EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAILWAY CYBERSECURITY

Good practices in cyber risk management

NOVEMBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Theocharidou Marianthi, Stanic Zoran, ENISA

De Mauroy Louise, Lebain Loïc, Haddad Jules, Wavestone.

ACKNOWLEDGEMENTS

We would like to warmly thank all the experts that took part in our workshops and provided comments. Their contributions and inputs were essential for the creation of this report.

ENISA would like to thank the European Railway Agency (ERA), the European Railway Information Sharing and Analysis Centre (ER- ISAC) and UNIFE's cybersecurity working group for their support.

Andersson Johan A., Tranfikverket
Boff Sacha, Banenor
Bos Stoffel, Prorail
Boss John, Prorail
Brouwer Riemer, Prorail
Cabral Pereira Mário Jorge, Infraestruturas de Portugal
Chatelet Thomas, ERA
Ciancabilla Attilio, RFI
Cosic Jasmin, DB Netz
De Visscher Olivier, ER-ISAC
Dyrlie Rune, Banenor
Fernandez Gonzalez Lola, Knorr-Bremse
Fritz Jérôme, CFL
Garcia Marta, UNIFE
Garnier Yseult, SNCF Reseau
Gomez Nieto Antonio, Adif
Hausman Francois, Alstom group
Houbion Catherine, Infrabel
Korving Evertjan, Prorail
Mager Joseph, NS
Magnanini Giulio, RFI
Meulders Philippe, CFL
Meyer, Andreas, Selectron

Ooms-Geugies Klaasjan, NS
Pizzi Giorgio, Ministero Infrastrutture e Trasporti
Paulsen Christian, Siemens
Pouet Nicolas, SNCF Reseau
Remberg Tom, Banenor
Rodrigues Susano Ana Beatriz, Infraestruturas de Portugal
Thesse Eddy, Alstom group
Van den Bossche Peter, Infrabel
Van Zantvliet Dimitri, NS

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-545-6, DOI 10.2824/92259

TABLE OF CONTENTS

EXECUTIVE SUMMARY

European railway undertakings and infrastructure managers systematically address cyber risks as part of their security risk management processes, especially after the Network and Information Security (NIS) Directive came into force in 2016. Addressing cyber risks in the railway sector can raise entirely new challenges for railway companies who often lack the internal expertise, organisational structure, processes or the resources to effectively assess and mitigate them.

The nature of railway operations and the interconnectedness of railway undertakings, infrastructure managers, and the supply chain requires all involved parties to achieve and maintain a baseline level of cybersecurity. European RUs and IMs use a combination of good practices, approaches, and standards to perform cyber risk management for their organisations, as they need to assess cyber risks for all functions and for both OT and IT. This report gathers insights on these current practices in a single document and can assist railway undertakings and infrastructure managers in their efforts to apply them. It provides examples of reference material, such as available taxonomies of assets and services, threat taxonomies, seven comprehensive threats scenarios, derived from real incidents, and available cyber risk mitigation measures, derived by guidelines and standards.

This report aims to be a reference point for current good practices for cyber risk management approaches that are applicable to the railway sector. It offers a guide for railway undertakings and infrastructure managers to select, combine or adjust cyber risk management methods to the needs of their organisation. It builds upon the 2020 ENISA report on cybersecurity in the railway sector (ENISA, 2020), which assessed the level of implementation of cybersecurity measures in the railway sector.

This report provides actionable guidelines, lists common challenges associated with the performance of the relevant activities, and outlines good practices that can be readily adopted and tailored by individual organisations. Additionally, a list of useful reference material is available, together with practical examples and applicable standards.

ABBREVIATIONS

ATP	Automatic train protection
CCS	Command, Control and Signalling
CCTV	Closed-Circuit Television
CVSS	Common Vulnerability Scoring System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CSIRT	Computer Security Incident Response Team
DoS/DDos	Denial of Service/Distributed Denial of Services
DSP	Digital Service Provider
EC	European Commission
ER-ISAC	European Railway Information Sharing and Analysis Centre
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
GDPR	General Data Protection Regulation
GSM/GSM-R	GSM-Railway
HR	Human Resources
HVAC	Heating, ventilation, and air conditioning
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IM	Infrastructure Manager
ISO	International Organisation for Standardization
ISP	Internet Service Provider
ISSP	Information System Security Policy
IT	Information Technology
LAN	Local Area Network
MS	Member State
NIS Directive	Directive on Security of Network and Information Systems
NIST	National Institute of Standards and Technology
OES	Operator of Essential Service
OT	Operational Technology
PKI	Public Key Infrastructure
RU	Railway Undertaking
SOC	Security Operation Centre
VLAN	Virtual LAN
VPN	Virtual Private Network

1. INTRODUCTION

Directive 2016/1148 (NIS Directive) is the first legislative document focusing on cybersecurity in the EU. It identifies Operators of Essential Services (OES) in the railway sector as:

Infrastructure managers (IM), as defined in point (2) of Article 3 of Directive 2012/34/EU, include: "any person or firm responsible in particular for establishing, managing and maintaining railway infrastructure, including traffic management and control-command and signalling. The functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or firms".

Railway undertakings (RU), as defined in point (1) of Article 3 of Directive 2012/34/EU, include: "any public or private undertaking licensed according to this Directive, the principal business of which is to provide services for the transport of goods and/or passengers by rail with a requirement that the undertaking ensures traction. This also includes undertakings which provide traction only". This also includes operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU as "any public or private entity responsible for managing one or more service facilities or supplying one or more services to railway undertakings".

The NIS Directive requires IMs and RUs to conduct risk assessments that "cover all operations including the security and resilience of network and information systems". According to the NIS Directive, these risk assessments, along with the implementation of appropriate mitigation measures, should promote "a culture of risk management" to be developed through "appropriate regulatory requirements and voluntary industry practices". This need for cyber risk management in the European railway sector was also identified as a key priority by the participants of the ENISA-ERA conference "Cybersecurity in Railways", which took place online on 16-17 March 2021 and brought together more than 600 experts from railway organisations, policy, industry, research, standardisation, and certification.

While some EU Member States (MS) have issued relevant national guidance to OESs on how to conduct cyber risk assessments, most railway operators choose to adopt one of the different methodologies introduced by industry standards. Indeed, there are currently varying approaches to tackle risk in the railway sector and for now, there is no single approach that covers both information technology (IT) and operational technology (OT) cyber risks. This document offers a guide to these different approaches, enabling railway operators to select, combine or adjust cyber risk management methods to the needs of their organisation. It builds upon the 2020 ENISA report on cybersecurity in the railway sector (ENISA, 2020), which assessed the level of implementation of cybersecurity measures in the railway sector.

1.1 OBJECTIVES, SCOPE AND AUDIENCE

This report aims at providing railway stakeholders with applicable methods and practical examples on how to assess and mitigate cyber risks. These good practices are gathered based on feedback from railway stakeholders and include tools, such as assets and services list, threat scenarios, mapping of security measures. These resources can be used as a base for cyber risk management for railway companies. The study aims at being a reference point to promote collaboration between railway stakeholders across the EU and raise awareness of relevant threats.

This report is concerned with the European railway sector, and it covers cyber risk management applicable to both the IT and OT systems of railway organisations. Other railway stakeholders such as rolling stock manufacturers and component vendors are not considered in the scope of this report.

The primary target audience of this study includes people responsible for cybersecurity (CISOs, CIOs, CTOs, etc.) within RUs and IM networks. This report aims to provide them with the means to understand their cybersecurity ecosystem, assess the risks to their assets or services and manage them via appropriate cybersecurity measures. In addition, the National Competent Authorities, who may wish to develop guidance for railway operators in conducting cyber risk management, may consult this document to understand the current practices in the sector and potential challenges.

1.2 METHODOLOGY

The report was created with cooperation of European IMs and RUs in an iterative process with multiple rounds of validation as follows:

Step 1 - Definition of the project scope and identification of experts. The first step consisted of defining the scope of the project and selecting subject matter experts whose input and insights could be considered for the development of the report. The experts chosen are mainly RU and IM stakeholders in charge of cybersecurity, as well as members of national and European agencies.

Step 2 - Desk research. During this step, extensive desk research for relevant documents in the context of the project was conducted. The identified sources served as a reference to develop good practices, a list of assets and threats, threat scenarios, and list of measures.

Step 3 - Series of workshops with selected subject matter experts. Four workshops were conducted to discuss and validate the key findings of the study, namely the list of assets, list of threats, threats scenarios, and list of measures. Additionally, the workshops were used as an opportunity to collect feedback on the challenges and good practices of risk management in the railway sector. The 20 experts originated from 10 European railway companies from Belgium, Germany, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, and Sweden. The European Rail Information Sharing and Analysis Centre (ER-ISAC) was also represented in the experts' pool.

Step 4 - Analysis of collected material and report development. The input collected from desk research and the stakeholder workshops were analysed. Based on this analysis, the first draft of this report was developed.

Step 5 - Review and validation. The report was then validated by 24 experts (primarily RUs and IMs) from Belgium, France, Germany, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, and Sweden, the ER-ISAC and the UNIFE cybersecurity working group. The experts reviewed the report and provided comments and suggestions for improvement. These were the basis for the final version of this document.

1.3 STRUCTURE OF THE REPORT

The report is organised in 6 chapters:

- **Chapter 2** describes cyber risk management concepts and the current approaches identified for the railway sector. It can help railway stakeholders to choose a risk management methodology.
- **Chapter 3** contains a list of railway assets and services (definitions and taxonomy), along with guidelines on how to identify those assets and services. Railway stakeholders can use this information to build their own list of assets and services.
- **Chapter 4** focuses on cyber threats, with a list of threats, their definitions and a list of risk scenarios applicable to the railway sector. Stakeholders can use those tools to identify the main risks to their assets and evaluate what should be prioritised for protection. The list of threats would be useful to conduct risk assessments, along with the abovementioned list of assets and services.
- **Chapter 5** examines current cybersecurity measures based on EU guidelines (NIS Directive) and international standards. It can help stakeholders to define a risk management plan.
- **Chapter 6** offers some concluding remarks.

2. CYBER RISK MANAGEMENT

The purpose of this chapter is to outline the risk management approaches that were used in the study and are applicable to the railway sector. Many definitions and concepts exist, thus making it difficult to choose one that is most relevant to the individual's case. To ensure a common risk management frame, this document proposes a set of definitions and principles extracted from ISO 31000:2018 "Risk management – Principles and guidelines", ISO-IEC 27005:2018 "Information security risk management" and the ISO-IEC 62443 series.

The information security risk management process is the coordination of activities to direct and control an organisation with regard to risk. It consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review. The information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase the depth and detail of the assessment at each iteration. It also provides a good balance between minimising the time and effort spent in identifying controls, while ensuring that strong risks are appropriately assessed.

As mentioned in the ISO 31000 principles chapter, risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.

For terms and definitions, please consult ISO 31000:2018 "Risk management – Principles and guidelines", ISO-IEC 27005:2018 "Information security risk management.

2.1 RISKS MANAGEMENT STEPS

ISO 27005:2015 defines a risk management process which integrates all necessary key activities to deploy a risk management methodology.

Figure 1: Risk management

The first step of launching a risk management process is **establishing the context**, both external and internal. It involves setting the basic criteria necessary for information security risk management (approach, risk evaluation criteria, impact criteria and risk acceptance criteria), defining the scope and boundaries (ensuring that all relevant

assets are taken into account in the risk assessment), and establishing an appropriate organisation to manage the information security risk management.

The second step is launching a **risk assessment**, i.e., quantifying or qualitatively describing risks and enabling managers to prioritise them according to their perceived seriousness or other established criteria. The risk assessment consists of three distinct tasks:

- **Risk identification**, to determine what could happen to cause a potential loss and to gain insight into how, where, and why the loss could occur.
- **Risk analysis**, to understand the nature of the risk and to determine the level of risk. A risk analysis methodology may be qualitative, quantitative, or a combination of both depending on the circumstances.
- **Risk evaluation**, to compare the level of risks against risk evaluation criteria and risk acceptance criteria. The purpose is to produce a list of risks prioritised according to risk evaluation criteria in relation to the incident scenarios that lead to those risks.

The third step is the **risk treatment**, which consists of defining a list of controls to reduce, retain, avoid, or share the risks. Then, a risk treatment plan can be defined. The risk treatment plan description will be elaborated in chapter 5 of this present document.

The fourth step is **risk acceptance**, i.e., the decision to accept the risks and responsibilities for the decision. Finally, a list of accepted risks with justification for those that do not meet the organisation's normal risk acceptance criteria is established.

The fifth step is the **risk communication**. Information about risks should be exchanged and/or shared between the decision-maker and other stakeholders.

The final step is **risk monitoring and review**. It consists of the monitoring and reviewing the risks and the various factors (i.e., value of assets, impacts, threats, vulnerabilities, likelihood of occurrence) that help to identify any changes in the context of the organisation at an early stage, and to maintain an overview of all risks.

2.2 RISK MANAGEMENT APPROACHES FOR THE RAILWAY SECTOR

Workshops with relevant European railway sector stakeholders were conducted to identify the most common risk management methods currently used by RUs and IMs. During these workshops, stakeholders indicated their chosen methods. They are complemented or combined with other approaches to reach the desired level of sophistication and to cover both IT and OT requirements for risk management. Their approaches are also linked to the overall enterprise risk method used by the organisation and have to offer adequate level of compliance with both EU and national cybersecurity requirements. For RUs and IMs operating in multiple EU Member States (MS), national requirements under the NIS Directive may not be fully harmonised, so these organisations face additional challenges in compliance. For all EU RUs and IMs to meet the cybersecurity requirements of their national competent authorities, support is needed from the railway industry. RUs and IMs rely on their suppliers, both for more accurate threat and vulnerability analyses, but especially for implementing cybersecurity requirements.

Indeed, existing approaches are multiple and varying across the railway companies, but they may present different scope and level of detail in terms of analysis. For the risk management of railway IT systems, the most cited approaches were the requirements of **NIS Directive at a national level**, **the ISO 2700x family of standards**, and the **NIST cybersecurity framework**. For OT systems, the frameworks cited were **ISA/IEC 62443**, **CLC/TS 50701**, and the recommendations of the **Shift2Rail project X2Rail-3,** or the ones from the **CYRail Project**. Those standards or approaches are often used in a complementary way to adequately address both IT and OT systems. While IT systems are normally evaluated with broader and more generic methods (such as ISO 2700x or NIS Directive), OT systems need specific methods and frameworks that have been designed for industrial train systems. For instance, the ISA/IEC 62443 standards are the most cited frameworks used for specific OT assets and risk identification, while many contributors to this report stated they intend to use the recently released CLC/TS50701 in the future.

Stakeholders that participated in this study indicated that they use a combination of the abovementioned international and European approaches to tackle risk management, which they then complement with national frameworks and methodologies. Examples include the Dutch A&K analysis[1], the German BSI Risk Management Standard 200-3[2] and the French E-BIOS Risk Manager method[3]. Moreover, other stakeholders designed their own modified versions of methodologies based on existing frameworks.

The difference between standards' completeness can also be tackled by building a bridge between the high-level company risk assessment, and the lower application, or asset risk, assessment level. The generic framework and standards can be used at a high level and the more technical or precise ones can be used at the applications and assets level. The risks and measures issued at the end of each process are consolidated in a global risk mapping and risk treatment plan.

A multitude of different approaches and methods have been recommended by national and international authorities regarding cyber risk management. This next section analyses a sample of European and international good practices.

ISO 27001, 27002 and 27005 standards. The ISO 2700x family are among the most used and cited standards for information security. ISO 27001 is the standard dedicated to establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. ISO 27001 and 27002 contain a list of requirements to consider when implementing a risk treatment plan and will be studied in more detail in chapter 5 of the present document. ISO 27005 is focused on risk management. It is the one selected in the present document as a reference for defining the risk management principles presented above. According to CLC/TS 50701 (see below), ISO27K series can be applied to the business part of railway infrastructure, which primarily includes IT systems.

NIS Directive Cooperation Group guidelines. In 2018, the NIS cooperation group[4] issued a "reference document" which provides a summary of the Group's main findings on cybersecurity measures for OESs (NIS Cooperation Group, 2018). The reference document primarily covers the risk treatment phase of risk management. It does not establish a new standard nor duplicate existing ones (e.g., ISO) but provides MS with a clear and structured picture of their current and often common approaches to the security measures of OESs. Beyond OESs, this reference document may be considered useful by other public or private actors looking to improve their cybersecurity. As it focuses on security measures, it will be studied in more detail in chapter 5.

ISA/IEC 62443 standards. The ISA/IEC 62443 series of standards provides a framework to address and mitigate security vulnerabilities in industrial automation and control systems (IACS). They described both technical and process-related aspects of industrial cybersecurity and provide a risk management approach, especially for OT systems, which can be applied to OT used in the railway sector. In particular, the ISA/IEC 62443-3-2, "Security Risk Assessment, System Partitioning and Security Levels" standard defines a set of engineering measures to guide organisations through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels. A key concept is the application of IACS security zones and conduits, which were introduced in ISA/IEC 62443-1-1, Concepts and Models. The standard provides a basis for

[1] The method Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K analysis) was developed in draft form by the Dutch public company RCC. The Dutch Ministry of Internal Affairs completed its development in 1996 and published a handbook describing the method. The method has not been updated since that time. The A&K analysis is the unique and preferred method for risk analysis by Dutch government bodies since 1994. In addition to the Dutch government, Dutch companies often use A&K analysis.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_dutch_ak_analysis.html

[2] With the BSI Standard 200-3, the BSI provides an easy-to-apply and recognised procedure which allows organisations adequate and targeted control of their information security risks. The procedure is based on the elementary threats described in the IT-Grundschutz Compendium on the basis of which the IT-Grundschutz-modules were drawn up.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html;jsessionid=A26D9630FC3E530CDEECEACC00297837.internet461?nn=128620

[3] EBIOS Risk Manager (EBIOS RM) is the method for assessing and treating digital risks, published by National Cybersecurity Agency of France (ANSSI) with the support of Club EBIOS. It provides a toolbox that can be adapted, the use of which varies according to the objective of the project. EBIOS Risk Manager is compatible with the reference standards in effect, in terms of risk management as well as in terms of cybersecurity.
https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

[4] The NIS Cooperation Group is composed of representatives of Member States, the Commission, and ENISA, has been established under the NIS Directive. It facilitates strategic cooperation between the Member States regarding the security of network and information systems.
https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

specifying security countermeasures by aligning the identified target security level with the required security level capabilities set forth in ISA/IEC 62443-3-3, System Security Requirements and Security Levels.

CLC/TS 50701. Following this standard, the Technical Specification 50701 was issued (CLC/TS 50701, 2021). This European Technical Specification applies ISA/IEC 62443 to the railway sector. It applies to the communications, signalling, processing, rolling stock and fixed installations domains. It provides references to models and concepts from which requirements and recommendations can be derived and which are suitable to ensure that the residual risk from security threats is identified, supervised, and managed to an acceptable level by the railway system duty holder. CLC/TS 50701 can be used to define a list of OT components for the railway sector, and to build a list of OT-specific security measures.

Shift2Rail Risk Assessment Methods (projects X2Rail-1 and X2Rail-3). Shift2Rail proposes a risk assessment based on IEC 62443-3-2 (X2Rail-1, 2019; X2Rail-3, 2020). It proposes a common railway framework, which includes:

- Attacker landscape dedicated to railway
- Threat landscape dedicated to railway based on (ISO 27005, ENISA's 2016 Threat Taxonomy 2016 and BSI: Threats Catalogue)
- Impact matrix
- Approach for high-level risk assessment and estimation of the security level targets based on the STRIDE threat classification
- Process for detailed risk assessment.

Based on this common approach, Shift2Rail performed a risk assessment of a generic railway signalling system compliant with the IEC 62443 and proposed target security levels for the different identified zones. X2Rail-3 proposed a Simplified Risk assessment approach in 2020 (X2Rail-3, 2020) which consists of the following workflow:

1. Description of the zone under assessment
2. Division of the assessment into six STRIDE threat domains[5]
3. Estimation of likelihood and impact
4. Risk computation
5. Security level mapping to risk level
6. Foundational Requirements[6] security level mapping to six STRIDE threat domains security levels

CYRail recommendations on cybersecurity of rail signalling and communication systems. The EU-funded project CYRail[7] issued a guide published in September 2018 (Cyrail, 2018). This guide provides an analysis of threats targeting railway infrastructures, in addition to the development of attack detection and alerting techniques, mitigation plans and Protection Profiles for railway control and signalling applications to ensure security by design of new rail infrastructures. It relies on the IEC62443 standard. The security assessment consists of the following 5 steps:

- Identification of the system under consideration (SUC)
- Performing a high-level cybersecurity risk assessment to identify the worst-case risks
- Partition of the SUC into zones and conduits and definition of the vulnerabilities
- Realisation of detailed risk assessment in each zone and conduit in 10 steps (identify threats, identify vulnerabilities, determine consequence and impact, determine unmitigated likelihood, calculate unmitigated

[5] The STRIDE model is a model of threats developed by Microsoft to identify computers security threats, as the first step in a proactive security analysis process. The next steps in the process are identifying the vulnerabilities in the implementation and then taking measures to close security gaps. STRIDE model defines a threat as any potential occurrence, malicious or otherwise, that can have an undesirable effect on the system resources. STRIDE stands for 6 main threats: Spoofing of user identity, Tampering with data, Repudiability, Information disclosure (privacy breach), Denial of Service (DoS) and Elevation of privilege. Vulnerability is an unfortunate characteristic that makes it possible for a threat to occur. An attack is an action taken by a malicious intruder to exploit certain vulnerabilities to enact the threat. It was created to be applied to a specific system or during the development of a product; therefore, it is less relevant at a company level, as it does not encompass the whole risk management process. Nevertheless, it can be used with a more global methodology when defining the threats.
https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach
[6] According to IEC62443, security capabilities are organised according to seven Foundational requirements (FR1 Identification and Authentication Control, FR2 – Use Control, FR3 - System Integrity, FR4 – Data Confidentiality, FR5 – Restricted Data Flow, FR6 – Timely Response to Events, and FR7 – Resource Availability.
[7] https://cyrail.eu/about-cyrail-project-1

cyber security risk, determine security level target, identify and evaluate existing countermeasures, revaluate likelihood and impact, calculate residual risk, document and communicate results)
- Documentation of the process

This guide is useful to conduct risk analysis within the railway sector, particularly on control and signalling applications, using the IEC62443 standard.

EULYNX, RCA, and OCORA approach. EULYNX is a European initiative led by 13 IMs to standardise interfaces and elements of signalling systems. EULYNX Reference Architecture defines the complete EULYNX system, describing the overall architecture, cross-cutting architectural concepts, and all generic functions of the system. Baseline Set 3 was completed in 2020[8].

RCA stands for Reference Control, Command & Signalling (CCS) Architecture. It is an initiative led by members of the ERTMS Users Group (EUG) and EULYNX to define a harmonised architecture for the future railway CCS, with the main goal of substantially increasing the performance/total cost of ownership (TCO) ratio of CCS. The RCA Baseline Set 0 Release 1 was updated with the Cyber Security guidelines created by OCORA, RCA and EULYNX. It defines a risk assessment process taking IEC 62443 and CLC/TS 50701 as security standards and gives an example on how to apply it to trackside CCS. The following process is defined:

- Definition of system under consideration
- Initial zoning concept based on risk assessment
- Definition of attacker types
- Evaluation of the attackers, strength, motivation
- Supplementation of threats
- Sorting of threats into foundational requirements
- Definition of the initial security level per threat
- Entering the foundational requirement value into the vector of the preliminary zone
- Application of reduction factors to determine the final security level
- Application of the measures according to IEC62443

The focus of RCA is on the architecture of the CCS trackside. There is a similar initiative, named OCORA, which addresses the architecture of the CCS on-board side[9]. It is a joint initiative by 5 European railway companies[10] which has been set up to define the architecture and interfaces for the next generation of on-board European Train Control System (ETCS) systems.

UIC Guidelines for Cyber-Security in Railways. In 2018, the UIC ARGUS WG decided to produce an enforced document to provide specific guidance to the 'Railway' (UIC, 2018). This guidance document is designed to support the rail industry in reducing its vulnerability to cyber-attacks and to ensure availability, integrity, confidentiality of railway systems and data at all times. The document has a particular but not exclusive focus on signalling and telecommunication within railway. The document is based on the ISO 27001 and 27002 standards and offers guidance specific to railway. It also describes common risk management steps such as: establishment of the security context, assets identification (primary and supporting), impact analysis (supported by operational impact scenarios), threat identification, selection of applicable threat scenarios, estimation of risk level for each applicable threat scenario based on the likelihood and the impact of those threat scenario, selection of risk treatment options, and selection of a list of additional controls.

[8] https://www.eulynx.eu/index.php/documents/published-documents/open-availability/baseline-set-3/257-20200623-eulynx-documentation-plan-eu-doc-11-v3-4-0-a/file
[9] https://github.com/OCORA-Public
[10] Deutsche Bahn (DB), Société nationale des chemins de fer français (SNCF), Nederlandse Spoorwegen (NS), Österreichische Bundesbahnen (ÖBB) and Schweizerische Bundesbahnen (SBB

3. RAILWAY ASSETS AND SERVICES

For RUs and IMs to manage cyber risks, it is crucial that they identify their railway assets and services that need to be protected. The railway sector is composed of multiple stakeholders who are responsible for their own infrastructure, assets and services, but they are strongly interconnected and interact with one another to deliver services. These interactions complicate risk assessment, because interdependencies between external stakeholders or suppliers must be considered in the analysis. The list resulting from this identification of assets and services should contain services the stakeholders have to deliver, and assets, such as devices, physical infrastructure, people and data needed to support these services.

In addition, stakeholders may develop indicators to assess cyber risk impact on the availability, integrity and confidentiality of these assets and services (e.g., number of users affected, economic impact, environmental impact, recovery time objectives, etc.).

Eight essential high-level railway services have been considered during the 2020 ENISA study (ENISA, 2020):

- Operating traffic on the network
- Ensuring the safety and security of passengers and/or goods
- Maintaining railway infrastructure and/or trains
- Managing invoicing and finance (billing)
- Planning operations and booking resources
- Information for passengers and customers about operations
- Carrying goods and/or passengers
- Selling and distributing tickets.

Railway stakeholders can use various taxonomies as the basis to identify their key cyber-related assets and services and adapt it to their own operational environment. Based on the desk research and information collected during the workshops, the key point is to maintain an asset inventory for cyber-related assets. Assets should be identified and registered in the asset inventory based on the system they relate to, the service they support and the information they handle. As mentioned, interdependencies between systems and third-party hardware and software, vendors, or other stakeholders must be considered. They should be identified in the specifications of technical interface (and/or data exchange) requirements. Finally, the department/division responsible for cybersecurity should be included in procurement contract review and implementation to ensure cybersecurity is addressed.

The identification of all interdependencies of the systems can be a real challenge. This is the case for external dependencies, but also for internal dependencies. Specifically, IT and OT interdependencies are complex because their boundaries are increasingly blurring, and OT and IT have different levels of maturity in terms of cybersecurity. Maintaining an exhaustive inventory is complex as systems are evolving fast, and the digitalisation of all processes is adding more and more systems that must be considered. This is exacerbated by the fact that the people responsible for the inventory often are unaware knowledge of all the assets and rely on systems engineers or security experts of the asset owner to maintain the inventory. Third-party-managed systems are also complicated to integrate in internal inventories due to this mix of responsibilities. To support this inventory, automated tools for asset management (identification, logging and monitoring) can be deployed, but the deployment of such tools requires strong interactions with systems that don’t always support such interactions. For asset identification, IT/OT asset discovery tools can be deployed, but care needs to be taken during their configuration so as not to affect the performance of systems.

3.1 TAXONOMY

To help RUs and IMs choose which assets and services to include in their risk assessment, a comprehensive list has been compiled. It is based on the systems' list described in the ENISA Report - Railway Cybersecurity of 2020[11]. It has been constructed from existing literature, validated during interviews with railway stakeholders in 2020, and enriched based on the feedback received during the 2021 workshops. It gives a robust and high-level overview of railway assets, with relevant categories.

Other, more detailed taxonomies exist in the sector and have been reviewed in order to complement and align (especially for the names and associated descriptions) this list with approaches on asset taxonomies, such as X2Rail Deliverables[12], RCA-OCORA-Eulynx Security Guideline[13] and TS50701. Indeed, RCA, OCORA, and Eulynx have created comprehensive asset architecture models specific to OT systems (on-board and trackside systems). They present assets at a more detailed level – up to the component level – and can be used for the risk assessment of a particular system, where such detail is required.

This list has been broken down to 5 areas; the **services** that stakeholders provide, the **devices** (technological systems) that support these services, the **physical equipment** used to provide these services, the **people** that maintain or use them, and the **data** used.

Fourteen **service** categories, together with sub-categories, are defined and depicted in Figure 2. For each service listed on (ENISA, 2020), assets have been identified. These are based on the list of systems by (ENISA, 2020), desk research, CLC/TS50701 and complemented with additions such as supply chain or freight assets. Supply chain assets refer to the assets provided by suppliers; as this present list may not be exhaustive, suppliers' threats can be additionally covered by defining a list of suppliers and applying specific measures to them. Freight assets are especially relevant as railways amount for a significant amount of EU freight transport. They can be targeted by specific attacks that are more focused on financial gain rather than disruption or passenger safety.

In addition, each asset has been characterised according to the kind of resources the asset uses:

- IT systems: refers to all components, devices and software used to store and process the information and realise IT operations.
- OT systems: refers to all components, devices and software used to conduct physical railway operations.
- Network and communications systems: refers to all components and devices used to physically convey information fluxes.
- Supply chain: refers to the assets provided by suppliers.

Four **device** categories have been identified, namely:

- Telecom
- IT & OT infrastructure
- Infrastructures and trackside
- On-board

These categories illustrate the systems to which the assets belong to and it is used to define the operation where the asset will be used: passenger comfort, signalling, corporate operations, etc. (see figure 3)

Moreover, physical equipment can be found either on infrastructure and trackside (buildings, tracks, etc.), or on-board (trains, wagon, lighting, etc.) (see Figure 4)

Finally, the different categories of people that are using these systems (clients or employees) and the different categories of data used by those systems are listed (see Figure 5).

These taxonomies can be used for developing an initial ontology-knowledge representation for the railway domain. For detailed descriptions of these five areas of assets, please consult Annex A.

[11] See https://www.enisa.europa.eu/publications/railway-cybersecurity
[12] See X2R3-T8_3-D-SMD-004-06_-_Deliverable_D8.2-3c_Protection_profile___On-board_components and X2R3-T8_3-D-SMD-009-06_-_Deliverable_D8.2-3b_Protection_Profile_-_Trackside
[13] See RCA Gamma published (eulynx.eu)

Figure 2: Railway Service categories

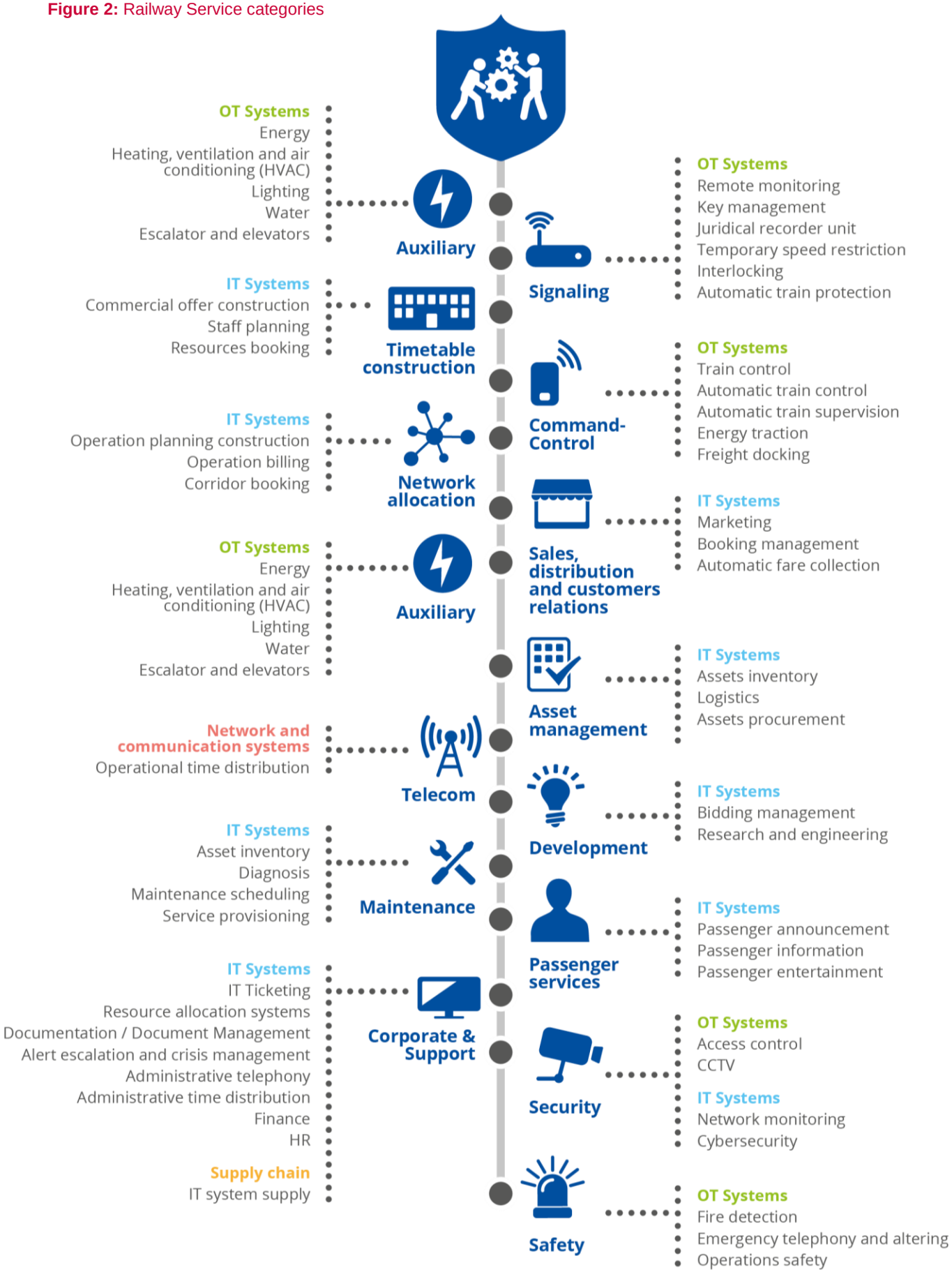


Figure 3: Railway devices

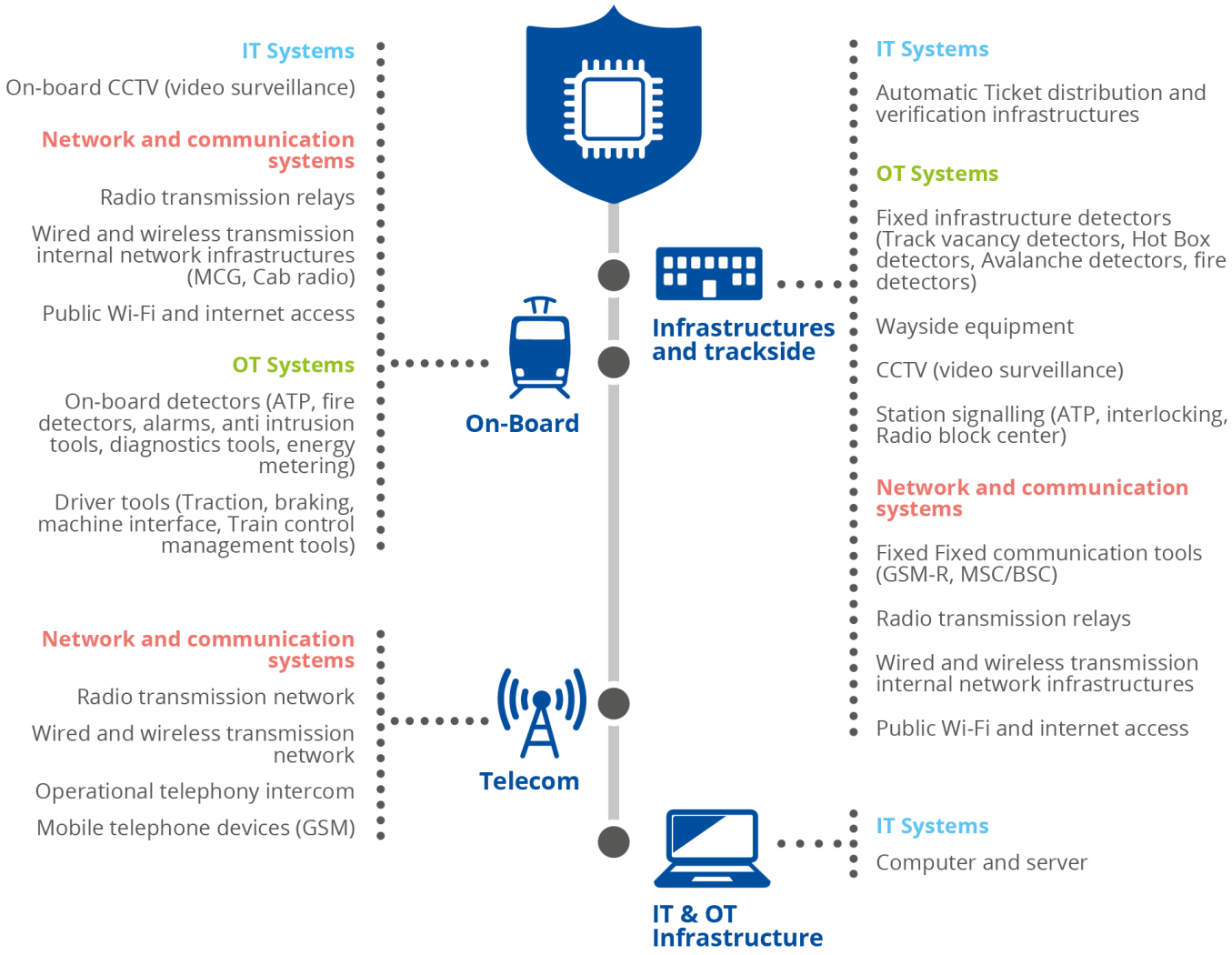


Figure 4: Railway Physical Equipment

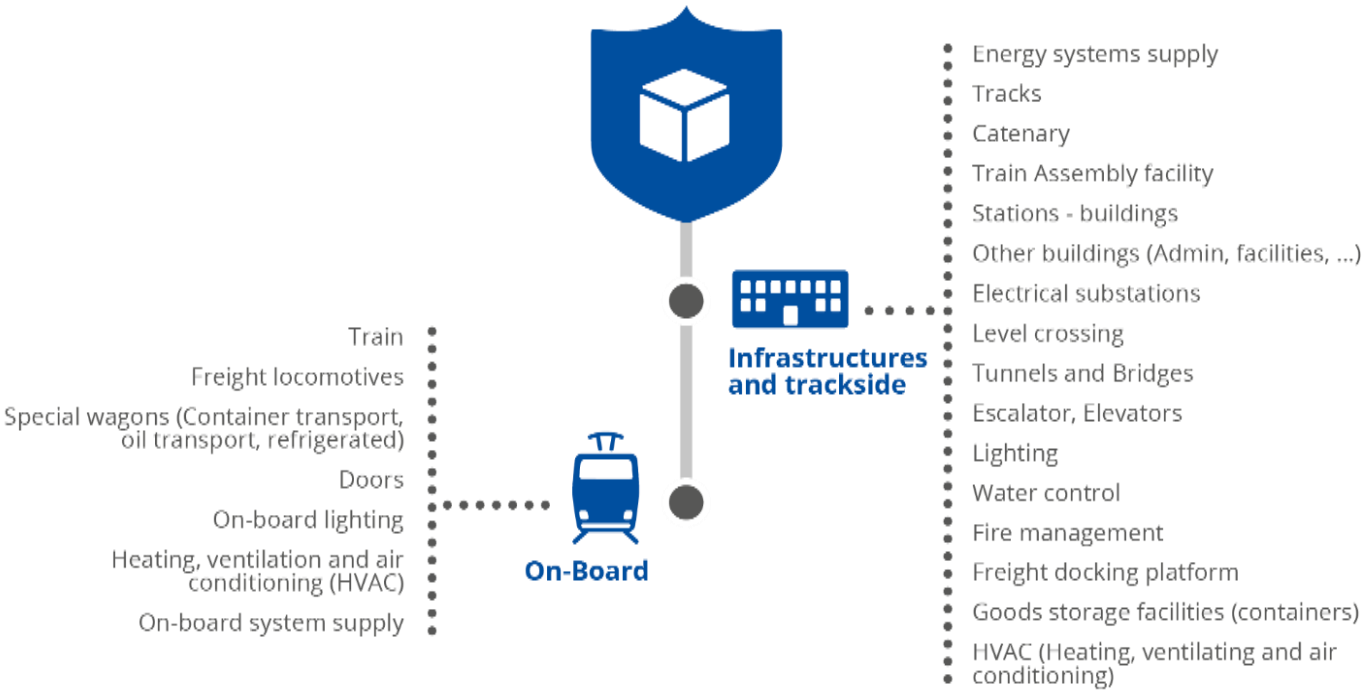
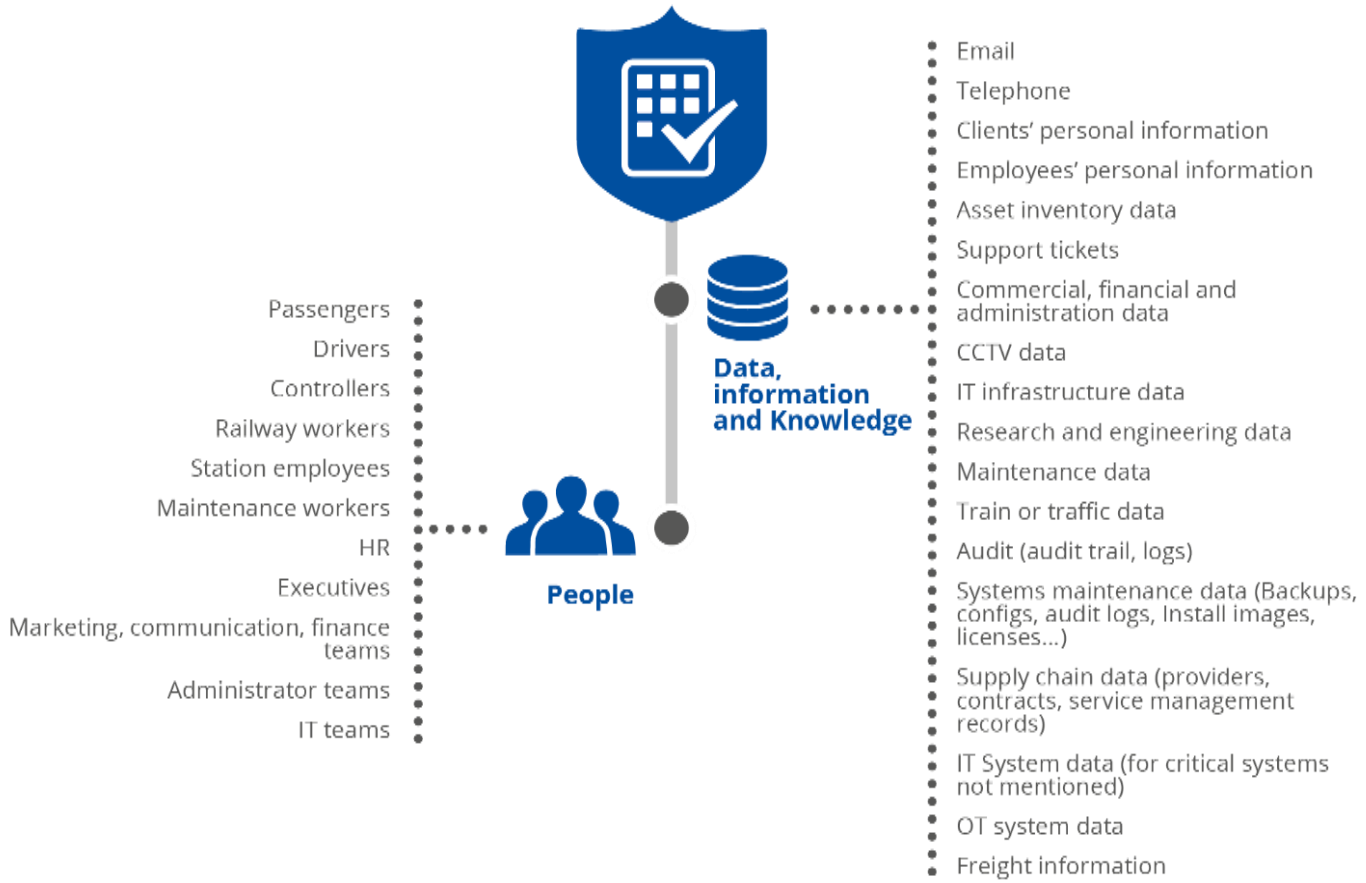


Figure 5: People and Data



4. CYBER-RELATED THREATS

In the railway sector, compromised OT systems can affect passengers' safety, cause a train accident, or interrupt traffic. OT systems are usually more vulnerable than IT systems, in part due to a lack of cybersecurity awareness in OT personnel, in part because they were not designed with cybersecurity in mind (long lifecycles of 30 years, presence of legacy systems) and because they are less controlled and decentralised compared to IT systems. While in the past they remained less exposed, often isolated from internet and other IT networks, they are now more and more interconnected with classic IT systems, which makes them even more vulnerable and exposed to cyber threats.

RUs and IMs need to identify which cyber threats are applicable to their assets and services. One of the common questions is whether threats, such as disasters, physical attacks, or outages, should be included or considered as not being specific to the "cyber" ecosystem. Most stakeholders include them, as they can affect information security. If they are not included, they should be considered in other risk management or business continuity management processes of the company, and this must be agreed on when the threat taxonomy is being developed.

Another challenge faced by the railway sector is assessing the likelihood of a threat scenario. One would need to consider the level of capability required for an attack, the level of exposure of the targeted asset, and the intent of an attacker, all of which are information that RUs and IMs may have difficulty in assessing accurately.

Several methods are proposed by the different cyber risk management frameworks. For example, X2Rail-3[14] proposes to rely on the Common Vulnerability Scoring System (CVSS). They have selected four CVSS Exploitability metrics in CVSS: Attack Vector (System Exposure), Attack Complexity, Privileges Required and User Interaction. Levels for these metrics have been defined, mathematically calculating the resulting likelihood. Other methods are less quantitative, but also simpler to apply, such as ISO27005, which combines the likelihood of occurrence of the threat (low, medium, high), the ease of exposure (low, medium, high) and the value of the asset (from 0 to 4) to calculate the likelihood of an incident scenario[15]. It is also very difficult to maintain this information because it changes through time as the threat landscape evolves.

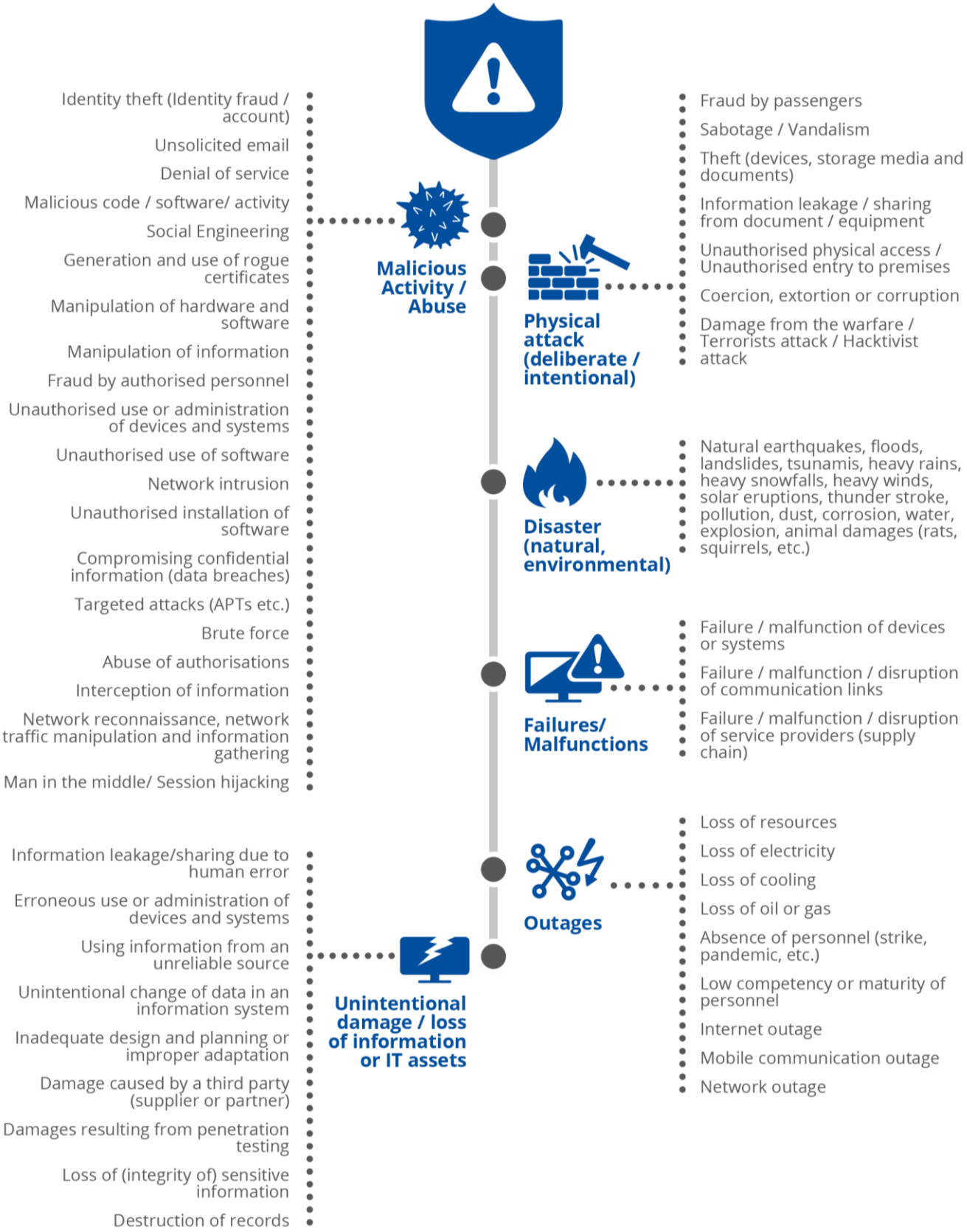
Finally, the railway sector faces challenges associated with supply chains. Security risks related to suppliers (e.g., remote access to the railway networks/systems) are less covered because of the heterogeneous and broad nature of the supplier landscape, but also because stakeholders do not have much control over the cybersecurity level of their suppliers and the cyber risks they may introduce. This topic can be reinforced by making an inventory of all the suppliers, categorising them in term of criticality (e.g., do they have access to a critical system, is there a strong interconnection between systems, do they manipulate sensitive data, etc.) and assessing the cybersecurity maturity of the most critical suppliers as a starting point.

4.1 TAXONOMY

RUs and IMs should decide on a list of threats to be used to perform their cyber risk analysis. There are several threat taxonomies available, without a consolidated version being available. For a detailed mapping of railway threat taxonomies, one can consult "Appendix to D8.2 Security Assessment: A mapping of threat landscapes" (X2Rail-1, 2019). This document maps various approaches to the proposed threat landscape by X2Rail-1 WP 8, which is based upon the ISO 27005 threat landscape with some improvements for railways. The ISO 27005:2011[16], ENISA Threat Taxonomy[17] and BSI Threats Catalogues are mapped to the threats considered under the X2Rail-1 WP 8 Threat landscape.

[14] See X2Rail-3 Deliverable D8.1 Guidelines for railway cybersecurity
[15] See ISO 27005, annex E, E.2 Detailed information security risk assessment
[16] See ISO 27005, annex E, E.2 Detailed information security risk assessment
[17] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

Figure 6: Threat taxonomy



To assist in this process, this report provides a comprehensive and tailored list of threats based on the 2016 ENISA Threat Taxonomy[18], as this is a more extensive list. It can be used as the basis to identify threats that apply in the context of the company and to assess railway cyber threats. It has been simplified to better apply to railways, and to ensure stakeholders can effectively use it. The resulting list of categories was reviewed and validated with experts during dedicated workshops. The main categories are as follows:

- Disaster (natural, environmental)
- Unintentional damage / loss of information or IT assets
- Physical attack (deliberate / intentional)
- Failures / Malfunction
- Outages
- Malicious activity / Abuse

Each threat belongs to a category and is applicable to one or more railway assets. This taxonomy has been represented graphically in Figure 6 and the threats are described in more detail in Annex B.

For an updated view of the current threat landscape, i.e. the current top threats, readers can consult the latest ENISA Threat landscape report[19]. For a more detailed analysis of adversary tactics, the MITRE ATT&CK® knowledge base[20] and the Common Attack Pattern Enumeration and Classification (CAPEC)[21] can also be used.

4.2 CYBER RISK SCENARIOS

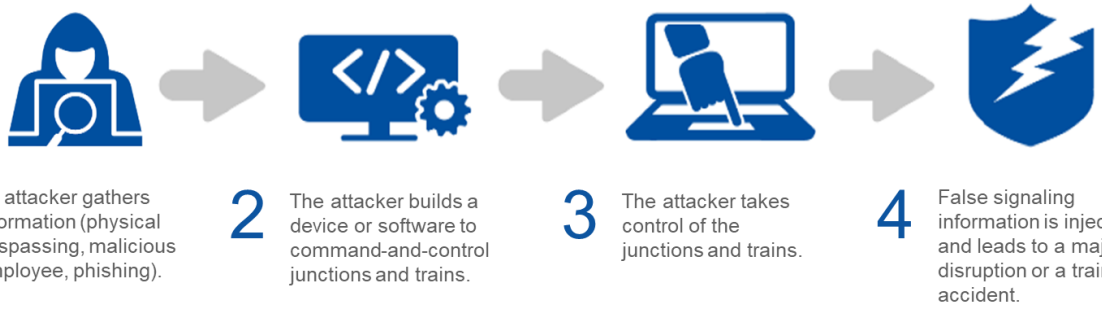
This section describes examples of cyber risk scenarios which can assist railway stakeholders when performing a risk analysis. They show how the asset and threat taxonomies can be used together and were based on the known incidents of the sector and the feedback received during the workshops. Each scenario is associated with a list of security measures, detailed later in chapter 28, which will mitigate the risk of this scenario occurring, and are derived from best practices. The following scenarios are described:

- Scenario 1: Compromising a signalling system or automatic train control system, leading to a train accident
- Scenario 2: Sabotage of the traffic supervising systems, leading to train traffic stop
- Scenario 3: Ransomware attack, leading to a disruption of activity
- Scenario 4: Theft of clients' personal data from the booking management system
- Scenario 5: Leak of sensitive data due to unsecure, exposed database
- Scenario 6: Distributed Denial of Service (DDoS) attack, blocking travellers from buying tickets
- Scenario 7: Disastrous event destroying the datacentre facility, leading to disruption of IT services

[18] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
[19] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[20] https://attack.mitre.org/
[21] https://capec.mitre.org/

4.2.1 Scenario 1 – Compromising a signalling system or automatic train control system, leading to a train accident

Figure 7: Compromising a signalling system or automatic train control system, leading to a train accident



This scenario requires high motivation of the attacker and in-depth knowledge of railway systems and networks. It is considered a low likelihood scenario. It has been included as the potential impact can be very high and this is one of the primary concerns of railway stakeholders when considering cyber risks. A similar incident took place in the city of Lodz, Poland in 2008 when an attacker managed to hack into a tram system.

<table>
<tr><th colspan="3">Attack details</th></tr>
<tr><td colspan="3">

An attacker gathers information (type of requests, IP address, etc.),

either trespassing on railway undertaking train facilities (e.g., depos, maintenance centre, etc.),
or from a malicious employee,
or using phishing to steal information from an employee;

An attacker builds a device or a software to command-and-control junctions and trains according to gathered information;
An attacker uses of the device to control the junctions and the trains;
An attacker provides false information to the system, leading to a major disruption or even a train accident.

</td></tr>
<tr><th>Impacts</th><th>Stakeholders</th><th>Assets affected</th></tr>
<tr><td>

Train casualties
Human casualties
Disruption of activity
Loss of reputation

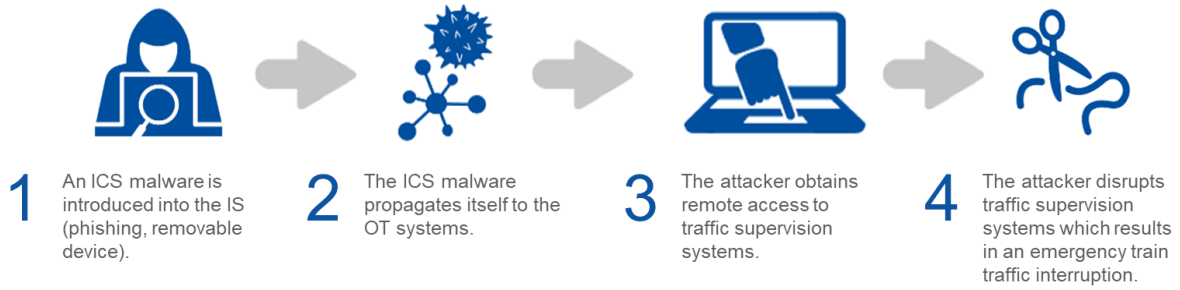
</td><td>Railway undertaking
Infrastructure manager</td><td>

Automatic train control system
Interlocking systems
Tracks, trains
Passengers

</td></tr>
<tr><th colspan="3">Security Measures</th></tr>
<tr><th colspan="2">High level security measures</th><th>Examples of specific measures</th></tr>
<tr><td colspan="2">NIS - PR.10 - Physical and environmental security
NIS - GV.6 Human resource security
NIS - PR.4 Cryptography
NIS - PR.8 Access right
NIS - DF.3 Logs correlation and analysis
NIS - DF.1 Detection</td><td>NIST - PR.AT Awareness & Trainings (1, 2, 3, 4, 5)
CLC/TS50701 SR 1.2 - Software process and device identification and authentication</td></tr>
</table>

4.2.2 Scenario 2 – Sabotage of the traffic supervising systems, leading to train traffic stop

Figure 8: Sabotage of the traffic supervising systems, leading to train traffic stop



This scenario is a targeted attack using a specific Industrial Control System (ICS) malware to disrupt the traffic supervising systems, thus leading to an urgent stop of train traffic. Such an incident has not yet occurred in the railway sector. This scenario could also be applied to freight docking systems, and thus disturb or interrupt freight activity.

<table>
<tr><th colspan="3">Attack details</th></tr>
<tr><td colspan="3">

An attacker introduces an ICS malware, through phishing emails sent to employee or removable devices used on OT systems;
The ICS malware propagates, takes over of the system, and gains remote access;
The malware allows the attackers to easily communicate with traffic supervising systems and remotely manipulate the system’s memory to inject shellcodes, eventually injecting a payload that disrupts traffic supervising systems;
The traffic supervising systems stop, preventing their supervision and leading to an urgent stop of train traffic.

</td></tr>
<tr><th>Impacts</th><th>Stakeholders</th><th>Assets affected</th></tr>
<tr><td>

Disruption of activity
Loss of reputation

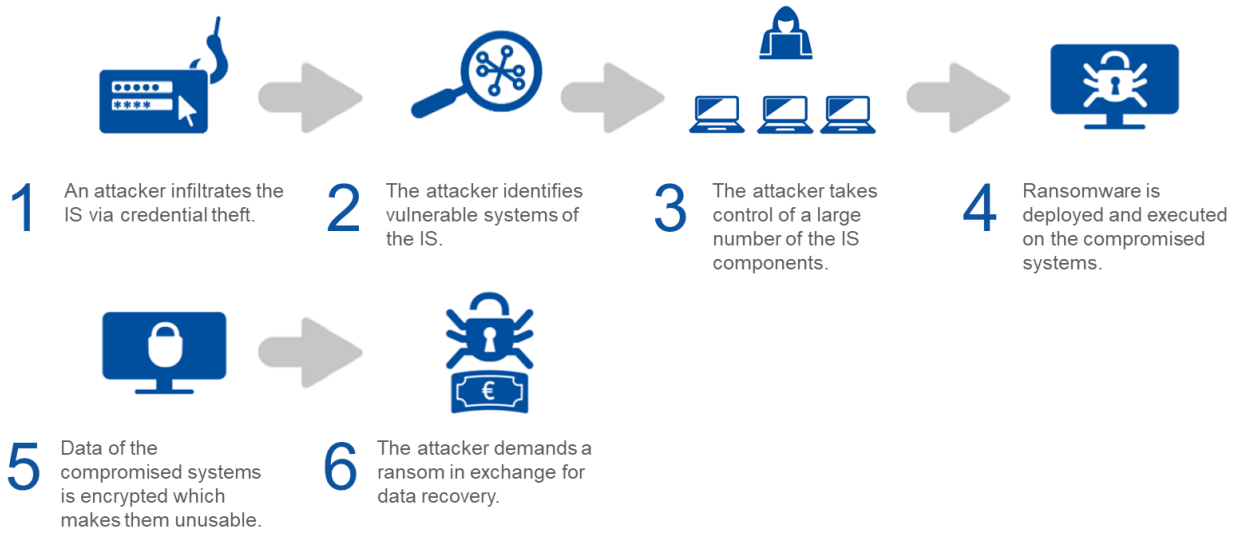
</td><td>Railway undertaking
Infrastructure manager</td><td>

Remote monitoring
Temporary speed restriction
Interlocking
Train control
Automatic train protection
Freight docking

</td></tr>
<tr><th colspan="3">Security Measures</th></tr>
<tr><th>High level security measures</th><th colspan="2">Examples of specific measures</th></tr>
<tr><td>NIS - GV.6 Human resource security
NIS - PR.9 IT security maintenance procedure
NIS - GV.5 Security Audit
NIS - DF.1 Detection
NIS - DF.3 Logs correlation and analysis</td><td colspan="2">NIST - PR.AT Awareness & Trainings (1, 2, 3, 4, 5)
CLC/TS50701 - SR 3.2 - Malicious code protection
CLC/TS50701 - SR 3.3 - Security functionality verification
CLC/TS50701 - SR 3.4 - Software and information integrity</td></tr>
</table>

4.2.3 Scenario 3 – Ransomware attack, leading to a disruption of activities

Figure 9: Ransomware attack, leading to a disruption of activities



In 2021, ransomware attacks are considered the top threat scenario and are targeting the transport sector. In this case, the attacker infiltrates the information system, exploits a vulnerability, and deploys a ransomware on a large amount of assets. A similar incident happened in May 2017 when Germany's Deutsche Bahn rail infrastructure was infected with WannaCry ransomware[22], leading to messages appearing on station information screens.

Attack details		
• An attacker infiltrates the information system by phishing or stealing credentials; • They scan the network for vulnerabilities, to exploit them and gather information; • They discover vulnerabilities on systems (e.g. due to inadequate patch management); • They deploy a ransomware that encrypts the data on all vulnerable systems; • The infected systems and devices cannot be used anymore; • They demand a ransom in bitcoins in a limited amount of time in exchange for data to be decrypted. • They further extort employees and customers by threatening to expose personal or confidential data.		
Impacts	**Stakeholders**	**Assets affected**
• Disruption of activity • Loss of data and information • Loss of reputation • Financial loss	Railway undertaking Infrastructure manager	• IT systems in services and devices • Data, information and knowledge
Security Measures		
High level security measures	**Examples of specific measures**	
NIS - PR.9 IT security maintenance procedure NIS - PR.2 System segregation NIS - PR.3 Traffic filtering NIS - GV.6 Human resource security NIS - DF.1 Detection NIS - DF.3 Logs correlation and analysis	CLC/TS50701 - SR 3.2 Malicious code protection CLC/TS50701 - SR 3.4 - Software and information integrity CLC/TS50701 - SR 5.2 Zone boundary protection CLC/TS50701 - SR 5.1 Network segmentation NIST - PR.AT Awareness & Trainings (1, 2, 3, 4, 5)	

[22] See https://www.railtech.com/digitalisation/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/

4.2.4 Scenario 4 – Theft of clients' personal data from the booking management system

Figure 10: Theft of clients' personal data from the booking management system

1 An attacker steals the credentials of one of the booking management system administrators via phishing.

2 The attacker obtains privileged access over the booking management system.

3 The attacker downloads the clients' personal data and proceeds to leak or sell it.

This scenario is a targeted attack, where the attacker steals the identity of an administrator and is therefore able to connect to a cloud-based booking management system and exfiltrate customer data. A similar incident happened in November 2017 with Rail Europe North America (RENA) suffering due to a 3-month long data breach[23] and in January 2019 when China Railway's official online booking platform suffered a massive data breach, with information later being sold on the dark web[24].

Attack details		

• Attackers identify and retrieve authentication data (credentials) to get access to useful systems:
  ○ by gathering information on railway systems through social engineering;
  ○ by identifying the targeted systems used for booking management and fetching the identity of the people using them;
  ○ once systems and their operators/users are identified, attackers launch phishing attacks to retrieve credentials to access to those systems;
• The attacker gets direct access, accesses the system using the administrator credentials;
• They get unauthorised access to customer data and retrieve it;
• They leak the data or sell them.		

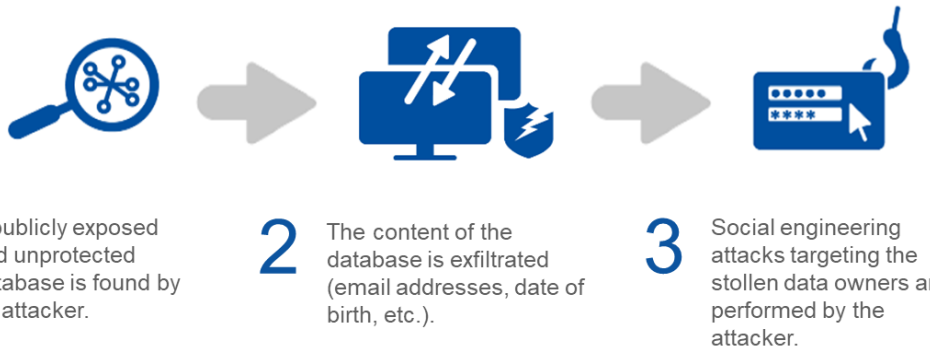
Impacts	**Stakeholders**	**Assets affected**
• Tarnished reputation • Regulatory sanction (GDPR)	Railway undertaking	• Booking management • Clients' personal information • Passengers

Security Measures	
High level security measures	**Examples of specific measures**
NIS - GV.5 Security Audit NIS - PR.2 System segregation NIS - PR.3 Traffic filtering NIS - PR.7 Authentication and identification NIS - PR.8 Access rights	NIST - PR.AT Awareness & Trainings (1, 2, 3, 4, 5) CLC/TS50701 - SR 1.1 Human user identification and authentication CLC/TS50701 SR 4.1 - Information confidentiality CLC/TS50701 - SR 5.1 Network segmentation CLC/TS50701 - SR 5.2 Zone boundary protection

[23] See https://d3security.com/blog/data-breach-of-the-month-rail-europe-north-america/
[24] See https://cyware.com/news/cyber-incidents-affecting-railways-a-threat-to-customer-data-a8d25ccc

4.2.5 Scenario 5 – Leak of sensitive data due to unsecure, exposed database

Figure 11: Leak of sensitive data due to unsecure, exposed database



This scenario is also related to data leakage, but the starting point here is a supplier with a low cybersecurity level. The attacker uses this third-party weakness to exfiltrate sensitive data. A similar incident happened in February 2020 with a database of C3UK[25], which offered Wi-Fi services to passengers in train stations. The database contained 146 million records, including personal contact details and dates of birth, and was exposed online without a password[26].

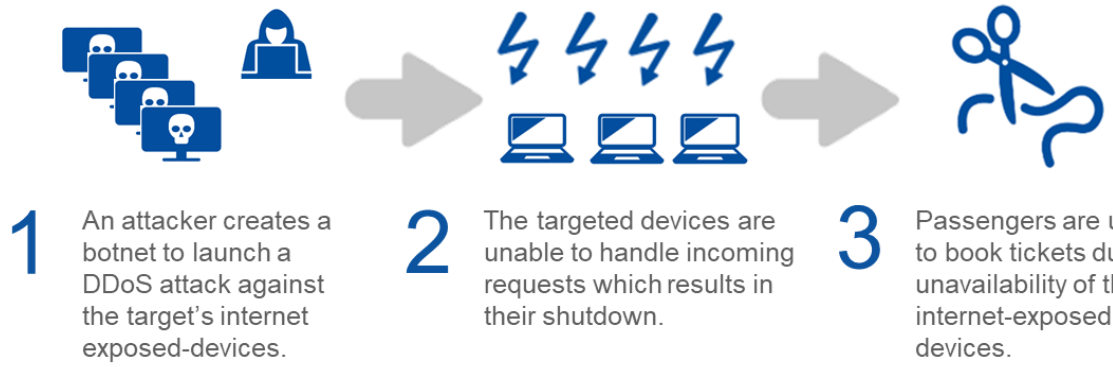
Attack details		
• A supplier providing services stores sensitive data (e.g., marketing company that manages a marketing campaign, data from an open Wi-Fi service available at a train station) in an unprotected database, exposed on internet, without password and without encrypting the information; • Hackers connect to the database and exfiltrate the information; • The database contains personal information, such as email addresses, date of birth, name, reason to travel and travel arrangements; • Hackers use the information for extortion attacks targeting employees and customers.		
Impacts	**Stakeholders**	**Assets affected**
• Loss of users' data • Regulatory sanction (GDPR) • Tarnished reputation	Railway undertaking	• Data, information and knowledge (sensitive data: personal, email, telephone, commercial and financial, train/traffic, supply chain data, freight data, IT infrastructure with audit/logs, other IT systems data) • People (Passengers; employees - executives, drivers and all other)

Security Measures	
High level security measures	**Examples of specific measures**
NIS - GV.5 Security Audit	NIST - ID.SC Supply Chain Risk (1, 2, 3, 4, 5)
NIS - GOV.7 Ecosystem mapping	ISO27002 - A.15 Supplier relationships
NIS - GOV.8 Ecosystem relations	CLC/TS50701 SR 4.1 - Information confidentiality

[25] Wi-Fi for transport service provider
[26] See https://www.bbc.com/news/technology-51682280

4.2.6 Scenario 6 – DDoS attack, blocking travellers from buying tickets

Figure 12: DDoS attack, blocking travellers from buying tickets

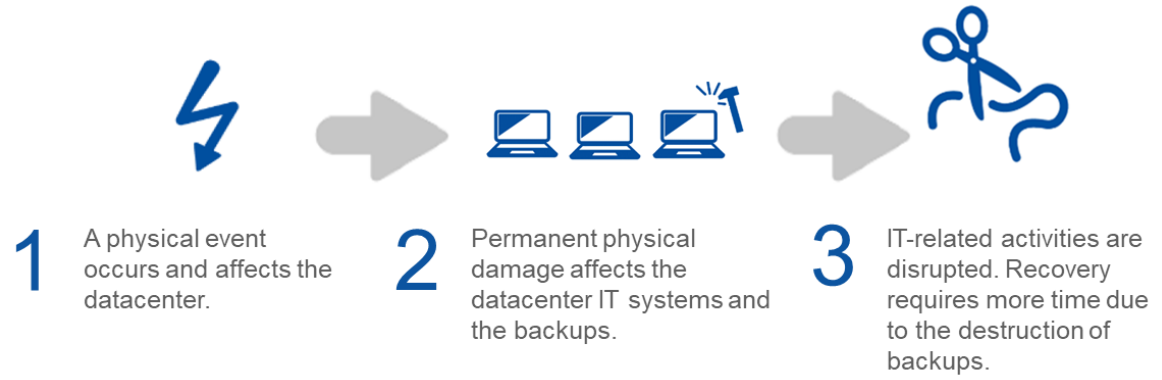


This scenario is a targeted attack, where the prerequisite for the attacker is to have created a botnet network (a set of compromised devices controlled by a hacker to perform their attacks). The attacker can then use the botnet to flood devices with requests and make them unavailable. Another possibility to consider for a DDoS scenario is a non-targeted attack, where an Internet Service Provider (ISP) is targeted with this type of attack, thus affecting railway services that use this ISP.

<table>
<tr><th colspan="3">Attack details</th></tr>
<tr><td colspan="3">An attacker has previously infected a number of computers, creating a botnet (a set of compromised devices controlled by a hacker to perform their attacks);
The botnet is used to launch a DDoS attack on the railway networks: the networks and servers exposed to the internet are flooded with requests and connection attempts and thus shut down, unable to sustain the flow;
All services and actions that need the internet-exposed devices are now unavailable: ticket-vending machines, sites or applications, and commercial websites. Passengers are unable to book tickets.</td></tr>
<tr><th>Impacts</th><th>Stakeholders</th><th>Assets affected</th></tr>
<tr><td>Tarnished reputation
Loss of revenue
Disruption of activities
Administrative and resource burden</td><td>Railway undertaking</td><td>Booking management
Automatic fare collection</td></tr>
<tr><th colspan="3">Security Measures</th></tr>
<tr><th colspan="2">High level security measures</th><th>Examples of specific measures</th></tr>
<tr><td colspan="2">NIS - DF.1 Detection
NIS - DF.3 Logs correlation and analysis
NIS - RS.1 Business continuity management
NIS - RS.2 Disaster recovery management</td><td>ISO27002 - A.17.1 Information security continuity
ISO27002 - A.17.2 Redundancies
CLC/TS50701 - SR 7.1 Denial of service protection</td></tr>
</table>

4.2.7 Scenario 7 – Disastrous event destroying the datacentre, leading to disruption of IT services

Figure 13: Disastrous event destroying the datacentre, leading to disruption of IT services



This scenario is the consequence of a disastrous event which leads to disruption of activity. The event (natural disaster, fire, etc.), affects the datacentre and destroys part of it, leading to a physical destruction of IT systems and thus a disruption of activities related to these services. Depending on the redundancy strategy of the company (geo-redundancy, cloud, external back-ups, etc.), the disruption can last more or less time. A similar incident happened in March 2021 when OVH[27] had a fire in one of its datacentres, making millions of websites unavailable for days[28].

Attack details		
• A disastrous event affects the datacentres and destroys part of it; it can be either a natural disaster (earthquake, flooding, storm, etc.) or a fire due to a physical malfunction; • The railway servers supporting the IT systems are physically destroyed; • The main IT systems are unavailable, leading to a disruption of all IT-supported services: corporate and support, sales and customers relations, timetable construction systems, asset management; • The back-ups stored in the datacentres are physically destroyed as well; data are thus lost, prolonging the disruption.		
Impacts	**Stakeholders**	**Assets affected**
• Loss of information • Disruption of activities • Loss of revenue	Railway undertaking Infrastructure manager	• IT systems in services and devices • Data, information and knowledge
Security Measures		
High level security measures	**Examples of specific measures**	
NIS - RS.1 Business continuity management NIS - RS.2 Disaster recovery management NIS - PR.10 - Physical and environmental security	ISO27002 - A.17.1 Information security continuity ISO27002 - A.17.2 Redundancies NIST - RC.RP Recovery Planning (1) CLC/TS50701 - SR 7.3 Control system backup CLC/TS50701 - SR 7.4 Control system recovery and reconstitution CLC/TS50701 - SR 7.5 Emergency power	

[27] French Hosting and Cloud company
[28] See https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU

5. CYBERSECURITY MEASURES

Once risks have been identified and prioritised according to risk evaluation criteria in relation to the incident scenarios that lead to those risks, they should be treated via a risk treatment plan. Four options are usually proposed regarding **risk treatment**[29] : risk modification, risk retention, risk avoidance and risk sharing.

- **Risk modification** is modifying the level of risk by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable.[30]
- **Risk retention** is accepting the risk without further action, if the level of risk meets the risks acceptance criteria.[31]
- **Risk avoidance** is avoiding the activity or condition that increases the particular risk.[32]
- **Risk sharing** is sharing the risk with another party that can most effectively manage the particular risk.[33]

As described in the ISO 27005 standard, these options must be selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. At the end of the process, no risk exceeding the risk acceptance criteria should be left. In order to reduce the identified risks to acceptable levels, appropriate security measures should be identified and prioritised. Security measures can be defined internally, using best practices and building a remediation plan tailored to the information system. However, a common practice is to use already-defined security measures published in security frameworks. These security frameworks often contain a list of controls or security requirements.

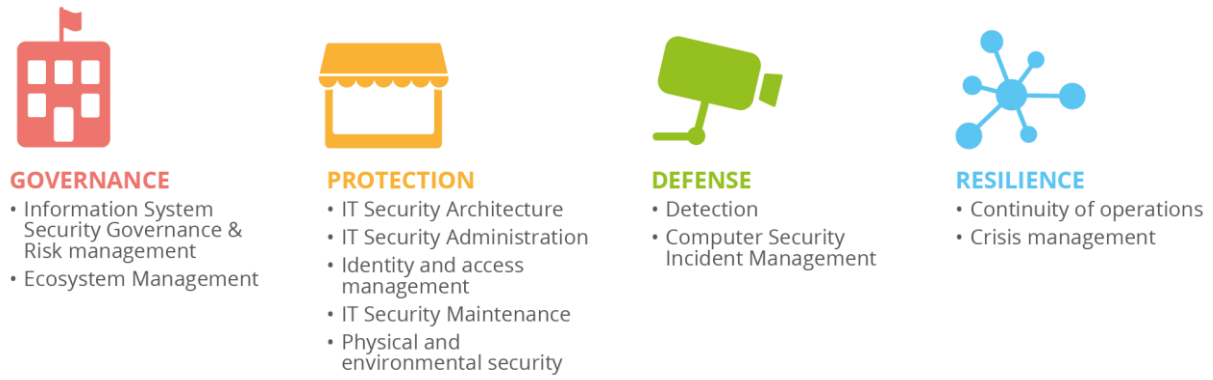
NIS Directive cybersecurity measures. The NIS cooperation group issued a list of security measures directed to OESs in a *Reference document on security measures for Operators of Essential Services*. The purpose of this list is "to provide Member States with a clear and structured picture of Member States' current and often common approaches to the security measures of OES".[34] The document examines a high number of domains where cybersecurity measures should be applied. For each domain, it gives a set of broad measures alongside their definitions (Figure 14).

These domains and measures could be used as the first basis for the risk treatment plan and complemented with measures from the CLC/TS 50701 regarding the OT cybersecurity and ISO/IEC 27002 security measures for IT cybersecurity.

Indeed, during the workshops, it was discovered that RUs and IMs often choose a two-step approach, by selecting a general framework for IT cyber risk treatment and complementing it with a more detailed, industry-driven one for the OT cyber risk treatment. ISA/IEC 62443 and CLC/TS 50701 are among the main references used for OT cybersecurity. For IT risk frameworks, NISD national security requirements, ISO27002 framework and the NIST Cybersecurity framework are among the more commonly used. Other less common frameworks have also been cited, such as the SANS Top 20 Critical Security Controls[35], or the Forrester Information Security Model[36].

[29] See for instance ISO 27005, chapter 9 Information security risk treatment
[30] See ISO 27005, chapter 9.2 Risk modification
[31] See ISO 27005, chapter 9.3 Risk retention
[32] See ISO 27005, chapter 9.5 Risk avoidance
[33] See ISO 27005, chapter 9.5 Risk sharing
[34] Reference document on security measures for Operators of Essential Services, p.5
[35] A list of 20 actions for cyber defence, that are close to the NIST 23 categories, and published by the SANS Institute, an organisation that provides information, resources, and training regarding cybersecurity.
[36] A security model declined in 123 security components (controls) divided into 25 functions and 4 domains has been cited. It is published by the market research company Forrester.

Figure 14: Domains of security measures for OESs (NIS Cooperation Group, 2018)



The ISO/IEC 27002 standard and Annex A' of ISO2001 describe requirements for information security management and a set of security controls[37]. These controls are organised in 12 categories[38]:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Operations security
- Communications security
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Similar to the NIS Directive security measures, ISO 27002 could be used as a basis for the risk treatment plan, and complemented with additional national security requirements, while OT systems could be complemented with CLC/TS 50701. Some measures from the NIST framework could also be used as they can be described in more detail.

The NIST Cybersecurity framework is accompanied by an exhaustive list of requirements. They are classified according to five functions (Identify, Protect, Detect, Respond, Recover) and 23 categories. Each of these categories contain a list of precise security requirements (over 900 in total). Those controls are also mapped against the ISA 62443 series and the ISO/IEC 27001:2013. The framework is quite detailed and focuses primarily on IT security. The NIST cybersecurity framework can be used as is and complemented by CLC/TS 50701 for OT railway systems requirements, or it can be used to complete another generic frameworks or standards, such as the ISO 27001 or the NIS Directive security requirements.

CLC/TS 50701 is based on or derived from **IEC 62443 series** standards. The purpose of the TS "is that, when a railway system is compliant to this TS, it can be demonstrated that this system is at the state of the art in terms of cybersecurity, that it fulfils its targeted Security Level and that its security is maintained during its operation and maintenance." It is best suited for industrial systems and designed specifically for the railway sector, as it applies to the Communications, Signalling and Processing domain, the Rolling Stock domain and to the Fixed Installations domain. It contains a list of security requirements for the OT components and services of the railway sector and thus

[37] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html
[38] ISO/IEC 27001 Standard - Information technology - Security techniques - Information security management systems – Requirements, p9

should be completed with a more generic approach, such as the ISO 27001, the NIST Cybersecurity Framework or the NIS Directive.

5.1 APPLYING CYBERSECURITY MEASURES

To help stakeholders implement the security measures, workshops were conducted with relevant experts and institutions to discuss challenges, priorities, and best practices. The purpose was to gather concrete feedback on the risk treatment plans.

Defining the list of measures that will be used was described as the top priority of the attendants of the workshops. To do so, operators draw a list of cybersecurity measures from known references. Assets' maturity is assessed against those measures, and measures that are not met are included in the list of security measures that must be applied to these assets. This list of security measures can also be used as a common basis for the manufacturers to implement minimum cybersecurity requirements by design or for security requirements to be included in contract specifications.

To define the set of measures that will be used, organisations also assess the level of compliance with national cybersecurity requirements (primarily according to the NIS Directive, but also against other requirements stemming from laws on national security, transport security or critical infrastructure protection).

During the workshops, stakeholders highlighted the importance of awareness raising and training sessions (especially against top threats, such as ransomware and phishing) or email security to prevent phishing. On the latter, the protection of endpoints and network segregation is also a top priority to reduce the risk of propagation of such attacks. As for OT security, the emphasis is placed mainly on network segregation and access control for critical systems. Adaptation of legacy systems is also a concern and should be considered as a priority, but it is also a big challenge, considering the complexity of updating systems with long lifecycles. Additionally, particular emphasis is placed on incident response.

Finally, applied security measures are often challenged by external audits or penetration testing. Some organisations use third parties to conduct such assessments. The systems tested can belong both on the IT and OT domains. In addition to technical audits, governance audits can also be conducted, such as an ISO-compliance audit. Furthermore, business continuity and recovery and incident response plans can also be tested with crisis exercises.

A challenge cited by multiple RUs and IMs is the management of relationships with third parties and ensuring that the products and services supplied meet cybersecurity requirements. Often, compliance with NIS Directive security requirements does not apply to third parties. To engage more with the industry and to encourage the implementation of cybersecurity measures, one solution could be to design a baseline at EU level to make the manufacturers and providers align their systems' compliance. Common baseline requirements should be reflected in tenders to allow for competing solutions achieving similar security capabilities across Europe. However, when considering minimum baseline requirements, there are risks involved, such as the minimum baseline not changing while the threat landscape changes, or that these minimum-security requirements do not meet the risks of the organisation. The use of EU certification schemes for IT or OT cybersecurity (should these become available) could be also a way to assess whether such requirements are met by the industry.

Another challenge that was identified is continuity, i.e., ensuring that the security level remains adequate and that the risks are continuously monitored. To do so, regular reviews and compliance assessments are needed. Maintaining an up-to-date threat landscape for the railway sector is equally important. An additional challenge is the separation between IT and OT, as it is often difficult to differentiate what is strictly OT from what is IT. In this case, it is difficult to know which controls to apply.

5.2 CYBERSECURITY MEASURES

To help stakeholders define cybersecurity measures, a list of controls from the NIS Directive has been mapped against various references (ISO27001, NIST CSF and CLC/TS50701[39]). It is up to the stakeholders to choose whether they will only select some measures from this list, use it as a basis for building their own list, or use it in entirety. Stakeholders should also remember that they may have to comply with national guidelines and specific

[39] The security measures of CLC/CS 50701 are matching the measures described in IEC 62443-3-3:2013.

national sectorial regulations. They should also verify which references apply to them and, if needed, complete the present list with the missing requirements.

The mapping was done in two phases: first, the references were reviewed and the most relevant measures were put in front of the NIS Directive measures, keeping these measures as the starting point of the review. Then, the reverse operation was carried out: the measures from the references that had been removed in the first phase were added to the most relevant NIS Directive measures. This ensures that all NIS Directive measures have been covered; and that all the other referenced measures are integrated into the mapping.

An example of a security measure is included below. It includes measures under the NIS Directive domain: Protection and the category of “Identity and Access Management”. The two measures of this category “Authentication and identification”, and “Access rights” are described according to the NIS Directive guidelines. They are then associated with relevant measures that can be found in ISO/IEC 27002, the NIST cybersecurity framework and CLC/TS50701.

A detailed list of security measures can be found in Annex C.

Table 1: Domain: Protection - Category: Identity and Access Management

Measure	Description	ISO/IEC 27002	NIST CSF	CLC/TS50701
NIS - PR.7 Authentication and identification	For identification, the operator sets up unique accounts for users or for automated processes that need to access resources of its Critical Information System (CIS). Unused or no-longer-needed accounts should be deactivated. A regular review process should be established.	A.9.1 Business requirements of access control A.9.3 User responsibilities A.9.4 System and application access control A.9.4.2 Secure log-on procedures A.9.4.3 Password management system	PR.AC Identity Management, Authentication and Access Control (1, 4, 6, 7) PR.DS Data Security (5)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 1.10 - Authenticator feedback SR 1.11 - Unsuccessful login attempts SR 1.12 - System use notification SR 1.13 - Access via untrusted networks SR 2.1 - Authorisation enforcement SR 2.2 - Wireless use control SR 2.3 - Use control for portable and mobile devices SR 2.4 - Mobile code SR 2.5 - Session lock SR 2.6 - Remote session termination SR 2.7 - Concurrent session control SR 5.2 - Zone boundary protection
NIS - PR.8 Access rights	Among the rules defined in its systems security policy, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its technical operations.	A.9.1 Business requirements of access control A.9.2 User access management A.9.4.4 Use of privileged utility programs A.9.4.5 Access control to program source code	ID.AM Assets management (5, 6) PR.AC Identity Management, Authentication and Access Control (1, 4, 6, 7) PR.DS Data Security (5) PR.PT Protective Technology (3)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 1.10 - Authenticator feedback SR 2.1 - Authorisation enforcement

6. CONCLUSIONS

European RUs and IMs use a combination of good practices, approaches, and standards to perform cyber risk management for their organisations. This report gathers insights on these current practices in a single document and can assist railway undertakings and infrastructure managers in their efforts to apply them. It provides examples of reference material, such as available taxonomies of assets and threats, comprehensive threats scenarios, derived from real incidents and cyber risk mitigation measures, derived by guidelines and standards.

The report also highlights the challenges faced when applying such approaches. Most importantly, there is a **lack of a single cyber risk management approach** for railway organisations to cover both IT and OT in a unified manner.

Railway organisations lack of a single cyber risk management approach to cover both IT and OT in a unified manner

IT vs OT risk management approaches. The differentiation between IT and OT in the railway sector is increasingly difficult and having discrete approaches and taxonomies for cyber risk management makes the issue more challenging. In many cases, it can be a complex process to identify which approach is better suited, whether a device can be considered IT or OT or which security measures and which standard should be applied. Having a more structured and unified approach with respect to cyber risk management would help the sector to harmonise, thus facilitating risk discussions between the different entities of the railway ecosystem. It can also enable more collaboration with the supply industry of the sector.

More harmonization and alignment of good practices. Future work could include further alignment of the sector-specific taxonomies and more guidance on the application of good practices. Wherever possible, further standardisation could be pursued, as this is also a request stemming from the railway supply industry, which advocates for more certification schemes at EU level. Significant sectoral challenges remain, including the cyber risk management of supply chains. This could be remedied with a regulatory approach encompassing the entire railway ecosystem under the same cyber risk management requirements. At present, key elements of the railway supply chain, both IT and OT, do not fall under the same European regulatory framework.

Keeping railway systems and cyber risk assessments up-to-date. Another significant issue specific to the sector is the plethora of legacy systems which add an additional degree of difficulty when managing cyber risk. At present, it is not possible to provide relevant recommendations to address the cybersecurity of legacy systems in the railway sector. It would be necessary to involve the railway industry in such an exercise. Additionally, even for newly developed systems, there is the need to ensure that the results of risk assessments remain current, that risks are continuously monitored, and that the security level remains adequate. Maintaining an up-to-date threat landscape for the railway sector could be a step towards this direction.

7. BIBLIOGRAPHY

CLC/TS 50701 Railway applications – Cybersecurity, 2021. https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/

Cyrail, 2018. CYRail Recommendations on cybersecurity of rail signalling and communication systems. September 2018. https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf

ENISA, 2016. ENISA Threat Taxonomy v 2016. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/

ENISA, 2020. Railway Cybersecurity - Security measures in the Railway Transport Sector. November 2020. https://www.enisa.europa.eu/publications/railway-cybersecurity

ENISA, 2021. Minimum Security Measures for Operators of Essentials Services (tool). https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.

IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

ISO 31000:2018, Risk management – Principles and guidelines.

ISO/IEC 27001: 2013, Information technology - Security techniques - Information security management systems – Requirements.

ISO/IEC 27002: 2013, Information technology - Security techniques - Code of practice for information security controls

ISO/IEC 27005: 2018, Information technology - Security techniques - Information security risk management.

ISO-IEC 62443 series. https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

NIS Cooperation Group, 2018. Reference document on security measures for Operators of Essential Services. CG Publication 01/2018, February 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

NIST Cybersecurity Framework, 2018. Cybersecurity Framework Version 1.1, April 2018. https://www.nist.gov/cyberframework

RCA OCORA Eulynx – CS Guideline, 2020. https://www.eulynx.eu/index.php/documents/rca/251-rca-publications

Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

UIC, 2018. Guidelines for cyber-security in railway, UIC-ETF, ISBN 978-2-7461-2732-6. https://www.shop-etf.com/en/guidelines-for-cyber-security-in-railways

X2Rail-1 Start-up activities for Advanced Signalling and Automation Systems (2016 - 2018). https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

X2Rail-1, 2019. Deliverable D8.2 - Security Assessment, rev.2. https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

X2Rail-3, Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication (2018 - 2020). https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

X2Rail3, 2020. Deliverable D8.1 - Guidelines for railway cybersecurity part 1 –Simplified Risk Assessment. December 2020. https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

A ANNEX: ASSET DESCRIPTIONS

Table 1: Assets per device category

Assets	Description	Attribute	Reference[40]
Telecom			
Radio transmission network	Radio network used for all railway processes: communication with trains, signalling, safety and security operations, logistics management, etc.	Network and communication systems	ENISA, 2020
Wired and wireless transmission network	Wired and wireless systems used for network communications in LAN or Internet connection.	Network and communication systems	ENISA, 2020
Operational telephone intercom	Telephone-related devices such as loudspeaker systems, walkie-talkies, etc.	Network and communication systems	ENISA, 2020
Mobile telephone devices (GSM)	GSM/GSM-R phone devices.	Network and communication systems	ENISA, 2020
IT & OT Infrastructure			
Computer & server	Computers and servers used as support goods by all IT & OT systems.	IT systems	ENISA, 2020
Infrastructures and trackside			
Automatic ticket distribution and verification infrastructures	Devices and equipment to distribute and control the tickets.	IT systems	-
CCTV (video surveillance)	Devices used for video surveillance of assets and people at risk.	OT systems	CLC/TS 50701
Fixed infrastructure detectors	Detectors such as track vacancy detectors, hot box detectors, avalanche detectors and fire detectors.	OT systems	CLC/TS 50701
Wayside equipment	Source and destination for information about approaching trains and their crews.	OT systems	-
Station signalling (automatic train protection, interlocking, radio block centre)	Equipment for station signalling regarding interlocking (safe setting of routes for trains by controlling signals, points, and the track vacancy), automatic train protection (ATP) or radio block centre (controls the movement authorities for the trains in an ETCS Level 2/3 system).	OT systems	CLC/TS 50701
Fixed communication tools (GSM-R, MSC/BSC)	Fixed devices to communicate with railway personnel and passengers.	Network and communication systems	CLC/TS 50701
Radio transmission relays	Relays antenna for radio communication.	Network and communication systems	CLC/TS 50701
Wired and wireless transmission internal network infrastructures	Equipment to support network communications.	Network and communication systems	CLC/TS 50701

[40] When a reference to a document is not given, the element was added based on the consultation with experts (workshops).

Assets	Description	Attribute	Reference[40]
Public Wi-Fi and internet accesses	Equipment to support public Wi-Fi and internet access.	Network and communication systems	CLC/TS 50701
On-Board			
On-board detectors	Various on-board detectors such as ATP, fire detectors, alarms, anti-intrusion tools, diagnostics tools and energy metering.	OT systems	CLC/TS 50701
Driver tools	On-board physical infrastructures related to driver tools: traction, braking driver machine interface, train control management tools. Traction is the system responsible for train movement. The driver machine interface includes all the technological objects used to manage communications between the train and the driver (e.g., screens, buttons, handles, etc.).	OT systems	CLC/TS 50701
Radio transmission relays	On-board equipment that communicates with the networks and allows the train to communicate with corporate IT systems.	Network and communication systems	CLC/TS 50701
Wired and wireless transmission internal network infrastructures	On-board equipment used for wired or wireless transmission on internal network (Mobile Communication Gateway, cab radio).	Network and communication systems	CLC/TS 50701
Public Wi-Fi and internet accesses	On-board equipment giving the users access to internet (through Wi-Fi, for example).	Network and communication systems	CLC/TS 50701
On-board CCTV	Equipment supporting CCTV on the train (cameras, recording systems), used for video surveillance of assets and people at risk.	IT systems	CLC/TS 50701

Table 2: Assets per service category

Assets	Description	Attribute	References[41]
Timetable construction			
Commercial offer construction	Systems which allow commercial offers to be created for customers, including timetables for each train line (track usage for railway undertakers and commercial offers of train tickets for passengers or freight).	IT Systems	ENISA, 2020
Staff planning	Systems which allow the preparation of resource rosters (assets and staff), providing the staff planning for all people working in railway (drivers, controllers, railway worker, station employee, maintenance workers, etc.)	IT systems	ENISA, 2020
Resources booking	Systems which allow resource booking (locomotive, wagon, etc.)	IT systems	ENISA, 2020
Sales, distribution, and customers relations			
Marketing	Systems that allow the management of customer relations (e.g., claims, loyalty cards, marketing campaigns).	IT systems	ENISA, 2020
Booking management	Systems enabling customers to buy tickets or book a train seat, including commercial websites and applications.	IT systems	ENISA, 2020
Automatic fare collection	Systems enabling the automatic collection of customers' fares.	IT systems	ENISA, 2020

[41] When a reference to a document is not given, the element was added based on the consultation with experts (workshops).

Assets	Description	Attribute	References[41]
Network allocation systems			
Operation planning construction	Systems enabling RUs to construct and plan operations and to inform the IMs of any special characteristics of trains or loads (e.g., dangerous goods, oversize).	IT systems	ENISA, 2020
Operation billing	Systems enabling IMs to apply costing policies to the RU for the use of the infrastructure.	IT systems	ENISA, 2020
Corridors booking	Systems enabling RUs to book infrastructure (corridors) to operate their trains on the network	IT systems	ENISA, 2020
Assets management			
Asset inventory	Systems enabling RUs and IMs to inventory their assets.	IT systems	ENISA, 2020
Logistics	Systems enabling RUs and IMs to manage their asset logistics.	IT systems	ENISA, 2020
Asset procurement	Systems enabling RUs and IMs to account for their assets (infrastructure, or trains for example), and to procure new assets.	IT systems	ENISA, 2020
Signalling			
Remote monitoring	Systems used to direct railway traffic and oversee the monitoring of train locations on tracks.	OT systems	ENISA, 2020
Key management	Systems used to direct railway traffic and secure communication between trains.	OT systems	ENISA, 2020
Juridical recorder unit	Systems used to direct railway traffic and record events on trains complying with the ERTMS/ETCS standard.	OT systems	ENISA, 2020
Temporary speed restriction	Systems used to direct railway traffic and reduce the speed of rail traffic to ensure safe passage on unsafe sections of tracks.	OT systems	ENISA, 2020
Interlocking	Systems used to direct railway traffic and prevent conflict in signalling movements through an arrangement of tracks. It includes wayside systems that give information on approaching trains and their crews.	OT systems	ENISA, 2020
Automatic train protection	Systems which activate emergency brakes if train speed is faster than allowed.	OT systems	ENISA, 2020
Command-Control			
Train control	Master system to control all train elements (speed, doors, etc.).	OT systems	ENISA, 2020
Automatic train control	System responsible for speed control in response to external inputs.	OT systems	ENISA, 2020
Automatic train supervision	Systems used to enable movement of trains and manage traffic loads.	OT systems	ENISA, 2020
Energy traction	System overseeing the supply of the electrified rail network.	OT systems	ENISA, 2020
Freight docking	Systems and services related to freight docking: loading and unloading of goods, cranes, and platforms management.	OT systems	-
Auxiliary			
Energy	System overseeing the management of power delivery.	OT systems	ENISA, 2020
Heating, ventilating and air conditioning (HVAC)	System overseeing the management of heating, ventilation, and air conditioning.	OT systems	ENISA, 2020
Lighting	System overseeing the management of lighting.	OT systems	ENISA, 2020
Water	System overseeing the management of water.	OT systems	-
Escalator and elevator	System overseeing the management of escalators and elevators.	OT systems	-

Assets	Description	Attribute	References[41]
Development			
Bidding management systems	Bidding systems for the RU or IM to answer invitations to tender for train operations or infrastructure management.	IT systems	ENISA, 2020
Research and engineering systems	Centralise and coordinate research and engineering.	IT systems	ENISA, 2020
Passenger services			
Passenger announcement	System overseeing the passenger announcement management.	IT systems	ENISA, 2020
Passenger information	System managing the passenger's general information about their trip: track number, time of arrival, delay, etc.	IT systems	ENISA, 2020
Passenger entertainment	System overseeing the management of passenger entertainment (internet access...).	IT systems	ENISA, 2020
Telecom			
Operational time distribution system	System which synchronises the clocks of the different IT equipment (servers, workstations, etc.).	Network and communication systems	ENISA, 2020
Security			
Access control	System allowing the control of physical access within buildings.	OT systems	ENISA, 2020
CCTV	Video-surveillance systems.	OT systems	ENISA, 2020
Network monitoring	Network intrusion detection systems to detect abnormal activities.	IT systems	ENISA, 2020
Cybersecurity	Devices and software allowing cybersecurity activities: surveillance (SOC), firewalls, Endpoint Detection and Response systems.	IT systems	ENISA, 2020
Safety			
Fire detection	Systems managing fire detection within buildings, stations, or datacentres.	OT systems	ENISA, 2020
Emergency telephony and alerting	System managing operational communication and sending alerts in case of emergency.	OT systems	ENISA, 2020
Operations safety	Systems that keep operations safe and secure.	OT systems	ENISA, 2020
Maintenance			
Asset inventory	Systems enabling RUs and IMs to create an inventory of their assets related to maintenance (parts, equipment, etc.).	IT systems	ENISA, 2020
Diagnosis	System overseeing direct diagnosis or tele-diagnosis with GSM communication from the train.	IT systems	ENISA, 2020
Maintenance scheduling	System scheduling and operating maintenance activities on track and trains.	IT systems	ENISA, 2020
Service provisioning	Systems enabling the provision of maintenance equipment.	IT systems	-
Corporate & Support			
IT ticketing systems	IT ticketing systems to create and attribute tickets detailing IT users' technical or help requests.	IT systems	ENISA, 2020
Resource allocation systems	System overseeing the management of allocation of resources used by RUs and IMs to perform usual business.	IT systems	ENISA, 2020

Assets	Description	Attribute	References[41]
Documentation systems / Document management	System overseeing the management of documents (shared folders, SharePoint, OneDrive, etc.).	IT systems	ENISA, 2020
Alert escalation and crisis management	Process and system used in case of crisis, in order to escalate and manage the situation.	IT systems	ENISA, 2020
Administrative telephone systems	Administration of the telephone systems used by employees.	IT systems	ENISA, 2020
Administrative time distribution	Network Time Protocol (NTP) systems that provide time management for all systems.	IT systems	ENISA, 2020
Finance	Manages all financial aspects (accounting, consolidation)..	IT systems	ENISA, 2020
HR	System for employee management: recruitment, pay, training, evaluation, etc.	IT systems	ENISA, 2020
IT-related (equipment, services) system supply	Vendor systems for IT services and equipment.	Supply chain	-

Table 3: Assets per physical equipment category (description)

Assets	Description	Reference[42]
On-Board		
Doors	Sub-system that controls the train doors.	CLC/TS 50701
On-board lighting	On-board physical infrastructures related to lighting. Includes the electronics dedicated to ensuring correct illumination of railway cars both internally and externally; special case of external lighting are headlights.	CLC/TS 50701
Heating, ventilating and air conditioning (HVAC)	On-board physical infrastructures related to heating, ventilating and air conditioning. This system provides crew and passengers with ambient comfort conditions.	CLC/TS 50701
Train	Physical equipment of trains including embedded devices and their software.	-
Freight locomotives	On-board physical infrastructures related to freight locomotives.	-
Special wagons (Container transport, oil transport, refrigerated)	On-board physical infrastructures related to special wagons.	-
On-board system supply	On-board physical infrastructures related to the system supply.	-
Infrastructure and trackside		
Energy systems supply	Infrastructures that support providing energy to all facilities.	-
Tracks	All physical equipment and infrastructures related to tracks.	-
Catenary	Supply of electric energy to trains.	-

[42] When a reference to a document is not given, the element was added based on the consultation with experts (workshops).

Assets	Description	Reference[42]
Train assembly facility	Facilities where trains are assembled.	-
Stations - buildings	All buildings used for train stations.	CLC/TS 50701
Other buildings (Administrative, facilities, …)	All building used for corporate, IT or OT purposes.	-
Electrical substations	Physical infrastructures that support electrical substations.	CLC/TS 50701
Level crossing	Physical infrastructures supporting level crossings. Protects the crossing area of rail and road traffic.	CLC/TS 50701
Tunnels and bridges	Physical infrastructures related to bridges or tunnels. "Tunnels" includes the electronics installed in railway tunnels to support tunnel specific infrastructure functions (e.g., ventilation, alarm systems, fire and smoke detectors, fire extinguisher, etc.) "Bridges" includes the electronics installed in railway bridges to support bridge specific infrastructure functions (e.g., monitoring systems, lift control, etc.)."	-
Escalators and elevators	Physical infrastructures related to escalators or elevators that allow passengers and employees' to move in buildings and infrastructures.	ENISA, 2020
Lighting	Physical infrastructures related to lighting.	ENISA, 2020
Water control	Physical infrastructures related to water control (wells, etc.).	-
Fire management	Physical infrastructures related to fire management (fire extinguisher, etc.)	-
Freight docking platform	Physical infrastructures related to freight docking platforms, allowing loading and unloading of goods.	-
Goods storage facilities	Physical infrastructures related to goods storage (such as containers).	-
Heating, ventilating and air conditioning (HVAC)	Heating and ventilating equipment, providing crew and passengers with ambient comfort conditions.	CLC/TS 50701

Table 4: People and data (description)

Assets	Description
Data, Information and Knowledge	
Email	Data used by email systems.
Telephone	Data used by telephone systems.
Clients' personal information	Name, address, credit card information, usage, etc.
Employee personal information	Name, address, salary, etc.
Asset inventory data	Asset-related data.
Support tickets	Tickets sent to support to detail users requests.
Commercial, financial, administration data	Data related to the commercial, financial or administrative information and activities.
CCTV data	Video tapes, recording, etc.
IT infrastructure data	Architecture figures, flow matrix, etc.
Research and engineering data	Data related to research and engineering activities.
Maintenance data	Train status, maintenance operations, etc.
Train or traffic data	Train location, train course, etc.
Audit (audit trail, logs)	Audits reports, audit trail, logs.
Systems maintenance data	Backups, configurations, audit, log, install images, licenses, certificates, etc.
Supply chain data/knowledge (providers, contracts, service management records)	Providers, data, contracts, service met records.
IT systems data (for critical systems not mentioned)	Data used in IT systems: IP mapping tables, credentials, etc.
OT systems data	Data used for control of the systems (e.g., signalling systems data to and from train, to and from trackside elements).
Freight information	Asset-related data.
People	
Passengers	People using train services.
Drivers	Employees driving trains.
Controllers	Employees in charge of controlling passengers' tickets.
Railway workers	Employees in charge of the railway.
Station employees	Employees in charge of managing the stations.
Maintenance workers	Employees in charge of the maintenance (train or tracks).
HR	Employees in charge of HR.
Executives	Company's executive staff.
Marketing, communication, finance teams	Employees in charge of marketing, communication, or finance.
Administrator teams	Employees in charge of administrating the systems.
IT teams	Employees in charge of IT.

B ANNEX: THREATS DESCRIPTION

Table 5: Threat categories and descriptions

Threats	Description
Disaster (natural, environmental)	
Natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds, solar eruptions, thunder stroke, pollution, dust, corrosion, water, explosion, animal damages (rats, squirrels, etc.)	Disastrous events caused by natural or environmental elements.
Unintentional damage / loss of information or systems	
Information leakage/sharing due to human error	Confidential data shared involuntarily by a member of the organisation via the information system (emails, social network...).
Erroneous use or administration of devices and systems	Error in the use or administration of the organisation's assets leading to information leakage, damage to such assets or physical harm.
Using information from an unreliable source	Using information in the organisation's processes and systems from a non-verified, non-official source, or an official but corrupted source.
Unintentional change of data in an information system	Harmful modification of data, mistakenly done by a member of the organisation.
Inadequate design and planning or improper adaptation	Error in the design of a system or its planning or delivery, leading to system unavailability.
Damage caused by a third party (supplier or partner)	Unintentional damage caused by a supplier or a partner.
Damages resulting from penetration testing	Unintentional damage caused by an IT team during a penetration test of an information system.
Loss of (integrity of) sensitive information	Loss of sensitive information, or unwanted modification of sensitive information, leading to the unavailability of the necessary data.
Destruction of records	Loss of recorded information in IT systems (back up) or OT systems (train system records or similar).
Physical attack (deliberate/ intentional)	
Fraud by passengers	Every type of fraud committed by a passenger, aiming at diverting the organisation's resources, particularly fraud regarding tickets or subscription.
Sabotage / Vandalism	All type of acts aiming at physically destroying or harming the organisation's properties.
Theft (devices, storage media and documents)	Theft of physically available resources.
Information leakage / sharing from document / equipment	Information publicly and physically leaked or shared by a member of the organisation, whether voluntarily or not (via the passenger announcement system, for instance).
Unauthorised physical access / Unauthorised entry to premises	Access to the organisation premises by a non-authorised person.
Coercion, extortion, or corruption	All type of pressure directed toward members or the organisation or stakeholders to gain an advantage over the organisation.
Damage from the warfare / Terrorist attack / Activist attack	All damages originating from a large organisation (country, terrorist group or other similar organisation) or damages that are ideologically motivated.

Threats	Description
Failures / Malfunction	
Failure / malfunction of devices or systems	Natural dysfunction or dysfunction stemming from a misconfiguration on a device or a system.
Failure / malfunction / disruption of communication links	Natural dysfunction or dysfunction stemming from a misconfiguration, on the communication networks.
Failure / malfunction / disruption of service providers (supply chain)	Natural dysfunction or dysfunction stemming from a misconfiguration on the services provided by the suppliers.
Outages	
Loss of resources	Unavailability of provided resources (maintenance parts, etc.).
Loss of electricity	Unavailability of electricity.
Loss of cooling	Unavailability of cooling.
Loss of oil or gas	Unavailability of oil or gas.
Absence of personnel (strike, pandemic, etc.)	Absence of key personnel (strike, pandemic, etc.).
Low competency or maturity of personnel	Personnel lacking competency to correctly and efficiently complete tasks causing unavailability of assets or services.
Internet outage	Unavailability of the services provided by the global internet suppliers.
Mobile communication outage	Unavailability of mobile (GSM) communication services.
Network outage	Unavailability of the organisation's network communication due to network dysfunction (natural or not).
Malicious Activity / Abuse	
Identity theft (Identity fraud/ Account)	Theft of a systems' legitimate user's identity: account theft, authentication means' theft (login, password, email, etc.).
Unsolicited E-Mail	Phishing or spear-phishing email to retrieve a stakeholders' credentials, or e-mail designed to retrieve sensitive information via social engineering.
Denial of service	Cyber-attack that aims at making a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
Malicious code/ software/ activity	Piece of code or software that infects a host (computers, servers, etc.) to harm an information system in various ways. This includes ransomwares, trojan horses, viruses, worms., etc.
Social engineering	Psychological manipulation of people into performing actions on the information systems or divulging confidential information.
Generation and use of rogue certificates	Legitimate certificates that have been compromised or forged to trick a system in thinking the certificate's user is legitimate and can access the protected resources.
Manipulation of hardware and software	Malicious changes in hardware or software configuration or code to cause harm to the information system.
Manipulation of information	Malicious breach of data integrity or transmission of false information.
Fraud by authorised personnel	Every type of fraud committed by authorised personnel aiming at diverting the organisation' resources.
Unauthorised use or administration of devices and systems	Unauthorised use or administration of the organisation's assets leading to information leakage, damage to such assets or physical harm.
Unauthorised use of software	Unauthorised use of a legitimate software leading to information leakage, damage to such assets or physical harm.

Threats	Description
Network Intrusion	Unauthorised access to a network, giving access to network resources.
Unauthorised installation of software	Installation of a software not allowed on a computer or server. This can create vulnerabilities that are not under control of the company.
Compromising confidential information (data breaches)	Intentional confidential data leakage from authorised or unauthorised access.
Targeted attacks (APTs etc.)	An attacker gains unauthorised access to a computer network and resources, remaining undetected for an extended period.
Brute force	Access to a protected resource using crafted passwords or passphrases with many trials to find the associated access credentials.
Abuse of authorisations	Legitimate users who use their authorisations for fraud or stealing sensitive data.
Interception of information	Physical interception of information (eavesdropping).
Network reconnaissance, network traffic manipulation and information gathering	Interception and identification of information about networks to identify security weaknesses.
Man in the middle / Session hijacking	Interception of information between two endpoints in information systems (computers, servers, etc.)

C ANNEX: SECURITY MEASURES

Table 6: Governance

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
Information System Security Governance & Risk Management					
NIS - GV.1	Security risk analysis	The operator conducts and regularly updates a risk analysis, identifying its Critical Information Systems (CIS) underpinning the provision of the essential services of OESs and identifies the main risks to these CIS.	6.1 Actions to address risks and opportunities 8 Operation 9.3 Management review 10 Improvement A.8.1 Responsibility for assets A.12.6.1 Management of technical vulnerabilities A.18.2.1 Independent review of information security	ID.GV Governance (4) ID.RA Risk Assessment (1, 3, 4, 5, 6) ID.RM Risk Management Strategy (1, 2, 3) RS.IM Improvements (1, 2) ID.SC Supply Chain Risk Management (1) PR.IP Information Protection Processes and Procedures (12) ID.AM Assets management (1, 2, 4, 5) DE.CM Security Continuous Monitoring (8) RS.MI Mitigation (3) RS.AN Analysis (5)	SR 7.8 - Control system component inventory *See sections 6 and 7 of CLC/TS50701 and IEC 62443-2-1 (section 4.2)*
NIS - GV.2	Security policy	The operator establishes, maintains and implements an information system security policy (ISSP) approved by senior management, guaranteeing high-level endorsement of the policy.	4.3 Determining the scope of the information security management system 4.4 Information security management system 5.1 Leadership and commitment 5.2 Policy 5.3 Organisational roles, responsibilities and authorities 6.2 Information security objectives and planning to achieve them 9.3 Management review A.5.1 Management direction for information security A.6.1 Internal organisation A.7.2.1 Management responsibilities A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights A.18.2.2 Compliance with security policies and standards	ID.BE Business Environment (1,2,3,4) ID.GV Governance (1,2,3,4) PR.AT Awareness & Trainings (2,3 4,5) DE.DP Detection Processes (1) ID.AM Assets Management (6)	*See IEC 62443-2-1 (section 4.3.2)*

NIS - GV.3	Security accreditation	Building on the risk analysis and according to an accreditation process referred to in the ISSP, the operator accredits the CIS identified in its information system risk analysis, including, inter alia, the inventory and architecture of the administration components of the CIS.	6.1 Actions to address risks and opportunities 8 Operation 9.2 Internal audit 10.1 Nonconformity and corrective action A.12.1.1 Documented operating procedures A.12.7.1 Information systems audit controls	ID.RA Risk Assessment (1,3,4,6) ID.RM Risk Management Strategy (1, 2, 3) RS.IM Improvements (1, 2) ID.SC Supply Chain Risk Management (1) PR.IP Information Protection Processes and Procedures (7, 12) PR.PT Protective Technology (1) ID.AM Assets management (1, 2, 4, 5) DE.CM Security Continuous Monitoring (8) RS.MI Mitigation (3)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation
NIS - GV.4	Security indicators	For each CIS and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organisation's performance, the maintaining of resources in secure conditions, users' access rights, authenticating access to resources, and resource administration.	6.2 Information security objectives and planning to achieve them 7.1 Resources 7.2 Competence 9 Performance evaluation A.12.1.3 Capacity Management	ID.AM Assets Management (5) ID.RM Risk Management Strategy (2, 3) PR.IP Information Protection Processes and Procedures (7, 8) PR.DS Data Security (4) ID.BE Business Environment (5)	SR 3.4 - Software and information integrity SR 4.1 - Information confidentiality
NIS - GV.5	Security audit	The operator establishes and updates a policy and procedures for performing information system security assessments and audits of critical assets and CIS, taking into account the regularly updated risk analysis.	6 Planning 8 Operation 9.2 Internal audit 9.3 Management review 10 Improvement A.5.1 Management direction for information security A.12.1 Operational procedures and responsibilities A.12.7 Information systems audit considerations A.18.2 Information security reviews	ID.GV Governance (3, 4) ID.RA Risk Assessment (1, 3, 4, 5, 6) ID.RM Risk Management Strategy (2, 3) DE.CM Security Continuous Monitoring (8) DE.DP Detection Processes (5) ID.SC Supply Chain Risk (4) PR.AC Identity Management, Authentication and Access Control (1) PR.PT Protective Technology (1) PR.IP Information Protection Processes and Procedures (7, 12) RS.IM Improvements (1, 2) RC.IM Improvements (1, 2)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation
NIS - GV.6	Human resource security	The established information system security policy has a CIS security awareness raising program for all staff and a security training programme for employees with CIS-related responsibilities.	4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 5.3 Organisational roles, responsibilities, and authorities 6.2 Information security objectives and planning to achieve them 7 Support	ID.AM Assets Management (6) ID.GV Governance (2, 3) RS.CO Communications (1) PR.IP Information Protection Processes and Procedures (7, 11, 12) DE.DP Detection Processes (1) PR.AT Awareness & Trainings (1, 2, 3 4, 5)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.9 - Strength of public key authentication

			9.1 Monitoring, measurement, analysis and evaluation A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties A.7.2 During employment A.7.1 Prior to employment (screening and terms & conditions) A.7.3 Termination and change of employment A.9.3 User responsibilities		SR 2.1 - Authorisation enforcement SR 5.2 - Zone boundary protection
Ecosystem Management					
NIS - GV.7	Ecosystem mapping	The operator establishes a mapping of its ecosystem, including internal and external stakeholders. This mapping may include suppliers, in particular those with access to or managing operator's critical assets.	4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 5.2 Policy 5.3 Organisational roles, responsibilities and authorities 8.1 Operational planning and control A.8 Asset management A.8.2 Information classification A.15 Supplier relationships	ID.AM Assets Management (3, 4, 6) ID.BE Business Environment (1,2,4) ID.AM Assets Management (6)	SR 5.3 – General purpose person-to-person communication restrictions
NIS - GV.8	Ecosystem relations	The operator establishes a policy for its relations with its ecosystem in order to mitigate the potential risks identified. This includes but is not limited to interfaces shared between the CIS and third parties.	4.2 Understanding the needs and expectations of interested parties 5.2 Policy 7.4 Communication 7.5 Documented information 8.1 Operational planning and control 9.3 Management review A.5.1 Management direction for information security A.7.1 Prior to employment A.7.2 During employment A.7.3 Termination and change of employment A.12.7 Information systems audit considerations A.13.2 Information transfer A.14.2 Security in development and support processes A.15 Supplier relationships A.18.1 Compliance with legal and contractual requirements	RS.CO Communications (4, 5) ID.RM Risk Management Strategy (1) ID.GV Governance (2) ID.SC Supply Chain Risk (1, 2, 3, 4, 5) RC.CO Communications (3)	SR 1.13 - Access via untrusted networks SR 2.6 - Remote session termination SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.1 - Communication integrity SR 3.5 - Input validation SR 3.8 - Session integrity SR 4 - Data confidentiality SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.3 - General purpose person-to-person communication restrictions SR 6.1 - Audit log accessibility SR 6.2 - Continuous monitoring SR 7.1 - Denial of service protection SR 7.6 - Network and security configuration setting

Table 7: Protection

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
IT Security Architecture					
NIS - PR.1	Systems configuration	The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS.	4.3 Determining the scope of the information security management system A.6.2 Mobile devices and teleworking A.8.1 Responsibility for assets A.8.3 Media handling A.12.1 Operational procedures and responsibilities A.12.5 Control of operational software A.12.6 Technical vulnerability management A.13.1 Network security management A.14.1 Security requirements of information systems A.14.2 Security in development and support processes	PR.IP Information Protection Processes and Procedures (1, 2, 3) DE.AE Anomalies and Events (1) PR.PT Protective Technology (3)	SR 1.13 - Access via untrusted networks SR 2.2 - Wireless use control SR 2.3 - Use control for portable and mobile devices SR 2.4 - Mobile code SR 2.6 - Remote session termination SR 3.1 - Communication integrity SR 3.3 - Security functionality verification SR 3.4 - Software and information integrity SR 3.5 - Input validation SR 3.8 - Session integrity SR 4.1 - Information confidentiality SR 4.2 - Information persistence SR 4.3 - Use of cryptography SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.3 - General purpose person-to-person communication restrictions SR 7.1 - Denial of service protection SR 7.2 - Resource management SR 7.6 - Network and security configuration settings SR 7.7 - Least functionality SR 7.8 - Control system component inventory
NIS - PR.2	System segregation	The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems.	A.12.1 Operational procedures and responsibilities A.13.1 Network security management	PR.DS Data Security (5, 7) PR.PT Protective Technology (3, 4) PR.AC Identity Management, Authentication and Access Control (5, 6)	SR 1.13 - Access via untrusted networks SR 2.6 - Remote session termination SR 3.1 - Communication integrity SR 3.5 - Input validation SR 3.8 - Session integrity SR 4.1 - Information confidentiality SR 4.2 - Information persistence SR 4.3 - Use of cryptography SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.3 - General purpose person-to-person communication restrictions SR 5.4 - Application partitioning SR 7.1 - Denial of service protection SR 7.6 - Network and security configuration settings

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
NIS - PR.3	Traffic filtering	The operator filters traffic flows circulating in its CIS. The operator therefore forbids traffic flows that are not needed for the functioning of its systems and that are likely to facilitate an attack.	8.1 Operational planning and control A.13.1 Network security management A.13.2 Information transfer	PR.DS Data Security (2) PR.PT Protective Technology (4) PR.AC Identity Management, Authentication and Access Control (3, 5) DE.CM Security Continuous Monitoring (6, 7)	SR 1.13 - Access via untrusted networks SR 2.6 - Remote session termination SR 3.1 - Communication integrity SR 3.5 - Input validation SR 3.8 - Session integrity SR 4.1 - Information confidentiality SR 4.2 - Information persistence SR 4.3 - Use of cryptography SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.3 - General purpose person-to-person communication restrictions SR 7.1 - Denial of service protection SR 7.6 - Network and security configuration settings
NIS - PR.4	Cryptography	In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in its CIS.	A.10.1 Cryptographic controls A.18.1 Compliance with legal and contractual requirements	ID.GV Governance (3) PR.DS Data Security (1, 2, 5, 6, 8) PR.PT Protective Technology (4)	SR 4.3 - Use of Cryptography SR 5.2 - Zone boundary protection
IT Security Administration					
NIS - PR.5	Administration accounts	The operator sets up specific accounts for the administration, to be used only for employees that are carrying out administrative operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list.	A.9.2 User access management A.12.4.3 Administrator and operator logs	PR.AC Identity Management, Authentication and Access Control (1, 4, 7) PR.AT Awareness & Trainings (2, 4)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 2.1 - Authorisation enforcement

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
NIS - PR.6	Administration information systems	Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorised to carry out administration operations.	A.9.3.1 Use of secret authentication information A.9.4 System and application access control A.12.1.4 Separation of development, testing and operational environments A.12.4.3 Administrator and operator logs	PR.AC Identity Management, Authentication and Access Control (1, 3, 4, 6, 7) PR.DS Data Security (5, 6, 7) PR.AT Awareness & Trainings (2, 3, 4) PR.PT Protective Technology (4)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 1.10 - Authenticator feedback SR 2.1 - Authorisation enforcement SR 5.2 - Deny by default, allow by exception SR 6.1 - Audit log accessibility
Identity and access management					
NIS - PR.7	Authentication and identification	For identification, the operator sets up unique accounts for users or for automated processes that need to access CIS resources. Unused or no longer needed accounts are to be deactivated. A regular review process should be established.	A.9.1 Business requirements of access control A.9.3 User responsibilities A.9.4 System and application access control A.9.4.2 Secure log-on procedures A.9.4.3 Password management system	PR.AC Identity Management, Authentication and Access Control (1, 4, 6, 7) PR.DS Data Security (5)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 1.10 - Authenticator feedback SR 1.11 - Unsuccessful login attempts SR 1.12 - System use notification SR 1.13 - Access via untrusted networks SR 2.1 - Authorisation enforcement SR 2.2 - Wireless use control SR 2.3 - Use control for portable and mobile devices SR 2.4 - Mobile code SR 2.5 - Session lock SR 2.6 - Remote session termination

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
					SR 2.7 - Concurrent session control SR 5.2 - Zone boundary protection
NIS - PR.8	Access rights	Among the rules defined in its ISSP, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its technical operations.	A.9.1 Business requirements of access control A.9.2 User access management A.9.4.4 Use of privileged utility programs A.9.4.5 Access control to program source code	ID.AM Assets management (5, 6) PR.AC Identity Management, Authentication and Access Control (1, 4, 6, 7) PR.DS Data Security (5) PR.PT Protective Technology (3)	SR 1.1 - Human user identification and authentication SR 1.2 - Software process and device identification and authentication SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5 - Authenticator management SR 1.6 - Wireless access management SR 1.7 - Strength of password-based authentication SR 1.8 - Public key infrastructure (PKI) certificates SR 1.9 - Strength of public key authentication SR 1.10 - Authenticator feedback SR 2.1 - Authorisation enforcement
IT Security Maintenance					
NIS - PR.9	IT security maintenance procedure	The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this end, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources.	6.2 Information security objectives and planning to achieve them 7.5.3 Control of documented information 8.1 Operational planning and control 10.1 Nonconformity and corrective action A.8.2 Information classification A.11.2 Equipment A.12.1.2 Change management A.12.6.1 Management of technical vulnerabilities A.13.1 Network security management A.14.1 Security requirements of information systems A 14.2 Security in development and support processes A.14.3 Test data A.15.2 Supplier service delivery management	PR.MA Maintenance (1,2) PR.IP Information Protection Processes and Procedures (1, 2, 3, 4, 7) PR.DS Data Security (3, 4) ID.SC Supply Chain Risk (4)	SR 3.1 - Communication integrity SR 3.3 - Security functionality verification SR 3.4 - Software and information integrity SR 3.8 - Session integrity SR 6.1 - Audit log accessibility SR 7.6 - Network and security configuration settings

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
Physical and environmental security					
NIS - PR.10	Physical and environmental security	The operator prevents unauthorised physical access and damage to, and interference with the organisation's information and information processing facilities.	A.6.2 Mobile devices and teleworking A.8.1 Responsibility for assets A.11 Physical and environmental security	ID.AM Assets management (1, 4) DE.CM Security Continuous Monitoring (2, 3, 6) PR.IP Information Protection Processes and Procedures (5, 6) PR.AC Identity Management, Authentication and Access Control (2, 3) PR.DS Data Security (3) PR.PT Protective Technology (2, 5)	SR 1.13 - Access via untrusted networks SR 2.6 - Remote session termination SR 2.8 - Auditable events SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failures SR 2.1 - Timestamps SR 2.12 - Non-repudiation SR 4.2 - Information persistence SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 7.5 - Emergency power SR 7.8 - Control system component inventory

Table 8: Defence

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
			Detection		
NIS - DF.1	Detection	The operator sets up a security incident detection system of the "analysis probe for files and protocols" type. The analysis probes for files and protocols analyses the data flows transiting through those probes to seek out events likely to affect the security of the CIS.	9.1 Monitoring, measurement, analysis and evaluation A.12.2 Protection from malware A.12.4 Logging and monitoring A.12.6.1 Management of technical vulnerabilities A.15.2.1 Monitoring and review of supplier services	PR.DS Data Security (6, 8) DE.AE Anomalies and Events (1, 5) DE.CM Security Continuous Monitoring (1, 2, 3, 4, 5, 6, 7) DE.DP Detection Processes (1, 2, 3) PR.PT Protective Technology (1)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.1 - Communication integrity SR 3.2 – Malicious code protection SR 3.3 - Security functionality verification SR 3.4 - Software and information integrity SR 3.8 - Session integrity SR 3.9 - Protection of audit information SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.4 - Application partitioning SR 6 - Timely response to events
NIS - DF.2	Logging	The operator sets up a logging system on each CIS to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the CIS.	9.1 Monitoring, measurement, analysis and evaluation A.12.4 Logging and monitoring A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.18.1.3 Protection of records	ID.RA Risk Assessment (1) ID.SC Supply Chain Risk Management (1) PR.MA Maintenance (1,2) DE.CM Security Continuous Monitoring (1, 2, 3, 6, 7) DE.AE Anomalies and Events (3) RS.MI Mitigation (3) PR.PT Protective Technology (1)	SR 1.12 - System use notification SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.9 - Protection of audit information SR 6 - Timely response to events SR 6.2 – Continuous monitoring SR 7.8 – Control system component inventory
NIS - DF.3	Log correlation and analysis	The operator creates a log correlation and analysis system that mines the events recorded by the logging system installed on each of the CIS to detect events that affect CIS security.	9.1 Monitoring, measurement, analysis and evaluation 9.3 Management review A.16.1.4 Assessment of and decision on information security events A.16.1.7 Collection of evidence	ID.RA Risk Assessment (4, 5) PR.PT Protective Technology (1) DE.AE Anomalies and Events (2, 3, 4) DE.DP Detection Processes (3, 4, 5) PR.IP Information Protection Processes and Procedures (7) RS.AN Analysis (1, 5)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.9 - Protection of audit information SR 6 - Timely response to events

Computer Security Incident Management					
NIS - DF.4	Information system security incident response	The operator creates, keeps up-to-date and implements a procedure for handling, responding to and analysing incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.	A.16.1 Management of information security incidents and improvements A.16.1.7 Collection of evidence	ID.RA Risk Assessment (3, 4, 5, 6) ID.SC Supply Chain Risk Management (5) PR.IP Information Protection Processes and Procedures (9, 10) RS.AN Analysis (1, 2, 3, 4, 5) RS.MI Mitigation (1, 2, 3) RS.IM Improvements (1, 2) RS.CO Communications (1, 3, 4, 5) RS.RP Response Planning (1) RC.RP Recovery Planning (1) RC.CO Communications (2)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.9 - Protection of audit information SR 5.1 - Network segmentation SR 5.2 - Zone boundary protection SR 5.4 - Application partitioning SR 6 - Timely response to events
NIS - DF.5	Incident reporting	The operator creates, keeps up-to-date and implements procedures for incidents reporting.	7.5 Documented information A.12.1 Operational procedures and responsibilities A.16.1 Management of information security incidents and improvements	RS.CO Communications (2, 3, 4, 5) DE.DP Detection Processes (4)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.9 - Protection of audit information SR 6 - Timely response to events
NIS - DF.6	Communication with competent authorities and CSIRTs	The operator implements a service that enables it to take note, without delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.).	7.4 Communication 7.5 Documented information A.6.1 Internal organisation A.8.2.2 Labelling of information	RS.CO Communications (2, 3, 4, 5) DE.DP Detection Processes (4) ID.RA Risk Assessment (2)	SR 2.8 - Auditable evens SR 2.9 - Audit storage capacity SR 2.10 - Response to audit processing failure SR 2.11 - Timestamps SR 2.12 - Non-repudiation SR 3.9 - Protection of audit information SR 6 - Timely response to events

Table 8: Resilience

ID	Security Measures	Description	ISO/IEC 27002 measures	NIST CSF measures	CLC/TS50701 measures
Continuity of operations					
NIS - RS.1	Business continuity management	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of an IT security incident.	9.3 Management review 10.2 Continual improvement A.5.1.2 Review of the policies for information security A.11.2.4 Equipment maintenance A.17.1 Information security continuity A.17.2 Redundancies	ID.RM Risk Management Strategy (1, 2, 3) PR.IP Information Protection Processes and Procedures (4, 7, 9, 10) RS.IM Improvements (2) RC.IM Improvements (1, 2) RC.RP Recovery Planning (1) RC.CO Communications (1, 2, 3) PR.PT Protective Technology (5)	SR 2.8 - Auditable evens SR 3.1 – Communication integrity SR 3.3 - Security functionality verification SR 3.6 - Deterministic output SR 3.7 - Error handling SR 4.1 – Information confidentiality SR 4.2 – Information persistence SR 5.2 - Zone boundary protection SR 6.1 - Audit log accessibility SR 7.1 - Denial of service protection SR 7.2 - Resource management SR 7.3 - Control system backup SR 7.4 - Control system recovery and reconstitution SR 7.5 – Emergency power
NIS - RS.2	Disaster recovery management	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding disaster recovery management, in case of a severe IT security incident.	A.17.2 Redundancies	ID.BE Business Environment (5) PR.PT Protective Technology (5) PR.IP Information Protection Processes and Procedures (9, 10) PR.DS Data Security (4) RC.IM Improvements (1, 2) RC.RP Recovery Planning (1)	SR 5.2 - Zone boundary protection SR 7.1 - Denial of service protection SR 7.2 - Resource management SR 7.3 - Control system backup SR 7.4 - Control system recovery and reconstitution SR 7.5 – Emergency power
Crisis management					
NIS - RS.3	Crisis management organisation	The operator defines the organisation for crisis management in its ISSP in case of IT security incidents and to ensure the continuity of the organisation's activities.	5.3 Organisational roles, responsibilities and authorities A.6.1.1 Information security roles and responsibilities A.11.2.4 Equipment maintenance A.17.1 Information security continuity	ID.BE Business Environment (5) PR.DS Data Security (4) PR.IP Information Protection Processes and Procedures (10)	SR 3.3 - Security functionality verification SR 7.1 - Denial of service protection SR 7.2 - Resource management SR 7.3 - Control system backup SR 7.4 - Control system recovery and reconstitution
NIS - RS.4	Crisis management process	The operator defines the processes for crisis management in its ISSP which the crisis management organisation will implement in case of IT security incidents and to ensure the continuity of an organisation's activities.	7.4 Communication 9.3 Management review 10.2 Continual improvement A.5.1.2 Review of the policies for information security A.6.1.3 Contact with authorities A.11.2.4 Equipment maintenance A.17.1 Information security continuity	RC.CO Communications (1, 2, 3) RC.RP Recovery Planning (1) RS.IM Improvements (1, 2) ID.SC Supply Chain Risk Management (5) PR.IP Information Protection Processes and Procedures (4, 9, 10) PR.PT Protective Technology (5)	SR 2.8 - Auditable evens SR 3.3 - Security functionality verification SR 6.1 - Audit log accessibility SR 7.1 - Denial of service protection SR 7.2 - Resource management SR 7.3 - Control system backup SR 7.4 - Control system recovery and reconstitution

TP-01-21-425-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-545-6
doi: 10.2824/92259