Оригинальная статья
https://doi.org/10.21683/1729-2646-2020-20-2-54-64

Перспективы повышения функциональной безопасности систем железнодорожной автоматики и телемеханики в условиях цифровизации

Алексей В. Озеров, *АО «НИИАС», Российская Федерация, Москва*

Алексей В. Озеров

Резюме. Цель. *Современное состояние развития микропроцессорных систем управления и обеспечения безопасности движения поездов характеризуется высокими требованиями, предъявляемыми к надежности, технической безопасности и кибербезопасности данных систем в условиях, когда цифровая трансформация и задачи повышения конкурентоспособности железнодорожного транспорта настойчиво требуют перехода к новым парадигмам проектирования, тестирования, верификации, валидации и стандартизации для ускорения процесса разработки и внедрения. Предполагается, что при сохранении уровня надежности и безопасности, по крайней мере, не хуже текущего, должно быть обеспечено максимальное использование инновационных решений и цифровых инструментов, направленных на дальнейшую автоматизацию систем управления с целью повышения пропускной способности железных дорог и производительности систем, минимизации влияния человеческого фактора и сокращения числа отказов и простоев. Важнейшими факторами при этом являются обеспечение интероперабельности (технической и эксплуатационной совместимости) систем и технологической независимости железнодорожных операторов и владельцев инфраструктуры от разработчика/поставщика устройств и систем железнодорожной автоматики.* **Методы.** *В работе дается обзор современного состояния развития микропроцессорных систем управления и обеспечения безопасности движения поездов на примере Европейского Союза и проводится системный анализ вопросов обеспечения надежности и безопасности данных систем в условиях перехода к новым уровням автоматизации.* **Результаты.** *Проведено рассмотрение эволюции систем управления и обеспечения безопасности движения поездов в Европейском Союзе на примере Европейской железнодорожной системы управления (ERTMS). Выполнен анализ общих тенденций и подходов к проектированию, тестированию, верификации, валидации и стандартизации железнодорожных систем управления. Рассмотрены основные научно-исследовательские и опытно-конструкторские программы развития железнодорожных систем управления ЕС с учетом используемых методологических подходов к обеспечению надежности и безопасности. Особое внимание уделено методам открытого проектирования, средствам удаленного лабораторного тестирования и стандартизации интерфейсов железнодорожной системы управления ERTMS.* **Выводы.** *В условиях цифровой трансформации развитие современных микропроцессорных систем на железнодорожном транспорте предполагает ускоренное внедрение целого ряда инновационных решений и широкое использование коммерческих продуктов (COTS), что в итоге делает системы более сложными и может влиять на показатели надежности. В целях сохранения этих показателей на заданном уровне и минимизации влияния человеческого фактора железнодорожное сообщество все шире использует на всех этапах жизненного цикла системы формальные методы и автоматизированные средства проектирования, диагностики и мониторинга. Важнейшим фактором для обеспечения надежности является стандартизация архитектуры, интерфейсов, открытых программных средств разработки и тестирования систем, в том числе, стандартизация подходов к удаленному лабораторному тестированию продуктов разных производителей для подтверждения безотказности работы на границах систем разных производителей.*

Ключевые слова: *системы управления, железнодорожная сигнализация, интервальное регулирование движения поездов, надежность, безопасность, TSI, ERTMS/ETCS, GoA4, человеческий фактор, формальные методы, верификация, валидация, сертификация, омологация, тестирование.*

Для цитирования: *Озеров А.В. Вопросы надежности систем управления и обеспечения безопасности на железнодорожном транспорте в контексте цифровизации // Надежность. 2020. № 2. С. 54-64. https://doi.org/10.21683/1729-2646-2020-20-2-54-64*

Поступила *18.02.2020 г.* / **После доработки** *21.04.2020 г.* / **К печати** *17.06.2020 г.*

1. Введение

Современное состояние развития микропроцессорных систем управления и обеспечения безопасности движения поездов характеризуется высокими требованиями, предъявляемыми к надежности, технической безопасности и кибербезопасности данных систем в условиях, когда цифровая трансформация и задачи повышения конкурентоспособности железнодорожного транспорта настойчиво требуют перехода к новым парадигмам проектирования, тестирования, верификации, валидации и стандартизации для ускорения процесса разработки и внедрения. Предполагается, что при сохранении уровня надежности и безопасности, по крайней мере, не хуже текущего, должно быть обеспечено максимальное использование инновационных решений и цифровых инструментов, направленных на дальнейшую автоматизацию систем управления с целью повышения пропускной способности железных дорог и производительности систем, минимизации влияния человеческого фактора и сокращения числа отказов и простоев. Важнейшими факторами также являются обеспечение интероперабельности (технической и эксплуатационной совместимости) систем и технологической независимости железнодорожных операторов и владельцев инфраструктуры от разработчика/поставщика устройств и систем железнодорожной автоматики.

Строго говоря, цифровая трансформация применительно к железнодорожным системам управления предполагает переход к новой парадигме управления 4.0. С точки зрения базового принципа интервального регулирования движения поездов, это означает эволюцию от простого разделения попутно следующих поездов сначала по времени, потом с помощью безопасного расстояния (фиксированный блок-участок) с переходом к управлению по радиоканалу (как в Европейской железнодорожной системе управления ERTMS) и к динамически регулируемому интервалу следования (вплоть до сближения поездов на небезопасное расстояние по принципу «виртуальной сцепки», по аналогии с автомобильным транспортом). Такой переход влечет за собой целый набор нормативных, регуляторных, технологических и технических изменений [1].

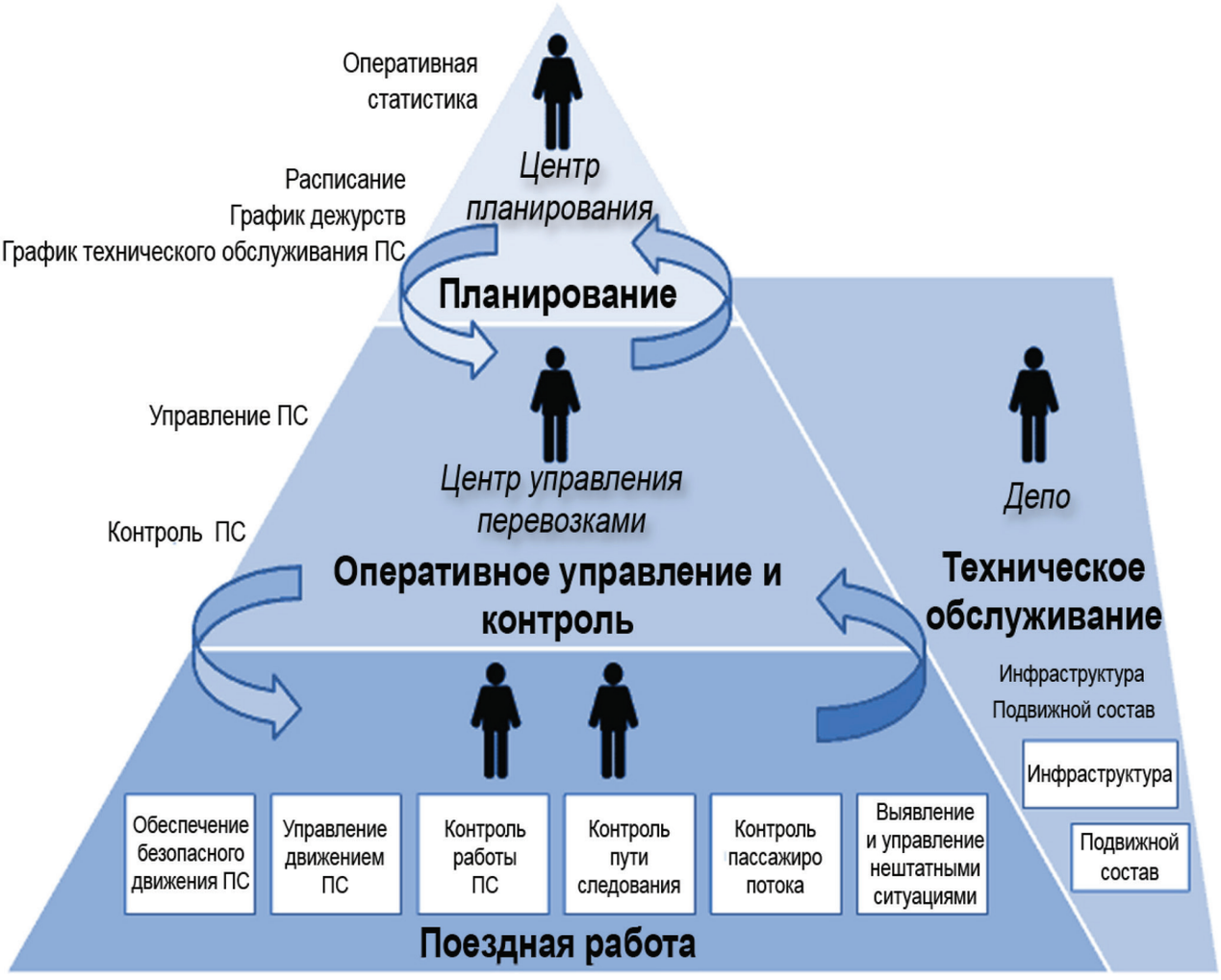

Рис. 1. Организация работы железнодорожного транспорта

Одним из существенных факторов, обусловливающих необходимость изменения методологических подходов к проектированию и эксплуатации систем управления и обеспечения безопасности движения поездов, является последовательное повышение уровня автоматизации управления подвижным составом (ПС) в направлении целевого состояния, декларируемого в общеевропейских программах инновационного развития и предполагающего переход к полностью беспилотным технологиям управления подвижным составом, т.е. без машиниста (так называемый уровень GoA4, или Grade of Automation, согласно стандарту МЭК 62290) [2].

Это значительно повышает значимость вопросов обеспечения надежности и безопасности на всех уровнях управления перевозочным процессом, где в настоящее время по-прежнему большую роль играет человеческий фактор, и особенно на уровне критически важных (ответственных) систем, связанных с безопасностью движения (рис. 1).

2. Требования интероперабельности ЕС и нормирование показателей надежности

Исторически сложилось так, что практически в каждой стране свои нормативные требования и правила эксплуатации железных дорог, а нередко и разная железнодорожная колея. Так, в Европе до образования Евросоюза функционировало более двадцати разных национальных железнодорожных систем управления и обеспечения безопасности движения поездов, устанавливаемых как на инфраструктуре, так и на борту поезда, а также собственные системы сертификации и омологации. После образования Евросоюза и открытия трансъевропейских транспортных коридоров TEN-T на первый план вышли вопросы интероперабельности (технической и эксплуатационной совместимости) железнодорожных систем и инфраструктуры и создания единой системы сертификации и омологации (так называемая «система взаимного признания сертификатов» – или cross acceptance).

Впоследствии в ЕС были утверждены разработанные Европейским железнодорожным агентством (ERA) так называемые «Директивы интероперабельности» и «Технические спецификации интероперабельности» (Technical Specification for Interoperability, или TSI, для всех элементов железнодорожной системы, включая единую железнодорожную систему управления ERTMS). В директивах интероперабельность определяется как способность железнодорожной системы обеспечивать безопасное движение поездов без замены или переключения оборудования на участках стыкования с достижением требуемых уровней эксплуатационных показателей [3].

Актуальной версией TSI применительно к системам управления и обеспечения безопасности движения поездов (TSI relating to Control-Command and Signalling – TSI CCS) является версия от 2016 года [4]. В данной спецификации нормируются требования совместимости бортового и напольного оборудования ERTMS, интерфейсы с внешними подсистемами и, в том числе, показатели безотказности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS). Требования совместимости опираются на корпус спецификаций функциональных требований к подсистемам и интерфейсам системы ERTMS, разрабатываемых промышленной группой UNISIG, объединяющей ведущих производителей оборудования железнодорожной автоматики, под эгидой ERA (так называемые Subsets).

Система ERTMS имеет три базовых элемента:

1. GSM-R (Global System for Mobiles – Railway) – система радиосвязи, построенная на специально выделенных частотах публичной сети радиосвязи GSM и предназначенная как для голосовой коммуникации между машинистами и диспетчерами, так и для передачи данных ETCS (между бортовым локомотивным устройством безопасности EVC – «Европейским безопасным компьютером» – и стационарным вычислительным управляющим комплексом RBC – «центром радиоблокировки»).

2. ETCS (European Train Control System) – система сигнализации, которая отвечает за контроль скорости, формирование и исполнение разрешений на движение, обмен информацией с устройствами электрической централизации стрелок и сигналов на железнодорожных станциях.

3. ETML (European Traffic Management Layer) – уровень управления поездопотоками на основе графиков движения, предназначенный для оптимизации движения поездов по участкам с учетом поездной информации в режиме реального времени.

Система ERTMS/ETCS имеет три варианта или уровня. Если говорить упрощенно, то уровень 1 представляет собой управление по светофорам и путевым приемопередатчикам (бализам), без использования радиоканала GSM-R и, соответственно, центра радиоблокировки RBC; уровень 2 – управление по радиоканалу GSM-R и, соответственно, с использованием центра радиоблокировки RBC, а также бализ в качестве реперных точек для целей навигации (это наиболее широко внедряемый вариант системы как в Европе, так и за ее пределами, – на данный момент оборудовано не менее 100 тыс. км железных дорог); уровень 3 предполагает дополнительное использование бортовых средств позиционирования и контроля целостности подвижного состава и реализацию принципа «подвижных блок-участков». Система ERTMS/ETCS уровень 3 до сих пор носит пока экспериментальный характер, разрабатывается и тестируется в виде гибридных решений с использованием спутниковой навигации, виртуальных бализ и цифровой карты маршрута.

Согласно спецификации Subset-026 («Спецификация системных требований») «эталонная» архитектура

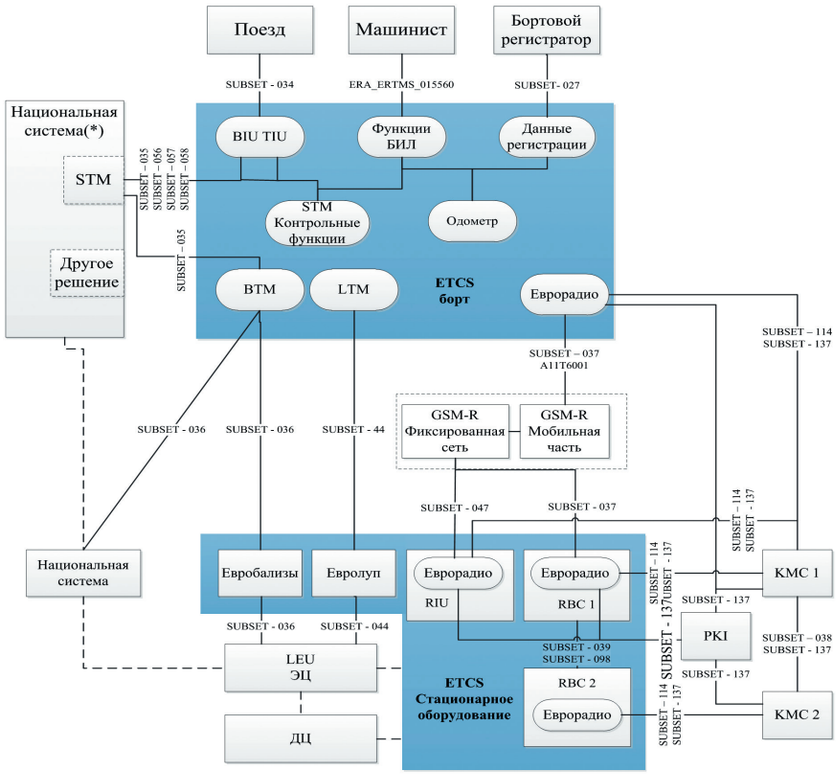

Рис. 2. Эталонная архитектура системы ERTMS/ETCS с указанием спецификаций интерфейсов

системы ERTMS/ETCS выглядит следующим образом (рис. 2) [5].

Пунктирной линией на схеме отмечены до сих пор не стандартизированные интерфейсы, и в этом случае применяются проприетарные (закрытые) протоколы и решения производителей. Это в особенности касается увязки центра радиоблокировки RBC с устройствами электрической централизации (ЭЦ) на станциях и оборудованием диспетчерской централизации (ДЦ), а также сопряжения между собой центров радиоблокировки RBC разных производителей. Это влечет за собой проблемы, связанные как с обеспечением интероперабельности, так и с обеспечением заданных показателей RAMS.

Кроме перечня обязательных технических спецификаций на подсистемы и интерфейсы системы ERTMS, TSI CCS содержит перечень обязательных стандартов, на соответствие требованиям которых должно сертифицироваться оборудование ERTMS, а именно:

1. EN 50126 «Железнодорожные применения. Спецификация и демонстрация безотказности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS)».

2. EN 50128 «Железнодорожные применения. Системы связи, сигнализации и обработки данных. Программное обеспечение для систем управления и обеспечения безопасности на железных дорогах».

3. EN 50129 «Железнодорожные применения. Системы связи, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью».

4. EN 50159 «Железнодорожные применения. Системы связи, сигнализации и обработки данных».

Согласно стандартам CENELEC, проектирование, верификация/валидация и сертификация подсистем ERTMS/ETCS с точки зрения программного обеспечения должны обеспечиваться на трех уровнях (рис. 3).

Рис. 3. Слои программного обеспечения

Если взять ключевой элемент системы ERTMS/ETCS уровень 2 – центр радиоблокировки RBC, то первый слой RBC – это программное ядро, в котором реализована безопасная логика и которое является единым и неизменным программным продуктом для всех железных дорог, на которых он применяется (сертифицируется однократно в уполномоченном органе ЕС, если впоследствии не вносятся изменения); второй слой (так называемое «технологическое программное обеспечение») интегрирует в себя логику и правила сигнализации той страны, для которой предполагается применение продукта, и является единым для всех применений продукта на железных дорогах данной страны (требует процедуры омологации для каждой страны); третий слой – это специфическая конфигурация логики сигнализации с топографической привязкой к конкретному железнодорожному участку (требует процедуры омологации для каждого участка).

В итоге нормативная пирамида системы ERTMS/ETCS в схематичном виде выглядит следующим образом (рис. 4).

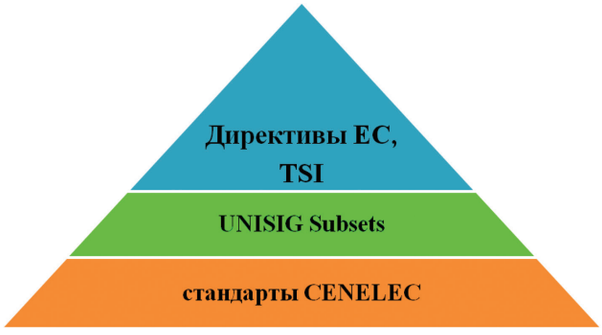

Рис. 4. Нормативная пирамида системы ERTMS/ETCS

3. Надежность системы ERTMS/ETCS

Стандарты, описывающие методологию RAMS, были разработаны еще во второй половине 90-х годов прошлого века Европейским комитетом электротехнической стандартизации CENELEC.Они используют комплексный подход к управлению показателями RAM, которые имеют непосредственное отношение к надежности системы, и безопасности (S) объектов железнодорожного транспорта на основе оценки рисков с учетом этапов жизненного цикла (V-образная модель).

Стандарты базируются на вероятностном подходе и используют как количественные показатели, так и рекомендации по обеспечению заданных показателей RAMS за счет применения апробированных методов (например, методы программирования, автоматизированного тестирования ПО и выявления ошибок и отказов). Изначально такой подход использовался в других отраслях промышленности – в атомной энергетике, авиации и космонавтике, откуда и был позаимствован [6].

Сертификация системы ERTMS/ETCS на соответствие стандартам CENELEC предполагает большой перечень мероприятий в области обеспечения надежности и безопасности (RAMS), т.е. подготовку и ведение значительного корпуса документов на всех этапах жизненного цикла системы, а также строгое соблюдение независимости друг от друга разработчика, верификатора/валидатора и оценщика системы с обязательным обеспечением менеджмента качества производства (аудит производства).

Документация RAM включает в себя программу обеспечения RAM и отчет о выполнении программы RAM (расчет внутренней надежности, листы планового и внепланового технического обслуживания).

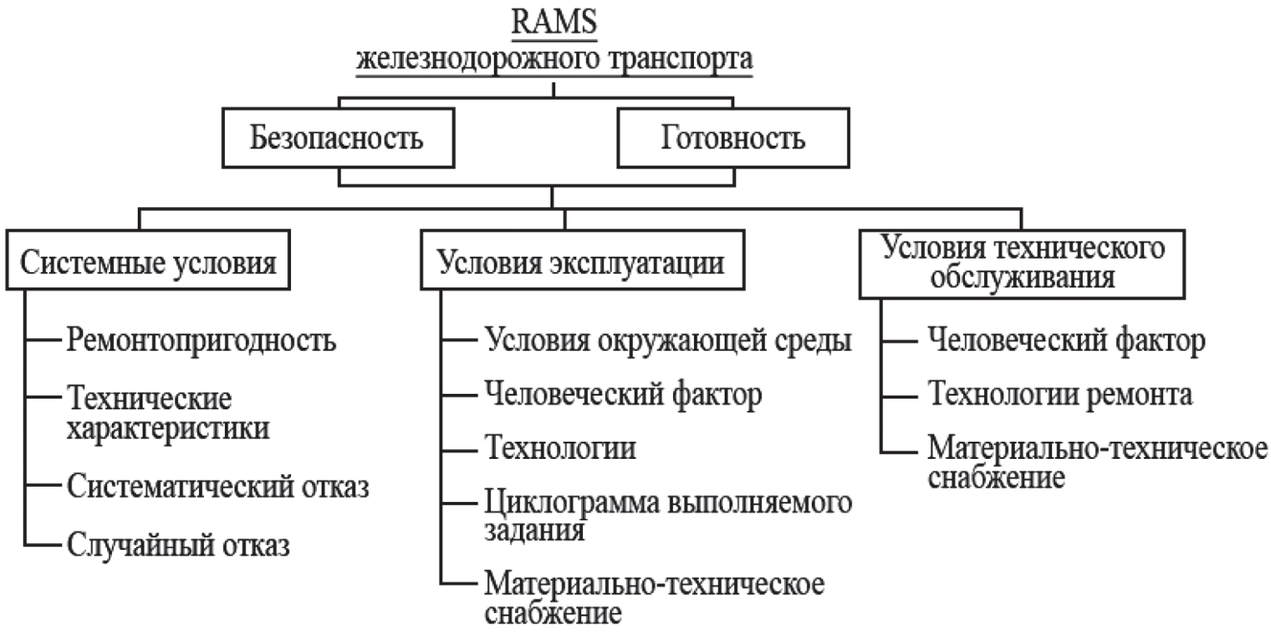

Рис. 5. Факторы, влияющие на RAMS (упрощенная схема на основе EN 50126)

Для сохранения надежности и эксплуатационных характеристик системы на этапах ее жизненного цикла должны определяться факторы, влияющие на показатели RAMS, анализироваться и оцениваться последствия их влияния, использоваться мероприятия по управлению ими, предусмотренные в стандартах.

Согласно EN 50126, характеристики RAMS железнодорожной системы подвержены тройному влиянию:

- ошибки и отказы, которые проявляют себя внутри системы на любом этапе жизненного цикла системы;
- мешающие влияния, которым подвергается система во время эксплуатации;
- ошибки, которым подвергается система во время работ по техническому обслуживанию.

При этом эти три источника влияния могут взаимодействовать между собой. Эффективное управление этими факторами позволяет сохранять показатели RAMS на заданном уровне. В упрощенном виде взаимосвязанность факторов, влияющих на надежность и безопасность, представлена на рис. 5 [7].

Эксплуатационные требования к системе управления и обеспечения безопасности на железнодорожном транспорте специфичны для каждой системы и определяются по соглашению между производителем и владельцем инфраструктуры на этапе разработки системы. Для системы в целом определены следующие три типа отказов:

- отказ, вызывающий остановку движения (по меньшей мере, два поезда вынуждены двигаться по условиям видимости);
- эксплуатационный отказ (не более одного поезда вынуждены двигаться по условиям видимости);
- незначительный отказ (требует внепланового ремонта, но не подпадает под предыдущие категории).

В документе «ERTMS/ETCS RAMS requirements specification» (1998), к примеру, приводятся следующие конкретные параметры [8]:

- вероятность задержки движения по причине отказов системы сигнализации не должна превышать 0,018, а вероятность отказов системы ERTMS/ETCS должна быть не выше 0,0027;
- допустимая средняя задержка на поезд по причине отказа ERTMS/ETCS в конце поездки средней продолжительности 90 мин. должна быть не выше 10 мин.;
- эксплуатационная готовность при любых причинах отказа должна быть не ниже 0,99973;
- отказы, приводящие к остановке поезда, не должны превышать 10% от всего количества отказов, влияющих на надежность системы; сервисные отказы не должны превышать 90% от всего количества отказов, влияющих на надежность системы;
- среднее время восстановления системы – 1,737 часа для распределенного напольного оборудования.

При этом следует отметить, что система ERTMS/ETCS уровень 2, как правило, работает как оверлейная система, то есть устанавливается поверх национальной системы сигнализации и использует последнюю в качестве резервной системы в случае отказа. В литературе часто дискутируется вопрос о необходимости использования дополнительных устройств и систем для повышения надежности основной системы сигнализации [9].

План обеспечения RAM системы ERTMS/ETCS должен, как минимум, включать в себя следующие мероприятия:

- системные условия и циклограмма выполняемого задания;
- периодические ревизии плана обеспечения RAM;
- моделирование, прогнозирование и пропорциональное распределение показателей безотказности;
- анализ видов, последствий и критичности отказов (FMECA);
- анализ безотказности программного обеспечения;
- анализ и верификация эксплуатационных показателей надежности;
- анализ превентивного технического обслуживания;
- анализ корректирующего технического обслуживания;
- планы по изолированию и поиску неисправностей;
- программа развития/повышения безотказности;
- предварительные тесты ремонтопригодности;
- демонстрационные тесты безотказности;
- демонстрационные тесты ремонтопригодности;
- система анализа отчетности об отказах и корректирующих воздействиях (FRACAS).

Разумеется, важнейшим фактором, влияющим на показатели RAMS системы, является человеческий фактор – причем как на этапе проектирования, так и на этапе эксплуатации. Поскольку человек может оказать большое влияние на RAMS, достижение заданных показателей RAMS железнодорожного транспорта требует более строгого учета человеческого фактора, чем в других отраслях. Этим также объясняются усилия, предпринимаемые железнодорожным сообществом по автоматизации как процесса эксплуатации и технического обслуживания, так и процессов проектирования, тестирования, верификации и валидации, особенно в контексте общего курса на цифровизацию и внедрения принципов Индустрии 4.0.

4. Новые подходы и требования

Как показывает анализ программных документов железнодорожных органов и ассоциаций ЕС и Международного союза железных дорог (МСЖД), главный мотивационный фактор поиска новых подходов и решений в железнодорожной отрасли в условиях цифровой трансформации – низкая скорость внедрения инноваций, обусловленная длительным периодом сертификации и омологации, который во многом связан с наличием проприетарных решений, отсутствием стандартизированных протоколов и интерфейсов, а также стандартизированных методов автоматизированного проектирования. Это влечет за собой высокие расходы на разработку и внедрение систем, их эксплуатацию и техническое обслуживание, быстрое устаревание систем, а также

технологическую зависимость от поставщика. Кроме того, это влияет на надежность и безопасность систем управления.

Для решения этих проблем в ЕС создано в 2014 г. и функционирует совместное предприятие Shift2Rail (с совокупным бюджетом – 900 млн евро) [10]. Это масштабная комплексная программа инновационного развития железнодорожного транспорта, объединяющая производителей железнодорожной техники, железнодорожных операторов и владельцев инфраструктуры. Ее основная цель заключается в разработке, интеграции, демонстрации и валидации инновационных цифровых технологий для железной дороги в целях повышения ее привлекательности для потребителей (отсюда и само название инициативы, буквально означающее «переориентация на железную дорогу»).

К основным целевым показателям программы Shift2Rail относятся следующие:

- сокращение стоимости жизненного цикла объектов железнодорожного транспорта на 50%;
- увеличение пропускной способности существующей железнодорожной инфраструктуры в 2 раза;
- повышение надежности транспортных услуг и точности соблюдения графика на 50%.

В основе изменения подходов к заданию и подтверждению RAMS и, как следующий этап, к сертификации продукции лежат требования бизнеса, соображения, связанные с сокращением затрат на разработку, сертификацию и омологацию продукции, а также с сокращением времени от разработки продукции до вывода на рынок и времени ее внедрения на конкретном объекте железнодорожного транспорта. Не удивительно, что в рамках проектов программы Shift2Rail рассматриваются и изучаются различные методы автоматизации процесса разработки, верификации и валидации, тестирования, в том числе те, которые используются в других отраслях промышленности – в первую очередь, в авиационной и автомобильной промышленности.

На основе выбранных и стандартизированных в дальнейшем методов планируется даже переход к «виртуальной» сертификации. Под виртуальной сертификацией понимают максимально допустимое использование объективных свидетельств, получаемых путем имитационного моделирования и виртуального тестирования на основе формальных моделей, для подтверждения соответствия продукта заявленным требованиям в процессе сертификации и омологации [11]. Данная методология исследуется, например, в рамках одного из проектов Shift2Rail – PLASA 2. Цель – добиться существенного сокращения времени на стыковку с уже установленными системами и проведение тестирования в полевых условиях за счет стандартизации интерфейсов, использования формальных методов проектирования, верификации и удаленного лабораторного тестирования.

В принципе, уже в стандарте EN 50128 рекомендовано использование полуформальных и формальных методов проектирования и автоматизированных средств тестирования, верификации и валидации, но реальная работа в этом направлении пока далека от завершения в плане выбора и стандартизации соответствующих методов и средств [12].

По мнению автора [13], подход к обеспечению качества разработки программного обеспечения, представленный в стандарте CENELEC, не может сам по себе гарантировать «корректность» работы микропроцессорной системы. Формальные методы как раз и стали применяться для того, чтобы повысить «качество разработки» и снизить стоимость жизненного цикла критически важных микропроцессорных систем железнодорожной автоматики, в первую очередь, электрической централизации. Основное преимущество методов в том, что они позволяют дать исчерпывающий анализ всех возможных сценариев поведения программируемой системы и обеспечить консистентность между формализованным поведением модели и поведением встроенного в систему программного кода.

5. История и дальнейшее применение формальных методов

История применения формальных методов в стандартизации систем железнодорожной сигнализации берет свое начало в 1997 году, когда МСЖД опубликовал отчет о проекте Европейского института железнодорожных исследований (ERRI), в котором был проведен подробный анализ правил функционирования систем электрической централизации и предлагалась гармонизация функциональных требований к системам сигнализации на основе формальных подходов. В дальнейшем в рамках рабочей группы МСЖД был разработан полуформальный метод под названием EURIS («Европейская спецификация железнодорожной централизации»), определяющий «строительные блоки» (светофор, путь, стрелка) и описывающий операции с каждым блоком с использованием диаграмм технологических процессов. В проекте МСЖД EURO-INTERLOCKING (1998–2008) формализованные требования к системе электрической централизации были конвертированы в модель, визуализируемую с использованием компьютерной программы. Выяснилось, что для такой работы требуются одновременно знания инженера в области железнодорожной автоматики и специалиста в области компьютерного моделирования. Кроме того, стало очевидно, что это процесс итерационный и требует дальнейшего совершенствования модели как с точки зрения улучшения качества вербализации требований, так и с точки зрения их полноты [14].

Работа была продолжена в рамках проекта EULYNX, в котором на основе моделей SysML ведется формализация описания интерфейсов напольных систем сигнализации разных производителей, включая подсистемы ERTMS/ETCS, для сокращения времени разработки и программно-аппаратной стыковки между собой. В развитие данных подходов ассоциацией разработчиков EUG («Группа пользователей ERTMS») и консорциумом

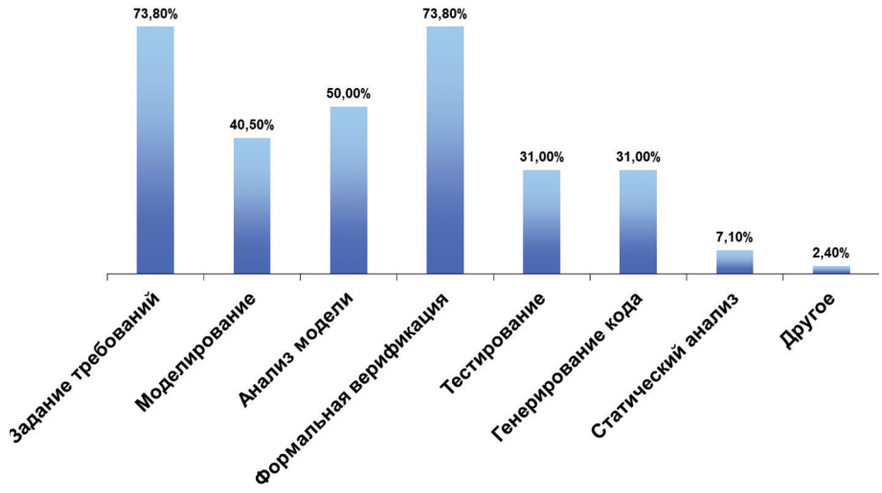

Рис. 6. Применение формальных методов на этапах ЖЦ системы

EULYNX был инициирован проект RCA (Reference CCS Architecture), направленный на разработку эталонной архитектуры системы ETCS нового поколения с интегрированными функциями автоведения (возможностью миграции к уровню GoA4), гармонизацию компонентов и стандартизацию интерфейсов и протоколов обмена на основе использования формальных методов. В 2019 году была выпущена альфа-версия описания будущей архитектуры [15].

Параллельно с проектом RCA по инициативе владельцев железнодорожной инфраструктуры ведущих европейских стран (Германии, Франции, Швейцарии, Нидерландов и др.) был создан консорциум OCORA (Open CCS Onboard Reference Architecture), который ставит перед собой задачи разработать и стандартизировать открытую модульную бортовую платформу ETC Snового поколения. Участники OCORA опираются на подходы EULYNX и RCA и также ориентируются на требования новой версии CCS TSI, выход которой планируется в 2022 году. Целью проекта OCORA является обеспечение технологической независимости от производителя (модульность, интероперабельность, заменяемость, модифицируемость компонентов системы, киберзащищенность, удобство эксплуатации) за счет создания новой открытой шины и стандартизации протоколов обмена всех модулей с максимальным использованием существующих промышленных стандартов. Ожидается, что такой подход позволит добиться, среди прочего, и заметного повышения эксплуатационных показателей системы, складывающихся из показателей безотказности, эксплуатационной готовности, ремонтопригодности и безопасности, в том числе киберзащищенности. В соответствии с программным документом проекта, результатом работы консорциума станет полный и логически связанный набор спецификаций, а также новейшие рекомендации по интеграции, верификации и валидации бортовой системы с максимальным использованием автоматизированных средств тестирования и формальных методов [16].

В рамках проекта ASTRail, входящего в программу Shift2Rail, исследователи из группы FMT (формальные методы и средства), созданной на базе Института информационной науки и технологий (ISTI) Итальянского национального исследовательского совета (CNR) провели анализ и оценку основных языков и средств формального моделирования и верификации, используемых в железнодорожной области. В ходе исследования, к примеру, выяснилось [17], что наиболее часто в литературе упоминаются следующие автоматизированные

Табл. 1 – Перечень проектов ЕС в области железнодорожной сигнализации

Проект	**ERTMS/ETCS/CBTC**
CRYSTAL	http://www.crystal-artemis.eu/
Deploy	http://www.deploy-project.eu/
DITTO	http://cs.swansea.ac.uk/dittorailway/
EuRailCheck	https://es.fbk.eu/projects/eurailcheck-era-formalization-and-validation-etcs
MBAT	http://www.mbat-artemis.eu/home/69-abstract.html
OpenCOSS	http://www.opencoss-project.eu
OpenETCS	http://openetcs.org/
PERFECT	https://trimis.ec.europa.eu/project/performing-enhanced-rail-formal-engineering-constraints-traceability
	Распределенная железнодорожная сигнализация
SafeCap	http://gow.epsrc.ac.uk/NGBOView-Grant.aspx?GrantRef=EP/I010807/1
	Система централизации
ADVANCE	http://www.advance-ict.eu/
EULYNX	https://eulynx.eu/
EuroInter-locking	http://test.swissrequirementsengi-neering.ch/en/projects/euro-interlock-ing-project
INESS	http://www.iness.eu
RobustRail	http://www.robustrails.man.dtu.dk

системы проектирования: Simulink, NuSMV, AtelierB, Prover, ProB, SCADE, IBM Rational Software Architect, Polyspace, S3.

Проведенные опросы показали, что разработчики используют указанные или другие автоматизированные инструменты для следующих целей (рис. 6).

Как видно из результатов опроса, чаще всего формальные методы применяются на этапах задания требований (спецификации) и верификации системы. Стандартизации подходов к написанию спецификаций функциональных и технических требований к системе (FRS, SRS), а также верификации на основе формальных методов посвящен целый ряд проектов в ЕС, не считая самой программы Shift2Rail. Так, с 1998 года по настоящее время можно насчитать не менее14 проектов ЕС в области железнодорожной сигнализации, посвященных данной тематике. Подробное описание всех этих проектов в рамках данной статьи, по понятным причинам, не представляется возможным, поэтому просто перечислим их (табл. 1).

Детальный анализ традиционных и формальных методов верификации представлен в работе [18]. Как правило, в процессе верификации критически важной системы, такой как система ERTMS/ETCS, используется взаимоувязанный набор методов и средств, который в настоящее время все чаще учитывает не только параметры RAMS, но и параметры киберзащищенности (еще одна область, подлежащая стандартизации в рамках железнодорожной отрасли, рис. 7).

Подробный анализ возможностей дискретно-событийного моделирования применительно к этапам жизненного цикла системы ERTMS/ETCS, в особенности на этапе верификации, представлен также в работе [19]. Автор указывает, что система ERTMS/ETCS характеризуется тем, что состояния системы дискретны, а механизм перехода состояний обусловлен событиями. Современные методы проектирования не позволяют гарантировать, что ответственная система, связанная с безопасностью, будет полностью соответствовать требованиям и вести себя безопасно, а потому крайне важно интегрировать процессы верификации на как можно более раннем этапе разработки системы. Это можно сделать за счет использования формальных языков и методов проектирования.

Существует большое число формальных методов, и им присущ ряд преимуществ:

- формальные репрезентации обладают точной семантикой, лишенной неопределенности или двусмысленности;

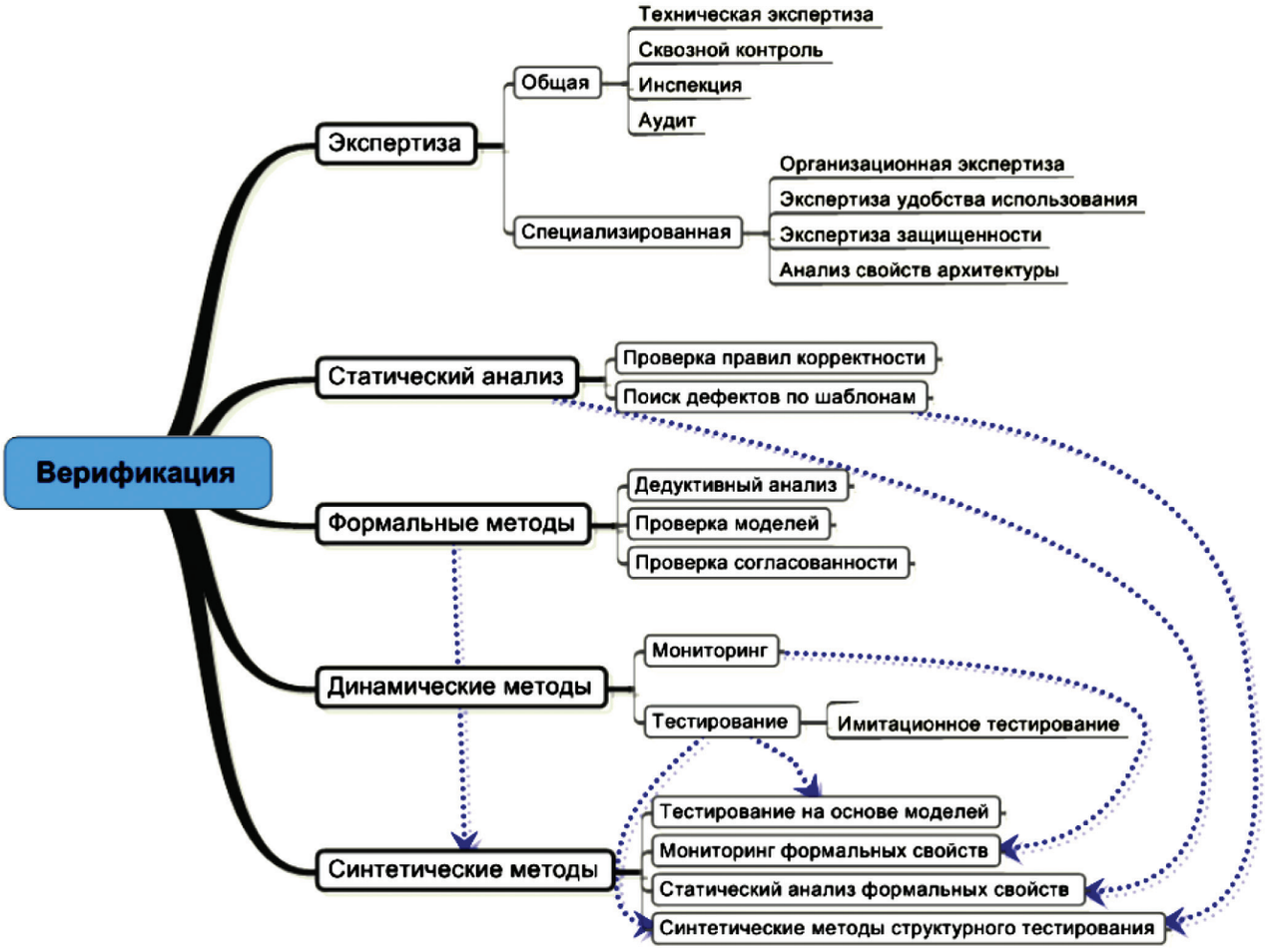

Рис. 7. Комбинированное использование методов верификации

- формальные модели могут быть верифицированы математически, а значит, их корректность может быть доказана;

- формальные модели могут читаться компьютерами, а, следовательно, процесс разработки системы может быть автоматизирован.

В идеале, применение формальных методов позволяет не только избежать небезопасных переходов системы, но и минимизировать число вносимых человеком ошибок, а следовательно, и отказов системы, что непосредственно влияет на ее надежность.

Важнейшим разделом программы Shift2Rail является блок инновационного развития IP2, среди задач которого – создание автоматизированных средств имитационного моделирования и лабораторного тестирования (в том числе, удаленного) для сокращения необходимости проведения интеграционных и валидационных тестов на объектах железнодорожного транспорта (так называемое «нулевое тестирование на месте установки» – «Zero on-site testing»).

По мнению авторов программы Shift2Rail [20], сегодняшняя ситуация в области тестирования систем управления и обеспечения безопасности характеризуется следующим образом:

- в большинстве случаев производители тестируют свою продукцию в лабораторных условиях;

- тестирование системы производится в лаборатории, но по-прежнему значительная часть тестов осуществляется на месте установки;

- тестирование на месте установки зачастую используется как резервное на тот случай, если лабораторное тестирование не завершено вовремя;

- лабораторное тестирование, как правило, производится в нестандартизированных условиях по принятым в компании правилам;

- увязка с оборудованием других производителей всегда вызывает необходимость использования сложных интерфейсных устройств, которые нельзя повторно использовать в последующих проектах;

- результаты тестирования не соотносимы между собой, поскольку применяются разные подходы на основе проприетарных решений.

В итоге, с точки зрения целевых задач программы Shift2Rail и ее проектов, предполагается обеспечить стандартизацию подходов на всех этапах жизненного цикла системы ERTMS/ETCS с учетом необходимости внедрения инновационных решений типа «подвижного блок-участка», «виртуальной сцепки», технического зрения в рамках реализации уровня автоматизации GoA4, будущего стандарта железнодорожной радиосвязи FRMCS, разрабатываемого под эгидой МСЖД на базе IP-протокола, взаимен устаревшего стандарта GSM-R. Результаты проектов должны быть положены в основу новых требований интероперабельности обновленной версии CCS TSI 2022 года, а также, возможно, рекомендаций для внесения изменений в стандарты CENELEC.

6. Заключение

В условиях цифровой трансформации развитие современных микропроцессорных систем на железнодорожном транспорте предполагает ускоренное внедрение целого ряда инновационных решений и широкое использование коммерческих продуктов (COTS), что в итоге делает системы более сложными и может влиять на показатели надежности. В целях сохранения этих показателей на заданном уровне и минимизации влияния человеческого фактора железнодорожное сообщество все шире использует на всех этапах жизненного цикла системы формальные методы и автоматизированные средства проектирования, диагностики и мониторинга.

Важнейшим фактором для обеспечения надежности является стандартизация архитектуры, интерфейсов, открытых программных средств разработки и тестирования систем, в том числе стандартизация подходов к удаленному лабораторному тестированию продуктов разных производителей для подтверждения безотказности работы на границах систем разных производителей. Возможное создание в перспективе единой открытой онтологии систем управления и обеспечения безопасности движения поездов и стандартизированных методов и средств разработки, тестирования и технического обслуживания на основе принципов интероперабельности и технологической независимости от производителя может обеспечить железнодорожному транспорту заметное конкурентное преимущество по сравнению с другими видами транспорта.

Разумеется, есть и другое большое направление исследований и практических работ, которое никак не затронуто в настоящей статье, связанное с использованием цифровых датчиков и цифровых моделей, а также комплексных информационных систем для мониторинга и прогнозирования показателей надежности системы, определения предотказных состояний на основе формального описания и имитационного моделирования возможных сценариев развития с применением технологии Data Science и Big Data. Но это уже тема для отдельной статьи.

Библиографический список

1. Doppelbauer J. Command and Control 4.0. // IRSE News, Issue 246, July/August 2018.

2. IEC 62290:2014. Railway applications – Urban guided transport management and command/control systems.

3. Interoperability Directive 2008/57/EC.

4. CCS (EU) No. 2016/919: Technical Specification of Interoperability relating to Control-Command and Signalling.

5. UNISIG Subset-026-2_v360.

6. Замышляев А.М. Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте. Ульяновск: Печатный двор, 2013. 140 с.

7. BS EN 50126:1999. Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

8. EUG. ERTMS/ETCS RAMS Requirements Specification, 1998.

9. Rumsey A. Achieving high levels of signalling system availability – is there a role for secondary systems? // IRSE News, Issue 247, September 2018.

10. Официальный сайт европейской инициативы Shift2Rail [Электронный ресурс]. URL: https://Shift2Rail.org/ (дата обращения 14.04.2020 г.)

11. Shift2Rail Plasa 2. Deliverable D 4.1: Virtual Certification: State of the art, gap analysis and barriers identification, benefits for the Rail Industry, 2019, p. 9.

12. BS EN 50128:2011. Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.

13. Antoni M. Formal Validation Method and Tools for French Computerized Railway Interlocking Systems // IRJ. 2009. Vol. 2. No. 3. P. 99-106.

14. Van der Werff M., Elsweiler B., Luttik B., Hendriks P. The use of formal methods in standardisation of interfaces of signalling systems // IRSE News, Issue 256, June 2019.

15. EUG, EULYNX. RCA Alpha – Architecture Overview, 2019.

16. OCORA Architecture – Alpha Release, 2019.

17. Shift2Rail ASTRail. D4.1 / Report on Analysis and on Ranking of Formal Methods. 2019. P. 26.

18. Estevan A.M. Dependability and safety evaluation of railway signalling systems based on field data. Doctoral thesis, Lulea, 2015.

19. Xie Y. Formal Modeling and Verification of Train Control Systems. Thesis, 2019.

20. Shift2Rail Multi-Annual Plan. 2015. P. 249.

Сведения об авторе

Алексей В. Озеров – начальник Международного управления АО «НИИАС», Москва, Российская Федерация, тел. +7 (495) 967-77-02, e-mail: A.Ozerov@vniias.ru

Вклад автора в статью

Озеров А.В. проанализировал основные параметры систем управления и обеспечения безопасности движения поездов на примере системы ERTMS/ETCS с учетом требований обеспечения надежности и безопасности на основе международных нормативных документов и стандартов, определил основные направления развития подходов в области проектирования, сертификации и омологации в условиях цифровой трансформации и перехода к новым парадигмам внедрения инноваций.