УДК 629.039.58

ПОСТРОЕНИЕ ДЕРЕВА ОТКАЗОВ КАК ЧАСТЬ ВАЛИДАЦИИ АРХИТЕКТУРЫ СИСТЕМЫ В МОДЕЛЕ-ОРИЕНТИРОВАННОЙ СИСТЕМНОЙ ИНЖЕНЕРИИ

А.С. Королев
МИРЭА – Российский технологический университет
Россия, 119454, Москва, просп. Вернадского, 78
E-mail: korolev@mirea.ru

О.М. Кировский
МИРЭА – Российский технологический университет
Россия, 119454, Москва, просп. Вернадского, 78
E-mail: kirovskij@mirea.ru

И.А. Ржаных
МИРЭА – Российский технологический университет
Россия, 119454, Москва, просп. Вернадского, 78
E-mail: rziluhaalyh@gmail.com

Ключевые слова: дерево отказов, диаграмма архитектуры, анализ безопасности, анализ дерева отказов, АДО, FTA.

Аннотация: В докладе рассматриваются методы и средства моделе-ориентированной системной инженерии для разработки интеллектуальных транспортных систем. Рассмотрен пример функционального анализа и анализа безопасности для интеллектуальной транспортной системы (ИТС) «Умный светофор». Выбранная система относится к области обеспечения безопасности дорожного движения и требует анализа связанных с ней рисков. Для обоснования безопасности выбран метод анализа дерева отказов (FTA). Расчет дерева отказов позволяет подтвердить правильность разработанной архитектуры с точки зрения достижения безопасности. Построение архитектурных решений производится по методологии ARCADIA, позволяющей выполнять моделирование на разных уровнях описания архитектуры систем. Для моделирования использован инструмент Capella с открытым исходным кодом. Показаны перспективы интеграции функционала Capella и инструментов построения деревьев отказов**.**

1. Введение

Сложные технические системы разрабатываются для достижения как функциональных, так и нефункциональных свойств. Функциональное свойство состоит в достижении какой-либо целевой функции, например, «перемещение на определенное расстояние в конкретных условиях окружающей среды». Нефункциональные цели включают достижение надежности, обеспечения доступности, простоты, гибкости, легкости сопровождения и т.д. В данной статье мы рассматриваем нефункциональное свойство безопасности. Безопасной называется система, в которой отсутствует

избыточный риск. Для создания безопасных систем применяются различные методы безопасной разработки. Основными источниками по этим методам для сложных систем являются международные стандарты.

В данной статье мы будем рассматривать стандарт ГОСТ Р ИСО 26262 «Функциональная безопасность дорожных транспортных средств», описанный в нем жизненный цикл системы безопасности (ЖЦ ФБ) и один из рекомендованных в указанном стандарте методов обеспечения безопасности – анализ дерева отказов (АДО, англ. Fault Tree Analysis, FTA).

2. Моделирование ИТС «Умный светофор»

2.1. ИТС «Умный светофор»

Одной из наиболее применяемых сегодня в России ИТС является система «Умный светофор» [4]. «Умный светофор» может работать в следующих режимах:

- Локальный режим предполагает автономную работу светофора по заранее заложенной программе;
- Координированное управление обеспечивает синхронную работу нескольких светофоров в связке;
- Адаптивный режим подразумевает, что светофор в реальном времени получает информацию, на основании которой проводит анализ ситуации на дороге, и подстраивает свою работу под нее. Именно этот режим и рассматривается далее.

2.2. Моделирование ИТС по методологии ARCADIA

При создании сложных систем общепризнанным стало применение подхода моделе-ориентированной системной инженерии (MBSE). На стадии разработки концепции в жизненном цикле (ЖЦ) систем это подразумевает построение так системной (архитектурной) модели. Существует ряд методов и инструментов, обеспечивающих эту деятельность, среди которых важное место занимает метод ARCADIA (Architecture Analysis and Design Integrated Approach) [5], позволяющий проводить функциональный анализ системы и разрабатывать соответствующие архитектурные описания. Этот метод поддерживается своим языком моделирования и программным инструментом – Capella, который функционирует на ядре Eclipse и носит характер open-source приложения.

2.3. Интеграция MBSE с методами обоснования безопасности

На стадии разработки концепции системы с учетом безопасности результаты функционального анализа целесообразно интегрировать с методами обоснования безопасности, в частности, с анализом рисков (HARA) и другими видами анализа: анализом видов и последствий отказов (АВПО, FMEA) и анализом дерева отказов (АДО, FTA). Цель интеграции – автоматизировать процедуру разработки безопасных систем на стадии концепции.

На рис. 1 показана V-модель ЖЦ системы безопасности согласно стандарту ГОСТ Р ИСО 26262 и соответствующие архитектурные слои метода ARCADIA.

Рис. 1. Метод ARCADIA в V-модели ЖЦ системы безопасности.

2.4. Результаты моделирования

Моделирование по методу ARCADIA начинается с операционного анализа. На этой стадии системы еще не существует, описывается только деятельность, в которой будущая система может принять участие. Анализ безопасности на этой стадии предполагает определение возможных опасных ситуаций и допустимого риска. Архитектура этого уровня приведена на рис. 2.

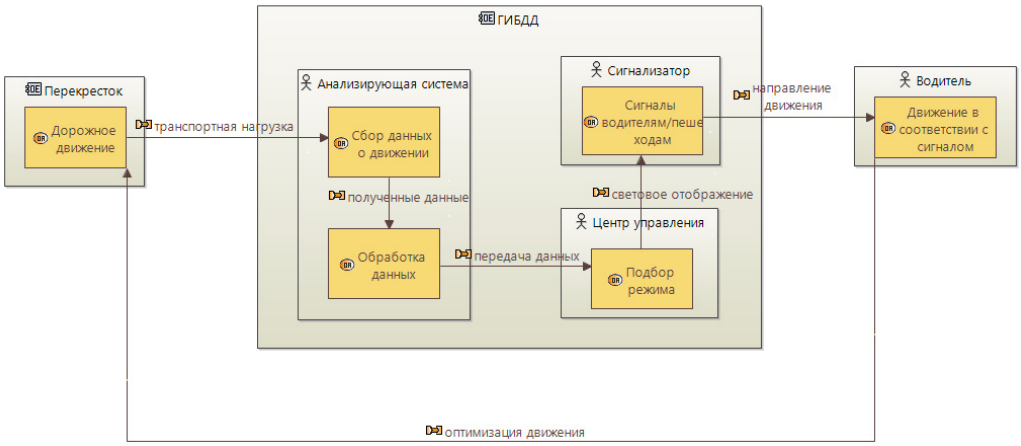

Рис. 2. Архитектура операционного уровня (OAB).

Из рис. 2 видно, что опасные ситуации в данном случае могут быть связаны с неверными сигналами о разрешенном направлении движения, которые вызовут неверную реакцию водителей.

Архитектура системного уровня, показанная на рис. 3, содержит функции системы. На этом уровне начинается работа по стандартам безопасности: проводится анализ опасностей и оценка рисков и т.д. Здесь же происходит первая функциональная декомпозиция.

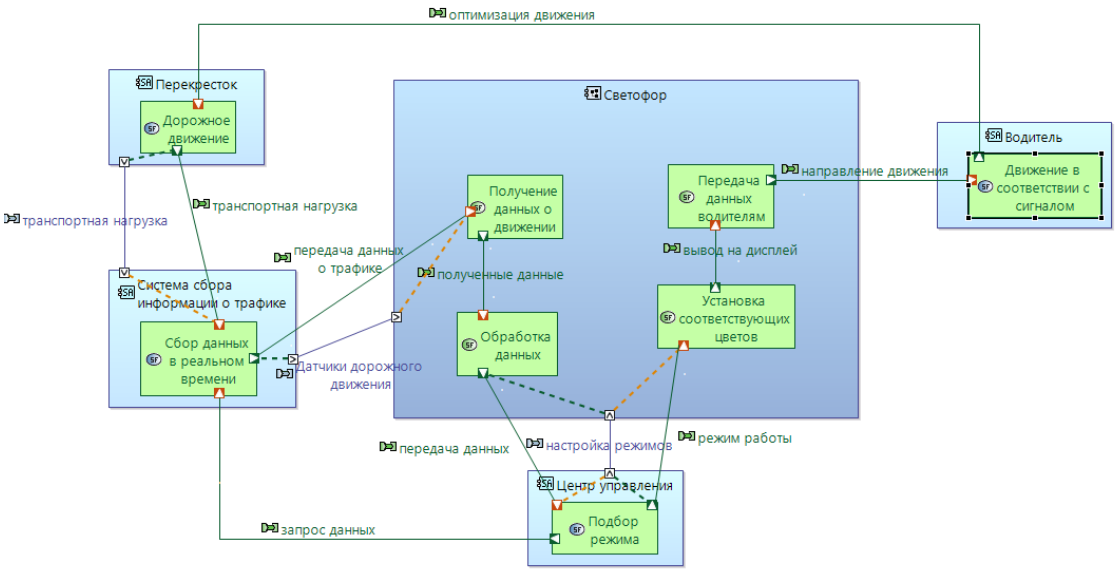

Рис. 3. Архитектура системного уровня (SAB).

2.5. Отказы и элементы архитектуры

Под отказами на всех уровнях имеется ввиду неверное функциональное поведение (malfunction) для функций соответствующего архитектурного уровня. Для выявления функциональных отказов используется метод HAZOP (hazard and operability). Суть метода состоит в использовании ключевых слов, отражающих специфический тип отклонения от необходимой функции.

2.6. Анализ дерева отказов (FTA)

FTA (Fault Tree Analysis) — это один из инструментов, применяемых в рамках жизненного цикла функциональной безопасности в соответствии с ГОСТ Р ИСО 26262. Цель этого метода – на этапе проектирования определить, как системы могут выйти из строя, определить лучшие способы снижения риска и определить (или почувствовать) событие.

FTA является дедуктивным («сверху вниз») анализом отказов, в котором заранее определенное нежелательное функциональное поведение системы анализируется с использованием алгебры логики для объединения серии событий нижнего уровня. В качестве событий рассматриваются отказы системы. Поскольку данный метод является дедуктивным, это означает, что сначала рассматривается отказ системы, а затем определяется, какие сбои могли к нему привести.

Для создания дерева отказов используются логические вентили «И», «ИЛИ», «Исключающее ИЛИ» и т.д., которые соединяют различные события (отказы) в зависимости от их влияния на систему. Анализ дерева отказов основывается на комбинации логических операций, вероятностных оценок и данных о надежности компонентов системы.

На рис. 4 в качестве примера изображено дерево отказов для события «Светофор не выводит сигналы». На этом дереве видны другие события, приводящие к верхнему и различные отказы, которыми вызваны интересующие события.

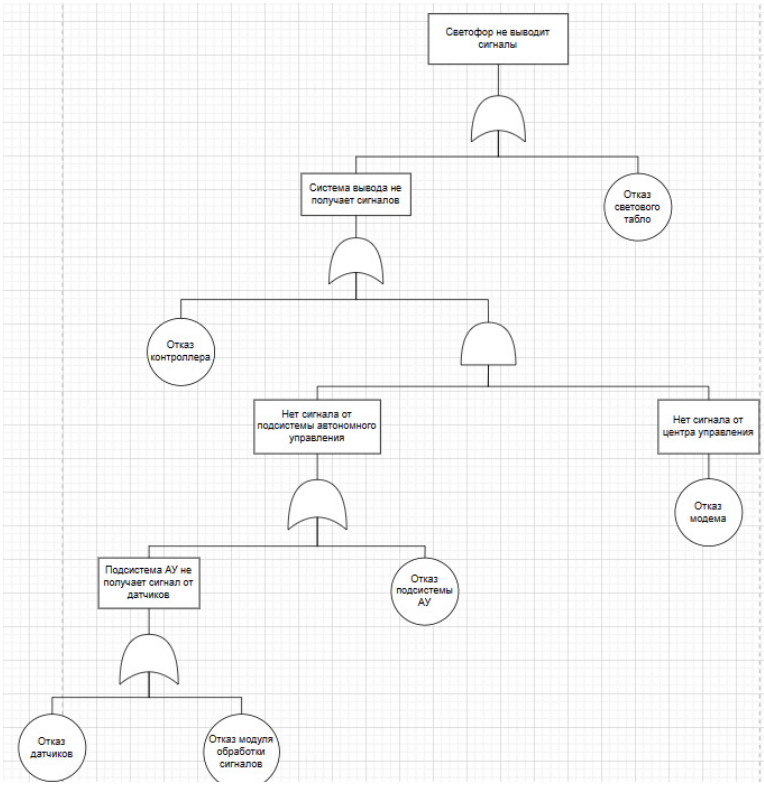

Рис. 4. Дерево отказов 1.

3. Интеграция архитектурных описаний и инструментов построения деревьев отказов

Анализ дерева отказов – аналитическая техника, в которой сначала описывается нежелательное событие (обычно в форме описания опасного состояния системы), а затем проводится поиск всех возможных путей, которыми система может прийти к этому состоянию и/или которыми может случиться это событие.

Проблемным местом применения существующих методов обоснования безопасности, включая указанные выше, является точность и полнота входных данных. Например, часто возникают сложности с описанием функций на всех уровнях декомпозиции системы, начиная от проблем, потребностей, целей и операционных возможностей на уровне операционной архитектуры и заканчивая функционалом физических элементов системы. Кроме того, без автоматизации деятельности по функциональному анализу системы является затруднительным выполнять такой анализ для сложных технических систем с сотнями и тысячами функций на всех уровнях декомпозиции.

Методология ARCADIA позволяет автоматизировать обоснование безопасности систем на этапах ЖЦ, относящихся к стадии разработки концепции.

4. Заключение

В статье продемонстрировано использования метода ARCADIA и инструмента Capella для анализа безопасности ИТС по стандарту ГОСТ Р ИСО 26262. Реальная область применения описанных методов и инструмента в моделе-ориентированной инженерии безопасности гораздо шире. ARCADIA и Capella позволяют создать единую

среду для системного моделирования, начиная с операционного уровня и до уровня аппаратного и программного обеспечения.

Список литературы

1. ГОСТ Р 57149-2016 Аспекты безопасности. Руководящие указания по включению их в стандарты. М.: Стандартинформ, 2016. 13 с.
2. ГОСТ Р ИСО 26262-2020 Функциональная безопасность дорожных транспортных средств – введен с 01.06.2021 взамен ГОСТ Р ИСО 26262-2014. М.: Стандартинформ, 2020 – XI. 402 с.
3. ISO 21448:2022. Road vehicles – Safety of the intended functionality. Geneve, International Organization for Standardization, 2022. 181 p.
4. Крылова, Е.И. Интеллектуальные транспортные системы. «Умный» светофор, «умный» перекресток // Аэрокосмическое приборостроение и эксплуатационные технологии: Сборник докладов Второй Международной научной конференции. С.Пб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. С. 115-118.
5. ГОСТ 27.302-2009. Надежность в технике. Анализ дерева неисправностей.