Resilience Management Concept for Railways and Metro Cyber-Physical Systems

Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland
jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.074

Abstract: Railways and metros are good examples of cyber-physical systems (CPS). They are safe, efficient, reliable and environmentally friendly. However, being such critical infrastructures turns metro, railway and related intermodal transport operators into attractive targets for cyber and/or physical attacks. SAFETY4RAILS H2020 project of the European Commission delivers methods and systems to increase the safety and resilience of track-based inter-city railway and intra-city metro transportation. Safety engineers have established strategies over decades to remove risks and increase safety that become manifest in railway systems. On the other hand, resilience is a multi-faced and not yet standardized concept so that a number of definitions and assessment methods exist, and until now, resilience management has largely focused on descriptive or diagnostic analytics following an expert judgment-based approach. This paper aims at introducing a conceptualization for resilience management of CPS and to bring the lessons to be learned from earlier projects for SAFETY4RAILS. The approach, earlier studied in the healthcare sector, is based on an integration of the concept of cyber-trust with cybersecurity science and resilience science. The paper proposes five principles that arise from the theory for resilience management processes of CPS: (1) design and implement a security management plan, (2) employ all appropriate security technologies, (3) ensure the adequacy and quality of security information, (4) make sure that situational awareness is always up to date, and (5) design and implement a resilience management plan that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems. In addition, the paper discusses the meaning of these principles in the rail transportation sector. The paper represents the author's views having taken part in SAFTEY4RAILS stakeholder workshops as part of the stakeholder needs and requirements analysis in the early stages of the project.

Keywords: cybersecurity, resilience management, cyber-physical systems, SAFETY4RAILS project, rail transportation systems

1. Introduction

Railway systems and metros are relatively safe, efficient, reliable, comfortable and environmentally friendly mass carriers. Nowadays, they have become even more important from a sustainable point of view since the consequences of the climate change have become more evident. However, being part of the critical infrastructure (CI) makes railway and metro operators and transportation operations that depend on safe railways and tracks attractive targets for cyber and/or physical attacks, which poses a security threat. SAFETY4RAILS H2020 project idea concentrates on a more reliable safety and security of inter-city transport (railways) and intracity transport (metros) that depend on railways and tracks. Until now, past incidents in Europe refer only to cyber-attacks (e.g. WannaCry) or physical attacks (e.g. the bombing attacks to the commuter trains in Madrid in 2004) and not to combined cyber-physical attacks. In the event of a combined cyber-physical attack, the reaction (response and mitigation) will need to take into account several aspects and to be structured to limit the casualties, serious transport disruptions and significant financial and economic losses. In the European Railways Infrastructures, cyber-attacks on industrial control systems increased by more than 600% between 2012 and 2014. Railway specifics, such as electronic components scattered along tracks or trains, a very long life cycle (in excess of 25 years), diversity both of supply chain and technology and other characteristics make this a complex and challenging domain from both cyber and physical security perspective (European Commission, 2020).

Safety engineers have established strategies over decades to remove risks and increase safety that become manifest in railway systems. On the other hand, resilience is a multi-faced and not yet standardized concept so that a number of definitions and assessment methods exist, and until now, resilience management has largely focused on descriptive (i.e., what happened) or diagnostic analytics (i.e., why it did happen) following an expert judgment-based approach (Bellini, et al., 2021). This paper aims at introducing a conceptualization for resilience management of cyber-physical systems (CPS), and discusses the meaning of that in the rail transportation sector. SAFETY4RAILS is well-connected to already existing and funded projects, and the target of this paper is to bring the knowledge and lessons to be learned for SAFETY4RAILS from earlier projects, such as SHAPES (c.f. Rajamäki, 2020) and ECHO (c.f. Rajamäki & Katos, 2020). According to SAFTEY4RAILS stakeholder workshops as part of the stakeholder needs and requirements analysis in the early stages of the project, resilience challenges of railway

and metro systems are quite similar than the ones of, for example, in the healthcare sector, both being critical cyber-physical systems having wide variety of Internet of things (IoT) sensors.

The knowledge base of this study consists of (1) concepts of trust-building in the digital world, (2) resilience science, and (3) cybersecurity science. The paper deduces five principles for cybersecurity and resilience management of cyber-physical systems from the theory. The rest of the paper is structured as follows: Section 2 presents the themes of cyber-trust and cyber resilience. Section 3 deduces a cybersecurity model for a cyber-physical system combining the concept of cyber-trust with cybersecurity science. Section 4 develops the model and presents the resilience management framework and the five principles. Section 5 discusses the results in the rail transportation sector, and Section 6 concludes the paper.

2. Cyber-trust

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cybersecurity is a key enabler for the development and maintenance of trust in the digital world, and the overall goal of cybersecurity is that all operational systems and infrastructures are resilient. According to DIMECC (2017), cybersecurity has the following four themes: (1) security technologies, (2) cognitive situational awareness, (3) security management, and (4) cyber resilience (resilience of operational systems), as shown in Figure 1.

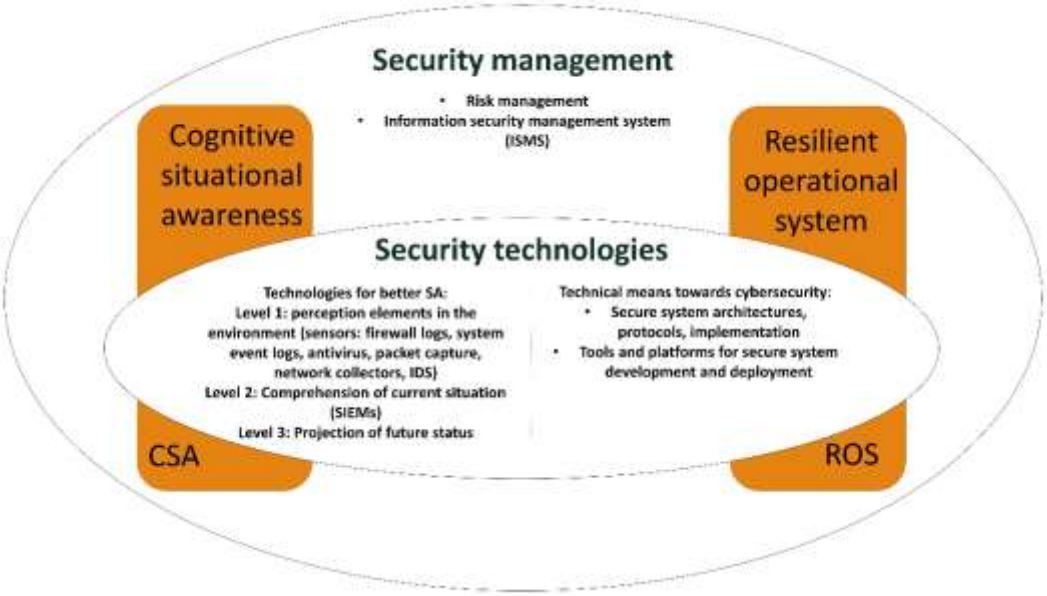


Figure 1: Themes of trust-building in the digital world (modified from DIMECC, 2017)

2.1 Security management

Security management focuses on the continuous management and operation of a system by the documented and systematic establishment of the procedures and processes to achieve confidentiality, integrity, and availability of the organization's information assets that do the preservation. Its focus areas include security policy development and implementation, risk management and information security investment, incentives, and trade-offs. From an organization's point of view, cybersecurity management starts by a risk management procedure. If cybersecurity risks are not prepared for, organizations will face severe disasters over time. Risk management research focuses on how to measure and quantify a state of cybersecurity, including quantifying the value of cybersecurity to an operation, how much of a threat is the operation exposed to, and scoring how mitigations and security controls affect the overall operational risk (Edgar & Manz, 2017). All organizations are becoming more and more dependent on unpredictable cybersecurity risks. Everywhere present computing means that organizations do not know when they are using dependable devices or services and there are chain reactions of unpredictable risks. An information security management system (ISMS) provides controls to protect organizations' most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that the security of the organization is properly managed and meets

regulatory security requirements. An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before a business relationship is established. Now, the most common information technology (IT) security standards are ISO/IEC 27001:2013 Information security management systems requirements, ISO/IEC 27002:2013 Code of practice for information security controls, and ISO/IEC 27005:2018 Information security risk management. Unfortunately, IT security standards are not perfect and they possess potential problems. Usually, guidelines are developed using generic or universal models that may not apply to all organizations. Guidelines based on common, traditional practices take into consideration differences of the organizations and organization-specific security requirements.

2.2 Security technologies

Security technologies include all technical means towards cybersecurity, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Security technologies enable the technical protection of infrastructures, platforms, devices, services, and data. Technical protection starts with secure user identification and authorization that are necessary features in most secure infrastructures, platforms, devices, and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. Well-known security technology standards are ISO/IEC 27033:2015 Network security, ISO/IEC 27034:2015 Application security, and ISO/IEC 27036-1:2014 Information security for supplier relationships.

Technologies that create or transfer security information from the resilient operational system (ROS) to the cognitive situational awareness (CSA) system include sensors that collect the first level of data. Commonly, host- and network-based tools generate logs that are used for CSA. Firewalls, system event logs, antivirus software, packet captures, net flow collectors, and intrusion detection systems are examples of common cyberspace sensors (Edgar & Manz, 2017). Level-two technologies generate information from the data to determine a current situation. Generally, level-two technologies require the bringing together of data and performing some level of analytics. The simplest form is signature-based tools such as antivirus and intrusion detection systems. These systems have encapsulated previous knowledge of detected attacks into signatures that detect and alert when attacks are detected in operational systems. More advanced systems such as security information and event managers (SIEMs) provide infrastructure to bring together datasets from multiple sensors for performing correlations. Vulnerability analysis to determine how many unpatched vulnerabilities exist in a system is also a form of level-two technology (Edgar & Manz, 2017). The third and final level is hard to achieve and only a few examples of effective tools exist. Cyber-threat intelligence provides information on active threat actor methods, techniques, and targets providing some level of predictive information to enable taking pre-emptive security measures (Edgar & Manz, 2017).

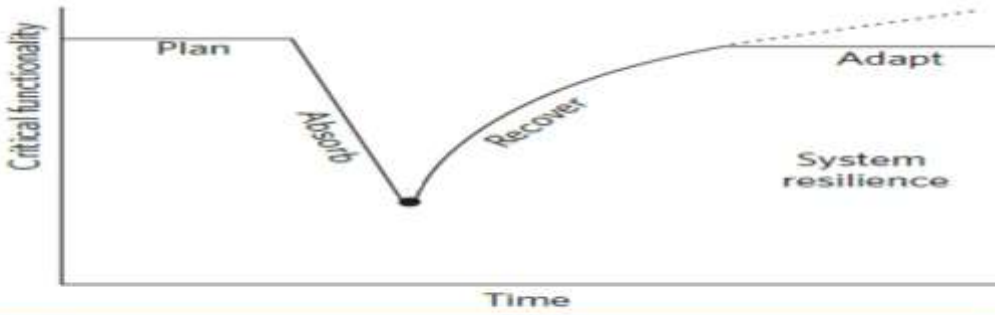
Security technologies are needed also when something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

2.3 Cognitive situational awareness

Cognitive situational awareness is the main prerequisite of cybersecurity and resilience. Without CSA, it is impossible to systematically prevent, identify, and protect the system from cyber incidents and if a cyber-attack happens, to recover from the attack. CSA involves being aware of what is happening around your system to understand how information, events, and how your actions affect the goals and objectives, both now and soon. It also enables the selection of effective and efficient countermeasures, and thus, protects the system from varying threats and attacks (DIMECC, 2017). Eckhart, Ekelhart & Weippl (2019) present a CSA framework for CPS based on digital twins that provides a profound, holistic, and current view on the cyber situation. CSA is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resilience focuses. The most important enablers of CSA are observations, analysis, visualization, governmental cyber-policy, and national and international cooperation. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed.

2.4 Cyber resilience

The concept of cyber resilience is similar than the general definition of resilience in other disciplines (Ligo, Kott & Linkov, 2021). Its one general definition includes four abilities: plan or prepare for, absorb, recover from, and adapt to known threats (National Academy of Sciences, 2012). Linkov et al. (2013) combine those abilities with cyber system metrics on four domains (Alberts, 2002), as shown in Figure 2: (1) physical resources and the capabilities and the design of those resources, (2) information and information development about the physical domain, (3) cognitive use of the information and physical domains to make decisions, and (4) the social structure and communication for making cognitive decisions. Cyber resilience of a system can be appreciated only when adequate resilience measures are defined and implemented (Ligo et al., 2021). The process of building resilience is a collective action of public and private stakeholders responding to infrastructure disruptions (Heinimann & Hatsector, 2017).



Domains	Stages of resilient system			
	Plan and prepare for	*Absorb*	*Recover from*	*Adapt to*
Physical	Physical resources and the capabilities and the design of those resources.			
Information	Information and information development about the physical domain.			
Cognitive	Cognitive use of the information and physical domains to make decisions.			
Social	The social structure and communication for making cognitive decisions.			

Figure 2: The cyber resilience matrix (modified from Linkov et al., 2013)

3. Cybersecurity model for a cyber-physical system

3.1 Cybersecurity science

Figure 3 shows three perspectives (domains) of cyberspace: (1) a data or information perspective that comes from the information theory space; (2) a technology perspective that includes the hardware, silicon, and wires, as well as software, operating systems, and network protocols, and (3) a human perspective that acknowledges that the human is as responsible for the dynamics of the system as the data and the technology are (Edgar & Manz, 2017).

Figure 3: Cyberspace at the overlap of data, technology, and human (Edgar & Manz, 2017)

3.2 Integration of cybersecurity science with the concept of cyber-trust

All cyber-physical systems have human, technology, and data domains. Previous Figure 1 shows the themes of a resilient CPS consisting of two sub-systems: CSA and ROS. Both of these sub-systems have human (social), technological (physical), and data (information) domains as illustrated in Figure 4. Security management, security technologies, and security information connect these sub-systems together. Security management covers the human and organizational aspects of cybersecurity. Security management also integrates the social layer's operational and cognitive aspects; all organizational and social components should learn from prior events and incidents. Security information is mostly created and/or transferred from ROS to CSA via security technologies. However, the CSA system requires information outside ROS, as shown in the lower part of Figure 4.

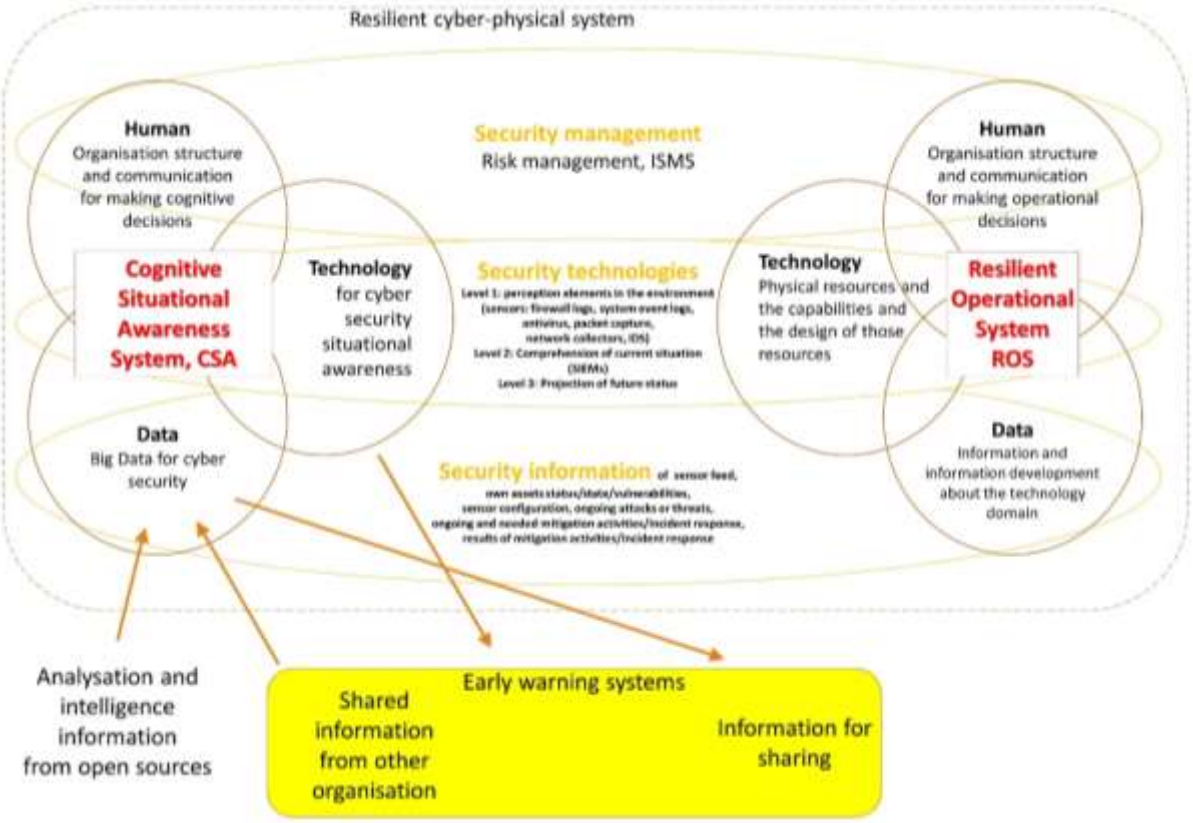


Figure 4: Cybersecurity conceptual model for a cyber-physical system

3.3 Cognitive decision-making process

The technology domain of the CSA system includes the data fusion engine, information interfaces and the human-machine interface (HMI) providing an effective visualization layer (Kokkonen, 2016). Cognitive decision-making functionalities should utilize artificial intelligence and be as automatic as possible without human interaction. However, there should be an operator for controlling the sensors and data fusion algorithms and inputting additional information into the system. The system implements HMI for effective visualization of the status of the cyber domain under control and for the input of information that cannot be entered automatically. Humans are needed for controlling the data fusion process and making decisions. HMI should implement different visualizations for different levels of users: e.g. a technical user who requires detailed technical information, whereas a decision-maker needs different visualization. HMI also implements filters for data allowed for different users.

The cognitive situational awareness system in Figure 4 utilizes the information from the operational system to make decisions that aim towards better resilience. The cognitive decision-making process utilizes cybersecurity sensor information as well as the status information of all the known cyber entities. Information on systems, devices, and sensors with their status and configuration information, but also data from used spare parts of physical devices are relevant information for CSA system (Kokkonen, 2016). In addition, information about the

status of saved data and the status of information flows should be reported. Some of that information can be automatically generated using data interfaces and some should be user-generated by using a HMI.

The cognitive decision-making process requires also information exchange between different stakeholders as well as data from open sources, as shown in the lower part of Figure 4. An early warning systems implement interfaces for cybersecurity information exchange with trusted companions. In addition, CSA needs analysation and intelligence information from open sources. That kind of information includes analysed impact assessment information, Indicator of Compromise (IOC) information, and early-warning information from open-source intelligence using, e.g., social media or Computer Emergency Response Team (CERT) bulletins. Further, required policies and objectives should be input into the system.

4. Resilience management framework

Figure 5 presents the conceptual resilience management framework for a resilient rail transportation cyber-system. It is based on the cybersecurity model of a CPS (Figure 4) and interconnections with other CPSs such as telecommunications and energy. Figure 5 presents six important cybersecurity and resilience themes: resilient operational system, security management, security technology, security information, cognitive situational awareness and resilience management. The goal of the management framework is the resilience of the operational system, and that will be achieved via the five other themes. Next, we will give principles how to deal with these themes.

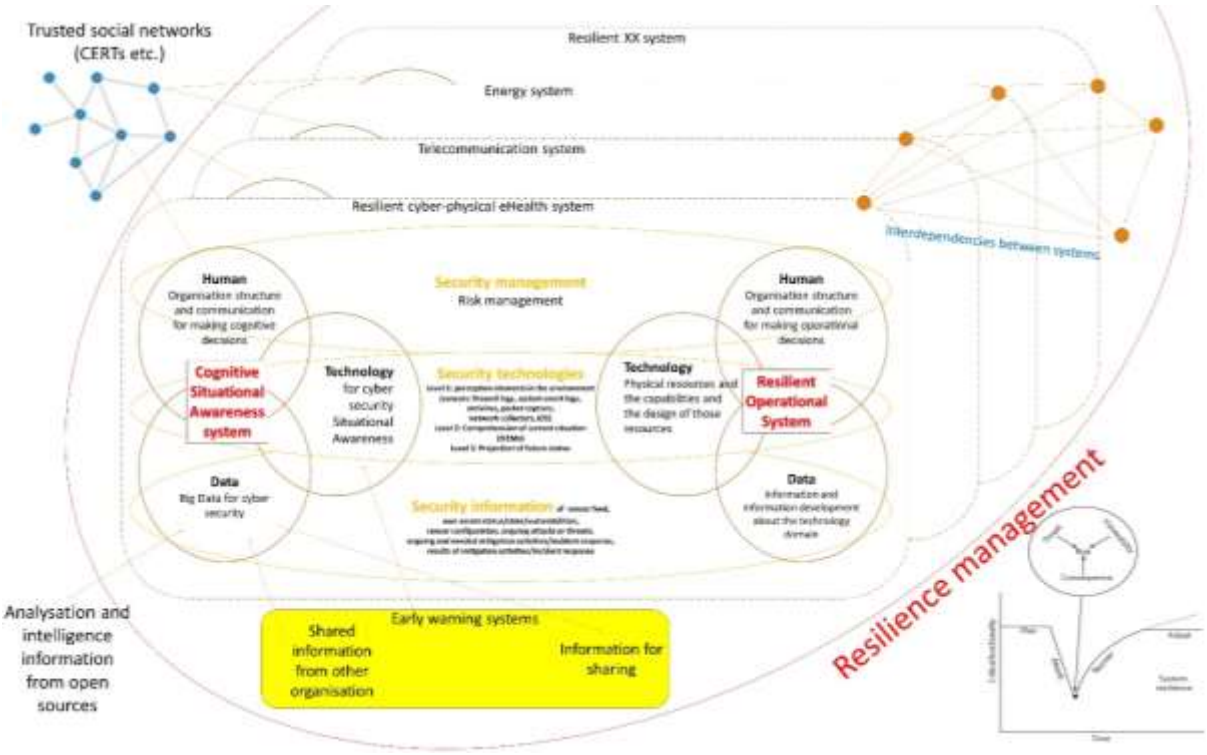


Figure 5: Conceptual resilience management framework for a resilient rail transportation system

Principle 1: Design and implement a security management plan. This will include the following sub-tasks: carry out cyber risk management; identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish a point of contact); educate and train employees about cybersecurity and the organization's security management plan; delegate all assets and services to specific employees; prepare security communications; and establish a cyber-aware culture.

Principle 2: Employ all appropriate security technologies. This will include the following sub-tasks: implement controls/sensors for critical assets; implement controls/sensors for critical services; assess network structure and interconnection to system components and the environment; implement redundancy of critical physical infrastructure; and assess the redundancy of data physically or logically separated from the network.

Principle 3: Ensure the adequacy and quality of security information. This information should be suitability for artificial intelligence and machine learning technologies. This guideline will include the following sub-tasks: categorize assets and services based on the sensitivity; document certifications, qualifications, and pedigree of critical hardware and/or software providers; prepare plans for storage and containment of classified or sensitive information; and identify internal system dependencies.

Principle 4: Make sure that situational awareness is always up to date. This cognitive domain will include the following sub-tasks: anticipate and plan for system states and events; understand the performance trade-offs of organizational goals; set up scenario-based cyber war gaming; utilize applicable plans for system state when available; and utilize artificial intelligence or prepare to utilize it for responding to threats with greater confidence and speed.

Principle 5: Design and implement a resilience management plan that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems. This will include the following sub-tasks: consider how all previous requirements can be utilized throughout the four event-management cycles; identify external system dependencies (i.e., telecommunication, energy, built environment), and plan the coordination framework with these systems (you have no control for these systems); and educate and train employees about resilience and the organization's resilience plan.

5. Resilience management of railway and metro systems

The complexity of railway and metro systems combined with existing and emerging cyber-physical threats constrains administrations to consider smart technologies and related huge amounts of data generated as a means to take timely and informed decisions. Therefore, the measures to be put in place for the protection, safeguard and resilience of their infrastructure need to be continuously tested and improved, without forgetting the security of railway workers and passengers (European Commission, 2020). Transportation systems need to be prepared for both expected and unexpected situations and the possibility to mitigate the effect of the uncertainty behind the causes of disruptions through the analysis of all the possible data generated by smart cities open new possibility for resilience operationalization (Bellini, et al., 2021).

5.1 Security management plan

In Europe, the legal background for security management of railway systems comes from the NIS Directive 2016/1148. Its main topics include (1) national capabilities; Member States must have a national Computer Security Incident Response Team (CSIRT), perform cyber exercises, etc., (2) cross border collaboration; cross border collaboration between EU countries, (3) supervision of critical sectors (energy, transport, water, health, digital infrastructure and finance sector); Operators of Essential Services (OES), and critical digital service providers. According to NIS, railway undertakings and infrastructure managers are OES. On the other hand, metros are not included, but it would be convenient to apply NIS to them as well. NIS does not enforce detailed requirements for OES, but the NIS Coordination Group defines the security measures for OES. ENISA maps out the security measures for the railway sector from the most spread standards (ISO 27001 and IEC 62443 Industrial Network and System Security). The proposal of NIS2 Directive has been issued; it has a more detailed framework with respect to NIS, but still it gives no detailed requirements nor mandatory standards.

The security management plan will enrich past natural, cyber and physical events and serve as a basis for identifying the challenges and the respective requirements. The plan will analyse threats, attack vectors and vulnerabilities of the rail-dependant infrastructures in terms of business criticality and support the definition of risk mitigation strategies at planning, protection and prevention level. The mitigation strategies may be either proactive, e.g. resulting in building more robust railway infrastructures and forecasting of events; or reactive, e.g. informing simultaneously the agencies responsible to tackle the threats and its consequences (e.g. railway and metro operators, transportation stakeholders, law enforcement authorities, medical assistance, fire alarms, etc.). In addition, crisis mitigation strategies will be provided, e.g. arranging alternative transportation, rerouting and micro-response activities on different levels, e.g. single stations or at individual passenger level.

5.2 Security technologies of railway and metro systems

Development and design of a resilient cyber-physical rail transportation system starts with the overall system architecture, which describes all systems and environments and then get the systems to work together in a

controlled way with cybersecurity and information security in mind. In addition, all relevant cybersecurity technologies discussed in the section 2.2 should be applied. Common standardised physical security technologies relevant for railway and metro systems include, e.g.:

- CENELEC EN 50132 7:2012 CCTV surveillance systems for use in security applications
- DD CLC/TS 50131 7:2010 Alarm systems Intrusion and hold up systems. Application guidelines
- OASIS Common Alerting Protocol (CAP)
- Open Network Video Interface Forum (ONVIF) Core.

5.3 Security information related to railway and metro systems

The data applied in the CSA system includes all the data generated within the transportation system; operational status information, sensor data from physical railway network (e.g. CCTV, gas sensors in metro systems, metal detectors) and sensor data from railway IT infrastructure. Bellini, et al. (2021) present a concept how to utilize urban big multimedia data (U-BMD) for operationalising the resilience of transport systems. U-BMD is very diverse in terms of volume, velocity, and variety, as well as in terms of accessibility and license for reuse. Useful U-BMD for CSA includes geographic information system maps (seismic risk maps, hydrological risk maps, services, descriptors of structures such as schools, hospitals, infrastructures, etc.), social media streams, IoT-data streams, CCTV streams, etc.

5.4 Cognitive situational awareness of railway and metro systems

The focus of SAFETY4RAILS is to develop a flexible multi-lingual SAFETY4RAILS Information System (S4RIS) that can be combined with already existing safety and security control systems of the railway operators. This combination will be an AI-oriented detection, mitigation, prevention, forecasting and fast response CSA system. S4RIS will analyse the impact of proposed strategies in both the prevention and response phases. S4RIS will combine simulation and monitoring capabilities as well as visualisation means to prevent, forecast, detect, defuse, respond and mitigate the impact of cyber and physical threats in a holistic methodological and operational approach resulting in a collaboration between cyber-physical security technologies and actors. The simulation capabilities will simulate the current practices of the considered railway infrastructure, identify potential vulnerabilities and cascading effects due to various incidents, test/stress the results of the designed security measures and propose alternatives for handling the critical points of the infrastructure.

5.5 Resilience management plan

Trains and metros play a crucial role for both inter-city and intra-city transportation as both may have cascading effects influencing the effectiveness of mobility of people not only between cities but also within cities. Resilience is not about the performance of individual railway or metro system elements but rather the emerging behaviour associated to intra and inter system interactions. Nowadays our societies provide a wide range of transportation and other services available to citizens in real-time, regardless of location or time. This also means that almost all systems are interconnected through different integration platforms. There are also many federations between information systems. Before we can design resilient cyber-physical systems, we need to look at different scenarios, use cases, and requirements. In addition, large cross-system integrations and federations in ICT systems mean that there is a lot of interdependence between different ICT systems and between organizations and stakeholders. We need to identify dependencies on all internal and external systems and data flows, and only then, we can design and implement resilience in cyber-physical systems.

SAFETY4RAILS aims at addressing cyber-physical railway threats resulting in business disruptions, causing time-consuming and even fatal consequences through innovative solutions consisting not only of rerouting approaches but also of mobile infrastructure components like mobile stations, mobile bridges or mobile signal systems in order to react more efficiently and to save time and recovery costs. On the other hand, Bellini, et al., 2021 propose the following multi-steps approach for the resilience management of urban transport systems:

- 1. Understanding the transportation system and utilizing the Functional Resonance Accident Model (FRAM) in managing critical events
- 2. Understanding what information is needed to take decisions
- 3. Selecting/producing U-BDM: methodologies to be adopted to select and collect the data needed

- 4. U-BDM collection and integration: data collection
- 5. U-BDM sense making, how the data is transformed into information
- 6. Knowledge driven decision: how the information is transformed into knowledge.

6. Conclusions

This paper offers a conceptual resilience management framework for resilient cyber-physical systems and presents five principles for resilience management. The first principle 'design and implement a security management plan' is based on the long security management tradition considering that we are safe and we must plan how to protect ourselves from the outside coming threats by risk management. The second principle 'employ all appropriate security technologies' continues this tradition giving tools for protection. The third principle 'ensure the adequacy and quality of security information' means that you need data for understanding your system, understanding informational needs for decision making and selecting/producing data needed to support such decisions. The fourth principle 'make sure that situational awareness is always up to date' means that you should transform above-mentioned data into knowledge that supports decision-making, and the future evolution of the CSA system may be represented by the digital twin (c.f. Bellini, et al., 2021). The last principle 'design and implement a resilience management plan that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems' goes beyond risk-based security management recognizing that no one can control and protect the whole system of infrastructures when grave incidents, such as the COVID-19 pandemic, happens in any case. Then, you should know your most critical assets and do everything to keep them in the life. These five principles above are deduced from the theory, and so, they are intended for permanent use. On the other hand, the descriptions of the principles and the discussion about them in the case of rail transport systems are based on the state of the art, and these descriptions and discussion will become out-of-date with the progress of technology.

Acknowledgements

Acknowledgement is paid to SAFETY4RAILS Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532. The sole responsibility for the content of this paper lies with the author. It does not necessarily reflect the opinion of the European Commission or of the full project. The European Commission is not responsible for any use that may be made of the information contained therein.

References

Alberts, D. (2002). Information age transformation, getting to a 21st century military. DOD Command and Control Research Program.

Bellini, E. et al., 2021. An IoE and Big Multimedia Data Approach for Urban Transport System Resilience Management in Smart Cities. *Sensors*, 21(435), pp. 1-34.

DIMECC. (2017). The Finnish Cyber-trust Program 2015–2017. Helsinki: DIMECC.

M. Eckhart, A. Ekelhart and E. Weippl, "Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins," 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 2019, pp. 1222-1225, doi: 10.1109/ETFA.2019.8869197.

Edgar, T., & Manz, D. (2017). *Research methods for cybersecurity*. Cambridge: Syngress.

European Commission. (2020). Grant agreement number 883532 – SAFETY4RAILS.

Heinimann, H., & Hatsector, K. (2017). Infrastructure Resilience Assessment, Management and Governance – State and Perspectives. In I. Linkov, J.M. Palma-Oliveira (eds.), *Resilience and Risk*, NATO Science for Peace and Security Series C: Environmental Security (pp. 147-187). Cham: Springer.

Kokkonen, T. (2016). Anomaly-Based Online Intrusion Detection System as a Sensor for Cybersecurity Situational Awareness System. Jyväskylä studies in computing 251. University of Jyväskylä.

Ligo, A., Kott, A. & Linkov, I. (2021) How to Measure Cyber Resilience of an Autonomous Agent: Approaches and Challenges, In AICA 2021, 1st International Conference on Autonomous Intelligent Cyber-defence Agents. Paris, France.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., & Kott, J. (2013). Resilience metrics for cyber systems. *Environ Syst Decis*.

National Academy of Sciences. (2012). Disaster resilience: a national imperative.

Rajamäki, J., 2020. Resilience Management Framework for Critical Information Infrastructure: Designing the Level of Trust that Encourages the Exchange of Health Data. *Information & Security*, 47(1), pp. 91-108.

Rajamäki, J. & Katos, V., 2020. Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. *Information & Security*, 46(2), pp. 198-214.