Certification Cycles of Train Cyber Gateway

Jan Prochazka

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic, E-mail: jpr@qma.cz
Czech Technical University, Jugoslávských partyzánů 3, 16000 Praha 6, Czech Republic

Petr Novobilsky

Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic.

Dana Prochazkova

Czech Technical University, Faculty of Mechanical Engineering, Technická 4, 16607, Praha 6, Czech Republic

Tomas Kertis

Czech Technical University, Jugoslávských partyzánů 3, 16000 Praha 6, Czech Republic

The Critical Infrastructure Protection (CIP) is a classic example of system of systems (SoS) management. We pay special attention to interdependencies among systems within SoS. The article deals with the requirements for the cyber gateway at the train transportation management system. More and more telemetry and remote control through communication systems are used on the track because of the technological development. The train at cyberspace acts as an end network that is connected to the operating center network via an open public network. The gateway must then meet the requirements of the railway infrastructure as well as the cyber infrastructure.
We deal with the integration of various requirements for the train gateway into one verification and certification cycle in this paper. The requirement integration is important because, in the first it is necessary to ensure coherence and consistency between different requirements. The second reason is to speed up possible re-certification. A re-certification is necessary because gateway adaptation or installation in a new environment. The European project certMILS deals with the issue of re-certification.

Keywords: Multiple Independent Levels of Security, certification, cyber-physic system, railway, system of system, critical infrastructure protection.

1. Introduction

The railway is an open complex system. It is interconnected with a number of other systems within the human system, and therefore, it must respect the interdependencies with other systems within the system of systems (SoS) approach. Procedures have been established to resolve conflicts with other systems in the territory during the long history and tradition. The railway can coexist for example with other transport infrastructures or human settlements.

New technologies used in trains, tracks or control centers lead to development of interdependencies with the communication and control systems. The railway cannot be considered only as a physical system any longer. We need apply the approach to railway system as to a cyber-physical system (CPS).

The CPS deals with interdependencies in two different spaces with their own rules of operation. It makes more difficult to ensure proper functioning of system. It is necessary to resolve the conflict between the cybernetic part and the physical part requirements at all phase of CPS life. The article will focus only on the first part of the CPS life cycle, when we need to design a safe architecture for the train's gateway. It must be proposed the architecture that respects the requirements of both spaces within which it is located.

We firstly introduce the standards that the train communication gateway must follow, Chapter 2 of the article. Chapter 3 describes the gateway architecture. Functional and safety requirements are expanded in Chapter 4.

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN/DOI: 978-981-14-8593-0

2. Certification Framework

The product needs to be defined before the entire cycle of product verification and certification start. Defining the products requires a general insight into the standards and requirements. We can talk about the internal certification framework and the external certification framework. We used the first one (internal) for standard with direct impact on the product and the second one (external) for standard, which affect the product through another processes.

2.1 *Internal Certification Framework*

The internal certification framework supervises the proper performance of functions provided by the certified product. Functional requirements can be based on both, the cybernetic and physical part of the system. We also observe security requirements in addition to functional requirements, Figure 1. The whole system has to be protected against threats and dangers of physical and cybernetic nature.

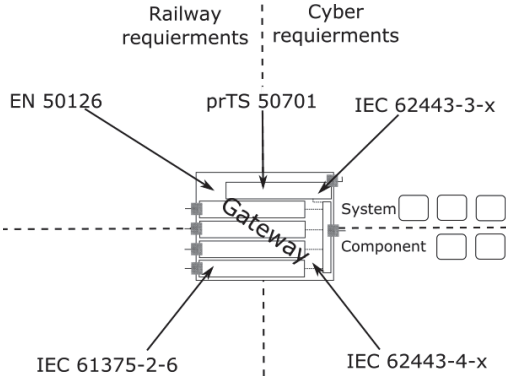

Fig. 1. Certification framework for train cyber gateway.

We received four areas of requirements that need to be implemented and verified in the case of intersection of the communication network and the railway infrastructure. The cybernetic requirements of CPS are based on the standard IEC 62443 (2019). The requirement definition issue can be divided into the functionality of individual components according to the fourth group of the standard part, and the security requirements of the whole product according to the third group of the standard part.

The requirements for the physical part, i.e. the railway, are divided into several standards. The train communication gateway is defined by requirements from IEC 61375-2-6 (2018) in our case. In design, we have mentioned one more standard from the railway environment, Figure 1, prTS 50701 (2019). The standard prTS 50701 is still in the process of approval at the time of writing the article. The aim of prTS 50701 is ensuring the smooth the cyber security requirements application in the railway sector. The standard is also a point of contact for the external certification framework.

2.2 *External Certification Framework*

While the internal certification framework places requirements directly on the certified product, the external certification framework supervises the development and installation environments. The external framework is not executed with the product certification. The environment of development or the environment of installation can be guided by several standards.

Two standards are common to ensure safety and security of products. The first standard deals with information security management in the development environment ISO 27001 (2017). Weaknesses in the product stakeholders' organizations and the data management in terms of information security decrease the product credibility.

In the defined certification framework above, requirements related to the most important assets of the human system are missing. The CPS also requires consideration of safety requirements next to security and functional requirements. Consideration and implementation of these requirements are demanded explicitly by prTS 50701. Safety requirements are specific for the installation site and the environment. The procedure of safety requirements determination for the railway can be found in EN 50126 (2017).

3. Train Cyber Gateway

We have introduced standards with requirements in the second chapter, that the train cyber gateway need to follow. The third chapter deal with standards for given architecture at the first part and with used technology at the second part.

3.1 *Gateway structure*

We established five different internal train networks in design according to prTS50701. Each network has different security level (SL) requirements. Requirements and measures for different SL are set by IEC 62443.

We must consider that the public network of category 3 is on train entry. The one of five train networks is the internet for passengers that is also category 3. Rest of the internal train networks should be in category 1 according to IEC 61375-2-6. The particular security requirements for network categories are again defined according to IEC 62443. The resulting structure is shown in Figure 2.

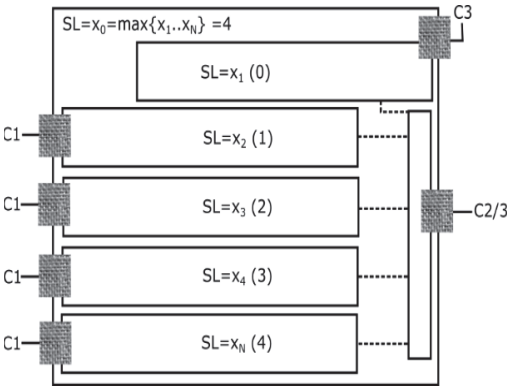

Fig. 2. Diagram of communication channels in the Train Cyber Gateway.

The individual internal networks of the train cyber space can be briefly described from SL 0 (the lowest security level) to SL 4 (the highest security level):

- Public services – SL0.
- Train comfort – SL1.
- Auxiliary functions – SL2.
- Control functions – SL3.
- Emergency functions – SL4.

3.2 *Multiple Independent Levels of Security*

Figure 2 shows that we also have a platform environment in which communication is divided to the individual communication channels. Creating the proper communications transmitter for each network would be expensive and space-consuming. Each network must be independent on each other from security reasons. The solution offers applications of multiple independent levels of security (MILS) approach, Harrison (2005).

The MILS platform is used for creating the several independent partitions, on a single computing unit. The architecture of several independent partitions is appropriate in a place where partition varies in terms of:

- security,
- persons who have access,
- or tasks, which are controlled.

Some parts of the human systems have already prescribed standards for partitioning, for example ARINC 653 (2012) in aviation.

The railway systems standard count only with a recommendation to use partitioning for network segmentation prTS50701 at present or in near future. It can be assumed that in the context of the increasing use of telemetry and remote access, the quality of separation of train control functions into independent partitions will become the mandatory subject for standards as well.

The article discusses the use of the MILS platform for the needs of communication separation on the train cyber gateway. The gateway uses the PikeOS (2019) operating system for kernel separation in our cause. PikeOS runs on a Power PC hardware unit. We have more control over the setting the traffic flow splitting rules, because configuration the of MILS.

The specific measures can be applied within the same computing unit under PikeOS environment to achieve the required SL. We decided on their application within individual internal networks after separation. Computational power demands for communication distributor and five or six firewalls are too high and structure would not be transparent.

The goal of the gateway architecture and its implementation is to ensure that the compromise of the less secured networks does not jeopardize the more critical function of the train networks. The testing of individual security technologies and functions on the train communication gateway will be carried out within of the European project ADMORPH (2020).

4. Requirements

The optimization of the certification cycle of the MILS platform is the subject of the European project certMILS (2017). The compilation and the verification of requirements for different environments is under the influence of new standards.

As we could read in the previous chapters, there are many requirements for a communication gateway. It is not possible to list and justify all of them in one article. Therefore, we go through the requirements of railway and cyber standards only in general. Requirements related to the division of the cyber system into independent partitions are discussed deeper. These requirements are of particular importance to the MILS platform and architecture of our gateway.

4.1 *Railway Security Related Requirements*

The requirements of prTS 50701 (2019) for the train gateway are already reflected in the design in Figure 2. The standard prTS 50701 refers also to the security requirements for product development according to ISO 27001 (2017) and cyber security according to IEC 62443 (2019). IEC 62443 is discussed the section below. The third goal of prTS 50701 is to addresses potential conflicts between security requirements and safety requirements, determined according to EN 50126-1 (2017).

The safety requirements are relevant to the location where the product is installed. The proper safety requirements can only be identified in cooperation with a potential operator. However, the two railway standards mentioned, prTS 50701 and IEC 61375-2-6 (2018), already keep them in mind. The measures and functions identified as relevant to safety are located in the own part of the network that can only be connected to the most secure network, protected by SL4 security functions, in Figure 2.

The part 4.9 of IEC 61375-2-6 defines communication security requirements, and therefore, care must be taken to avoid a conflict with IEC 62443 requirements.

4.2 *Cybernetic Requirements*

We compile the certification framework based primarily on the IEC 62443 (2019). The certification process is subject of the European project certMILS. The project also gain experience and practices from older standards, such as the Common Criteria ISO 15408 (1999). The operation system PikeOS (2019) is certified to the standard ISO 15408 (1999). The MILS platform management process is described at Prochazka (2019) and Schulz (2018 and 2019).

The IEC 62443 consists of several parts. Some of them deal with the product development process. We find the reference to ISO 27001, the application of defence-in-depth approach, the implementation of security architecture, or the product control rules, at IEC 62443-4-1. IEC 62443-4-1 demand from product developer:

- The development following processes from IEC 62443-4-1 or from other reputable standards;
- The security related processes at all phases of development;
- The documentation of security related processes of development;
- The documentation of security related requirements of product and its traceability;
- The security design, implementation and testing;

The part IEC 62443-4-2 deals with several areas of cyber security of component like train gateway. The assessment of requirements for each areas are necessary for secure operation in cyberspace. It is necessary to determine

- The quantity and the type of identifiers by which the control will be proven and the method of their verification (FR1);
- The control and maintenance rules for the element (FR2);
- The system monitoring and the integrity protection (FR3);
- The level of the information confidentiality and ensure it (FR4);
- The segmentation of the network and set allowed flows between partitions (FR5);
- The monitoring and recording of the phenomena that occur in the system during life for possible prevention or response to problems (FR6);
- The system resource management during normal and emergency states (FR7).

All these tools then have assigned SL from 0 to 4.

The state of system can be written using vector (FR1, FR2, FR3, FR4, FR5, FR6, FR7). The desired degree of SL is then achieved in several ways. Standard IEC 62443-4-2 allows to choose convenient approach. The FR5 is of particular interest to the MILS platform from the given list. Network segmentation and control over inter-partition communication is the main asset of MILS approach.

4.3 *Zone boundary protection*

The train's cybernetic gateway is a network device, and therefore, it is mainly subject to network device requirements (NDR), given in the clause 15 of the IEC 62443-4-2 standard. The train communicates with the control centre through an open network. It is, therefore, necessary to set the method of approval (FR1) for individual commands (NDR-1.13).

The gateway architecture for MILS is defined in the configuration file. The configuration file determines both, the partitioning of individual partitions and the communication between partitions (FR5). The configuration also allocates individual system resources to each partition, both in default and in an adapted (emergency) state (FR7). Monitoring and protecting the configuration file as well as protecting its booting process (FR3) requires special attention (NDR-3.14).

Following of configured communication rules has to be monitored (FR3 and FR6). Individual sections should be able to reject communication flows in unwanted directions or without the required verified identifiers (FR5). If monitoring identify suspicious activity, system have to be able close the given communication channel (NDR-5.2).

5. Conclusion

Requirements for securing the communication systems of individual infrastructures are growing with new communication technologies. It is a matter of creating a new standard in the case of railways. The new standard will define the transmission of cybernetic requirements to the railway environment. The new requirements overlap with the old ones and extend them in some ways.

The article describes the requirements for the train cybernetic gateway based on the newly assumed requirements. The main advantage of the developed gateway is segmentation into partitions. The MILS platform enables the creation of independent partitions and controlling of communication among them. The MILS procedure is a way of effectively meeting current requirements, which will be necessary in the event of a vision of the future.

The procedure at article apply to a product that is being certified at the time of writing. The certification framework was defined on the basis of experience with already installed products. However, changes may occur during the realization of certification.

Acknowledgement

This work is part of the certMILS project under grant agreement No. 73145 and ADMORPH project under grant agreement No. 871259, funded by the European Union's Horizon 2020 research and innovation programme.

References

ADMORPH. (2020). *Towards Adaptively Morphing Embedded Systems*. EU, Horizon 2020, no 871259

ARINC 653. (2012). *Avionics Application Software Standard Interface*, Airlines Electronic Engineering Committee.

certMILS. (2017). *Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats*. EU, Horizon 2020, no 731456.

EN 50126-1. (2017). *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. CENELEC, Brussels.

Harrison W. S. (2005, October). *The MILS Architecture for a Secure Global Information Grid*. The CrossTalk Journal of Defense Software Engineering.

IEC 61375-2-6. (2018). *Electronic railway equipment - Train communication network: On-board to ground communication*. International Electrotechnical Commission.

IEC 62443. (2019). *Security for industrial automation and control systems*. International Electrotechnical Commission / International Society of Automation. IEC and ISA.

ISO 27001. (2017). *Information technology. Security techniques. Information security management systems. Requirements*, International Organization for Standardization.

ISO / IEC 15408. (1999). *Common Criteria for Information Technology Security Evaluation*. ISO and IEC. https://www.commoncriteriapo rtal.org.

PikeOS. (2019). *PikeOS® 4.2 Certified Hypervisor*, SYSGO, ttps://www.sysgo.com/products/pikeos-hypervisor

Prochazka J., Novobilsky P., Prochazkova D., (2019), *Cyber Security of Urban Guided Transport Management according MILS Principles*. In: Proceedings of the 29th European Safety and Reliability Conference (ESREL); eds: M. Beer, E. Zio. ISBN: 978-981-11-2724-3. Singapore: ESRA 2019, Research Publishing 2019, pp. 4107 - 4413, doi:10.3850/978-981-11-2724-3_0220-cd, e:enquiries@rpsonline.com.sg,

prTS 50701. (2019). *Railway applications – Cybersecurity*, draft version D6E4, CENELEC.

Schulz T., Griest C., Golatowski F., Timmermann D., (2018). *Strategy for Security Certification of High Assurance Industrial Automation and Control Systems*, IEEE 13th SIES, ISSN: 2150-3117, DOI: 10.1109/SIES.2018.8442081.

Schulz T., Golatowski F., Timmermann D., (2019). *Integration Approach for Communications-based Train Control Applications in a High Assurance Security Architecture*, Springer Nature Switzerland AG. The nal authenticated version is available online at https://doi.org/10.1007/978-3-030-18744-6_18