Применение моделе-ориентированного подхода для управления процессом анализа функциональной безопасности

А.А. Сковикова, Д.В. Рязанов, О.М. Кировский, А.С. Королев

***Аннотация* — Данная статья посвящена проблеме анализа функциональной безопасности (ФБ) систем, чей отказ может повлечь за собой риски для жизни и здоровья пользователей. При росте количества компонентов и выполняемых функций растет сложность анализа безопасности. Так как анализ ФБ начинается на ранних стадиях ЖЦ системы, возможны частые изменения входных данных. В такой ситуации не обойтись без инструмента, позволяющего сократить количество ошибок проведенного анализа и модернизировать его при необходимости, минимизируя время на такие изменения.**

В данной статье предлагается описание инструмента управления процессом анализа ФБ, построенного с использованием моделе-ориентированного подхода. Преимуществом предлагаемого инструмента является минимизация количества ошибок анализа опасностей. Если пропустить такие ошибки на начальном этапе, обнаружить их будет возможно только на заключительных стадиях проектирования и разработки. Программный инструмент позволяет автоматизировать процесс работы с аналитикой ФБ и избежать неточностей, возникающих при ручном проектировании, снизить вероятность потери данных за счет создания хранилища данных. В статье подробно рассмотрены основные этапы разработки концептуального решения программного инструмента для проведения анализа ФБ. В первую очередь был смоделирован процесс анализа ФБ. Затем эта модель была оптимизирована. Требования и архитектура инструмента построены на основе оптимизированной модели процесса анализа ФБ.

***Ключевые слова* — функциональная безопасность, инструментальная поддержка, системная инженерия, ISO 26262**

I. Введение

Повышение безопасности, т.е. снижение риска смерти или вреда здоровью пользователей, является крайне важным аспектом разработки любой системы, в том числе автомобильной. Термин «*безопасность*» может толковаться по-разному. В случае с современными техническими системами, применяется определение из ГОСТ Р 57149-2016: «Безопасность – это свойство системы, заключающееся в отсутствии избыточного риска» [1]. Для удобства работы разделяют различные аспекты безопасности. Разделение проходит по релевантным источникам опасности. В данной работе рассматривается *функциональная безопасность (ФБ)* – аспект безопасности, нацеленный на исследование и устранением рисков, касающихся сбоев и отказов в работе электронных систем.

Для придания системе свойства функциональной безопасности необходимо выявить соответствующие требования, а затем воплотить, верифицировать и валидировать их. Такие требования выявляются в ходе анализа ФБ.

Основными этапами анализа функциональной безопасности являются:

1. **Идентификация потенциальных опасностей** – источники рисков определяются на основе исходных данных и моделирования возможных сценариев работы.
2. **Оценка вероятности опасных событий** проводится на основании статистических данных и опыта.
3. **Оценка возможного вреда** на жизнь и здоровье пользователей, на окружающую среду и имущество, также на основании статистических данных и опыта.
4. **Разработка мер** по устранению возможных рисков и повышению функциональной безопасности системы

Анализ ФБ выполняется чаще всего одним или несколькими аналитиками на основе нормативно-технической документации (стандартов и спецификаций). Это сложный процесс, требующий опыта, знаний о процедурах обеспечения ФБ, знаний о системе, коммуникативных навыков.

В качестве инструмента анализа ФБ используется либо офисное ПО общего назначения, либо специализированное ПО, являющееся по сути лишь СУБД, содержащей таблицы с необходимыми для анализа полями. На текущий момент не существует инструментального ПО для анализа ФБ, которое могло бы проверять правильность сделанных аналитиками выводов.

Ошибки при анализе ФБ называют в качестве вероятных причин серии ДТП с автомобилями Тойота [2], приведшей к смерти нескольких десятков человек, первого в истории «беспилотного» ДТП, при котором погиб человек, с участием беспилотника компании Uber ATG [3], и серии ДТП с автомобилями Tesla, вызванных неисправностью функции «автопилот» [4].

Статья получена 20 июля 2023.
А.А. Сковикова, магистр ВИШ НИЯУ МИФИ, anskovikova@gmail.com
Д.В. Рязанов, аспирант ИФТИС НИЯУ МИФИ, deniss.ryazanov@ya.ru
О.М. Кировский, ассистент РТУ МИРЭА, oleg.kirovskii@gmail.com
А.С. Королев, доцент НИЯУ МИФИ, заведующий кафедрой РТУ МИРЭА, askorolev@mephi.ru

II. АНАЛИЗ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ НА НАЧАЛЬНЫХ ЭТАПАХ РАЗРАБОТКИ СИСТЕМЫ СОГЛАСНО ГОСТ Р ИСО 26262.

Для обеспечения ФБ автомобильных систем следует использовать стандарт ИСО 26262 «Функциональная безопасность дорожных транспортных средств». В России этот стандарт гармонизирован как ГОСТ Р ИСО 26262. Далее перечислены шаги анализа ФБ на уровне концепции функциональной системы транспортного средства, как их описывает стандарт.

A. Определение устройства

Аналитику ФБ важно иметь четкое представление о том, как работают транспортное средство и его системы. На этапе определения устройства не проводят анализа, а собирают исходные данные.

Устройство - это система или набор систем, которые воплощают функции на уровне транспортного средства. Например, устройством является антиблокировочная тормозная система (функция: снижать пробег при торможении на скользкой поверхности), но не спидометр (он является частью устройства человеко-машинного интерфейса).

Определение устройства содержит следующие компоненты [5]:

- Название устройства и описание,
- Основная технология, на которой работает система (электронная/ электрическая/механическая и т. д.),
- Интерфейсы взаимодействия с другими функциями (как внешними, так и внутренними),
- Требования безопасности и известные виды отказов,
- Функциональная зависимость одного элемента от других

B. Анализ опасностей и оценка рисков (АООР)

АООР проводится на основании определения устройства. Его цель – получение целей безопасности, т.е. высокоуровневых требований безопасности для всего устройства. Для каждой цели безопасности должен быть определен уровень полноты безопасности транспортного средства (УПБТС), соответствующий этой цели.

УПБТС одновременно определяет два фактора: (1) насколько риск эксплуатации устройства до введения мер безопасности превышает допустимый и (2) какие меры безопасности нужно принять, чтобы риск эксплуатации устройства после их внедрения был приемлемым. В зависимости от УПБТС меняются релевантные для разработки требования стандарта ИСО 26262, целевые значения различных метрик (например, метрик вероятности опасных отказов) и также рекомендации по методам разработки. В стандарте ISO 26262 определены 5 уровней полноты безопасности: QM, A, B, C и D. Уровень A представляет собой самую низкую степень, а D – наивысшую степень снижения риска. УПБТС определяется зависит от значений следующих метрик:

Влияние (E): мера вероятности возникновения рассматриваемой дорожной ситуации, которая в сочетании с неисправностью может стать опасной.

Способность к контролю (C): определяет степень контролируемости ситуации, т.е. насколько водитель может своими действиями снизить риск при управлении транспортным средством в условиях неисправности.

Тяжесть (S): степень вреда, который может быть нанесен водителю и другим пассажирам в опасной ситуации.

Процесс АООР можно представить в виде следующих шагов:

- Идентификация всех соответствующих опасностей;
- Идентификация операционных сценариев, режимов, условий окружающей среды и т.д.;
- Объединение ситуации и неисправности, описание опасного события;
- Выполнение классификации опасных событий (определяются параметры S, E, C и уровень ASIL).
- Определение целей безопасности, которые охватывают все возможные опасные события.

C. Концепция функциональной безопасности

Концепция функциональной безопасности определяет более подробные требования, т.е. отвечает на вопрос «как система должна вести себя в случае отказа?». Кроме того, требования безопасности распределяются по предварительным компонентам архитектуры и системам в окружении. Основной концепции ФБ являются цели безопасности, полученные во время АООР.

III. МОДЕЛЕ-ОРИЕНТИРОВАННЫЙ ПОДХОД И ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Моделе-ориентированный подход при проведении анализа функциональной безопасности (Model-based approach for Functional Safety Analysis) представляет собой методологию, согласно которой процесс анализа функциональной безопасности рассматривается с точки зрения моделирования работы подсистем анализируемого продукта [6] .

Для применения данного подхода требуется использование аналитиком безопасности специализированных инструментов, дополненных модулями для анализа безопасности. Это позволяет проводить часть процессов анализа функциональной безопасности проводить в автоматическом режиме, сокращая время на проведение анализа и повышая его качество.

Моделе-ориентированный подход широко применяется для проектирования критических систем. При данном подходе разного рода процессы, такие как симуляция, верификация, тестирование, генерация кода (в случае наличия встраиваемого программного обеспечения), основываются на формализованной модели системы. Моделе-ориентированная разработка позволяет моделировать не только элементы встраиваемого ПО, но и электрические, электронные и механические элементы. Путем комбинирования моделей, состоящих из цифровых компонентов (аппаратное и программное обеспечение), с моделями механических компонентов (насосы, клапаны, генераторы и пр.) возможно создать единую модель, которая позволит симулировать номинальное поведение системы. Данная модель может быть масштабирована путем добавления любых дополнительных данных, образовывая в результате так

называемую расширенную системную модель, которая может точно представлять необходимые параметры системы [7] . Так, например, при обогащении модели дополнительными данными в области функциональной безопасности, надежности, ремонтопригодности, обслуживаемости она становится отличным источником исходных данных для проведения всех необходимых видов анализа и расчетов в этих предметных областях.

IV. Модификация процесса проведения анализа функциональной безопасности

Повысить качество анализа функциональной безопасности и снизить вероятность ошибок поможет автоматизация части процессов путем создания программного инструмента. До того, как приступить к автоматизации, необходимо идентифицировать и описать процессы ФБ, как их воплощают аналитики. Затем возможна модификация, чтобы учесть особенности автоматизированного исполнения.

Аналитики безопасности при проведении анализа функциональной безопасности автомобильных систем работают с проектной документацией, содержащей множество данных, которые необходимо перемещать из одного источника в другой, используя разные сервисы и приложения для работы при переходе между различными этапами анализа. Рассмотрим use-case диаграмму процесса анализа функциональной безопасности в общем виде AS IS (рис.1)

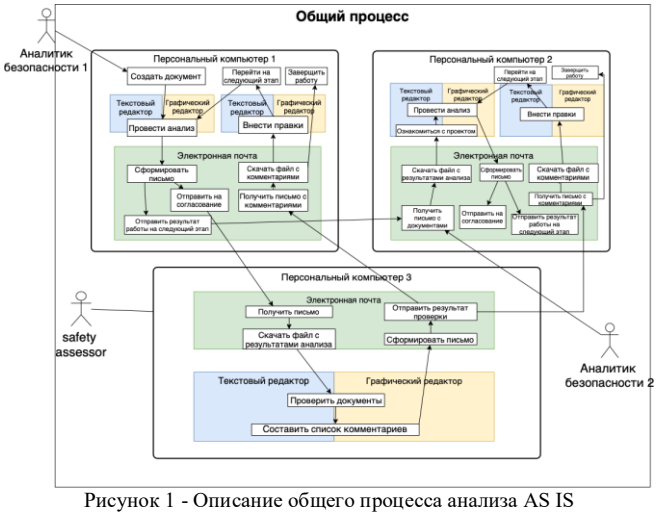

Рисунок 1 - Описание общего процесса анализа AS IS

Основный процесс, т.е. процесс анализа функциональной безопасности и согласования полученных результатов осложняется наличием большого количества рутинных процессов, которые непосредственно влияют на качество анализа и приводят к ошибкам.

Чтобы снизить вероятность ошибки, необходимо организовать работу аналитика безопасности таким образом, чтобы при проведении анализа функциональной безопасности фокус внимания был направлен на качестве анализа, а не на перенос данных из системы в систему и мониторинга писем с результатами работы коллег. Отсюда возникает потребность пересмотра концепции работы и размещения всех этапов анализа в рамках одного программного инструмента. Для этого необходимо выявить процессы, которые можно автоматизировать, проработать пути их оптимизации:

- Сохранение данных в текстовом документе;
- Перенос данных в графический инструмент;
- Обратных перенос данных в текстовый редактор;
- Перенос данных между этапами анализа;
- Отправка данных;
- Согласование результатов;
- Получение данных;
- Скачивание и обработка данных.

Рассмотрим u se case диаграмму процесса анализа функциональной безопасности в общем виде TO BE (рис. 2)

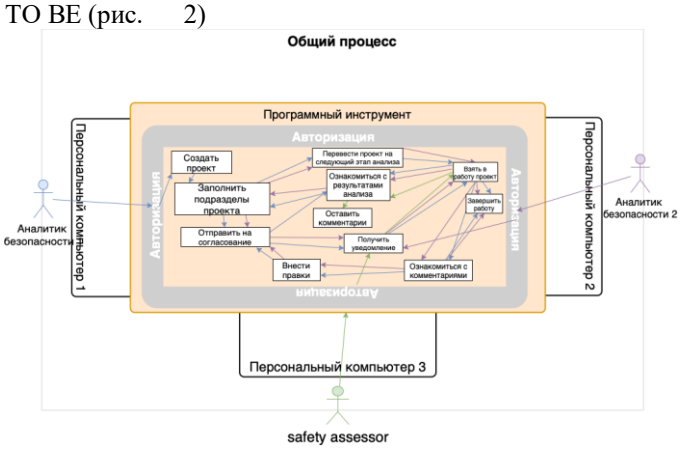

Рисунок 2 - Описание общего процесса анализа TO BE

Таким образом, можно сделать вывод, что использование программного инструмента для проведения анализа функциональной безопасности позволит сократить время и ресурсы специалистов в области анализа функциональной безопасности и позволит сфокусироваться на качестве анализа.

V. Логические компоненты и модель данных программного инструмента поддержки процесса анализа функциональной безопасности

Для достижения целей автоматизации процесс анализа функциональной безопасности был пересмотрен также с использованием моделе-ориентированного подхода. Внедрение этого подхода в процесс анализа возможно за счет создания единой реляционной базы данных, которая в дальнейшем может модернизироваться в единое интегрированное хранилище данных, представляющее собой распределенную базу с помощью объединения (или карты данных/индекса) разрозненных источников данных [8].

В ходе анализа представленных на схемах сценариев использования системы были выявлены следующие логические компоненты системы:

- Программный интрефейс;
- Подсистема ввода данных;
- Подсистема обработки данных;
- Подсистема построения графических элементов
- Подсистема анализа данных
- Подсистема вычислений
- Подсистема вывода данных

Логическая архитектура (рис 3) отражает взаимосвязь подсистем, выполняющих операционные функции и позволяющие автоматизировать процессы сохранения, обработки, передачи данных между этапами анализа функциональной безопасности, а также расчет значения ASIL и выявления опасных значений, которые требуют дополнительной обработки аналитиком.

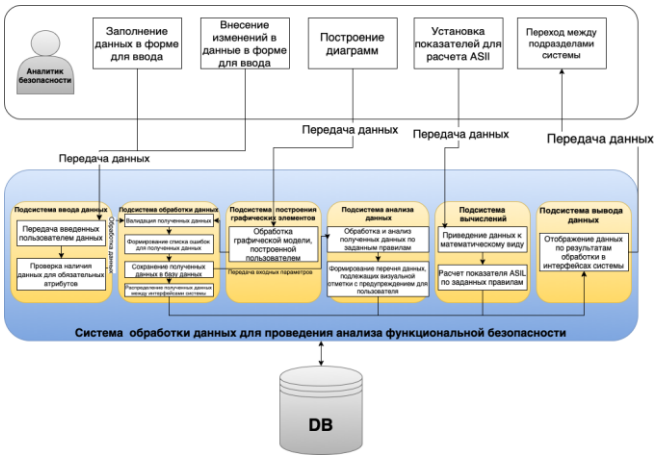

Рисунок 3 – Логическая архитектура подсистем программного инструмента

Разработка модели потока данных (рис 4) для программного инструмента для анализа функциональной безопасности согласно ISO 26262 включает создание и хранение артефактов анализа на всех этапах, начиная от выявления пожеланий и требований заинтересованных сторон, заканчивая проверкой соответствия системы этим требованиям и подтверждением соответствия.

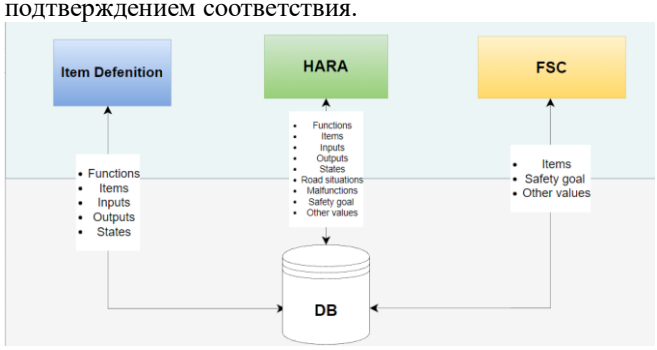

Рисунок 4 – Модель потока данных между интерфейсами системы

Важно учесть взаимосвязи и зависимости между элементами данных, а также осуществлять трассируемость, что обеспечивает согласованность на всех этапах жизненного цикла и оценку влияния изменений в любом элементе на всех этапах [8].

VI. Заключение

Использование единой программной среды позволяет объединить процессы на всех этапах анализа в единую систему. Программный инструмент позволит реорганизовать процесс анализа функциональной безопасности в нелинейную структуру, благодаря которой у аналитика появится возможность выполнения всех этапов анализа в произвольном порядке без риска снижения качества анализа из-за потери данных.

Таким образом, для российского рынка необходима разработка инструмента, обладающего следующими ключевыми преимуществами перед существующими инструментами:

- Выполнение всех этапов анализа функциональной безопасности на этапе концепции (ISO 26262) в рамках одного сервиса;
- Митигация риска потери данных вследствие потери носителя;
- Оптимизация процесса проведения анализа путем автоматизации части процессов;
- Снижение вероятности ошибки при анализе путем автоматического контроля наполненности данных;
- Сокращение времени на согласования правок и их исправление;
- Продукт не имеет российских аналогов;
- Продукт имеет потенциал для развития (ядро многих сервисов в данной предметной области).

Требования к разрабатываемому программному инструменту для проведения анализа функциональной безопасности выстроены учетом моделе-ориентированного подхода. Модель данных представляет собой организованное взаимодействие между этапами процесса анализа функциональной безопасности. Разработка единой реляционной базы данных масштабируема и учитывает дальнейшую возможность модернизации в единое интегрированное хранилище данных.

Библиография

[1] ГОСТ Р 57149-2016 Аспекты безопасности. Руководящие указания по включению их в стандарты .

[2] Купман, Ф. "A Case Study of Toyota Unintended Acceleration and Software Safety". Carnegie Mellon University, 2014.

[3] Uber’s Incident and Crucial Brake Wire Systems for Autonomous Vehicles [Электронный ресурс]. URL: https://www.automotive-iq.com/autonomous-drive/articles/ubers-incident-and-crucial-brake-wire-systems-autonomous-vehicles (дата обращения: 10.05.2023)

[4] Национальный Совет по Безопасности Транспорта (NTSB). News Release. (2020). NTSB Issues Safety Recommendations for Heliports and Helipads After Investigating Fatal 2018 Medical Helicopter Crash [Электронный ресурс]. URL: https://www.ntsb.gov/news/press-releases/Pages/NR20200225.aspx (дата обращения: 10.05.2023)

[5] ISO 26262 Дорожные транспортные средства. Функциональная безопасность. Стандарт ИСО (2020 г.)

[6] H. Peukert, M. Broy, F. W. von Henke, Model-Based Testing of Automotive Systems: The ARTIST Approach, Springer, 2012.

[7] Келли, Т.: Системный подход к управлению случаем безопасности. В: Учеб. Всемирный конгресс Общества автомобильных инженеров (SAE) (2004 г.)

[8] H. Peukert, M. Broy, F. W. von Henke, Model-Based Testing of Automotive Systems: The ARTIST Approach, Springer, 2012

Applying model-oriented approach for functional safety analysis management

A.A. Skovikova, D.V. Ryazanov, O.M. Kirovsky, A.S. Korolev

***Abstract* — Functional safety analysis of complex systems is a large and important task. The more complex is the system, the more effort is required to analyze it. As the functional safety analysis starts very early in the system lifecycle, a lot of modifications in the analyzed system are to be expected, with the respective impact on the analysis. A software tool is required to facilitate the analysis and the implementation of changes while reducing the number of errors and minimizing the time analysts spend on the formalities. These goals can be achieved by model-based approach both to safety analysis and the specification. The model-based approach includes modelling of the "as is" process, optimization performed on the process model, and finally the implementation of the tool is based on the optimized process model.**

***Key Words* — functional safety, software tool, model-based system engineering, model-based safety assurance, MBSE, MBSA, ISO 26262**

REFERENCES

[1] GOST R 57149-2016 Safety aspects. Guidelines for including them in standards.

[2] Koopman, F. "A Case Study of Toyota Unintended Acceleration and Software Safety". Carnegie Mellon University, 2014.

[3] Uber's Incident and Crucial Brake Wire Systems for Autonomous Vehicles [Electronic resource]. URL: https://www.automotive-iq.com/autonomous-drive/articles/ubers-incident-and-crucial-brake-wire-systems-autonomous-vehicles (accessed 05/10/2023)

[4] National Transportation Safety Board (NTSB). News release. (2020). NTSB Issues Safety Recommendations for Heliports and Helipads After Investigating Fatal 2018 Medical Helicopter Crash [Electronic resource].URL:https://www.ntsb.gov/news/press-releases/Pages/NR20200225.aspx (accessed 05/10/2023)

[5] ISO 26262 Road vehicles. functional safety. ISO standard (2020)

[6] H. Peukert, M. Broy, F. W. von Henke, Model-Based Testing of Automotive Systems: The ARTIST Approach, Springer, 2012.

[7] Kelly, T.: A systems approach to security case management. In: Study. Society of Automotive Engineers (SAE) World Congress (2004)

[8] H. Peukert, M. Broy, F. W. von Henke, Model-Based Testing of Automotive Systems: The ARTIST Approach, Springer, 2012