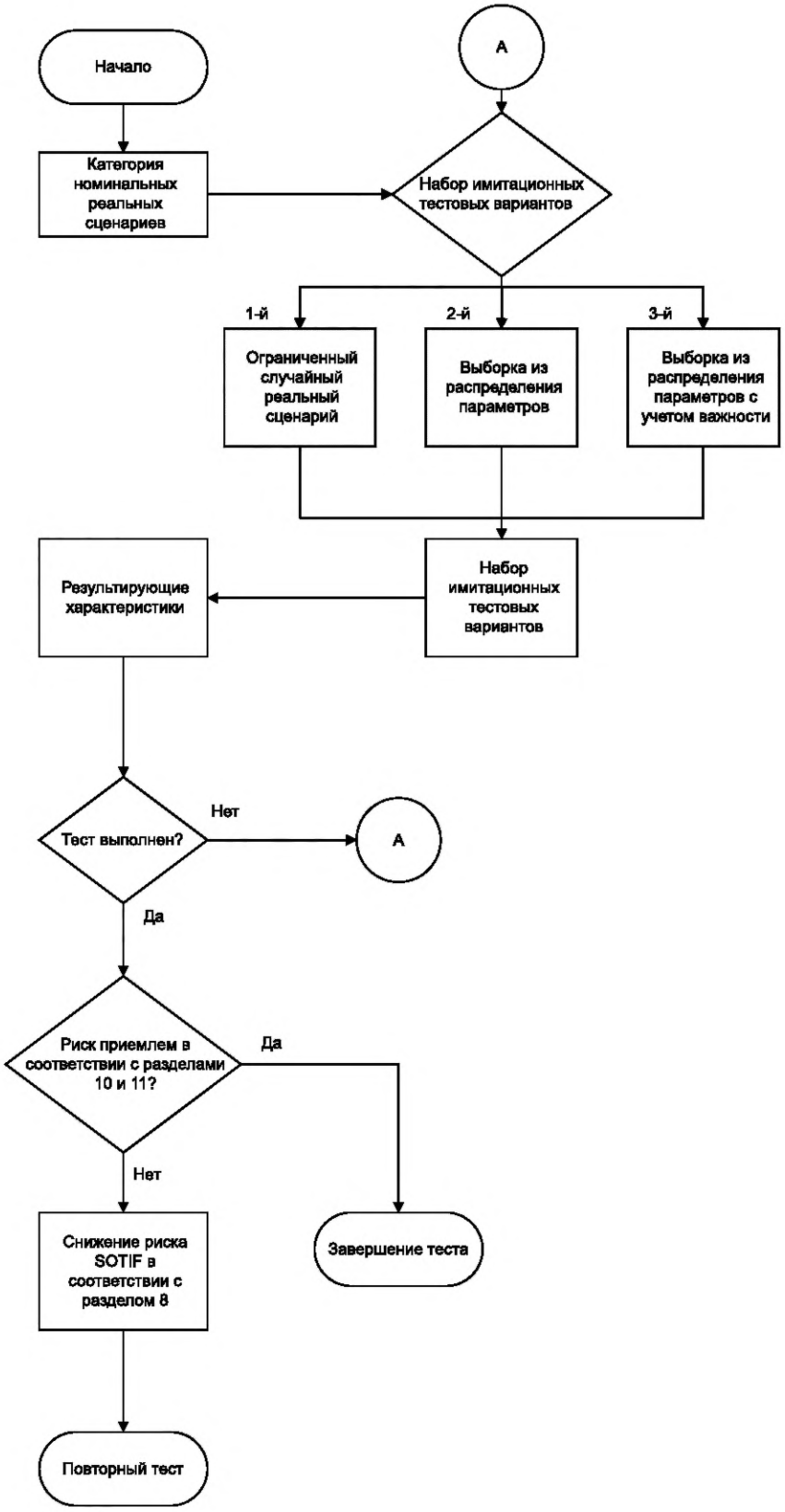


Рисунок С.15 — Пример блок-схемы моделирования на основе сценариев

Валидация систем автоматизации вождения может включать в себя большое количество сценариев моделирования, которые охватывают максимально широкий спектр реальных ситуаций. Для такого моделирования могут требоваться значительные объемы данных о характеристиках дорог и сценариях вождения, а сбор и/или создание этих данных отличаются крайне высокой трудоемкостью. Использование корпоративных и межкорпоративных стандартов хранения и обмена данными таких сценариев может способствовать систематическому и полному исследованию ситуаций.

Для поддержки интеграции различных инструментов или их компонентов также можно использовать стандарты (например, FMI [35]), которые позволяют интегрировать различные элементы моделирования друг с другом.

Примеры стандартов моделирования:

- OpenDRIVE (см. [36]): логическое описание дорожных сетей;
- OpenCRG (см. [37]): описание дорожных покрытий;
- OpenSCENARIO (см. [38]): описание сценариев вождения;
- открытый интерфейс моделирования (OSI) (см. [39]): связь с данными датчиков;
- NDS (см. [40]): картографические данные высокой четкости;
- CityGML (см. [41]): 3D-модели городов;
- FMI (см. [35]): обмен моделями и совместное моделирование динамических моделей.

С.6 Рекомендации по сокращению испытаний в процессе валидации

С.6.1 Оценка охвата тестируемыми сценариями

Надлежащим образом определенный план тестирования (моделирование, реальные тесты или их сочетание) позволяет сокращать объем тестирования, который необходим для демонстрации достижения целей валидации.

Если наборы сценариев, используемых клиентом, можно разделять с помощью одной переменной, которая принимает разные модальности, информация об использовании продукта клиентом позволяет оценивать вероятность каждой модальности.

Если дополнительное обоснование (которое основано, например, на моделировании или экспертной оценке) демонстрирует, что способность системы управлять данным сценарием для конкретной модальности намного выше, чем для других модальностей (например, день или ночь), это обоснование можно использовать для концентрации усилий по валидации на наиболее серьезной модальности и сокращения времени, которое уделяется менее серьезной модальности.

Примечание — Охват, который обеспечивают тестируемые сценарии, зависит от типа количественной цели валидации, которых может быть много. Помимо целей типа $P_{harm} < \epsilon$, где вред рассчитывается на единицу времени или пробега при репрезентативном вождении, а ϵ является небольшим положительным числом, другие типы количественных целей валидации могут включать в себя дополнительные аспекты, такие как справедливость (т. е. представителям определенной демографической группы не причиняется непропорциональный вред). Например, чтобы показать, что автоматизированное транспортное средство не подвергает определенные группы, выделяемые по некоторым характеристикам, значительно более высокому риску причинения вреда, чем другие группы, формируются тестовые примеры, которые предназначены для этих конкретных групп.

С.6.2 Достаточные условия для компонента относительно количественной цели

При работе с модульными проектами может быть полезным формирование достаточных условий на уровне компонента в отношении цели валидации на уровне транспортного средства. Достаточное условие для компонента определяется таким образом, что если оно выполнено, то цель валидации также достигается для выбранного доверительного уровня вероятности причинения вреда с учетом знаний о функционировании остальной части системы (например $P_{harm} < \epsilon$). Можно получать достаточные условия, исходя из (консервативных) предположений о том, что окружающая среда и остальная часть системы ведут себя хуже, а не лучше, чем на самом деле.

Полезные достаточные условия получают из детального анализа ODD (в том числе его вероятностных аспектов) и архитектуры системы с ее отдельными компонентами и их зависимостями. Для подтверждения выполнения достаточных условий на уровне компонентов можно делать статистические обоснования, используя практически управляемые объемы данных при изучении существующих знаний о проблеме и связанных с ней аспектах системы (например, динамике транспортных средств, физике сенсорных технологий). Внимательное рассмотрение достаточных условий на уровне компонентов позволяет не только сокращать затраты на валидацию, но и повторно использовать большую часть результатов анализа безопасности при внесении изменений в ODD или компонент системы. Еще одно преимущество этого подхода заключается в том, что обоснования достижения более сложных количественных целей (например, с учетом соображений справедливости) могут быть более достижимыми на практике благодаря достижению их достаточных условий на уровне компонентов.

С.6.3 Влияние архитектуры системы на валидацию

С.6.3.1 Общие положения

В 11.3 рассматривается выбор подходящей совокупной длины теста для каждого из применяемых методов, которые описаны в таблице 11. С учетом метрики комплексной валидации системы надлежащим образом определенная архитектура системы может приводить к уменьшению требуемой длины теста.

С.6.3.2 Пример: статистическое обоснование безопасности модуля с использованием достаточных условий

Критерий приемлемости часто математически определяется как $P_{harm} < \epsilon$ или E[вред] < ϵ, при этом вред рассчитывается на единицу времени или пробега репрезентативного вождения, а ϵ является небольшим положительным числом. Любое статистически аргументированное обоснование неизбежно содержит неопределенность, которая обусловлена случайной выборкой. Количественная оценка этой неопределенности помогает поддерживать обоснование.

Несмотря на то, что критерий приемлемости формулируется на уровне транспортного средства, желательно, чтобы обоснование безопасности поддерживало модульные проекты. Это означает, что анализ на уровне компонентов и анализ ODD можно объединять в окончательное обоснование безопасности на уровне транспортного средства. Потенциальные преимущества обоснования безопасности модуля заключаются в снижении затрат на валидацию. Отдельный анализ на компонентном уровне и анализ ODD менее затратны и пригоднее для повторного использования по сравнению с выборочными дорожными испытаниями на уровне транспортного средства. По этой причине в настоящем пункте представлен пример обоснования безопасности со следующими желательными характеристиками:

- структурированность, использование модульного анализа на уровне компонентов;
- статистическая строгость с количественной характеристикой неопределенности соблюдения критерия приемлемости.

Этот простой пример в доступной и конкретной форме иллюстрирует основные идеи без учета всего спектра нюансов работы с реальной системой.

Описание системы и ODD:

- автоматизированное транспортное средство предназначено для движения с постоянной скоростью v по прямой дороге, на которой присутствуют только неподвижные объекты. Важные для системы условия внешней среды, такие как освещение, осадки, трение дорожного покрытия и т. д., являются фиксированными;
- транспортное средство оснащено функцией автоматического торможения со следующими характеристиками:
  - комбинированный алгоритм обнаружения объекта и оценки глубины с фиксированной частотой обеспечивает оценку расстояния до ближайшего объекта;
  - если оценка расстояния до ближайшего объекта становится ниже порога c, транспортное средство начинает тормозить до полной остановки; фактический тормозной путь является постоянной величиной $b < c$;
- при трогании с места и после удаления неподвижного объекта по окончании каждого торможения транспортное средство безопасно перезапускается (повторно ускоряется) так, что следующий встречный неподвижный объект приближается со скоростью v с интервалом не менее c. Это позволяет сохранять допущение о постоянной скорости в поставленной задаче во избежание дополнительных математических сложностей;
- датчик и алгоритмы являются фиксированными при тестировании и реальном использовании.

Целью проекта транспортного средства является движение по прямым дорогам без столкновения с какими-либо объектами. Эту систему также можно рассматривать как функцию обнаружения мусора с автоматическим торможением, которая входит в состав более сложной автоматизированной системы вождения.

Критерий приемлемости определяется ожидаемым количеством столкновений на единицу длины пробега.

E (количество столкновений на единицу длины пробега c) < ϵ,

где $\epsilon > 0$ — заранее заданный целевой уровень.

Эта концепция показана на рисунке С.16 с использованием следующих обозначений:

b — общий тормозной путь до полной остановки;

($c - b$) — продольное буферное расстояние между транспортным средством и объектом;

m — количество оценок расстояния, которые система восприятия генерирует с фиксированной частотой при прохождении буферного интервала с расстоянием до объекта между b и c;

l — расстояние, пройденное на скорости v между последовательными итерациями алгоритма восприятия;

L — фактическое расстояние до препятствия;

D — расчетное расстояние до препятствия, полученное с помощью алгоритма восприятия;

D^m — расчетное расстояние до препятствия, определяемое системой восприятия объекта при $b \le L < b + l$, т. е. последняя возможная итерация по обнаружению препятствия и предотвращению столкновения;

V^h — скорость, с которой происходит столкновение с объектом, при этом $V^h = 0$, если транспортное средство своевременно останавливается и не сталкивается с объектом.

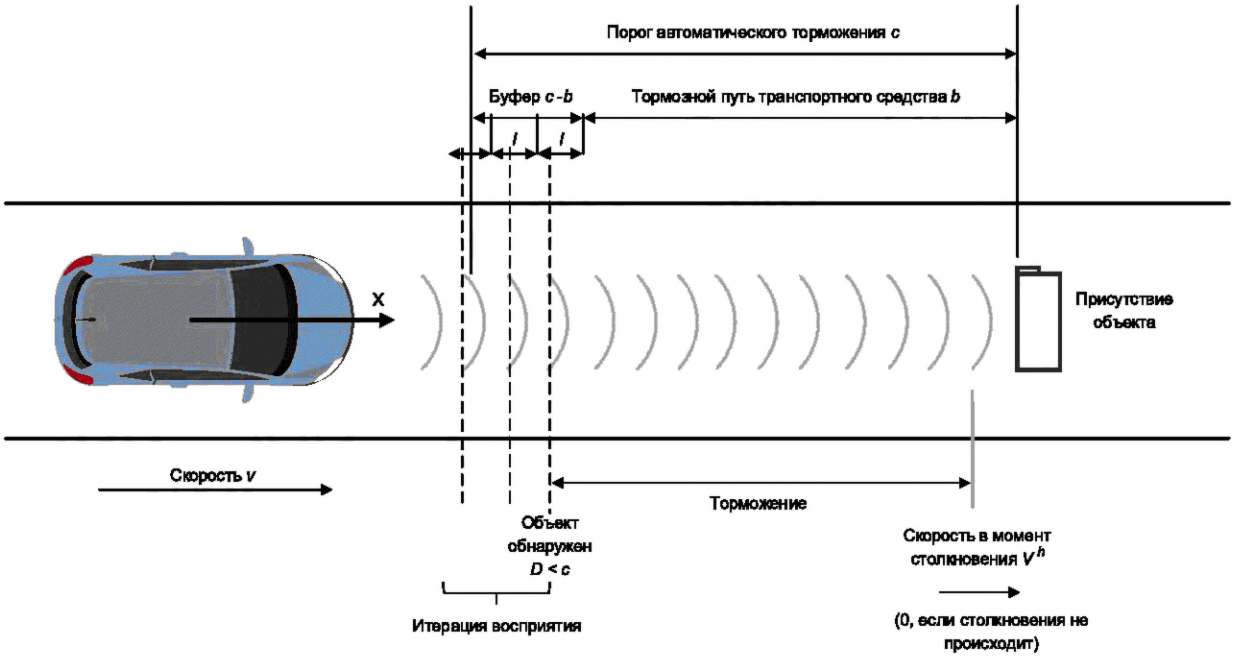


Рисунок С.16 — Пример эксплуатации транспортного средства

В этом примере ожидаемое количество столкновений можно получить путем декомпозиции характеристик компонентов и ODD в виде:

$$E\,[\text{столкновения на единицу расстояния}] = P(V^h > 0)\,E\,[\text{объекты на единицу расстояния}],$$

где $P(V^h > 0)$ — вероятность того, что при наличии случайного препятствия впереди объект не будет обнаружен и торможение начнется после того, как целевое транспортное средство окажется на расстоянии от препятствия, при котором столкновение неизбежно. Все компоненты приведенной выше формулы являются вероятностными величинами распределения объектов при реальном использовании.

При наличии препятствия вероятность столкновения $P(V^h > 0)$ равна вероятности невыполнения торможения до того, как целевое транспортное средство оказывается слишком близко, и вероятности необнаружения (т. е. $D > c$), когда $b \le L < c$.

Следовательно, при рассмотрении единичного столкновения с объектом

$$P(V^h > 0) = P(D > c \text{ для всех } L\,[b, c]) \le P(D^m > c).$$

Таким образом, в этом конкретном примере количественная мера безопасности может быть ограничена сверху как

$$E\,[\text{столкновения на единицу расстояния}] = P(D^m > c)\,E\,[\text{объекты на единицу расстояния}]$$

и поэтому достижение определенной эффективности обнаружения $P(D^m > c) \le \epsilon$ /E [объекты на единицу расстояния] является достаточным условием для соответствия критерию приемлемости.

$P(D^m > c)$ и E [объекты на единицу расстояния] можно оценивать отдельно с помощью доверительных интервалов, которые, в свою очередь, можно использовать для обоснования безопасности на уровне транспортного средства с помощью приведенного выше неравенства, получив утверждение в виде E [столкновения на единицу расстояния] $\le \epsilon$ с уровнем достоверности не менее $1 - \alpha$. Поскольку оценка $P(D^m > c)$ может быть достигнута с помощью сочетания моделирования, структурированных испытаний (например, на полигоне) и случайных эксплуатационных испытаний, а E [столкновения на единицу расстояния] можно оценивать из источников, отличных от дорожных испытаний (например, данных о дорожном движении, обычных данных о вождении, визуализации местности), объем случайных дорожных испытаний на уровне транспортного средства может быть значительно меньше, чем требуется для обоснования валидации посредством реальных случайных дорожных испытаний на уровне транспортного средства.

Пример 1 — Критерием приемлемости является величина менее одного столкновения на 100 000 км вождения в среднем с уровнем достоверности не менее $1 - \alpha$, т. е. E [столкновений на км]

< 1/100 000 с достоверностью не менее 1 − α. Предположим, что по оценкам имеется менее одного стационарного дорожного объекта на 100 км с достоверностью не менее 1 − α_1, т. е. E [столкновений на км] < 1/100 с достоверностью не менее 1 − α_1. Также предположим, что оценочная эффективность обнаружения P(Dm > c) < 1/1000 с достоверностью не менее 1 − α_2, где $\alpha_1 + \alpha_2 = \alpha$. Тогда, используя предложенную выше верхнюю границу, E [столкновений на км] < 1/100 · 1/1000 с достоверностью не менее 1 – ($\alpha_1 + \alpha_2$) = 1 − α. Здесь уровни достоверности объединяются в соответствии с правилами элементарной теории вероятностей[1)].

Соответствующий план экспериментов позволяет оценить $P(D^m > c)$ и E [объекты на единицу расстояния].

Пример 2 — Величину $P(D^m > c)$ можно оценить путем случайной выборки встреченных объектов таким образом, чтобы распределение L в интервале [b, b + l] было равномерным.

Моделирование, достаточные условия и методы статистической оценки можно дополнительно совершенствовать [42].

С.6.3.3 Резервирование и независимость

Если архитектура системы спроектирована так, что:

- определены резервные каналы для реализации заданной подфункции в системе;
- каждый канал может выполнять эту подфункцию самостоятельно в заданных условиях вождения;
- для обеспечения безопасности заданной функциональности достаточно правильного поведения любого из этих каналов.

Можно применять анализ безопасности для расчета вероятности потенциально опасного поведения системы с пониженным уровнем валидации для каждого канала.

Это снижение можно проиллюстрировать на примере двухканальной системы, которая изображена на рисунке С.17.

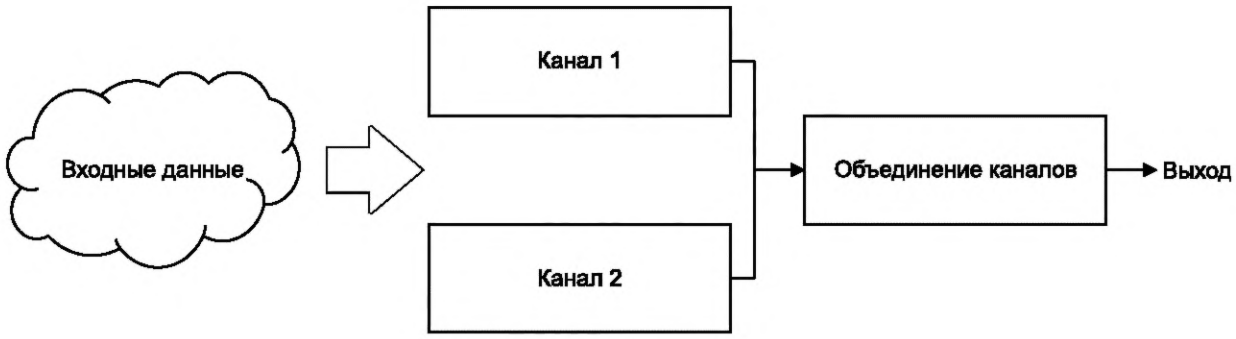


Рисунок С.17 — Архитектура двухканальной системы

Предполагается, что в системе на рисунке С.17 каналы 1 и 2 выполняют одну и ту же функцию и каждый из них может предотвращать потенциально опасное поведение.

Также предполагается, что в элементе объединения каналов отсутствуют функциональные недостаточности и он способен объединять информацию из обоих каналов так, что для предотвращения опасного поведения на выходе достаточно правильной оценки входных данных любым каналом. В этих условиях возможная функциональная недостаточность в любом канале представляет собой множественную функциональную недостаточность.

У каналов 1 и 2 могут существовать общие причины отказа, например идентичные функциональные недостаточности. В этом случае определенное триггерное условие может активировать эту функциональную недостаточность и приводить к опасному поведению.

При этих предположениях можно смоделировать поведение системы, которое приводит к опасному событию, в дереве причин, представленном на рисунке С.18 (руководство по анализу дерева причин см. в В.3.2).

---

1) Если для любых двух событий *A* и *B* имеем $P(A) \geq 1 - \alpha_1$ и $P(B) \geq 1 - \alpha_2$, то
$P(A \cap B) = P(\Omega) - P(\Omega \setminus (A \cdot B)) = 1 - P((\Omega \setminus A) \cdot (\Omega \setminus B)) \geq 1 - (P(\Omega \setminus A) + P(\Omega \setminus B)) \geq 1 - (\alpha_1 + \alpha_2)$.

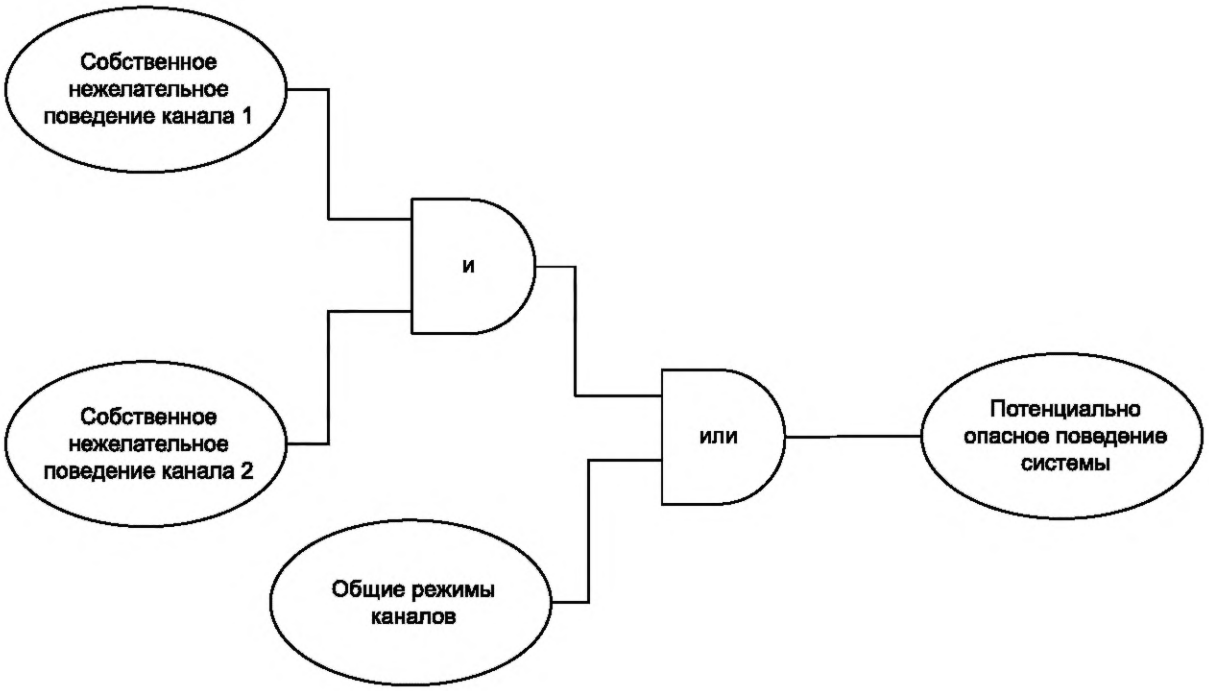


Рисунок С.18 — Моделирование поведения системы

Индивидуальное тестирование каналов 1 и 2 может ускорять тестирование по сравнению с тестированием системы исключительно как «черного ящика». Снижение может существенно зависеть от фактора, представляющего общие причины отказа каналов 1 и 2. Общие причины возникают из-за того, что в каналах 1 и 2 реализуются одни и те же триггерные условия или из-за разных триггерных условий в каналах, где одновременно происходят статистически зависимые инциденты. Этот фактор можно оценивать качественно с учетом разнообразия каналов. Его также можно оценивать с помощью специального моделирования или плана поэтапных испытаний.

В идеальном случае каналы можно считать независимыми (т. е. значение фактора = 0). Независимость можно подтверждать специальными исследованиями, которые качественно расширяют стратегию количественного определения. Методы установления независимости двух элементов:

- аналитические:
  - анализ зависимостей каналов, включающих известные явления;
  - использование различных наборов датчиков в каналах;
  - использование в каналах различных принципов и/или алгоритмов датчиков;
- специальные эксперименты и валидация:
  - тестирование, которое демонстрирует, что система справляется с предполагаемыми общими причинами или зависимостями;
  - систематическое планирование валидации прочности так, чтобы все выявленные или предполагаемые недостатки датчиков, компонентов и каналов были испытаны в достаточной степени;
- специальные методы:
  - методы, которые, как доказано, охватывают ограничение общей причины, полученные на основе теоретической или наблюдаемой зависимости:
  - анализ функциональных недостаточностей, которые наблюдаются в других системах, где используются аналогичные датчики или функции;
  - анализ функциональных недостаточностей одного канала, которые наблюдаются при разработке или мониторинге в ходе эксплуатации, свидетельствующий о том, что эта проблема не нарушает функционирование другого канала.

Приложение D
(справочное)

Руководство по отдельным вопросам обеспечения SOTIF

D.1 Руководство по определению политики вождения

D.1.1 Цель и структура

Целью настоящего раздела является предоставление рекомендаций по разработке политики вождения и нескольких примеров ее реализации.

Политика вождения представляет собой реализацию стратегии обеспечения SOTIF, которая относится к уровню транспортного средства, на уровне принятия решений.

Пример 1 — Требования, которые связаны с переходом из нормального состояния в состояние с ухудшенными характеристиками вследствие выхода из ODD или недостаточностей производительности, входят в область применения стратегии обеспечения SOTIF на уровне транспортного средства (VLSS).

После определения VLSS можно определять политику вождения посредством анализа определенных проблемных областей, которые могут повлиять на ее проект и спецификацию. В этом процессе могут учитываться домен штатной эксплуатации (ODD) и уровень автоматизации вождения (см. [2]) целевого транспортного средства. В настоящем разделе представлены некоторые (неисчерпывающие) примеры формирования VLSS и требований к политике вождения.

VLSS — это комплексная спецификация, которая обеспечивает общую безопасность транспортного средства, оснащенного ADS, и, соответственно, может влиять на проект всех его узлов.

Если VLSS и политика вождения реализованы, они документируются в спецификации и проекте (в соответствии с разделом 5, с учетом разделов 6—8) и верифицируются в соответствии со стратегией верификации и валидации (см. раздел 9). Существует множество способов реализации номинальной политики вождения, которая адаптируется для поддержания SOTIF.

Пример 2 — См. [43] и [44].

Примечание — В политике вождения может учитываться инфраструктура транспортного средства (система восприятия, исполнительные механизмы, ЧМИ) и ее влияние на безопасность дорожного движения с точки зрения взаимодействия с другими субъектами (участниками дорожного движения).

Нарушение политики вождения можно использовать во время разработки для измерения способности транспортного средства с ADS адекватно реагировать на опасные ситуации, создаваемые другими агентами (это измерение описано в концепции мастерства вождения в [45]).

D.1.2 Разработка политики вождения

D.1.2.1 Обзор примера разработки политики вождения

На рисунке D.1 показан пример упрощенной архитектуры, которая основана на модели Восприятие—План—Выполнение (4.2.3) для автоматизированного транспортного средства:

Рисунок D.1 — Пример упрощенной архитектуры транспортного средства, оборудованного ADS, с политикой вождения

В этом примере архитектуры политика вождения разработана как часть подсистемы планирования, которая отвечает за анализ информации, предоставляемой подсистемой считывания (или восприятия). Эта подсистема может включать в себя несколько подэлементов, цель которых состоит в том, чтобы сначала воссоздавать внешнюю среду вокруг транспортного средства, оснащенного ADS, с требуемым уровнем точности, а затем принимать решение о следующем действии системы в соответствии с политикой вождения. Один из подходов — разработать подходящую реакцию.

Примечание 1 — Подходящая реакция определяется как набор корректирующих действий, выполнение которых может требовать политика вождения для поддержания SOTIF, когда другие участники дорожного движения ведут себя обоснованно предсказуемым образом. Подходящая реакция имеет два основных свойства:

- может оцениваться для транспортного средства, управляемого ADS, относительно любого другого участника сценария дорожного движения;
- ее безопасность статистически доказана при любых условиях эксплуатации, которые не требуют перехода в состояние минимального риска.

Пример 1 — Корректирующими действиями, которые реализуются подходящей реакцией, могут являться команды ускорения, замедления или рулевого управления в зависимости от сценария дорожного движения.

Реализация политики вождения также может использовать внешние системы.

Пример 2 — Зависимость от обновления карт при изменении дорожной инфраструктуры является примером допущения о внешних системах, которое может влиять на проект политики вождения.

В соответствии с политикой вождения управляющие действия системы управления транспортным средством, оснащенного ADS, должны обеспечивать безопасность его вождения в условиях взаимодействия с другими участниками дорожного движения с учетом местных правил дорожного движения и обычаев. Можно реализовывать политику вождения в виде монитора или непосредственно включать ее в реализацию решения. В ходе разработки политики вождения можно рассматривать следующие основные категории мер:

- упреждающие: меры, которые могут являться специфичными для конкретного варианта использования и проверяются на этапах верификации и валидации (например, на полигоне или дороге общего пользования). Эти меры могут включать в себя проверки несоблюдения правил, мастерства вождения и вывода из зацепления путем имитационного моделирования и тестирования на полигонах и дорогах общего пользования (см. [45]);
- реактивные: меры, которые формируются на основе статистических данных, подтверждающих оправданность риска после выпуска SOTIF. Эффективность этих мер можно отслеживать в ходе эксплуатации системы. См. раздел 13 о действиях на этапе эксплуатации.

Пример 3 — Упреждающие меры могут включать в себя допущения о внешних системах, таких как карты, локализация и системы связи транспортных средств с инфраструктурой, друг с другом и другими участниками дорожного движения.

Согласно определению, которое указано в D.1.1, основным предназначением политики вождения является мониторинг системы автоматизации вождения для минимизации риска опасного поведения с точки зрения воздействия на безопасность дорожного движения. С учетом этого определения можно формировать политику вождения согласно ряду основных принципов:

- измеримость;
- отражение динамики транспортного средства и физических принципов, которые лежат в его основе;
- пригодность для использования современных технологий;
- соответствие правилам дорожного движения;
- разделение инициатора опасного сценария и ответчика (отказ от наказания за уклонение);
- поощрение предсказуемости и способности к прогнозированию.

Для эффективного обеспечения SOTIF политика вождения также может предусматривать прогнозирование и смягчение функциональных недостаточностей подсистемы восприятия, исполнительных механизмов или ЧМИ пассажиров транспортного средства:

- восприятие ODD: использование транспортного средства с ADS вне определенной ODD может повышать риск опасного поведения. Политика вождения может гарантировать, что автоматизированная функция не выполняется вне ODD, используя информацию, которая поступает от системы восприятия (в том числе набора датчиков и внешней инфраструктуры — например, карт). Использование системы восприятия с этой целью приводит к возникновению дополнительных требований, связанных с SOTIF, — система восприятия не должна создавать риск из-за ложноположительных ошибок (которые указывают на то, что ODD выполняется, когда на самом деле это не так), поскольку они могут приводить к причинению вреда, когда транспортное средство под управлением ADS эксплуатируется вне ODD;
- активация и деактивация транспортного средства, оборудованного ADS, может сбивать с толку пассажиров и водителя автомобиля при наличии систем, которые допускают как автоматическое, так и ручное управление. В

этом случае в политике вождения может быть предусмотрено использование ЧМИ при включении и выключении транспортного средства, управляемого ADS;

- ограничения системы восприятия: в системе восприятия транспортного средства, оборудованного ADS, могут возникать недостаточности производительности при неблагоприятных погодных условиях или в определенных случаях использования. При разработке политики вождения в нее можно включать меры противодействия таким недостаточностям и ограничениям (например, ограничение полномочий системы управления в отношении исполнительных механизмов или безопасной остановки транспортного средства).

Можно поддерживать разработку стратегии SOTIF на уровне транспортного средства и политики вождения с помощью анализа проблемных областей. Эти области можно классифицировать по типу взаимодействия со средой эксплуатации, пассажирами, участниками дорожного движения, а также бортовыми и внешними системами:

- проблемные области, которые связаны со средой эксплуатации транспортного средства, оборудованного ADS. Эти категории могут рассматриваться в данном примере проекта политики вождения с помощью следующих упреждающих мер:
  - ODD;
  - правила дорожного движения и обычаи в данной ODD;
  - дорожная инфраструктура (например, светофоры, схема дороги и тип перекрестка);
- проблемные области, которые возникают в результате взаимодействия системы автоматизации вождения с водителем или пассажирами транспортного средства, оборудованного ADS. В данном примере политики вождения могут быть предусмотрены следующие упреждающие и реактивные меры:
  - переключение режимов вождения и допущения о поведении подсистемы транспортного средства, оборудованной ADS, вне области действия политики вождения (например, ЧМИ);
  - переход в режимы работы с ухудшенными характеристиками и поддержание этих режимов;
- проблемные области, которые возникают в результате взаимодействия транспортного средства, управляемого ADS, с другими участниками сценария дорожного движения, бортовыми и внешними системами. Эти категории могут учитываться в данном примере проектирования политики вождения в виде следующих реактивных мер:
  - набор правил, необходимых для безопасной навигации среди участников дорожного движения;
  - взаимодействие, предотвращение или прогнозирование ограничений или недостаточности транспортных средств, управляемых ADS (например, выявленное ограничение пробега без дозаправки или отсутствие достаточного охвата датчиков системы восприятия).

В следующих пунктах приводятся примеры использования анализа проблемных областей для обеспечения полноты проектирования VLSS и политики вождения. В таблицах D.1—D.6 анализируются различные проблемные области системы автоматизации вождения для определения требований VLSS и политики вождения, а также описывается ожидаемое поведение транспортного средства с ADS при отклонении от таких требований.

Примечание 2 — Таблицы D.1—D.6 содержат примеры спецификации и разработки политики вождения. В настоящем контексте используются утверждения «должен»; в указанных таблицах такие утверждения являются лишь примерами требований и не требуются для соблюдения настоящего стандарта.

D.1.2.2 Проблемные области, связанные с условиями эксплуатации транспортных средств, управляемых ADS

Можно проектировать, разрабатывать политику вождения и проверять возможность ее использования только в заданной ODD, которая ограничена рядом факторов. Эксплуатация за пределами ODD может увеличивать риск опасного поведения.

ODD может основываться на разных аспектах:

- географические ограничения: транспортное средство с ADS может действовать без контроля только на определенной и ограниченной территории (город, страна и т. п.);
- ограничение типа дороги: транспортное средство с ADS может двигаться без контроля только по определенному типу дорог (только автомагистрали, только городские дороги и т. п.) или их комбинации;
- погодные условия: транспортное средство с ADS не допускается к эксплуатации в определенных погодных условиях (сильный дождь, снег и т. д.);
- скорость транспортного средства: транспортному средству с ADS не разрешается двигаться со скоростью выше определенного порога.

Таблица D.1 — Проблемы, вытекающие из анализа ODD

Цель	Учет рисков, связанный с работой функций вне ODD (включая возможное непонимание или незнание водителем ODD)	
VLSS	Транспортное средство, оборудованное ADS, должно обеспечить отключение режима автоматического вождения за пределами ODD	
Проблема транспортного средства, управляемого ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска

Окончание таблицы D.1

Транспортное средство, управляемое ADS, эксплуатируется за пределами обозначенной географической зоны	Опасное событие (например, столкновение любого типа) из-за движения транспортного средства с ADS в зоне, где его поведение не проверено	R: политика вождения должна следить за тем, чтобы транспортное средство, управляемое ADS, двигалось в назначенной зоне
		R: политика вождения должна следить за тем, чтобы транспортное средство, управляемое ADS, переходило в состояние минимального риска, если оно работает за пределами обозначенной зоны
		A: политика вождения получает обновленную информацию о местоположении от внешней независимой подсистемы (например, локализации)
Транспортное средство с системой ADS превышает максимальную расчетную скорость	Опасное событие (например, столкновение любого типа) из-за того, что транспортное средство, управляемое ADS, подвергается возможным ограничениям (при восприятии или срабатывании)	R: политика вождения должна следить за тем, чтобы транспортное средство с ADS двигалось со скоростью ниже максимальной расчетной
Ожидаемое поведение автомобиля под управлением ADS	Политика вождения должна: - следить, находится ли транспортное средство, оборудованное ADS, внутри или за пределами ODD; - если транспортное средство, оборудованное ADS, находится за пределами ODD, реализовывать одну из следующих стратегий: - запрещать включение автоматизации вождения (если автоматика вождения еще не включена); - требовать от водителя взять управление на себя (если это предусмотрено функцией автоматизации вождения); - отключать автоматику вождения и переходить в безопасное состояние (если водитель не входит в состав контура управления)	

Таблица D.2 — Проблемы, вытекающие из предположений о поведении других участников дорожного движения

Цель	Обеспечить применение методов безопасного вождения транспортным средством с системой ADS для предотвращения потенциальных столкновений	
VLSS	Автомобиль с ADS соответствует применимым правилам вождения, законам и обычаям, за исключением случаев, когда нарушение одного или нескольких правил является единственным способом избежать аварии	
Проблема транспортного средства, управляемого ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска
Другие участники дорожного движения (кроме транспортного средства с ADS), не соблюдающие правила светофора	Опасное событие (например, столкновение любого типа) из-за того, что транспортное средство, управляемое ADS, заняло перекресток, не имея права проезда	R: политика вождения должна определять, основываясь на допущениях о поведении других участников дорожного движения, имеет ли другой участник дорожного движения возможность остановиться
Транспортное средство с системой ADS игнорирует право проезда других участников дорожного движения	Опасное событие (например, столкновение любого типа) из-за того, что транспортное средство, управляемое ADS, подвергается возможным ограничениям (при восприятии или срабатывании)	R: политика вождения должна использовать заданные допущения о разумном поведении других агентов в наихудшем случае для учета ограничений восприятия или окклюзии
Ожидаемое поведение автомобиля под управлением ADS	Политика вождения должна: - применять приемы контраварийного вождения; - соответствовать местным правилам и обычаям; - нарушать местные правила и обычаи, только если это необходимо для предотвращения несчастного случая	

Пример — В [43] и [44] установлена необходимость внедрения контраварийных методов вождения согласно принципу «дорогу уступают, а не захватывают».

Примечание — Спецификация политики вождения может отличаться (или требовать другой конфигурации) в зависимости от целевого рынка транспортных средств, управляемых ADS (географический дискриминатор), и местного поведения (например, в Европе и США предусмотрены различные правила проезда четырехсторонних перекрестков равнозначных дорог).

Таблица D.3 — Проблемы, обусловленные дорожной инфраструктурой

Цель	Гарантировать, что транспортное средство, которое управляется ADS, может эксплуатироваться без нарушения SOTIF при любых дорожных условиях, заданных в ODD	
VLSS	Транспортное средство, которое управляется ADS, должно гарантировать, что средства автоматизации вождения неактивны за пределами ODD	
Проблема, связанная с транспортным средством, которое управляется ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска
Транспортное средство, которое управляется ADS, не распознает суженные полосы в местах проведения дорожных работ	Опасное событие (например, столкновение по касательной), связанное с тем, что транспортное средство, которое управляется ADS, сбивается с полосы и перемещается на соседнюю полосу	R: политика вождения должна учитывать дорожную инфраструктуру и наблюдать за поведением транспортного средства, которое управляется ADS
Ожидаемое поведение транспортного средства, которое управляется ADS	В политике вождения должны быть реализованы методы контраварийного вождения или мониторинг перехода транспортного средства, которое управляется ADS, в режим работы с ухудшенными характеристиками	

D.1.2.3 Проблемные области, которые вытекают из перехода транспортного средства, управляемого ADS, в режим работы с ухудшенными характеристиками

В политике вождения могут быть предусмотрены несколько режимов работы с ухудшенными характеристиками, соответствующих состоянию транспортного средства, управляемого ADS. Взаимодействие между пользователями и транспортным средством, которое управляется ADS, может влиять на мониторинг выполнения задачи навигации политики вождения.

Таблица D.4 — Проблемы, вытекающие из необходимости прогнозирования, предотвращения и смягчения нарушений в транспортном средстве, которое управляется ADS

Цель	Прогнозирование, предотвращение или смягчение выявленных ограничений инфраструктуры системы автоматизации вождения (пример — подсистемы восприятия или силового привода)	
VLSS	Транспортное средство, которое управляется ADS, должно гарантировать, что средства автоматизации вождения неактивны за пределами ODD.	
Проблема, связанная с транспортным средством, которое управляется ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска
Характеристики транспортного средства, управляемого ADS, ухудшаются при неблагоприятных погодных условиях	Опасное событие (например, столкновение любого типа), обусловленное тем, что транспортное средство, управляемое ADS, не способно реагировать на ухудшение характеристик подсистемы восприятия и силового привода при неблагоприятных погодных условиях)	R: политика вождения должна следить за тем, что характеристики транспортного средства, управляемого ADS, корректируются в соответствии с погодными условиями. A: политика вождения должна получать информацию о текущих погодных условиях от внешних по отношению к ней подсистем

Окончание таблицы D.4

Характеристики транспортного средства, управляемого ADS, ухудшаются на конкретных типах дорог или при конкретных условиях	Опасное событие (например, столкновение любого типа), обусловленное тем, что транспортное средство, управляемое ADS, не способно реагировать на ухудшение характеристик подсистемы силового привода на конкретных типах дорог (например, низкое сцепление с гравийными дорогами)	R: политика вождения должна следить за адаптацией характеристик транспортного средства, управляемого ADS, к типу дороги. A: политика вождения должна получать информацию о текущем типе дороги от внешних по отношению к ней датчиков
Транспортное средство, которое управляется ADS, слишком быстро достигает закрытых областей (закрытой называется область, в которой подсистема восприятия не способна надежно выполнять свои функции из-за того, что ее поле зрения перекрыто зданиями или другими объектами инфраструктуры)	Опасное событие (например, столкновение любого типа), обусловленное тем, что транспортное средство, управляемое ADS, не способно своевременно воспринимать других агентов при достижении закрытых областей	R: политика вождения должна следить за тем, чтобы транспортное средство, управляемое ADS, снижало скорость (показывать предупреждение) при наличии преград, обусловленных инфраструктурой или конструкцией дороги. A: политика вождения должна получать информацию о преградах в поле зрения системы восприятия от внешних по отношению к ней подсистем
Ожидаемое поведение транспортного средства, которое управляется ADS	Политика вождения должна наблюдать за состоянием инфраструктуры транспортного средства, управляемого ADS: - адаптировать поведение транспортного средства при приближении к закрытым областям; - адаптировать поведение транспортного средства при сложных погодных условиях, которые могут затруднять навигацию транспортного средства; - адаптировать поведение транспортного средства при ухудшении характеристик подсистемы силового привода, которое может затруднять навигацию транспортного средства; - адаптировать поведение транспортного средства при движении по поверхности с низким сцеплением	

Пример — В [43] и [44] показана необходимость соблюдения осторожности, когда поле зрения системы восприятия перекрывается объектами инфраструктуры, конструктивными элементами дороги и/или движущимися объектами (например, транспортными средствами, пешеходами, велосипедистами). Осторожность может выражаться в замедлении транспортного средства, управляемого ADS, при приближении к пересечению дорог, на котором здания или конструкция дороги ухудшают способность системы восприятия обнаруживать других агентов.

Таблица D.5 — Проблемы, возникающие вследствие необходимости управления переходами между режимами работы

Цель	Прогнозирование, предотвращение или смягчение известных ограничений инфраструктуры системы автоматизации вождения (пример — подсистемы восприятия или силового привода)	
VLSS	Транспортное средство, которое управляется ADS, должно гарантировать, что средства автоматизации вождения неактивны за пределами ODD	
Проблема, связанная с транспортным средством, которое управляется ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска

Окончание таблицы D.5

Транспортное средство, которое управляется ADS, переходит в режим работы с ухудшенными характеристиками, используя противоречивую информацию (относится к уровням автоматизации вождения, на которых водитель может входить в состав контура управления при определенных условиях)	Транспортное средство, которое управляется ADS, может создавать опасное событие (например, столкновение любого типа) вследствие неспособности водителя вернуть управление транспортным средством	R: политика вождения должна следить за процессом передачи управления транспортным средством, которое управляется ADS, водителю. A: политика вождения гарантирует, что транспортное средство, которое управляется ADS, переходит в безопасное состояние, если водитель не принимает управление до окончания ODD
Транспортное средство, которое управляется ADS, не учитывает ограничения водителей-людей при необходимости передавать им управление (например, при приближении к границам ODD)	Транспортное средство, которое управляется ADS, может создавать опасное событие (например, столкновение любого типа) вследствие нехватки у водителя времени на возврат управления транспортным средством	R: политика вождения должна достаточно информировать водителя о необходимости принять управление транспортным средством. A: политика вождения гарантирует, что транспортное средство, которое управляется ADS, переходит в безопасное состояние, если водитель не принимает управление до окончания ODD
Ожидаемое поведение транспортного средства, которое управляется ADS	Политика вождения должна информировать водителя о том, что ему необходимо вернуть управление транспортным средством. При отказе водителя принять управление транспортным средством политика вождения должна: - следить за переходом транспортного средства, которое управляется ADS, в безопасное состояние; - блокировать работу системы автоматизации вождения	

Примечание — Это множество проблем относится к уровням автоматизации вождения, на которых водитель входит в состав контура управления при определенных условиях.

D.1.2.4 Проблемные области, обусловленные взаимодействием транспортного средства, управляемого ADS, с другими участниками дорожного движения

Существует множество методов мониторинга и корректировки поведения транспортного средства, управляемого ADS, с учетом других агентов. В RAND (см. [45]) представлена классификация этих методов, при этом отмечено, что мониторинг «защитной оболочки», охватывающей транспортное средство, управляемое ADS, является самым эффективным методом для высоких уровней автоматизации вождения. Остальные методы рекомендуется применять на других уровнях.

«Защитная оболочка» — общая концепция, с помощью которой можно формулировать все принципы, определяющие политику вождения. В соответствии с этой концепцией транспортное устройство, управляемое ADS, может иметь одну или несколько границ вокруг целевого транспортного средства. В некоторых сценариях нарушение одной или нескольких из этих границ вызывает различные реакции транспортного средства, управляемого ADS. Например, политика вождения адаптируется к этим сценариям и поддерживает SOTIF, реализуя надлежащий отклик.

Поскольку надлежащий отклик по своему характеру относится к уровню транспортного средства, D.1.2.4 основан на следующих допущениях:

- транспортное средство, управляемое ADS, не может контролировать поведение каких-либо других участников сценария дорожного движения. Следовательно, надлежащий отклик транспортного средства, управляемого ADS, можно определять так, что транспортное средство, управляемое ADS, не инициирует ДТП, создавая опасный сценарий;
- SOTIF транспортного средства, управляемого ADS, достигается только по отношению к другим участникам сценария дорожного движения (агентам), как указано на рисунке D.2. Следовательно, надлежащий отклик транспортного средства, управляемого ADS, можно определять относительно любого пользователя дороги, который участвует в сценарии дорожного движения. Таким образом, каждый из указанных аспектов накладывает ограничения на динамическое поведение транспортного средства, управляемого ADS (продольное и поперечное ускорение, скатывание и свес).

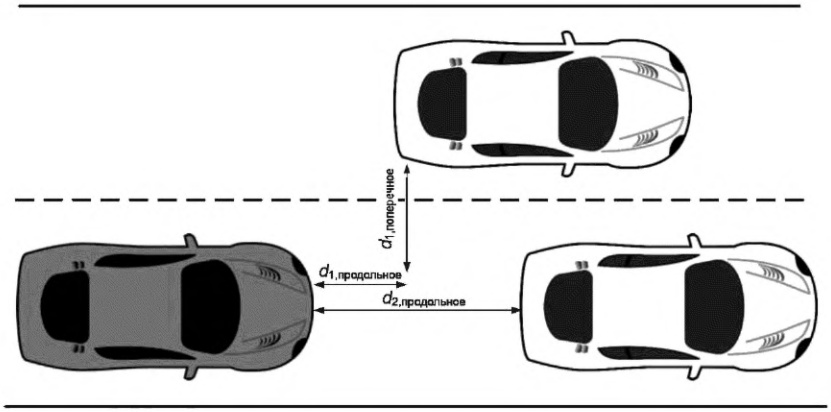


Рисунок D.2 — Определение положения относительно других агентов

Таблица D.6 — Проблемы, вытекающие из множества обязательных правил безопасной навигации

Цель	Обеспечить способность устройства, управляемого ADS, безаварийно функционировать в пределах ожидаемой ODD с учетом: - риска, создаваемого другими пользователями дороги; - риска, возникающего при маневрах транспортного средства, управляемого ADS, обладающих достаточным уровнем управляемости для других пользователей дороги; - риска, создаваемого другими агентами, поведение которых не соответствует обоснованно предсказуемым допущениям; - риска, создаваемого характеристиками исполнительного механизма целевого транспортного средства.	
VLSS	1) Поведение транспортного средства, управляемого ADS, должно быть максимально предсказуемым для окружающих пользователей дороги (например, оно может выражаться в отсутствии необоснованных перестроений между полосами и понятными действиями при приближении к смыканию полос). 2) Транспортное средство, управляемое ADS, должно соблюдать следующие правила управления рисками: - не должно являться причиной ДТП; - быть максимально устойчивым к рискам, которые создают другие участники дорожного движения; - соблюдать осторожность в условиях ограниченной видимости; - соблюдать осторожность в присутствии неизвестных объектов и при неожиданном поведении других участников дорожного движения; - учитывать поведение других транспортных средств (соблюдать безопасное расстояние до впереди идущего автомобиля, избегать неосмотрительного вклинивания между автомобилями); - соблюдать применимые правила и законы вождения при отсутствии крайней необходимости избежания ДТП. Необходимо соблюдать эти правила при вождении: - в любом месте (например, в сельской местности и на дороге); - в любой момент времени (например, при динамическом назначении полос, изменчивых во времени правилах, введении новых типов дорожных знаков и правил движения)	
Проблема, связанная с транспортным средством, которое управляется ADS	Возможные последствия	Функциональное требование политики вождения (R) или предположение (A) для снижения риска

Окончание таблицы D.6

Транспортное средство, управляемое ADS, движется слишком близко к впереди идущему транспортному средству или слишком агрессивно	Транспортное средство, управляемое ADS, создает опасное событие (например, столкновение сзади) вследствие несоблюдения дистанции до впереди идущего транспортного средства	R: политика вождения должна следить за тем, чтобы транспортное средство, управляемое ADS, всегда соблюдало минимальное расстояние до впереди идущего транспортного средства во избежание столкновения
Транспортное средство, управляемое ADS, меняет полосу без учета других транспортных средств	Транспортное средство, управляемое ADS, создает опасное событие (например, столкновение по касательной) вследствие несоблюдения поперечного расстояния до других агентов	R: политика вождения должна следить за тем, чтобы транспортное средство, управляемое ADS, всегда соблюдало минимальное расстояние до каждого агента во избежание столкновения
Транспортное средство, управляемое ADS, движется по заснеженной дороге со слишком большой скоростью без учета характеристик привода на скользкой поверхности	Транспортное средство, управляемое ADS, создает опасное событие (например, столкновение с предметом/пешеходом) вследствие несоблюдения скоростного режима и нарушения правил безопасного вождения	R: политика вождения должна следить за тем, чтобы команды на привод транспортного средства, управляемого ADS, соответствовали условиям внешней среды
Ожидаемое поведение транспортного средства, управляемого ADS	Политика вождения должна следить за поведением транспортного средства, управляемого ADS, и корректировать его в соответствии с поведением других агентов	

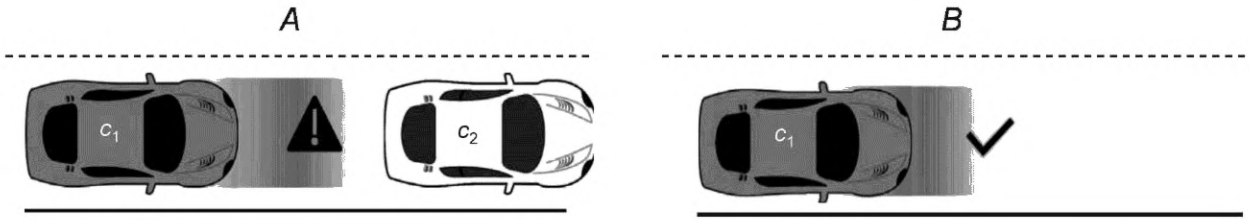


Рисунок D.3 — Пример опасного сценария до и после реализации надлежащего отклика

Пример — В [43] и [44] рассматривается ситуация при вождении, которая представлена на рисунке D.3. Целевое транспортное средство c_1 следует за транспортным средством c_2 с положительной скоростью сближения (c_1 движется быстрее c_2). Этот сценарий считается опасным для автомобилей c_1 и c_2 в момент времени t_d, если в момент времени t_d расстояние между ними не позволяет избежать столкновения в течение заданного времени реагирования. Автомобиль c_1 несет ответственность за столкновение сзади.

Для автомобиля c_1 разрабатывается политика вождения, которая исключает риск его столкновения с автомобилем c_2 сзади благодаря тому, что в любой момент времени t_d продольное расстояние между c_1 и c_2 превышает тормозной путь автомобиля c_1. Для этого транспортное средство, управляемое ADS, регулирует расстояние между c_1 и c_2 с помощью педали тормоза и акселератора так, чтобы оно составляло не менее d_{min}.

Примечание — Статистика дорожного движения может рассматриваться в качестве подходящего метода определения наиболее распространенных и серьезных вариантов столкновений между транспортным средством, управляемым ADS, и другими участниками дорожного движения в соответствии с целевым уровнем автоматизации вождения, ODD и рынком. Эти варианты могут представлять наиболее серьезные опасные ситуации, возникающие в процессе эксплуатации транспортного средства, управляемого ADS, и использоваться для составления правил, с помощью которых политика вождения наблюдает за его поведением.

D.1.3 Верификация и валидация стратегии SOTIF на уровне транспортного средства и политики вождения

Политики вождения разрабатываются в контексте целевой ODD для реализации логики принятия решений VLSS (см. D.1.2). Тем не менее, политика вождения, которая неадекватно отражает реальные ситуации, может являться потенциальным источником функциональных недостаточностей. С помощью действий по верификации и

валидации (см. разделы 9—11) можно выявлять недостатки политики вождения путем составления сценариев, комбинирования связанных между собой параметров и др., а затем устранять обнаруженные недостатки с помощью итеративного процесса обеспечения SOTIF (см. рисунок 10), в том числе дальнейшего анализа (см. разделы 6 и 7) и изменения политик вождения (см. раздел 8).

Политику вождения также можно использовать в качестве обоснования при определении критериев выбранных методов верификации и валидации в соответствии с разделом 9, задавая показатели эффективности автоматизированной системы вождения.

Пример — Характеристики транспортного средства, управляемого ADS, можно измерять посредством мониторинга нарушений политики вождения. Например:

- количество сбоев мониторинга поведения транспортного средства, управляемого ADS, политикой вождения;

- количество критических условий, не выявленных политикой вождения;

- количество происшествий, возникших из-за транспортного средства, управляемого ADS.

D.1.4 Политика вождения в процессе эксплуатации

В процессе эксплуатации может требоваться оценка эффективности политики вождения. Для этого можно сравнивать статистику эксплуатации системы (см. 13.3) и наблюдаемой эффективности политики вождения.

D.2 Аспекты применения машинного обучения

D.2.1 Общие положения

В сфере автоматизации транспортных средств часто применяются технологии машинного обучения, особенно для обнаружения и классификации объектов. Как правило, алгоритмы машинного обучения применяются в ситуациях, когда невозможно полностью описать решаемую проблему (например, не существует данных, которые определяют все возможные разновидности пешеходов для их обнаружения с помощью алгоритма на основе правил). Алгоритмы машинного обучения позволяют преодолевать эти ограничения; они связывают входы и выходы путем обнаружения корреляций между данными. В отличие от людей алгоритмы машинного обучения не способны учитывать семантический контекст. Несмотря на то, что они, как правило, эффективнее необучаемых алгоритмов, изучение процессов формирования прогнозов является более сложным; многие ограничения машинного обучения алогичны и, следовательно, не могут быть описаны в спецификации.

В целях минимизации остаточного риска, обусловленного неверным прогнозированием, можно определять и применять методы преодоления ограничений компонента машинного обучения (например, распознавание объектов с точностью ниже 100 %, незапланированная необъективность), которые могут являться причиной его недостаточной эффективности. При подготовке машинного обучения, в том числе используемых данных, могут возникать проблемы безопасности, которые приводят к недостаточностям производительности. Например, данные обучения и верификации могут содержать распределения и корреляции, которые обусловлены их необъективностью. Они могут не иметь отношения к целевым функциям системы и даже быть некорректными по отношению к ним. Поскольку надежность и точность компонентов машинного обучения критически важны для безопасной эксплуатации транспортного средства, в целях преодоления ограничений этих компонентов разрабатываются системы обучения и процессы сбора данных для них.

D.2.2 Различия между подходами к машинному обучению в стандартах серии ИСО 26262 и SOTIF

В D.2.2 сравниваются аспекты безопасности машинного обучения, предусмотренные в стандартах серии ИСО 26262 и SOTIF.

1) Инструменты автономной подготовки регламентируются ИСО 26262-8:2018 (раздел 11), а процесс автономной подготовки — D.2.4.

Примечание 1 — Программные и аппаратные компоненты инструмента (например, автономные серверные парки и обучающее программное обеспечение) оцениваются в ходе его квалификации.

2) Аспекты, которые относятся к аппаратным компонентам (например, ЦП), используемым для реализации алгоритмов машинного обучения в транспортном средстве:

a) случайные и систематические сбои аппаратных компонентов рассматриваются в ИСО 26262-5;

b) ограничения характеристик аппаратных компонентов могут одновременно являться проблемами SOTIF и системными проблемами в стандартах серии ИСО 26262.

3) Аспекты, которые относятся к программному обеспечению, используемому для реализации алгоритма машинного обучения:

a) программное обеспечение машинного обучения преобразует входные данные в выходные посредством заданных вычислительных операций (например, умножение матриц, дискретная свертка, нелинейные функции). В этом отношении машинное обучение не отличается от других необучаемых алгоритмов и может верифицироваться традиционными методами. Верификацию реализации вычислительных операций можно осуществлять в соответствии с ИСО 26262-6.

Пример — Библиотеки операций над вещественными числами и различия между этими библиотеками в обучающей инфраструктуре и встраиваемой целевой среде могут представлять особый интерес в контексте вычислений машинного обучения;

b) еще одним аспектом являются функции программного обеспечения машинного обучения (например, характеристики обнаружения объекта). Модель и весовые коэффициенты, которые определяются при обучении (процессе, управляемом данными), могут создавать неопределенности при прогнозировании модели, которые, в свою очередь, могут относиться к функциональным недостаточностям, рассматриваемым в настоящем стандарте. Обнаружение и смягчение ограничений машинного обучения (например, обусловленных предопределенной необъективностью или неполнотой наборов данных для обучения, некорректной маркировкой, внутренними предубеждениями, переоценкой редких событий) входят в состав процесса SOTIF по уменьшению областей 2 и 3 (в соответствии с моделью, показанной на рисунках 2 и 3) и участвуют в действиях по валидации и верификации;

c) весовые коэффициенты алгоритма машинного обучения можно рассматривать как калибровку прикладного программного обеспечения или конфигурационные данные и применять к ним соответствующие требования ИСО 26262-6:2018 (приложение C).

Примечание 2 — Несмотря на то, что весовые коэффициенты машинного обучения являются числами, они могут оказывать качественное воздействие на заданную функциональность. Данные калибровки в контексте стандартов серии ИСО 26262 используются для корректировки поведения известной модели, а весовые коэффициенты модели машинного обучения — для определения самой модели. Следовательно, при изменении весового коэффициента машинного обучения могут проводиться анализ последствий и повторная валидация системы.

Примечание 3 — Внедрение мониторов реального времени, которые проверяют условия, предполагаемые при разработке компонентов машинного обучения, допускается как стандартами серии ИСО 26262, так и SOTIF. Проверку этих условий монитором с последующим переводом в безопасное состояние можно использовать для обнаружения случайных и систематических аппаратных сбоев и систематических программных сбоев (стандарты серии ИСО 26262), а также ограничений системы (SOTIF).

D.2.3 Обеспечение безопасности при использовании машинного обучения в заданной функциональности

При использовании технологий машинного обучения в реализации систем, связанных с безопасностью, важно определять соответствующие функции. Системы, в которых применяются технологии машинного обучения без определения заданных функций, не могут считаться безопасными, поскольку затруднительно предоставить достаточные обоснования их безопасности в отсутствие надлежащих вариантов и сценариев использования. Например, для алгоритмов глубокого обучения, как правило, недостаточно достижения оптимальных характеристик в отдельных вариантах и сценариях использования по причине естественных нелинейных аспектов и отсутствия формальной валидации. Дополнительное проведение валидации может являться подтверждением безопасности при использовании таких подходов.

Поведение сложных алгоритмов машинного обучения определяется преимущественно наборами данных для обучения, архитектурами моделей машинного обучения и процессом обучения (алгоритмом обучения, размером, начальными весовыми коэффициентами, функцией и др.), которые отражают трудноанализируемую спецификацию. Таким образом, важно оценивать безопасность функций, реализуемых алгоритмами машинного обучения, путем надлежащего тестирования в соответствии с рекомендациями настоящего стандарта (см. разделы 9—11) и анализа ограничений, специфичных для машинного обучения (см. раздел 7).

Элемент, в котором используется машинное обучение, также может обнаруживать условия, которые ограничивают его характеристики (например, низкий уровень достоверности обнаружения объекта датчиком при плохих погодных условиях). В соответствии с 4.4 эти выявленные условия и результирующее поведение выходов элемента передаются разработчикам системы более высокого уровня.

Кроме того, автономный процесс машинного обучения элемента может приводить к принятию результирующих параметров несмотря на то, что аннотированные данные для обучения, валидации или тестирования содержат выявленные остаточные сценарии с триггерными условиями (например, приводят к ложноположительным или ложноотрицательным срабатываниям). Обнаруженные триггерные условия, их оценка и возможные меры по снижению риска для SOTIF передаются разработчикам системы более высокого уровня для выполнения соответствующих действий. Эти действия могут выполняться на системном уровне, если, например, нарушения в элементе машинного обучения нейтрализуются одним из следующих компонентов в последовательности обработки. Обнаруженные триггерные условия также можно использовать для совершенствования процедуры обучения на уровне элемента машинного обучения.

При применении настоящего стандарта к элементам машинного обучения можно принимать во внимание следующие аспекты:

- функциональность и проект системы (см. разделы 5 и 8)

Спецификация вариантов использования, в том числе соответствующей ODD, играет важную роль не только в процессе обеспечения SOTIF, но и при сборе и формировании наборов данных для подготовки, валидации и тестирования функций машинного обучения. Полное определение всех аспектов ODD или факторов, имеющих

отношение к машинному обучению, не всегда представляется возможным. Надлежащее функционирование в выявленных и неопасных сценариях (область 1) в значительной степени зависит от качества набора данных для обучения.

Достаточный набор данных для тестирования повышает надежность обеспечения безопасности компонентов машинного обучения (области 2 и 3). Проект системы (ее архитектура) также крайне важен для описания функций, возлагаемых на алгоритмы машинного обучения.

Примечание 1 — В машинном обучении существуют два основных типа неопределенностей: эпистемологическая и случайная (см. [46], [47]). Эпистемологическую неопределенность часто можно уменьшать путем добавления данных при недостаточном количестве знаний. Случайная неопределенность — это внутренняя неопределенность, которая связана с шумом данных и соответственно не снижается путем увеличения их количества.

Пример 1 — Подсистема обнаружения объектов, которая включает в себя технологию распознавания изображений на основе машинного обучения и механизмы постобработки. В этой концепции ошибка при классификации, допускаемая алгоритмом машинного обучения, считается не сбоем, а событием, относящимся к характеристикам, поскольку механизмы постобработки, как правило, отделяют их от последовательности изображений, и влиять на безопасность может только частота остальных ошибок классификации;

- анализ (см. разделы 6 и 7)

В результате анализа определяются тестовые варианты и наборы сценариев для проверки функционирования компонентов с машинным обучением;

- стратегия верификации и валидации (см. раздел 9)

Обнаружение границ компонентов для тестирования является важной задачей. Выбор границ влияет не только на точность и полноту тестирования, но и на возможности и пригодность тестовых оракулов, таких как имитационное моделирование, тестовые и эксплуатационные данные.

Тестирование может выполняться на трех уровнях абстракции:

1) автономное тестирование — только если алгоритм машинного обучения способен эффективно обнаруживать невыявленные нарушения, типичные для компонента машинного обучения (например, визуализация);

2) тестирование на уровне компонента, которое, в зависимости от функциональности и тестируемых аспектов, может являться предпочтительным методом оценки поведения алгоритма, который содержит другие связанные компоненты (например, фильтры постобработки в примере с обнаружением объектов);

3) тестирование на уровне транспортного средства проверяет опасное поведение на уровне транспортного средства.

Для тестирования всей последовательности обработки может требоваться значительно больше тестовых примеров и времени, чем для тестирования компонентов по отдельности;

- оценка (см. разделы 10 и 11).

SOTIF на основе машинного обучения обеспечивается оценкой, как правило, с помощью тестирования (см. разделы 10 и 11). По этой причине важно, чтобы методы оценки отражали реальное поведение.

При дальнейшем машинном обучении компонента с целью улучшения его функций (см. раздел 8 — например, добавление категорий классификации для обнаружения объектов) компонент тестируется повторно, поскольку определить воздействие изменения на внутреннее поведение алгоритма машинного обучения трудно или даже невозможно. Таким образом, результаты предыдущих тестов, как правило, являются недействительными и не используются.

Примечание 2 — Управление изменениями применяется ко всем обновлениям выпущенных алгоритмов машинного обучения или параметров. При повторном обучении (в автономном или оперативном режиме) разработка возвращается к соответствующему этапу процесса SOTIF;

- этап эксплуатации (см. раздел 13)

В соответствии с разделом 13 при эксплуатации выполняется мониторинг функциональности. Обнаруженные новые риски анализируются с целью поиска функциональных недостаточностей, в том числе при использовании компонентов машинного обучения. Если в соответствии с результатами этого анализа в компоненты машинного обучения вносятся улучшения (см. раздел 8), можно применять все действия SOTIF (см. разделы 5—12), в том числе сбор данных.

D.2.4 Аспекты автономной подготовки алгоритмов машинного обучения

Как правило, машинное обучение включает в себя автономный процесс подготовки, целью которого является определение значений параметров алгоритма машинного обучения. Автономная подготовка машинного обучения может выполняться в несколько этапов с использованием различных инструментов; ее характерными проблемами являются естественная необъективность, неполнота наборов данных для подготовки и недостаточная верификация модели.

К общим проблемам разработки процесса машинного обучения относятся:

- неполные наборы данных для подготовки или недостаточная верификация подготовленных параметров;

- алогичные причины прогнозов (например, состязательные атаки);
- влияние выбранных данных для подготовки на характеристики машинного обучения (например, необъективность данных для подготовки может приводить к ошибочному определению корреляций);
- отсутствие у человека возможности управлять процессом подготовки (например, исправлять ошибочные корреляции;
- зависимость точности оценки эксплуатационных характеристик от выбора тестовых данных (например, некорректное разделение тестовых данных может приводить к искажению характеристик в большую или меньшую сторону).

Алогичный характер алгоритмов машинного обучения делает невозможным достижение их 100 %-ной эффективности, особенно в сложных задачах с ODD для открытого мира (например, используемых в системах восприятия для автоматизации вождения) из-за неизбежного возникновения ситуаций, в которых алгоритм генерирует ошибочные прогнозы. Корректная подготовка уменьшает количество ошибочных результатов, но никогда не исключает их полностью. Одна из задач SOTIF — гарантировать, что эти ограничения не приводят к неоправданному риску.

Пример процесса подготовки показан на рисунке D.4.

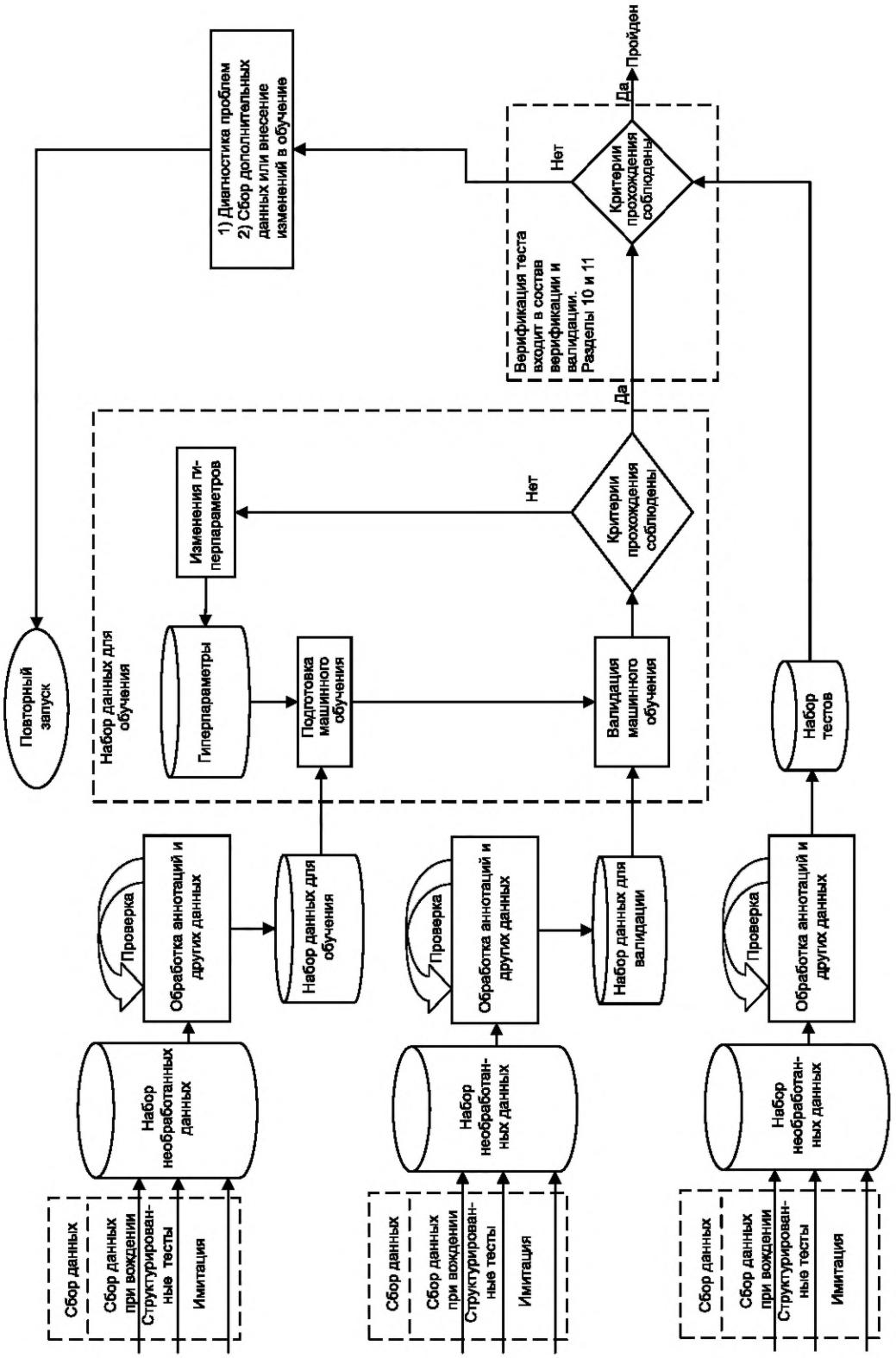


Рисунок D.4 — Пример автономного процесса разработки машинного обучения

Первым этапом на рисунке D.4 является подготовка набора данных, который соответствует сценам/сценариям ODD и является ограниченным и приближенным представлением реального мира. Для того, чтобы подготовленная модель машинного обучения эффективно обрабатывала редкие варианты использования, можно использовать методы выборки с учетом важности.

В наборе данных могут учитываться дополнительные аспекты — например, изменение продукта во времени (старение датчиков). Можно собирать данные из множества источников — например, испытаний на полигоне, результатов имитационного моделирования, эксплуатации, а также использовать стандартные наборы эталонных данных.

Данные, которые с высокой степенью точности представляют предполагаемую реальную среду эксплуатации системы автоматизации, включают в себя большое количество вариантов и сочетаний различных действующих условий и факторов. Имитационное моделирование и специализированные испытания (например, на испытательном полигоне) можно использовать при сборе эксплуатационных данных о ситуациях, которые редко возникают в реальном мире, а также для увеличения степени разнообразия вариантов. Наборы данных можно дополнять синтезированными данными, если их валидация подтверждает их соответствие реальному миру.

Затем данные подвергаются предварительной обработке, которая предшествует их использованию в подготовке/валидации машинного обучения или тестировании его модели. На этапе предварительной обработки можно выполнять маркировку (аннотирование) данных в соответствии с их классами (примеры — границы дороги, автомобили, мотоциклы, транспорт экстренных служб), свойствами (примеры — цвета, края) и реакциями (пример — требуемое управляющее действие). Маркировка данных может осуществляться вручную специально обученным персоналом или автоматически. Как правило, при ручной маркировке выполняется проверка аннотаций. Тщательная маркировка данных обеспечивает правильность их классификации и достаточную точность работы с граничными рамками при выполнении действий машинного обучения. В зависимости от варианта использования машинного обучения и особенностей набора данных предварительная обработка может включать в себя дополнительные процедуры, такие как фильтрация, аугментация данных и понижение размерности. Результаты предварительной обработки часто улучшаются с помощью методов очистки данных (например, удаления повторяющихся или неактуальных наблюдений).

На следующем этапе данные разделяются на (достаточно) независимые наборы для подготовки, валидации и тестирования, которые имеют различные предназначения. Для надежной оценки модели машинного обучения с помощью тестовых данных важно предотвращать утечки информации из одних наборов данных в другие (особенно между наборами данных для подготовки и тестирования). Наборы для подготовки и валидации используются в процессе подготовки модели машинного обучения, который представляет собой цикл настройки гиперпараметров, охватывающий подготовку и валидацию. При подготовке модели машинного обучения данные непрерывно подаются на ее вход одновременно с настройкой параметров (например, весовых коэффициентов нейронной сети) с учетом изменения количества ошибок на выходе. Подготовка продолжается до тех пор, пока не достигаются заданные критерии (например, допустимая частота ложноположительных и ложноотрицательных результатов при обнаружении или классификации объектов). Для выполнения других задач могут требоваться другие специальные критерии.

После завершения подготовки модель машинного обучения оценивается на предмет соответствия критерию пригодности/непригодности с помощью набора для валидации. При получении неудовлетворительных результатов гиперпараметры модели машинного обучения уточняются, и процесс подготовки выполняется повторно. После завершения подготовки машинного обучения оценивается соответствие подготовленной системы критерию пригодности с использованием набора данных для тестирования в рамках верификации и валидации (см. разделы 10 и 11).

Независимость наборов данных для подготовки, валидации и тестирования гарантирует, что система машинного обучения получила знания об основных характеристиках данных для подготовки, а не о случайных внутренних корреляциях в них (см. [48]).

Например, создают два набора тестовых данных:

1) тестирование с использованием данных, отделенных от данных для подготовки и валидации, позволяет оценивать обобщаемость компонента машинного обучения;

2) тестирование с использованием отдельно собранного набора данных предотвращает воздействие случайных корреляций на машинное обучение.

Для точной оценки эксплуатационных характеристик машинного обучения и исследования невыявленных опасных сценариев тестовые данные используются только в целях верификации теста, но не участвуют в подготовке компонента машинного обучения. Во избежание чрезмерного обучения желательно использовать большой набор тестовых данных; это можно обеспечить при выполнении верификации и валидации на уровне транспортного средства в соответствии с разделами 10 и 11.

Параметры, которые получены в ходе подготовки, принимаются, если соблюдены требования к успешности тестирования, указанные в спецификации и проекте. При неуспешной верификации можно перезапускать процесс после сбора дополнительных данных и/или внесения изменений в подготовку. Если при дальнейшем тестировании наблюдаются некорректное поведение или недопустимые характеристики принятой модели, весь процесс выполняется повторно с учетом новой информации. Этот цикл соответствует процессу разработки SOTIF, который показан на рисунке 10.

Ключевым параметром надежности подготовки для указанной ODD является достаточный охват сценариев аннотированными наборами данных. Обнаружение новых сценариев на итерациях SOTIF при разработке или эксплуатации может являться причиной обновления наборов данных для подготовки, валидации и тестирования.

Можно повышать надежность программного обеспечения машинного обучения путем анализа его интерпретируемости (см. [49] и [50]), который позволяет демонстрировать, что решения машинного обучения (например, классификация) основаны на релевантных данных, а не на артефактах (см. [51]). Результаты анализа интерпретируемости могут входить в состав критериев пригодности при валидации машинного обучения и/или верификации теста (см. рисунок D.4).

D.2.5 Анализ автономного процесса подготовки алгоритмов машинного обучения

Многие проблемы, связанные с ограничениями подготовки, можно обнаруживать путем анализа, а также верификации и валидации. На рисунке D.5 показан общий процесс анализа проблем подготовки.

Рисунок D.5 — Этапы анализа автономного процесса подготовки алгоритмов машинного обучения

Этот анализ охватывает все этапы процесса, в том числе:

- планирование маршрутов для сбора данных;
- сбор данных;
- выгрузку и поглощение данных;
- маркировку и обзор данных;
- курирование и извлечение данных;
- маркировку и обзор метаданных;
- создание наборов данных для подготовки, верификации и валидации тестирования;
- подготовку машинного обучения;
- валидацию машинного обучения;
- управление конфигурациями машинного обучения;
- развертывание машинного обучения и его интеграцию в программный комплекс.

С точки зрения указанной задачи и ODD целью сбора данных является обеспечение разнообразия и полноты:

- транспортных средств и водителей;
- маршрутов и условий вождения;
- сбора структурированных данных (например, данных, собранных с использованием сценариев для испытательного полигона).

Примечание — Для обнаружения и устранения возможных источников необъективности и ограничений внутри автономного процесса подготовки можно выполнять анализ, аналогичный анализу видов и последствий отказов (FMEA).

Результаты этого анализа позволяют не только совершенствовать процесс подготовки (см. D.2.5), но и влиять на следующие аспекты разработки системы:

- спецификацию и проект (см. раздел 5) посредством обнаружения потенциальных систематических проблем (см. раздел 7 и A.2.8) и выполнения последующих действий по усовершенствованию (см. рисунок 11);
- надежность использования программных инструментов (см. A.2.9).

D.3 Аспекты SOTIF для карт

D.3.1 Общие положения

Карты могут поддерживать или реализовывать ADAS и необходимые функции автоматического вождения, такие как локализация, движение по траектории, сопоставление полос объектам и опознавание наземных ориентиров (например, перекрестков и слияний полос). Карты также могут интегрироваться с датчиками восприятия для повышения надежности работы системы восприятия и/или обнаружения сбоев. В D.3 рассматриваются некоторые аспекты применения карт, предназначенных для поддержки или реализации функций, связанных с безопасностью.

D.3.2 Спецификация и проектирование карт

Свойства карт определяются в спецификации и проекте (см. раздел 5). В проекте могут быть отражены следующие аспекты:

- функциональные возможности транспортного средства:
  - использование карт;
  - функции, зависящие от карт;

- поведение и функционирование на уровне транспортного средства в условиях, когда карты:
  - недоступны (например, при потере связи с сервером карт или недоступности карты на устройстве, встроенном в транспортное средство);
  - являются неточными или устаревшими;
  - требуется разрешить конфликт между картами и системой восприятия транспортного средства, управляемого ADS;
- определение характеристик карты:
  - системные требования к картам;
  - требования к данным карт;
  - требования к точности карт;
  - степень подробности карт (высокое или низкое разрешение);
  - описание потока информации карт;
  - требования к точности указания местоположения объектов на картах;
  - регион действия карты;
  - механизм поддержки корректности карты (гарантии уровня ее качества);
- технические средства обновления карт:
  - механизм обновления карт;
  - частота обновления карт;
  - облачные и встроенные решения для хранения и обновления карт;
- известные ограничения карт:
  - ограничения сбора данных;
  - ограничения обработки данных;
  - ограничения слияния карт (при обновлении карт, объединении нескольких карт, объединении нескольких приводов).

Примечание — По мере устаревания карты достоверность данных уменьшается.

D.3.3 Аспекты SOTIF, связанные с картами

Примерами проблем, связанных с SOTIF и относящихся к картам, являются некорректность или устаревание карт вследствие изменений внешней среды — временных (например, временное закрытие полос движения) или постоянных (например, новые стационарные дорожные знаки).

Необходимо принимать меры для того, чтобы нарушения на карте не препятствовали достижению SOTIF. В спецификации и проекте можно указывать методы реагирования на ограничения карт, например:

- блокировать функции в областях, которые отсутствуют на карте;
- сокращать функции в областях карты с низкой точностью;
- обновлять карту или допуски.

Требования SOTIF могут регламентировать частоту обновлений карт. Для обнаружения устаревшей информации на карте можно сравнивать ее содержимое с данными восприятия внешней среды автономным транспортным средством, однако несовпадения могут быть обусловлены ограничениями системы восприятия; сама по себе система восприятия не может гарантировать обнаружение всех нарушений на карте.

Несмотря на то, что карты не всегда отображают состояние дорог в реальном времени (например, перекрытия полос из-за аварий, ремонтных работ и погодных условий, таких как наводнения), требования SOTIF можно формулировать так, чтобы карты отображали постоянную дорожную инфраструктуру с некоторой точностью, определяемой путем анализа безопасности. При проектировании системы также можно включать в нее мониторинг показателей, позволяющих прогнозировать необходимость обновления карт (проблему «застывшей карты»). Кроме того, все выявленные ограничения системы работы с картами должны указываться в спецификации и проекте. Любая функция, которая использует карты и их службы, должна учитывать эти ограничения.

Примечание 1 — Проблемы, которые связаны с повреждением карт в результате сбоя в системе, рассматриваются в стандартах серии ИСО 26262 и не входят в состав SOTIF. Повреждения карт могут быть обусловлены, например, повреждением памяти, некорректным доступом к картам и ошибками при загрузке карт.

Примечание 2 — Систематические ошибки и функциональные недостаточности могут учитываться в процессе построения карт. Их можно обнаруживать путем анализа или аудита процесса.

D.4 Аспекты SOTIF, связанные с V2X

D.4.1 Общие сведения

V2X (vehicle-to-everything, система обмена информацией между транспортным средством и его окружением) представляет собой механизм взаимодействия транспортного средства с другими транспортными средствами, дорожной инфраструктурой, пешеходами и облаком. V2X позволяет повышать безопасность и эффективность дорожного движения, а также снижать загрязнение окружающей среды (см. [52] и [53]). Можно использовать V2X как технологию связи для решения различных задач — удаленного технического обслуживания транспортного средства, управления дорожным движением, транспортом и информационно-развлекательной системой автомобиля.

V2X может сообщать целевому транспортному средству о состоянии внешней среды, особенно при неблагоприятных погодных условиях и затрудненном дорожном движении (см. [54]). Например, с помощью V2X транспортное средство может с легкостью определять состояние, режим и подробные временные характеристики работы светофора. V2X также может передавать автоматизированным транспортным средствам дополнительную информацию о погодных условиях, авариях, ремонтных работах и присутствии пользователей дороги.

Кроме того, существует большое количество многофункциональных прикладных систем и вариантов использования, в которых технологии связи V2X играют важную роль (например, формирование автоколонн и удаленное вождение [55]). В этих автомобильных системах сообщения V2X используются как механизм активации, а к V2X применяются аспекты SOTIF.

Можно анализировать SOTIF системы с V2X на уровне дополненного транспортного средства, который включает в себя внебортовые элементы (источник информации и средства связи). В этом случае система V2X может рассматриваться как сложный датчик (пример см. на рисунке D.6).

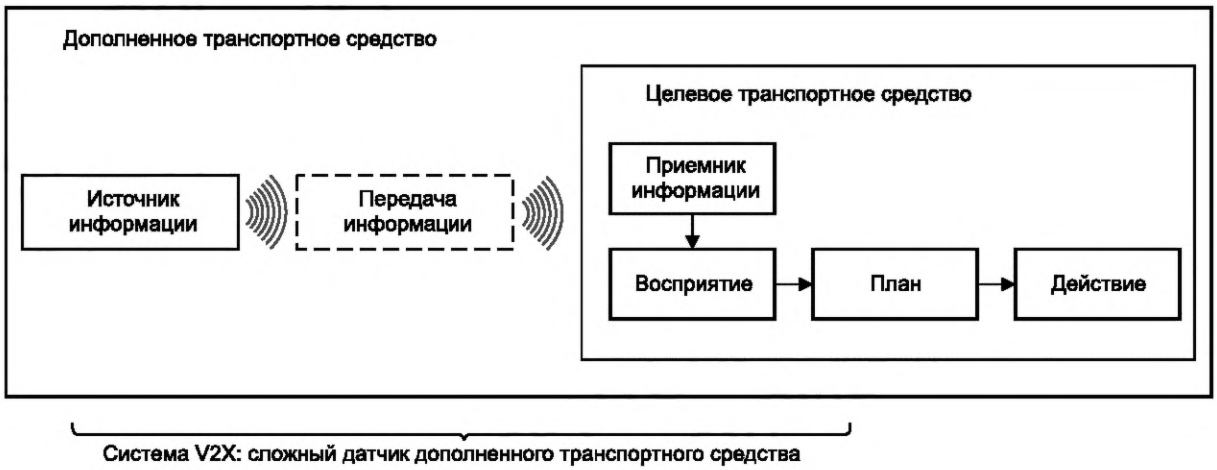


Рисунок D.6 — Пример системы V2X в составе дополненного транспортного средства

В D.4 подробно рассматриваются некоторые аспекты использования V2X в составе критически важных для безопасности функций.

D.4.2 Спецификация и проект системы связи V2X

Свойства системы связи V2X определяются в спецификации и проекте (см. раздел 5). Примеры положений, подлежащих рассмотрению, включают:

- требования к системе V2X:
  - требования к задержкам;
  - требования к надежности;
  - требования к оперативной совместимости;
- требования к данным V2X:
  - требования к точности объекта или события в сообщении V2X: расстояние, на котором данные можно считать корректными и достоверными (в том числе точность указания места и времени);
  - требования к целостности объекта или события в сообщении V2X: защита элементов данных от повреждения;
  - требования к точности: стандартное отклонение от среднего значения;
  - требования к разрешению: наименьшая разность между двумя соседними значениями;
  - требования к прослеживаемости: возможность прослеживания обеспечения качества;
  - требование соответствия стандартам совместимости, базовым профилям связи, системным профилям, профилям защиты, уровней доверия и безопасности;
  - использование сообщения V2X в функциях уровня транспортного средства;
  - выявленные ограничения V2X (например, неспособность воспринимать инфраструктуру на обочине дороги, помехи от других устройств).

D.4.3 Реализация SOTIF для V2X

Проблемы SOTIF в контексте V2X в основном связаны с некорректностью (например, неточностью или просроченностью) сообщений из-за недостаточностей производительности V2X. Проблемы можно обнаруживать, сравнивая сообщение V2X с результатами восприятия автономным транспортным средством и оценивая новизну и точность сообщения.

Типы сообщений V2X, которые используются в различных прикладных системах, могут отличаться друг от друга с точки зрения требований к их задержкам, надежности и обновлению.

Сообщения V2X можно классифицировать по частоте изменения содержимого:

- статические сообщения V2X, содержимое которых изменяется редко (например, дорожный знак изменяется раз в неделю);
- полудинамические сообщения, содержимое которых изменяется раз в несколько часов (например, авария или погодные условия);
- динамические сообщения, содержимое которых изменяется в реальном времени (например, сигналы светофора, динамическое поведение транспортного средства при формировании автоколонн).

Таким образом, в спецификации системы можно указывать требования к задержке, надежности и/или частоте обновления для различных типов сообщений V2X с целью соблюдения допусков, установленных по результатам анализа безопасности функции/системы.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 26262-1	IDT	ГОСТ Р ИСО 26262-1—2020 «Дорожные транспортные средства. Функциональная безопасность. Часть 1. Термины и определения»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] COMMISSION RECOMMENDATION of 22 December 2006 on safe and efficient in-vehicle information and communication systems: update of the European Statement of Principles on human machine interface (2007/78/EC): https://data.europa.eu/eli/reco/2007/78/oj

[2] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE Recommended Practice J3016_201806, https://www.sae.org/standards/content/j3016 201806

[3] Ulbrich S., Menzel T., Reschka A., Schuldt F., Mauer M., Defining and Substan-tiating the Terms Scene, Situation, and Scenario for Automated Driving, 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), https://doi.org/10.1109/ ITSC.2015.164

[4] CENELEC EN 50126-2:2017, Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety (Применение на железнодорожном транспорте. Спецификация и демонстрация надежности, доступности, ремонтопригодности и безопасности (RAMS). Часть 2. Системный подход к безопасности)

[5] ISO 34502:2022, Road vehicles — Engineering framework and process of scenario-based safety evaluation (Транспортные средства. Тестовые сценарии для систем автоматического вождения. Система оценки безопасности на основе сценариев)

[6] Statistics and data about reported accidents and casualties on public roads in Great Britain (STATS19), UK Department for Transport, https://www.gov.uk/government/collections/road-accidents-and-safety-statistics

[7] German In-Depth Accident Study (GIDAS), accident data collection project in Germany, https://www.gidas.org/start-en.html

[8] NASS General Estimates System (GES), US Department of Transportation, https://www.nhtsa.gov/national-automotive-sampling-system/nass-general-estimates-system

[9] CARE database (Community database on Accidents on the Roads in Europe), https://road-safety.transport.ec.europa.eu/statistics-and-analysis/methodology-and-research/care-database-en

[10] IGLAD (Europe) http://www.iglad.net/

[11] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3; https://www.acea.be/uploads/publications/ 20090831_Code_of_Pratice_ADAS.pdf

[12] DIN SAE SPEC 91381:2019, Terms and Definitions Related to Testing of Auto-mated Vehicle Technologies

[13] Kuhn D.S., Kacker R.N., Lei Y., Combinatorial testing, NIST report, June 25, 2012, https://www.nist.gov/publications/combinatorial-testing

[14] Kelly T., Rob Weaver R., The Goal Structuring Notation — A Safety Argument Notation", https://www-users.cs.york.ac.uk/tpk/dsn2004.pdf

[15] Stellet J.E., Brade T., Poddey A., Jesenski., Branz W., Formalisation and algo-rithmic approach to the automated driving validation problem, 2019 IEEE Intelli-gent Vehicles Symposium (IV), https://doi.org/10.1109/IVS.2019.8813894

[16] Shappell S.A., Wiegmann D.A., The Human Factors Analysis and Classification-System — HFACS, February 2000 Final Report. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

[17] Hartjen L., Philipp R., Schuldt F., Howar F., Friedrich B., Classification of Driving Maneuvers in Urban Traffic for Parametrization of Test Scenarios in: 9. Tagung Automatisiertes Fahren, Lehrstuhl für Fahrzeugtechnik mit TÜV SÜD Akademie: https://mediatum.ub.tum.de/1535131

[18] BSI PAS 1883:2020, AVSC Best Practice for Describing an Operational Design Domain

[19] Leveson N., Engineering a Safer World — Systems Thinking Applied to Safety. M IT Press, Cambridge, Massachusetts, USA 2011

[20] Leveson N., Thomas J., STPA-Handbook. 2018. Available for download at psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[21] Abdulkhaleq A. et al., A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles, 4th European STAMP Workshop 2016, Procedia Engineering, 179, 41-51, 2017 https://www.sciencedirect.com/science/article/pii/S1877705817312109

[22] Abdulkhaleq A., Wagner, S, Lammering, D, Boehmert, H, Blueher, P, Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. arXiv preprint arXiv:1703.03657, 2017

[23] Abdulkhaleq A., Wagner S., Leveson N., A Comprehensive Safety Engineering approach for Software-Intensive Systems Based on STPA. Procedia Engineer-ing, 128:2-11, 2015, https://www.researchgate.net/publication/265508075 Expe-riences with Applying STPA to Software-Intensive_Systems_in_the_Automotive_Domain

[24] Sabaliauskaite G., Shen Liew L., Cui J., Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model. International Journal on Advances in Security, 11(1&2):160—169, 2018

[25] ISO 26262 (all parts), Road vehicles — Functional safety (Дорожные транспортные средства. Функциональная безопасность)

[26] Fabris S., Priddy J., Harris F., Method for Hazard Severity Assessment for the Case of Unintended Deceleration, presented at 2012 VDA Auto SYS conference in Berlin

[27] Piao J., M cDonald M., Low speed car following behaviour from floating vehicle data'. IEEE IV2003 Intelligent Vehicles Symposium.

[28] Allen R., Magdaleno R., Serafin C., Eckert S., Sieja F., Driver Car Following Behavior Under Test Track and Open Road Driving Condition, SAE Technical Pa-per 970170, 1997, https://doi.org/10.4271/970170

[29] Traffic Safety Facts N.H.T.S.S.A., 2 015, https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812384

[30] Fabris S., Priddy J., Harris F., Method for hazard severity assessment for the case of undemanded deceleration., Presented at VDA Automotive SYS Conference, Berlin, June 19/20, 2012, https://www.researchgate.net/publication/344452155_Method_for_hazard_severity_for_Method_for_hazard_severity_assessment_for_the_case_of_undemanded_deceleration_-_Simone_Fabris

[31] Littlewood B., Wright D., Some Conservative Stopping Rules for the Operational Testing of Safety-Critical Software, IEEE Trans. SW Engng., 23(11), 673—683, Nov. 1997

[32] SIPOC — Wikipedia https://en.wikipedia.org/wiki/SIPOC

[33] Hirsenkorn N., Kolsi H., Selmi M., Schaermann A., Hanke T., Rauch A., Rasshofer R., Biebl E., Learning Sensor Models for Virtual Test and Develop-ment. 11. Workshop Fahrerassistenzsysteme und automatisiertes Fahren, Uni-DAS, Walting, 2017

[34] de Gelder E., Paardekooper J.P., Assessment of Automated Driving Systems using real-life scenarios, IEEE Intell. Veh. Symp. Proc., no. IV, pp. 589—594, 2017

[35] Functional Mockup Interface http://functional-mockup-interface.org/

[36] ASAM OpenDRIVE http://www.asam.net/standards/detail/opendrive/

[37] ASAM OpenCRG http://www.asam.net/standards/detail/opencrg/

[38] ASAM OpenSCENARIO http://www.asam.net/standards/detail/openscenario/

[39] Open Simulation Interface (OSI) https://github.com/OpenSimulationInterface

[40] Navigation Data Standard https://www.nds-association.org/

[41] CityGML http://www.opengeospatial.org/standards/citygml

[42] Vaicenavicius J., Wiklund T., Grigaite A., Kalkauskas A., Vysniauskas I., Keen S. D., Selfdriving car safety quantification via component-level analysis. SAE Inter-national Journal of Connected and Automated Vehicles, Volume 4, Issue 1, pp 35—45, 2021

[43] Shalev-Schwarz S., Shammah S., Shashua A., On a Formal Model of Safe and Scalable Selfdriving Cars https://arxiv.org/abs/1708.06374v6

[44] Nistér D., Lee H.-L., Ng J., Wang Y., An Introduction to the Safety Force Field, https://www.nvidia.com/content/dam/en-zz/Solutions/self-driving-cars/safety-force-field/an-introduction-to-the-safety-force-field-v2.pdf

[45] FRAADE-BLANDAR L, BLUMENTHAL M. S., ANDERSON J. M. KALRA N. — RAND: Measuring Automated Vehicle Safety — https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2662/RAND RR2662.pdf

[46] Kendall A., Gal Y., What Uncertainties Do We Need in Bayesian Deep Learning for Computer Vision?, NIPS 2017

[47] Phan B., Khan S., Salay R., Czarnecki K., Bayesian Uncertainty Quantification with Synthetic Data. WAISE 2019

[48] Koopman P., Wagner M., Autonomous Vehicle Safety: An Interdisciplinary Chal-lenge, IEEE Intelligent Transportation Systems Magazine, Special Issue on SSIV, 2017, in press Vol. 9 #1, Spring 2017, pp. 90—96

[49] Molnar C., A Guide for Making Black Box Models Explainable, 2021, https://christophm.github.io/interpretable-ml-book/

[50] Zhang Q., Zhu S.-C., Visual Interpretability for Deep Learning: a Survey, 2018, https://arxiv.org/ abs/1802.00614

[51] Lapuschkin S., Wäldchen S., Binder A., Montavon G., Samek W., Müller K. R., Unmasking Clever Hans predictors and assessing what machines really learn, 2019, In: Nature Communications 1096 (2019), https://www.nature.com/articles/s41467-019-08987-4

[52] U.S. Department of Transportation. (Jul.2017). Vehicle-to-vehicle communication technology. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/ docments/v2v_fact_sheet_101414_v2a.pdf

[53] Tsugawa S., Jeschke S., Shladover S. E., A Review of Truck Platooning Pro-jects for Energy Savings, IEEE Transactions on Intelligent Vehicles, vol. 1, no. 1, 2016

[54] Wang J., Liu J., Kato N., Networking and communications in autonomous driv-ing: A survey, IEEE Communications Surveys & Tutorials, vol. 21. no.2, Q2, 2019

[55] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancement of 3GPP support for V2X scenarios; Stage 1(Release 16) 3GPP TS 22.186 V16.2.0 (2019-06)

[56] IATF 16949, Quality management system requirements for automotive produc-tion and relevant service parts organizations

[57] ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes (Системная и программная инженерия. Процессы жизненного цикла системы)

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

Ключевые слова: безопасность заданной функциональности (SOTIF), дорожные транспортные средства, жизненный цикл систем, функциональные недостаточности, устранение рисков, выявленные и невыявленные сценарии, оценка сценариев, реализация SOTIF, верификации и валидации SOTIF

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректоры *И.А. Королева, М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 29.09.2025. Подписано в печать 21.10.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 20,46. Уч.-изд. л. 18,52.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru