Management of Security of Cyber Gateway

JAN PROCHAZKA[1,2], PETR NOVOBILSKY[1], DANA PROCHAZKOVA[2,3]

[1]Q-media s.r.o
Počernická 272/96, 10800 Praha 10, CZECH REPUBLIC
[2]Institute of Forensic Engineering
BUT, Purkynova 464, 61200 Brno, CZECH REPUBLIC.
[3]Department of Energy
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6, CZECH REPUBLIC

Abstract: - The necessity to protect the critical infrastructure in way as the cyber-physical system (CPS) is growing with the development of communication and control technologies. The one of elementary approach of protection is to close critical elements to a protected area with secure access. This principle is used in both spaces, the physical and the cyber. Access to these protected areas is then through the gateways. Gateways shall be able identify and authenticate of persons or processes with authorized access and to prevent the access of unauthorized.
The presence of many moving elements (for example, trains) is the specific problem of transport infrastructures, as railway is. The security of moving elements within the CPS must therefore be ensured against both physical and cyber intrusion. We will deal with the cyber gateway of the train at this article, which is called a mobile communication gateway (MCG). The MCG is associated with problems of the standard cyber gateway and the problems specific to the moving systems. It is impossible to secure communication between train and control centrum through a closed communication system only, it must take place through open space because of extensive infrastructure with assistance of ground communication gateway (GCG).
The MCG design shall ensure the security functions of the gateway as well as sufficient communication capacity. Our control over environmental conditions of MCG is limited because it is in open space, both physical and cyber, often in motion. The MCG therefore needs to be able to respond dynamically to environmental changes caused by deliberate attacks or unintentional changes in the system. The ability of the adaptability must be given to the MCG in design.

Key-Words: - Cyber-Physical System, Multiple Independent Levels of Security, Mobile Communication Gateway, Railway, Security.

Received: June 20, 2021. Revised: March 27, 2022. Accepted: April 29, 2022. Published: July 2, 2022.

1 Introduction

The basic function of the State from its establishment has been provided the protection of the human society and public assets, which humans need for life and development. Today, that function is fulfilled by the public administration which according to the European Union should realize so-called good governance. The important role plays the critical infrastructures protection.

The critical infrastructure is a set of mutually interconnected networks, i.e. the systems of various sectors of human system (model of present world). Interconnections of systems mean the mutual dependence. Therefore, their behaviours are dependent on many factors internal or external, which have permanent or random occurrences and under their special combinations they cause emergent phenomena leading to the cascade failures of interconnected infrastructures [1,2].

One of the important critical infrastructures is railway infrastructure. We concentrate to its part, namely to the train infrastructure, especially trains. Train safety is associated with a number of influences that cannot be fully controlled. The train can move along large networks of railway routes in different environments – weather, climate, day and season, geographical influences such as rivers, mountains, forests, countryside, heavily urbanized area.

Moreover, the environment in which the train moves is open and thus comes into contact with other human interests and activities, some of which may be directed against the train itself. Last

but not least, the different stages of movement of the train can have a different effect on its safety situation.

At present, automation penetrates the life of all technical installations. On the one hand, it brings huge benefits and savings in human's work and, on the other hand, other risks. In the context of automation, the control is defined as the targeted action of the control system on the controlled object in order to achieve the specified goal. In this context, control is broken down into automatic realized by information technologies and manual. In practice, control, regulation and higher forms of management (optimal and adaptive management, learning and artificial intelligence) are distinguished. Introduction of automation leads to interconnection of physical and cyber space, i.e. Cyber-Physical systems, the complexity of which increase.

The general requirements for the function of the train control system according to defined levels of degree of automation are given by European standards control system (UGTMS) broken down into several levels according to the level of problem solving (operational planning, traffic control, train control) and according to the degree of automation (GOA 0 to GOA 5, operation of trains at the lookout and non-automated operation up to fully automatic operation of unmanned trains) IEC 61508 [3]. Requirements are marked separately as mandatory, conditional, or optional for each automation level.

This situation of the train in physical space is also reflected in cyberspace. Communication with the train shall be ensured over a large area, independently of the position, environment and movement of the train. Communication takes place through an open space (category 3 IEC 61375-2-6 [4]) network. Therefore, we don't have full control over the operating conditions of the train. The answer may then be the ability of the train to adapt to current changes in operating conditions.

The area of control at the time of automation is the most sensitive area. A cyberattack like any other attack is the most effective when it exploits a vulnerability, i.e. in the case of information technologies sensitive information. The protection of sensitive information can be ensured either by making sensitive information not publicly available (cyber barrier is not enough, it must also be physical) or by encrypting it with modern cryptology methods. According to present knowledge and experiences, the terrorist attacks on control systems as the most dangerous. Therefore, they consider the security of the protection of control systems to be of the highest importance.

It is reality that due Cyber-Physical systems complexity it is not enough to respect valid norms and standards for ensuring the safety and security, but it is necessary to apply the risk engineering principles. The paper shows the procedure of generation of risk-based design of safe / secure train system that has been compiled and tested in several European countries in the frame of the EU projects. under auspice and has been already used in several cases.

The article deals with research on adaptivity of cyber-physical systems (CPS), which in the case of this article is financed by European projects ADMORPH [5] and COSMOS [6].

Based on the present findings [7], each engineering system is characterized by the structure, hardware, procedures, environment, information flows, organization, and interfaces among these components. The safe Cyber-Physical Systems operation means operation which is reliable, functional and does not threatening themselves and their surroundings. The basic element of safe operation of Cyber-Physical Systems in the field of technical solutions is the application of safe technical elements, their qualified interconnections and operating modes allowing safe (i.e. reliable and trouble-free) operation, and proper maintenance, back-up of priority parts of technical fittings, components or systems, use of various back-up principles and thoughtful deployment of back-ups.

The aim is to create a mobile communication gateway (MCG) that will be able to detect some undesirable phenomena. The detection of unpleasant events can take place both in physical and cyberspace. The MCG should then be able to respond to the situation.

In Chapter 2, we will deal with the basic structure of the MCG as it is designed on the basis of standards and its location within Czech railways. Chapter 3 summarizes knowledge on problem solved. Chapter 4 will address the identification of risks to which the MCG should be able to respond. Chapter 5 should then elaborate on monitoring and Chapter 6 of the MCG's response to the monitored influences.

2. Summary of Knowledge on Problem Solved

Cyber-Physical Systems (CPS) are integrations of computation and physical processes. Embedded computers and networks monitor and control the

physical processes, usually with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general- purpose computing. Moreover, physical components are qualitatively different from object-oriented software components. Standard abstractions based on method calls and threads do not work [8]. The CPS concept map compiled by Lee [9] shows a lot of interfaces.

The world dynamically changes, and therefore, the CPS will not be operating in a controlled environment, and must be robust to unexpected conditions and adaptable to subsystem failures. An engineer faces an intrinsic tension; designing predictable and reliable components makes it easier to assemble these components into predictable and reliable systems. But no component is perfectly reliable, and the physical environment will manage to foil predictability by presenting unexpected conditions. Given components that are predictable and reliable, how much can a designer depend on that predictability and reliability when designing the system? How does designer avoid brittle designs, where small deviations from expected operating conditions cause catastrophic failures? Based on present knowledge the risk-based design must be used [10].

We further concentrate to the train safety management system, namely the part of the CPS concept map [9]. According to present knowledge, this system is a complex system, i.e. interconnected physical, cyber and organizational systems (including personnel). Although automation would eliminate the human factor, because it eliminates the presence of human in process, so this is not so, because on the other side the automation increases the complexity and this is also the source of the errors.

The complexity of train system, i.e. system of systems, is based on the required features of the systems, which are: a large dimension; the use of multiple technologies; complex functional dependencies; great interoperability; great performance; high safety, i.e. functionality and reliability, as well as low threat to protected assets under normal, abnormal and critical conditions. The complexity not only creates new dangers, but makes them even worse identified; new hazards are e.g.: increasing the automation [7,11,12].

According to knowledge in cited works, two systemic characteristics are important to complex systems, namely: interactive complexity; and tight connections. Complex interactions are unplanned, unexpected, and mostly unknown sequences that are not immediately understandable. Complex interactions in system systems result in ambiguous decisions, unstable preferences, and conflicting goals. Tight connections are a necessary condition for escalation of undesirable events leading to failure or accident. They are characterized as a time-dependent process, have small slacks, are invariant (there is only one continuation in the process – B must follow A), and as a result of the characteristics in question, there is limited room for improvisation.

Interactive complexity and tight connections between elements in a Cyber-Physical system can lead to a critical situation due to system failure. Complexity not only creates new dangers, but also makes them harder to detect. This means that risk thus becomes a systemic feature. Due to the complexity and high interconnectedness of the train system, systematic analysis of vulnerabilities and robustness with regard to failures is difficult, and therefore, simulation results are used. Security is defined as a non-functional requirement and is associated with the emergent properties of the system. The properties under consideration cannot be assigned to individual system components. They emerge as an integrating result of system behavior. Therefore, security requirements are formulated at the level of the entire Cyber-Physical system and then by a descending process to sub-systems. The result of a disaster of a certain size depends on the immediate state of the system.

In addition to the inherent complexity of the systems in question, their interdependences are important. Emergent connections that arise only under specific conditions are of particular importance. Just, these unpredictable addictions that are the cause of the cascade failures, or unwanted domino effects and other uncomfortable events that result from various synergies and cumulations, and which are the greatest threat to today's societies.

Moreover, present knowledge and experiences show that using the redundancy can actually increase complexity to the point where they themselves are already contributing factors to accidents. When designing the redundant systems, a number of aspects should be considered, e.g. the fact that they increase the complexity of the sys-

tem, creating the possibility of unexpected connections that cause unwanted events or entire cascades of such events.

In harmony with Schneier's assertion [13], it shows that ensuring the security and safety is a process in which measures are applied to the human security in variable conditions. The high degree of uncertainty (knowledge uncertainty) does not allow a satisfactory prediction of the behavior of a complex system of systems in conditions in which many disasters of internal and external arise and a human factor acts. From this reason, the railway protection and train protection are difficult.

Depending on train system complexity, three risk-related objectives are distinguished:

- operation safety,
- process safety (component operation, production line)
- and entity integral safety.

Because the higher the objective is used, the higher the demands (knowledge, data, finance, time) are connected with its use, so in practice they are preferred tools with the lowest demands, which, based on current knowledge and experience, have the capability to solve a task if they are respected the safety culture basic rules and the operating regulations correspond-ding to operation conditions; i.e. it is not considered intent to damage the entity.

Due to train system complexity, its problems cannot be only solved theoretically by analytical methods, because they are very influenced by characteristics of regions in which they are located, which are multifarious. It is also caused by reality that each region has different possibilities for problems solution and these have been changing in time because the world and its parts have been dynamically varied.

The research [10] shows that:

- each technical facility design has a certain danger. The designer art is to select such solution that is optimal, i.e. it is sufficiently safe and it is possible to realize with regard to investor and public administration options. The near the same holds for manufacturer´ skill (craftsmanship) at realization,
- impressive and low robust designs with insufficient safety margins often fail sooner or later,
- wrongly determined limits and conditions for critical technical facility parts lead to frequent disturbances up to serious accidents; they are not able to react to condition changes.

According to above cited research, it follows that in design of security of train system, it is necessary to follow the requirements for:

- durability,
- manageability of equipment and processes,
- lifespan,
- human resources,
- costs,
- technical services,
- other service,
- safety of employees, humans in surroundings and environment.

From safety viewpoint, the main goal of designing process is to avert unwanted combinations of incidents that have potential to cause accidents accompanied by major damages. To do this, it is necessary to use:

- safety functions for control safety under border conditions, thereby the occurrence possibility of unlikely severe accident is reducing,
- seven principles of resilience as: backup; to insert ability of sleek and controlled degradation; to insert ability to return from degraded state; flexibility in both, the system and the organization; to insert ability to control limit conditions close to the performance interface; to insert optimal management models; to reduce complexity; and to reduce possible non-demanded couplings.

Big roles play *limits and conditions*, which are a set of clearly defined conditions for which it is proven that the operation of the train system is safe. In design, it is necessary to include program for safety increase that ensures:

- safety and functionality of all fittings that corresponds to their missions,
- identification, evaluation, elimination or regulation of potential risks at acceptable level for important installations, systems and their various parts,
- risk management, which includes all possible disasters with resources inside and outside the technical facility that cannot be eliminated,
- protection of personnel, people in the vicinity, environment, facilities and property,
- use of new materials or products and test techniques only in a way that is only associated with minimal risk,
- insertion of safety factors that ensure corrective measures that lead to improvement,
- consideration of all appropriate historical data.

The processes risk management strategy in design needs to use: principles of inherent safety;

passive safety systems; active safety systems; different barriers types; procedural procedures that are proven or thoroughly tested in such a way that they do not contain latent sources of danger under possible conditions; and in important Cyber-Physical systems, the Defence-In-Depth principle [7].

3. Mobile Communication Gateway

For solution of problem we use the knowledge summarized in previous Chapter and existing train management system which we further describe. A mobile communication gateway is a cyber-physical device that connects a mobile system such as a train to a fixed ground infrastructure. Mobile communication gateways must follow a wide range of standards and rules, determined areas of their deployment. In the case of a train, the list of standards within the certification cycle is detailed in the article [14].

The communication between the train and the ground infrastructure demand that we have communication gateways on both sides. The gate on the ground infrastructure side is called the ground communication gate (GCG) and the gate on the mobile system side, such as the train, is called the mobile communication gateway (MCG), Figure 1.

The train's cyber network is divided into several areas, such as public services, train comfort, train auxiliary systems, train control systems and critical train systems, prTS50701 [15]. Communication for these areas can be ensured by independent communication channels. More practical, however, is the use of a single communication channel, where communication gateways on both sides support communications with different level of criticality.

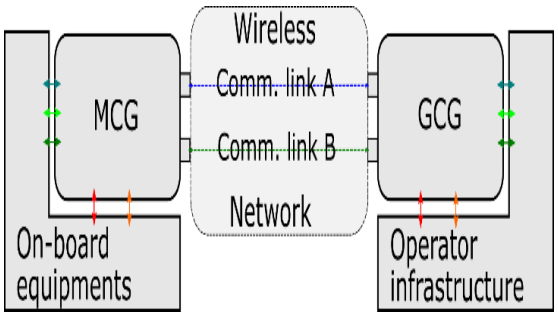

Fig. 1. Scheme of communication between train and ground infrastructure.

To ensure communication with different level of criticality, described gateway uses the principles of multiple independent levels of security (MILS) as it is shown [16,17]. The communication gates in Figure 1 also contain redundant communication lines, in case of security incidents on main line A. Wireless communication takes place through an open system. The communication operator reserved communication band for the needs of the train operator, however, anybody cannot guarantee prevention of intrusion from any third-party agents.

The security of the train's cyber network must therefore be ensured on the side of the train's communication gate. The MCG, which ensures safe communication for different train systems using the PikeOS operating system, PikeOS [18] and MILS principles, is shown in Figure 2.

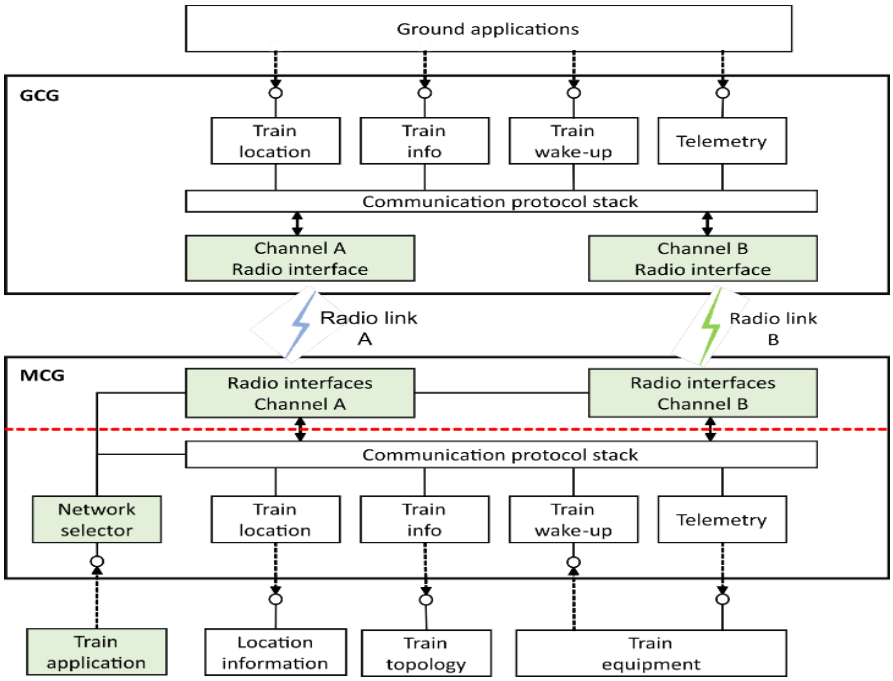

Fig. 2. Structure of MCG and GCG divided in supported areas of communication.

In Figure 2, we can also see the structure of the GCG, which reflects the structure of the MCG. The structure of the MCG is based on the functional requirements of the train operator and reflects the prTS50701 standard [15]. The security of individual zones is based on the security requirements of IEC 62443 [19].

4. Selected Risks of Mobile Communication Gateway

The MCG [14] was developed according to standard IEC 62443-4-1 [19]. A risk analysis was carried out within the given network context of MCG as one of the first tasks. 28 specific threats were identified during the risk analysis. Sources of threats was both inside and outside the railway infrastructure system. The identified risks have been evaluated and measures have been proposed according to the IEC 62443-4-2 [19] requirement.

Measures set up before commissioning are sufficient to achieve the required security within the current situation in the field of communication security at the place of deployment, i.e. the railway operator. However, with increasing demands on communication security with time, it is necessary to develop tools to enable the operator to respond to operational situations.

As part of the identified threats, we have selected threats which have the potential to increase in the future and which can also be monitored directly or indirectly. The risks selected are listed in Table 1.

TABLE 1: SELECTED SOURCES OF RISKS OF MCG. Risks which are monitored by the MCG monitors.

Item	Risk source
1	The attacker manipulates internal network systems.
2	The attacker accesses operator's information.
3	HW failure
4	Bad operational input data.
5	Many unauthorized accesses.
6	Communication will not take place due to lack of resources.
7	Alteration of forwarded data (intentional or unintentional).

The MCG [14] was developed according to standard IEC 62443-4-1 [19]. A risk analysis was carried out within the given network context of MCG as one of the first tasks. 28 specific threats were identified during the risk analysis. Sources of threats was both inside and outside the railway infrastructure system. The identified risks have been evaluated and measures have been proposed according to the IEC 62443-4-2 (2019) requirement.

Table 1 contain six selected sources of risks which are monitored by the MCG. This does not mean that the gateway is equipped with six different monitoring systems, each for individual risks. Some risks can be detected by one monitoring system. For safety increase we need more monitors for different scenarios of others risks. Therefore, we divided the risks and their scenarios into three areas for further processing.

The first area deals with the proper functioning of the physical part of the MCG. Hardware misbehavior can be caused by technical errors, altered system functionality by an attacker, or MCG overload.

The second area concerns the information flow that enters the gate. We can observe quality of the information flow, if it has not been altered and we can also monitor quantity, i.e. whether its density corresponds to standard operation values.

The third area is then associated with activities at the MCG that may be related to attempts to infiltrate or successfully infiltrate the MCG.

We connected the risks from Table 1 or their scenarios of realization to individual areas. Each of the three areas is then connected with a monitoring system, which will be described in the chapter 4. With the development of technologies, the amount monitored risks may increase. However, it will always be necessary to select the most critical risks, considering the limited available MCG resources.

5. Monitoring Systems

Three different systems for monitoring are developed. They are based on the risk areas identified in Chapter 3. Each of the monitoring systems can be divided into three subsystems:

1. A network of sensors or detectors that monitor the quantity or quantities associated with the monitored phenomenon.
2. A transmission channel with a messaging protocol,
3. Evaluation of monitored quantities over time.

The MQTT protocol [20] is used for the transmission of information between detectors, sensors on the one side and evaluation subsystem on the other side within MCG. Sensors send monitored data also to operator's network.

The computing unit for evaluation may be theoretically placed in different part of network. Using the operator servers is connected with risk at open communication space among servers. MCG has, therefore, some of resources reserved for monitoring and other for monitored data processing.

Evaluation of monitored quantities need to be simple and effective this way and it is necessary to set the thresholds for the monitored quantities correctly. Monitoring sensors or detectors rarely recognize the problem as such, they only respect setting the limits for defining green, orange, and red areas for monitored quantities leads to alarms or other procedures. Poor limit setting can lead to insensitive monitoring or false alarms. The wide variability of the railway infrastructure can lead to fluctuations in operating parameters.

If train has own computing unit with enough computing capacity, evaluation of monitored quantities could be transferred there.

All three monitoring systems share communication protocols and a monitoring evaluation server. They differ in the use of sensor detectors of individual monitoring systems. Individual monitoring systems can be identified as:

1. Physical monitoring of the MCG,
2. Communication flow to MCG,
3. Intruder at the MCG.

5.1 *Physical Monitoring of the MCG*

The main monitoring system of the MCG monitor physical parameters of the gateway. Within the CPS, cyber processes are supported by technologies represented in physical space. Changes in cyber processes can result in changes in states within the physical part of the system. Physical monitoring can detect the failure of the physical part of the CPS as well.

Physical monitoring consists of several sensors. Temperature sensors are implemented on the central power unit and power source according to [21]. The temperature sensors also monitor the conditions of the individual peripherals that will be connected to the gateway. The last temperature sensor then monitors the reference temperature of the environment. The electrical voltage and electric current are other parameters monitored by MCG.

The main goal of physical monitoring is to monitor the intensity of activities of critical hardware components. The performance intensity of each hardware component has a standard operating band of values. A significant deflection from these values can then reveal non-inherent activities at the MCG before critical overload or other unwanted changes of the system occurs, for example, due to a DDoS attack.

Utilization of physical monitoring is part of project ADMORPH [5], which prepare system monitoring and identification of non-inherent activities.

5.2 *Communication Flow to MCG*

Communication flow to the MCG is monitored on the level of statistics observation. Communication module logs information of sent and received packets. The packet intensity, the packets accepted, and the packets rejected are stored. Any deflection from normal operating intensities or an increase in rejected packets is then assessed.

Communication flow monitoring at the MCG is implemented within the ADMORPH project as a reference to physical monitoring.

5.3 *Intruder at the MCG*

Intruder activity can be detected through physical changes at the MCG. However, if the intruder behaves subtly enough, his activity may remain hidden within the tolerance of parameter fluctuation. It is therefore necessary to prepare an additional monitoring system for detection of intruder activities within the MCG. As part of the COSMOS project [6], we prepare for the development of a system for monitoring software processes. The MCG software representation assumes 4 different levels of structure, see Figure 3. Each of these levels is then associated with certain processes enabled for it. While processes at the level of the operator-specified software may have a certain degree of fluctuation. Detecting operational deviations in lower layers must be more sensitive.

6. Adaptive Respond of MCG

The response is conditional on monitoring of an unacceptable situation. Monitoring systems send information about the MCG to the monitored assessment center. The response then begins on this computational unit. The monitored quantities are assessed on the basis of a defined algorithm and if the situation is evaluated as emergency or critical, the relevant alarm is triggered and the response with it.

6.1 *Alarm Setting*

There are many ways and algorithms to determine emergency situation in academic areas. The development of IT systems is associated with the development of cognitive functions of artificial intelligence nowadays and its ability to respond to specific problems.

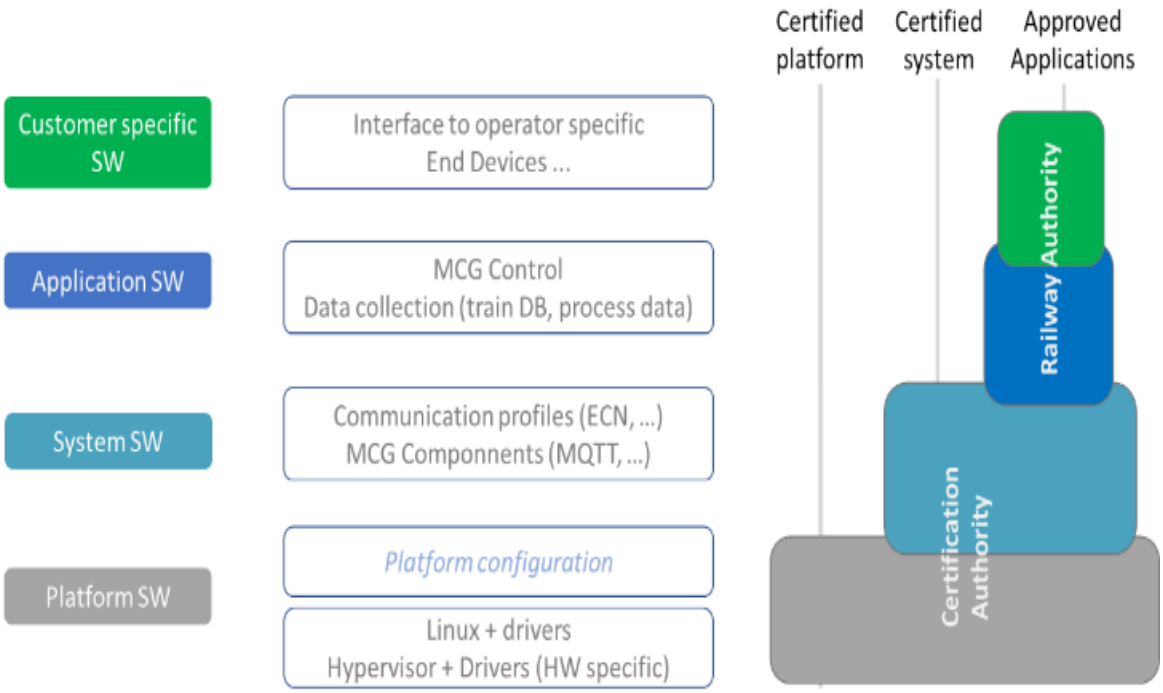

Fig. 3. MCG software structure.

Such an approach is risky however in area of critical infrastructure for now because cognitive IT systems need time to learn it had high demands on initial programming. The more complex algorithms are, the more demanding for resources and time it makes them.

The MCG in our cause, therefore, implement a conservative approach, rules-based adaptivity. The rules-based MCG has strictly given behavior, how to behave in what situation, deterministic behavior in other words.

We have four different areas of values for parameters that can be for monitored, such as temperature on individual sensors, voltage, information flow intensity, or number of rejected packets; scheme is in Figure 4.

Fig. 4. Areas where monitored values may be located. Green corresponds to optimal operating values.

Green is the area of expected operating values. The gray area corresponds to smaller values to indicate that one of the internal systems is not running or not working properly. The orange area means exceeding the limits for operating parameters. It may be emergency situation, but it can be an overrun caused by non-critical influences. Red is then an area requiring a quick system response to the situation.

If the monitored values are in a gray area. The system may use an alternative communication channel, Figures 1 and 2. The MCG has no control over the internal train systems or the operator's external systems and can only send warning in the cause of their malfunction. The green area does not require any response.

The orange and red areas are associated with the same response. The difference is that in the case of an orange area, it is first necessary to compare this output with the outputs from other monitors. Thus, the response is not triggered immediately, but only after comparing more data. If the suspicion is confirmed by other monitored parameters, or if the monitored quantity is in the orange area longer, the same alarm is triggered as for the

red area. The alarm is triggered immediately for the red area.

6.2 *Respond Setting*

Response management tools must be implemented in the MCG ahead, Figure 2, so that the MCG can use them in case of adaptation process. The MCG from Figure 2 has 2 communication channels and other sources that support these communication channels. Independence must be ensured for the response to fail of channel or attack on channel to work.

The MCG from Figure 2 uses PikeOS [18] to implement the MILS approach. If channel A or one of its sources is compromised, the system switches to channel B. Channel B has its own resources and is independent of channel A. Channel B will not be affected by a failure on Channel A, and the Channel A attacker will have to start an attack on Channel B from the beginning. Channel A, meanwhile, may restart in an attempt to deal with a technical problem. A disused channel is inactive, so it is not possible to attack it.

The system image protection of is important for the security of the MCG. The MCG image, verified by the manufacturer, digitally signed, and encrypted, is enclosed in a separate partition. In case of any problem, the individual part or the entire system can be automatically restarted and loaded according to the saved image.

Of course, the set response only addresses attacks on the MCG of train, not attacks inside the train or inside the operator's network. At the same time, the response assumes that carrying out an attack is not a trivial process, and failure is not a common phenomenon. However, the MCG is developed and certified according to IEC 62443 [19], which should ensure that these essential requirements are met.

7. Conclusion

The security of the train's cyber network requires increasing attention in the communication age of the twenty-first century. The train, as CPS, is affected by both subsystems. The behaviour of the train in physical space is associated with movement on a large infrastructure that makes it difficult to supervise the train. Communication with the operations centre in cyberspace is then conducted through an open communication space.

The MCG must be prepared to respond to growing threats. This means not only better passive security according to modern technical standards, but also the development of active security. The active security of the MCG cannot rely on the timely intervention of a human operator, it needs its own ability to adapt to situations.

In connection with this, we have developed the MCG, which is inherently equipped with monitoring systems to detect undesirable events and phenomena. We are currently testing MCG with monitoring of several parameters in operating conditions. The quantity and quality of the monitored parameters may increase in the future.

The ability to adapt to new conditions and identified threats must be given to the MCG during the development. The developed MCG uses basic tools such as redundancy or system parts recovery. We also deal with flexibility in allocating resources to individual processes. However, this flexibility must not undermine the security advantages of the MILS approach.

The paper shows the procedure of generation of risk-based design of safe / secure train system that has been compiled and tested in several European countries in the frame of the EU projects. It has been tested in practice is countries participating in the EU projects. On the tests results, the improvements are included in the design. Tests in the Czech Republic [22] show big progress in security in practice at application of design which is described above.

Acknowledgement: This work is part of the ADMORPH project under grant agreement No. 871259 and COSMOS project under grant agreement No. 957254, funded by the European Union's Horizon 2020 research and innovation programme. It is also part of project CK01000095 under TAČR program DOPRAVA 2020+.

References

[1] EU. *Green Paper on European Programme for Critical Intrastructure Protection*. Brussels: EU 17. 11. 2005, COM(2005) 576.

[2] PROCHAZKOVA, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218 p.

[3] IEC 61508. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related System*. Geneva: International Electrotechnical Commission 2011.

[4] IEC 61375-2-6. *Electronic Railway Equipment - Train Communication Network: On-board to Ground communication*. International Electrotechnical Commission 2018.

[5] ADMORPH. *Towards Adaptively Morphing Embedded Systems*. EU, Horizon 2020, no 871259.

[6] COSMOS. *DevOps for Complex Cyber-Physical Systems*. EU, Horizon 2021, no 957254.

[7] PROCHÁZKOVÁ, D. *Principles of Management of Risks of Complex Technological Facilities*. ISBN 978-80-01-06180-0, Praha: ČVUT 2017, 364 p. http://hdl.handle.net/10467/72582

[8] LEE, E. A. *Cyber Physical Systems: Design Challenges.* DOI 10.1109/ISORC.2008.25

[9] LEE, E. A. *Cyber-Physical Systems- a Concept Map.* http://CyberPhysicalSystems.org

[10] PROCHAZKOVA, D., PROCHAZKA, J. *Risk Management at Technical Facilities Designing, Building and Commissioning*. Praha: ČVUT 2020, 145 p. https://doi.org/10.14311/BK.9788001067 161

[11] HOLLNAGEL, E. *FRAM: the Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems.* Ashgate Publishing, Ltd. 2012.

[12] OECD. Machine-to-Machine Communications: Connecting Billions of Devices. *Digital Economy Papers, No. 192.* Paris: OECD 2004.http://dx.doi.org/10.1787/5k9gsh2gpn43-en

[13] SCHNEIER, B. *Schneier on Security.* New York: John Wiley & Sonns 2002.

[14] PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D. Certification Cycles of Train Cyber Gateway. In: *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (ESREL 2020 PSAM15). No. 3728. ISBN 978-981-14-8593-0. Singapore: ESRA 2020, Research Publishing Singapore 2020. e:enquiries@rpsonline.com.sg

[15] prTS 50701. *Railway Applications – Cybersecurity*, draft version D8E5, CENELEC 2020

16] HARRISON W. S. The MILS Architecture for a Secure Global Information Grid. The CrossTalk .*Journal of Defense Software Engineering* 2005.

[17] PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D. *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,

[18] PikeOS. *PikeOS® 4.2 Certified Hypervisor*, SYSGO, 2019. https://www.sysgo.com/products/pikeos-hypervisor

[19] IEC 62443. (2019). *Security for Industrial Automation and Control Systems*. International Electrotechnical Commission / International Society of Automation. IEC and ISA.

[20] MQTT. *MQTT: The Standard for IoT Messaging*. 2020. Online on https:/mqtt.org.

[21] CORBETTA S., ZONI D., FORNACIARI W. A Temperature and Reliability Oriented Simulation Framework for Multi-Core Architectures. In: *2012 IEEE Computer Society Annual Symposium on VLSI*, IEEE.

[22] Q-MEDIA. *Archives.* Praha: Q-media 2021.