PROBLEMY KOLEJNICTWA
RAILWAY REPORT Issue 189 (December 2020)
DOI: 10.36137/1896E
ISSN 0552-2145 (print) ISSN 2544-9451 (on-line)

Cybersecurity of Railway Network Management and Partitioning

Jan PROCHÁZKA[1], Petr NOVOBILSKY[2], Dana PROCHÁZKOVA[3]

Summary
The railway transport infrastructure ensures the transfer of large numbers of people and cargo every day. The importance of the railway in terms of ensuring the serviceability of the territory makes it a critical infrastructure. We can observe the development of the use of IT technologies on railway, as in all areas of the human system. The management of the railway as a physical system needs to be superseded by management of the railway as a cyber-physical system. The railway infrastructure has a large area of attack in both, physical space and cyber space.
Multiple Independent Levels of Security (MILS) can meet the high system security requirements. The MILS is a high-assurance security architecture based on the concepts of separation and controlled information flow. The article discusses the possibilities of using the MILS platform in the data communication system and the control system of the railway.

Keywords: Cyber Physical Systems, Critical Infrastructures, Multiple Independent Levels of Security

1. Introduction

The critical infrastructure protection has become an essential part of the advanced human systems security strategies. Critical infrastructures exist often at several spaces:

- Physical space – a extensive network of physical elements (either point or line types);
- Process space – a management system, human factor, technical standards, relevant legislation and management strategy as well [3, 9, 12];
- Cyber space – a communication network, a control technology.

It is necessary to take care on the security barriers for all mentioned types of elements (hard elements, soft elements, human factor and technical standards), because the physical protection is not enough. The physical components and the operator center (management system and control system) are connected through the communication system. The communication takes place through the cyber space, and it together with the physical components forms the cyber-physical system (CPS). The communication system needs to ensure the reliable and available information flow at maintainable intensity, which will be also safe, RAMS, EN 50126-1 [2]. The purpose of the article is introduced MILS platform as useful and verified way of cybersecurity in network with different security level. The MILS platform is considered with the requirements of existing and preparing standards of cybersecurity and railways.

The physical extensiveness of infrastructure forms a large attack surface in physical space. The infrastructure has high demands on coverage of the communication system, and therefore, the public communication infrastructure is also used for communication between infrastructure elements. The vastness, openness and dynamism of the public communication network lead to a large attack surface in cyberspace, however with possible impacts in cyberspace and physical space as well, Peerenboom [10]. The railway is an example of such infrastructure. The design of the railway system at cyberspace is described in the Chapter 2.

The security of the gateways, which the information flow uses for overcoming the interfaces between systems, can be ensured in the usual ways – access keys, passwords, firewalls, and so on. However, the regular gateway security techniques may not be sufficient in the case of critical infrastructures. A system with multiple independent levels of security (MILS) is appropriate to

[1] Dr., Ph.D.; Czech Technical University in Prague, Faculty of Transportation Sciences; e-mail: japro2am@seznam.cz.
[1] Eng.; Q-media, s.r.o. Pocernicka 272/96, Prague.
[1] Assoc. Prof., Ph.D.; Czech Technical University in Prague, Critical Infrastructure Safety.

use at this causes. The system with the MILS principle guarantees that overcoming of one barrier does not influence the confidentiality of other barriers. The MILS principles are described in Chapter 3.

The Chapter 4 deals with aspects of application of MILS principles at the railway environment.

2. Train cybernetic network

The chapter is devoted to the internal cybernetic train network. It is necessary to start with the overall cybernetic network of railway infrastructure for a better understanding. First, we introduce the principles of the infrastructure network. Then we focus on the internal train network zones.

2.1. Railway Cybernetic Network

The description of the railway cybernetic network is based on the standard prTS [13]. This standard has so far been subject to comments and endorsements, but it already carries information on which we can rely. The main objective of prTS 50701 is to implement the requirements from IEC 62443 [7] to communication systems in the railway environment.

The standard for the security of cybernetics and control systems IEC 62443 divides the network into three levels, enterprise, industrial/enterprise and industrial. The prTS 50701 standard deals only with the technical part of the cybernetic network. The technical part of the network is divided into 4 areas, figure 1. The part of the network associated with the operation, management, and maintenance corresponds to the industrial/enterprise network, figure 1 yellow. Above it is an enterprise network whose parameters are not addressed by the standard.

Figure 1 shows the industrial parts of the network under the industrial/enterprise part. The industrial parts of the railway can be divided into the part connected to the railways, figure 1 green. For railways, we have systems at the infrastructure level and systems along the track. The train industrial railway network is then connected to the train in operation, Figure 1 blue.

Individual network segments can then be plotted in the context of cyber-spatial dependence, Figure 2. Figure 2 shows the area of operation, management, and maintenance, which is connected via secure access to a wide area network. Individual infrastructure elements, such as stations, and systems along the track are then connected to this wide area network. Since securing a large communication space is demanding, all connections must be secured. The connection of the train communication to the railway network is secure via stationary communication elements along the track. The access to the trains must be again secured.

2.2. Train network segmentation

A train in operation can only communicate wireless in principle. While there are ways to secure air communication, the area of attack remains too large. The security must therefore also be implemented on the communication gateway of the train.

At Figure 2 we see 5 different network segments that need to be provided in the train network. One of them is for public services that are in the open communication space of the Internet. It is necessary to ensure a secure separation of access into individual segments to ensure that unsecured or less secure network segments do not endanger critical train functions, Figure 3.

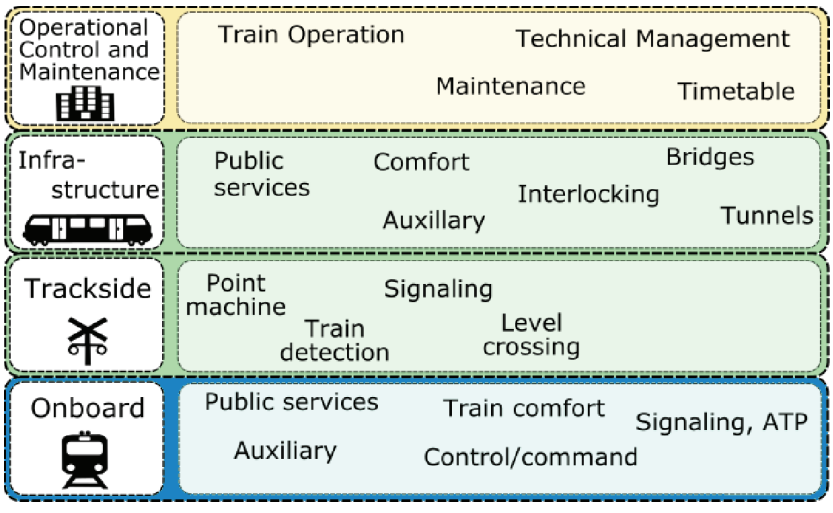

Fig. 1. Railway Cyberspace Assets, prTS50701 [13]

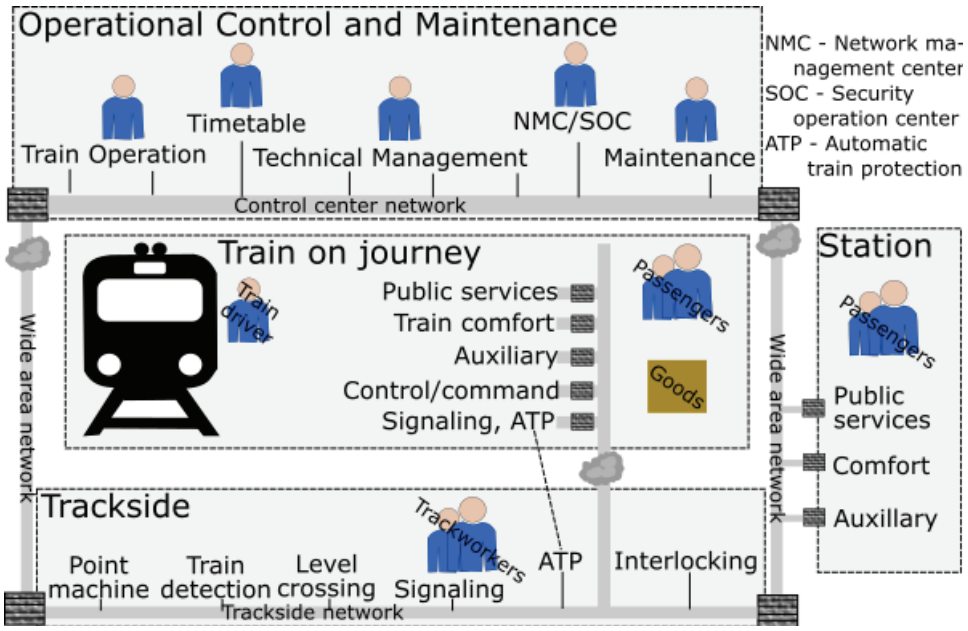

Fig. 2. Railway cyberspace prTS50701 [13]

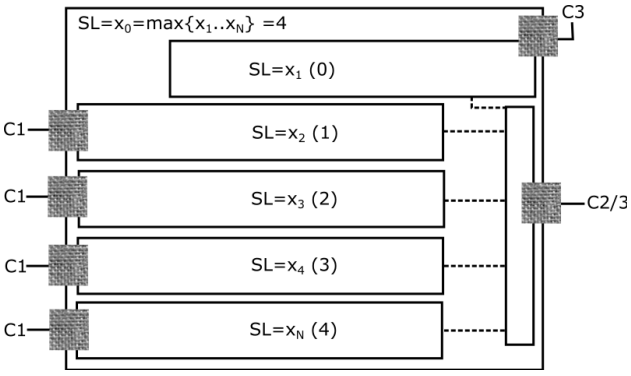

Fig. 3. Train communication gateway according to network needs in Figure 2 [13]

The communication segment must be secured so that the disruption of one part does not compromise the functions of others. The MILS [8] platform application is one way how manage this requirement. The MILS will be discussed in Chapter 4. The individual communication channels in Figure 3 correspond to:

- The public services (not part of the internal train network);
- The comfort of the train (it is controlled locally on trains at present);
- The auxiliary systems (Onboard multimedia and telematics services, OMTS);
- Control and command (Train control and monitoring system for normal operation, TCMS);
- Train protection systems (Train control and monitoring system for emergency operation).

We have also a network segment with safety-critical devices and functions. However, this zone cannot be connected to the open network, but only to the secured zone of the train protection systems. We can also use the diagram of IEC 61375-2-6 [6], Figure 4, to simplify the internal train network. The OMTS zone corresponds to the auxiliary systems of Figure 2. The TCMS zone then includes train control systems for normal and emergency conditions, divided into safety-relevant and non-safety-relevant.

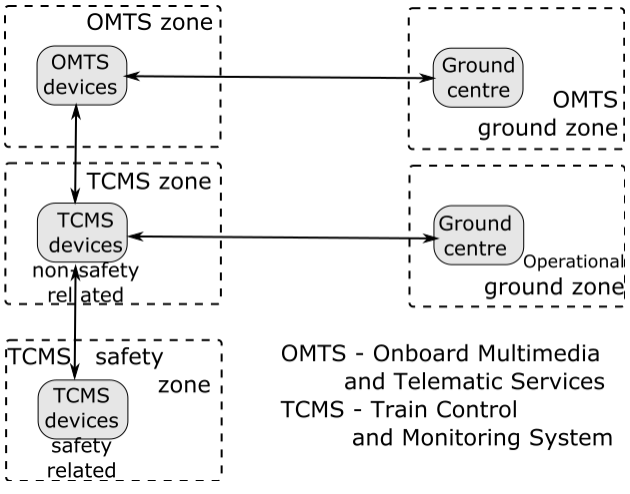

Fig. 4. Simplified train safety zones, IEC 61375-2-6 [6]

3. Multiple Independent Levels of Security

Third chapter describes Operation principles, Operation planes and physical realization of MILS, MILS Community [8].

3.1. Operation principles of MILS

The previous chapter includes the situation where we have interfaces between subsystems with different security level requirements in cyberspace. We can also talk about trustworthy and untrustworthy space. The Information flow between these spaces needs to be secured, and it is necessary to build the security gates to prevent the compromising of a trusted subsystem, figure 5. Types of security barriers are described for example in the standard IEC 62443 [7].

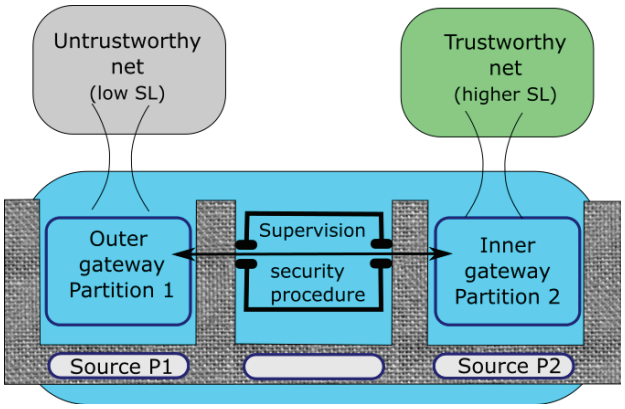

Fig. 5. Schematic representation of the interface between trusted and untrusted networks when applying MILS principles [7]

The Standard IEC 62443 does not only describe the elemental safety barriers and procedures for the control and autonomous systems in cyberspace but far more. It contains foremost the principles and requirements, the application of which should be met. One of the fundamental philosophies of standard IEC 62443 is the application of the "Defense in Depth" principle.

From this reason, the MILS concept applying the defense in depth principles. It means, that each individual security barriers counts with the possibility of failure of the other barriers. The principles included in the MILS approach, Harrison [4] fully meet requirements of defense in depth strategy in the security area of information flow between trusted and untrusted parts of cyberspace.

Principles of MILS approaches stand for the creation of multiple gateways and security procedures through which the information flow needs to pass, Figure 3. Each gateway and each security procedure have its own resources (CPU, Hard drive, RAM, Ethernet, etc.). Disruption of one security barrier will not compromise the other barriers.

3.2. Operation planes of MILS

The MILS Approach application assumes that security setting starts already at the hardware level. Independent operation of individual gates and procedures also requires in order that the security settings of system might be respected on all operation planes of MILS, Figure 6. Following principles need to be comply with:

- The operating system may not randomly allocate the sources, as in the case of conventional operating systems. It must firmly follow the configuration plane – "real time operation systems with the separation kernel hypervisor technology (for example PikeOS).
- The configuration plane or configuration file is the weakest point of the system, and therefore, it needs to be protected (because it affects all partitions).
- The robustness of safety procedures on the monitoring plane greatly influences the benefits of the MILS system.

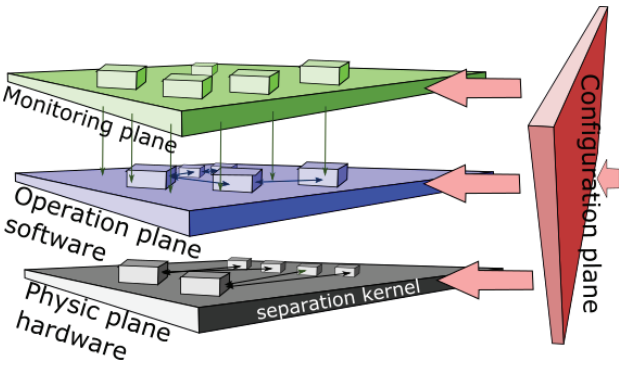

Fig. 6. Planes of MILS implementation, Physical plane (Hardware), Operation plane (Software), Monitoring plane (Security procedures) and Configuration plane (Configuration file) [1]

The adaption plane is sometimes present in the planes of MILS implementation, Figure 6. The adaption hold position on the right side to the configuration plane, which it affects. Adaptation can take place either in the form of maintenance within the update and defect management, or it can be automated. Automated platform response to more complex problems, without compromising security procedures, is still the subject of research.

3.3. Physical realization of MILS

Several ways how to implement the MILS principles are known. A way of fixed allocation of resources, such as an Ethernet connection or Hard disk space,

are obvious. A question of fixed allocation of CPU is more complicated.

It is of course possible to have own processor for each barrier. This is, however, a very impractical option. Therefore, in practice, the MILS is implemented on a single processor. A processor can be either multi core or single core. Distribution of resources for multicore CPU logically suggests to assign each core to different partition. If we have single core processor or there are less cores than security barriers, "kernel separations" Rushby [14] can be performed and individual core partitions are assigned to individual interface partition.

The security levels of individual barriers are also important for the functioning of the whole system. The benefit of MILS approach is weak or negligible in the case of weak or negligible barriers. However, we will get overall MILS security level with combination of barriers with high security level that we would otherwise find difficult or impossible to achieve.

Barriers should also be of different settings. The MILS principle also allows combining the technologies from multiple manufacturer for different partitions so that none of them has "keys" from the entire system. We can then measure and compare barriers from individual manufacturer to get information about their behaviors. However, the integrator needs to remember that the complexity of the system (the number and variety of barriers) increases the demands for system operation and that new threats can arise.

4. Pilot Project

We give example of introducing the MILS pilot project in the Czech railway.

4.1. Train cybernetic gateway

We can use the train cybernetic gateway as an example of the MILS platform at context with the railway cybernetic network, described in Chapter 2. The MILS platform is also suitable for the segmentation of the internal train network, not just at the entry of communication. We have 5 different zones with different functions and security requirements in Figure 2 at the entrance to the train communication network. The gateway can be technically secured, by the communication unit in Figure 7.

The train communication gateway in Figure 7 contains 2 Wi-Fi transmitters, the first for communication with stationary communication units along the line (connection to the ground control center) and the second for providing passenger services. The remaining communication channels are realized via Ethernet connections. The gateway operating system is PikeOS [11]. PikeOS is a hypervisor that ensures a fixed allocation of resources to individual departments. The allocation of communication resources (Ethernet, Wi-Fi) to the partition in Figure 7 is an example of fixed allocation. Allocation of hard disk space, operating memory, or processor time are other examples.

Gateway from figure 7 enable transfer of some resources allocated under normal mode to less critical partitions (public services) to partition with higher criticality (control and command or train protection) for the emergency mode in the context of adaptability.

4.2. Integration and adaption

A concept of solution is not enough to solve technological problems, such as cyber-attacks in practice. A choice of suitable components (hardware and soft-

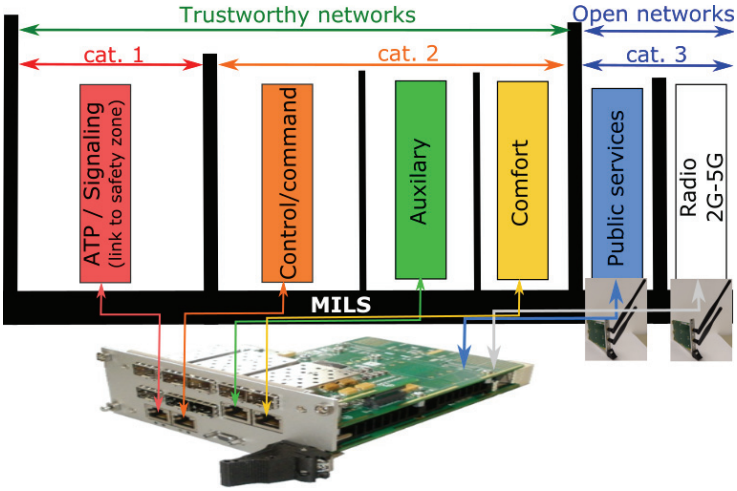

Fig. 7. Train communication gateway [11]

ware), a way of their integration, certification, and in a dynamic environment such as cyberspace, a procedure of adaptability to new threats are also necessary.

A diversification of the suppliers and manufacturers of individual components of the system can increase the security as well as the complexity of the security barrier system. We have three levels of access and responsibilities in the question of gate control, Figure 8:

- Manufacturers of individual elements.
- The integrator.
- An operator / user.

All three levels have their own rules (standards), which they are managed by, and the supervisory authorities that oversee them.

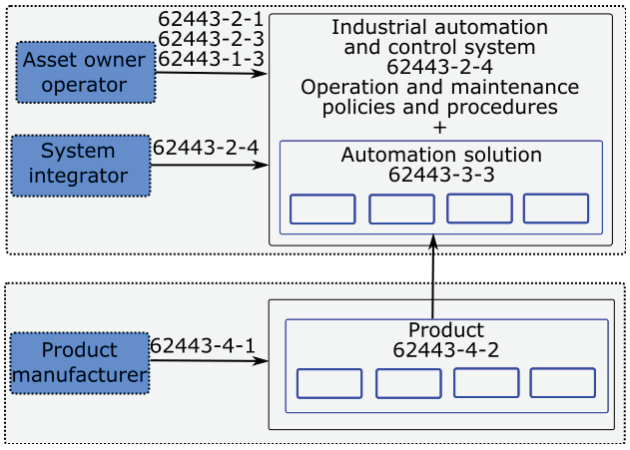

Fig. 8. Three Levels of Responsibility, Manufacturer, Integrator and Operator. Different parts of standard IEC 62443 [7] for different phase of application

The technological setup of MILS called "T-Composition" was designed for the needs of pilots, certMILS [1]. The T-Composition is described in deliverable 8.1 of project certMILS. The verification of MILS T-Composition usability in the railway systems is one of the projects activities.

The next step in project certMILS deals with is the certification. The certification in relation to adaptability (or adaptability in relation to certification) is the issue for a separate article. The manufacturer, integrator and operator must follow the various standards for operation, depending on the area of their activities. The standards do not create obligations only for them, but they also create requirements for the previous segment of supply chain, Figure 7.

The area of cyber security is covered by own standards. We mainly describe a standard IEC 62443 [7]. The standard IEC 62443 is not legally binding at Europe, but it gives guidance, how to proceed or what to expect from previous segments of supply chain point of view of individual technological parts as well as from the point of view of the whole system integration. However, the CENELEC working group is working, for example, on the standard for rail systems cybersecurity, prTS 50701 [13], which is based on the IEC 62443 standard.

The cyber security of individual components can be also standardized with the Common Criteria, IEC 15408 [5]. Both mentioned standards IEC 62443 and IEC 15408 are considered in the European projects certMILS.

The possibility of reconfiguration based on operation requirements, adaptability, is one of the most important features of the system. Implementation of this quality in practice has considerable financial resources. Processes that can easily verify and implement these reconfigurations are necessary to prepare and apply. The solution of this issue is the technological setup of MILS called "I-composition", deliverable 8.1 of certMILS.

The I-composition forms the certified foundation of the system. The I-composition are expanded with another attachments until the desired T-composition is achieved. The system capability of adaptation has several levels: fully self-adaptable system, semi self-adaptable system and manual-adaptable system.

1. The system, which can evaluate situation, define the most optimal configuration, secure safe switch and accomplish certification without the human intervention, stand at the highest level of the dynamic self-configuration. The difficulty of fully self-adaptable system creation lies in maintaining the independence of individual security barriers and real-time certification.
2. The semi self-adaptable system is easier to setup. The semi-dynamic system has several the "allowable states" of resource distribution. All allowable states are verified and certified beforehand. The system can switch only between allowable states. The secure procedure of switching needs to be prepared.
3. The manual-adaptable system is lest progressive from discussed ways of adaption, but it is also connected with lesser risk from unsupervised procedures. The manual-adaptable system use the "I-composition". Verified and certified I-composition has form of box with slot for cards. The card can be easily removed, modified, and installed back to the box. The box and cards together create the T-composition.

5. Conclusion

The criticality of infrastructures as well as the vulnerability are increasing with the increasing dependence of human systems on infrastructures, To-

run [15]. The cybernetic infrastructure is one of such area where new harmful phenomena are dynamically emerging. The security failure inflicted by unknown attacker, hardware manufacturer or software developer has a great media attention today, although these phenomena have been present for a long time.

The protection of information and communications only at the information level with the help of the software is not sufficient. The hardware measure at the cybernetic security level is also necessary. The CPSs are particularly critical from the point of view of cyber-attack because they are associated with the physical world and the physical impacts.

The increase of infrastructure criticality and arise of new harmful cybernetic phenomena demand the application of advanced security procedures. The concept of the MILS enables the effective way to reach high overall security level. The way of certification and adaption need to be prepared in dynamic environment like the cyber space.

References

1. certMILS: Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats [Kompozytowa certyfikacja bezpieczeństwa dla średnio- i wysokowydajnych systemów opartych na COTS w środowiskach, w których występują zagrożenia], EU, Horizon 2020, nr 731456, 2017.
2. EN 50126-1: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [Zastosowania kolejowe – Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS)]. CENELEC, Brussels, 2017.
3. Green Paper on a European Programme for Critical Infrastructure Protection [Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej], EU COM(2005) 576 final, Brussels, 2005.
4. Harrison W.S.: *The MILS Architecture for a Secure Global Information Grid* [Architektura MILS dla bezpiecznej globalnej sieci informacyjnej], The CrossTalk Journal of Defense Software Engineering, 2005.
5. IEC 15408: Common Criteria for Information Technology Security Evaluation [Wspólne kryteria oceny bezpieczeństwa technologii informatycznych], ISO i IEC, 1999, https://commoncriteriaportal.org/.
6. IEC 61375-2-6: Electronic railway equipment – Train communication network: On-board to ground communication [Elektroniczne urządzenia kolejowe – Sieć łączności z pociągiem: Łączność pomiędzy instalacjami pokładowymi i naziemnymi], International Electrotechnical Commission, 2018.
7. IEC 62443: *Security for industrial automation and control systems* [Bezpieczeństwo dla automatyki przemysłowej i systemów sterowania], *International Electrotechnical Commission / International Society of Automation* [Międzynarodowa Komisja Elektrotechniczna/Międzynarodowe Stowarzyszenie ds. Automatyki IEC i ISA], 2019.
8. MILS Community [Społeczność MILS], 2019, WWW http://mils.community.
9. Moteff J., Copeland C., Fischer J.: *Critical Infrastructures: What Makes an Infrastructures Critical*? [Infrastruktura krytyczna: Co sprawia, że infrastruktura jest krytyczna?], CRS Web, Report for Congress, Order Code RL31556, 2003.
10. Peerenboom J.: *Infrastructure Interdependencies: Overview of Concepts and Terminology* [Współzależności infrastrukturalne: przegląd pojęć i terminologii], Argonne National Laboratory, National Science Foundation Workshop, Argonne, 2001.
11. PikeOS Certified Hypervisor, SYSGO, 2019, WWW https://www.sysgo.com/products/pikeos-hypervisor.
12. Procházkova D.: *Challenges connected with critical infrastructure safety* [Wyzwania związane z bezpieczeństwem infrastruktury krytycznej], Lambert Academic Publishing ISBN: 978-3-659-54930-4. s. 218, 2014.
13. prTS 50701: Railway applications – Cybersecurity [Zastosowania kolejowe – Cyberbezpieczeństwo], wersja robocza D6E4, CENELEC, 2019.
14. Rushby J.: *The Design and Verification of Secure Systems, Eighth ACM Symposium on Operating System Principles* [Projektowanie i weryfikacja systemów bezpiecznych, ósme sympozjum ACM na temat zasad systemu operacyjnego, pp. 12–21, Asilomar (ACM Operating Systems Review, Vol. 15, No. 5), 1981.
15. Toruń A. et.al.: *Challenges for Air Transport Providers in Czech Republic and Poland* [Wyzwania dla przewoźników lotniczych w Czechach i Polsce], Journal of Advanced Transportation, nr. 6374592, 2018.

Acknowledgement

This work is part of the certMILS project, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731456.