DOI: 10.25728/mlsd.2023.0981

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ВЫСОКОАВТОМАТИЗИРОВАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Королев А.С., Кировский О.М., Смирнов Б.С.
РТУ МИРЭА, Москва, Россия
korolev@mirea.ru, kirovskij@mirea.ru, bovan526@gmail.com

Аннотация: В статье рассмотрены подходы к управлению жизненным циклом высокоавтоматизированных транспортных средств с учетом задач по обеспечению их безопасности. Предложен метод системной инженерии для разработки безопасных систем и дан пример использования этого метода. Исследованы возможности инструментализации предложенного метода с целью автоматизации деятельности на стадиях жизненного цикла безопасных систем.

Ключевые слова: высокоавтоматизированные транспортные средства, безопасность систем, системная инженерия, моделе-ориентированная системная инженерия, управление жизненным циклом, ARCADIA.

Введение

В инженерии сложных, высокоавтоматизированных технических систем, использование которых может негативно повлиять на жизнь и здоровье людей, большое внимание уделяется обеспечению безопасности. Безопасность, согласно ГОСТ Р 57149-2016, определяется как нефункциональное свойство системы, отражающее соответствие величины риска для пользователей системы и людей в ее окружении приемлемому уровню.

Для обеспечения безопасности в разных отраслях развивается методическое обеспечение и разрабатываются стандарты, часть которых приобрели официальный статус на международном уровне.

К таким стандартам можно отнести:

- ГОСТ Р ИСО 26262-2015 – Функциональная безопасность. Дорожные транспортные средства.
- ISO 21448:2022 – Safety of the intended functionality.
- ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering.
- EN 50129:2003 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
- ГОСТ Р МЭК 61508-1-2012 – Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью
- ГОСТ Р МЭК 60880-2010 – Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А.
- ГОСТ Р МЭК 61226-2011 – Атомные электростанции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления.

Общепризнанные стандарты и методики обеспечения безопасности используют процессный подход, т.е. в них заданы стадии жизненного цикла (ЖЦ) системы и описаны конкретные работы, направленные на обеспечение безопасности, которые нужно проводить на каждой стадии. Также в стандартах описаны критерии, по которым система признается безопасной, и методы документации обоснования безопасности.

Можно выделить следующие проблемы в существующих практиках по разработке безопасных систем:

1. Неполное понятийное соответствие в стандартах и методиках разных отраслей;
2. Увеличение трудоемкости разработки систем при внедрении стандартов по безопасности;
3. Трудность в выявлении, определении и декомпозиции функций систем на всех уровнях иерархии;
4. Отсутствие полноценной инструментальной поддержки в виде программного обеспечения (особенно российской производства) на всех стадиях ЖЦ систем.

В данном материале авторы, ограничиваясь автомобильной отраслью, исследуют следующие вопросы:

- сопоставление понятий автономных систем в западных и российских стандартах, рекомендациях и нормативно-правовых актах;
- анализ общепризнанных на мировом уровне концепций по достижению безопасности автономных систем;
- описание процесса обеспечения безопасности автономных систем;
- выбор и применение метода системной инженерии для разработки безопасных систем;
- исследование возможностей инструментализации разработки.

Основным результатом представленных работ, актуальным для применения на предприятиях, является основанная на подходе моделе-ориентированной системной инженерии методика разработки систем с учетом обеспечения безопасности. Данная методика привязывается к типовым моделям жизненного цикла согласно стандарту ИСО 26262 и инструментализируется как в области функционального анализа системы с точки зрения безопасности, так и в области автоматизации таких методов доказательства (обоснования) безопасности, как FMEA, HARA, FTA.

1. Понятие ВАТС и проблема их безопасности

Понятие высокоавтоматизированного транспортного средства (ВАТС) в России определяют Проект Федерального закона о высокоавтоматизированных транспортных средствах [1] и Постановление Правительства РФ № 2495 от 29.12.2022 [2].

В западных источниках нет единого понятия транспортного средства, соответствующего российскому понятию ВАТС. Большую популярность приобрели понятия «Autonomous», «Self-Driving», «Driverless», «Unmanned», «Robotic». Рекомендации SAE J3016 [3] вносят подробные разъяснения в употребление этих терминов, а также дают общепризнанную классификацию систем по уровням автономности. В этом документе определено шесть уровней автономности в зависимости от распределения задач по управлению между системой автоматического управления (САУ) транспортного средства и человеком-оператором. В неавтономных ТС (ТС уровней автономности с нулевого по третий, L0 – L3) задачи по реагированию на неожиданные или опасные ситуации (fallback), возложены на водителя. В автономных ТС (уровни 4 и 5, L4 – 5) система автоматического управления сама в любых дорожных сценариях управляет движением, обнаруживает объекты и события и реагирует на них, а также гарантирует безопасность в экстренных случаях.

Анализируя тексты приведенных выше российских нормативно-правовых актов, можно сказать, что эти документы сокращают количество уровней автономности ТС по отношению к международным стандартам, которые базируются на рекомендациях SAE J3016, до трех уровней (табл. 1).

Таблица 1. Соответствие уровней автономности

SAE J3016	Российские правовые акты
Уровень 0	Обычный автомобиль, техническая безопасность которого регламентируется ТР ТС 018/2011 [4]
Уровень 1	
Уровень 2	
Уровень 3	ВАТС 1-й категории
Уровень 4	ВАТС 2-й категории
Уровень 5	

Согласно упомянутому выше постановлению Правительства РФ категории ВАТС определяются следующим образом:

- ВАТС 1 категории – высокоавтоматизированное транспортное средство, осуществляющее движение с водителем-испытателем, находящемся на месте водителя или переднем пассажирском сиденье;
- ВАТС 2 категории – высокоавтоматизированное транспортное средство, осуществляющее движение без водителя (в том числе, водителя-испытателя) в салоне при удаленных маршрутизации и диспетчеризации со стороны оператора.

Независимо от терминологических особенностей, в процессе создания и использования высокоавтоматизированных ТС при повышении уровня автономности характеристика безопасности системы становится одним из ключевых параметров. Если не будет приведено обоснование безопасности их использования, автономные транспортные системы не приобретут нужного уровня доверия и не получат разрешения на применение на дорогах общего пользования.

В отношении технических систем, имеющих в своем составе электрические и/или электронные системы (чаще всего это системы управления, основной риск для которых связан с их неправильным функционированием и следующими из него ошибочными командами оборудованию), современные стандарты, приведенные выше, разделяют безопасность на три вида: функциональная безопасность, кибербезопасность и безопасность целевой функции. На рис. 1 приведена привязка этих видов безопасности к предпочтительной методологии в области автомобильной техники.

Рис. 1. Виды безопасности систем и соответствующие стандарты [5]

Анализ свойства безопасности позволяет сделать следующие выводы для разработки и стандартизации высокоавтоматизированных систем:

1. Безопасность заведомо «невидима» пользователю, и он не может ее оценить до использования системы;
2. Безопасность не должна быть дополнительной опцией, она должна быть гарантирована для всех систем.
3. Методы обеспечения безопасности должны обсуждаться и внедряться не на уровне отдельных компаний-производителей, а на уровне экспертных сообществ, отраслевых объединений, или обеспечиваться государственными механизмами;
4. Для обеспечения безопасности должны применяться научные достижения и ведущие, общепризнанные методические подходы в этой области.

К признанным подходам и методам, применяемым в современной инженерии, относятся концепции, принципы и методы системной инженерии, включая моделе-ориентированную системную инженерию, а также подход жизненного цикла. Эти методы хорошо зарекомендовали себя в процессах разработки и обоснования безопасности других систем высокого риска, в частности, авиационных и медицинских. Актуальной задачей является применение этого инструментария совместно с признанными методами обоснования безопасности систем для эффективной разработки автономных систем, в частности ВАТС.

2. Управление жизненным циклом для обеспечения безопасности

2.1. Стратегия достижения безопасности

Важным аспектом современного производства является управление моделью жизненного цикла создаваемых систем, с целью обеспечения эффективности разработки с точки зрения всех заинтересованных сторон. Подход жизненного цикла является одним из подходов системной инженерии и задает основу применения метода системной инженерии. Жизненный цикл можно рассматривать как модель деятельности по созданию, эксплуатации и утилизации сложных систем. Основными шагами в реализации управления жизненным циклом являются:

- Установление стратегии управления ЖЦ;
- Определение модели ЖЦ;
- Формализация процессов на стадиях модели ЖЦ;
- Определение метода системной инженерии;
- Итеративное применение метода системной инженерии на всех стадиях ЖЦ системы.

Стратегия управления ЖЦ формируется как общая цель_развития системы и общие принципы и способы ее достижения. При определении наиболее эффективной стратегии управления жизненным циклом необходимо сформировать общие правила, в соответствии с которыми на надлежащим образом выстроенной методической основе будут устойчиво удовлетворяться потребности заинтересованных сторон [6].

В нашем случае, стратегия управления ЖЦ формируется с учетом обеспечения безопасности, как мы определили это понятие в разделах выше. Высокоуровневая стратегическая цель обеспечения безопасности будет служить, как мы увидим ниже, одной из основ для определения целей и

потребностей заинтересованных сторон на операционном уровне разработки архитектуры системы и затем декомпозироваться на требования к функциям системы в целом и отдельных ее модулей и компонентов.

2.2. Модели жизненного цикла

Если пользоваться международными стандартами по разработке безопасных систем, то, в основном, в них предлагается V-образная модель ЖЦ. При работе с такого рода моделями совокупность процессов обычно организуют с использованием стандарта ISO/IEC 15288 – «Системная и программная инженерия – Процессы жизненного цикла систем». Этот стандарт описывает процессы на достаточно абстрактном уровне, что очень удобно для адаптации процессов, но, с другой стороны, эти процессы трудно с ходу применить на практике. Поэтому техники реализации процессов нужно либо разрабатывать самостоятельно, либо искать их в других стандартах и рекомендациях. Относительно рассматриваемой предметной области это можно сделать, например, с использованием стандарта ISO 26262.

Хотя V-модель – это и распространенный вариант модели ЖЦ, но не единственный из тех, которые сейчас применяют на практике. Известны материалы, в которых делаются активные попытки применить гибкие методологии и соответствующие модели ЖЦ для разработки сложных систем с учетом безопасности. К одному из таких материалов относится [7].

Для показанного ниже примера применения метода системной инженерии совместно с методами обоснования безопасности мы взяли за основу классическую V-образную модель ЖЦ.

2.3. Метод системной инженерии

Под методом системной инженерии можно понимать систематическое, формализованное применение системного подхода в контексте инженерной деятельности по созданию сложных систем. Любой метод системной инженерии представляет собой совокупность действий, которая рекурсивно применяется по отношению к выделенным уровням структурной иерархии, когда результаты, полученные на одном из уровней, используются в качестве входов на следующих иерархических уровнях для получения более общих или более детальных результатов. Известно множество типовых методов системной инженерии. Они подробно описаны в учебниках, стандартах, рекомендациях и лучших практиках. Все методы системной инженерии можно разделить на три категории: классические методы; адаптивные методы; моделе-ориентированные методы.

В современной системной инженерии активно развивается моделе-ориентированный подход к разработке (Model-Based Systems Engineering – MBSE), при котором разработка систем ведется с применением моделей вплоть до выпуска изделия. Модели, обладающие достаточной степенью детализации и прошедшие верификацию и валидацию, используются в качестве заданий для разработки системы. Применение принципов MBSE позволяет выполнять верификацию и валидацию системы на ранних этапах проектирования и добиваться основных декларируемых системной инженерией преимуществ – снижению рисков, относящихся к бюджету и срокам проекта.

3. Пример применения метода системной инженерии при разработке безопасных систем

3.1. Операционный анализ

В качестве метода системной инженерии рассмотрим ARCADIA (Architecture Analysis & Design Integrated Approach), который применяет архитектурный подход к функциональному анализу систем в соответствии со стандартом ИСО/МЭК 42010 [8]. Этот метод задает правила для формирования архитектурных описаний, относящихся к одному из пяти слоев (уровней) анализа системы: операционному (Operational Analysis), анализу назначения системы (System Needs Analysis), логической архитектуре (Logical Architecture), физической архитектуре (Physical Architecture), иерархической структуре конечного изделия и контрактов на комплексирование системы (End Product Breakdown Structure and Integration Contracts level, EPBS). Capella является одним из инструментов, который совмещает язык построения архитектурных описаний системы, метод такого построения (ARCADIA) и программную реализацию системы поддержки [9].

На уровне операционного анализа изучается деятельность отдельных лиц или их групп, которые называются акторами (Actors), и сущностей (Entities), формулируется миссия, выявляются возникающие проблемы, ставятся цели и задаются операционные возможности (Operational Capabilities), необходимые для достижения поставленных целей.

Миссия, цели и операционные возможности формулируются в соответствии с установленной стратегией УЖЦ и с учетом системы показателей эффективности, для достижения которых будут разрабатываться и внедряться в процесс деятельности системные решения.

Например, миссия с учетом обеспечения безопасности может звучать следующим образом: «Обеспечение безопасного дорожного движения с приемлемой скоростью и комфортом водителя».

На рисунке 2 в качестве примера приведена диаграмма операционных возможностей, связанных с системой электрического усилителя руля в автомобиле (electric power steering – EPS).

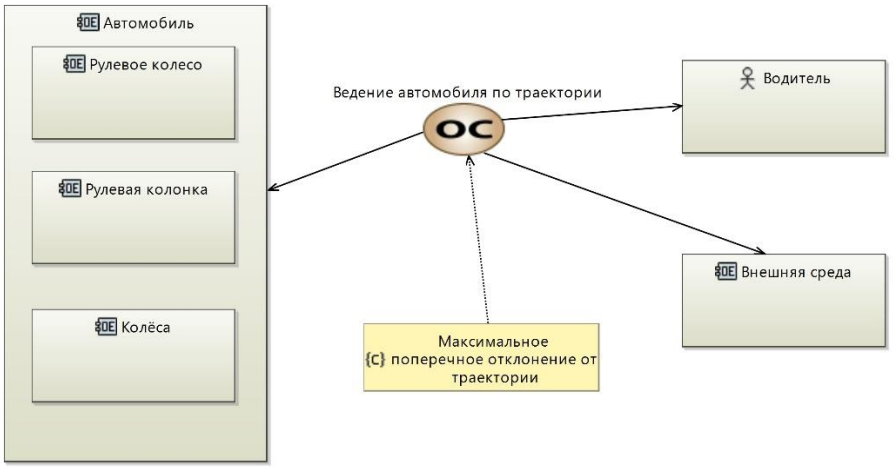

Рис. 2. Диаграмма операционных возможностей

На рисунке 3 показана архитектура операционной деятельности, на которой отображены операционные действия, совершаемые акторами и сущностями для выполнения операционной возможности «Ведение автомобиля по траектории».

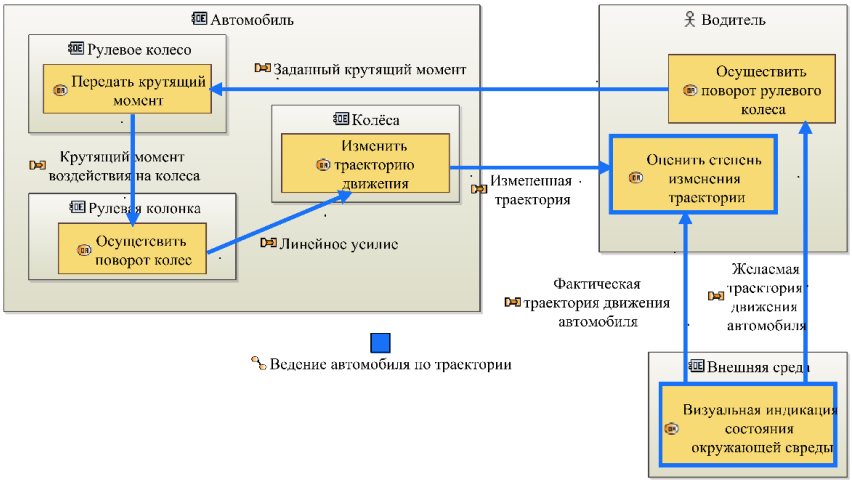

Рис. 3. Архитектура операционной деятельности

3.2. Выявление и декомпозиция функций

Выявление и декомпозиция функций по методике ARCADIA происходят на уровне анализа системы в целом, а также при проектировании логической и физической архитектур системы. Одновременно, моделируются требования к системе в целом, к логическим и физическим компонентам.

На рисунке 4 приведена архитектура на уровне назначения системы, где показаны функции системы в целом, реализующие установленные ранее операционные действия.

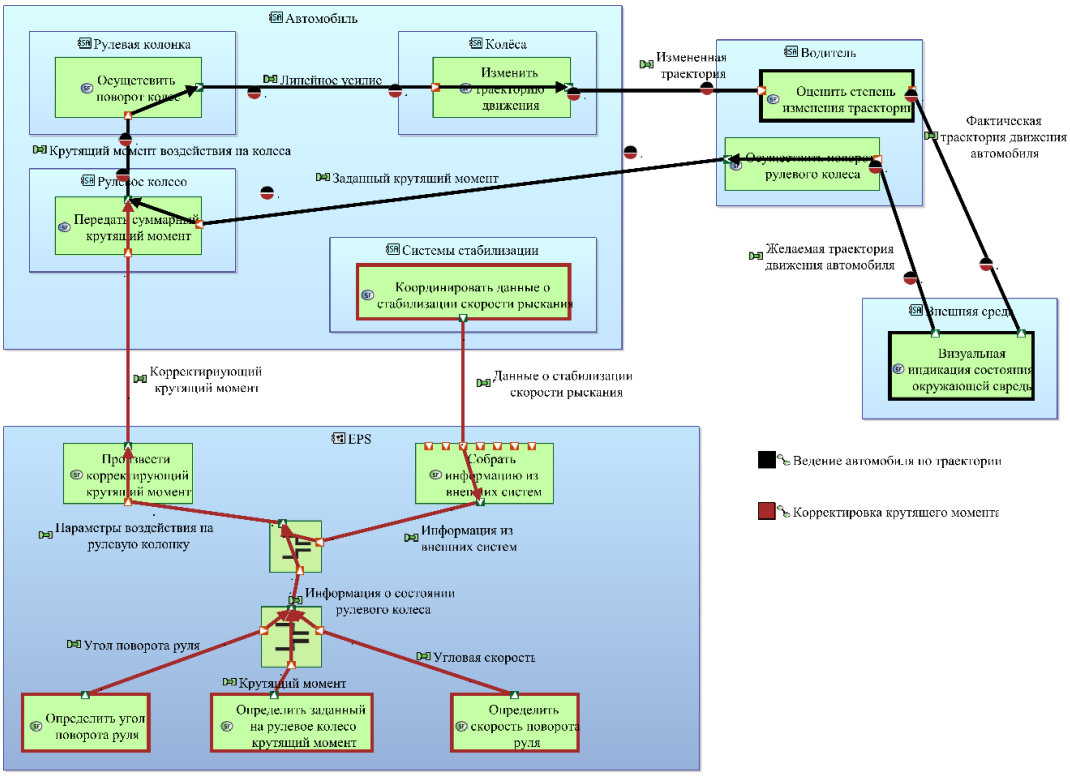

Рис. 4. Архитектура на уровне назначения системы

На рисунке 5 для примера приведена декомпозиция функции передачи крутящего момента на системном уровне.

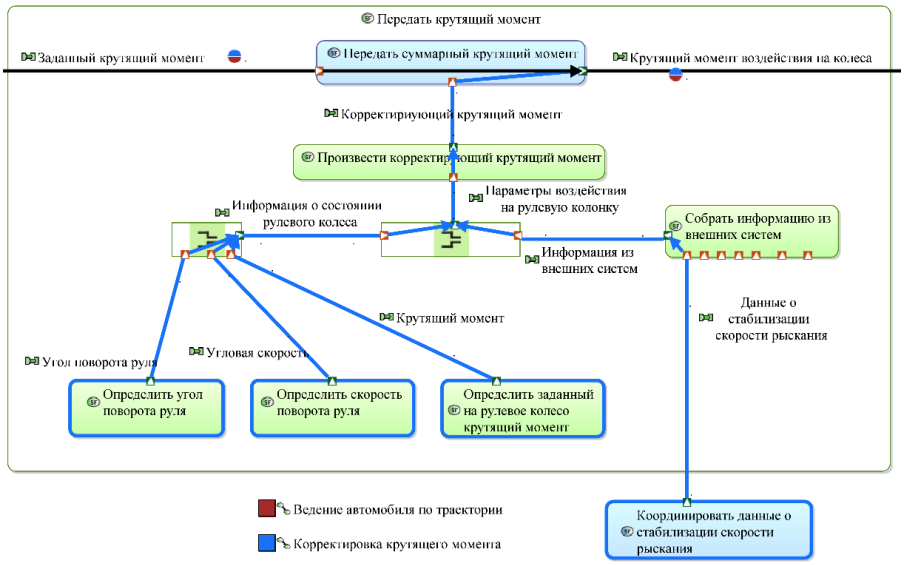

Рис. 5. Определение функции передачи крутящего момента на системном уровне

3.3. Применение методов обоснования безопасности

Результаты функционального анализа системы целесообразно интегрировать с методами анализа безопасности, в частности, анализом опасностей и оценкой рисков (Hazard analysis and risk assessment, HARA), анализом видов и последствий отказов (failure modes and effects analysis, FMEA), анализом дерева отказов (fault tree analysis, FTA). Подобная интеграция является шагом к автоматизации разработки безопасных систем на стадии концепции в жизненном цикле системы.

Анализ на уровне назначения системы по методике ARCADIA позволяет сформировать функции системы в целом, необходимые для HARA.

При разработке логической архитектуры раскрывается логика работы системы, при этом декомпозируются функции системы в целом и порождаются новые функции. Совокупность функций

на этом уровне позволит выполнить методы обоснования безопасности F-FTA, F-FMEA, т.е. FTA и FMEA на функциональном уровне.

При разработке физической архитектуры системы проводится дальнейшая декомпозиция, формулирование функций и распределение их по физическим элементам системы. Это дает возможность выполнить методы обоснования безопасности S-FTA, S-FMEA т.е. FTA и FMEA на системном уровне.

Таким образом, анализ устройства (системы или совокупности систем с выделенными функциями на уровне надсистемы) на функциональном и системном уровнях в инструментарии моделе-ориентированной системной инженерии может быть выполнен с учетом аспекта безопасности.

Автоматизация описанных выше процедур обоснования безопасности выполняется рядом зарубежных инструментов, особую популярность среди которых приобрел ANSYS medini analyze. Этот инструмент обладает рядом недостатков, среди которых следует отметить высокую цену лицензии, отсутствие в настоящее время технической поддержки в России, ориентированности на конкретные стандарты безопасности вместо общей методики, недостаточная поддержка моделе-ориентированной системной инженерии (процесс, воплощенный в инструменте, основан на создании и управлении требованиями). Поэтому актуальным является подход, позволяющий выгружать результаты функционального анализа в ARCADIA/Capella и формировать на основе них артефакты методов обоснования безопасности. На рисунке 6 показан сделанный авторами пример автоматического формирования таблицы FMEA на основе архитектурных описаний, полученных в Capella и выгруженных из нее на промежуточных этапах в формат XML.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Идентификационный номер	Предмет/ Функциональный Идентификатор	Вероятный дефект	Возможные последствия деффекта	Значимость(S)	Вероятная причина	Возникновение (O)	Методы контроля	Обнаружение (D)	RPN	Действия	Исполнитель	Результат			
2													S	O	D	RPN
3	01-01-02	Седло	Ослабление крепления седла	Падение седла во время езды, некомфорт	6	Неправильная эксплуатация, брак на производстве	3	Регулярная проверка крепления седла, использование качественных материалов	5	60	Проверить крепления, заменить дефектные детали	---	6	1	5	30
4	02-02-02	Рама	Трещина, разрыв	Рухнувшая рама, потеря контроля над велосипедом	8	Брак, перегрузка, удар, коррозия	2	Визуальный осмотр, неразрушающий контроль	4	64	Замена, сварка, антикоррозийная обработка	---	8	1	4	32
5	01-01-07	Педали	Сломанная или ослабленная педаль	Потеря управляемости велосипеда, травма ноги	7	Износ, неправильная эксплуатация, брак на производстве	3	Регулярная проверка педалей, использование качественных материалов	4	84	Проверить крепление педалей, заменить при необходимости	---	7	1	4	28
	01-01-04	Цепь	Растяжение или разрыв цепи	Внезапное остановление движения, падение	4	Износ, неправильная эксплуатация, недостаточное смазывание	5	Регулярная проверка и смазывание цепи, замена п	5	100	Проверить состояние и натяжение цепи, заменить при необходимости, регулярно смазывать	---	4	1	5	20

Рис. 6. Результат автоматического формирования таблицы FMEA на основе архитектурных описаний, полученных в Capella

4. Заключение

В статье была описана проблема управления жизненным циклом высокоавтоматизированных систем с учетом обеспечения свойства безопасности.

Рассмотрены особенности имеющихся на сегодняшний день формальных процессов обоснования безопасности систем на примере транспортных средств и указаны их ограничения.

Описан механизм применения принципов системной инженерии и подхода ЖЦ для создания эффективных систем с учетом их безопасности. В том числе, продемонстрировано, что с помощью инструментов моделе-ориентированной системной инженерии с использованием архитектурного подхода, может быть построено семейство цифровых моделей, полностью соответствующее набору информационных объектов, требуемых стандартами безопасности для создания аргументов безопасности.

В качестве инструментария моделе-ориентированной системной инженерии при создании сложных технических систем можно использовать ARCADIA/Capella – инструмент с открытым исходным кодом. Его можно, при необходимости, интегрировать с аналитическими методами и инструментами создания обоснования безопасности. В работе рассмотрены методические аспекты такой интеграции и

представлены примеры построения архитектурных описаний, функциональной декомпозиции и автоматического формирования некоторых артефактов обоснования безопасности.

Литература

1. Проект Федерального закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» – Режим доступа: https://regulation.gov.ru/projects#search=О высокоавтоматизированных транспортных средствах=116763, свободный.
2. Постановление Правительства Российской Федерации от 29.12.2022 № 2495 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации».
3. SAE J3016. Surface Vehicle Recommended Practice. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Sep 2016.
4. Технический регламент таможенного союза ТР ТС 018/2011 «О безопасности колесных транспортных средств». – утвержден Решением Комиссии Таможенного союза от 9 декабря 2011г. No877.
5. *Kirovskii, O., Gorelov, V.* Driver assistance systems: analysis, tests and the safety case. ISO 26262 and ISO PAS 21448. In: IOP Conference Series: Materials Science and Engineering, Volume 534, International Automobile Scientific Forum (IASF-2018), Intelligent Transport System Technologies and Components 18–19 October 2018, Moscow, Russian Federation. IOP Publishing Ltd (2018).
6. *Батоврин В.К.* О методических основах управления жизненным циклом сложных технических систем // XIII Всероссийское совещание по проблемам управления ВСПУ-2019: Труды [Электронный ресурс] 17-20 июня 2019 г., Москва / Под общ. ред. Д.А. Новикова. – М.: ИПУ РАН, 2019. – С. 3092-3097
7. *Thor Myklebust, Tor Stalhane*. The Agile Safety Case. Springer International Publishing AG 2018. − 242 pages.
8. *Jean-Luc Voirin.* Model-based System and Architecture Engineering with the Arcadia Method 1st Edition // ISBN: 9780081017944 ISTE Press – Elsevier. 2017.
9. *Pascal Roques.* Systems Architecture Modeling with the Arcadia Method // ISBN: 9780081017920 ISTE Press – Elsevier. 2018