Cyber Security of Urban Guided Transport Management according to MILS Principles

Jan Prochazka

Q-media, s.r.o. Jahodová 1283/33, Prague 10, 106 00, Czech Republic.
Czech Technical University in Prague, Faculty of Transportation Sciences, Konviktská 20, Prague 1, 110 00, Czech Republic.
E-mail: japro2am@seznam.cz

Petr Novobilsky

UniControls a.s. Křenická 2257, Prague 10, 100 00, Czech Republic.

Dana Prochazkova

Czech Technical University in Prague, Prague 6, 160 00, Czech Republic.

The Urban guided transport management system (UGTMS) as subway, transports from several hundreds of thousands to millions of passengers per day. Size and irreplaceability of subway transport capacity include the subway transport to the critical infrastructures of cities, regions or countries. Modern transport critical infrastructures contain in addition to physical and social parts also the cyber control systems and they are marked as cyber- physical systems (CPS). The CPSs are characterized by safety-critical nature, complexity, connectivity, and open technology. The CPS complexity, openness and dynamics form a large attack surface that may lead to failures and irreparable damage.

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 subsystem, which connects the individual UGTMS subsystems (Wayside subsystem, On-board subsystem and operation control subsystem). Therefore, the communication system should guarantee transmission parameters and do not affect security level of the respective subsystems.

Keywords: Urban guided transport management system, cyber physical systems, critical infrastructures, Multiple Independent Levels of Security.

1. Introduction

The critical infrastructure protection has become an essential part of advanced human systems security strategies. Critical infrastructures are often formed by extensive networks of physical elements (either point or line types), their management system, human factor, technical standards, relevant legislation and management strategy as well, (EU 2005, Moteff 2003, Prochazkova 2014). 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 protection of infrastructure management systems is mostly linked to a single environment of the communication infrastructure, through which the operation control is implemented into whole infrastructure. The protected system can be divided into three parts in terms of elements protection. We have a network of physical components distributed over an extensive territory that needs to be coordinated. The physical components may be stationary (lights, switches) or mobile (train sets). The second part is dispatch management. The dispatch management consist of a human factor and an information system.

The physical components and the dispatch management are connected through third part, i.e. 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 1999).

The article will exclusively address the security of interfaces between the communication system and the internal cyber environment of the critical infrastructure (Dunn 2004). The solution with the least risk would be built up its own isolated data transmission system from the cyber security of the communication system point of view. Such

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0220-cd

a solution would be safe and reliable, but difficult and expensive to reach and maintain.

The physical extensiveness of infrastructure form 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 2001). The Urban Guided Transport Management System (UGTMS) is an example of such infrastructure; it is described in the Chapter 2.

The security of the gates, 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 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 Prague metro/subway as representatives of UGTMS.

2. The Urban Guided Transport Management

The paper discusses three aspects of UGTMS: System Management Levels, System Architecture and problems of cyber-attacks on the CPS.

2.1 *System Management Levels*

The structure of UGTMS can be divided according several various plane. One is the management viewpoint, where we distinguish three elemental levels, Figure 1. The "Operation planning" is ensured at the highest level, both long-term (strategic management) and short-term (tactical management). Only the level of politic management lies above the operation planning. The policy level for UGTMS is given by standard (IEC 62290 2018).

The lower two levels of the pyramid at Figure 1, are "Operation management and supervision" (Operational Management) and "Train operation" (Technical Management). Operation management and train operation lie at lower level of management pyramid than operation planning at offices; however, they are more critical from the point of view of cyber security. Operation control center and decentralized control of trains and waysides are an example of CPS. It is also necessary to ensure the proper maintenance of the whole system in addition to management levels of operation. Maintenance pervades through the whole pyramid, from operation planning at top to train management at bottom.

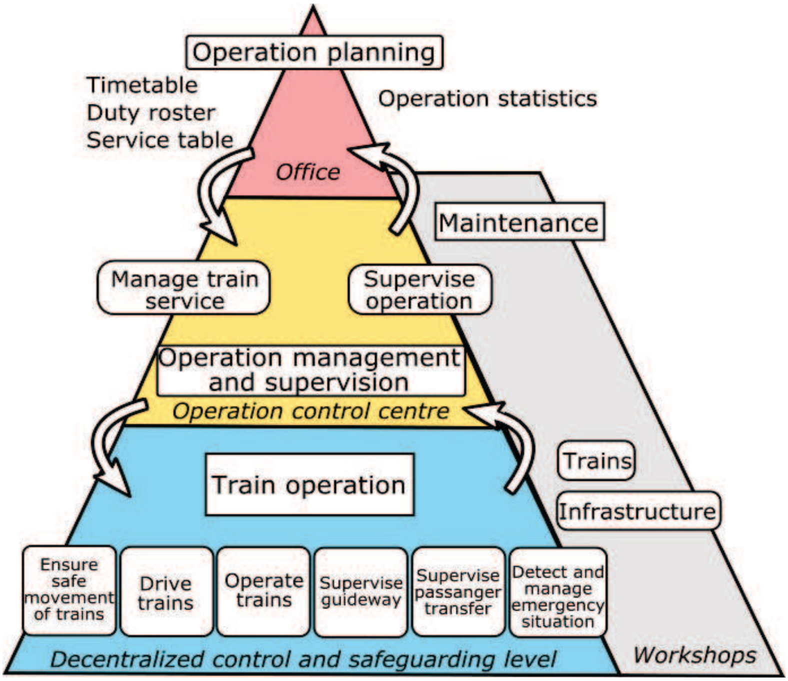

Fig. 1 Organization and operation structure of UGTMS (IEC 62290 2018).

2.2 *System Architecture*

Critical points need to be identified, before we begin to build the security measures of the system. We use the UGTMS architecture according to the standard (IEC 62290 2018); it is shown in Figure 2. Figure 2 represents the lower two levels of the pyramid shown in Figure 1, i.e. the Operation management and supervision, and train operation. Moreover, Figure 2 also shows the links from these two levels in direction out of the system, for example to operation planning or maintenance.

The cybernetic core of the UGTMS composes of three subsystems:

- Operation Control Subsystem.
- Onboard Subsystem.
- Wayside Subsystem.

Exchange of data and information is necessary to ensure among these three subsystems. Data Communication Subsystem secures the exchange of data and information.

As it is discussed at introduction, a dedicated network of communication systems through the open radio space and public communications links are used for communication. Figure 2 illustrates a big number of interfaces between cybernetic systems with different security level requirements. Interfaces are located on the outer edge of UGTMS cyberspace (passenger information, operation planning, central surveillance, etc.) and also at inner space of the system itself (Data Communication Subsystem). Security gates are necessary to build on these interfaces to ensure the security level requirements.

The number of security gates needs to be large, because we need to ensure the safety of the Operation Control Subsystem and as well as to guarantee the transmission path for each train and wayside elements. Security levels requirements must be set up and ensured in view of the fact, that it is the CPS. A cyber-attack on the CPS can lead to great material and human health damage and harm as it is shown e.g. in (Kertis 2018).

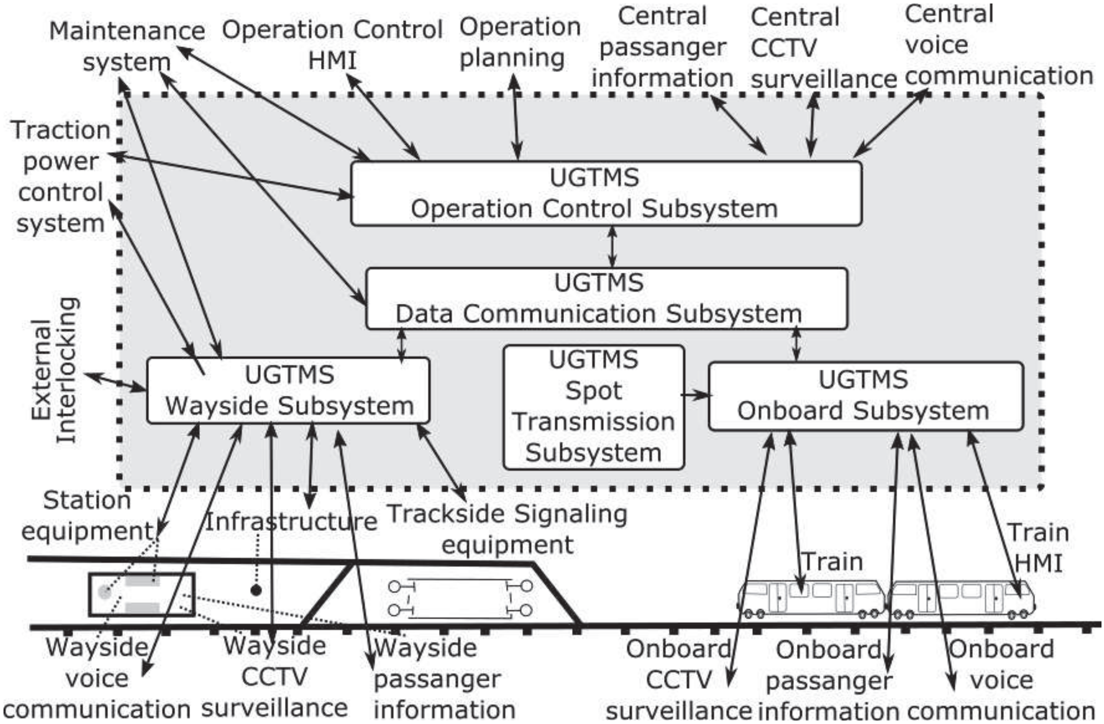
Maintenance system
Operation Control HMI
Operation planning
Central passanger information
Central CCTV surveillance
Central voice communication
Traction power control system
UGTMS Operation Control Subsystem
UGTMS Data Communication Subsystem
External Interlocking
UGTMS Wayside Subsystem
UGTMS Spot Transmission Subsystem
UGTMS Onboard Subsystem
Station equipment
Infrastructure
Trackside Signaling equipment
Train
Train HMI
Wayside voice communication
Wayside CCTV surveillance
Wayside passanger information
Onboard CCTV surveillance
Onboard passanger information
Onboard voice communication

Fig. 2. The Urban guided transport management system architecture (IEC 62290 2018).

2.3 *Cyber-attacks at cyber-physical systems*

We live at a time when there are in public media regular reports of cyber threats, whether associated with unknown invaders or technology manufacturers. Information security is very often discussed in the context of these cases, but there is a little talk of possible impacts on the CPS.

The disruption of information security, for example at the office level on Figure 1, may lead to financial damages depending on the value of the infringed information.

The disruption of the cyber security of the CPS as Operation Control Center, on the other hand, can lead to damage of both parts, the cybernetic as well as the physical part of the system. Losses on information, materials and human health and lives of the CPS can be accompanied with the losses on protected assets of neighborhood systems connected by links and flows with the CPS. Although, the CPS parts are at the bottom, from the point of view of the management levels, the requirements for their security levels are much greater than their position. From this reason, the critical infrastructure operators need to be convinced about this fact, as well as in case of industry 4.0, in particular the heavy and chemical industry operators.

3. Multiple Independent Levels of Security

Third chapter describes Operation principles, Operation planes and physical realization of MILS.

3.1 *Operation principles of MILS*

The previous chapter describes 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 3. Types of security barriers are described for example in the standard (IEC / ISA 62443 2018).

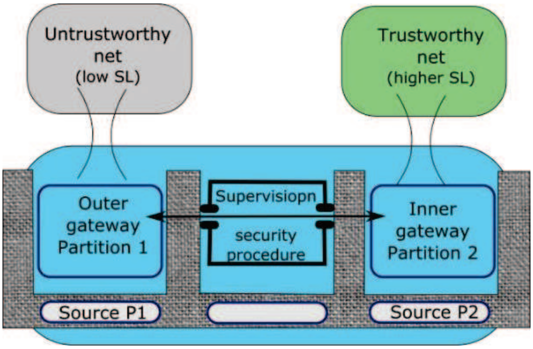
Untrustworthy net (low SL)
Trustworthy net (higher SL)
Outer gateway Partition 1
Supervisiopn
security procedure
Inner gateway Partition 2
Source P1
Source P2

Fig. 3. Schematic representation of the interface between trusted and untrusted networks when applying MILS principles.

The Standard (IEC / ISA 62443 2018) 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 / ISA 62443 2018) 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 barrier of security barriers counts with the possibility of failure of the other barriers. The principles included in the MILS approach (Harrison 2005) 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 4. Following principles need to be comply with:

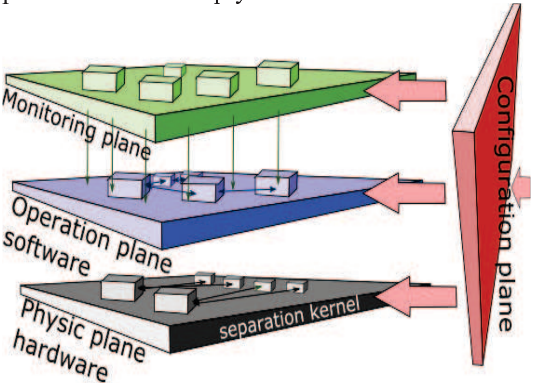

Fig. 4. Planes of MILS implementation, Physical plane (Hardware), Operation plane (Software), Monitoring plane (Security procedures) and Configuration plane (Configuration file) (CITADEL 2016 and certMILS 2017).

- 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.

The adaption plane is sometimes present in the planes of MILS implementation, Figure 4. The adaption hold position on the right side to the configuration plane, which it affects. The way to implement the dynamic adaptability in the MILS without compromise of its security is the subject of an invention. For example, the projects (CITADEL 2016) and (certMILS 2017) deal with it in the European space; for more details see Chapter 4.

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 1981) 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. The system integrator is than only one, who has the access to the whole 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 Praha subway.

4.1 *Metro / Subway*

The MILS Community addresses the development of the MILS approaches and its implementation into the protection of European infrastructures (MILS Community 2019). The MILS Community brings together the European technology companies and Academia, representatives of cyber security science from different areas.

The MILS Community supports various European projects and addresses through them the challenges that arise in the application and development of new technologies.

The EU projects deal with compatibility of standards such as (IEC / ISA 62443 2018), respond to security changes at cyber space and so on. Projects (CITADEL 2016) and (certMILS 2017) use the pilot projects, for example, at railway or smart grids for identification and solving the different issues. Implementation of MILS procedure at the Praha subway is one of such pilot.

The Praha subway is the classic representative of UGTMS (IEC 62290 2018). It does not reach the scale or intensity of transport of the largest European metropoles, however, their three lines transport 1.2 million people per day - 1.6 million journeys per day - 0.4 million transfer between lines (DPP 2015). These numbers document that the Praha subway is at least a critical regional infrastructure. The most occupied route C connects the largest Praha suburbs (middle class inhabitation) and the center of the city (offices and other workplaces) and its disturbance, such as falling the person into the railroad track, leads very fast to overflowing the other transport infrastructures.

The MILS protection is tested in the UGTMS Onboard Subsystem at the Praha subway, at present, Figure 2. The plan is that every metro train will be equipped with the MILS protection. The transfer of information about position and other driving properties, as well as the remote control and communication with the operating center, should, therefore, be protected from cyber-attacks. The MILS principles are applying at gateway between the UGTMS Operation Control Subsystem and the Operation planning (Operation statistics).

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 software), 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 5:

- 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.

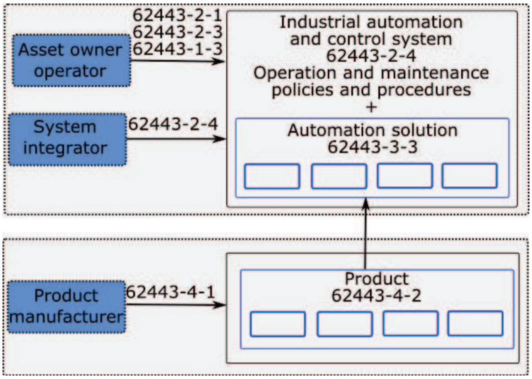

Fig. 5. Three Levels of Responsibility, Manufacturer, Integrator and Operator. Different parts of standard (IEC / ISA 62443 2018) for different phase of application.

The technological setup of MILS called "T-Composition" was designed for the needs of the Praha subway and other pilots (CITADEL 2016) and (certMILS 2017). The T-Composition is described in deliverable 8.1 of projects (CITADEL 2016) and (certMILS 2017). The verification of MILS T-Composition usability in the subway is one of the projects activities.

The next step in projects (CITADEL 2016) and (certMILS 2017) 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, e.g. the UGTMS operator follow (IEC 62290 2018) standard. The standards do not create obligations only for them, but they also create requirements for the previous segment of supply chain, Figure 5.

The area of cyber security is covered by own standards. We mainly describe a standard (IEC / ISA 62443 2018). The standard (IEC / ISA 62443 2018) 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 (CLC / prTS 50701), which is based on the 62443 standard

The cyber security of individual components can be also standardized with the Common Criteria (ISO / IEC 15408 1999). Both mentioned standards (IEC / ISA 62443 2018) and (ISO / IEC 15408 1999) are considered in the European projects (CITADEL 2016) and (certMILS 2017).

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 (CITADEL 2016) and (certMILS 2017). 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 in Figure 6. The project (certMILS 2017) deals with this issue.

Fig. 6. T-composition, box with card, according to (CITADEL 2016 and certMILS 2017).

The system capability of adaptation has several levels. Projects (CITADEL 2016) and (certMILS 2017) work now with three possible way of adaptability: fully self-adaptable system, semi self-adaptable system and manual-adaptable system.

- 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 (CITADEL 2016). The difficulty of fully self-adaptable system creation lies in maintaining the independence of individual security barriers and real-time certification.
- The semi self-adaptable system is easier to setup. The semi-dynamic system has several the "allowable states" of resource distribution (CITADEL 2016). 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.

- 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" (CITADEL 2016) and (certMILS 2017). Verified and certified I-composition has form of box with slot for cards, Figure 6. 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 (Torun 2018). 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 the arise of new harmful cybernetic phenomena demand the application of advanced security procedures. The concept of 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.

Acknowledgement

The results published in the article were created with the support of the European projects "**CITADEL**" ID: 700665, "**certMILS**" ID: 731456 and "**RIRIZIBE**" CZ.02.2.69 / 0.0 / 0.0 / 16-018 / 0002649.

References

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

CITADEL. (2016). *Critical Infrastructure Protection using Adaptive MILS*. EU, Horizon 2020, no. 700665.

Dunn M. I. Wiegert. (2004). *Critical Information Infrastructure Protection*. International IIP Handbook. 405p. ETH. Zurich.

DPP. (2015, 11. December). *Pražské metro v den přepravního průzkumu přepravilo 1 272 143 cestujících*. DPP. Praha. http://www.dpp.cz

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

EU. (2005, 17. November). *Green Paper on European Programme for Critical Infrastructure Protection*. EU COM(2005) 576. Brussel.

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

IEC 62290-3. (2018). *Railway applications – Urban guided transport management and command/control systems*. IEC, draft.

IEC / ISA 62443. (2018). *Security for industrial automation and control systems. International Electrotechnical Commission / International Society of Automation*. IEC and ISA, draft.

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

Kertis, T, Prochazkova. D. (2018). Impacts of lacks in design of control systems in rail transportation. In: *Smart Cities Symposium Prague 2018,* pp. 1-6. ISBN: 978-1-5386-5018-9. IEEE 2018, doi: 10.1109/SCSP.2018.8402668.https://ieeexplore.ieee.org/document/8402676/

MILS Community. (2019, January). *MILS Community*. http://mils.community

Moteff J. C. Copeland, and J. Fischer. (2003). *Critical Infrastructures: What Makes an Infrastructures Critical*? CRS Web, Report for Congress, Order Code RL31556.

Peerenboom J. (2001). *Infrastructure Interdependencies: Overview of Concepts and Terminology*, Argonne National Laboratory, National Science Foundation Workshop, Argonne.

Prochazkova D. (2014). *Challenges connected with critical infrastructure safety*. Lambert Academic Publishing ISBN: 978-3-659-54930-4. 218p.

Rushby J. (1981, December). The Design and Verification of Secure Systems, Eighth ACM Symposium on Operating System Principles, pp. 12-21, Asilomar. (ACM Operating Systems Review, Vol. 15, No. 5).

Torun, A. et al. (2018) Challenges for Air Transport Providers in Czech Republic and Poland. Journal of Advanced Transportation, Vol. 2018, No. 6374592.