4. Формальная грамматика [Электронный ресурс]. – Режим доступа: https://ru.wikibooks.org/wiki/Формальная_грамматика, свободный (дата обращения: 04.04.2021)

5. Альбомы форм первичной учетной документации (распоряжение ОАО "РЖД" № 2017р от 12.09.11) [Электронный ресурс]. – Режим доступа http://scbist.com/dokumentaciya/38279-albomy-form-pervichnoi-uchetnoi-dokumentacii-rasporyazhenie-oao-rzhd-2017r-ot-12-09-11-a.html, свободный (дата обращения: 04.04.2021)

А.В. Озеров, А.М. Ольшанский

ПОДХОДЫ К ОЦЕНКЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ АВТОМАТИЧЕСКОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПОЕЗДОМ БЕЗ МАШИНИСТА

(АО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте»)

В настоящее время в разных странах мира, включая Россию, тестируются решения в области автоматизации пассажирских перевозок на железнодорожном транспорте с переходом к беспилотному управлению[1,2].

В отличие от систем управления метрополитена, системы городского железнодорожного транспорта вынуждены решать указанные задачи иными средствами, в том числе за счет стационарных и бортовых подсистем автоматического обнаружения препятствий, использующих методы машинного обучения при принятии управляющих решений. Введение последних в контур управления заметно усложняет общую задачу анализа угроз и оценки безопасности столь многоконтурной системы управления, связанной с безопасностью людей. Данная задача не может быть решена с помощью традиционных методов анализа угроз FTA и FMEA.

Постановка задачи

Цель данной статьи – разработка новой методологии анализа уровня безопасности сложных многоконтурных систем, состоящих из не полностью контролируемых контуров управления, подсистем и блоков. В практическом плане данная методология может быть использована при оценке безопасности системы управления без машиниста, которая планируется к внедрению на Московском центральном кольце (МЦК).

Ключевые факторы, создающие угрозу функциональной безопасности сложной системы, можно описать следующим перечнем:

- потеря команд или ошибка при подаче внешней входной информации
- неполнота, несовместимость, некорректность процессной модели
- ошибки алгоритма управления (дефект генерации, в изменениях процесса (сценарных, очевидно), нарушения адаптивности, обучаемости, неправомерные

изменения, ошибки в оценке состояния системы, ошибки идентификации системы);

- неподходящие, ошибочные или отсутствующие управляющие команды;
- не подходящие процессу действия мишени или механизма;
- неадекватные ответы сенсора и наблюдателей;
- неподходящие, ошибочные или отсутствующие обратные связи;
- неточные измерения или задержки обратной связи;
- задержки при передаче управления, потери в подаче на вход или входная ошибка;
- отказы компонентов, не распознанные внешние шумы/команды, их возможное наложение.

Основные предпосылки построения новой методологии:

1. Разбиение на элементарные подсистемы и анализ деревьев ошибок для каждой подсистемы не учитывает взаимодействия данных подсистем.
2. При функционировании сложной системы может случиться событие, при котором, несмотря на физически исправные составные подсистемы, произойдет неполное взаимодействие или несколько одновременных задержек, действие внешних факторов, которое вызовет непредусмотренную реакцию анализируемой системы.
3. Сложность и трудоемкость полного анализа событий в системе.
4. Одновременно с этим действия сложных систем не могут быть признаны Марковскими, следовательно, применять аппарат Марковских случайных процессов для анализа безопасности некорректно. Не определен также входной и выходной алфавит, а также правила формализации состояний для цифровых двойников, ассоциированных с Марковскими моделями и описываемых в [3].

Методология оценки безопасности на основе STPA

Согласно [4], при создании модели безопасности сложной системы строится многоуровневая система управления, включающая описания и разграничения функциональной ответственности между компонентами системы. Верхний иерархический уровень представляет собой контроллер (управляющий элемент) с процессной моделью. Процессная модель генерирует команды управления через отношения в пространстве состояний и вычисленный алгоритм управления, который доводится до нижних структур (мишеней-исполнителей). Мишени и прочие устройства низового уровня сообщают через устройства обратной связи о выполнении команд более высокого уровня. Верхний контроллер адресуется к модели безопасности и, сравнивая ее с поступившей обратной связью, корректирует внутреннее состояние модели.

При такой модели безопасности вероятность инцидентов сводится к ситуациям, когда внутреннее состояние и обратная связь в процессной модели не согласуются между собой. Такая модель является релевантной по отношению к функциональной структуре рассматриваемой системы, учитывает взаимоотношения между блоками и выглядит как развитие многоуровневых схем управления.

Предлагаемая методология базируется на методе STPA, согласно которому строятся контуры управления, контуры обратной связи, мишени-исполнители, сенсоры и управляющие процессы, устанавливаются отношения между ними, которые могут выступить ограничениями в области безопасности, проектируемые как заранее системно определенные случаи (конструкцией и структурой самих подсистем). Непосредственно анализируя риски через соответствующую управляющую процессную модель, необходимо оценивать требования к безопасности и все возможные управляющие решения для каждой части системы, чтобы идентифицировать потенциально опасные управления и усовершенствовать уровень безопасности и ограничения, не позволяющие проявиться опасному поведению от таких управлений.

Сам метод STPA («системно-теоретический анализ процессов») стал развитием модели STAMP («системно-теоретические модели и процессы аварий»), предложенной в 2004 году Левесон и основанной на теории управления. Метод активно используется в авиации, ядерной энергетике и др. отраслях, связанных с особыми требованиями безопасности и сложными системами. Последовательность применения метода состоит из 4 шагов, указанных на рис. 2 [5]:определение рисков и угроз, построение структуры управления, определение небезопасных управляющих действий, определение причин небезопасного управления.

Очевидно, что на первом шаге необходимо построить карту сценариев для всей сложной системы с правилами перехода из одного сценария к другому. Такие сценарии могут включать в себя запускающие события, которые приводят к ущербу [6].

На втором шаге необходимо построить полную структурную схему рассматриваемой системы управления. Так, на МЦК система управления реализуется как многоконтурная система управления, в которой предполагаются два режима управления – «автономный» и дистанционный («режим телеуправления») [7]. Помимо традиционной системы обеспечения безопасности на основе рельсовых цепей, в контуре управления предусматривается взаимодействие по радиоканалу стационарных и бортовых комплексов управления и обеспечения безопасности движения поездов, а также решаются задачи автоматического обнаружения препятствий бортовыми и стационарными устройствами визуального контроля с применением искусственных нейронных сетей с передачей соответствующей информации в центр дистанционного контроля и управления (ЦДКУ). Общая схема построения предполагаемой системы управления МЦК представлена на рис. 5:

Третий шаг исследования самый трудоемкий – формирование и описание угроз функциональной безопасности в соответствии с перечнем для каждого блока системы на различных иерархических уровнях. Для работы с полученными угрозами введем следующие обозначения: Sc – общее количество предварительных причинных сценариев, которое получено комбинаторным путем (так обеспечивается 100% охват всех устройств и их сочетаний), Mod – множество устройств в контурах управления, влияющих на функциональную без-

опасность системы, F – множество опасных (отказных) режимов, R – матрица отношений между устройствами и отказными режимами, предполагается, что каждое устройство инцидентно само с собой, т.е. минимальная сумма баллов в строке каждого устройства составляет 1 (единицу).

В данном случае применим с небольшими изменениями, касающимися реализации на том или ином языке программирования, алгоритм, предложенный в [8] для формирования библиотеки причинных сценариев с помощью исключения нереальных сценариев.

Таким образом, с учетом введенной нотации, получаем следующую последовательность действий по описанию угроз функциональной безопасности:

0. В результате обработки полной библиотеки сценариев, построенных по оговоренным синтаксическим правилам, формируются множества Mod, F.

1. Создадим R как матрицу ($|Mod|, |F|$); мощность множества F превосходит величину общего числа отказных режимов, так как один и тот же отказный режим содержится в нескольких сценариях. На первом этапе $|F| \gg |M|$.

2. Если в строке матрицы R содержится более, чем одна единица, то это говорит о том, что то или иное устройство из M, записанное в данной строке, участвует в нескольких отказных режимах.

3. Далее производится поиск одинаковых столбцов, это говорит о том, что отказные режимы в этих столбцах совпадают. Их можно включить в один итоговый сценарий.

4. Таким образом формируется библиотека актуальных сценариев.

Такие сценарии могут быть сформированы на всех структурных уровнях рассматриваемой системы. В рамках генерального подхода основные этапы анализа функциональной безопасности выглядят следующим образом:

1.Целевое составление типичных сценариев, проектирование иерархической структуры управления, диаграмм информационных потоков.

2.Идентификация причин опасностей.

3.Разработка мер безопасности.

Иерархическая структура управления представляет собой графическое изображение уровней управления, ключевых сигналов по отношению к нижним звеньям и сигналов от таких звеньев, учитывая в пределе сенсоры, двери, человека, микроконтроллеры. Затем для выбранных блоков и устройств описывается поведение в нормальном и аварийном сценариях в таком формате: к примеру, «в нормальных условиях, блок N системы X обеспечивает (гарантирует) объекту заданное свойство в заданном диапазоне».

Набор подобных утверждений в отношении элементов структурной иерархической схемы делает простым и доступным построение таблицы небезопасных управляющих действий (небезопасных управлений). Формат описания задается таблицей: опасности на системном уровне/управляющие действия/не исполняются/неверно исполняются/управление слишком раннее или слишком позднее/время исполнения данного управления слишком малое или слишком долгое. Последние 4 рубрики и составляют небезопасные сценарии (управляю-

щие действия). Для каждого небезопасного управления описывается комплекс «причина – ограничение», при этом ограничение описывает принципы безопасного поведения в той или иной ситуации при выбранных небезопасных управлениях. Например, контур «центр дистанционного контроля и управления ЦДКУ – поезд – стационарный комплекс обнаружения препятствий СКОП» содержит в себе, как минимум, 2 источника небезопасного управления: это сигнал из ЦДКУ, который может не поступить на поезд, и система СКОП, которая может не отправить запрос или отправить его слишком поздно. В результате связь становится критическим источником риска для всей системы транспортного обслуживания МЦК.

Заключение

Таким образом, в статье показаны недостатки методик локального анализа рисков и предложен универсальный новый подход на основе сочетания методологии системно-теоретического анализа процессов STPA и теории управления. Проиллюстрированы основные этапы такого анализа и сформирована первичная методика выполнения анализа безопасности транспортных систем. Намечен подход к анализу безопасности системы транспортного обслуживания МЦК.

Литература

1. https://www.uitp.org/publications/world-report-on-metro-automation/
2. IEC 26690:2014. Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts.
3. Шубинский И.Б., Шебе Х., Розенберг Е.Н. О функциональной безопасности сложной технической системы управления с цифровыми двойниками // Надежность. Том 21, №1 (2021).
4. Qi Y., Cao Y., Sun Y. Safety analysis on typical scenarios of GTCS based on STAMP and STPA //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2020. – Т. 768. – №. 4. – С. 042042.
5. Chaima Bensaci, Youcef Zennir, Denis Pomorski. A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System. European Conference on Electrical Engineering & Computer Science, EECS 2018, Dec 2018, Bern, Switzerland. hal-02014905.
6. ISO/PAS 21448:2019 (SOTIF). Road Vehicles – Safety of the Intended Function.
7. Попов П.А. Развитие отечественных и зарубежных беспилотных технологий // Автоматика, связь, информатика. №9 (2020), с.6 – 12.
8. Yan F., Zhang S., Tang T. Autonomous Train Operational Safety assurance by Accidental Scenarios Searching //2019 IEEE Intelligent Transportation Systems Conference (ITSC). – IEEE, 2019. – С. 3488-3495.