# Gaps in Asset Management Systems to Integrate Railway Companies' Resilience

**Jyri Rajamäki[1], Jari Savolainen[1], Rauno Pirinen[1] and Eduardo Villamor Medina[2]**
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]ETRA, Valencia, Spain

jyri.rajamaki@laurea.fi

**Abstract:** Railways and metros are safe, efficient, reliable, and environmentally friendly mass carriers. They are critical cyber-physical systems (CPS) that are attractive targets for cyber and/or physical attacks. SAFETY4RAILS project delivers methods and systems to increase the safety and resilience of track-based inter-city railway and intra-city metro transportation. Asset management plays a fundamental role in resilience management. This study analyses the gaps in asset management systems of rail infrastructure. The objective of the study is to understand the weaknesses and vulnerabilities in an asset management system that impacts resilience. The form of triangulation fashion was used for the analysis of consequences for each threat event. The research conducted included: a systematic literature review; a multiple case study review; and an analysis. The strength of asset inventory, condition inspection methods and decision-making scenarios were analysed, and as an expanded part of this analysis, mitigation actions linked to the vulnerabilities were identified. The study implies that asset management systems are most important in resilience management's response and recovery phases where the largest sudden economic implications can take place. The results of the gap analysis could be used to provide policy recommendations and standardisation efforts.

**Keywords:** Asset management, Cybersecurity, Resilience management, Cyber-physical systems, SAFETY4RAILS project, Rail transportation systems

## 1. Introduction

The EU funded SAFETY4RAILS project delivers methods and systems to increase the safety and recovery of track-based inter-city railway and intra-city metro transportation (SAFETY4RAILS, 2022). It develops a resilience-oriented framework covering the identification, protection, detection, response, and recovery of rail and metro infrastructure against cyber, physical, and combined cyber-physical threats. According to Bellini, et al. (2021), resilience is a multi-faced non-standardized concept having many different definitions and assessment methods exist, and resilience management has traditionally focused on descriptive (i.e., what happened) or diagnostic analytics (i.e., why it did happen) following an expert judgment-based approach.

Individuals and organisations have been managing assets for a long time; however, the term "asset management" started to be used more recently, since the 1980s, when private and public organisations in various sectors and industries initiated policies and procedures related to this topic. Since then, "asset management" has become a relatively new discipline, including such as knowledge, principles, scientific and practical approaches, standards and models, which have been developed across the world. It is now widely recognised that asset management is much more than an extension of maintenance practices, as the new discipline encompasses broader views than those of traditional engineering. Asset management has been gradually adopted and used by a broad range of sectors, as a systematic approach to the governance and realisation of value from the things that a group or entity is responsible for, over their whole life cycle (Zhou, et al., 2019). Therefore, it is now applied to both tangible assets (physical objects such as buildings or equipment) and intangible assets (such as human capital, intellectual property, and financial assets). Due to the different approaches in specific industries and businesses, there are various definitions and qualifying descriptors for asset management, however, these do not change the consistent core, regardless of the type and nature of the assets to be managed.

This paper comprises results obtained in the analysis of gaps in asset management systems to integrate resilience in the railway and metro context. A combination of literature and case study review is conducted with triangulation. The objective of the paper is to understand the weaknesses and vulnerabilities in an asset management system that impacts to the resilience. Such analysis supported the assessment of consequences for each threat event. The strength of asset inventory, condition inspection methods, and decision-making scenarios were analysed. As part of this analysis, mitigation actions linked to the vulnerabilities were identified.

The rest of the paper organised as follows: After this introduction, Section 2 presents the applied research methodology and research design. Section 3 deals with the literature review and discusses vulnerabilities for

improving resilience. Section 4 describes the multi-case study, the selected cases and presents its results divided into intentional and unintentional incidents. Finally, Section 5 concludes the paper.

## 2. Methodology

This study is addressed to understanding of weaknesses and vulnerabilities in an asset management system in a resilience management. Because the objective of the study is to understand a phenomenon, a combination of a literature review and a case study is the best option. Literature review is a summary, analysis, and evaluation of all the existing research on a well-formulated and specific question. Case studies are a way to explore a real-world phenomenon in-depth, illustrate a point, discuss the implications or meaning of an event, or compare the experiences of different individuals (Yin, 2010).

A multi-case study analysis is performed to extend existing knowledge in the research literature about gaps in asset management systems. According to Yin (2009), a case study analysis relies on multiple sources of evidence with data needing to converge in a triangulation fashion, and it benefits from the prior development of theoretical propositions to guide data collection and analysis. Here, the term "triangulation fashion" refers to the usage of multiple sources of evidence such as 1) multiple data sources; 2) among different evaluators as investigators (Patton, 1990; Miles & Huberman, 1994; Nunamaker, 2010).

The addressed form of research question during the study was "how can a vulnerability or weakness be understood in the domain of a typical infrastructure asset management system and in considering life cycle vulnerabilities under extreme events". The Unit of Analysis (UoA) was collectively discussed and considered in international meetings (n=2 work package meetings) and the most feasible and selected was as "a gap" or "a vulnerability" or as "a weakness". The paper provides the results of the gap analysis with the identification of weaknesses in asset management systems, referred to as "vulnerabilities", and improvement measures to integrate resilience, referred to the mitigation adversary tactics and techniques based on real-world observations.

The triangulation fashion is used in the analysis in the following form: 1) data sources as data triangulation (multiple literature references and case-study references); and 2) among different evaluators as investigator triangulation (n=4, researchers). The process included qualitative data from the literature and cases, which are analysed in terms of categorisation as data reduction, displays, and drawings of data (Miles & Huberman, 1994; Robson, 2002). The used form of analysis addresses to data reduction as the process of selecting, focusing, simplifying, and abstracting the used research data collection (literature and cases). The design of extended analysis is described in Figure 1.

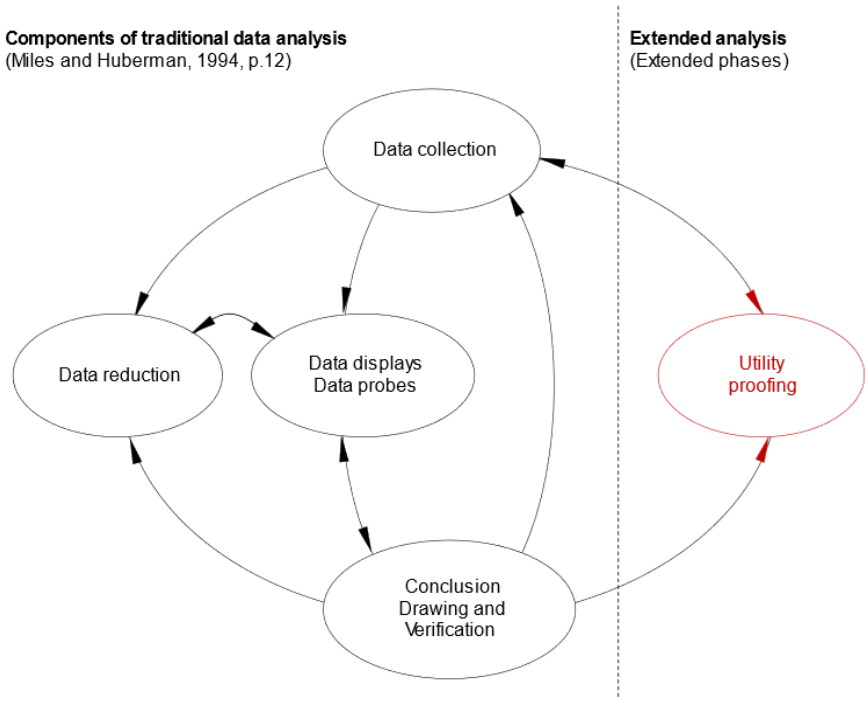


**Figure 1: Research design (Miles & Huberman. 1994)**

## 3. Literature review

The literature review was performed following the research design explained in figure 1; the Unit of Analysis (UoA) in the literature review was as “a gap” or “a vulnerability” or as “a weakness” related to the vulnerabilities and possible mitigation tactics from the perspective of asset management systems in rail infrastructure. Feasible literature was first selected as addressed reference accepted or rejected, and then selected literature was reviewed. The earlier referenced literature in SAFETY4RAILS was verified for avoiding duplicative analysis. The form of performed literature review setting was considered as including a combination of a well-conducted literature review with metadata-based analysis. The attributes of selection criteria in the literature review included: 1) metadata analysis; 2) verification of keywords; 3) existence of Unit of Analysis as a sample of evidence in the addressed literature; 4) independent three reviewers’ (n=3) collective consideration and analysis (n=5 meetings); and 5) international consortium work package meetings were arranged to ensure data quality and accuracy of relevant literature and avoiding duplicative literature (n=6 meetings). The research attributes included: research question (n=1), forming criteria (n=3); search strategy as metadata and content analysis including such functionalities as searching of title, abstract review, federated metadata search, full-text screening activities, extracting data, quality assessment, avoiding double data checking, using of searching of tactics and techniques databases for comparison, deliverable writing, and international consortium review.

### 3.1 Results

This section includes gathered findings of the completed literature review, including descriptions of the most frequently found literature references related to weakness or vulnerability as a sample of evidence in the literature regarding rail infrastructure asset management systems. The theoretical view of the selected analysis design is on a well-known strategic-tactical-operational-technical line, here namely functional-operative-practical-quality-human categories of attributes addressed to a typical asset management system.

From the top 40 research literature references, such as literature references (n=32) and resilience literature (n=8), the number was reduced to 6 for the third detailed extended analysis phase. Each of the 40 references was carefully reviewed taking into consideration the attributes defined in the research setting. Table 1 lists the most selected articles.

**Table 1: Sample Articles**

| Authors | Article title | Theme studied | Sector |
|---|---|---|---|
| Emanuele Bellini, Pierfrancesco Bellini, Daniele Cenni, Paolo Nesi, Gianni Pantaleo, Irene Paoli and Michela Paolucci | An IoE and Big Multimedia Data Approach for Urban Transport System Resilience Management in Smart Cities | Resilience management | Urban Transport |
| DIMECC Oy | The Finnish Cyber-Trust Program 2015–2017 | Security Management | Cybersecurity |
| Hong, Wei-Ting, Clifton, Geoffrey, Nelson, John D | Rail transport system vulnerability analysis and policy implementation: Past progress and future directions | Resilience management | Rail infrastructures |
| Noritaka Matsumoto, Junya Fujita, Hiromichi Endoh, Tsutomu Yamada, Kenji Sawada and Osamu Kaneko | Asset Management Method of Industrial IoT Systems for Cyber-Security Countermeasures | Asset management | Industries |
| Rajamäki, J. | Resilience Management Concept for Railways and Metro Cyber-Physical Systems | Resilience management | Rail infrastructures |
| Junwei Wang; Raja R. Muddada; Hongfeng Wang; Jinliang Ding; Yingzi Lin; Changli Li | Toward a Resilient Holistic Supply Chain Network System: Concept, Review and Future Direction | Resilience management | Supply chain (rail infrastructure included) |

#### 3.2 Vulnerabilities for improving resilience

In this Section, the contribution of the literature research is addressed to the improvements of maturity aspects of a typical asset management system in the rail domain related to progress of resilience. While risk management considers all efforts to prevent or absorb threats before they occur, resilience is focusing more on recovery from losses after a shock has occurred as the figure below presents. This means that the main target of risk management is to protect the system from hazards outside, while the focus on resilience management is

to improve the functionality of the own system regardless of what threat it might face. In this way, resilience management covers unknown hazards that cannot be considered in risk analysis.

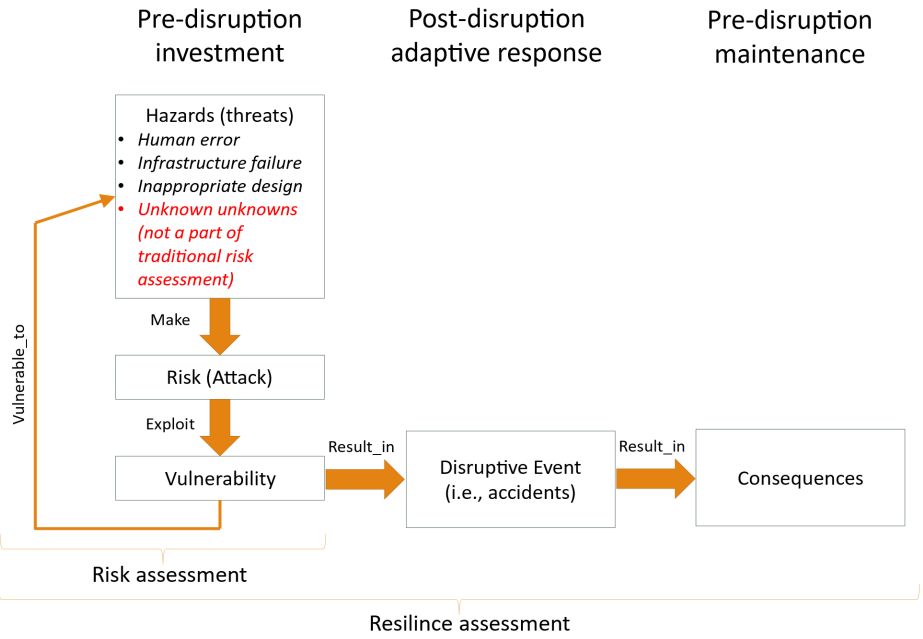


**Figure 2: The relationship between hazards, risk, vulnerability, accident and consequences (adapted from Hong, Clifton & Nelson, 2022)**

Previous studies usually interpret the concept of vulnerability and resilience as two sides of the same coin as shown in Figure 3. Rapidity is used to describe the time that a system requires to return to a state of normal function after a severe perturbation, such as after an intentional terrorist attack (Wang et al., 2016). The goal of resilience engineering is to improve resilience by reducing the drop in capability and speeding up recovery, and the goal of resilience management is also to learn from unwanted events and thus improve the system's capability as shown in Figure 4. Good resilience management can increase the capability of a system after a disruptive event (e.g., improved working methods after the Covid-19 pandemic).

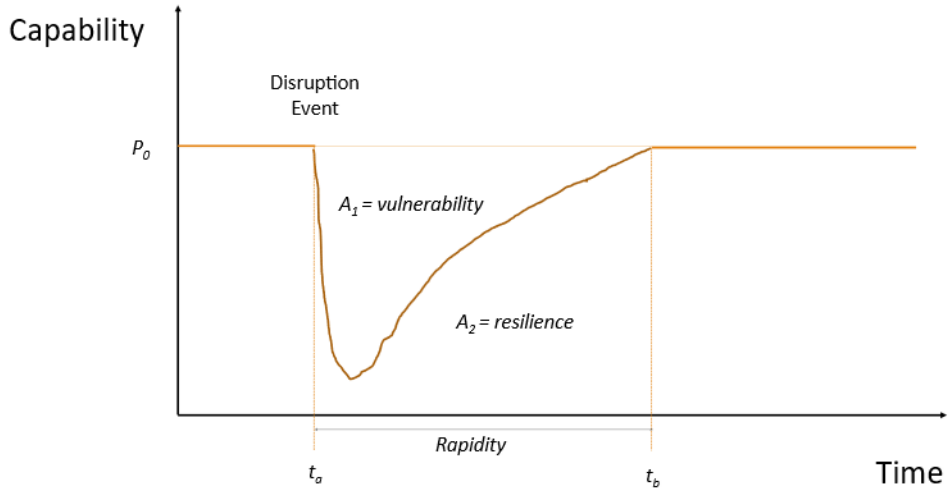


**Figure 3: Concepts of vulnerability and resilience**

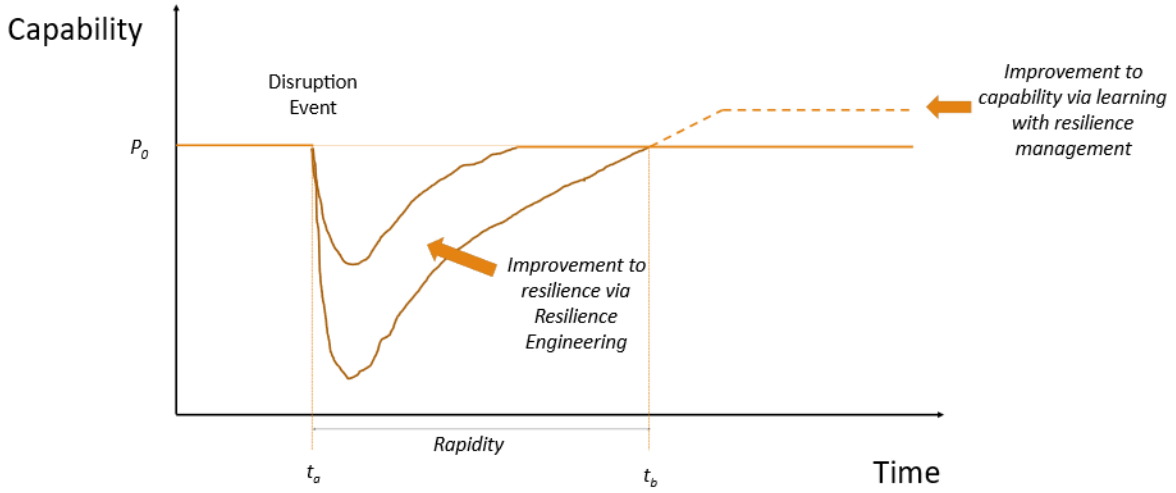


**Figure 4: Resilience engineering and resilience management**

The connotation of vulnerability in the context of transportation links to the reduction of capacity caused by a disruptive event, which can be estimated by any quantifiable metrics, such as total delay to passengers or the number of canceled trains. Resilience challenges of railway and metro systems are quite similar to the ones of, for example, in the healthcare sector, both being critical cyber-physical systems in which IT (information technology) and OT (operational technology) are integrated and they have a wide variety of Internet of things (IoT) sensors (Rajamäki, 2021). The appropriate asset management of IoT systems is the key to creating resilient systems. However, the timely and coherent asset management methods used for conventional IT systems are difficult to be implemented for IoT systems, because these systems are composed of various network protocols, various devices, and open technologies (Matsumoto, etc, 2021). Also, the analysis of the vulnerability of railway disruptions is seldom reviewed, and the connection between theory and policy implementation in this context is not dealt with in-depth.

The vulnerabilities identified in this literature review were checked against the ones already identified in the project. To sum up, the following vulnerabilities were found:

- Reconnaissance – Lack of monitoring of asset information and status
- Discovery of resources – Data about available resources listed in plain text
- Decision-making – Lack of quality data for decision-making (planning and control)
- Compliance Lack of compliance with asset management regulation

## 4. Multiple Case Study Review

The analysis of past failures is an important step toward defining the requirements of the assets management system for railway companies. The analysis will help to avoid the reproduction of known events, already experienced by railways and metro sectors, by being better prepared to face them. In this section, 94 cases were defined collecting information on recurrent, on-going and emerging threats targeting railways and metros to support the development of solutions and enable operators to enhance their resilience capabilities.

Information of the case studies was based on open sources, articles available from internet public pages. In the articles the descriptions of incidents have mainly focused on what has happened and what have been the consequences without going deeply into the reasons which have caused the incident. The press releases also do not talk about the success of the recovery phase e.g., whether the operational capability has been restored within a reasonable time. Therefore, in most of the cases the analysis of the gaps in asset management system is at most indicative.

This case study analysis was conducted in three phases:

1. Building up a data collection of the information available from internet open sources, allowing possible further studies
2. Estimation of the assets targeted in each of the cases based on expert knowledge
3. Assessment of the possible gaps in asset management system

## 4.1 Results

The results of the analyses are presented in Table 2 and Table 3. In the tables, the columns below the headline "Asset" describes in which asset the incidents have been targeted and in how many cases. Columns below the headline "Asset management functionality" describes in which functions the deficiencies have been assumed to exist and in how many cases.

### *4.1.1 Unintentional incidents*

In Table 2, the unintentional incidents have been categorised based on the threat origin (natural/human) and the threat event (natural disaster, natural/environmental disaster, human failure, technical failure, environmental disaster and natural/environmental disaster).

**Table 2: Unintentional incidents**

| UNINTENTIONAL | | Asset | | | | | | Asset management functionality | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Station | | Track line | | Passenger rolling stock | Other | Asset status tracking | Maintenance management | Not classifiable |
| | Cases | Overall roof | Station facilities | Fastening system | Rails geometry | Wagon | | | | |
| NATURAL | 12 | | 3 | | 5 | 2 | 2 | 6 | 2 | 4 |
| Natural disaster | 2 | | 1 | | | 1 | | 1 | | 1 |
| Natural/Environmental disaster | 10 | | 2 | | 5 | 1 | 2 | 5 | 2 | 3 |
| HUMAN | 11 | 1 | | 4 | | 4 | 2 | | 3 | 7 |
| Human failure | 3 | | | | | 2 | 1 | | | 3 |
| Technical failure | 6 | 1 | | 4 | | | 1 | 1 | 3 | 2 |
| Environmental disaster | 1 | | | | | 1 | | | | 1 |
| Natural/Environmental disaster | 1 | | | | | 1 | | | | 1 |

Natural disasters have mainly focused on solid structures like track lines and station structures. The public articles do not tell if it would have been possible to be prepared against such disasters e.g., with structural protection or if the existing protective measures have worked properly. Pre-maintenance measures for track lines might have prevented accidents in some of the cases if the problem areas could have been identified in time.

In the unintentional incidents where human has been involved the question has been of technical failure or what a person has done or left undone. For the technical failures, the gap might have been in the asset status i.e., if the asset has fulfilled the set requirements in the very beginning or if the requirements have been correctly set. The gap could have been also in maintenance if the pre-maintenance measures have not been conducted in a timely manner or in an acceptable manner.

Not classifiable cases mentioned in the table are related to such incidents which could have not been able to predict with any available asset like sudden natural landslides or human unprofessional and neglectful behaviour.

## 4.2 Intentional incidents

In Table 3, the intentional incidents have been categorised based on the failure type (cyber/physical/cyber-physical) and the threat event (cyber-attack, physical attack, physical attack on infrastructure, physical attack on persons and technical failure).

**Table 3: Intentional incidents**

| INTENTIONAL | | Asset | | | | | | | | | | | | | Asset management functionality | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Station | | | | | Track line | | | Control centre | | Passenger rolling stock | | Other | | | |
| | Cases | Electrical and lighting system | Overpass/Underpass | Station facilities | Ticketing system | Signalling | Fastening system | Overhead line | Communication system | Monito ring software | Traffic control software | Wagon | Info board | | Asset status tracking | IT asset management | Not classifiable |
| CYBER | 22 | | | | 15 | | | | | | 2 | | 2 | 3 | | 22 | |
| Cyber attack | 22 | | | | 15 | | | | | | 2 | | 2 | 3 | | 22 | |
| PHYSICAL | 37 | | 1 | 3 | | | 1 | 4 | 2 | | | 22 | | 4 | 7 | | 30 |
| Physical attack | 16 | | | 1 | | | | 3 | 1 | | | 10 | | 1 | 6 | | 10 |
| Physical attack on infrastructure | 17 | | 1 | 2 | | | 1 | 1 | 1 | | | 10 | | 1 | | | 17 |
| Physical attack on persons | 2 | | | | | | | | | | | | | 2 | | | 2 |
| Physical attack on infrastructure and on persons | 1 | | | | | | | | | | | 1 | | | | | 1 |
| Technical failure | 1 | | | | | | | | | | | 1 | | | 1 | | |
| CYBER-PHYSICAL | 12 | 2 | | | 1 | 1 | | 1 | | 1 | 3 | | 1 | 2 | | 10 | 2 |
| Cyber attack | 10 | 1 | | | 1 | 1 | | 1 | | 1 | 3 | | 1 | 1 | | 10 | |
| Physical attack | 1 | | | | | | | | | | | | | 1 | | | 1 |
| Technical failure | 1 | 1 | | | | | | | | | | | | | | | 1 |

In most cases, the target for cyber-attacks has been passengers' private data (Station/Ticketing system). The gap in asset management system has assumingly been in IT asset management as no evidence has been presented of failed systems functioning. Passengers' behaviour in securing their own privacy has also caused leaks in the systems as people too often tend to use the same passwords in different applications.

Physical attacks have been most common against wagons in passenger rolling stock. Means used against wagons have been obstacles on the track lines and explosives placed on the wagons in advance or carried by suicide bombers. A gap in asset management is in asset status tracking and insufficient surveillance capability (not classifiable cases in Table 3), both in technical means and in surveillance conducted by professional security personnel. Insufficient surveillance capability causes inadequate situational awareness.

Cyber-physical activities have been targeted mainly against railway/metro companies' C3 systems. As in the purely cyber-related cases studied in this analysis the challenges are in IT asset management.

In the cases that have been analysed, the cyber-physical actions have not been combined attacks, but the goal of a cyber-attack has been to make something physical to happen or vice versa the physical attack or other physical incident has caused malfunctioning in the IT systems.

### 4.3 Vulnerabilities identified for improving resilience

Based on the cases studied in this analysis, the biggest challenges in the current asset management system are the limited situational awareness and the lack of asset status tracking, surveillance in different information systems to reveal unauthorised intrusion attempts as well as surveillance in the real world by technical devices and physical surveillance conducted by professional security personnel to reveal physical threats. These observations are consistent with literature research, according to which situational awareness is an absolute prerequisite for resilience.

The timely and coherent asset management methods used for conventional IT systems are difficult to be implemented for rail transportation systems because these systems are composed of various network protocols, various devices, and also open IoT technologies.

## 5. Conclusions

The paper studies weaknesses and vulnerabilities in asset management systems that impact the dimension of cyber resilience. It supports the assessment of consequences for each threat event including a systematic literature review and a multiple case studies review. The strength of asset inventory, condition inspection methods and decision-making scenarios are analysed.

Asset management plays a fundamental role in all different phases of the resilience cycle from preparation to recovery including debriefs and audits. In the identification phase, such systems enable the identification of assets relevant to the resilience framework and in the protection phase, the management of maintenance is crucial. However, arguably, asset management systems are most important in resilience management's response and recovery phases where the largest sudden economic implications can take place. An assessment of the existing gaps in asset management systems used in these critical infrastructures will provide the necessary understanding to enforce technical and non-technical measures to integrate resilience.

In further studies with larger research material, resilience costs and time used to recover could be explored to find out how the available assets and resources have been utilised to restore the service after an accident or a criminal incident.

The paper studies existing gaps in railway asset management systems that hinder resilience integration within these organisations. Main gaps identified included vulnerabilities such as the lack of a unified system for the management both IT and OT assets, integration of the system across the various departments in the organisation, lack of revision prioritisation on key assets and manual monitoring of key assets. As part of this work, relevant mitigations actions to these vulnerabilities were also identified. The results of the gap analysis could be used to provide policy recommendations and standardisation needs. The materialisation of these gaps into a new regulatory/standardisation framework for asset management systems would provide the required mechanisms to overcome such gaps.

## 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

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.

Hong, W.-T., Clifton, G., & Nelson, J. (2022). Rail transport system vulnerability analysis and policy implementation: Past progress and future directions. Transport Policy. https://doi.org/10.1016/j.tranpol.2022.02.004

Matsumoto, N., Fujita, J., Endoh, H., Yamada, T., Sawada, K. & Kaneko, O. (2021). Asset Management Method of Industrial IoT Systems for Cyber-Security Countermeasures. Information 12(460). https://doi.org/10.3390/info12110460

Miles, M. B. & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Thousand Oaks: Sage Publications.

Nunamaker, J. F. (2010). Interview with Jay F. Nunamaker, Jr: On toward a broader vision of IS research. Business and Information Systems Engineering, 5, 321–323.

Patton, M. (1990). Qualitative evaluation and research methods (2nd ed.). London: Sage Publications.

Rajamäki, J. (2021). Resilience Management Concept for Railways and Metro Cyber-Physical Systems. In T. Eze (Ed.) Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS. Reading: Academic Conferences International Limited, 337-345.

Robson, C. (2002). Real world research (2nd ed.). Oxford: Blackwell Publishing.

SAFETY4RAILS (2022). Home - SAFETY4RAILS project [online] Available from: https://safety4rails.eu/ Accessed 13.10.2022.

Wang, J. et al. (2016). "Toward a Resilient Holistic Supply Chain Network System: Concept, Review and Future Direction," in IEEE Systems Journal, vol. 10, no. 2, pp. 410-421, June 2016, doi: 10.1109/JSYST.2014.2363161

Yin, R. K. (2009). Case study research design and methods (4th ed.). Thousand Oaks: Sage Publications.

Zhou, Y. Ting, Ma, T., Zhang, H. & Chen, G. (2019). Summary - 360° of Asset Management [online] Available from: https://web.cventhen.com/event/3445a728-bd10-4019-95bd-3f39436c91f1/summary Accessed 22.11.2022.