

# Построение семейства сценариев использования с целью анализа функциональной безопасности систем управления

А.А. Мишкина, О.М. Кировский, И.А. Мозолин

**Аннотация:** В статье рассматриваются вопросы анализа функциональной безопасности системы управления высокоавтоматизированными транспортными средствами. Статья предлагает метод описания сценариев использования транспортных средств, который может быть использован в анализе опасностей и оценке рисков – составной части жизненного цикла функциональной безопасности. Проведен обзорный анализ методов исследований описания сценариев по стандарту ASAM OpenScenario в области функциональной безопасности. Рассмотрены вопросы основ функциональной безопасности согласно стандарту ISO 26262:2018. Кроме того, рассматриваются основные направления в области моделирования сценариев. Описание сценариев является важным для тестирования и проверки безопасности высокоавтоматизированных транспортных средств. Однако в реальном процессе разработки форматы данных и интерфейсы, используемые различными производителями и поставщиками средств моделирования, разнообразны, и унифицировать стандарты сложно. В статье обсуждается метод выделения набора сценариев дорожных ситуаций, который затем, после анализа, позволит обеспечить безопасность на дорогах, а также чтобы справиться с растущим трафиком. Для обеспечения безопасности необходимо определить наиболее часто повторяющиеся сценарии, описать их на формальном языке, провести анализ опасностей и оценку рисков. Результатом работы является перечень описанных сценариев использования к системе управления высокоавтоматизированными транспортными средствами.

**Ключевые слова:** сценарий, функциональная безопасность, анализ, система управления, транспортное средство, движение, требование.

## 1 ВВЕДЕНИЕ

В 1886 году на улицах города Мангейма (Германия) появился первый автомобиль. Через некоторое время его стали продавать под названием «Бенц Патент-Моторваген № 1», т. е. «Патентованный автомобиль Бенца». Это был первый в мире самодвижущийся механизм, приводимый в движение двигателем внутреннего сгорания (ДВС); он мог разогнаться до 16 км/ч. Карл Бенц, создатель первого автомобиля, не позаимствовал никаких конструктивных особенностей из существовавших до него телег и колясок. В его Patent-Motorwagen всё необходимое

для приведения в движение при помощи ДВС было разработано и спроектировано с нуля – двигатель, шасси, привод и управление. Motorwagen стал прародителем каждого автомобиля, построенного после него, он имел все части, присущие современным транспортным средствам: двигатель, систему охлаждения, трансмиссию, колеса и тормоза.

В то же время была проведена дискуссия о целесообразности внедрения этой новой технологии в массы. Сторонники Motorwagen настаивали на преимуществах его использования и победили в полемике, несмотря на сопротивление сторонников «старых» методов передвижения: конных повозок и железных дорог на паровой тяге. После этого автомобиль был представлен в качестве коммерческого продукта и стал доступен для многих людей.

Сегодня автомобили влияют на жизнь людей во всем мире и постоянно меняют индивидуальную мобильность. В XXI веке многие новые технологии достигают высшего уровня готовности, что вновь требует обсуждения вопроса о целесообразности внедрения этих технологий в качестве коммерческих массовых продуктов. Автоматизированное вождение является одним из таких решений.

Прошло около 80 лет с момента появления первой осмысленной идеи об автономных автомобилях до тех пор, пока эксперты не предсказали, что инновация достигнет уровня готовности технологии, выходящего за рамки исследований. Представители производителей транспортных средств уверены в том, что “примерно через два года у нас будет полная автономия”. В настоящий момент передовые образцы автомобилей достигают четвертого уровня автоматизации (Классификация по стандарту SAE J3016 «Системы автоматизированного управления движением АТС. Классификация, термины и определения»). Они способны самостоятельно перемещаться по известным маршрутам, полностью удовлетворяя потребность в безопасном и удобном перемещении без вмешательства водителя. Такие автомобили ещё находятся в стадии опытной эксплуатации и не вышли в массовое производство. Что касается полной автономии, для ее достижения необходимо достигнуть последнего – пятого уровня автоматизации автомобиля.

Сегодня заинтересованные стороны все еще обсуждают, действительно ли они хотят полной автономии на дорогах. Это обсуждение важно, потому что автономное вождение, как и большинство других технологий, принесет не одну только пользу. Необходимо всеми возможными способами обеспечивать максимальную безопасность на дорогах.

Для понимания того, что необходимо будет улучшать или изменять в городах, где будут использоваться автономные транспортные средства, нам требуется произвести исследования, создать симуляции дорожного движения и описать сценарии использования транспортных средств с целью обеспечения безопасного управления.

## 2 ОСНОВНАЯ ЧАСТЬ

На сегодняшний день сочетание свойств активной и пассивной безопасности транспортных средств, состояние дорожных условий, подготовленность участников дорожного движения и организация дорожного движения в подавляющем большинстве дорожно-транспортных ситуаций таково, что для предотвращения аварии требуется максимально проанализировать все возможные риски, связанные с использованием высокоавтоматизированных транспортных средств, обеспечить их мерами для надежной эксплуатации, и для этого необходимо воспользоваться описанием сценариев использования [3, с. 99-100].

Как нам известно, сценарии могут описываться на разных стадиях жизненного цикла с разной детализацией. Сценарии необходимо описывать, начиная со стадии, в которой разрабатывается документация для идентификации опасностей и оценки рисков (Hazard Identification & Risk Evaluation) (логический уровень), затем во время ТСА (Triggering Conditions Analysis) (начало технического уровня) описанный ранее сценарий уточняется и дополняется техническими характеристиками, которые были получены. После уточнения из имеющихся логических сценариев и инициирующих условий (Triggering Conditions) создаются технические сценарии, которые используются для валидации.

Таким образом, сценарии начинаются на функциональном уровне и продолжают на техническом (используя терминологию ИСО 26262). На рисунке 1 изображена V-модель жизненного цикла адаптированная под стандарт ИСО 26262, разработанная на основе стандартной V-модели.

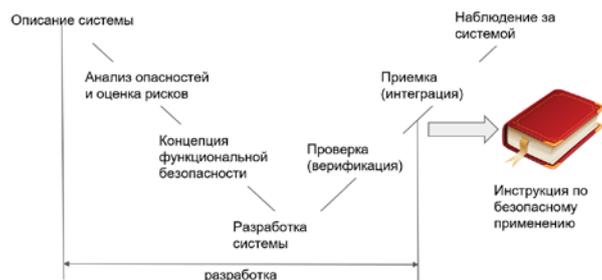


Рисунок 1 – V-модель жизненного цикла по ИСО 26262

Сценарии использования транспортных средств будут разрабатываться для дальнейшего определения требований к автоматизированной системе управления (АСУ) высокоавтоматизированными транспортными средствами (далее - ВАТС). Очевидно, что АСУ ВАТС должна выполнять требования, которые не позволяют транспортному средству (ТС) сталкиваться с другими ТС, создавать угрозы любым участникам дорожного движения, делать резких движений, и так далее [1]. Но такие требования не несут в себе практической пользы. Требования необходимо максимально конкретизировать всеми возможными техническими характеристиками.

Описанный ранее ИСО 26262 содержит в себе этап HARA (Hazard analysis and risk assessment) (Анализ опасностей и оценка рисков). Данный этап определяет высокоуровневые требования путём анализа сочетаний функциональных отказов (malfunctions) и операционных ситуаций. Требования, выявленные на этапе HARA называются целями безопасности. Эти требования сравнительно простые, например: "Не допускать активации подушек безопасности вследствие отказов", "Гарантировать давление в тормозной системе" и т.п. Технические требования в дальнейшем разрабатываются из анализа системы, на таких этапах, как FMEA (Failure Modes and Effect Analysis) (режимы отказов и анализ последствий), FTA (Fault Tree Analysis) (анализ дерева отказов).

Описание сценариев является важным для тестирования и проверки безопасности высокоавтоматизированных транспортных средств. Однако в реальном процессе разработки форматы данных и интерфейсы, используемые различными производителями и поставщиками средств моделирования, разнообразны, и унифицировать стандарты сложно.

Исходя из этого, немецкая ассоциация стандартизации систем автоматизации и измерений (ASAM) запустила серию стандартов OpenX в области моделирования - OpenSCENARIO.

OpenSCENARIO определяет стандартный формат сценария имитационных испытаний, который специально используется для описания динамического содержимого приложений симуляции вождения и совместим с различным программным обеспечением симуляционных испытаний. Применимые сценарии в основном включают действия, траектории, транспортные средства

(геометрия, тип, ось, производительность), водители (статус), окружающую среду (погода, время, дорожные условия) и т. д.

Описание маневров является наиболее важной частью тестирования, проверки и сертификации безопасности систем помощи водителю и автономных автомобилей. Промышленность, агентства по сертификации и государственные органы совместно работают над определением библиотек маневров, которые можно использовать для обеспечения безопасной работы таких систем [2]. Для этой цели хорошо подходит независимый от производителя стандарт ASAM OpenSCENARIO.

Сценарии необходимо описывать на трёх уровнях уровня абстракции: функциональный, логический и конкретный. Конкретный уровень должен быть описан методом ASAM OpenSCENARIO.

Далее описан пример сценария поворота транспортного средства направо (рисунок 2).

Функциональный уровень: поворот направо на регулируемом перекрёстке.

Логический уровень: автомобиль движется в соответствующем крайнем положении на проезжей части, предназначенной для движения в данном направлении. Приближаясь к перекрёстку, целевой автомобиль сбрасывает скорость и начинает торможение до полной остановки. После разрешающего сигнала светофора автомобиль возобновляет движение и совершает поворот направо из крайнего правого с дальнейшим ускорением в крайний правый ряд.

Для того, чтобы описать сценарии использования транспортных средств необходимо создать симуляцию в выбранной ранее методикой иерархий среде моделирования – SUMO. Была произведена первичная интеграция среды моделирования SUMO и стандарта для описания сценариев OpenSCENARIO. В начале была загружена карта для создания симуляции, затем местность была проанализирована на предмет количества объектов, при нахождении рядом с которыми необходимо обеспечивать наибольшую безопасность, такие как пешеходные переходы, железнодорожные переезды и т.д. Таким объектам присваивались веса для определения критичности. Далее запускалась симуляция дорожного движения в SUMO, производился анализ полученных данных после завершения симуляции, на основе этих данных разрабатывались сценарии. В данном разделе описаны шаги присвоения весов критичным объектам местности, а также шаги моделирования сценариев с использованием стандарта OpenSCENARIO и последующего их описания на основе симуляции.



Рисунок 2 – Поворот направо на регулируемом перекрёстке

## 2.1 ИНСТРУМЕНТЫ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ

Для понимания того, что необходимо будет улучшать или изменять в городах, где будут использоваться автономные транспортные средства, нам требуется произвести исследования, создать симуляции дорожного движения и описать сценарии использования транспортных средств с целью обеспечения функциональной безопасности автоматизированных систем управления.

SUMO (Моделирование городской мобильности) - мультимодальная среда моделирования трафика с открытым исходным кодом, предназначенная для работы в больших сетях. Он доступен с 2001 года и позволяет моделировать системы интермодального движения, включая дорожные транспортные средства, общественный транспорт и пешеходов. В состав SUMO входит множество вспомогательных инструментов, которые автоматизируют основные задачи по созданию, выполнению и оценке моделирования трафика, такие как импорт сети, расчеты маршрутов, визуализация и расчет выбросов. SUMO может быть расширен с помощью пользовательских моделей и предоставляет различные API для удаленного управления моделированием [5].

## 2.2 ШАГИ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ

Дискретный симулятор SUMO позволяет несколькими способами задавать дорожные сценарии. Один из них заключается в прописывании вручную конфигурационных файлов. Второй способ позволяет импортировать уже готовую дорожную сеть из таких программных продуктов для моделирования, как OSM, VISSIM, VISUM и т.д. Для загрузки карты необходимо произвести следующие действия:

- 1) Найти и загрузить карту из Open Street Map (OSM)
- 2) Конвертировать карту в SUMO Network  
netconvert --osm-files map.osm -o test.net.xml
- 3) Добавить путь и дорогу в нетворк используя скрипты Python

```
randomTrips.py python PATHrandomTrips.py -n
test.net.xml -r test.rou.xml -e 50 -l py
PATHrandomTrips.py -n test.net.xml -r test.rou.xml -e
50 -l
```

4) Настроить файл конфигурации и запустить Network:

```
<configuration>
<input>
<net-file value="pak.net.xml"/>
<route-files value="pak.rou.xml"/>
</input>
<time>
<begun value="0"/>
<end value="2000"/>
</time>
</configuration>
```

5) Импорт карты и перенос её в netedit SUMO

6) Открытие карты для запуска симуляции в SUMO-gui

### 2.3 ОПРЕДЕЛЕНИЕ КРИТИЧНЫХ ОБЪЕКТОВ В СИМУЛЯЦИИ

После загрузки карты были выделены следующие критические объекты, рядом с которыми наиболее вероятно могут произойти опасные события, причиной которых может стать ВАТС:

- светофор
- пешеходный переход
- перекрёсток
- автобусная остановка
- детская площадка
- АЗС
- жилой дом
- школа

Итак, был сформирован список из 8 объектов, для выявления наиболее значимых. Далее эксперты проставляли баллы каждому объекту (таблица 1).

Таблица 1 – Матрица оценок

Эксперты	Критерии							
	Светофор	Пешеходный переход	Перекресток	Автобусная остановка	АЗС	Жилой дом	Школа	Детская площадка
1	h11=8	h12=8	h13=5	h14=7	h15=6	h16=9	h17=9	h18=9
2	h21=7	h22=6	h23=4	h24=8	h25=4	h26=8	h27=8	h28=9
3	h31=8	h32=8	h33=7	h34=7	h35=5	h36=7	h37=9	h38=8

Для дальнейших расчётов необходимо найти сумму оценок в каждой строке (таблица 2).

Таблица 2 – Сумма значений каждой строки

Эксперты	Критерии								Сумма
	Светофор	Пешеходный переход	Перекресток	Автобусная остановка	АЗС	Жилой дом	Школа	Детская площадка	
1	h11=8	h12=8	h13=5	h14=7	h15=6	h16=9	h17=9	h18=9	61
2	h21=7	h22=6	h23=4	h24=8	h25=4	h26=8	h27=8	h28=9	54
3	h31=8	h32=8	h33=7	h34=7	h35=5	h36=7	h37=9	h38=8	59

Далее разделив оценку на сумму, были получены веса  $g_{ik}$ , а затем рассчитана сумма каждого столбца (таблица 3).

Таблица 3 – Веса оценок

Эксперты	Критерии							
	Светофор	Пешеходный переход	Перекресток	Автобусная остановка	АЗС	Жилой дом	Школа	Детская площадка
1	0,1311475	0,131147541	0,161290323	0,1147541	0,098361	0,14754	0,14754	0,147541
2	0,1296296	0,092592593	0,074074074	0,14814815	0,074074	0,14815	0,14815	0,1666667
3	0,1355932	0,13559322	0,11864068	0,11864407	0,084746	0,11864	0,13559	0,1355932
Сумма	0,3963704	0,359333354	0,354008464	0,38154631	0,25718	0,41433	0,43128	0,4498009

В итоге были получены весовые коэффициенты каждого объекта (таблица 4).

Таблица 4 – Весовые коэффициенты объектов

	Светофор	Пешеходный переход	Перекресток	Автобусная остановка	АЗС	Жилой дом	Школа	Детская площадка
$r1/ri$	0,15	0,10	0,08	0,90	0,07	0,15	0,15	0,17

Таким образом, было установлено, что наиболее важными объектами являются: детская площадка, школа, жилой дом, светофор.

В дальнейшей работе будут описаны сценарии использования ТС с учётом полученных данных.

### 2.4 ПОЛУЧЕНИЕ РЕАЛЬНЫХ ДАННЫХ С ТРАНСПОРТНЫХ СРЕДСТВ

Определение данных дорожной обстановки, ориентированное на автомобиль (Floating Car Data). Floating Cars обозначает "плавающие вместе" в дорожной обстановке автомобили. Floating Cars собирают Floating Car Data (FCD), т. е. данные о дорожной обстановке. FCD – это выходной файл, содержащий местоположение, скорость, угол наклона транспортного средства, положение, полосу движения наряду с другой информацией для каждого транспортного средства в сети на каждом временном шаге [3].

FCD – это аналог GPS-устройства для каждого автомобиля. Выходные данные могут быть обработаны далее с помощью инструмента Tracer Exported tool (рисунок 3).

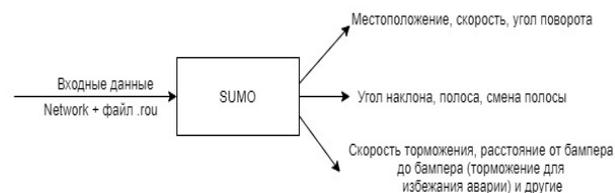


Рисунок 3 – Схема работы операции FCD

В командной строке пишем команду:  
`sumo-gui -n Your.net.xml -r Your.routes.xml --fcd-output Your.fcd-output.file.xml`

После запуска симуляции файл наполняется необходимой информацией

Симуляция начинается с нулевой секунды:

```
<timestep time="0.00">
<vehicle id="0" x="693.53" y="2103.92"
angle="190.21" type="DEFAULT_VENTYPE"
speed="0.00" pos="5.10" lane="155884644#2_0"
slope="0.00"/>
```

Например, описание движения автомобилей через 5 секунд после начала симуляции:

```
<timestep time="5.00">
```

```
<vehicle id="0" x="688.69" y="2077.05"
angle="190.21" type="DEFAULT_VEHICLE"
speed="8.81" pos="32.41" lane="155884644#2_0"
slope="0.00"/>
```

## 2.5 ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ДОРОГАХ

Файл xml содержит подробную информацию для каждого транспортного средства и каждого шага моделирования. Из-за высокого уровня детализации он очень гибкий, но часто требует дополнительного программирования для анализа и фильтрации действительно необходимой информации.

Для получения информации о том, на каких дорогах едут автомобили в каждую секунду времени, вводим в командную строку:

```
sumo -c pak.sumocfg --netstate-dump
my_dump_file.xml
```

Далее создается файл с названием: my\_dump\_file. Необходимо его открыть для просмотра информации.

## 2.6 ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СМЕНЕ ПОЛОСЫ ДВИЖЕНИЯ АВТОМОБИЛЯМИ

С помощью команды sumocfg мы можем отслеживать все события, когда транспортное средство переходит с одной полосы на другую (определяется как момент, когда центральная линия транспортного средства переходит в новую полосу движения). В нем также содержится основная причина этого маневра изменения.

Для получения информации о смене полосы движения автомобилями вводим в командную строку:

```
sumo -c pak.sumocfg --lanechange-output
my_lane_change_file.xml
```

После выполнения команды создается файл my\_lane\_change\_file. Для просмотра информации необходимо открыть файл.

Часть полученного кода смены полосы движения:

```
<lanechanges>
<change id="6" type="DEFAULT_VEHICLE"
time="12.00" from="-137148148#3_0" to="-137148148#3_1" dir="1" speed="12.70" pos="47.02"
reason="keepRight" leaderGap="None"
leaderSecureGap="None" leaderSpeed="None"
followerGap="None" followerSecureGap="None"
followerSpeed="None" origLeaderGap="None"
origLeaderSecureGap="None"
origLeaderSpeed="None"/>
```

Таким образом, были получены файлы, из которых извлекаются данные для создания сценариев:

- Net файл (net.xml) – сетевой файл.
- Route – файл маршрута, генерируется автоматически из файла потока и сетевого файла. Содержит конкретную информации о движении транспортных средств, выбор кратчайшего пути.
- Edge файл (edg.xml) – содержит информацию о дорогах. В качестве дорог выступают ребра между точками, содержащие идентификатор точки-начала, точки-конца, количество полос и скоростной лимит.

- Sumocfg файл – конечный конфигурационный файл. Файл Sumocfg используется для запуска симуляции дорожной сети.

При получении каждого из вышеперечисленных файлов проводился анализ на предмет выявления сценариев использования транспортных средств. На основе данных, полученных из симуляции, и анализа непосредственно запущенной симуляции разрабатывались сценарии в отдельных файлах согласно стандарту OpenSCENARIO.

ParameterDeclarations – это отдельный файл в формате .xml, который был использован для удобства, чтобы зафиксировать параметры, которые описывают движение ТС и координаты триггеров.

В файле «ParameterDeclarations» перечислены параметры, которые будут использоваться позже в виде имен параметров. Они включают координаты триггеров и основные характеристики ТС, такие как скорость, ускорение, замедление. Используя «ParameterDeclarations» наиболее удобно напрямую ссылаться на имена параметров, тем самым облегчая изменение и конфигурацию параметров. Ниже представлено описание файла «ParameterDeclarations».

Необходимо присвоить имена всем соответствующим параметрам. Так, начальная скорость целевого ТС должна быть задана следующим образом, например:

```
name="$A1_Speed1".
```

Далее необходимо выбрать тип параметра, например:

```
parameterType="double"
```

Затем необходимо задать величину каждому параметру, например:

```
value="0"
```

Файл «ParameterDeclarations» должен содержать все необходимые параметры и выглядеть следующим образом, например, для задания начальной скорости:

```
<ParameterDeclaration>
<ParameterDeclaration name="$A1_Speed1"
parameterType="double" value="0"/>
```

Файл «Scene Participants Entities» в формате .xml описывает участников сцены. Раскадровка Entities включает Performance и BoundingBox, которые описывают характеристики (максимальная скорость, ускорение) и форму (геометрический центр: длина и ширина) транспортного средства.

В файле необходимо задать имя объекта: <ScenarioObject name="A1">, название транспортного средства с выбором категории: <Vehicle name="XXX" vehicleCategory="car">. Затем, с помощью среды моделирования, необходимо определить скорость и ускорение ТС и записать в следующем виде: <Performance maxSpeed="22.22" maxAcceleration="5.2"/>.

Затем в раскадровке <BoundingBox> необходимо описать следующие параметры: <Center x="1.5" y="0.9"/> - где описываются длина и ширина ТС.

Initial State Storyboard->Init – раскадровка Init включает в себя статическое описание начальных условий сценария.

Init включает начальное состояние погодной среды (описанное в GlobalAction) и начальное состояние участников (описанное в Private). Среди них GlobalAction включает: TimeOfDay, например, год, месяц, день, час, минуту и секунду; Weather, например, состояние облачности, азимут солнца, видимое расстояние и коэффициент сцепления с дорогой. Private включает: состояние движения, такое как начальная скорость SpeedAction, описанная в LongitudeAction; положение, описанное в TeleportAction.

```
<Storyboard>
  <Init>
    <Actions>
      <GlobalAction>
        <EnvironmentAction>
          <Environment name="Environment1">
            <TimeOfDay animation="false" dateTime="2021-02-20 T 12:13:20"/>
            <Weather cloudState="free"/>
            <RoadCondition/>
            ...
          </GlobalAction>
        Private содержит состояние движения, такое как начальная скорость SpeedAction, описанная в LongitudeAction и положение, описанное в TeleportAction.
        <Private entityRef="A1">
          <PrivateAction>
            <LongitudeAction>
              <SpeedAction>
                <SpeedActionDynamics dynamicsShape="step" value="0" dynamicsDimension="time"/>
                <SpeedActionTarget>
                  <AbsoluteTargetSpeed value="$A1_Speed1"/>
                </SpeedActionTarget>
              ...
            </PrivateAction>
            <PrivateAction>
              <TeleportAction>
                <Position>
                  <LanePosition route cost="21.99" probability="1.00000000" edges="-21319337#1 -21319337#0 -46679182#1 -46679182#0"/>
                </Position>
                ...
              </PrivateAction>
            </Init>
```

Файл «Story» содержит изменения в поведении всех участников маневров. В Act изменения поведения описываются последовательно в соответствии с уровнем ManeuverGroup-> Maneuver-> Event. Основные изменения поведения описаны в Action. Условия, при которых происходит действие, описываются StartTrigger в разделе Event. Рассказовка «Story» для Сценария 1 представлена ниже, в данном примере A1 сбрасывает скорость до 0 при замедлении 4,6 м / с<sup>2</sup>.

```
<Story name="MyStory">
  <Act name="Act1">
    <ManeuverGroup maximumExecutionCount="1" name="Sequence1">
      <Actors selectTriggeringEntities="false">
```

```
<EntityRef entityRef="A1"/>
</Actors>
<Maneuver name="Maneuver1">
  <Event name="Event1" priority="overwrite">
    <Action name="Action1">
      <PrivateAction>
```

```
      Действие замедления TC (LongitudeAction) представлено в <SpeedActionDynamics dynamicsShape="linear" value="$A1_Rate" dynamicsDimension="rate"/>. В данном примере скорость изменяется линейно, с замедлением $A1_Rate (4,6 м / с2). Целевая скорость A1 находится в <SpeedActionTarget>.
      <LongitudeAction>
        <SpeedAction>
          <SpeedActionDynamics dynamicsShape="linear" value="$A1_Rate1" dynamicsDimension="rate"/>
          <SpeedActionTarget>
            <AbsoluteTargetSpeed value="$A1_Speed2"/>
          </SpeedActionTarget>
        ...
      </Action>
```

Условия замедления StartTrigger описаны в Condition Group. Когда условие изменяется с неудовлетворенного на удовлетворенное (TC достигает \$A1\_TriggeringDistance1), действие по замедлению начинает выполняться.

```
<StartTrigger>
  <ConditionGroup>
    <Condition name="StartCondition1" delay="0" conditionEdge="rising">
      <ByEntityCondition>
        <TriggeringEntities triggeringEntitiesRule="any">
          <EntityRef entityRef="A1"/>
        </TriggeringEntities>
        <EntityCondition>
          <TraveledDistanceCondition value="$A1_TriggeringDistance1"/>
        </EntityCondition>
        ...
      </ConditionGroup>
    </StartTrigger>
  <Maneuver>
    <Maneuver name="Maneuver2">
      <Event name="Event1" priority="overwrite">
        <Action name="Action1">
          <PrivateAction>
            <LongitudeAction>
              <SpeedAction>
                <SpeedActionDynamics dynamicsShape="angular" value="$A1_Rate2" dynamicsDimension="rate"/>
                <SpeedActionTarget>
                  <AbsoluteTargetSpeed value="$A1_Speed2"/>
                </SpeedActionTarget>
              ...
            </PrivateAction>
          </Action>
        <StartTrigger>
          <ConditionGroup>
            <Condition name="StartCondition2" delay="0" conditionEdge="rising">
              <ByEntityCondition>
```

```

    <TriggeringEntities
triggeringEntitiesRule="any">
    <EntityRef entityRef="A1"/>
    </TriggeringEntities>
    <EntityCondition>
    <TraveledDistanceCondition
value="A1_TriggeringDistance2"/>
    </EntityCondition>
    ...
</Maneuver
<Maneuver name="Maneuver3">
    <Event name="Event1" priority="overwrite">
    <Action name="Action1">
    <PrivateAction>
    <LongitudinalAction>
    <SpeedAction>
    <SpeedActionDynamics
dynamicsShape="linear" value="$A1_Rate3"
dynamicsDimension="rate"/>
    <SpeedActionTarget>
    <AbsoluteTargetSpeed value="$A1_Speed1"/>
    </SpeedActionTarget>
    ...
    </Action>
    <StartTrigger>
    <ConditionGroup>
    <Condition name="StartCondition1" delay="0"
conditionEdge="rising">
    <ByEntityCondition>
    <TriggeringEntities
triggeringEntitiesRule="any">
    <EntityRef entityRef="A1"/>
    </TriggeringEntities>
    <EntityCondition>
    <TraveledDistanceCondition
value="A1_TriggeringDistance3"/>
    </EntityCondition>
    ...
    </Act>

```

Описание Сценария 1 выполнено в полном объёме на всех уровнях абстракции. Проверка работоспособности всех XML файлов, представленных в работе, была выполнена с помощью экспорта файла в совместимый симулятор дорожной сети [4].

### 2.7 СЦЕНАРИИ НА УРОВНЕ АНАЛИЗА ПРИМЕНЕНИЯ

Для описанного выше сценария существует операционная возможность – управление. Пользователь имеет возможность управления транспортного средства с помощью системы управления ВАТС.

Для данной операционной возможности создается диаграмма деятельности по применению или Operational Activity diagram. Такие диаграммы показывают какую последовательность действий необходимо применить чтобы достичь поставленной цели. В дальнейшем именно эти диаграммы будет служить для создания сценариев на уровне операционного анализа. Рисунок 4 показывает диаграмму деятельности по применению

«Управление», элементы данной диаграммы описывают процесс достижения автоматического управления ВАТС. Анализ сценариев и построение всех диаграмм проводилось в среде моделирования Capella.



Рисунок 4 – Диаграмма деятельности «Управление» на уровне Анализа применения

Следующим этапом была представлена диаграмма архитектуры применения на уровне анализа применения (рисунок 5).

На диаграмме показаны взаимодействия между деятельностью, такими как «Набор скорости» (при смене полосы) и «Вывод информации» и другими, участниками – «Водитель», а также сущностями на примере «СУ ВАТС» и «Внешние датчики».

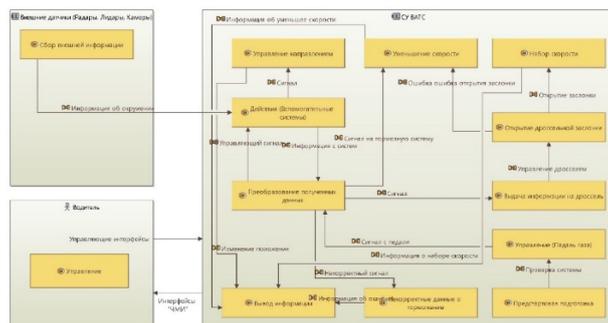


Рисунок 5 – Архитектура применения на уровне Анализа применения

Из диаграммы деятельности следуют сценарии применения или Operational Activity Scenario. Эти сценарии представляют собой диаграмму последовательных действий, по вертикальной оси отражается временная шкала. Они описывают деятельность и поведение объектов в контексте возможности применения. На рисунке 6 показана диаграмма сценария применения деятельности по применению «Управление». Наглядно видно последовательность действий и их поведение.

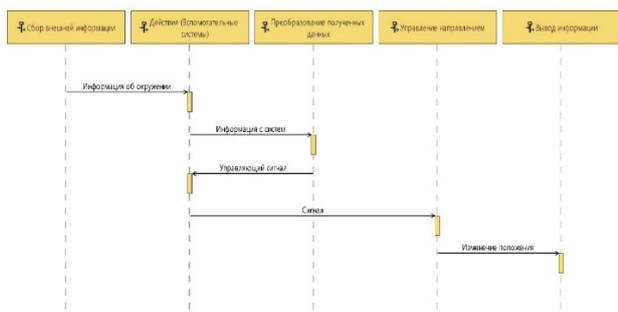


Рисунок 6 – Сценарий деятельности по применению «Управление»

## 2.8 СЦЕНАРИИ НА УРОВНЕ ФУНКЦИОНАЛЬНЫХ И НЕ ФУНКЦИОНАЛЬНЫХ ПОТРЕБНОСТЕЙ

Capella предоставляет несколько типов диаграмм на каждом уровне методологии ARCADIA:

- Functional Scenarios (FSs): на временных отрезках помещаются функции;
- Exchange Scenarios (ESs): на временных отрезках помещаются компоненты/акторы, а последовательностями взаимодействий являются функциональные или компонентные обмены;
- Interface Scenarios (ISs): на временных отрезках помещаются компоненты/акторы, а последовательности взаимодействий состоят из обмена элементами.

В данном случае была построена диаграмма функционального сценария (FS), включающего функциональные цепочки.

Функции представлены вертикальными линиями, а функциональные обмены – горизонтальными стрелками, упорядоченными последовательно сверху-вниз.

Диаграммы сценариев в Capella очень схожи с диаграммами последовательностей в UML/SySML. Поэтому на диаграмме возможно видеть сообщения с обратной связью. Также можно создавать синхронные/асинхронные варианты сообщений, использовать ограничения по продолжительности и так далее.

Функциональный сценарий системы управления ВАС для смены полосы движения автомобилем представлен на рисунке 7.

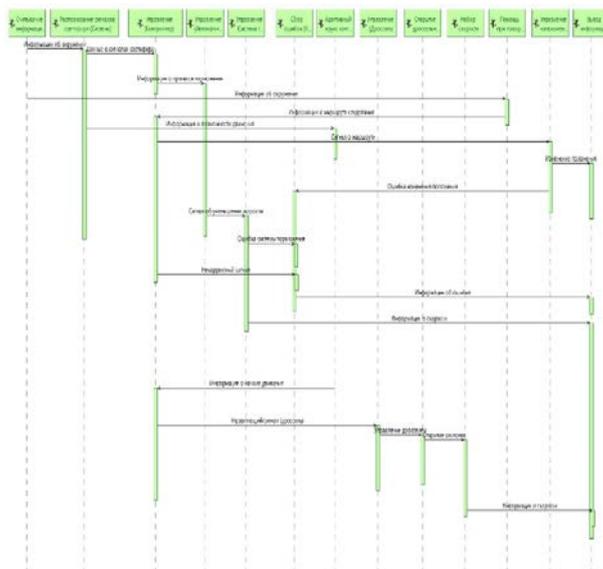


Рисунок 7 – Функциональный сценарий «Смена полосы движения автомобилем»

## 3 ЗАКЛЮЧЕНИЕ

В настоящее время влияние автомобиля на образ жизни человека приобрело самые широкие масштабы. Для повышения мобильности в будущем предполагается использование автономных транспортных средств. Чтобы сделать автономные автомобили максимально безопасными, необходимо гарантировать не-нанесение ими вреда человеку во всех возможных сценариях использования. А для этого необходимо рассмотреть и проанализировать каждую ситуацию! В связи с этим обсуждается метод выделения набора сценариев дорожных ситуаций, который затем, после анализа, позволит обеспечить безопасность на дорогах, а также чтобы справиться с растущим трафиком. Для обеспечения безопасности необходимо определить наиболее часто повторяющиеся сценарии, описать их на формальном языке, провести анализ опасностей и оценку рисков.

Разработка единого метода описания поспособствует развитию общепринятой и стандартизированной процедуры тестирования и утверждения функций автоматизированного вождения на практике. Процедура стандартизации в области тестирования и экспериментов необходима для получения одобрения более высокого уровня автоматизации.

## БИБЛИОГРАФИЯ

- [1] ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска – Москва: 2020. – 35 с.
- [2] ГОСТ Р ИСО 26262-3-2020 Дорожные транспортные средства. Функциональная безопасность. Часть 3. Стадия формирования концепции. – Москва: 2020. – 36 с.
- [3] Майоров В.И. Содержание понятия «Безопасность дорожного движения»: Теоретические основы // Вестник Южно-Уральского государственного университета. Серия: «Право». – 2012. – № 7. – с. 99-100.
- [4] Salinesi: Authoring Use Cases. In: I. F. Alexander, N. Maiden (Eds.): Scenarios, Stories, Use Cases – Through the Systems Development Life-Cycle, Wiley, Chichester, 2010.

[5] Becker, C. J., Brewer, J. C., & Yount, L. J. (2020, November). Safety of the intended functionality of lane-centering and lane-changing maneuvers of a generic level 3 highway chauffeur system (Report No. DOT HS 812879). National Highway Traffic Safety Administration.

Мишкина Анна Андреевна, студент МИРЭА - Российский технологический университет (РТУ МИРЭА), Институт кибернетики, кафедра системной инженерии, направление подготовки 27.04.03 «Системный анализ и управление», E-mail: mishkina.a.a@inbox.ru;

Кировский Олег Михайлович, Консультант, ООО «Сейфети Консалт», oleg.kirovskii@safetyconsult.tech;

Мозолин Игорь Александрович, студент ФГАОУ ВО «Национальный исследовательский университет МИФИ», Высшая инженеринговая школа, направление подготовки 27.04.03 «Системный анализ и управление», E-mail: mozolinia@gmail.com

# Creating a set of scenarios for the purpose of analyzing the functional safety of control systems

Anna Mishkina, Oleg Kirovsky, Igor Mozolin

**Abstract:** The article deals with the analysis of the functional safety of the control system of highly automated vehicles. The article proposes a method for describing scenarios for the use of vehicles, which can be used in hazard analysis and risk assessment - an integral part of the functional safety life cycle. A review analysis of research methods for describing scenarios according to the ASAM OpenScenario standard in the field of functional safety was carried out. The issues of the basics of functional safety according to the ISO 26262:2018 standard are considered. In addition, the main directions in the field of scenario modeling are considered. The description of the scenarios is essential for testing and verifying the safety of highly automated vehicles. However, in the real development process, the data formats and interfaces used by different manufacturers and vendors of simulation tools are diverse, and it is difficult to unify standards. The article discusses a method for extracting a set of traffic scenarios, which then, after analysis, will allow to ensure road safety, as well as cope with growing traffic. To ensure safety, it is necessary to identify the most frequently repeated scenarios, describe them in a formal language, and conduct a hazard analysis and risk assessment. The result of the work is a list of described use cases for the control system of highly automated vehicles.

**Keywords:** scenario, functional safety, analysis, control system, vehicle, traffic, requirement.

## REFERENCES

- [1] GOST R 58771-2019 Menedzhment riska. Tehnologii ocenki riska – Moskva: 2020. – 35 s.
- [2] GOST R ISO 26262-3-2020 Dorozhnye transportnye sredstva. Funkcional'naja bezopasnost'. Chast' 3. Stadija formirovanija koncepcii. – Moskva: 2020. – 36 s.
- [3] Majorov V.I. Soderzhanie ponjatija «Bezopasnost' dorozhnogo dvizhenija»: Teoreticheskie osnovy // Vestnik Juzhno-Ural'skogo gosudarstvennogo universitety. Serija: «Pravo». – 2012. – # 7. – s. 99-100.
- [4] Salinesi: Authoring Use Cases. In: I. F. Alexander, N. Maiden (Eds.): Scenarios, Stories, Use Cases – Through the Systems Development Life-Cycle, Wiley, Chichester, 2010.
- [5] Becker, C. J., Brewer, J. C., & Yount, L. J. (2020, November). Safety of the intended functionality of lane-centering and lane-changing maneuvers of a generic level 3 highway chauffeur system (Report No. DOT HS 812879). National Highway Traffic Safety Administration.