Cybersecurity of Railway Command and Control Systems

Alexey Ozerov
JSC NIIAS

Contribution to the state of the art
DOI: **10.7251/JIT19020530** UDC: **725.31:[681.513.6:007.5**

Abstract: With the large-scale migration to computer-based and network technology, the threat of unauthorized remote access to railway command and control systems does not appear to be something extraordinary.But external effects shall be considered alongside with internal factorsof signalling software and hardware such errors and undocumented features. Risk mitigation in terms of cybersecurity of signalling installations can onlybe achieved as a combination of means designed within some holistic approach integrating both safety and IT security aspects.

Keywords: Cybersecurity, functional safety, signalling, undocumented features, wrong-side failure.

Introduction

Railways are generally considered as critical infrastructure. This means that failures and incidents can ultimately cause national-level disruptions.They could also have a dramatic effect on the safety of the public, business performance and reputation.

Year to year, the number, sophistication and diversity of registered cyberattacks are steadily growing. Attackers use a variety of tactics; they have different motivations – from financial benefits to revenge.

In 2016, the UK's railway system was affected by at least four major cyber attacks, while in 2017 the WannaCry virus caused the failure of the PIS/PAS system of a German railway carrier and affected other railways.In 2018aDDoS attack at Danske Statsbaner, the biggest Danish train operator, halted trains operations and blocked passenger services.

What is more important is that cyber attacks can also cause wrong-side failures within the command and control system. And that could mean severe harm to assets, environment and people. Nowadays "malicious cyber activity" is becoming more of a safety concern for digitalized railway command and control systems rather than just a security concern.

The range of potential consequences of cyber security incidents related to railway command and control is wide and includes:

- Loss of system availability
- Degradation of system performance
- Manipulation or loss of data
- Loss of production control
- Environmental disaster
- Risk of death and grave injury
- Damage to company image
- Financial loss [1].

Cybersecurity threats and railway command and control

Until recently, it was generally believed that railway signalling systems,being isolated from external effects, are immune to any cybersecurity threats and attacks. That is no longer the case. Now, the focus is on providing resilience, rather than preserving immunity.

The potential scenarios of cyber attacks against safety critical systems are many. They include unauthorized access to equipment, tampering with hard-

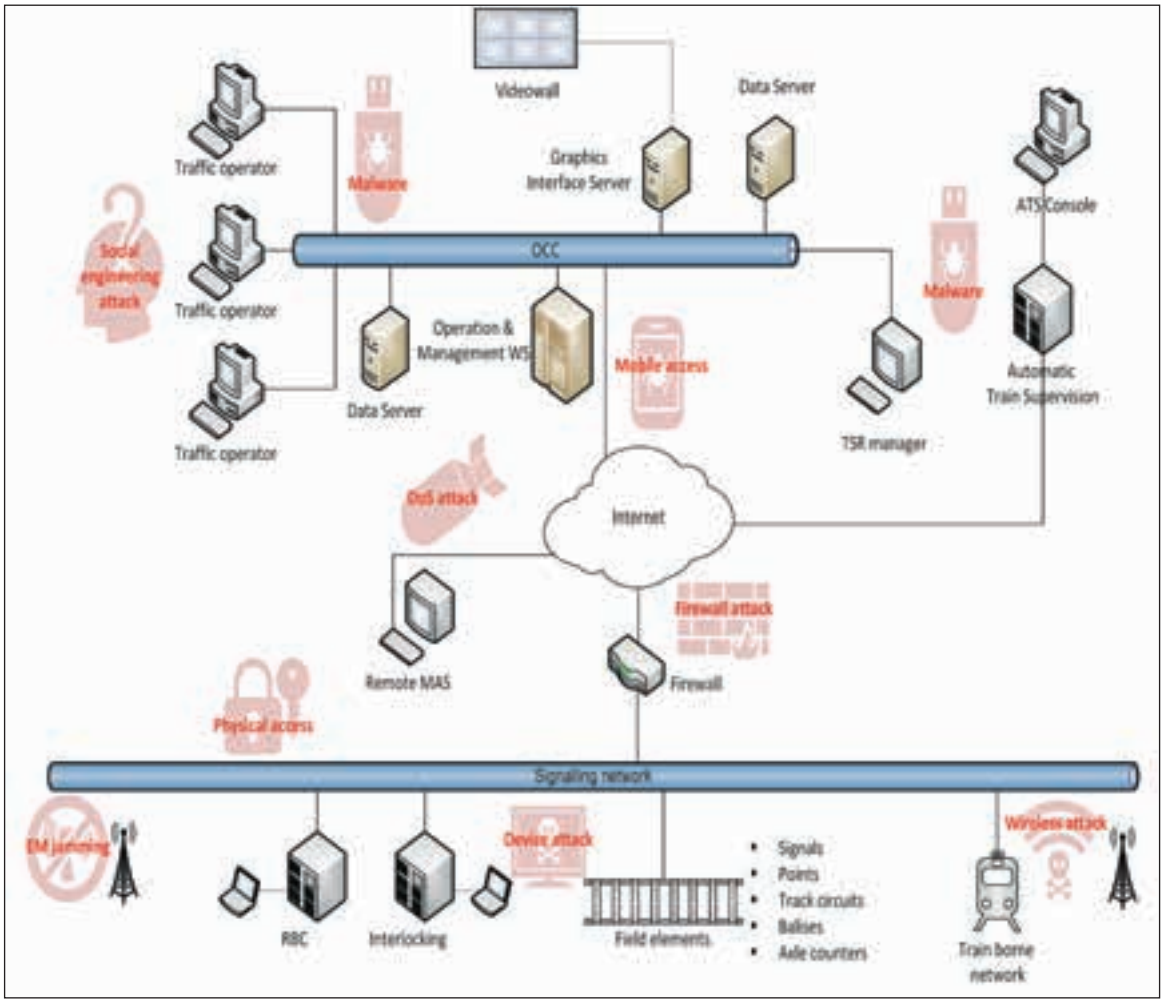


Figure 1. *Railway command and control levels and cyber threats*

ware and software and more. But unlike non-critical IT systems, their aim does not consist in the breach of confidentiality.The motivation can include compromising the system safety and manipulating critical commands and controls in order to cause train collisions, unexpected train stops, power cuts etc. That, for instance, can be achieved by clearing the signal that should not be cleared, releasing the track section that should be blocked, etc.

Even a simple USB flash drive can be used to compromise the functional safety of a critical signalling installation. Social engineering (man in the middle) is a very important factor here. A lot depends on the company's cybersecurity policy and personnel training, monitoring of staff behavior and motivation assessment.

The vulnerability of signalling installations has been shown by various projects and by in-house hackers. The vulnerability of the ERTMS system was demonstrated in the SECRET (Security of Railways against Electromagnetic Attacks) project. The project focused on assessing the risks and consequences of electromagnetic attacks on the rail infrastructure and developing protection solutions. Such critical data channels as GSM-R and balises were identified as the most probable "targets". The possibility of effective suppression of these communication channels with the low-priced «jammers» was experimentally confirmed [2].

The railway system includes a number of layers and interfaces to external systems. Therefore, we must take into account and map all possible threats, techniques and devices that could target each zone and conduit of signalling installations.

From the perspective of safety-critical signalling installations' operators, it is not the issue of confidentiality, integrity and availability of information in general, rather than the issue how to be protected

Vulnerabilities	Source of threat	Examples of threats	
Company data transmission network level			
Software vulnerabilities	Outside intruder	• Execution of a malicious code on a gateway computer • Denial of service	• Remote application launch • «Password attack»
Vulnerabilities of network protocols and communication channels	Outside intruder	• Network scanning • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Information support level			
Software vulnerabilities	Outside intruder	• Execution of a malicious code at workplaces • Denial of service	• Remote application launch • «Password attack»
Vulnerabilities of network protocols and communication channels	Outside intruder	• Network scanning • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Information logic processing level			
Software vulnerabilities	Insider	• Execution of a malicious code on an industrial control computer • Denial of service	• Wrong route setting • Network scanning • Substitution of the entrusted object
Vulnerabilities of network protocols and communication channels	Insider	• Network scanning • Wrong signal setting • Substitution of the entrusted object	• Network traffic analysis • Denial of service
Input/output interface and actuators levels			
Vulnerabilities of network protocols and communication channels	Outside intruder or insider	• Substitution of the entrusted object • Decoy object embedding • Network scanning	• Network traffic analysis • Denial of service

against malicious code in the software and undocumented features of the signalling system, to prevent open access to safety-critical installations, to identify and eradicate vulnerabilities etc.

Below are some examples of software and network vulnerabilities and threats [3].

With all these threats in mind, we need to face the current and emerging challenges of cybersecurity of railway systems and to understand the risks and their possible impact. It means that we have to carefully study all the historical cases of cybersecurity incidents, their consequences and who was be-

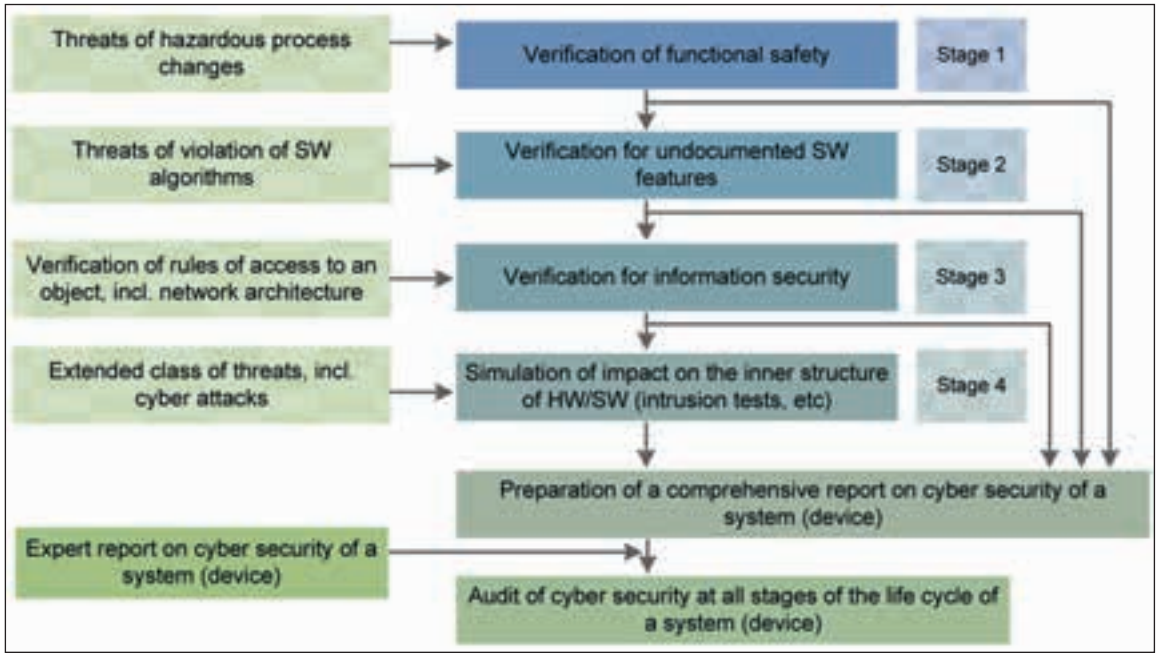


Figure 2. *Railway system assessment and evaluation cycle*

hind and how they deployed them. That must be followed by a thorough risk assessment and an inventory of vulnerabilities and threats, and those have to be updated at every stage of a system's life cycle starting from the design stage. So, it's like a V model with review and revision at each stage.

Assessment and audit of a railway system's software includes detection and identification of undocumented features which are not intended for use by end users, but left available for use by the vendor for software support and development.

The problem, though, is that if hackers discover such undocumented features, they can also remotely access the device and possibly take control of the entire system. This is why all types of undocumented features present potential security and cyber security risks.

- Unintended undocumented features could be the result of developer errors,
- Intentional undocumented features could be deliberately introduced in the software during its development. Intentional undocumented features include design, algorithmic and malicious logics.

SECURITY AND SAFETY OF RAILWAY CRITICAL SYSTEMS

In railway control systems that make use of today's networking technologies, cyber security is the continuation of technical (functional) safety and must be taken into consideration in the system lifecycle the same way as the technical safety. As one of the fundamental principles of the dependability theory postulates, there is no absolute safety. The only option isto take measures to minimize the possible risk, a procedure that leaves the residual risk. And as we know, risk is a combination of the rate (probability) of an event and the gravity of its consequences.

For a railway operator, the basic task consists in defining the justified acceptable level of residual risk subject to the available funds and other means of reducing the risk at the company's disposal. A comprehensive approach to safety management based on the risk assessment allows examining the aspects of technical safety and cyber security as a whole. A widely used tool is the risk matrix that allows classifying the existing risks based on their probability and possible damage (see the Figure below). The risks classified as intolerable must be eliminated at the design stage. For tolerable risks, damage reduction measures are to be developed [4].

System safety and system security are closely related to each other in terms of the availability of authorized functions. The safety and security of a system in general mean that a system does what it is supposed to do and does not do what it is not supposed to do.

However, while the tolerable hazard rate(THR) of functional safety is in fact a mathematical probability, the security level cannot be based on the prob-

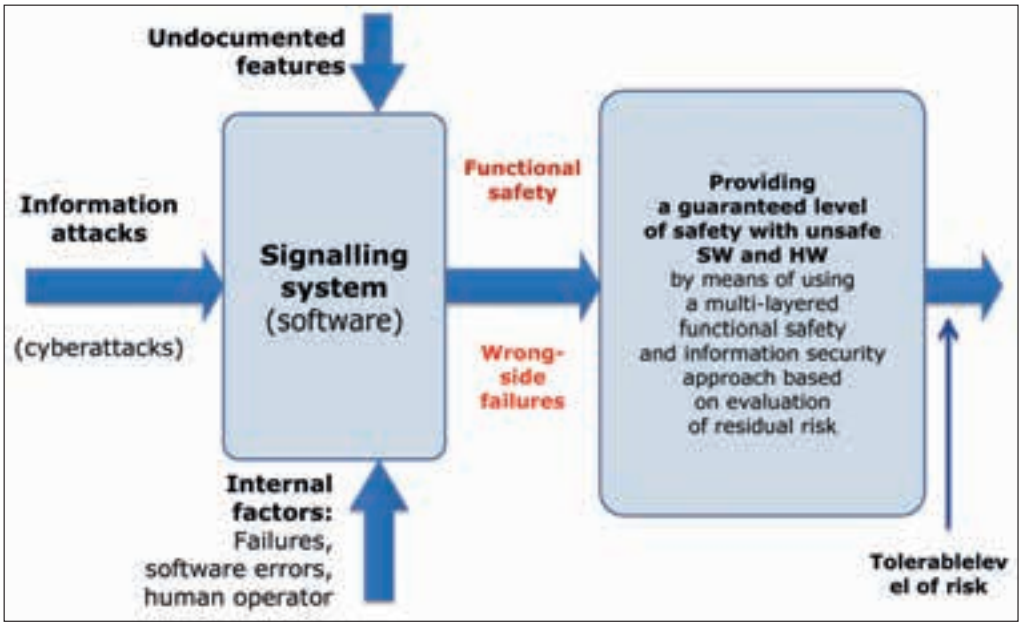
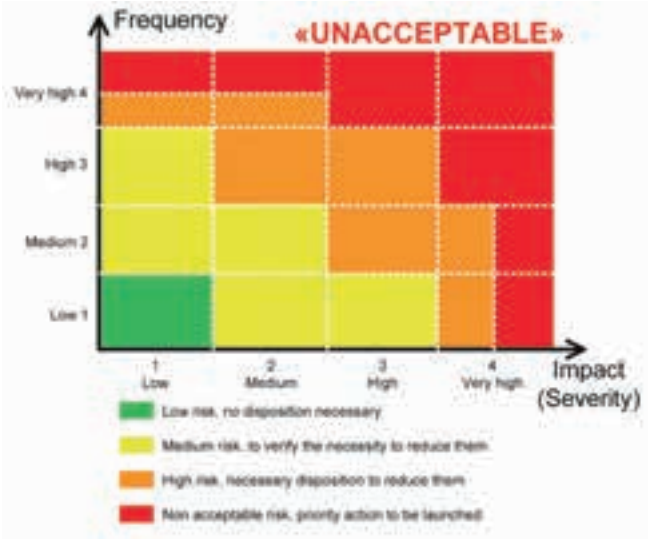


Figure 3. *Software assesment and evaluation*



ability principle since there is an intentional action by an attacker or a group of attackers.

There are still other conflicts between safety and security requirements and approaches. For example, safety requirements may overrule security requirements: security requires complex and unique passwords to login, safety requires short term login to avoid critical loss of time in stressful situation.

The great number of international conferences dedicated to the cyber security of railway systems held over the past few years demonstrates the growing awareness of the existing cyber threats. Railway companies have accumulated some experience in correlating cyber threats with types of technical failures, conducting penetration tests and identifying the vulnerabilities of existing systems. However, these activities are performed in a situation when there is no common international railway cyber security standard and no standardized procedures and methodology.

Cybersecurity as a multi-layered approach

Various research projects aim to cover the existing lack of a common safety/security standard.

For example, the European project CYRail (Cybersecurity in the railway sector) defined a number of recommendations for the development of a structured cybersecurity strategy for the railway industry with some emphasis on the identification of most critical railway services, zones and conduits, and definition of detection and mitigation strategies. As a basis the project uses a series of IEC 62443 standards intended for industrial automated control systems. The standards are considered by many experts as a guideline for building a cyber security management system. The project also uses these standards to develop requirements for a secure-by-design railway system [5].

In IEC 62443 security levels (SLs) are parts of the qualitative approach to addressing security for a zone.

SL0 – no special protection requirements

SL1 – protection against casual or coincidental violation

SL2 – protection against intentional violation using simple means with low resources, generic skill and motivation

SL3 – protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation

SL4 – protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

Research and practice produces a long list of recommended measures to be used as part of a cybersecurity strategy. Among other things, they include regular updating of critical signalling systems software, as well as application of trusted software and hardware.

Naturally, a secure-by-design system could be one of the options. In particular, a cybersecurity system should have a number of independent inbuilt security mechanisms to ensure sufficient protection in case of failure or compromise of any of them.Apart from the inbuilt security mechanisms, of utmost importance is the availability of tools for early attack detection, suspicious activity monitoring within hosts and networks. Though such features can only be regarded as complimentary to the inbuilt mechanisms and security procedures.

The UIC ARGUS (Security & Safety Analysis for Electric and Computerized Signalling Systems) project addressed the safety and security issues of computerized railway signaling systems. The project aimed at identifying vulnerabilities of signaling systems from the perspective of cyber threats and developing counteraction methods. The project also considered human factor management during the life cycle of the system.

The results of UIC ARGUS project as well as the activities of the UIC Cybersecurity Platform laid the

foundation for the development of a comprehensive standardized approach to the issue of safety and security, like UIC Guidelines for Cyber-Security in Railway issued in 2018.

The Guidelines have some particular focus on railway signalling and telecommunication and describe how to evaluate the security needs through ISO 27001 and using best practices applied in others industries, with company's Information Security Management System taken into account. In some way the Guidelines provide recommendations about how to develop a Security Management System for the railway cyber security that should present "a systematic approach aiming at establishing, operating, monitoring, auditing, updating and improving the railway cyber security in order to achieve the organization's objectives". It shall be based on risk management and on the implementation of solutions designed to protect the railway assets.

As to the UIC Guidelines for Cyber-Security in Railway, a multi-layered approach should be used meaning that "for every threat, several protection barriers should exist. These should be established in such a way that, to overcome them, a potential intruder would need professional skills in several unrelated areas".

According to the UIC philosophy, evaluating SL in close relation to SIL as part of the comprehensive, holistic approach to safety-security of signalling installations, infrastructure manager (IM) should apply some well-structured strategy incorporating the following fundamental components:

- Conscious and well-grounded selection of a governing principle (modus operandi) ofthe company in terms of acceptable risk level
- Identification of threats and their consequences (threat scenarios)
- Treatment of threats and their consequences at the system level
- Formalized safety and security requirements (with identification of 4 SIL/SL levels) imposed on suppliers
- Well-substantiated choice of system design and mitigation measures.

Cyber security is intertwined with all the business issues from service availability to safety. Nowadays, all systems rely on their computer and communications systems for all operational purposes including availability and safety. Moreover, they also rely on the integrity of the data itself.

So, cyber security issues should be treated as integral part of the IM's asset management system. Cyber security must be considered in the complete scope of railway exploitation and operations (network security, deployment security, signalling security) and atall stages of development (design, architecture, etc.), assessment and audit. Existing international standards traditionally treat safety and security issues from the point of requirements for railway systems suppliers. However, it is usually infrastructure managing companies who are ultimately in charge of security of railway transportation and the lives of passengers, while outside threats are rapidly growing. IMshave two options – either to just rely on suppliers, or to incorporate in their asset management system some measures and methods how to protect their safety-critical installations against cyber threats using a cycle of assessment and evaluation iterations based on a railway-specific methodology.

Conclusion

Currently there is no common international standard for safety and security. Railway operators have to take care of security of their signalling installations on their own. They develop management systems to identify and eliminate existing vulnerabilities, establish cybersecurity teams and units and elaborate internal regulatory provisions.

In a number of countries, national railway authorities and companies have been gaining experience and best practice in terms of security threat mapping and specifying security requirements as part of tendering procedures. Though one problem is still there – a cybersecurity expert in the railway signalling domain isnot an easy target for a market headhunter.The industry definitely needs a robust cybersecurity strategy that would include training of a new kind of experts equally well-versed in both signalling systems engineering and information technology.

References

[1] UIC Guidelines for Cyber-Security in Railway.June 2018, ISBN: 978-2-7461-2732-6.
[2] http://www.secret-project.eu/ (10 September 2019)
[3] Methods of Assessment of Signalling Systems for Cybersecurity. International Union of Railways (UIC). May 2019, ISBN: 978-2-7461-2819-4.
[4] http://www.secret-project.eu/IMG/pdf/20150128-02-uic-argus.pdf (10 September 2019)
[5] CYRail Recommendations on cybersecurity of rail signalling and telecommunications systems. UIC-ETF, September 2018, ISBN: 978-2-7461-2747-0.

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

Alexey Ozerov is the Head of International Department of JSC NIIAS, Research & design for Information Technology, Signalling and Telecommunications on Railway Transport, subsidiary of Russian Railways. Hehas been working with JSC NIIAS for 14 years in various positions related to research, signalling business unit and international cooperation. He is Deputy Chairman of the Committee for Development of Electrotechnical and Intellectual ATP/ATC Systems of the Russian Association of Railway Manufacturers, JSC NIIAS representative in UIC, member of UIC Rail System and Cybersecurity Platforms, expert of IEC/TC 9.

For citation

Alexey Ozerov, Cybersecurity of Railway Command and Control Systems, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:53-59, (UDC: 725.31:[681.513.6:007.5), (DOI: 10.7251/JIT19020530), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004