ПРОГРАММА
XI МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
«Системы безопасности на транспорте»

12-14 апреля 2018 г. Отель Best Western Premier Hotel Slon, Любляна, Словения

Модератор конференции:
***Розенберг Е.Н.**, д.т.н. проф., Председатель Проблемного совета АЭН РФ, Первый заместитель генерального директора АО «НИИАС»*

12 апреля 2018 года	
08:45–09:30	*РЕГИСТРАЦИЯ УЧАСТНИКОВ*
09:30	*ОТКРЫТИЕ КОНФЕРЕНЦИИ*
	Вступительное слово **Розенберг Ефим Наумович**, д.т.н., проф., Председатель Проблемного совета АЭН РФ, Первый заместитель Генерального директора АО «НИИАС»
	ДОКЛАДЫ
09:45–11:30	**I Сессия**
	Подходы МСЖД к вопросам обеспечения безопасности и кибербезопасности железнодорожных систем в условиях цифровизации **Марк Антони**, Директор департамента железнодорожных систем, Международный союз железных дорог (МСЖД)
	Основные вопросы развития цифрового транспорта **Розенберг Ефим Наумович**, д.т.н., проф., Председатель Проблемного совета АЭН РФ, Первый заместитель Генерального директора, АО «НИИАС»
	Деятельность железнодорожного научно-исследовательского института **Антонин Блажек**, доктор технических наук, директор по техническим вопросам, Институт железнодорожных исследований
	Оптимальная конструкция оптико-электронной системы всепогодного наблюдения для обеспечения безопасности движения железнодорожного транспорта **Бутырин Павел Анфимович,** д.т.н., президент АЭН РФ, член-корр. РАН
	Применение спутниковых технологий для IoT на железнодорожном транспорте **Филипп Моретто**, директор по маркетингу, Sat4M2M **Ханс де Вит**, директор по инновационному развитию, Sat4M2M
11:30–12:00	**КОФЕ-БРЕЙК**

12:00–15:00	**II Сессия**
	Синтез параметров тракта аналого-цифрового преобразования в системах управления, диагностики и обеспечения безопасности движения **Баранов Леонид Аврамович**, д.т.н., проф., заведующий кафедрой, Российский университет транспорта (РУТ)
	Структурные методы обеспечения безопасности в системах управления движением поездов **Бестемьянов Пётр Филимонович**, д.т.н., проф., директор института, Российский университет транспорта (РУТ)
	Развитие систем управления и обеспечения безопасности движения поездов **Шухина Елена Евгеньевна**, руководитель НТК, АО «НИИАС»
	Эволюция систем интервального регулирования движения поездов **Озеров Алексей Валерьевич**, начальник управления АО «НИИАС»
	Обеспечение кибербезопасности железных дорог – управление угрозами **Грега Прешерен**, менеджер по разработке продуктов в области кибербезопасности, Iskratel
	Основные направления и результаты деятельности рабочей группы «Кибербезопасность на железнодорожном транспорте» – COLPOFER **Ададуров Сергей Евгеньевич**, д.т.н., проф., заместитель генерального директора, АО «ВНИИЖТ»
15:00–16:00	**ОБЕД**
16:30–18:00	**Посещение Железнодорожного музея Словении**
19:30–21:00	**ТОРЖЕСТВЕННЫЙ УЖИН**
13 апреля 2018 года	
09:00–11:30	**III Сессия**
	Комплексирование информации и интеллектуальные решения для реализации технологии беспилотного управления локомотивом **Уманский Владимир Ильич,** заместитель генерального директора, АО «НИИАС»
	Разработка систем диагностики подвижного состава как средство повышения безопасности эксплуатации **Иньков Юрий Моисеевич**, д.т.н., проф., Российский университет транспорта (РУТ)
	Современные бортовые приборы обеспечения безопасности **Батраев Владимир Владимирович**, начальник сектора, АО «НИИАС»
	Система безопасности грузового поезда **Финк Юрий Михайлович**, генеральный директор, ООО «Финк Электрик»

	Перспективные направления систем управления и безопасности железнодорожного транспорта **Ципп Андрей Леонардович**, инженер, ООО «НПО САУТ»
	Применение систем M-Max в релейных системах автоматики **Клоков Александр Валентинович**, генеральный директор, ООО «МикроМакс Системс»
11:30–12:00	**КОФЕ-БРЕЙК**
12:00–15:00	**IV Сессия**
	Критически важные коммуникации на транспорте **Гейко Наталья Юрьевна,** руководитель направления, ПАО «Вымпел-коммуникации»
	Архитектура и организация информационно-коммуникационной системы на железной дороге **Зоран Ж. Аврамович**, проф., Белградский университет
	Основные аспекты перехода от системы IMS к FRMCS **Дэвид Шмид,** менеджер производственного подразделения, Iskratel
	Применение спутниковых систем связи на железнодорожном транспорте **Тамаркин Владислав Михайлович**, зам. руководителя Центра АО «НИИАС» **Филиппов Сергей Вячеславович**, коммерческий директор по Европейской части, Группа компаний «Искра»
	Обзор уровня киберзащищенности современных систем управления движением поездов на высокоскоростных магистралях **Хмелевская Наталья Владимировна**, директор Центра кибербезопасности, ФГУП «ЗащитаИнфоТранс»
	Киберзащищенность МПСУ ЖАТ. *Опыт компании «Бомбардье Транспортейшн (Сигнал)»* **Перов Алексей Алексеевич**, руководитель направления киберзащиты МПСУ ЖАТ, ООО «Бомбардье Транспортейшн (Сигнал)»
	Обеспечение безопасности критической информационной инфраструктуры **Гросс Вадим Александрович**, технический директор, ООО «Локотех-Сигнал», Содокладчик: эксперт Федеральной службы по техническому и экспортному контролю (ФСТЭК)
15:00–16:00	**ОБЕД**
14 апреля 2018 года	
10:00–19:00	**Выездное заседание участников конференции:** ■ подведение итогов конференции; ■ обсуждение протокола решения конференции; ■ церемония награждения участников; ■ заключительное слово организаторов конференции.

PROGRAM
OF XI INTERNATIONAL CONFERENCE
SAFETY & SECURITY SYSTEMS ON TRANSPORT

12-14 April 2018. Hotel Best Western Premier Hotel Slon, Ljubljana, Slovenia

Chairman:
Efim Rozenberg, *Doctor of Technical Sciences, Prof., member of Russian Academy of Electrotechnical Sciences, First Deputy Director General, JSC NIIAS*

12 April 2018	
08:45–09:30	*REGISTRATION*
09:30	*OPENING CEREMONY*
	Welcome speech **Efim Rozenberg**, Doctor of Technical Sciences, Prof., member of Russian Academy of Electrotechnical Sciences, First Deputy Director General, JSC NIIAS
	REPORTS
09:45–11:30	**Session I**
	UIC Vision of Safety & Security Aspects of Railway Digitalization **Dr. Marc Antoni**, Rail System Director, International Union of Railways (UIC)
	Key Aspects of Digital Transport Development **Efim Rozenberg**, Doctor of Technical Sciences, Prof., First Deputy Director General, JSC NIIAS
	Railway Research Institute, j.s.c. **Antonín Blažek**, Ph.D, Managing Director, Railway Research Institute
	The optimal design of an optoelectronic all-weather surveillance system for ensuring the safety of railway traffic **Pavel Butyrin,** Doctor of Technical Sciences, President of Academy of Electrotechnical Sciences
	Railway Applications of Satellite-based IoT **Philippe Moretto**, MSc/MBA – CMO, Sat4M2M **Hans de With**, Project and Innovation Director, Sat4M2M
11:30–12:00	**COFFEE BREAK**
12:00–15:00	**Session II**
	Synthesis of parameters of the analog-to-digital conversion tract in the control, diagnostics and traffic safety systems **Leonid Baranov**, Doctor of Technical Sciences, Prof., Head of Department, Russian University of Transport

	Structural methods for safety ensuring in railway control systems **Petr Bestemyanov**, Doctor of technical Sciences, Prof., Institute Director, Russian University of Transport
	Current trends in the development of the infrastructure complex of safety and traffic management devices **Elena Shuhina**, Head of the Scientific and Technical Complex, JSC NIIAS
	Evolution of Train Separation Systems **Alexey Ozerov**, Head of International Department, JSC NIIAS
	Cyber Security in Railways – managing the threats **Grega Prešeren**, Cyber Security Manager, Iskratel
	The key areas and results of activities of the COLPOFER Cybersecurity Working Group **Sergey Adadurov**, Doctor of Technical Sciences, Prof., Deputy Director
15:00–16:00	**LUNCH**
16:30–18:00	**Visit to the Slovenian Railway Museum**
19:30–21:00	**GALA DINNER**
13 April 2018	
09:00–11:30	**Session III**
	Integration of Data from Various Sources of Computer Vision **Vladimir Umanskiy**, Deputy Director General, JSC NIIAS
	Development of diagnostic systems for rolling stock to increase operation safety **Uri Inkov**, Doctor of Technical Sciences, Prof., Russian University of Transport
	Onboard Integrated Safety Systems **Vladimir Batraev**, Head of the Sector, JSC NIIAS
	Digital solutions for transport security **Uri Fink**, General Director, «Fink Electric» Ltd.
	Prospective directions for development of control and safety systems for railway transport **Andrey Zipp**, Engineer, NPO SAUT Ltd
	Application of M-Max solutions for the relay automation systems **Alexander Klokov**, Director general, Micromax Systems Ltd.
11:30–12:00	**COFFEE BREAK**
12:00–15:00	**Session IV**
	Critical Communications in Transport **Natalia Geyko**, Senior manager, VimpelCom
	Architecture and Organization of Railways Information and Communication System **Zoran Avramovic**, Prof., The University of Belgrade

	IMS based migration aspects towards FRMCS **David** Šmid, Product Manager, Iskratel
	Satellite technologies for railway transport **Vladislav Tamarkin**, deputy Head of the Center, JSC NIIAS **Co-speaker: Sergey Filippov**, Commercial Director, Group of companies «Iskra»
	Overview of cybersecurity level of modern train control systems on the high-speed lines **Natalia Chmelevskaya**, Director of Cybersecurity Center, FGUP «ZashchitaInfoTrans»
	Cyber security solution for train control systems. Experience of Bombardier Transportation (Signal) **Alexey Perov**, Head of Cybersecurity Department, Bombardier Transportation (Signal) Ltd.
	Safety of Critical Information Infrastructure **Vadim Gross**, Technical Director, Locotesh-Signal Ltd., **Co-speaker**: expert from the Federal Service for Technical and Export Control of Russia
15:00–16:00	Lunch
14 April 2018	
10:00–19:00	*Visiting Session:* ■ Summarizing of the Conference; ■ Discussion of the Conference decision protocol; ■ Awarding ceremony; ■ Closing remarks.

Marc Antoni

International Union of Railways (UIC)

UIC Vision of Safety & Security Aspects of Railway Digitalization

Railways are generally considered as critical infrastructure. This means that failures and incidents could ultimately result in disruption of normal operations of a state.

Until recently, it has been thought that railway signalling systems are isolated from external impacts, and therefore, are immune to any cybersecurity threats and attacks. This is no longer the case. In the growing digital environment, the cyber risk is not a myth, it is a reality. Now the idea is how to provide resilience, rather than to preserve immunity.

There is a strong interrelation between system safety and system security as regards the availability of authorized functions. The safety and security of a system in general terms means that a system does what it is supposed to do and does not do what it is not supposed to do.

What is common to safety and security is the fact that there is neither absolute safety nor absolute security. Both concepts should deal with residual risk which is the combination of event frequency (probability) and its consequences (harm). The point is what kind of residual risk could be accepted as an inevitable evil.

From the UIC's point of view, Security is Safety and Safety is Security. Therefore, the design of a safety critical system must consider security challenges. It should include the right "axioms" using formal methods, consider operational rules and management of the degraded mode, follow a multi-layered approach and preserve Class1 relay etc.

The UIC sees its task in providing railway undertakings with an integrated approach to safety and security issues in the form of International Railway Standards (IRS) and Guidelines as well as in the form of specific tools and project cases.

Марк Антони

Международный союз железных дорог (МСЖД)

Подходы МСЖД к вопросам обеспечения безопасности и кибербезопасности железнодорожных систем в условиях цифровизации

Железные дороги считаются критически важной инфраструктурой, поэтому различные сбои и отказы потенциально могут привести к нарушению жизнедеятельности всего государства и общества.

До недавнего времени было принято считать, что системы железнодорожной сигнализации изолированы от внешних воздействий и потому не подвержены каким-либо угрозам кибербезопасности и кибератакам. Теперь ситуация изменилась, и киберугрозы стали реальностью. Сегодня в фокусе внимания находится обеспечение устойчивости, а не сохранение неуязвимости.

Между безопасностью и кибербезопасностью системы существует сильная взаимосвязь с точки зрения функциональной готовности железнодорожных систем для авторизированных сторон. В общем и целом, безопасность и кибербезопасность системы означают, что система выполняет те функции, для которых она предназначена, и не выполняет те функции, которые не предусмотрены системой.

Общей чертой безопасности и кибербезопасности является отсутствие как абсолютной безопасности, так и абсолютной кибербезопасности. И в том, и в другом случае приходится иметь дело с остаточным риском, который представляет собой сочетание частоты (вероятности) события и его последствий (вреда). Вопрос заключается в том, какой уровень остаточного риска можно принять как «неизбежное зло».

Согласно подходу МСЖД, безопасность и кибербезопасность неразделимы. Вопросы кибербезопасности должны учитываться еще на этапе проектирования критически важных систем. Необходимо изначально включать в систему правильные «аксиомы» с применением формальных методов, учитывать правила эксплуатации и управление режимом ограниченной функциональности, применять многоуровневый подход с сохранением реле 1-го класса и т.д.

Со стороны железнодорожных предприятий существует явная потребность в некотором общем системном подходе:

- Необходимо интегрировать эксплуатационные требования (операции) и средовые требования (окружение, топология, бизнес) к безопасности и кибербезопасности.
- Безопасность и кибербезопасность неразделимы. Данные концепции связаны между собой на уровне системы.
- Кибербезопасность должна быть включена в процесс управления активами.

МСЖД стремится к тому, чтобы выработать для железнодорожных предприятий комплексный подход к вопросам обеспечения безопасности и кибербезопасности в виде международных железнодорожных стандартов (IRS) и руководящих документов, а также в форме конкретных инструментов и проектов.

Rozenberg Efim
JSC NIIAS

Key Aspects of Digital Transport Development

The concept of «Digital railway» is the basis for the development of the modern railways both in Russia and around the world. This concept is presented in the UIC Roadmap for digital railways as well as in the EU Shift2Rail innovation program. The key block of Shift2Rail is the program IP2 which covers such areas as automatic train operation, safe train positioning, virtual coupling, cybersecurity etc.

Russian Railways (RZD) has developed the Comprehensive program of Innovative Development for 2016-2020. A high accuracy coordinate system (HACS) on the basis of GLONASS is being implemented on the Russian Railways network. Such system allows implementing innovative coordinate models in the onboard train control and protection systems.

On the basis of HACS the digital route maps integrated in GLONASS/GPS-enabled onboard train control and train protections systems (KLUB-U, BLOCK) are being improved.

The capability of scheduled monitoring with coordinate referencing of data on track deterioration and non-compliance with standard maintenance requirements within the single HACS coordinate space allows the collection and accumulation of the information on failures associated with non-compliant track geometry.

There are prospects for correlated data of many measurements at railway infrastructure facilities to be taken and processed for the purpose of identifying critical deviations from standard requirements and onset of pre-failure conditions based on the URRAN methodology, as well as targeted deployment of Internet of Things (IoT) software and hardware, and Big Data technology.

Russian railways has been developing and testing the ATO technology. At the Luzhskaya freight terminal, an automatically controlled shunting locomotive has been tested successfully. An additional technology for controlling the shunter from a remote operator workstation is now being tested at the same site.

Cybersecurity issues are of great importance for Russian Railways. Basic regulatory documentation was developed by the RZD experts.

Розенберг Ефим Наумович
АО «НИИАС»

Основные вопросы развития цифрового транспорта

Концепция «цифровой железной дороги» является основой развития современных железных дорог в России и в мире.

Концепция представлена в «Дорожной карте цифровых железных дорог» МСЖД, а также сформулирована в рамках программы инновационного развития железнодорожного транспорта ЕС Shift2Rail.

Ключевым блоком Shift2Rail является инновационная программа IP2 «Инновационные системы управления и обеспечения безопасности движения поездов», охватывающая такие направления, как беспилотное управление, безопасная система позиционирования поезда с применением спутниковой навигации, виртуальная сцепка, кибербезопасность и др.

В ОАО «РЖД» разработана и активно реализуется Комплексная программа инновационного развития на период 2016-2020 гг. На сети ОАО «РЖД» внедряется высокоточная координатная система (ВКС) на основе ГЛОНАСС, обеспечивающая переход на использование инновационных координатных методов в задачах управления инфраструктурой, перевозочным процессом и обеспечения безопасности движения поездов.

На основе высокоточных координатных моделей пути ведется совершенствование цифровых карт маршрутов, применяемых в составе оборудованных средствами ГНСС ГЛОНАСС/GPS бортовых комплексов управления и обеспечения безопасности движения поездов (КЛУБ-У, БЛОК).

Возможность периодического мониторинга с координатной привязкой данных о расстройствах пути и отклонениях от норм содержания в едином координатном пространстве ВКС позволяет получать и накапливать информацию об отказах по причине нарушения нормативов геометрии рельсовой колеи.

Благодаря этому появляется возможность увязки данных различных измерений и их обработки с целью выявления критичных отклонений от нормативов, и формирования предотказных состояний с использованием методологии УРРАН, а также внедрения аппаратно-программных средств «Интернета вещей» и технологии Big Data.

В ОАО «РЖД» разрабатывается и тестируется технология беспилотного движения. На сортировочной станции Лужская Октябрьской железной дороги успешно испытана технология роспуска вагонов с полностью автоматически управляемым горочным локомотивом. На полигоне тестируется технология телеуправления маневровым локомотивом с удаленного рабочего места оператора-машиниста. Ведется работа по адаптации данной технологии применительно к управлению движением пассажирских поездов на МЦК.

Большое внимание уделяет вопросам кибербезопасности. Разработан пакет отраслевых документов, ведется планомерная работа по проверке на киберзащищенность всех АСУ ЖТ, разрабатываются новые методологические подходы к обеспечению кибербезопасности систем управления ОАО «РЖД».

Antonín Blažek

Railway Research Institute, j.s.c.

Railway Research Institute

The contribution is focused on basic activities and technical equipment of the Railway Research Institute, j.s.c. (VUZ). VUZ provides professional services and comprehensive solutions in the field of assessment, testing and consultancy for railway systems and railway transport. The basis for providing these services is the Test Center VUZ Velim with two test rings, power supply station, dynamic test laboratory, test preparation halls and other administrative facilities. One of VUZ's key activities is the area of assessment and evaluation. The VUZ has the necessary authorization documents for the assessment and evaluation of individual railway subsystems. The contribution informs about the scope of VUZ activities in this area, including the procedure for the approval of subsystems into operation and the VUZ's scope of these activities on the international market.

Антонин Блажек

Железнодорожный научно-исследовательский институт

Деятельность железнодорожного научно-исследовательского института

В своем докладе автор уделяет особое внимание основным направлениям деятельности железнодорожного научно-исследовательского института (VUZ). Институт предоставляет профессиональные услуги и комплексные решения в области оценки, тестирования и консалтинга по железнодорожным системам и железнодорожному транспорту. Основой предоставления таких услуг является испытательный центр института Velim с двумя полигонами, электростанцией, лабораторией для проведения динамических испытаний и т.д. Одним из основных направлений деятельности является оценка и сертификация железнодорожных систем.

Butyrin Pavel

Russian Academy of Electrotechnical Sciences

The optimal design of an optoelectronic all-weather surveillance system for ensuring the safety of railway traffic

An optoelectronic system for surveillance in poor weather conditions (darkness, fog, slightly smoggy atmosphere) and reliable detection and identification of potentially dangerous objects (people, animals, various obstacles) is considered.

The developed devices can be installed on transport facilities as well as free-standing infrastructure facilities (contact-line mast, lighting towers, etc.) in order to automatically analyze the traffic situation (detecting and counting vehicles and pedestrians).

The optimal design of an optoelectronic system includes composite optical and thermal-imaging channels that provide longer objects detection range, improved objects recognition and identification when combined

The developed optoelectronic system has smaller weight-size parameters compared to the existing devices.

The developed device designs are efficient in a wide range of operating temperatures and are resistant to atmospheric factors (dust, snow, rain, etc.).

The materials used in the optical path are low cost and are processed with innovative patented technologies.

Бутырин П.А., Смирнова Е.И., Товмасян В.М., Шакирзянов Ф.Н.

Академия электротехнических наук РФ , Национальный исследовательский университет «МЭИ»

Оптимальная конструкция оптико-электронной системы всепогодного наблюдения для обеспечения безопасности движения железнодорожного транспорта

Рассмотрена оптико-электронная система, предназначенная для обеспечения возможности наблюдения обстановки в сложных погодных условиях (темное время суток, туман, легкая задымленность атмосферы), надежного обнаружения и идентификации потенциально опасных объектов: люди, животные, различные препятствия.

Разработанные приборы, помимо непосредственной установки на объектах транспорта, могут быть размещены на отдельно стоящих объектах инфраструктуры (например, на опорах контактной сети, на осветительных башнях и т.п.) с целью автоматического анализа дорожной обстановки (обнаружения и подсчета транспортных средств и пешеходов).

Структура оптимальной по конструкции оптико-электронной системы включает совмещенные оптический и тепловизионный каналы, обеспечивающие, при совместном использовании, повышенные технические характеристики: большую дальность обнаружения объектов, улучшенные показатели их распознавания и идентификации, что обеспечивает высокий уровень безопасности управления транспортными средствами.

Кроме того, в отличие от существующих приборов, разработанная оптико-электронная система обладает меньшими массо-габаритными параметрами, достигаемыми за счет запатентованной конструкции, обеспечивающей соосное совмещение оптического и тепловизионного каналов.

Разработанные конструкции приборов работоспособны в широком диапазоне рабочих температур и устойчивы к воздействию атмосферных факторов (пыль, снег, дождь и т.п.).

Отличительной чертой материалов, используемых в оптическом тракте прибора, является их низкая стоимость, обеспечивающаяся за счет инновационных запатентованных технологий получения высококачественных оптических материалов, прозрачных в широком диапазоне спектра. Высокое качество оптического тракта обеспечивается также использованием специальных защитно-просветляющих покрытий.

Работа проводилась при поддержке РФФИ для реализации проекта № 17-20-03151-офи-м-РЖД.

Hans de With, Philippe Moretto
SAT4M2M

Railway Applications of Satellite-based IoT

Today, in many occasions business optimisation based on advanced big data analysis is not achievable because the available data is unreliable, patchy and/or expensive.

It is well known that today there is a lack of data continuity due to poor GSM-based service in rural areas, even within Central Europe. Existing telematics services are regarded as too expensive for the limited service level they can provide, especially in transnational operation (roaming costs etc.) and operations in rural and remote environments.

The TELDASAT system/service provides IoT/M2M data connectivity service over satellite, concentrating on global, energy-autonomous operations at low cost.

The feasibility study shows that the opportunity lies in the provision of IoT data connectivity where no reliable (terrestial) service is available or as a back-up solution, using a device that has sufficient autonomy (battery life) to send the data reliably and securely for many years, at a low cost, comparable to LPWA connectivity providers such as SigFox and LoRa.

The main drivers, given an acceptable cost level, are therefore autonomy and coverage. This service can be referred to as Low Power Ultra Wide Area Network, or LPUltraWA, and is expected to be much in demand in future.

The total addressable market is a combination of the traditional SpaceIoT market – conservatively estimated at 5% of the total IoT market – and capturing part of the traditional LPWAN IoT market by enriching their connectivity through space. The market space of enriching LPWAN is a Blue Ocean market opportunity, and will grow over time from 0 to 5% of the total IoT market. Therefore, the market share for Space IoT will double from the traditional SpaceIoT share today from 5 to 10% of the IoT market potential.

Ханс де Вит, Филипп Моретто
SAT4M2M

Железнодорожное применение спутникового Интернета вещей

В современных условиях задачи оптимизации бизнес-процессов на основе использования передовых методов анализа «Больших данных» (Big Data) оказываются невыполнимыми ввиду того, что доступные данные ненадёжны, фрагментарны и/или дорогостоящи.

Хорошо известно, что сегодня даже в Центральной Европе ввиду низкого качества GSM-связи в сельской местности отсутствует непрерывная система передачи данных. В Восточной Европе, где наземные системы связи сосредоточены в густонаселённых районах, ситуация ещё хуже. В России на железнодорожном транспорте информация собирается при помощи напольных средств, которые обеспечивают полноту сведений, но только в определённых точках, что не позволяет должным образом организовать оперативное управление парком подвижного состава и обслуживание по состоянию. Существующие телематические сервисы считаются излишне дорогостоящими, учитывая ограниченность их возможностей, в особенности применительно к международным операциям (стоимость роуминга и т.д.) и операциям в сельской местности и труднодоступных районах.

Система/сервис TELDASAT обеспечивает сервис обмена данными IoT/M2M на базе спутниковой связи посредством использования низкоза-тратных глобальных энергоавтономных технических средств.

Проведённое технико-экономическое обоснование показало, что решение проблемы заключается в обеспечении передачи IoT-данных там, где нет надёжного (наземного) сервиса, либо в качестве резервного решения, используя устройство, обладающее значительной автономией по питанию, для надёжной отправки данных в течение многих лет, относительно недорогой в сравнении с такими LPWA-сервисами, как SigFox и LoRa.

Таким образом, при условии обеспечения приемлемой стоимости ос-новными стимулами к внедрению такого решения будут автономность и покрытие. Такой сервис можно называть «энергоэффективной сетью сверхдальнего радиуса действия» (Low Power Ultra Wide Area Network, LPUltraWA), и можно ожидать, что в перспективе он будет пользоваться большим спросом.

Общий потенциальный рынок можно оценить как сумму традиционного космического Интернета вещей, который по сдержанным оценкам составляет 5% от рынка Интернета вещей в целом, и части рынка традиционного Интернета вещей на базе LPWAN, который можно занять посредством внедрения космического сегмента в схему передачи данных. Рыночное пространство расширенного LPWAN представляет собой возможный рынок «голубого океана», который со временем вырастет с 0 до 5% от общего рынка Интернета вещей. Следовательно, доля космического Интернета вещей в общей структуре рынка Интернета вещей удвоится с 5 до 10 %.

Baranov Leonid

Russian University of Transport (RUT – MIIT)

Synthesis of parameters of the analog-to-digital conversion tract in the control, diagnostics and traffic safety systems

The analog-to-digital conversion tract is widely used in modern digital traffic control and analog diagnostic systems. The author deals with the questions of synthesis of tract for analog-to-digital conversion in the control, diagnostics and traffic safety systems.

In particular, speed control system and system of target point of braking of the rolling stock use analog-to-digital converters (ADC) as «velocity-to-digit» and «distance covered-to-digit». Modern relay protection systems of traction substation feeders (the so-called «intelligent protection systems») use ADC «current-to-digit» and digital analysis of measured signals. To select signal parameters in the track circuits (TC) of the traffic safety system digital interference measurements in the TC with further digital processing are experimentally carried out. In closed control systems, the analog-to-digital conversion tract errors are not parried by the system feedback. The selection of the analog-to-digital conversion tract parameters, as well as the choice of the control law, determines the system performance level. The systematic errors of the analog-to-digital conversion tract are determined by the quantization by level errors and temporal sampling upon the given recovery method. When the value of the signal dispersion is significantly greater than the square of the quantization by level step, the conversion error dispersion equals the sum of quantization by level errors dispersion, temporal sampling and output noise of the conversion tract. The author proposed a method to select temporal sampling step for a given input signals model.

Баранов Леонид Аврамович

Российский университет транспорта (МИИТ)

Синтез параметров тракта аналого-цифрового преобразования в системах управления, диагностики и обеспечения безопасности движения

Тракт аналого-цифрового преобразования используется во всех современных цифровых системах управления и диагностики аналоговых процессов. В частности, системы управления скоростью, прицельной остановкой подвижного состава используют аналого-цифровые преобразователи (АЦП) скорость-цифра, пройденный путь-цифра. Современные системы релейной защиты фидоров тяговых подстанций (так называемые «интеллектуальные системы» защиты), используют АЦП ток-цифра и цифровой анализ измеряемых сигналов. Для выбора параметров сигналов в рельсовых цепях системы обеспечения безопасности движения экспериментально производятся цифровые измерения помех в этих цепях с дальнейшей их цифровой обработкой. Отдельно отметим, что в замкнутых системах управления погрешности тракта аналого-цифрового преобразования не парируются обратной связью системы. Качество функционирования рассматриваемых систем определяет выбор параметров тракта аналого-цифрового преобразования так же, как и выбор закона управления. Методические погрешности аналого-цифрового преобразования определяются погрешностями квантования по уровню и временной дискретизацией при заданном способе восстановления. Помехоустойчивость определяется уменьшением отношения мощности помехи к мощности сигнала на выходе аналого-цифрового преобразования. Доказано, что погрешность квантования по уровню, определяемая разрядностью АЦП, можно рассматривать не коррелированной с сигналом, когда дисперсия сигнала много больше квадрата шага квантования по уровню. Тогда дисперсия погрешности преобразования ровна сумме дисперсии погрешностей от квантования по уровню, временной дискретизации и помехи на выходе тракта преобразования. Дисперсию квантования по уровню можно оценить как $q^2/12$, где шаг квантования по уровню $q=(x_{max}-x_{min})/(2^n-1)$ n – разрядности АЦП, $x_{max}-x_{min}$ диапазон изменения входного сигнала. Моделью восстанавливающего оператора в системах управления, диагностики, обеспечения безопасности обычно является экстраполятор нулевого порядка ЭНП (ступенчатое восстановление), амплитудно-фазовая характеристика которого имеет вид (1), где T – шаг временной дискретизации, ω – частота. Откуда следует, что ЭНП является фильтром нижних частот, носящим запаздывания на $T/2$. В ряде публикаций обоснованием выбора шага временной дискретизации является теорема Котельникова, в соответствии с которой $T=1/2F_{max}$, где $F_{max}=\omega_{max}/2\pi$ максимальная частота входного сигнала. Однако в теореме Котельникова восстанавливающий оператор – идеальный фильтр нижних частот. Замена его экстраполятором нулевого порядка приводит к среднеквадратической погрешности преобразования равной 141% по отношению к среднеквадратическому отклонению входного сигнала. Для этого разработана методика выбора шага временной дискретизации при заданной модели входного сигнала.

$$K(j\omega)=\frac{\frac{\sin\omega T}{2}}{\frac{\omega T}{2}}Te^{-i\omega\frac{T}{2}}, \quad (1)$$

Bestemyanov Petr

Russian University of Transport (RUT – MIIT)

Structural methods for safety ensuring in transport control systems

The algorithm of the safety system equipment at the centralized placing includes the following basic guidelines: all actions related to the management and control of trackside devices as well as commands for making critical decisions must be constantly controlled and checked. Two sets of equipment are used. Each microcomputer has its own software. The security of the system is ensured by the redundancy of each module that runs under its own disk-operating system. The modules are connected via the serial communication link. The two sets are synchronized programmatically. The modules outputs are compared by the monitoring circuit with asymmetric failures. The system has a built-in diagnostics that detects and indicates failures. The channeling equipment uses multiple transmission of information, as well as information messages redundancy. The comparison elements and executive elements for the implementation of critical commands follow the principles of self-monitoring of single failures. The duration of the cyclic processing of information from communication channels periods is monitored. Information processing channels cycle through the operational and test information. The soft synchronization of channels allows their failures due to external interference to be considered independent, while each information processing channel software has different algorithms, execution times for the elementary blocks of the program, and output options for the semantic information received by the monitoring circuit with asymmetric failures. The safety of the comparison device circuit, input circuits isolation elements and single failures executive elements is ensured by the dynamic work principles using polarity converters and galvanic separation units. All independent information processing channels convert control information into a serial message received by the safe comparison circuit. Different software tools in information processing channels are used to ensure software security. The absence of errors in the software proof is based on the data processing tasks specification control.

Бестемьянов Пётр Филимонович

Российский университет транспорта (МИИТ)

Структурные методы обеспечения безопасности в системах управления на транспорте

Алгоритм работы аппаратуры системы обеспечения безопасности движения поездов при централизованном размещении включает в себя следующие основные положения: постоянно должны контролироваться и проверяться все действия связанные с управлением и контролем напольных устройств, а также команды на принятие ответственных решений. Для решения этих проблем используются два комплекта аппаратуры. В каждой микро ЭВМ имеется свое программное обеспечение. Концепция обеспечения безопасности базируется на следующих основных принципах. Безопасность системы обеспечивается дублированием каждого модуля, которые работают под своей дисковой операционной системой. Взаимосвязь модулей осуществляется на основе обмена данными по последовательному каналу связи. Синхронизация работы двух комплектов осуществляется программным способом. Сравнение результатов работы модулей осуществляется схемой контроля с односторонними отказами. Предусмотрена встроенная диагностика, выявляющая и индицирующая отказы, в том числе в системе предусмотрен фоновый тест в каналах обработки информации, который способствует обнаружению скрытых ошибок. В каналообразующей аппаратуре используется многократная передача информации, а также избыточность в информационных сообщениях с минимальным кодовым расстоянием по Хэммингу d_{min}=4. Элементы сравнения и исполнительные элементы для реализации ответственных команд строятся по принципам самоконтроля одиночных отказов. Производится контроль длительности периодов циклической обработки информации, поступающей из каналов связи. Каналы обработки информации циклически обрабатывают рабочую и тестовую информацию. Осуществление мягкой синхронизации между каналами позволяет считать независимыми их отказы под действием внешних помех, при этом программное обеспечение в каждом канале обработки информации имеет разные алгоритмы работы, разное время выполнения элементарных блоков программы и разные варианты вывода семантической информации, поступающей на схему контроля с односторонними отказами. Безопасность схемы устройства сравнения, элементов изоляции входных цепей и исполнительных элементов по классу одиночных отказов обеспечивается принципами динамической работы с использованием преобразователей полярности и гальванических развязок как элементов защиты от подпиток ответственных цепей. Каждый из независимых каналов обработки информации содержит специальный преобразователь контрольной информации в последовательное сообщение, синхронно поступающее на безопасную схему сравнения. Концепция обеспечения безопасности в программных средствах базируется на использовании разных программных средств в каналах обработки информации. При этом гарантия отсутствия ошибок в программном обеспечении основана на контроле спецификации задач обработки данных.

Shuhina Elena

JSC NIIAS

Current trends in the development of the infrastructure complex of safety and traffic management devices

The author deals with the current trends in the development of the safety and traffic management infrastructure complex.

The train control and protection systems science and technology complex (STC) of JSC NIIAS covers such areas as new principles of design, signaling, organization of a modern secure radio channel, risk assessment and further automation.

JSC NIIAS specialists have implemented innovative principles of traffic management on the Small Moscow Ring Road using a modern Automatic Block System (ABTC-MSh).

A dynamic high-precision locomotive localization system with optical vibration sensors and reference points based on track circuits is already developed and is being tested.

The STC has developed such products as integrated train control and protection systems, secure legally significant data transfer systems based on certified tools, automatic train operation and remote control systems, diagnostic systems.

Шухина Елена Евгеньевна

АО «НИИАС»

Современные тенденции развития инфраструктурного комплекса устройств безопасности и организации движения

Доклад посвящен современным тенденциям развития инфраструктурного комплекса организации движения и обеспечения безопасности. Обилие технологических задач и реализующих их систем подтверждает необходимость рассматривать в комплексе системы автоматики, телемеханики и информатизации как взаимосвязанную структуру управления и обеспечения безопасности.

В рамках задач Научно-технического комплекса систем управления и обеспечения безопасности движения поездов АО «НИИАС» основной целью является переход к единому комплексу цифровизации и организации движения, который должен реализовывать базу для дальнейшего увеличения маршрутной скорости и обеспечения высочайшего уровня безопасности.

Бортовые устройства и СЦБ – это инструмент для реализации задачи верхнего уровня, используемый в качестве достоверного датчика информации и исполнительного модуля воздействия. Требуется отметить, что при этом безопасность выходит на более высокий уровень, так как исключается влияние человеческого фактора.

Новые принципы проектирования, сигнализации, организация современного защищенного радиоканала, оценка рисков и дальнейшая автоматизация управление локомотивом – вот направления, которые охватывает работа НТК.

Силами специалистов АО «НИИАС» в настоящее время реализованы современные принципы организации движения на Малом московском кольце, современная система автоблокировки АБТЦ-МШ, благодаря защищённому высокоскоростному радиоканалу, работает в едином комплексе с бортовыми устройствами, а также имеет возможность увязки с отраслевыми АСУ и аппаратно-программными комплексами диспетчерского контроля.

Уже в настоящее время организована и проходит апробацию динамическая система высокоточного позиционирования локомотива, как по оптическим датчикам вибрации, так и по запатентованным точечным синхроузлам на базе рельсовых цепей.

Единые системы управления и обеспечения безопасности, системы защищенной юридически значимой передачи данных на базе сертифицированных средств, системы автоведения и дистанционного управления, а также системы диагностики – это доказанные и закрепленные правовыми документами разработки НТК, которые позволят осуществить переход к современной железной дороге в соответствии со Стратегией развития железных дорог до 2030 года.

Ozerov Alexey
JSC NIIAS

Evolution of Train Separation Systems

Today the innovative development of the railway sector is based on the implementation of digital technologies. The main objectives of the «digital railway» concept are:

- Increase of capacity;
- Trackside infrastructure cost reduction;
- Traffic optimization and adaptive planning.

To achieve these goals, new technical solutions for train separation are needed.

One possible solution is moving from the traditional train separation principles based on fixed block signaling with trackside signals to virtual block signalling without trackside signals. This solution can be implemented using both radio channel and track circuits (as it is done at the Moscow Ring).

The next evolution step is train separation based on full moving block. In this case the minimum permissible headway between trains following one another on the same track is determined based on the safe braking distance. This solution can be most useful on high-density suburban lines or intra-city metropolitan railways.

Implementation of this approach together with trackside infrastructure reduction requires fulfillment of a number of conditions such as a reliable wireless communication infrastructure, high-precision positioning means, and train integrity and track vacancy control.

The alternative approach to the moving block principle is the “virtual coupling” concept. The idea is that a group of trains that are not mechanically coupled but rather linked together by radio channels is treated as a single train. The most promising condition for this principle is driverless train operation. In this case virtually linked trains actually form a single network with a master-slave type of management. An important prerequisite here is the availability of synchronized control and safety computer devices of the same type with a single algorithm of operation installed on all units.

Озеров Алексей Валерьевич
АО «НИИАС»

Эволюция систем интервального регулирования движения поездов

Основой инновационного развития железнодорожной отрасли на текущем этапе является переход к концепции «цифровой железной дороги». Ее основными задачами являются:

- Повышение пропускной способности;
- Сокращение затрат на напольную инфраструктуру;
- Оптимизация графика движения и адаптивное планирование.

Для реализации указанных задач требуется разработка новых технических решений в области интервального регулирования.

Одним из таких решений является переход от традиционных принципов интервального регулирования на основе светофорной сигнализации с фиксированными блок-участками к бессветофорной сигнализации с виртуальными блок-участками. Данное решение может быть реализовано как с использованием радиоканала, так и на базе рельсовых цепей (как это сделано на МЦК).

Дальнейшая эволюция видится как переход к интервальному регулированию на основе полностью подвижного блок-участка. В этом случае разделение попутно следующих поездов осуществляется исходя из длины безопасного тормозного пути, который и определяет минимально допустимый интервал попутного следования. Данное решение является наиболее целесообразным для применения на высоконагруженных пригородных участках или внутригородских железных дорогах мегаполисов.

При одновременном сокращении напольной инфраструктуры реализация данного подхода требует целого ряда условий – наличие надежной инфраструктуры беспроводной связи, высокоточных средств позиционирования, контроля полносоставности и свободности пути.

В качестве альтернативы подвижному блок-участку рассматривается организация движения поездов по принципу «виртуальной сцепки». В этом случае группа попутно следующих поездов управляется как единый объект, части которого связаны не механически, а при помощи радиоканала. Реализация движения по данному принципу представляется наиболее перспективной в условиях перехода к беспилотному управлению движением поездов. В данном случае виртуально сцепленные поезда фактически образуют единую сеть с управлением по принципу «ведущий-ведомый». Важным условием при этом является наличие на подвижных единицах синхронизированных между собой однотипных компьютерных устройств управления и обеспечения безопасности с единым алгоритмом действия.

Grega Prešeren
Iskratel

Cyber Security in Railways – managing the threats

New era of transport digitalization beside a great deal of benefits bring also its dark side – the cyber threats. Which are the threats, where do they come from, how to avoid them and most importantly, how to minimize the damage they might cause? These are the questions that need a special attention in every aspect of product life cycle. From product specification, architecture design, coding, testing and integration, to field deployment, maintaining and customer education, security is always a subject of a special focus.

In addition, the transport infrastructure is very complex organization with huge amount of equipment placed along railroad tracks. The systems that have been used to control and communicate are located along the routes in stations, road crossings, signal towers, tunnels, maintenance yards, power stations, etc. Every part of every business activity in the Railway sector relies in some way on computerized system (an IT). Transit control systems can be grouped into different types such are traffic control systems, SCADA systems, communication systems, Incident control systems, data transportation systems and fare collection systems.

Today, it is not enough for IT systems to perform efficiently and continuously; and to also provide greater added value for users through their mutual integration. They must also ensure that unauthorized persons cannot access and steal or compromise the data. A key role in data protection and damage reduction has a decision support system. The main tasks that this system performs are evaluation of the cyber threat, identification, localization and prioritization of suspected cyber events, decision support and analysis of the threat.

How to fulfil the «security by design» principles and managing the cyber threats will be shown on concrete railway application examples.

Грега Прешерен
ИСКРАТЕЛ

Обеспечение кибербезопасности железных дорог – управление угрозами

Новая эра цифровизации транспорта также влечет за собой новые угрозы, а именно угрозы кибербезопасности. Что представляют собой такие угрозы, как они появились, как их избежать и, самое главное, как минимизировать ущерб, который они могут нанести? Решение данных вопросов требует особого внимание на всех этапах жизненного цикла продукта.

Транспортная инфраструктура представляет собой достаточно сложную систему с огромным количеством устройств и оборудования, расположенных вдоль железнодорожного пути. Функционирование таких устройств и оборудования зависит от компьютеризированных систем, которые должны быть защищены от различного рода кибератак. В своем докладе автор представит основные принципы обеспечения безопасности и управления киберугрозами на железнодорожном транспорте.

Adadurov Sergey

JSC VNIIZHT

The key areas and results of activities of the COLPOFER Cybersecurity Working Group

The author deals with the venues of international cooperation of the COLPOFER Cybersecurity Working Group in the areas of information security and cybersecurity on railway transport.

In 2013 within the framework of the international organization COLPOFER Cybersecurity Working Group was established to exchange experiences and information related to cybersecurity in the railway environment, develop recommendations regarding data protection and support cybersecurity system deployment. The author also analyzes the main documents with the recommendations for the critical information infrastructure security:

- Cybersecurity measures and techniques for the railway critical information infrastructure;
- Application of cybersecurity measures to detect and prevent computer attacks on the information infrastructure of the railway transport;
- Application of recovery methods after cyber attacks on the information infrastructure of the railway transport.

Ададуров Сергей Евгеньевич

АО «ВНИИЖТ»

Основные направления и результаты деятельности рабочей группы «Кибербезопасность на железнодорожном транспорте» – COLPOFER

Для совместного решения проблем информационной безопасности и кибербезопасности на железных дорогах России и Европы в рамках международной организации COLPOFER, объединяющей службы безопасности европейских железных дорог и подразделения полиции на железнодорожном транспорте, в 2013 году под председательством ОАО «РЖД» была создана рабочая группа «Кибербезопасность на железнодорожном транспорте».

Обозначены следующие цели функционирования рабочей группы:

- организация обмена опытом и информацией в области обеспечения кибербезопасности информационной инфраструктуры;
- разработка рекомендаций по защите информационной инфраструктуры;
- оказание методической и, при необходимости, иной поддержки на всех этапах организации защиты инфраструктуры от кибератак.

На заседаниях рабочей группы «Кибербезопасность на железнодорожном транспорте» российская сторона, опираясь на собственный опыт по созданию систем обеспечения и управления информационной безопасностью холдинга ОАО «РЖД», предложила к обсуждению следующие вопросы:

- формирование однозначно трактуемого понятийного аппарата и терминологии, разработка нормативных методических документов в области информационной безопасности и кибербезопасности на железнодорожном транспорте;
- разработка методологических подходов к защите от кибератак (компьютерных атак) в комплексе с минимизацией других угроз и обеспечением приемлемых рисков информационной безопасности;
- определение принципов организации работы в условиях полной или частичной невозможности использования устройств железнодорожной автоматики, связи, сигнализации и автоблокировки, средств вычислительной техники и автоматизированных систем управления и другие вопросы.

Для реализации указанных целей разработаны рекомендации по защите информационной инфраструктуры: «Основные положения защиты информационной инфраструктуры на железнодорожном транспорте от компьютерных атак», «Основные положения порядка использования сил и средств обнаружения и предупреждения компьютерных атак на информационную инфраструктуру железнодорожного транспорта», «Основные положения использования сил и средств ликвидации последствий компьютерных инцидентов в компьютерной инфраструктуре железных дорог».

В 2017 году разработаны документы: «Базовая модель угроз кибербезопасности в микропроцессорных системах железнодорожной автоматики и телемеханики» и «Базовые меры защиты информации в микропроцессорных системах железнодорожной автоматики и телемеханики». Также планируется разработать дополнительные документы в 2018-2019 годах.

Umanskiy Vladimir
JSC NIIAS

Integration of data from various sources of computer vision

Automatic locomotive operation requires reliable obstacles detection based on sensors of different physical nature, such as cameras, radar, lidars. Each of the devices has its advantages and disadvantages so the combination of them may bring good results. Data integration from sensors is a mathematical challenge since all information is of different type and asynchronous.

After the obstacle is detected it is monitored using the Kalman filter. When new measurements appear, the time from the last estimation is calculated, the expected location of the object is predicted and the object position is verified based on the received measurement data. The algorithm also defines and monitors the geometric dimensions of an object.

The position of each detected object relative to the path of the locomotive is evaluated. Depending on the proximity of obstacles to the path of motion, various actions are carried out, such as sound and light alarm application, reduction in speed and braking if necessary.

Уманский Владимир Ильич
АО «НИИАС»

Комплексирование данных различных источников технического зрения

Автоматическое управление локомотивом требует надежного обнаружения препятствий впереди движения, что возможно только при использовании датчиков разной физической природы, таких как камеры, радары, лидары. Каждый из перечисленных приборов имеет свои преимущества и недостатки, и их объединение позволяет получить хорошие результаты. Сложной математической задачей является комплексирование данных от датчиков, так как вся информация поступает в отличающемся виде в асинхронные моменты времени.

Агоритм обнаружения препятствий предполагает на первом шаге ассоциацию данных от разных источников. Особенностью обнаружения препятствий для локомотива является то, что на большом расстоянии объекты обнаруживаются датчиками в виде точки (например, одно отражение от лидара, 1-2 пикселя от камеры), а по мере приближения объекты представляют собой геометрическую фигуру. Задачей комплексирования является сопоставление информации от разных датчиков, причем в зависимости от расстояния комплексирование осуществляется либо как точечное, либо в виде сопоставления простейших геометрических фигур.

После обнаружения объекта-препятствия – выполняется его отслеживание на основе фильтра Калмана с оценкой состояния на каждом шаге. После поступления новых измерений вычисляется прошедшее время от последней оценки, выполняется предсказание ожидаемого местоположения объекта и производится уточнение местоположения на основе данных поступившего измерения. Важной особенностью алгоритма является также определение и отслеживание геометрических размеров объекта, моделируемой простейшей геометрической фигурой, такой как прямоугольник.

Для каждого обнаруженного объекта выполняется оценка его положения относительно пути движения локомотива. В зависимости от близости препятствий до пути движения выполняются разные действия бортового оборудования, такие как подача звукового и светового сигнала, снижение скорости и торможение при необходимости.

Inkov Uri, Kosmodamianskii Andrey, Pugachev Alexander
Russian University of Transport (RUT – MIIT)

Development of diagnostic systems for rolling stock to increase operation safety

The development of digital technologies promotes the development of the monitoring and diagnostics systems for the railway track. The most difficult task in the development process of such systems is the design technique. The author suggests using the method of variation of effects with the revealed particular functions, where the developer initially creates an ideal structure of object's functions, determines the physical effects that allow the implementation of such functions and specific technical solutions. The author concludes that the application of modern monitoring and diagnostics systems combined with the information technologies allows to perform a full cycle of checking the functional and technical status of the rolling stock equipment and develop recommendations on elimination or prevention of emergency situations during operations.

Иньков Юрий Моисеевич, Космодамианский А.С., Пугачев А.А.
Российский университет транспорта (МИИТ)

Разработка систем диагностики подвижного состава как средство повышения безопасности эксплуатации

Быстрое развитие цифровых технологий предопределяет столь же бурное развитие систем диагностики транспортных средств, как в процессе проектирования новых транспортных средств, так и в сфере эксплуатации, для оперативного решения проблем, выявляющихся в депо и ремонтных заводах по мере освоения новой техники. При этом основной трудностью становится сама методика проектирования. Анализ показывает, что необходимо использование таких методов создания системы диагностики, которые позволили бы избегать ошибок в условиях недостатка знаний и опыта. Одним из таких является метод вариации эффектов при выявленных частных функциях. Сущность этого метода заключается в том, что разработчик изначально создает идеальную структуру функций объекта, определяет физические эффекты, позволяющие реализовать данные функции и конкретные технические решения, в которых используются эти эффекты.

Типичное решение, принимаемое в эксплуатации, представляет собой вывод о способности диагностируемого объекта выполнять свои функции в течение определенного периода времени, на основании чего лицо, принимающее решение, производит действия, определенные регламентирующими документами. При обнаружении отказов оборудования, в том числе ограничения его функциональных возможностей в пути следования перед машинистом и службой эксплуатации стоит задача выбора конкретных действий. Осмысление потребности в выборе, формализация и перевод описания потребностей эксплуатационника в потребности разработчика диагностики происходят на постановочной стадии разработки. Авторами предложена реализация данного алгоритма на конкретном примере, в целях упрощения, полагая найденные решения одновариантными, и рассмотрены только процессы получения новой диагностической информации.

Синтез технических решений диагностических систем отчасти упрощается тем, что в большинстве случаев часть потребительских функций не уникальны, они поддаются типизации. Такие функции классифицированы в работе и представлены в виде иерархической системы. Основные потребительские функции систем диагностирования – получение информации (измерение), ее анализ, хранение, передача и отображение.

В качестве примера прогнозирования технического состояния подвижного состава рассмотрен вариант для двухсистемного электропоезда.

В заключении показано, что применение современных систем диагностики, синтезированных с использованием информационных технологий, позволяет осуществить полный цикл проверки функционального и технического состояния оборудования на подвижном составе и выработать (реализовать) рекомендации по устранению или предотвращению нештатных или аварийных ситуаций во время эксплуатации.

Batraev Vladimir
JSC NIIAS

Onboard integrated safety systems

The author deals with modern onboard control and safety units with new functions based on digital technologies.

JSC NIIAS is implementing the «Digital Railway» long term project including the concepts of «smart» station and «smart» locomotive.

Modern onboard control systems SOB-400 and BLOK-M were developed by NIIAS specialists. They can perform all existing functions of safety devices as well as support innovative solutions.

The current areas of work include the development of new generation of safety and control devices and insuring information security at the software level.

Батраев Владимир Владимирович
АО «НИИАС»

Бортовые интегрированные системы обеспечения безопасности

Доклад посвящен современным бортовым устройствам обеспечения безопасности и управления с реализацией новых функций на базе современных цифровых технологий, которые позиционируются, в настоящее время, как единая среда для интеграции существующих информационных систем, организующих перевозочный процесс, и предусматривают последовательную реализацию технологических и информационно взаимоувязанных комплексов, обеспечивающих функциональную полноту процесса перевозок.

В ходе работ по модернизации и разработке современных бортовых комплексов в АО «НИИАС» особое внимание было уделено «Стратегии развития цифровой железной дороги» и «Стратегии развития интеллектуального железнодорожного транспорта», благодаря которым однозначно формируется трехуровневая структура: «*Низовой*» уровень – минимум устройств на пути; «*Средний*» уровень – автоматическое управление маршрутами с реализацией на «верхнем» уровне; решение конфликтных ситуаций, включая новую технологию мобильной диагностики с подвижного состава объектов инфраструктуры на «среднем» уровне; «*Верхний*» уровень, обеспечивающий прогнозирование и расчет рисков.

В дальнесрочной перспективе должен быть реализован проект «Цифровая железная дорога», с реализацией концепций «умная» станция и «умный» локомотив.

В рамках развития Транспортной Стратегии РФ до 2030 года и реализации технологии создания высокоскоростных поездов (до 400 км/ч) и интеллектуальных систем управления разработаны: перспективный комплекс СОБ-400 (производство ДООО «ИРЗ-Локомотив») и модернизированный комплекс БЛОК-М (производство ПО «Октябрь»).

В данные современные бортовые комплексы заложены как все существующие функции приборов обеспечения безопасности и отдельных устройств, так и перспективные решения, предусматривающие дальнейшее развитие инфраструктуры ж.д. транспорта.

Отдельно проведен комплекс работ по переводу данной аппаратуры на отечественную элементную базу, в тесном сотрудничестве с ведущими предприятиями страны РАН и ГК «РОСАТОМ».

Благодаря проведенным работам начато не только формирование и создание нового поколения устройств обеспечения безопасности и управления, но и решен вопрос об информационной безопасности на уровне программно-аппаратных средств в условиях киберугроз.

Fink Uri

Fink Electric, Ltd.

Digital solutions for transport security

The author deals with a number of systems developed and implemented to ensure the safety of passenger and freight transport. Such innovative element of the traffic safety system as the autonomous axle counter is also considered.

The train safety and communication control system (TSCCS) is considered. It provides emergency voice notification and wireless telephone communication for train crew members, video surveillance from the staff car using WiFi channels, data transmission from automated boarding control system to conductors and automatic cars registration. An axle box heating wireless control system integrated in the TSCCS allows for continuous monitoring of the axle boxes temperature dynamics and alerts the train crew about the critical temperature increase.

Freight train safety improving system ensures continuous monitoring of the axle boxes, wheel pairs, truck side frames and transported loads condition, performs a dynamic analysis of the most important joints of the truck and analysis of the train-track interaction. It also generates alarm signals.

Autonomous axle counter is an innovative element of the future train separation system. It is used for track vacancy control and for warning track maintenance crew members about the approaching train. The axle counter can also provide diagnostics of wheel pairs and car trucks faults.

Финк Юрий Михайлович

ООО «Финк Электрик»

Цифровые решения в области обеспечения безопасности на железнодорожном транспорте

В докладе рассмотрен целый ряд систем, разрабатываемых и внедряемых в целях обеспечения безопасности пассажирских и грузовых перевозок. Также рассматривается такой инновационный элемент системы обеспечения безопасности движения, как автономный счетчик осей.

Одной из рассматриваемых систем является система контроля безопасности и связи пассажирского поезда (СКБ и СПП), которая обеспечивает речевое оповещение должностных лиц поездной бригады об аварийных ситуациях (пожар, перегрев букс, тревога), возникающих в пассажирских вагонах, беспроводную телефонную связь должностным лицам поездной бригады, видеонаблюдение из штабного вагона за ситуацией в пассажирских вагонах с использованием каналов WiFi, а также получение проводниками в линейных вагонах данных МАСКПП (автоматизированной системы контроля посадки пассажиров) из штабного вагона по внутрипоездной связи и автоматическую регистрацию вагонов в составе поезда. В СКБ и СПП интегрирована система беспроводного контроля нагрева букс (СБКНБ), которая позволяет непрерывно контролировать динамику изменения температуры буксовых узлов и своевременно предупреждать поездную бригаду о критическом увеличении температуры до её выхода за допустимые пределы.

Система повышения безопасности движения грузового поезда обеспечивает непрерывный контроль состояния буксовых узлов, колёсных пар, боковых рам тележек и перевозимых грузов, осуществляет динамический анализ состояния наиболее важных узлов тележки по различным параметрам (уровень вибрации, ударные нагрузки, температура подшипников, блокировка колёс, сход колёсной пары, а также пробег вагона и колёсных пар, излом боковой рамы и других узлов), анализ взаимодействия тележки с рельсовым путём и вырабатывает сигналы опасности.

Инновационным элементом перспективной системы интервального регулирования является автономный счётчик осей. Одной из задач применения автономного счётчика осей является контроль свободности перегона, а также отправка сигнала предупреждения работникам путевых бригад, находящихся на железнодорожных путях, о приближающемся поезде.

Кроме того, счётчик осей обеспечивает диагностику неисправностей колёсных пар и тележек вагонов и рельсового пути в зоне доступности измерений с возможностью передачи полученной информации на локомотив.

Zipp Andrey, Veselov Evgeny
LTD NPO SAUT

Prospective directions for development of control and safety systems for railway transport

NPO SAUT is the scientific production association which develops and manufactures microprocessor systems for the traction and multiple rolling stock as well as track equipment that ensures safety and reliability of railway traffic.

The author deals with the results of the joint work on the development of control and safety systems for railway transport. All systems are developed within the framework of the JSC RZD Digital Railway project concept. As an example, NPO SAUT together with partner companies has developed an automatic train operation system (ATO) for the new generation electric trains (ES2G), operated on the Moscow Railway Ring. Together with JSC NIIAS the concept of a new generation security system, designed to improve resilience and survivability, was developed. The concept provides full redundancy of inter-module communication channels, implementing of high-speed interfaces, as well as split of functions into several levels to ensure necessary safety integrity on each level.

Ципп Андрей Леонардович, Веселов Евгений Васильевич
ООО «НПО САУТ»

Перспективные направления развития систем управления и безопасности железнодорожного транспорта

Научно-производственное объединение САУТ разрабатывает и производит микропроцессорные системы для тягового, мотор-вагонного подвижного состава, а также устройства путевой инфраструктуры, обеспечивающие безопасность и надежность железнодорожных перевозок грузов и пассажиров. Все разрабатываемые системы ориентированы на выполнение концепции проекта АО «РЖД» «Цифровая железная дорога». Для грузовых электровозов 2ЭС6 ранее разработанная микропроцессорная система управления локомотивом МПСУиД оснащается дополнительной функцией измерения плотности и объёма тормозной сети поезда, позволяющей в автоматическом режиме выполнять необходимые проверки без участия машиниста. Совместно с предприятиями-партнёрами разработана система автоведения для электропоездов нового поколения ЭС2Г, эксплуатирующихся на Московском центральном кольце.

В результате применения бортовых датчиков приближения к платформе и методов передачи данных между системами, позволяющих компенсировать задержки в каналах связи на электропоезде, обеспечивается позиционирование и остановка состава на платформе с точностью 50 см. В 2017 г. при участии партнёров АО «НИИАС», НЕЙРОКОМ, ТрансИнфоПроект системы МПСУ и БЛОК-М были объединены в многофункциональную систему МПСУ-БД, что подтверждает дальнейшее направление развития к более тесной интеграции локомотивных систем управления и безопасности. В системе исключены дублирующие функции, применён единый регистратор, осуществлено резервирование каналов и способов отображения информации для машиниста. Ведутся работы по дальнейшему совершенствованию системы автоматического управления торможением. Новая система САУТ-К призвана объединить функции ранее выпущенных систем САУТ-ЦМ/485, КИО-САУТ и КИО-САУТ-2. Применение универсального шлюзового блока, включающего в себя также функции связи со сменным носителем информации, позволило отказаться от ряда периферийных узлов. Существенно расширены объёмы индикации параметров работы системы.

Совместно с АО «НИИАС» разработана и реализуется концепция системы безопасности нового поколения, направленная на повышение отказоустойчивости и живучести. Предусматривается полное резервирование межмодульных каналов связи, добавление высокоскоростных интерфейсов, а также разделение выполняемых функций по уровням для обеспечения необходимой полноты безопасности на каждом из них.

Klokov Alexander

Micromax Systems, Ltd.

Application of M-Max solutions for the relay automation systems

The author deals with M-Max solutions for the relay automation systems. «MicroMax Systems» LLC develops and manufactures various computer systems as well as computer components, communication products and specialized electronics for automation and control systems capable of operating under severe conditions. Micro-Max produces a model range of M-Max blocks supplied as part of ABTC-MSh complexes for the railway automation systems. When building systems, M-Max pays special attention to increasing the reliability of signal processing and transmission. Such systems include RTU (Remote Terminal Unit) blocks and the recently developed communication device with relay systems (BURS).

Клоков Александр Валентинович

ООО «МикроМакс Системс»

Применение систем M-Max в релейных системах автоматики

ООО «МикроМакс Системс» разрабатывает и производит различные вычислители с повышенным ресурсом и способные работать в тяжелых условиях эксплуатации, будь то низкие или высокие температуры, различные воздействия на системы в виде влаги и пыли, вибраций и ударов. Для систем железнодорожной автоматики МикроМакс выпускает модельный ряд блоков М-Max, поставляемых в составе комплексов АБТЦ-М(Ш). Это АРМ-ДСП, АРМ-ШН, АРМ-РС, CAN-регистратор. В составе устройств цифрового радиоканала используется блок УСО, а в системах безопасности поездов «Ласточка» и «Сапсан» блок ШЛЮЗ-CAN-MVB2.

В поездах «Ласточка» применяется также блок ШЛЮЗ-РК. Все загружаемое прикладное программное обеспечение разработано АО «НИИАС». Все блоки М-Max являются мало обслуживаемыми и отличаются межсервисным интервалом в 6-8 лет. Основными способами повышения надежности электронных блоков является отсутствие подвижных элементов в конструкциях и обмена воздухом с окружающей средой. В настоящее время особое внимание уделяется построению систем с требованием повышенной достоверности обработки и передачи сигнала. К таким прежде всего относятся блоки УСО и разработанный недавно Блок Увязки с Релейными Системами (БУРС). БУРС применяется для увязки электронных систем управления с релейными системами железнодорожной автоматики. Он обеспечивает вынос по оптоволоконному кабелю до 20 км и управление до 24-х спаренных электромагнитных реле типа 1Н-1350. Блок обладает расширенными функциями внутреннего контроля и диагностики.

Для повышения достоверности обработки и передачи информации блоки УСО и БУРС работают по схеме «2-из-2». Надежность работы повышена применением встроенных источников бесперебойного питания на суперконденсаторах в каждой секции блока. В настоящее время в рамках программы по расширению локализации осуществляется перевод данного оборудования (одной секции) на процессорные модули САЛЮТ.

Geyko Natalia
Vimpelcom

Critical communications in transport

The author presents a set of innovative solutions in the field of transport security that include critical communications networks, intelligent video stream processing systems, modern diagnostic methods and interactive communication channel monitoring systems. The report addresses key requirements for public safety networks and professional mobile radio based on LTE, as well as its main advantages over TETRA and DMR standards.

A modern approach to the communication channels and switching equipment maintenance is given. It allows for reduction of the network troubleshooting time enhancing the uninterrupted connectivity of security systems in transport. The trend towards the transition from traditional video monitoring to an intelligent hardware-software video analytics system is described.

Гейко Наталья Юрьевна
ПАО «Вымпел-Коммуникации»

Критически важные коммуникации на транспорте

В рамках доклада будет предложен комплекс инновационных решений в области обеспечения безопасности на транспорте путем построения сетей связи для критически важных коммуникаций, интеллектуальных систем обработки видеопотока, а также современные методы диагностики и интерактивные системы мониторинга каналов связи. Критически важные коммуникации – это связь, от надежности которой зависят жизни людей, например, в зоне чрезвычайных ситуаций и на объектах, аварии на которых могут принести разрушительные последствия. Обеспечение безопасности на транспорте, последовательное снижение показателей аварийности, производственного травматизма, и, прежде всего, предупреждение и/или минимизация последствий этих аварий, как транснациональная проблема современности актуальна для всего мирового социума. В докладе затрагиваются ключевые требования для сетей общественной безопасности и профессиональной мобильной радиосвязи на базе LTE, а также основные преимущества перед стандартными ПМР – TETRA и DMR.

Озвучен современный подход в обслуживании каналов связи и коммутационного оборудования для сокращения времени реакции на поиск и устранение неисправностей в сети, что непосредственно влияет на обеспечение бесперебойной связанности систем безопасности на транспорте. Определены тенденции к переходу от традиционного видеонаблюдения к построению интеллектуального программно-аппаратного комплекса видео аналитики, как необходимого элемента обеспечения безопасности работников, объектов и материальных ресурсов компании.

Возможностями использования интеллектуального видеонаблюдения являются обеспечение производственной безопасности и охраны труда, контроль соблюдения норм технологических процессов и повышение их эффективности, контроль доступа и антитеррористическая защита объектов, контроль хода строительства и, как следствие, рассмотрение и анализ причин аварий и несчастных случаев, в том числе, со смертельным исходом, произошедших на объектах инфраструктуры, что помогает в подготовке предложений по снижению уровня аварийности и травматизма, качеству материалов специального расследования.

Zoran Avramovic
The University of Belgrade

Damir Zaborski
Panevropski Univerzitet APEIRON

Architecture and Organization of Railways Information and Communication System

Considering that the modernization of the railway represents an uninterrupted process, it is necessary to take care of constant technical and technological development and application of the latest achievements in the field of information and communication systems (ICS). The railway ICS, among other things, provides infrastructure for the automatic control systems, traffic management and control, monitoring and navigation systems, data processing devices, and also provides support to other subsystems designed for safe and consistent use of the line, as well as efficient management of the modern rail transportation system.

In accordance with the previous exposure and decomposition of the functional railways ICS subsystems, we will implement different functional subsystem modules at different physical locations (stations and trackside), and then we will generate a comprehensive physical architecture of the information communication system. Based on the proposed model, it is possible to sort all the official points on the railways network at the SR and anticipate the necessary equipment that will enable the required services for regular and safe operation of the railway transport and placing the complete rail service to a higher level.

The paper defines the place of the information and communication system in the entire railway technology and transport system, as well as the need of connection with other railway technological systems and external communication and other systems of interest for the functioning of the railway. On the basis of traffic and technological requirements and characteristics ICS of the official positions on the lines, the paper gives the proposal of ICS architecture with all the necessary subsystems, and depending on the technological and hierarchical level of the railway network in the SR. The levels of nodes in the railways ICS and their physical and logical organization were also identified, as well as the equipment and services characteristic for the individual nodes. It is proposed an organizational model for the information and communication system of the railways, which would be applicable at the railways network of the SR and other modern railway administrations, especially in our region.

Зоран Аврамович
Белградский университет

Дамир Заборски
Паневропейский университет APEIRON

Архитектура и строение железнодорожных информационно-коммуникационных систем

Поскольку развитие железнодорожного транспорта представляет собой сложный и непрерывный процесс и играет важную роль в функционировании и развитии государства, необходимо позаботиться о разработке и внедрении современных информационно-коммуникационных систем (ИКС). Такие системы обеспечивают связь железнодорожной инфраструктуры с системами автоматического управления движением, системами мониторинга и навигации, устройствами обработки данных и т.д. В докладе определено основное назначение ИКС для вей железнодорожной системы, а также представлена архитектура ИКС со всеми необходимыми подсистемами. Представлена организационная модель информационно-коммуникационной системы, которая будет применяться на железнодорожной сети Сербских железных дорог и других железнодорожных администраций.

David Šmid

Iskratel

IMS based migration aspects towards FRMCS

GSM-R is unquestionably a success story, but it is already yesterday's technology. FRMCS (Future Railway Mobile Communication System) aims, as the successor of GSM-R, to cover the rail telecommunication requirements and will provide the transport facilities to increase the automation level for rail operations. Consequently FRMCS has to be flexible to support various kinds of present and future rail applications encompassing real time and non-real time characteristics.

Scalable, secure, IP-based transmission networks are required to unlock many of the benefits of the digital railway, and the next-generation system will be vital to provide interoperability between different railway communication systems. 3GPP core network technology provides a framework with enabling mechanisms and services to support railway requirements (Quality of Service, Reliability and robustness, Virtualization, Interworking, Security …).

Key challenges, drivers and how a possible evolution concept based on IMS or some other SIP core network could look like will be presented. The benefits of such approach and how the new architecture will help in introducing new applications will be addressed.

Давид Шмид

ИСКРАТЕЛ

Основные аспекты перехода от системы IMS к FRMCS

Несомненно, беспроводная коммуникационная платформа повышенной надежности для железных дорог GSM-R имеет успешную историю, однако в настоящее время является устаревшей технологией. Новое поколение железнодорожной системы мобильной связи (FRMCS) приходит на смену GSM-R. Главными задачами системы FRMCS является удовлетворение требований железнодорожной связи и повышение уровня автоматизации железнодорожных перевозок. Для решения данных задач необходимо обеспечить гибкость и совместимость системы FRMCS с другими системами. Технология 3GPP обеспечивает основу для создания механизмов и услуг для поддержки железнодорожных требований (качество обслуживания, надежность и безопасность и др.). В своей работе автор рассматривает основные проблемы, возможности и преимущества перехода к системе FRMCS.

Tamarkin Vladislav
JSC NIIAS

Filippov Sergey
Group of companies «Iskra»

Satellite technologies for railway transport

Satellite technologies have become widespread in various transportation domains including railways. The report examines the possibility of the application of such mobile satellite systems as «Gonets», «Iridium» and «Thuraya» in railway transport in combination with fixed satellite communication systems operating at Ku and Ka bands in accordance with VSAT technology, the calculation of satellite channels availability at the Moscow–Valdimir section and the Northern Latitudinal Railway is given, the results of the trial operation of the mobile satellite network systems «Gonets» and «Iridium» at the Bologoe–Ostashkov sections are presented.

Тамаркин Владислав Михайлович
АО «НИИАС»

Филиппов Сергей Вячеславович
Группа компаний «Искра»

Применение спутниковых систем связи на железнодорожном транспорте

Целесообразность применения спутниковых систем связи (ССС) определяется рядом причин. В первую очередь это касается малодеятельных линий, общая протяженность которых составляет порядка 8000 км. Эксплуатация традиционных систем связи на этих линиях в связи с малой интенсивностью движения и большими расстояниями между станциями экономически нецелесообразна.

Другой сферой применения ССС на железнодорожном транспорте может служить Северный широтный ход и ряд участков БАМа, где ССС могут выступать в качестве дублирующей системы. Еще один пример возможного применения ССС – участок ВСМ Москва–Владимир в условиях дефицита частотного ресурса.

В докладе рассмотрена возможность использования на железнодорожном транспорте систем подвижной спутниковой сети «Гонец», «Иридиум», «Турайя» в сочетании с системами фиксированной спутниковой связи Ka и Ku диапазонов по технологии VSAT, приведена блок-схема комбинированной системы связи, дан расчет доступности спутниковых каналов на участке Москва–Владимир и на Северном широтном ходе, приведены результаты опытной эксплуатации систем подвижной спутниковой сети «Гонец» и «Иридиум» на участке Бологое–Осташков.

Chmelevskaya Natalia

FGUP «ZashchitaInfoTrans»

Overview of cybersecurity level of modern train control systems on the high-speed lines

One of the key research issues in further strengthening the role of railways in the transportation system is to achieve the highest possible level of cyber security against significant threats to the signalling and telecom systems. Cybersecurity is crucial for the lines operated at speeds of more than 200 km/h, because traffic control process is based primarily on the use of automation systems.

The author deals with an analytical overview of the research results in assessment of train control systems for cybersecurity conducted by various expert organizations and companies. A description of the main vectors of possible cyber attacks on train control systems, including such components as signalling systems and onboard train/locomotive control systems are presented in the report. The assessment of the feasibility of conducting such attacks and their possible consequences, as well as the requirements and priority measures to ensure cybersecurity of control systems, taking into account the specific of high-speed lines, are given.

Хмелевская Наталья

ФГУП «ЗащитаИнфоТранс»

Обзор уровня киберзащищенности современных систем управления движением поездов на высокоскоростных магистралях

Внедрение современных микропроцессорных систем управления движением поездов и, в первую очередь, технических средств железнодорожной автоматики и телемеханики способствует повышению интенсивности и скорости движения поездов, оптимизации процесса организации перевозок пассажиров и грузов. При этом на первый план выходят вопросы кибербезопасности таких устройств. Применительно к организации высокоскоростного движения эти вопросы имеют решающее значение, т.к. на скоростях свыше 200 км/ч. процесс управления движением основан преимущественно на использовании автоматики. Базовые требования по информационной безопасности систем управления движением поездов, изложенные в технических регламентах Таможенного Союза достаточно поверхностны и сводятся к обеспечению «защищенности от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных изменений информации».

Таким образом, речь идет, в основном, о «случайных воздействиях», не учитывающих целенаправленную атаку. Тем не менее в этих документах упоминается «несанкционированный доступ», что косвенно подтверждает необходимость учета антропогенного фактора при анализе защищенности. Проводимые экспертами в области кибербезопасности исследования защищенности ряда широко распространенных систем управления движением поездов выявили дефекты и уязвимости, используя которые злоумышленники не только могут снизить ключевые показатели надежности и обойти механизмы функциональной безопасности, но и реализовать атаки, напрямую влияющие на безопасность движения поездов. Примечательно, что с точки зрения информационной и функциональной безопасности эти системы соответствуют всем выдвигаемым требованиям, имеют все необходимые международные, отраслевые и государственные сертификаты.

В докладе будет приведен аналитический обзор результатов исследований кибербезопасности систем управления движением поездов, проводимых различными экспертными организациями и представленных в открытых источниках. Также будет представлено составленное по результатам такого анализа описание основных векторов возможных кибератак на системы управления движением поездов, включая такие их компоненты как устройства автоматики и телемеханики и бортовые системы управления поездом/локомотивом. Будет дана оценка возможности реализации таких атак и их возможных последствий, а также описаны направления и первоочередные меры по обеспечению киберзащищенности систем управления движением поездов с учетом особенностей организации высокоскоростного движения.

Perov Alexey

Bombardier Transportation (Signal) Ltd.

Cyber security solution for train control systems Experience of Bombardier Transportation (Signal)

Modern trends of developing computer-based signalling systems imply wide use of information technologies. First of all, this is true for operating systems and data communications protocols.

Computer-based interlocking systems can be highly distributed to control geographically dispersed assets. Being scattered over miles of rail infrastructure makes them vulnerable to cyber security threats.

Ensuring information security of signalling systems means ensuring protection from unauthorized access to a local network due to a multi-layered security approach.

To mitigate the risks posed by cyber-attacks to rail networks, Bombardier Transportation in cooperation with Research Institute NIIAS and Positive Technologies has developed a complex cyber security solution for train control systems. The solution addresses threats to the security of computer-based rail control systems, including interaction with external systems and unauthorised access, and consists of

- CyberSafemon, a cyber secure tool with «data diode» (one-way communication) principle;
- Industrial Security Incident Manager (ISIM).

CyberSafemon's software has been developed in Russia with exclusive rights for it belonging to Bombardier Transportation (Signal) Ltd. It also has been certified by Russian authority FSTEC as an information security tool.

Main customer benefits:

1. No need to adapt for a specific station;
2. Linux-based software, standard and unified hardware;
3. Fully made-in-Russia product.

Delivering solutions that protect rail networks from the evolving threats posed by cyber-attack is of paramount importance. We are proud to have made a significant contribution to ensuring the continued safety of the rail transportation network in Russia.

Перов Алексей Алексеевич

ООО «Бомбардье Транспортейшн (Сигнал)»

Киберзащищенность МПСУ ЖАТ. Опыт компании «Бомбардье Транспортейшн (Сигнал)»

Функциональная безопасность МПСУ ЖАТ оказывается зависимой от угроз информационной безопасности, что в совокупности создает новый аспект жизненного цикла систем – кибербезопасность (киберзащищенность).

Обеспечение информационной безопасности МПСУ ЖАТ заключается в обеспечении защиты от несанкционированного доступа к внутренней локальной сети за счет построения многоуровневого контура защиты.

С этой целью ООО «Бомбардье Транспортейшн (Сигнал)» совместно с АО «НИИАС» и ЗАО «Позитивные технологии» разработало комплексную систему повышения киберзащищенности, которая состоит из:

- устройства кибербезопасного мониторинга (программно-аппаратный комплекс CyberSafemon);
- сенсора анализа сетевого траффика системы (САСТС).

Программно-аппаратный комплекс «CyberSafemon» представляет собой односторонний шлюз передачи диагностической информации от устройств МПСУ в центр удаленного мониторинга. Прикладное программное обеспечение комплекса разработано в России. Исключительное право на все результаты интеллектуальной деятельности, полученные при создании CyberSafemon, принадлежат ООО «Бомбардье Транспортейшн (Сигнал)».

Комплекс сертифицирован по требованиям безопасности информации во ФСТЭК РФ.

В случае возникновения инцидента, оперативный персонал на объекте имеет возможность скопировать локально данные об инциденте на внешний носитель и передать их в центр расследования. При необходимости, информация об инцидентах может в автоматическом режиме передаваться в общий центр расследования.

В качестве основных преимуществ решения можно отметить следующие:

1. CyberSafemon оптимизирован для передачи данных телесигнализации и системных журналов МПСУ ЖАТ одновременно и не требует адаптации под каждую конкретную станцию.
2. Применяемое оборудование и базовое программное обеспечение стандартизировано и унифицировано. При этом, в качестве системного программного обеспечения для всех компонентов системы используются операционные системы с открытым исходным кодом семейства Linux.
3. Система является полностью российской разработкой.

В заключение хотелось бы отметить, что ООО «Бомбардье Транспортейшн (Сигнал)» в очередной раз подтверждает свои лидирующие позиции в отрасли и совместно с ОАО «РЖД» первым решает новые научно-технические задачи в области кибербезопасности.

Gross Vadim

Locotech-Signal Ltd.

Safety of critical information infrastructure

On January 1st, 2018, the Federal Law on «Security of the Critical Information Infrastructure of the Russian Federation» No. 187-FZ was put into force and set requirements for information security of the critical information infrastructure facilities.

Taking into account stated requirements, as well as established principles of functional safety mentioned in the standards of GOST R IEC 61508 series, it is proposed to consider the process of ensuring information and functional safety for rail traffic management systems within the common system life cycle.

In this case, it becomes necessary to reconsider the tasks and roles of the process participants. Thus, at least the following key components can be highlighted at a number of stages in the system life cycle:

- At the design stage it is necessary to take into account the information security requirements in accordance with the class of importance for the critical information infrastructure facilities;
- At the manufacturing stage developers must integrate information security tools into the control systems. In such case, an additional role of an integrator may appear, having the necessary competencies in the field of information protection, confirmed by the licenses of FSTEC and Russian Federal Security Service;
- At the validation stage for necessary to update the procedure for system acceptance for operation with system certification for information security requirements, which consequently leads to consolidation of competences in the field of functional and information security for the side which performs acceptance.
- During the operation and maintenance stage, there is a need to establish information security monitoring center integrated with GOS SOPKA Russian FSB (State system of detection, prevention and elimination of consequences of computer attacks on information resources of the Russian Federation) as well as to perform system scheduled audits in accordance with the assigned class of importance.

Гросс Вадим Александрович

ООО «Локотех-Сигнал»

Обеспечение безопасности критической информационной инфраструктуры

С 1 января 2018 года вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ, устанавливающий требования по информационной безопасности объектов КИИ.

В соответствии с требованиями данного ФЗ разработаны нормативно-правовые документы, конкретизирующие данные требования:

- постановление Правительства РФ от 8.02.2018 № 127;
- приказы ФСТЭК России: № 227 от 6.12.2017, № 229 от 11.12.2017, № 235 от 21.12.2017, проект приказа № 236 от 22.12.2017, № 239 от 25.12.2017.

Учитывая указанные требования, а также сложившиеся принципы обеспечения функциональной безопасности, заложенные в стандартах серии ГОСТ Р МЭК 61508, предлагается рассмотреть процесс обеспечения информационной и функциональной безопасности систем управления перевозочным процессом в рамках единого жизненного цикла систем.

В данном случае возникает необходимость пересмотреть задачи и роли самих участников процесса. Таким образом, на ряде этапов жизненного цикла системы можно выделить как минимум следующие ключевые составляющие:

- на этапе проектирования необходимо дополнительно учитывать требования информационной безопасности в соответствии с категорией значимости объекта КИИ;
- на этапе изготовления разработчикам требуется интегрировать средства защиты информации в системы управления. При этом возможно появление дополнительной роли интегратора, обладающего необходимыми компетенциями в области защиты информации, подтвержденными лицензиями ФСТЭК и ФСБ России. Кроме того, для типовых компонентов системы целесообразно проводить сертификацию. В связи с этим возникает необходимость в объединении компетенций в области функциональной и информационной безопасности в одном сертифицирующем органе для обеспечения полноты оценки с учетом всего комплекса внешних дестабилизирующих факторов среды, а также оптимизации временных и материальных ресурсов;
- на этапе валидации системы необходимо дополнить процедуру приемки системы в эксплуатацию аттестацией по требованиям безопасности информации, что в свою очередь приводит к объединению компетенций в области функциональной и информационной безопасности принимающей стороны;
- на этапе эксплуатации и технического обслуживания возникает необходимость создания центра мониторинга информационной безопасности, интегрированного с ГОС СОПКА ФСБ России, а также проведение плановых аудитов системы в соответствии с присвоенной категорией значимости.