Оригинальная статья
https://doi.org/10.21683/1729-2646-2021-21-2-31-37

О построении модели безопасности сложной автоматической системы транспортного обслуживания

Алексей В. Озеров[1]*, Алексей М. Ольшанский[1]
[1]АО «НИИАС», Москва, Российская Федерация
*a.ozerov@vniias.ru

Алексей В. Озеров

Алексей М. Ольшанский

Резюме. Цель *статьи – рассмотреть подходы к анализу модели безопасности сложных многоконтурных систем транспортного обслуживания, состоящих из не полностью контролируемых подсистем.* **Методы.** *Для описания модели безопасности используются методы системно-теоретического анализа процессов STPA и принципы, изложенные в стандарте ISO/PAS 21448:2019 (SOTIF).* **Результаты.** *В статье показаны недостатки методик локального анализа рисков FTA и FMEA и продемонстрирована необходимость более универсального подхода на основе сочетания методологии системного анализа и теории управления. Проиллюстрированы основные этапы такого анализа модели безопасности сложных систем транспортного обслуживания на примере Московского центрального кольца, обеспечивающие обратную связь для оценки безопасности планируемой структуры системы управления. Рассмотрен вариант схемы управления с виртуальной моделью в виде так называемой «контролируемой искусственной нейронной сети».* **Выводы.** *В настоящее время активно тестируются системы беспилотного управления (без машиниста) на железнодорожном транспорте, которые имеют в своем составе модули автоматического обнаружения препятствий, использующие методы машинного обучения. Введение последних в контур управления крайне усложняет задачу анализа рисков и угроз и оценку безопасности таких систем с помощью традиционных методов построения деревьев ошибок и анализа отказов и их последствий FTA и FMEA. При построении модели безопасности столь сложных многоконтурных систем транспортного обслуживания, состоящих из не полностью контролируемых подсистем, в которых используются методы машинного обучения с не до конца предсказуемым поведением, требуется применение системного подхода для анализа небезопасных сценариев с формированием библиотеки сценариев и формализацией описания модели угроз, в том числе на границах различных контуров управления, в целях сокращения области неизвестных небезопасных сценариев для проектируемых систем беспилотного транспортного обслуживания.*

Ключевые слова: *железнодорожный транспорт, беспилотное управление, модель безопасности, метод STPA, машинное обучение, искусственная нейронная сеть (ИНС).*

Для цитирования: *Озеров А.В., Ольшанский А.М. О построении модели безопасности сложной автоматической системы транспортного обслуживания // Надежность. 2021. №2. С. 31-37. https://doi.org/10.21683/1729-2646-2021-21-2-31-37*

Поступила *23.03.2021 г. /* **После доработки** *12.05.2021 г. /* **К печати** *21.06.2021*

1. Введение

В настоящее время в разных странах мира, включая Россию, тестируются решения в области автоматизации пассажирских перевозок на железнодорожном транспорте с переходом к беспилотному управлению. На данный момент полностью автоматический режим управления (без машиниста и персонала на борту поезда) пассажирскими поездами реализован только в метрополитене. По данным UITP [1], в таком режиме функционирует 64 линии метрополитена в 42 городах мира.

В стандарте IEC 26690:2014 [2] описаны общие требования к автоматической системе управления для наземного городского железнодорожного транспорта и предложена следующая «градация уровней автоматизации» (Grades of Automation) системы (рис. 1).

Очевидно, что при повышении уровня автоматизации и переходе к полностью автоматическому режиму управления возникают дополнительные риски безопасности, требующие оценки и учета при формировании концепции функциональной безопасности данной сложной системы управления, объединяющей в своем составе большое количество подсистем.

В отличие от систем управления метрополитена, в котором ограничен доступ на путь посторонних лиц и объектов, а также легче решаются вопросы посадки/высадки пассажиров за счет использования платформенных дверей, 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 и без того сложную общую задачу анализа угроз и оценки безопасности столь многоконтурной системы управления, связанной с безопасностью людей. Данная задача не может быть решена только с помощью традиционных методов анализа угроз FTA и FMEA.

2. Постановка задачи

Цель статьи – рассмотрение новых подходов к анализу модели 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, ошибки сценарных изменений процесса, 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;

Уровень автоматизации	Режим эксплуатации	Отправление поезда	Движение и остановка поезда	Открытие / закрытие дверей	Управление в нештатных ситуациях
GoA1	Система безопасности с участием машиниста	Машинист	Машинист	Машинист	Машинист
GoA2	Системы безопасности и автоведения с участием машиниста	Машинист или автоматически	Автоматически	Машинист	Машинист
GoA3	Без участия машиниста	Автоматически	Автоматически	Проводник или автоматически	Проводник
GoA4	Без поездной бригады на борту	Автоматически	Автоматически	Автоматически	Автоматически

Рис. 1. Уровни автоматизации (GoA) режимов эксплуатации на железнодорожном транспорте

- задержки при передаче управления, потери в подаче на вход или входная ошибка;

- отказы компонентов, не распознанные внешние шумы/команды, их возможное наложение.

К основным предпосылкам формирования нового подхода к построению модели безопасности сложных систем транспортного обслуживания можно отнести следующее:

Разбиение на элементарные подсистемы и анализ деревьев ошибок для каждой подсистемы не учитывает взаимодействия данных подсистем.

При функционировании сложной системы может случиться событие, при котором, несмотря на физически исправные составные подсистемы, произойдет неполное взаимодействие или несколько одновременных задержек под действием внешних факторов, которые вызовут непредусмотренную реакцию анализируемой системы.

Сложность и трудоемкость полного анализа событий в системе.

Недостаточность классической модели построения двухканальной системы безопасности при использовании в одной или нескольких подсистемах искусственных нейронных сетей. Необходимость применения дополнительных методов обеспечения безопасности, как, например, реализация решающего алгоритма на основе цифрового двойника. При этом введение в состав системы цифрового двойника (или виртуальной модели) – совершенно новый и не апробированный подход к обеспечению безопасности системы, требующий дополнительных исследований (см. Шубинский И.Б. и др. [3]).

3. Методология оценки безопасности на основе STPA

Согласно Qi Y. и др. [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 Левесон [5] и основанной на теории управления. Метод активно используется в авиации, ядерной энергетике и других отраслях, связанных с особыми требованиями безопасности и сложными системами. Последовательность применения метода состоит из 4 шагов, указанных на рис. 2 (см. Chaima Bensaci и др. [6]):

Рис. 2. Последовательность применения метода STPA

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. В соответствии со стандартом ISO/PAS 21448:2019 (SOTIF) [7], необходимо учитывать 4 типа сценариев, представленных на рис. 3.

При построении модели безопасности сложной системы задача состоит в обеспечении максимального покрытия всех сценариев и сведении количества сценариев небезопасного управления до приемлемого уровня. Применительно к системе транспортного обслуживания МЦК может быть предложен базовый набор эксплуатационных сценариев 1-2 типа, которые должны учитываться при построении модели безопасности с формированием общей библиотеки сценариев (рис. 4).

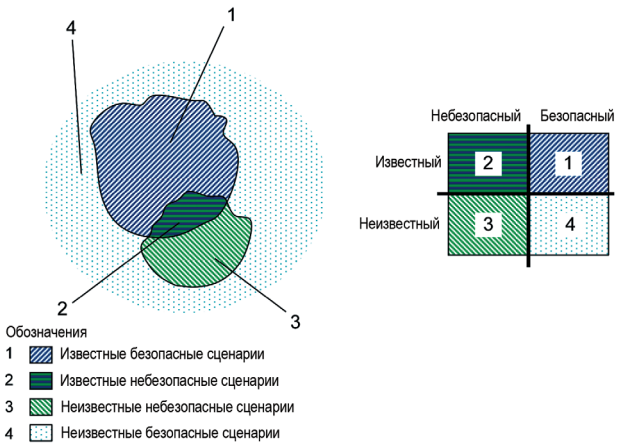

Рис. 3. Типы эксплуатационных сценариев, учитываемые при оценке безопасности системы

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») (см. Попов П.А. [8]). 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). Предлагаемая схема построения системы управления МЦК

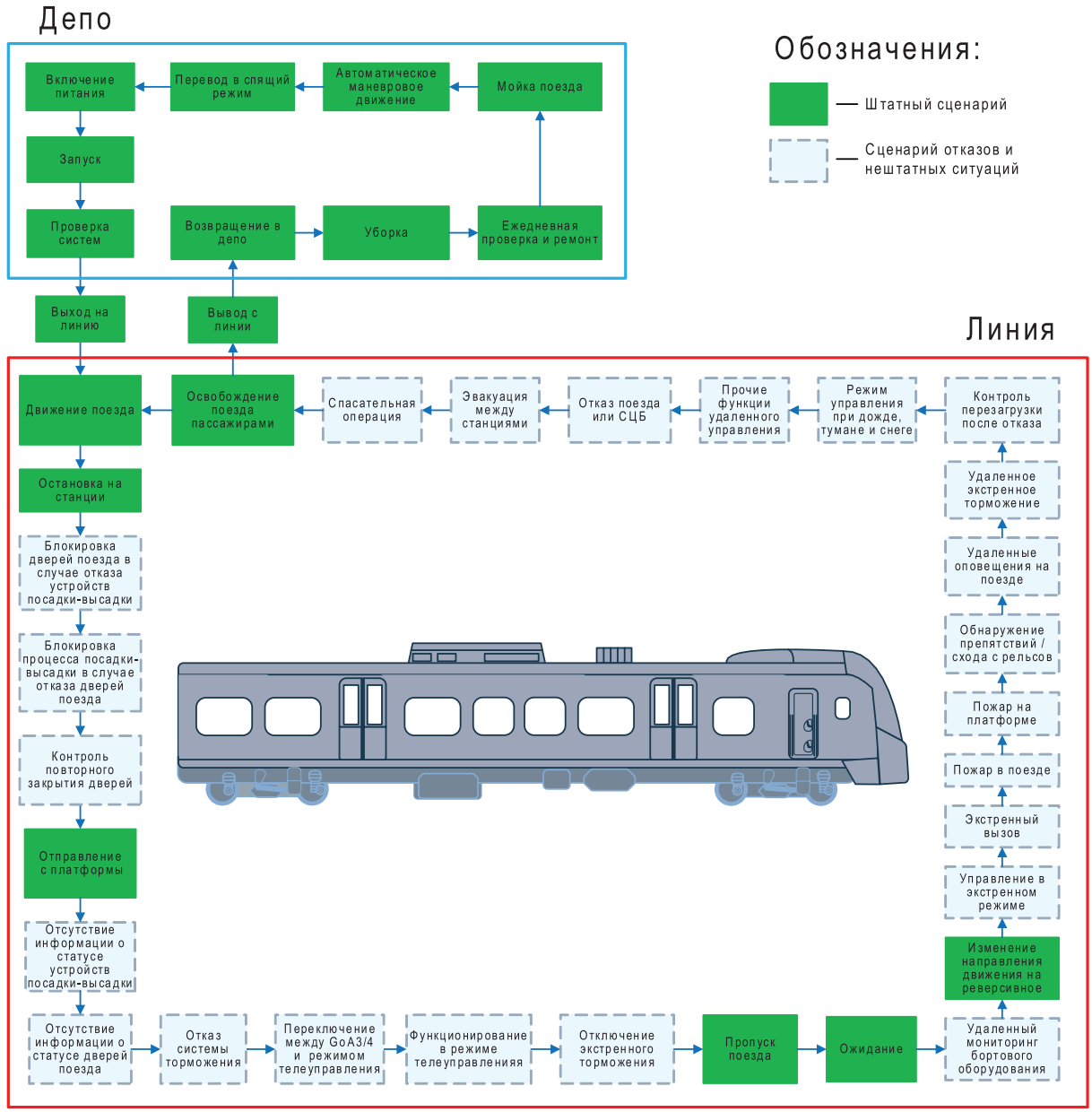

Рис. 4. Базовые эксплуатационные сценарии на городской железной дороге типа МЦК

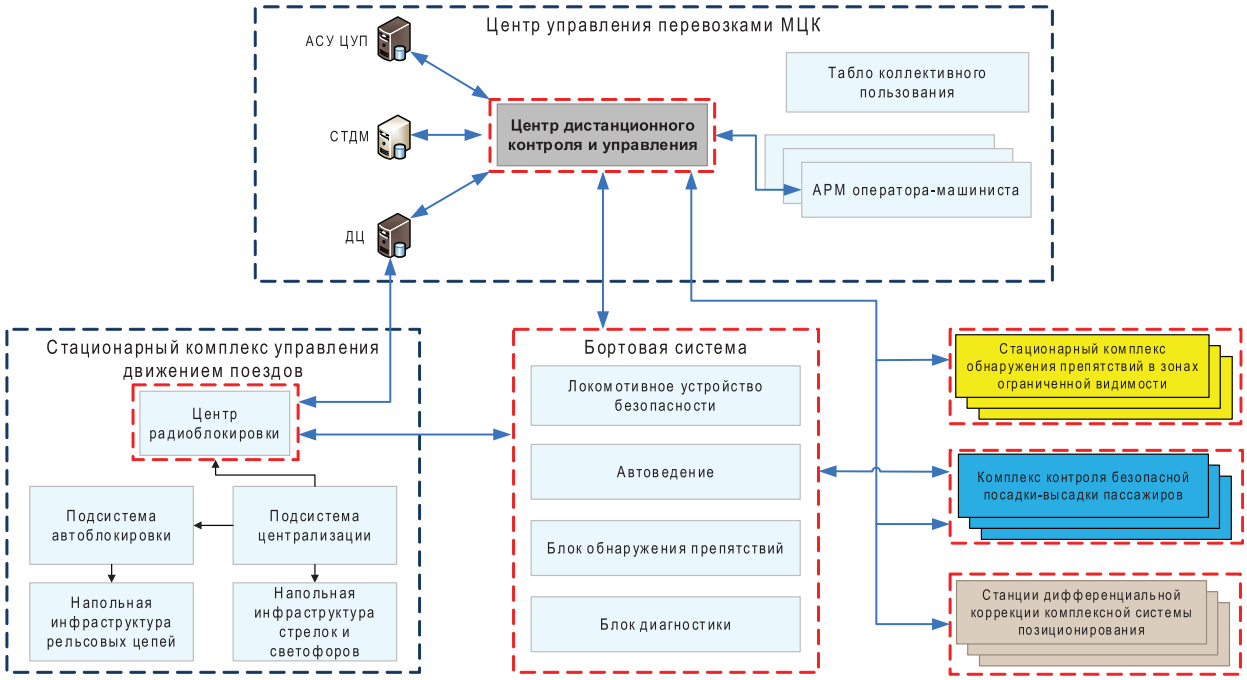

Рис. 5. Общая схема управления и обеспечения безопасности на МЦК

в режиме GoA3/4 представлена на рис. 5 (красной штриховой линией выделены подсистемы, составляющие контур безопасности режима GoA3/4):

Представленная схема уже на этапе системного проектирования сокращает число уровней управления и вносит иерархический порядок, при котором число уровней управления равно двум. В работе Арнольда [9] убедительно показано, что системы с числом уровней управления, равным 2, могут быть устойчивыми при правильно спроектированных управлениях высшего уровня. Однако необходимо провести дальнейшие исследования и оптимизацию такой схемы для упорядочения взаимоотношений между комплексами управляющих систем.

Третий шаг исследования самый трудоемкий – формирование и описание угроз функциональной безопасности в соответствии с перечнем эксплуатационных сценариев для каждого блока системы на различных иерархических уровнях. Для анализа полученных угроз введем следующие обозначения: *Sc* – общее количество первичных сценариев, которое получено комбинаторным путем (так обеспечивается 100% охват всех устройств и их сочетаний), *Mod* – множество устройств в контурах управления, влияющих на функциональную безопасность системы, *F* – множество небезопасных режимов, *R* – матрица отношений между устройствами и небезопасными режимами – предполагается, что каждое устройство инцидентно само с собой, т.е. минимальная сумма баллов в строке каждого устройства составляет 1.

В данном случае применим с небольшими изменениями, касающимися реализации на том или ином языке программирования, алгоритм, предложенный Yan F. и др. [10] для формирования библиотеки причинно-обусловленных (детерминированных) сценариев с помощью исключения нереальных сценариев.

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

1. В результате обработки полной библиотеки сценариев, построенной по оговоренным синтаксическим правилам, формируют множества *Mod, F*.

2. Строят *R* как матрицу (|*Mod*|, |*F*|). Следует отметить, что мощность множества *F* превосходит величину общего числа режимов отказа, так как один и тот же режим отказа содержится в нескольких сценариях. На первом этапе должно выполняться неравенство |*F*Yan F|>>|*M*|.

3. Если в строке матрицы *R* содержится более, чем одна единица, то это говорит о том, что хотя бы одно устройство из M, записанное в данной строке, участвует в нескольких режимах отказа.

4. Далее производят поиск одинаковых столбцов. Их наличие свидетельствует о том, что режимы отказа в этих столбцах совпадают. Их можно включить в один итоговый сценарий.

5. 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. Формирование типовых сценариев (см. выше), проектирование иерархической структуры управления, диаграмм информационных потоков.

2. Идентификация причин опасностей.

3. Разработка мер безопасности.

Иерархическая структура управления представляет собой графическое изображение уровней управления, управляющие команды от верхних к нижним звеньям и сигналы от нижних звеньев, учитывая в пределе сенсоры, двери,

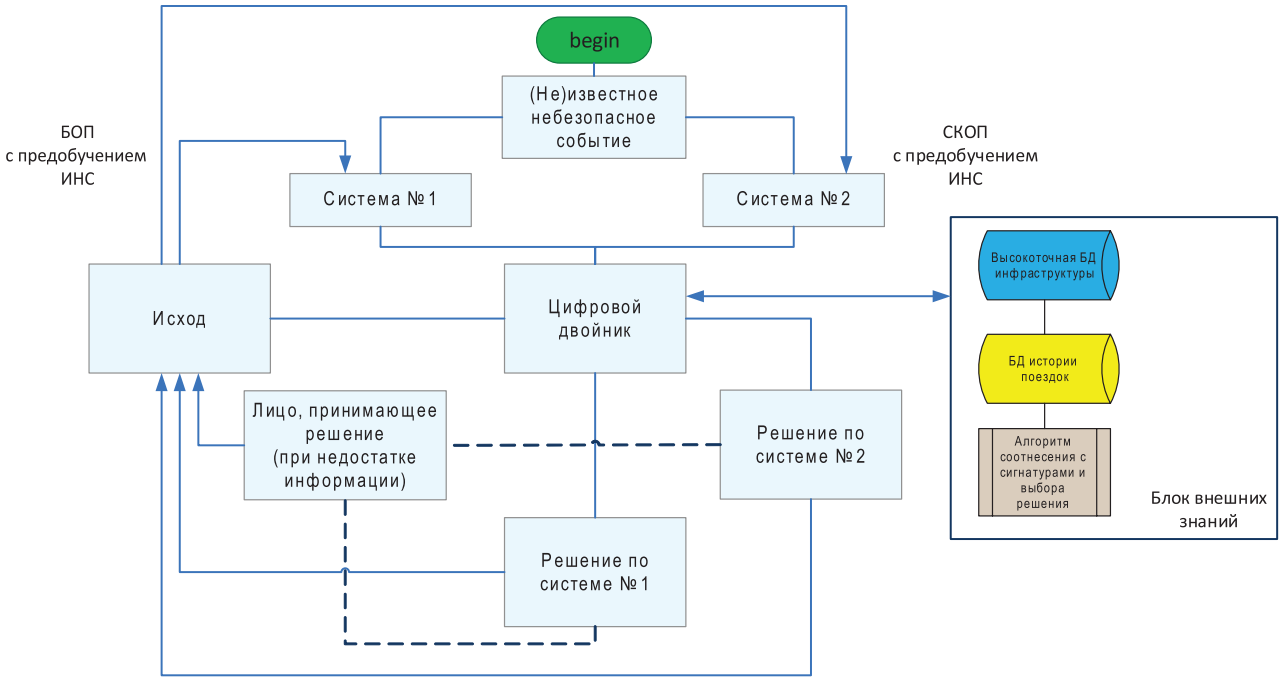

Рис. 6. Схема управления с виртуальной моделью

человека, микроконтроллеры. Для выбранных блоков и устройств затем формализуется поведение в нормальном и аварийном сценариях в таком формате: «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 составляют небезопасные сценарии (управляющие 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 «поезд – центр дистанционного контроля и управления ЦДКУ – стационарный комплекс обнаружения препятствий в зонах ограниченной видимости СКОП» содержит в себе, как минимум, два 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.

Отдельное исследование в дальнейшем, очевидно, потребуется для рассмотрения небезопасных сценариев, которые могут иметь место на границе или при пересечении идентифицированных комплексов «причина – ограничение», или контуров управления. Особое внимание должно быть уделено «пересечению» контуров «ЦДКУ – СКОП» и «блок обнаружения препятствия БОП – ЦДКУ», поскольку существует вероятность небезопасного управления со стороны обоих контуров при нахождении поезда в зоне ограниченной видимости (действия СКОП). При этом следует иметь в виду, что ни тот, ни другой контур не является полностью наблюдаемым, так как и БОП, и СКОП построены на использовании алгоритмов машинного обучения (искусственных сверточных нейросетей семейства VoVNet), поведение которых не может считаться до конца предсказуемым.

Это может привести в последующем к необходимости пересмотра и корректировки модели безопасности системы транспортного обслуживания путем введения дополнительного элемента, выполняющего функцию контроля и ограничения. В качестве ограничителя изучаются разные варианты – от конечного автомата на «жесткой» логике до сети-супервайзера. На рис. 6 представлена упрощенная схема управления с виртуальной моделью («цифровым двойником»), которая может быть реализована как «контролируемая искусственная нейронная сеть».

К сожалению, супервайзер в виде так называемой «контролируемой искусственной нейронной сети» обладает задержкой (если правильное решение не вырабатывается на втором шаге, то его поиск может длиться свыше двух шагов и до бесконечности, пока не будет прерван лицом, принимающим решение), а кроме того, алгоритмы оценки допустимости и выработки решений в супервайзере должны быть достаточно быстродействующими, чтобы общая задержка была разумной во времени. При этом уровень уверенности P, возвращаемый алгоритмом выработки решений, всегда будет меньше 100%. Надеемся, что последующие исследования помогут решить указанные вопросы.

4. Выводы

При повышении уровня автоматизации и переходе к полностью автоматическому режиму управления для системы транспортного обслуживания возникают дополнительные риски безопасности, связанные с не до конца предсказуемым поведением входящих в ее состав подсистем, вследствие использования в них методов машинного обучения. Введение в контур управления модулей автоматического обнаружения препятствий на основе искусственных нейронных сетей крайне усложняет задачу анализа рисков и угроз и оценку безопасности с помощью традиционных методов построения деревьев ошибок и анализа отказов и их последствий FTA и FMEA. Очевидно, что при построении модели безопасности столь сложных многоконтурных систем транспортного обслуживания требуется применение комплексного подхода.

Данный подход должен обязательно включать системный анализ небезопасных эксплуатационных сценариев с формированием библиотеки причинно-обусловленных сценариев и формализацией описания модели угроз, в том числе на границах различных контуров управления. Результатом системного анализа может стать последующий пересмотр и корректировка модели безопасности проектируемой системы транспортного обслуживания и вывод о необходимости наличия в модели дополнительного элемента, выполняющего функцию контроля и ограничения – например, путем реализации решающего алгоритма на основе цифрового двойника. При этом введение в состав системы цифрового двойника (или виртуальной модели) – совершенно новый и не апробированный подход к обеспечению безопасности системы, требующий дополнительных исследований и разработок. Остается надеяться, что дальнейшие работы в этом направлении позволят обосновать возможность создания «контролируемой искусственной нейронной сети», отвечающей традиционным требованиям безопасности, предъявляемым к системам транспортного обслуживания, либо разработать иной адекватный алгоритм контроля и ограничения.

В свою очередь, предложенный в статье подход на основе системного анализа и теории управления может стать универсальной методологической платформой для моделирования и проектирования систем беспилотного транспортного обслуживания. Как логическое развитие, в дальнейшем может также последовать разработка и создание на базе изложенного подхода специализированного программного комплекса для автоматизированной оценки уровня риска проектируемых систем и технологических процессов.

Библиографический список

1. World Report on Metro Automation. URL: 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. 2021. № 1. С. 38-44.

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. P. 042042.

5. Leveson N.G., A systems-theoretic approach to safety in software-intensive systems // IEEE Transactions on Dependable and Secure Computing. 2004. Vol. 1. No. 1 P. 66-86.

6. 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.

7. ISO/PAS 21448:2019 (SOTIF). Road Vehicles – Safety of the Intended Function.

8. Попов П.А. Развитие отечественных и зарубежных беспилотных технологий // Автоматика, связь, информатика. 2020. № 9. С. 6-12.

9. Арнольд В.И. «Жесткие» и «мягкие» математические модели. М.: Издательство МЦНМО, 2004. 32 с.

10. Yan F., Zhang S., Tang T. Autonomous Train Operational Safety assurance by Accidental Scenarios Searching // 2019 IEEE Intelligent Transportation Systems Conference (ITSC). IEEE, 2019. P. 3488-3495.

Сведения об авторах

Алексей Валерьевич Озеров – начальник Международного управления АО «НИИАС», ул. Нижегородская, д. 27, стр. 1, Москва, Российская Федерация, 109029, e-mail: a.ozerov@vniias.ru

Алексей Михайлович Ольшанский – кандидат технических наук, руководитель Центра перспективных разработок НТК по РОД и ОПР АО «НИИАС», ул. Нижегородская, д. 32, стр. Б, оф. 512, Москва, Российская Федерация, 109029, e-mail: a.olshanskiy@vniias.ru

Вклад авторов в статью

Автором **Озеровым А.В.** проанализированы основные подходы, выявлены их преимущества и недостатки, разработана общая схема управления и обеспечения безопасности, базовые эксплуатационные сценарии, схема управления с виртуальной моделью.

Автором **Ольшанским А.М.** предложены концепция «контролируемой искусственной нейронной сети» и последовательность действия по описанию угроз функциональной безопасности.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.