EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAILWAY CYBERSECURITY

Security measures in the Railway Transport Sector

NOVEMBER 2020

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. For more information, visit 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

Dimitra Liveri, Marianthi Theocharidou, Rossen Naydenov, ENISA

Activities supporting this study were conducted under contract with Wavestone (2019) and Systra (2020)

ACKNOWLEDGEMENTS

European Railway Agency (ERA)
European Railway Information Sharing and Analysis Centre (ER- ISAC)
International Union of Railways (UIC)
Infrabel

Lies Alderlieste, NS
Thomas Chatelet, ERA
Geir Arild Engh-Hellesvik, Vy
Yseult Garnier, SNCF
Mikkel Jochimsen, Banedanmark
Georgios Karaiskos, STASY
Antanas Kedys, AB „Lietuvos geležinkeliai“
André Shant Hagope Khatchik, infraestruturasdeportugal
Helmut Klarer, OEBB
Szlatényi Miklós, VPE
Marek Pawlik, Railway Research Institute Poland
Giorgio Pizzi, Ministero Infrastrutture e Trasporti
Quentin Rivette, SNCF
Christophe Rome, Lineas
Aryldo Ar. Russo, Certifer
Christian Schlehuber, DB
Olivier de Visscher, ER-ISAC
Tuulaniemi Virpi, Traficom
Christoffer Neesen, DB Regio AG

LEGAL NOTICE

It should be noted that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed as a legal action by ENISA or ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent the state of the art, ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of external sources, including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for any use made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-412-1
DOI: 10.2824/235164

TABLE OF CONTENTS

FIGURES AND TABLES

FIGURES

TABLES

GLOSSARY

CENELEC	European Committee for Electrotechnical Standardization
CER	Community of European Railway and Infrastructure Companies
CERT	Computer Emergency Response Team
CIS	Critical Information System
CISO	Chief Information Security Officer
COTIF	Convention Concerning International Carriage by Rail
CSIRT	Computer Security Incident Response Team
CVV	Card Validation Value
DDoS	Distributed Denial of Service
DG	Directorate-General
ENISA	European Union Agency for Cybersecurity
ERA	European Railway Agency
ERFA	European Rail Freight Association
ER-ISAC	European Rail Information Sharing and Analysis Centre
ERTMS	The European Railway Traffic Management System
ETCS	European Train Control System
ETML	European Traffic Management Layer
EU	European Union
GDPR	General Data Protection Regulation
GSM-R	Global System for Mobile Communications – Rail(way)
HR	Human Resources
ICS	Industrial Control System
ICT	Information and Communication Technology
IM	Infrastructure Manager
IMS	Information Management System
ISA	International Society of Automation
IT	Information Technology
KMC	Key Management Centre
KPI	Key Performance Indicator
LEU	Lineside Electronic Unit
NIS Directive	Directive on the security of network and information systems
OBU	On-Board Unit
OCC	Operation Control Centre
OES	Operator of Essential Services
OT	Operational Technology
OTIF	Intergovernmental Organisation for Carriage by Rail
PC	Personal Computer
RBC	Radio Block Centre
RU	Railway Undertaking
SIL	Safety Integrity Level
SL	Security Level

TSI	Technical Specification for Interoperability
UIC	International Union of Railways

EXECUTIVE SUMMARY

The railway sector enables goods and passengers to be transported within countries and across borders, and is key to the development of the European Union. The main players within this sector are the railway undertakings (RU), in charge of providing services for the transport of goods and/or passengers by rail; and the infrastructure managers (IM), in charge of establishing, managing and maintaining railway infrastructure and fixed installation, including traffic management, control-command and signalling, but also station operation and train power supply. Both are in the scope of the NIS Directive, and their identification as operator of essential service (OES) respects the transposition of laws to the majority of member states.

Trends

According to surveys and interviews conducted under this study, overall trends for the implementation of the NIS Directive for operator of essential service (OES) in the railway sector are as follows:

- The general implementation of security measures regarding governance and the ecosystem is heterogeneous and low compared to other types of measures. Most mature OES have already been applying these measures for a long time. Meanwhile for less mature OES, implementation of these measures has just started.
- Protective security measures seem to be the best implemented. While cybersecurity basics appear to be already implemented, security measures requiring advanced technical expertise show a lower level of implementation. In the special context of operational technology (OT) (legacy, number of systems, dependence on suppliers, safety concerns), it is often impossible to implement security basics without applying compensating countermeasures,
- For defensive security measures[1], the simplest security measures (e.g. communications with competent authorities and computer security incident response teams) seem to be well implemented. Others, however, are rarely or not implemented, as they require considerable cybersecurity expertise and maturity (e.g. log correlation and analysis),
- For resilience measures, the level of implementation appears to be good. Managing crises and incidents is part of the daily business of the railway sector. However, this must be qualified: there are still opportunities to improve the full integration of new cybersecurity threats into existing processes for dealing with crises and ensuring resilience.

Challenges

The study also identifies the main challenges faced by the sector to enforce the NIS Directive:

- Railway stakeholders must strike a balance between operational requirements, business competitiveness and cybersecurity, while the sector is undergoing digital transformation which increases the need for cybersecurity.
- Railway stakeholders depend on suppliers with disparate technical standards and cybersecurity capabilities, especially for operational technology.

[1] See NIS Directive Cooperation Group Publication 01/2018 - Reference document on security measures for Operators of Essential Services http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

- OT systems for railways have been based on systems that were at a point in time secure according to the state-of-the art but due to the long lifetime of systems they eventually become outdated or obsolete. This makes it difficult to keep them up-to-date with current cybersecurity requirements. Furthermore, these systems are usually spread across the network (stations, track, etc.), making it difficult to comprehensively control cybersecurity.
- Railway operators report issues of low cybersecurity awareness and differences in culture, especially among safety and operations personnel.
- Existing rail specific regulation doesn't include cybersecurity provisions. OES often have to comply with non-harmonized cybersecurity requirements deriving from different regulations.

ERTMS is also covered in this study as a separate infrastructure due to its special requirements and its cross-European nature.

Finally, trying to address some of the challenges described above, several European initiatives which are presented in this report take place. ENISA is teaming up with the European Railway Agency and the overall Railway community to bring these activities in the forefront.

1. INTRODUCTION

Representing 472 billion passenger-kilometres[2], 216,000 km of active railways[3] and 430 billion tonne-kilometres[4] for freight transport, the railway sector plays an important and fast-growing role. Railway infrastructure and systems are key assets, crucial to developing and protecting the European Union.

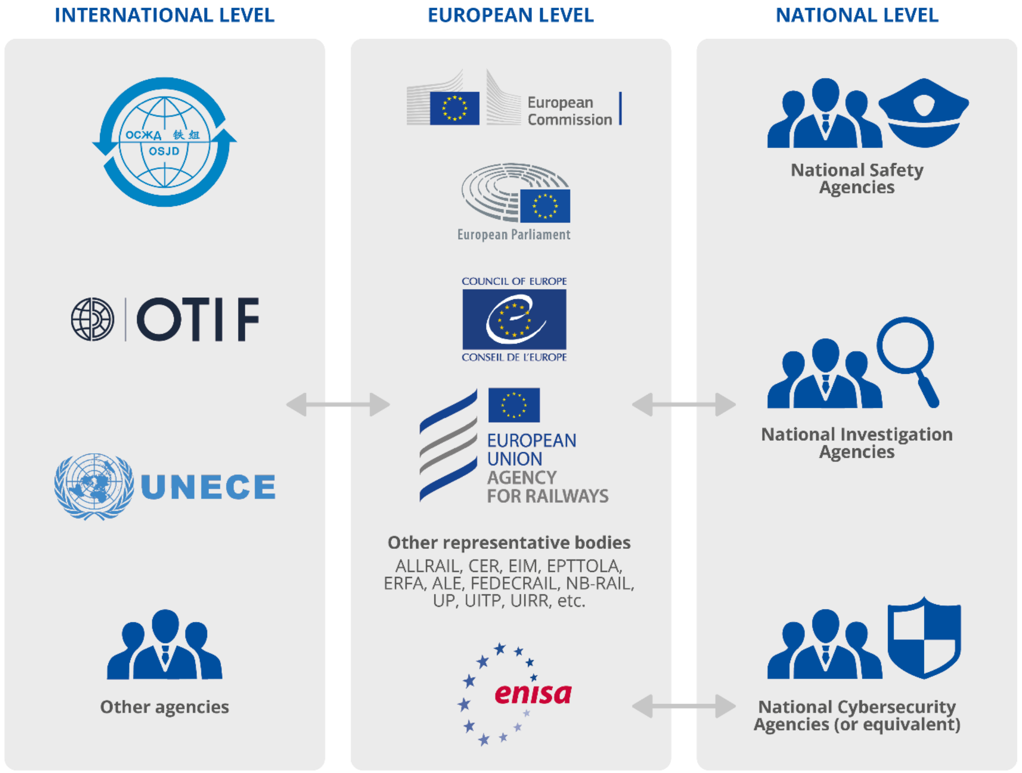
The railway sector is undergoing a major transformation of its operations, systems and infrastructure due to the digitisation of OT and IT systems and infrastructure, the automation of railway processes, the issues of mass transit and the increasing numbers of interconnections with external and multimodal systems. This sector is also evolving as it gradually opens up to competition. This leads to the reallocation of responsibilities and the separation of railway systems and infrastructure, which also affect IT systems.

In this context, it is becoming even more crucial for the railway sector to tackle cyber threats.

1.1 POLICY AND REGULATORY CONTEXT

Several bodies define and enforce regulations for the railway sector at International, EU or national levels. Figure 1: **Regulators overview** presents the main stakeholders.

Figure 1: Regulators overview


INTERNATIONAL LEVEL
EUROPEAN LEVEL
NATIONAL LEVEL
ОСЖД 铁组 OSJD
OTIF
UNECE
Other agencies
European Commission
European Parliament
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
EUROPEAN UNION AGENCY FOR RAILWAYS
Other representative bodies
ALLRAIL, CER, EIM, EPTTOLA, ERFA, ALE, FEDECRAIL, NB-RAIL, UP, UITP, UIRR, etc.
enisa
National Safety Agencies
National Investigation Agencies
National Cybersecurity Agencies (or equivalent)

[2] See https://ec.europa.eu/eurostat/statistics-explained/index.php/Railway_passenger_transport_statistics_-_quarterly_and_annual_data
[3] Knapčíková, Lucia & Konings, Rob. (2018). EUROPEAN RAILWAY INFRASTRUCTURE: A REVIEW. Acta logistica. 5. 71-77. doi:10.22306/al.v5i3.97.
[4] See https://ec.europa.eu/eurostat/statistics-explained/index.php/Railway_freight_transport_statistics

The railway sector is historically bound by regulations controlling interoperability, safety, dangerous goods management and certification, at international, European and national levels.

At international level, the first initiative concerning the railway sector was the creation of the International Union of Railways (UIC)[5] in 1922, with 194 members across 5 continents. Today it plays an important role in standardising and classifying railways through its UIC Codes[6], facilitating the sharing of best practice, promoting interoperability and developing skill centres.

Moreover, the first and unprecedented regulatory framework was the Convention Concerning International Carriage by Rail (COTIF)[7] of 9 May 1980, amended by the Vilnius Protocol of 3 June 1999 ("the Accession Agreement"), which resulted in the creation of the Intergovernmental Organisation for Carriage by Rail (OTIF) with, in 2019, 51 members (the European Union acceded to COTIF in 2011)[8]. The objectives are to develop uniform laws and rules for the carriage of passengers and freight by rail, through technical functional requirements and model contracts.

At European level, to develop a competitive railway transport system, promote the Single European Railway Area and align with international regulations, the European Commission has enforced several directives – mostly in four railway legislation packages listed in the Appendix (Table 5). To fulfil these objectives, three main priorities have been defined:

- opening the railway transport market up to competition,
- improving the interoperability and safety of national networks, and
- developing railway infrastructure.

However, the existing regulatory framework described above does not fully consider security, particularly the cybersecurity issues specific to the railway sector. Over the past few years, the European Commission has enforced directives and regulations regarding cybersecurity, but which are applicable to all markets and sectors, described in the Table 6 (in the appendix at the end of the document).

Directive 2016/1148 (NIS Directive) is the first legislative document focusing on cybersecurity, extending the scope also to the railway sector. The following Operators of Essential Services (OES) are identified:

- **Infrastructure managers** as defined in point (2) of Article 3 of Directive 2012/34/EU[9] namely: "*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** as defined in point (1) of Article 3 of Directive 2012/34/EU namely "*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"*;
    - including operators of **service facilities** as defined in point (12) of Article 3 of Directive 2012/34/EU namely *"any public or private entity responsible*

[5] See https://uic.org/
[6] The company code (also called RICS: "Railway Interchange Coding System" or railway code) is a 4 digit code used in various applications to identify a company involved in the railway business.
[7] See https://otif.org/fr/?page_id=172
[8] See https://otif.org/en/?page_id=53
[9] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0034&from=FR

> *for managing one or more service facilities or supplying one or more services to railway undertakings*"

In 2018, the UIC launched several events and publications to address cybersecurity issues in the railway sector (*e.g.* Guidelines for Cyber-Security in Railways)[10]. Moreover, the **Shift2Rail Joint Undertaking**[11] was launched under the Horizon 2020 programme to seek focused research and innovation (R&I) and market-driven solutions and promote competitiveness in the European railway industry. The initiative included cybersecurity issues in the railway sector, for example, under the CYRAIL (CYbersecurity in the RAILway sector) project[12], or under the X2Rail-1[13] project and X2Rail-3[14] projects which included cybersecurity work packages.

1.2 STUDY SCOPE

This study regards the level of implementation of cybersecurity measures in the railway sector, within the context of the enforcement of the NIS Directive in each European Member State. The stakeholders involved in the scope of this study are European infrastructure managers (IM) and railway undertakings (RU).

1.3 STUDY OBJECTIVES

The main objective of the study is to share a preliminary analysis of the level of maturity of the railway sector regarding the implementation of security measures enforced by the NIS Directive. An additional important element of the study is to identify the cybersecurity challenges that OES in the railway sector face when applying these measures. Finally, this study takes a closer look at cybersecurity for the European Railway Traffic Management System (ERTMS), because some OES have already integrated parts of their services into ERTMS.

1.4 TARGET AUDIENCE

The main target audience for this study is composed of professionals in charge of IT and OT security in the railway sector: railway undertakings (RU) and infrastructure managers (IM), or any other stakeholders involved in the enforcement of security measures.

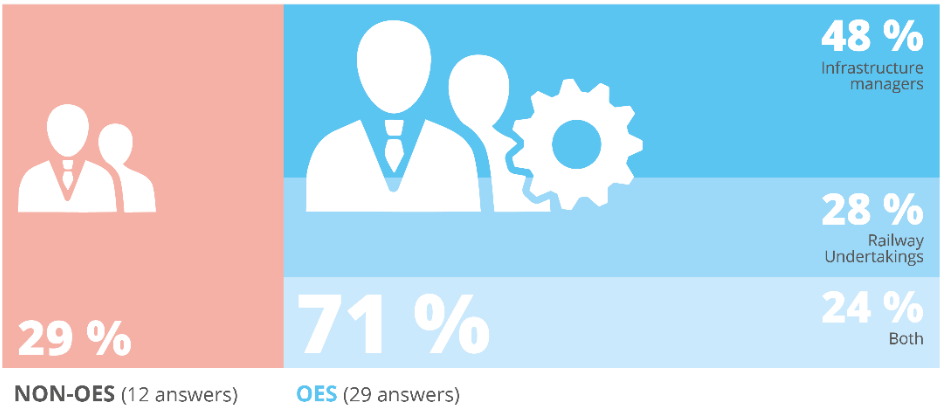
1.5 METHODOLOGICAL APPROACH

An online survey addressing cybersecurity issues was sent to stakeholders of the European railway sector (railway undertakings and infrastructure managers).

The survey collected 41 answers, including 29 answers from OES (71%), representing 21 member states (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Poland, Portugal, Romania, Spain, Sweden) and Norway. 48% of the respondents are infrastructure managers, 24% are railway undertakings and 28% are organisations that have both roles. The non-OES respondents (12 in total, 29%) represent certification bodies, companies from the railway manufacturing industry, governmental bodies and authorities, or railway undertakings and infrastructure managers that are not identified as OES, e.g. operating in countries such as the Netherlands, and Norway.

[10] See https://uic.org/IMG/pdf/uic_activity_report_2018.pdf
[11] See https://shift2rail.org
[12] See https://cyrail.eu/
[13] X2Rail-1, Start-up activities for Advanced Signalling and Automation Systems, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1
[14] X2Rail-3, Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

Figure 2: Survey respondents



Based on the survey answers, 14 OES were interviewed in order to understand their priorities with respect to cybersecurity, challenges in implementing security measures and their relationship with their competent national authority regarding the NIS Directive. The information collected from the survey and interviews was analysed thoroughly and completed from desk research to draft the report.

1.6 STRUCTURE OF THE REPORT

The report is structured as follows:

- analysis of the policy and regulatory context of railways, particularly cybersecurity for rail,
- identification of status regarding the transposition of the NIS directive to EU countries, especially the railway sector,
- identification of essential services and critical information systems for the railway sector, based on answers from the survey and interviews,
- maturity assessment of the sector concerning implementation of the NIS directive, based on answers from the survey and interviews,
- a focus on European Railway Traffic Management System, the most critical services and information system for the railway sector in Europe.

2. THE RAILWAY SECTOR

To date, the railway sector does not seem to have been a direct target for cyber criminals, however several cyberattacks and incidents have taken place indicating the vulnerability of the sector. Below a detailed list (not extensive) of the most referenced ones is presented (always with a focus on the EU). Note that no OT and IT combined related incidents have occurred to this day (based on publicly available information at the time of editing).

- **2015, Ukraine -** DoS attack. An advanced persistent threat (APT) actor carried out a large-scale coordinated attack to destabilize the Ukrainian government by targeting power stations, mining and railway infrastructure. The aim of these attacks was to paralyse public and critical infrastructure by disabling industrial control systems (ICS).[15]
- **July 2015-2016, United Kingdom -** Intrusion. Between July 2015 and July 2016, four cyberattacks were discovered on the UK railway network. After analysis, these attacks were considered as part of a reconnaissance operation before an APT (Advanced Persistent Threat) attack, probably led by a national state threat actor. No disruption or modification of data was detected. [16]
- **May 2017, Germany -** Ransomware. Deutsche Bahn was a victim of the WannaCry ransomware. Some devices were corrupted and due to this could show no information to the passengers anymore. Train operation was not disrupted[17].
- **October 2017, Sweden -** DoS attack. The first attack took place on 11th of October, affecting the Sweden Transport Administration (Trafikverket) via its two internet service providers, TDC and DGC. The DDoS attack reportedly affected the IT system that monitors trains' locations. It also took down the federal agency's email system, website, and road traffic maps. Customers during this time were unable to make reservations or receive updates on the delays. As a result, train traffic and other services reportedly had to be managed manually, using back-up processes. The next day, a second DDoS attack impacted the website of the Swedish Transport Agency, a separate governmental body responsible for regulating and inspecting transportation systems. It also affected Western Sweden public transport operator Vasttrafik, reportedly crashing its ticket booking app and online travel planning service[18].
- **May 2018, Denmark -** DDoS. A DDoS attack impacted the ticketing systems of DSB. The Danish travellers could not purchase tickets from ticket machines, the online application, website and certain station kiosks. DSB estimated that approximately 15,000 customers were affected[19].
- **March 2020, United Kingdom -** Data breach. The email addresses and travel details of about 10.000 people who used the free Wi-Fi provided UK railway stations have been exposed online. Network Rail and the service provider C3UK confirmed the incident. The database contained 146 million records, including personal contact details and dates of birth. A breach involved the app ‘Indian Rail’ which is a top app on the Apple App Store. It was due to an exposed Firebase database. The breach contained 2.357.684 rows of emails, usernames and plain-text passwords[20].

[15] See https://www.bbc.com/news/technology-38573074
[16] See https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558
[17] See https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM
[18] See https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963
[19] See http://cphpost.dk/news/hackers-target-danish-train-service-over-the-weekend.html
[20] See https://www.bbc.com/news/technology-51682280

- **May 2020, Switzerland -** Malware. Swiss rail vehicle manufacturer Stadler was hit by a malware attack that impacted all of its locations and may have allowed attackers to steal sensitive company data. After compromising Stadler systems, attackers reportedly infected its systems with malware that was then used to exfiltrate sensitive corporate data from breached systems. Internal documents stolen during the cyber-attack on Stadler's headquarters have been published online after the manufacturer refused to give in to ransom demands. [21]
- **July 2020, Spain -** Ransomware. Spanish Infrastructure Manager ADIF has been hit by a ransomware not affecting critical infrastructure but exposing gigabytes of personal and business data[22].

2.1 RAILWAY STAKEHOLDERS

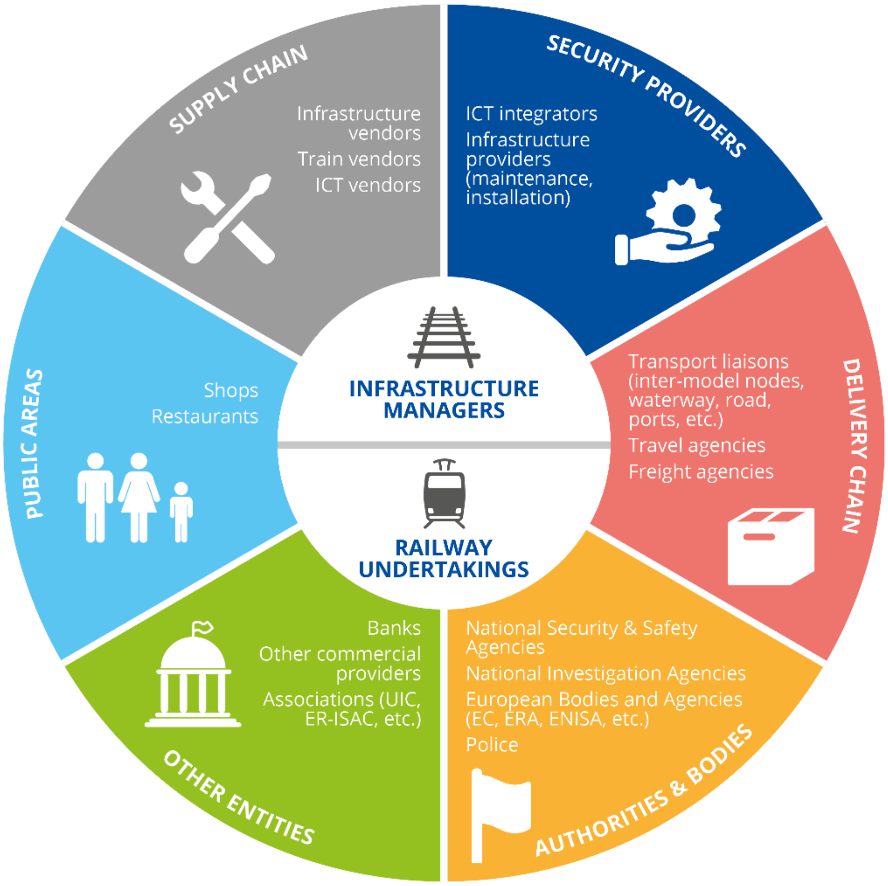
The rail ecosystem is well defined and organised, with several roles and responsibilities shared between the stakeholders. The table and figure below depict and describe the ecosystem actors.

Table 1: Descriptions of stakeholders

Stakeholder	Description
Infrastructure Manager	In Directive 2012/34/EU, the European Union defines an infrastructure manager as "any person or firm responsible particularly 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	In Directive 2012/34/EU, the European Union defines a railway undertaking as "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 ensure traction. This also includes undertakings which provide traction only".
Supply chain	Supply chain stakeholders provide railway and IT/OT assets to RUs and IMs. They may be vendors of trains, ICS systems, IT systems, etc. The railway sector is dependent on these suppliers, and their collaboration is vital to ensuring cybersecurity in the railway sector.
Service providers	Service providers can be any third party contracted by RUs or IMs to perform all or part of a service, which could be a business service (e.g. entity in charge of train maintenance) or an IT/OT service (e.g. IT monitoring). Service providers include advisors, works contractors, project management consultants, system providers, integrators.
Delivery chain	The delivery chain consists of all stakeholders involved in delivering the transport service to customers, for freight (e.g. freight agencies, logistical companies) or passengers (e.g. travel agencies, tourist brokers). It covers also third parties who interact with the railway for service delivery (e.g. road transport companies).
Authorities and bodies	Authorities and bodies consist of all stakeholders in charge of applying policies and regulations in the railway sector (e.g. railway regulators, national and European authorities for safety or cybersecurity, conformity assessment bodies, as notified body and designated body).
Public areas	Public areas consist of all third parties who use railway premises to deliver goods or services (more specifically in stations). They include providers of services for passengers (e.g. sitting areas, lounges), as well as restaurants or retail outlets in stations.
Other entities	Other entities (e.g. banks, freight insurance) have relations with railway stakeholders. In particular, several associations or working groups focus on certain topics in the railway sector.

[21] See https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf https://www.railjournal.com/technology/internal-documents-published-after-stadler-refuses-us-6m-ransom/
[22] see https://www.railjournal.com/technology/adif-hit-by-cyberattack/

Figure 3: Railway stakeholder map


SUPPLY CHAIN
Infrastructure vendors
Train vendors
ICT vendors
SECURITY PROVIDERS
ICT integrators
Infrastructure providers (maintenance, installation)
DELIVERY CHAIN
Transport liaisons (inter-model nodes, waterway, road, ports, etc.)
Travel agencies
Freight agencies
AUTHORITIES & BODIES
National Security & Safety Agencies
National Investigation Agencies
European Bodies and Agencies (EC, ERA, ENISA, etc.)
Police
OTHER ENTITIES
Banks
Other commercial providers
Associations (UIC, ER-ISAC, etc.)
PUBLIC AREAS
Shops
Restaurants
INFRASTRUCTURE MANAGERS
RAILWAY UNDERTAKINGS

Based on the analysis of the survey answers:

- the majority of OES collaborate on cybersecurity matters with national bodies, e.g. government, safety or cybersecurity agencies, ministries of transport or infrastructure, national computer security incident response teams (CSIRTs) or computer emergency response teams (CERTs), authorities responsible for crisis or emergency management, disaster management, national security, counterterrorism, or data protection;
- many OES report collaboration with European bodies, such as ENISA, ERA[23], DG CONNECT[24], DG MOVE[25], CENELEC[26], and the European Rail ISAC[27];
- several OES also mention other organisations and associations that they work with, such as UIC[28], CER[29], ERFA[30], RailNetEurope[31], FTE[32], COLPOFER[33], Hitrail[34].

[23] See https://www.era.europa.eu/
[24] See https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en
[25] See https://ec.europa.eu/knowledge4policy/node/6657_fr
[26] See https://www.cenelec.eu/
[27] See https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[28] See https://uic.org/
[29] See http://www.cer.be/
[30] See http://erfarail.eu/
[31] See https://rne.eu/
[32] See http://www.forumtraineurope.eu/home/
[33] See http://www.colpofer.org/content/cfer/en.html
[34] See https://www.hitrail.com/

2.1.1 NIS Directive implementation – Authorities

All EU Member States (MS) have already transposed the NIS Directive in their national regulatory framework. The European Commission published in October 2019 a report[35] establishing a first assessment on the different approaches chosen by Member States to enforce the NIS Directive and develop a special focus on the railway subsector.

The report highlights the fact that MS have chosen different approaches to enforcing NIS implementation, and explains the variations between MS. Several variations are explained, the identification methods chosen by each national authority, the definition of the list of essential services, and the identification of OES.

Table 2 details the different approaches chosen by MS for the transport sector and the railway subsector, and the overarching authority. The key findings relating to the context of this report are the following:

- All member states have identified the transport sector as essential.
- All member states, with the exception of the Netherlands, have identified the railway subsector explicitly as essential.
- There are two approaches to the identification of the competent authority for the NIS Directive: either a unique national authority, chiefly focussing on cybersecurity issues, or one authority per sector, usually the relevant ministry, addressing sectorial issues including cybersecurity.

Table 2: Implementation of the NIS Directive for the railway sector in each EU MS

Member State	Transport sector is identified	Railway subsector is identified	National Single point of contact for the NIS Directive	National Competent Authority for OES (Transport)	National Rail Safety Authority[37]
Austria (AT)	Yes	Yes	Federal Ministry of Interior	Federal Ministry of Interior	Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK)
Belgium (BE)	Yes	Yes	Centre for Cybersecurity Belgium (CCB)	Centre for Cybersecurity Belgium (CCB)	Federal Mobility Minister (Federal Public Service - FPS Mobility and Transport)
Bulgaria (BG)	Yes	Yes	State e-Government agency	Ministry of Transport, Information Technologies and Communications	Ministry of Transport – Railway Administration Executive Agency
Croatia (HR)	Yes	Yes	The Office of the National Security Council	Ministry of the Sea, Transport and infrastructure	Agencija za sigurnost željezničkog prometa (Railway Safety Agency)
Cyprus (CY)	Yes	No	Digital Security Authority (DSA)	Digital Security Authority (DSA)	-
Czech Republic (CZ)	Yes	Yes	National Cyber and Information Security Agency (NCISA)	National Cyber and Information Security Agency (NCISA)	Drážní Úřad (DU) (Rail Authority)
Denmark (DK)	Yes	Yes	Danish Centre for Cybersecurity	Danish Transport, Construction and Housing Authority	Danish Transport, Construction and Housing Authority

[35] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546
[36] See https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive
[37] Source: https://www.era.europa.eu/agency/stakeholder-relations/national-safety-authorities_en

Member State	Transport sector is identified	Railway subsector is identified	National Single point of contact for the NIS Directive	National Competent Authority for OES (Transport)	National Rail Safety Authority[37]
Estonia (EE)	Yes	Yes	Estonian Information System Authority	Estonian Information System Authority	Consumer Protection and Technical Regulatory Authority
Finland (FI)	Yes	Yes	Finnish Transport and Communications Agency (Traficom)	Finnish Transport and Communications Agency (Traficom)	Finnish Transport and Communications Agency (Traficom)
France (FR)	Yes	Yes	National Cybersecurity Agency (ANSSI)	National Cybersecurity Agency (ANSSI)	Établissement Public de Sécurité Ferroviaire (EPSF)
Germany (DE)	Yes	Yes	Federal Office for Information Security (BSI)	Federal Office for Information Security (BSI)	Federal Railway Authority
Greece (EL)	Yes	Yes	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)	Regulatory Authority for Railways
Hungary (HU)	Yes	Yes	National Cybersecurity Centre	National Directorate General for Disaster Management	Ministry of Innovation and Technology Transportation Safety Bureau
Ireland (IE)	Yes	Yes	National Cyber Security Centre (NCSC)	National Cyber Security Centre (NCSC)	Commission for Railway Regulation (CRR)
Italy (IT)	Yes	Yes	Presidenza del Consiglio dei Ministri	Ministry of Transport and Infrastructure	Agenzia Nazionale per la Sicurezza delle Ferrovie (Railway Safety Agency)
Latvia (LV)	Yes	No	Ministry of Defence	Ministry of Transport	State Railway Technical Inspectorate
Lithuania (LT)	Yes	Yes	National Cyber Security Centre (NCSC/CERT-LT)	National Cyber Security Centre (NCSC/CERT-LT)	Lithuanian transport safety administration
Luxembourg (LU)	Yes	Yes	Institut Luxembourgeois de Régulation	Institut Luxembourgeois de Régulation	Ministère de la Mobilité et des Travaux publics (Administration des chemins de fer)
Malta (MT)	Yes	No	Malta Critical Infrastructure Protection Unit (CIIP)	Malta Critical Infrastructure Protection Unit (CIIP)	-
Netherlands (NL)	Yes	No[38]	National Cyber Security Centre (NCSC)	N/A (for Railway sector)	Human Environment and Transport Inspectorate
Poland (PL)	Yes	Yes	Ministry of Digital Affairs, Department of cybersecurity	Ministry of Infrastructure	Office of Rail Transport (UTK)
Portugal (PT)	Yes	Yes	Portuguese National Cybersecurity Centre (CNCS)	Portuguese National Cybersecurity Centre (CNCS)	Institute for Mobility and Transport (IMT, I.P.)
Romania (RO)	Yes	Yes	Romanian National Computer Security Incident Response Team (CERT-RO)	Romanian National Computer Security Incident Response Team (CERT-RO)	Romanian Railway Safety Authority (ASFR)
Slovakia (SK)	Yes	Yes	National Security Authority	National Security Authority	Transport Authority
Slovenia (SI)	Yes	Yes	Information Security Administration	Information Security Administration	Public Agency of the Republic of Slovenia for Railway Transport

[38] In 2019, the Netherlands identified only Schiphol Airport and the port of Rotterdam in the transport sector.

Member State	Transport sector is identified	Railway subsector is identified	National Single point of contact for the NIS Directive	National Competent Authority for OES (Transport)	National Rail Safety Authority[37]
Spain (ES)	Yes	Yes	National Security Council, through the National Security Department	Private sector: Secretary of State for Security, -Ministry of Interior-, through the National Center for the Protection of Infrastructures and Cybersecurity (CNPIC) Public sector: Ministry of Defence, through the National Cryptologic Centre	Agencia Estatal de Seguridad Ferroviaria (Railway Safety Agency)
Sweden (SE)	Yes	Yes	Swedish Civil Contingencies Agency (MSB)	Swedish Transport Agency	Swedish Transport Agency

2.2 ESSENTIAL RAILWAY SERVICES

The above-mentioned report by the European Commission[39] shows that member states have chosen approaches of varying levels of granularity to define the essential services of the railway sector. In particular, member states have chosen:

- not to specify rail-specific essential services,
- to distinguish between RU and IM, as two essential rail services,
- to distinguish between separate activities such as freight and passenger transport, or
- to draw a detailed list of essential services, such as dangerous goods management, or maintenance.

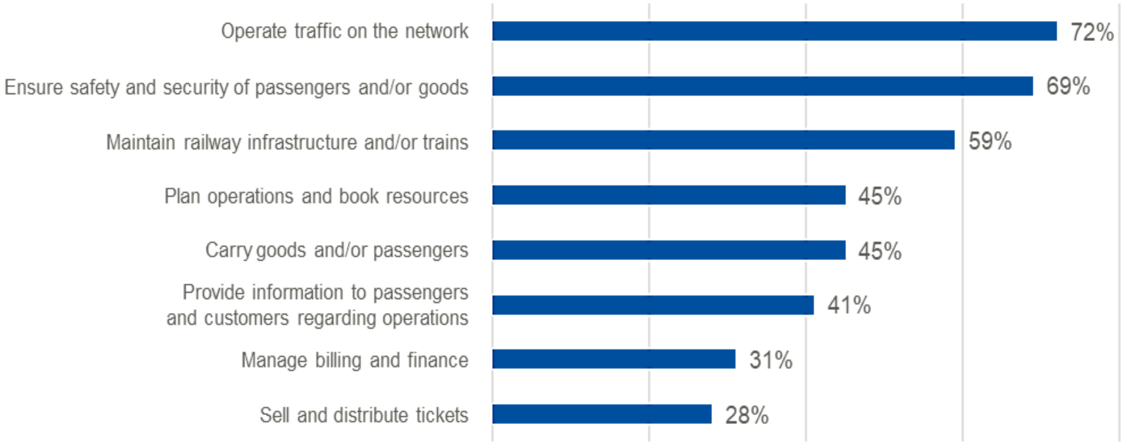
To ensure that data is comparable, and for drafting this report, eight essential railway services have been defined and specified in the survey:

- 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 book resources,
- information for passengers and customers about operations,
- carrying goods and/or passengers, and
- selling and distributing tickets.

The respondents to the survey were asked to assess which of these services were essential for their organisation. The essential services identified by the majority of respondents are "**operating traffic on the network**" (72%), "**ensuring the safety and security of passengers and/or goods**" (69%), and "**maintaining railway infrastructure and/or trains**" (59%).

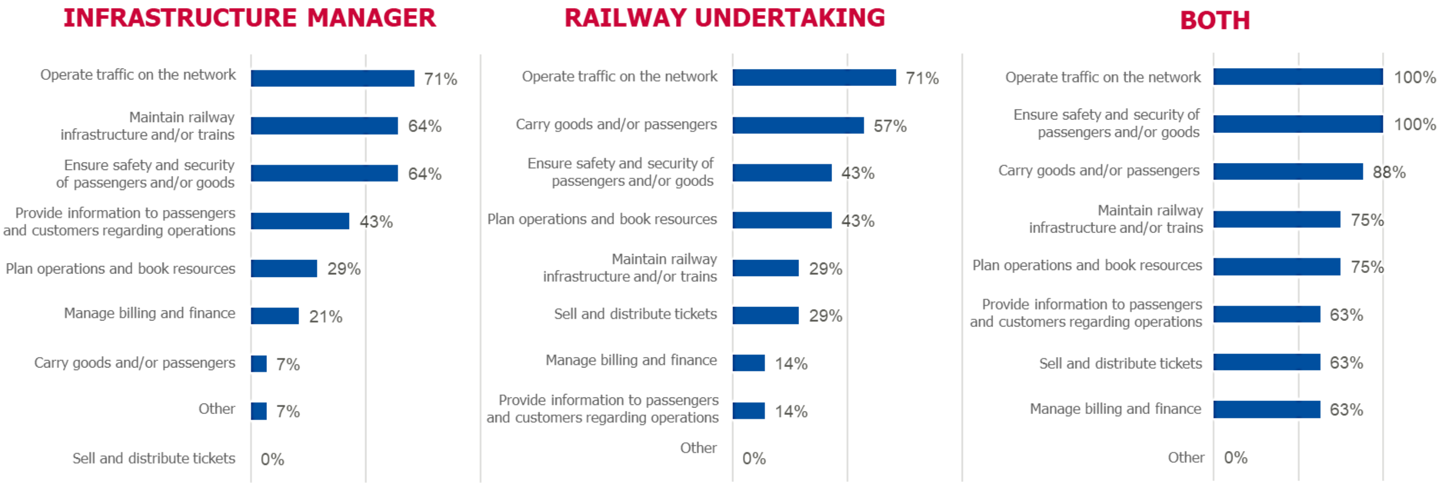
[39] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

Figure 4: Identification of essential railway services



The assessment of these essential services differs for each type of OES (RU, IM and OES that with both roles). Figure 5 illustrates the differences between the services selected as essential for each type of OES.

Figure 5: Essential services identified for each type of OES



From the results above, we make the following observations.

- “Operating traffic on the network” is considered the most essential service for all OES (71% for IM, 71% for RU and 100% for OES with both roles).
- “Maintaining railway infrastructure and/or trains” is identified as essential for IM (64%) and for OES with both roles (75%), but fewer RU considered it as essential (only 29%).
- “Carrying goods and/or passengers” is identified as one of the most essential services by RU (57%) and for OES with both roles (88%), whereas only 7% of IM considered it as essential.
- “Ensuring the safety and security of passengers and/or goods” was identified as one of the more essential services for all types of OES (64% for IM, 43% for RU and 100% for OES with both roles).

The results offer no surprises; they represent well the implemented split in hierarchy in the area of responsibility of the two actors in the sector. Security and safety is a priority for the entire sector. Due to the increasing competition in several European MS, several RUs share train operations, but only a few are in charge of infrastructure management. This makes the IM's role in delivering essential services for railways more prominent, as multiple RUs depend on often a single IM.

2.2.1 NIS Directive Implementation – Essential Services

In the implementation of the NIS Directive each MS has identified essential railway services (when railway has been identified as essential sector). It needs to be underlined that the definition of essential services related to the railway subsector has not been standardised. MS apply varying levels of granularity in the definition of rail essential services (detailed in the next section).

Table 3: Essential railway services identified per MS

Member State	Railway subsector is identified?	Identified Railway Essential Services[40]
Austria (AT)	Yes	- Railway infrastructure - Railway cargo transport - Railway passenger transport - Railway stations
Belgium (BE)	Yes	- Infrastructure managers - Railway undertakings
Bulgaria (BG)	Yes	- Providing, maintaining and managing service facilities - Railway transport by carriers - Providing guidance on railway transport
Croatia (HR)	Yes	- Managing and maintaining railway infrastructure, including traffic management and control-command and signalling subsystem - Railway transport services of goods and/or passengers - Managing service facilities and providing services in service facilities - Providing additional services necessary for railway transport of goods or passengers
Cyprus (CY)	No	N/A
Czech Republic (CZ)	Yes	- Railway operation - Operation of railway transport or service facility
Denmark (DK)	Yes	- Railway infrastructure management - Railway transport
Estonia (EE)	Yes	- Railway infrastructure manager - Railway transport service
Finland (FI)	Yes	- State infrastructure management - Traffic management services
France (FR)	Yes	- Railway services - Control and management of railway traffic - Infrastructure maintenance - Freight and hazardous materials - Passenger transport - Rolling stock maintenance - Metros, tram and other light railway services (including underground services)

[40] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

Member State	Railway subsector is identified?	Identified Railway Essential Services[40]
Germany[41] (DE)	Yes	- Railway stations - Large shunting yards - Railway network according to TEN-V (including infrastructure and operation centres) - Operating centres
Greece (EL)	Yes	- Railway infrastructure management - Railway services
Ireland (IE)	Yes	- Infrastructure managers - Railway undertakings
Italy (IT)	Yes	N/A
Latvia (LV)	No	Specific criteria for the transport sector[42]
Lithuania (LT)	Yes	- Carriage of passengers and luggage by railway service - Railway freights service - Railway infrastructures development, management and maintenance service
Luxembourg (LU)	Yes	- Railway infrastructure management - Cargo and passenger railway transport
Malta (MT)	No	N/A
Netherlands (NL)	No[43]	N/A
Poland (PL)	Yes	- Preparing train timetables - Passenger railway transport - Freight railway transport
Portugal (PT)	Yes	- Infrastructure managers - Railway undertakings
Romania (RO)	Yes	- Traffic control and management - Freight transport - Transport of dangerous goods - Passenger transport - Metro, tramway and other light railway services - Maintenance of railway infrastructure - Maintenance of rolling stock
Slovakia (SK)	Yes	- Infrastructure operators - Railway undertakings
Slovenia (SI)	Yes	- Passenger railway transport, interurban - Freight railway transport - Service activities incidental to land transportation (operation of railway stations etc.)
Spain (ES)	Yes	- Railway service management - Railway transport management - Railway network services - Railway information and telecommunication management

[41] The services were derived from: Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21.06.2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, ausgegeben am 29.06.2017, Seite 1903

[42] Latvia does not identify a subsector for transport: specific criteria have been defined to identify OESs, listed in Article 5 of the Regulations of the Cabinet of Ministers Nr. 43. See https://likumi.lv/ta/id/304327-noteikumi-par-nosacijumiem-drosibas-incidenta-butiski-traucejosas-ietekmes-noteiksanai-un-kartibu-kada-pieskir-parskata

[43] In 2019, the Netherlands identified only Schiphol Airport and the port of Rotterdam in the transport sector.

Member State	Railway subsector is identified?	Identified Railway Essential Services[40]
Sweden (SE)	Yes	- Infrastructure management - PAX transport - Cargo transport

2.3 RAILWAY SYSTEMS

Based on desk research and the feedback by the survey respondents, a high-level overview of the main railway systems was prepared for this report. Figure 6 represents this overview, with systems whose responsibilities are shared between RU or IM, depending on national legislation and policies, local specificities, historical reasons, etc.

This overview defines five categories of systems, which are presented in Figure 6 and described in more detail in Table 4. It should be noted that the list of systems was updated at a later stage to match the terminology used in the upcoming CENELEC TS50701[44].

Table 4: Description of main railway systems

Category	Systems	Description
Pre-Operations	Timetable construction	Systems which allow commercial offers to be created for customers (timetable for each train line) and to prepare resource rosters (assets and staff).
	Sales, distribution and customers relations	Systems enabling customers to buy tickets or book a train seat, as well as managing customer relation (e.g. claims, loyalty cards, marketing campaign).
	Network allocation	Systems enabling RU to book infrastructure (corridors) to operate their trains on the network, and to inform the IM of any special characteristics of trains or loads (e.g. dangerous goods, oversize). They also enable the IM to apply costing policies to the RU for the use of the infrastructure.
	Asset procurement	Systems enabling RU and IM to account for their assets (infrastructure, or trains for example), and to procure new assets and manage logistics.
Operations	Signalling	Systems used to direct railway traffic, such as electronic interlocking systems, level crossing systems, etc.
	Command and control	Systems used to enable movement of trains, e.g. Automatic Train Control (ATC), Automatic Train Supervision (ATS) and Energy Traction system.
	Auxiliary	Systems such as Energy Systems, HVAC and Lighting Systems for emergencies.
	Passenger comfort and services	Systems that facilitate comfort and service to the passenger, such as Passenger Announcement Systems, Passenger Information Systems, HVAC and lighting systems, lifts and escalators, etc.
	Telecom systems	Systems to enable communication, such as Radio systems dedicated to signalling and other systems, Wired systems for network communications, Voice communications, Time keeping. *Note: These telecommunication systems are shared infrastructure for the operation systems above, as well as for security, safety and maintenance systems.*

[44] At the time of publication, CENELEC (TC9X - Working Group 26) had been finalising Technical specification 50701: "Railway Applications –Cybersecurity".

Category	Systems	Description
Security, safety & maintenance	Security and safety systems keep operations safe and secure. They include access control systems, video surveillance, fire detection, accreditation systems for personnel. Maintenance systems enable the RU and IM to perform maintenance on all their assets. They include asset management, scheduling systems, fault reporting systems, resource allocation/planning systems, document databases, fault follow-up and escalation systems.	
Corporate & support	Corporate systems are used by RUs and IMs to perform usual business. They include email, PCs, finance, HR, communications.	
Development	Development systems include everything used to develop the undertaking. They include bidding systems for the RU or IM to answer invitations to tender for train operations or infrastructure management, as well as all the systems used for research and engineering.	

Figure 6: Overview of railway systems

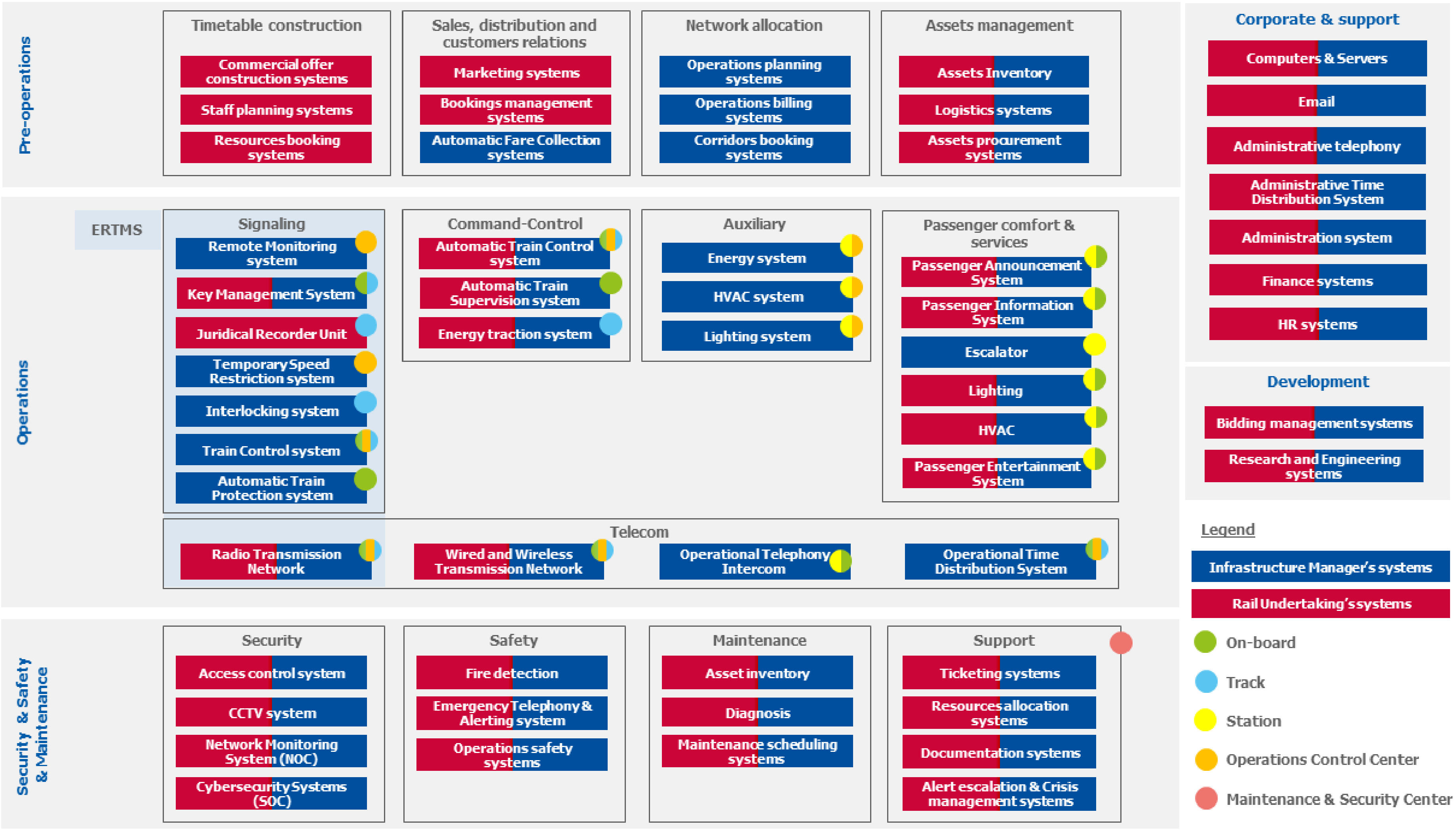
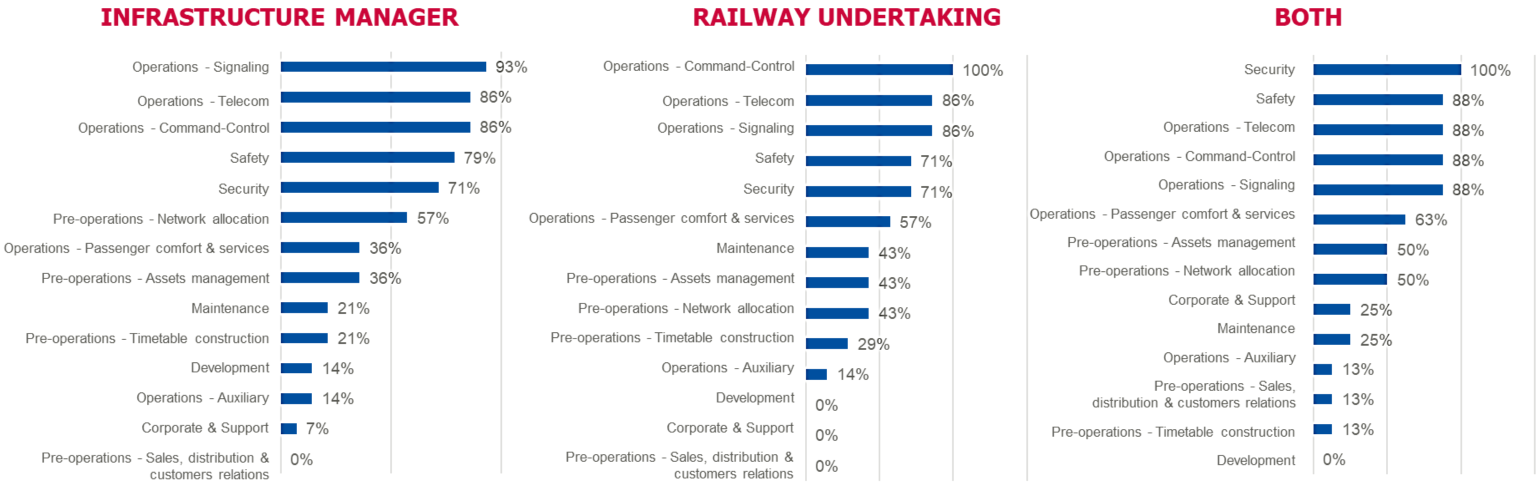

Pre-operations
Timetable construction
Commercial offer construction systems
Staff planning systems
Resources booking systems
Sales, distribution and customers relations
Marketing systems
Bookings management systems
Automatic Fare Collection systems
Network allocation
Operations planning systems
Operations billing systems
Corridors booking systems
Assets management
Assets Inventory
Logistics systems
Assets procurement systems
Operations
ERTMS
Signaling
Remote Monitoring system
Key Management System
Juridical Recorder Unit
Temporary Speed Restriction system
Interlocking system
Train Control system
Automatic Train Protection system
Command-Control
Automatic Train Control system
Automatic Train Supervision system
Energy traction system
Auxiliary
Energy system
HVAC system
Lighting system
Passenger comfort & services
Passenger Announcement System
Passenger Information System
Escalator
Lighting
HVAC
Passenger Entertainment System
Telecom
Radio Transmission Network
Wired and Wireless Transmission Network
Operational Telephony Intercom
Operational Time Distribution System
Security & Safety & Maintenance
Security
Access control system
CCTV system
Network Monitoring System (NOC)
Cybersecurity Systems (SOC)
Safety
Fire detection
Emergency Telephony & Alerting system
Operations safety systems
Maintenance
Asset inventory
Diagnosis
Maintenance scheduling systems
Support
Ticketing systems
Resources allocation systems
Documentation systems
Alert escalation & Crisis management systems
Corporate & support
Computers & Servers
Email
Administrative telephony
Administrative Time Distribution System
Administration system
Finance systems
HR systems
Development
Bidding management systems
Research and Engineering systems
Legend
Infrastructure Manager's systems
Rail Undertaking's systems
On-board
Track
Station
Operations Control Center
Maintenance & Security Center

Figure Note: Background colours indicate the actor who is usually in charge of the system (this could vary according to the organisation or project). A coloured pastille shows the most likely location of the system; some systems have assets in several locations. ERTMS is considered as it is the ATC that is harmonised for EU. The scope of the ERTMS is depicted with a light blue colour, covering Signalling and Radio systems.

Based on this overview, the OES respondents of the survey identified their critical information systems which support their essential services. Overall, the most critical systems identified by all types of OES (IM, RU and OES with both roles) are systems for **Security and Safety**, and for **Operations (Signalling, Command-Control and Telecommunications)**.

Figure 7: Critical Information Systems for each type of OES



3. CYBERSECURITY MEASURES

3.1 CYBERSECURITY CHALLENGES

Based on answers to the survey, interviews and findings shared by experts with ENISA, the following cybersecurity challenges for OES in the railway sector seeking to implement security measures can be highlighted:

- Low digital and cybersecurity awareness in the railway sector.
- Difficulty in reconciling safety and cybersecurity worlds.
- Digital transformation of railway core business.
- Dependence on the supply chain for cybersecurity.
- Geographic spread of railway infrastructure and the existence of legacy systems.
- The need to balance security, competiveness and operational efficiency.
- Complexity of regulations for cybersecurity.

Railway stakeholders must strike a balance between operational requirements, business competitiveness and cybersecurity, while the sector is undergoing digital transformation.

Low digital and cybersecurity awareness in the railway sector. Overall, staff awareness of the need for cybersecurity remains quite low, but OES report that awareness is slowly increasing, as cyber incidents targeting the railway sector increase and become public. For instance, after the Wannacry and NotPetya attacks, the cybersecurity teams of some OES in the railway sector have grown in numbers, following the examples of other sectors.

Difficulty in reconciling safety and cybersecurity worlds. In the railway sector, the importance of safety requirements is undisputable. For each update to introduce provisions for cybersecurity, safety teams need to ensure that safety mechanisms remain intact. This requires extra time and money. Moreover, stakeholders in charge of safety issues are not historically aware and trained to deal with cybersecurity. This complicates relations between safety and cybersecurity staff. Additionally, it appears to be difficult to deal simultaneously with safety and security authorities. Each have their own requirements that may sometimes overlap or contradict each other (e.g. managing system updates for cybersecurity, while obsolete IT components may still be accredited for the highest level of safety). This actually indicates that the discrepancy is evident not only from a technical perspective but in governance issues as well.

Digital transformation of railway core business. Most railway OES are currently undergoing digital transformation and a wide range of IT and connected devices (IoT) are introduced to railway systems, often without being properly procured, mapped and managed. These changes introduce new vulnerabilities and highlight the need for OT systems to comply with the same, or even higher, cybersecurity provisions as IT systems. Network assets, network connected devices, software developments should be treated with the same (or greater) care in the operational field. Like IT systems, OT systems should come with monitoring, supervision and administration tools offered or even embedded. Moreover new OT systems should have integrated already safety and cybersecurity requirements by design.

Dependence on the supply chain for cybersecurity. OES report that are heavily reliant on their suppliers, providers and other third parties for system updates, patch management, and lifecycle management (supplier as a term can even include cloud service providers). Reasons for this dependence include safety, operational and financial responsibilities, compliance with safety, cybersecurity and technical standards, cost, and contractual obligations. RUs and IMs rely on multiple suppliers for their IT systems, and even more so when it comes to OT systems on board trains or on trackside and OCC. Each supplier may adopt individual techniques to satisfy similar functional requirements. This can increase the challenge of standardization and the ability to define and implement baseline cybersecurity measures for all systems. Awareness of the need for cybersecurity and the associated skills vary according to each supplier. This leads to disparate levels of cybersecurity in OT systems. Moreover, provisions for suppliers are not defined under the NIS Directive, so they have less stringent statutory requirements to apply cybersecurity. Finally, several years may elapse between a tender process for a system and its deployment. In the meantime, cybersecurity requirements change and the supply chain may not be agile enough to integrate the new requirements.

Geographic spread of railway infrastructure and the existence of legacy systems. Railway infrastructure is distributed over a wide territory shared between metropolitan areas - where critical nodes of railway systems and networks require maximum availability, and in the countryside – where protection and maintenance costs time and money. Trackside equipment updates, in particular, can have an important financial repercussion.

Moreover, IMs and RUs manage many legacy or obsolete systems – with lifecycles calculated in decades – which are difficult or even impossible to upgrade in order to implement cybersecurity measures. Some manufacturers have even lost the technical skills to upgrade them. Obsolescent OT requires procedures, policies and human intervention for patches and updates, to ensure an adequate security level. Lifecycle management which covers cybersecurity should be planned and anticipated for new systems.

The need to balance security, competiveness and operational efficiency. Rail transport is often a public service, to be affordable for travellers. OES must keep ticket prices as low as possible, otherwise travellers will choose other transport modes. However, OES must implement cybersecurity measures which are costly, without being able to increase their own revenue by raising the price of train tickets. Therefore, OES often encounter major problems reserving budgets for cybersecurity projects. They have to tread a fine line between respecting the budget and increasing the level of security, as in other transport sub-sectors. Additionally, railways require nationwide investment (for trackside systems) by IMs, which also need to be financed by service revenue. By comparison, transport by water or air travels do not require investment all over the territory. Moreover, reinforcing the security of systems can complicate data flows and systems (*e.g.* cryptography, system segregation). These can strongly impact system performance or availability if any issues arise (e.g. expiry of a certificate).

Complexity and lack of harmonization of regulations for cybersecurity. For some OES, understanding statutory constraints, especially the NIS Directive, may be difficult. Compliance may require time-consuming work integrating large volumes of information and performing many administrative tasks, as OES try to comply with cybersecurity requirements imposed by different national regulations. Several report that beyond the NIS Directive, they have to comply with other national laws, such as national security or critical infrastructure ones. In general, OES recognise the importance of developing statutory cybersecurity requirements and initiatives at national and European levels. Benefits identified by OES include awareness raising, sharing of best practices, potential funding, and stronger requirements for cybersecurity on suppliers. However, such requirements should be harmonized across the EU, as OES that operate in multiple MS often face different compliance requirements. Such harmonization is key for the suppliers as well, as they often offer products and services across the EU. Finally, the security measures promoted by the NIS Directive are not at present specific to each sector. Some OES have expressed the need for more flexible operational guidelines to fit the specificities and organisation of the railway sector.

3.2 MINIMUM SECURITY MEASURES

The security measures examined in the survey were defined by the NIS Directive Cooperation Group[45]. They have been classified in 4 domains, and 29 security measures as depicted in the figure below. They are described in more detail in Table 8 of the Appendix.

Figure 8: Security measures for OES

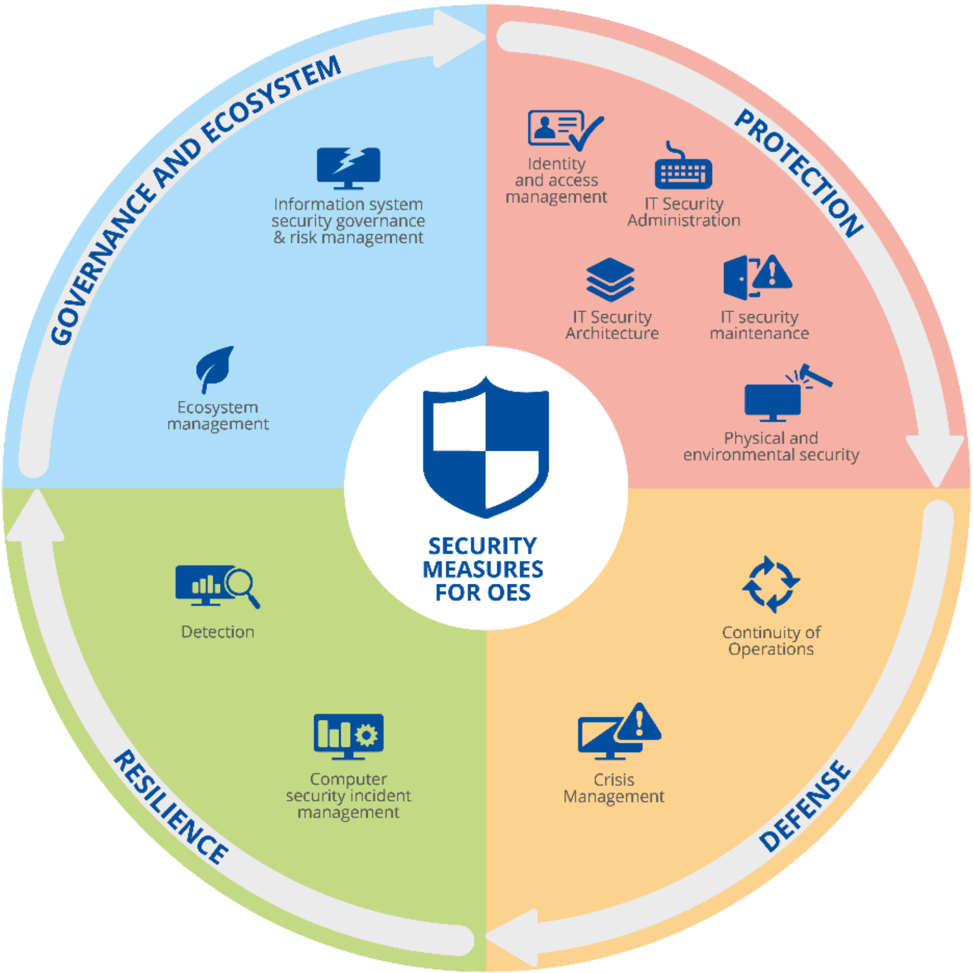

GOVERNANCE AND ECOSYSTEM
PROTECTION
DEFENSE
RESILIENCE
Information system security governance & risk management
Ecosystem management
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
SECURITY MEASURES FOR OES
Detection
Computer security incident management
Continuity of Operations
Crisis Management

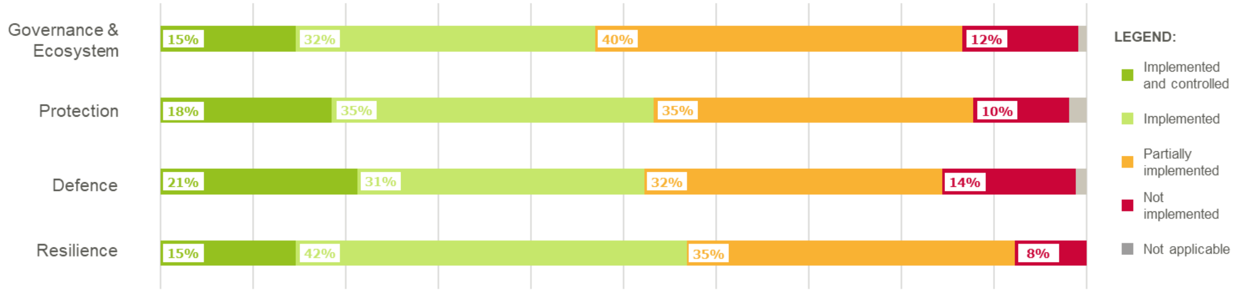
Figure 9 provides a high-level view of the level of implementation of security measures for OES in the railway sector, highlighting the differences between the four main domains of security measures.

- **Security measures related to governance, risk management and ecosystem management are either implemented or implemented and controlled by 47% of OES.** Several such measures are partially implemented because, in fact, several OES report that they are currently launching organisation-wide cybersecurity programmes, to comply with the NIS Directive and other national cybersecurity requirements, and to improve their cybersecurity posture. These measures can be particularly important as they often are a requisite step to increasing the implementation level for all security measures.

[45] See CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

- **Protection measures are implemented or implemented and controlled by 53% of OES**. Basic cybersecurity seems to be already well implemented and under control, e.g. access control, or system segregation. However, the security measures that require higher technical expertise, such as cryptographic controls, or cybersecurity controls on industrial control systems (OT) are implemented at a lower rate. This can be explained by specific context of railway OT that poses challenges to OES in fully implementing such minimum protection security measures. Reasons include the presence of legacy systems, the high number of systems and complexity of IM networks, dependence on suppliers for security solutions and safety concerns when updating such systems.
- **Security measures regarding defence are either implemented or implemented and controlled by 52% of OES.** Security measures that require less technical expertise, e.g. communications with competent authorities and CSIRTs, or incident reporting, appear to be well implemented and under control. Other measures that require resources, maturity and expertise (e.g. log correlation and analysis) appear to be more challenging for OES to implement.
- **Resilience measures are implemented or implemented and controlled by 57% of OES.** OES report that managing crises and incidents is part of the daily business in the railway sector. The sector is already regulated for safety and security, and operational continuity. However, these statistics should be treated with caution. Although measures to protect operations and prevent safety or security incidents are generally well applied, the same level of preparedness is not observed when countering cybersecurity threats and incidents. Current processes for crisis and business continuity management need to be adapted to cover cybersecurity incidents.

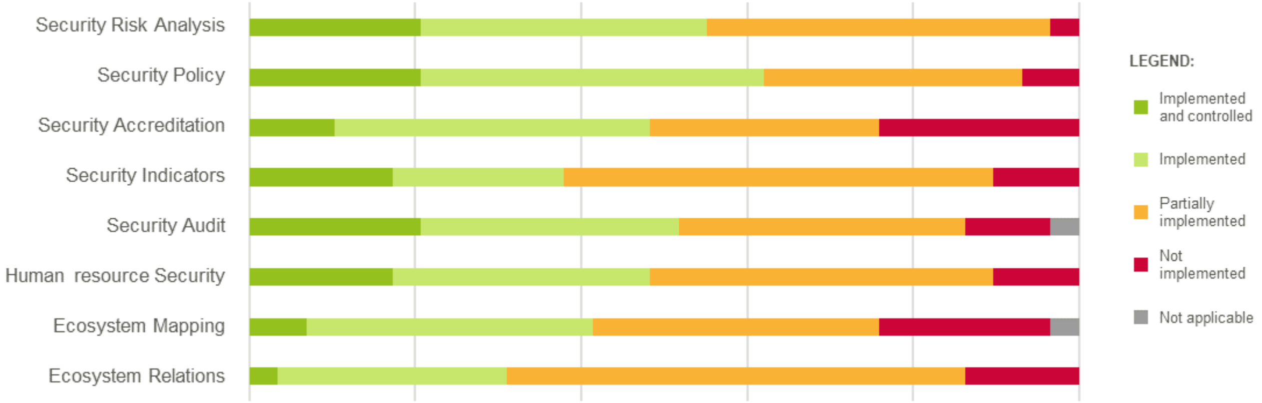
Figure 9: Overall view of the implementation level for cybersecurity measures



3.2.1 Governance and ecosystem

Based on the analysis of answers to the survey, Figure 10 highlights the implementation level of the eight security measures related to "Governance and ecosystem". This figure is followed by key findings, based on answers to the interview and desk research.

Figure 10: Implementation level of "Governance and ecosystem" security measures



Key findings

Key findings regarding the "Governance and ecosystem" security measures are as follows:

66% of OES have updated their Security Policy to include all systems of the organisation, including operational technology.

- The measure "Security Risk Analysis" seems to be partially implemented (55%). Indeed, when as IMs and RUs are identified as OES according to the NIS Directive, they are asked to identify their critical systems, based on a risk-based approach. Conducting a risk analysis is usually one of the first steps toward compliance with the NIS Directive. Most of the OES interviewed have on-going activities to fully apply this measure in the near future, coupled with updating their Security Policy to cover all systems of the organisation (66% have already implemented this measure).
- Regarding "Security Accreditation", security assessments seem to be implemented by 48% of the OES. OES recognise the importance of protecting critical systems by including cybersecurity reviews in all projects. However, it is not so easy to include cybersecurity in all railway projects, particularly because of their special characteristics. The construction of railway infrastructure and systems are lengthy projects, involving third parties and suppliers who are not always familiar with cybersecurity. Moreover, the requirements of cybersecurity regulations are relative newcomers, unlike safety requirements which already require systems accreditation. Enforcing a cybersecurity accreditation process seems to be perceived as a secondary step after setting up security measures.
- Defining, assessing and monitoring security indicators seem to be only partially implemented (38%). Governance and policies must be fully enforced, and experience on several security measures must be acquired before taking a step back to define the relevant Key Performance Indicators (KPIs). Furthermore, it must be possible to collect and process data from a potentially wide range of sources, which can pose an additional challenge to OES.
- For the "Security audit" measure (52%), two main trends can be highlighted: the most mature OES conduct regular audits to check the level of cybersecurity and compliance with their security policy, whereas the least mature ones regard this as a secondary step, to be taken after implementing security measures. For some OES, audits of legacy systems and others may be difficult to conduct. Finally, most OES are aware of the measures that need to be implemented to better protect their critical systems, but

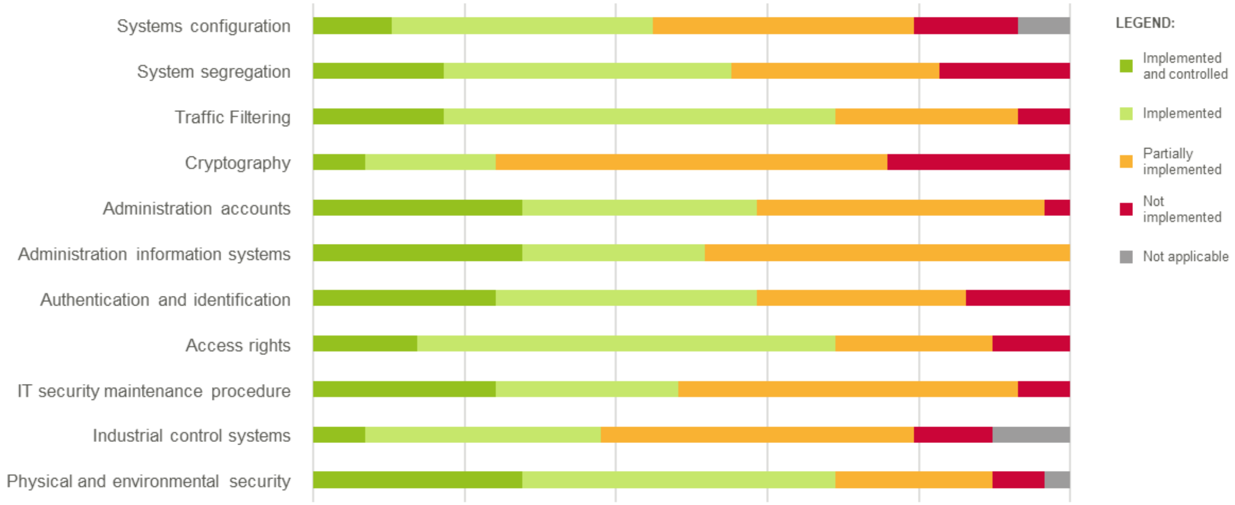
they perceive an audit a waste of time and budget, if implementation of measures has not progressed beforehand.

- "Human resource security" seems to be partially implemented (48%) for two main reasons: key personnel have been appointed by most OES (chief information security officers (CISO) and cybersecurity project managers are already at work, there are plans to appoint more cybersecurity experts) and awareness campaigns are being planned or conducted. However, awareness campaigns take time to produce results, especially in the railway sector where the core business is closer to the physical than the digital world, and even further from cybersecurity issues.
- The two security measures related to "Ecosystem management" appear difficult to implement and control completely. 41% of OES report that they have mapped their ecosystem and 31% have mapped relations to third parties. The railway ecosystem is complex to map, due to the number of third parties and suppliers. For instance, for one single system there may be several suppliers, with widely differing levels of technology thus cybersecurity.

3.2.2 Protection

Based on the analysis of answers to the survey, figure 11 presents the implementation of 11 security measures related to the security domain "Protection". This figure is followed by key findings, based on answers to the interview and desk research.

Figure 11: Implementation level of "Protection" security measures



Key findings

For security measures from the "Protection" domain, the key findings are as follows:

- Security measures, such as "Traffic filtering", and "Physical and environmental security" seem to be the most implemented (69% report that they have implemented them). "Traffic filtering" is considered as cybersecurity basics, is already set up for many years and every OES seem to have already deployed firewall systems and access control policies. "Physical and environmental security" is covered in the existing safety and security regulatory requirements and widely deployed. This shall be balanced as the rail network is usually very wide and it seems complicated to keep a homogeneous physical security of all local IT assets, which can be located in stations or near the tracks;
- The security measure "System configuration" has low implementation rate of this category (45%). Indeed, it seems that this security measure is difficult to apply to

legacy or old systems. As a result, most of the interviewed OES reserve this measure for the newest systems.

- The security measures "System segregation" seem to be the most implemented (50% for both) in this domain. Most OES have already segregated OT and IT systems and networks, but not yet tackled more advanced segregation (separating IT and OT systems based on business criticality for example). However, IT and OT tend to become more interconnected, so this could change the way of implementation and further complicate the segregation of critical systems from the others. European standards are seeking to propose a common definition as a solution to help solve this complexity.
- The security measure "Cryptography" seems to be the most difficult to implement (only 24%). Indeed, OT systems, often legacy systems, usually do not natively support cryptography mechanisms. Moreover, this measure requires setting up complex projects and defining special architecture for cybersecurity (e.g. public key infrastructure, certificate management) which requires specialised cybersecurity expertise. Lastly, implementing such measures can severely limit the availability of systems if they are not well managed (e.g. certificate lifecycle management).
- The security measures "Administrative accounts", "Access Rights" and "Authentication and identification" seems mostly implemented (59%, 69% and 59% respectively). It seems the railway sector is acutely aware of the criticality of administrative accounts and access rights. OES seem to have already set up the authentication and identification mechanisms (e.g. nominative accounts, strong passwords, logging registration), considered as cybersecurity basics. This is not always the case for legacy and embedded systems, usually OT, for which such measures (e.g. complex passwords) may not be possible. Projects are ongoing to fully implement this measure, while efforts are taken by OES to control better such access control processes.
- The security measure "Administration information systems" is relatively implemented (52%) which is expected due to the high dependencies the OES have against suppliers' systems and services. This rate will rend cybersecurity configuration into a requirement during procurement.
- The security measure "IT Security Maintenance procedure" seems less difficult to implement for RUs (71%) than for IMs (28%). It appears to be more difficult for IMs to map and maintain their systems, geographically distributed over the national territory with strong local specificities. By contrast, it seems easier for RUs which have to maintain their fleet of trains (mobile systems). Moreover, due to the ongoing trend for deregulating the railway sector, the railway market is being shared out among RUs – including newcomers managing fleets of new and modern trains which are easier to maintain. In the meantime, IMs have to go on managing more-or-less the same infrastructure and systems, some of which are legacy and obsolete and are difficult to maintain.
- The security measure "Industrial control systems" (ICS) has a lower implementation rate (38%). Indeed, usual security measures are not always applicable for those systems, as often they are legacy systems, without security by design, and changes to them raises safety concerns. It requires strong cybersecurity expertise to enforce compensatory security measures on those systems and rail ecosystem has a strong dependency on the supply chain on this. For newest systems, OES need to adapt the procurement process to include cybersecurity requirements and involve cybersecurity experts from the beginning, for systems that may be deployed on the network up to 5 years after the process. A few RUs also reported that those systems are not directly under their responsibility but under the responsibility of train suppliers.

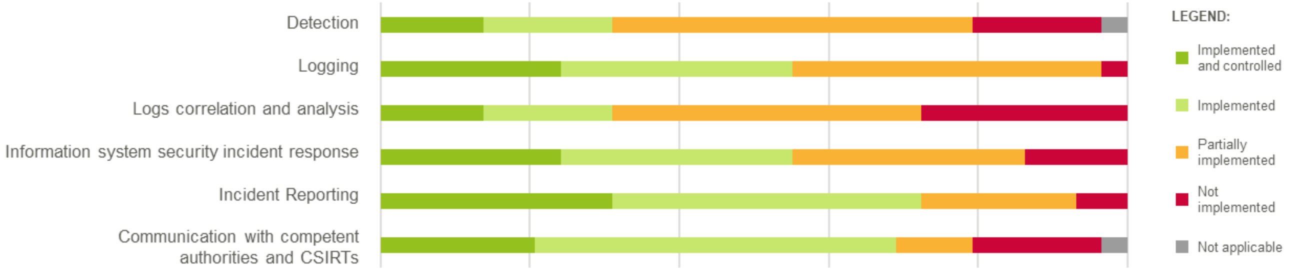
Cryptographic controls are the most difficult measure to implement in the sector (only 24% implement the measure). They require specialised cybersecurity expertise, and support from vendors, to ensure availability of systems and safety are guaranteed.

3.2.3 Defence

Based on the analysis of survey answers,

Figure 12 highlights the implementation level of the 6 security measures related to “Defence”. This figure is followed by key findings, based on answers to the interview, and desk research.

Figure 12: Level of implementation of “Defence” security measures



Key findings

Regarding “Defence”, the key findings are as follows:

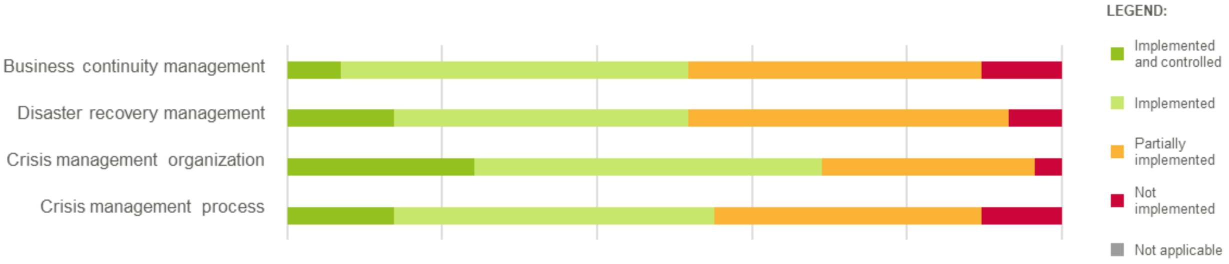
- The security measure “Communication with competent authorities and computer security incident response teams (CSIRT)” seems to be the most widely implemented (69%). Indeed, most of the OES communicate with the competent authorities about the NIS Directive and its implementation. This is only natural, as communication with relevant authorities in case of an incident is nowadays a legal requirement.
- The security measure “Logging” seems to be the most partially implemented by the majority of OES (55%), including IMs and RUs. Logging seems to be perceived as a cybersecurity basic, especially for standard logs (*e.g.* authentication, management of account and access rights). However, works are ongoing in order to apply these measures to IT systems or to update log management (logs are stored for longer).
- The security measures “Detection” (31%) and “Log correlation and analysis” (31%) seem to be the most difficult to implement. Specialised cybersecurity expertise and complex projects are required to deploy detection and log correlation and analysis mechanisms (e.g. vulnerability monitoring, identification of feared events, definition of detection rules based on existing or feared events). This finding is even more pronounced for OT systems, managed more generally by IMs.
- “Information system security incident response” (55%) and “Incident reporting” (72%) seem to be widely implemented. Dealing efficiently with incidents and reporting are vital skills in the railway sector. RUs and IMS must deal with safety or security incidents daily. However, existing incident management processes may need to be reviewed, to fully cover the specificities of cyber incidents.

69% of OES report that they fully implement “physical and environmental security” on all their infrastructures and networks.

3.2.4 Resilience

Based on the analysis of survey answers, Figure 13 highlights the implementation level of the 4 security measures related to "Resilience". This figure is followed by key findings, based on answers to the interview and desk research, in order to highlight the trends.

Figure 13: Implementation level of "Resilience" security measures



Key findings

- Security measures "Business continuity management" and "Disaster recovery management" seem to be partially implemented (both at 52%), for the same reasons as incident management. In the railway sector, most RUs and IMS seem to have already defined and tested business continuity and disaster recovery plans for safety, security and disaster (e.g. fire or flood prevention), managed and followed up by business teams. These plans must be updated to include cyber threats and their evolution (e.g. offline backups for resilience in case of a ransomware attack).
- The security measures "Crisis management organization" (69%) and "Crisis management process" (55%) also seem to be well implemented. For the reasons described above, stakeholders of the railway sector are accustomed to managing crises as part of their daily work. However, crisis management processes and exercises appear to concern mainly physical security and safety incidents (e.g. derailment, obstacles on track, power outages), but cybersecurity scenarios are not fully covered yet, and they require a different approach to crisis management. Crises require rapid intervention by IT and cybersecurity experts, and they may be more widespread – occurring in many stations at once - than local safety incidents - in a specific station for example. Most mature OES perform emergency exercises to simulate cyberattacks.

Cybersecurity scenarios are not covered yet on all railway OES, but mature railway organisations already perform emergency exercises to simulate cyberattacks.

4. CYBERSECURITY IN ERTMS

4.1 ERTMS DEFINITION AND ARCHITECTURE

The European Rail Traffic Management System (ERTMS) is a single European signalling and speed control system that ensures interoperability of the railway systems, with the aim of reducing the purchasing and, possibly, maintenance costs of the signalling systems. It can, in some cases, as well increase the speed of trains and the capacity of infrastructure. The main added benefit of ERTMS is to allow interoperability, stepping away from the installation of diverse trackside systems requiring the corresponding distinct on-board systems. ERA plays the role of system authority for ERTMS. In that respect, it establishes a transparent process to manage, with the contribution of the sector's representatives, any system changes.

ERTMS comprises of the European Train Control System (ETCS), i.e. a cab-signalling system that incorporates automatic train protection, the Global System for Mobile communications for Railways (GSM-R) and operating rules. More specifically:

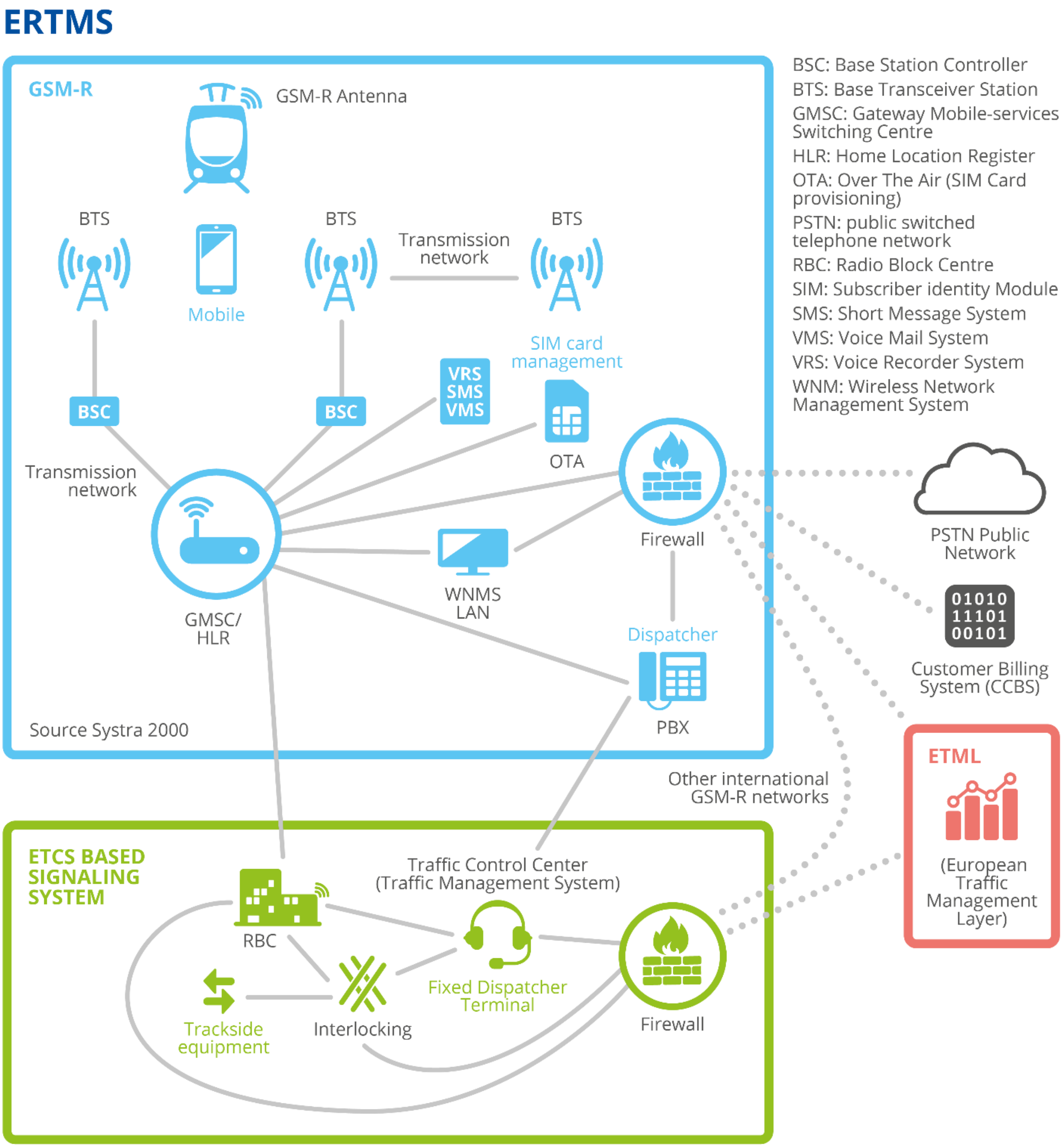
ERTMS comprises of the European Train Control System (ETCS), i.e. a cab-signalling system that incorporates automatic train protection, the Global System for Mobile communications for Railways (GSM-R) and operating rules. More specifically:

- ETCS (European Train Control System). The signalling element of the system which includes the control of movement authorities, automatic train protection and the interface to interlocking in a harmonised way. It allows the stepwise reduction of complexity for train drivers (automation of control activities) - It brings trackside signalling into the driver's cabin - It provides information to the on-board display - It allows for permanent train control – The train driver concentrates on core tasks.
- GSM-R (Global System for Mobiles - Railway). The telecommunication network offers both a voice communication service between driving vehicles and line controllers and a bearer path for ETCS data. It is based on the public standard GSM with specific railway features for operation e.g. Priority and Pre-emption (eMLPP) - Functional Addressing Location Dependent Addressing - Voice Broadcast Service (VBS) - Voice Group Call (VGC) - Shunting Mode - Emergency Calls - Fast call set-up. General Packet Radio Service (GPRS option) can also be used in GSM-R networks to offer more data possibilities.

ETML (European Traffic Management Layer). The operation management level is intended to optimise train movements by the "intelligent" interpretation of timetables and train running data. It is expected to involve the improvement of real-time train management and route planning - railway node fluidity - customer and operating staff information across international railway networks.

The following illustration provides an overview of the main ERTMS equipment and its interconnections.

Figure 14: ERTMS systems


ERTMS
GSM-R
GSM-R Antenna
BTS
Mobile
BTS
Transmission network
BTS
BSC
BSC
VRS
SMS
VMS
SIM card management
OTA
Transmission network
GMSC/ HLR
WNMS LAN
Firewall
Dispatcher
PBX
PSTN Public Network
01010
11101
00101
Customer Billing System (CCBS)
Other international GSM-R networks
ETML
(European Traffic Management Layer)
ETCS BASED SIGNALING SYSTEM
RBC
Traffic Control Center (Traffic Management System)
Fixed Dispatcher Terminal
Trackside equipment
Interlocking
Firewall
BSC: Base Station Controller
BTS: Base Transceiver Station
GMSC: Gateway Mobile-services Switching Centre
HLR: Home Location Register
OTA: Over The Air (SIM Card provisioning)
PSTN: public switched telephone network
RBC: Radio Block Centre
SIM: Subscriber identity Module
SMS: Short Message System
VMS: Voice Mail System
VRS: Voice Recorder System
WNM: Wireless Network Management System

Source Systra 2000

Figure 15: Communication in the ERTMS

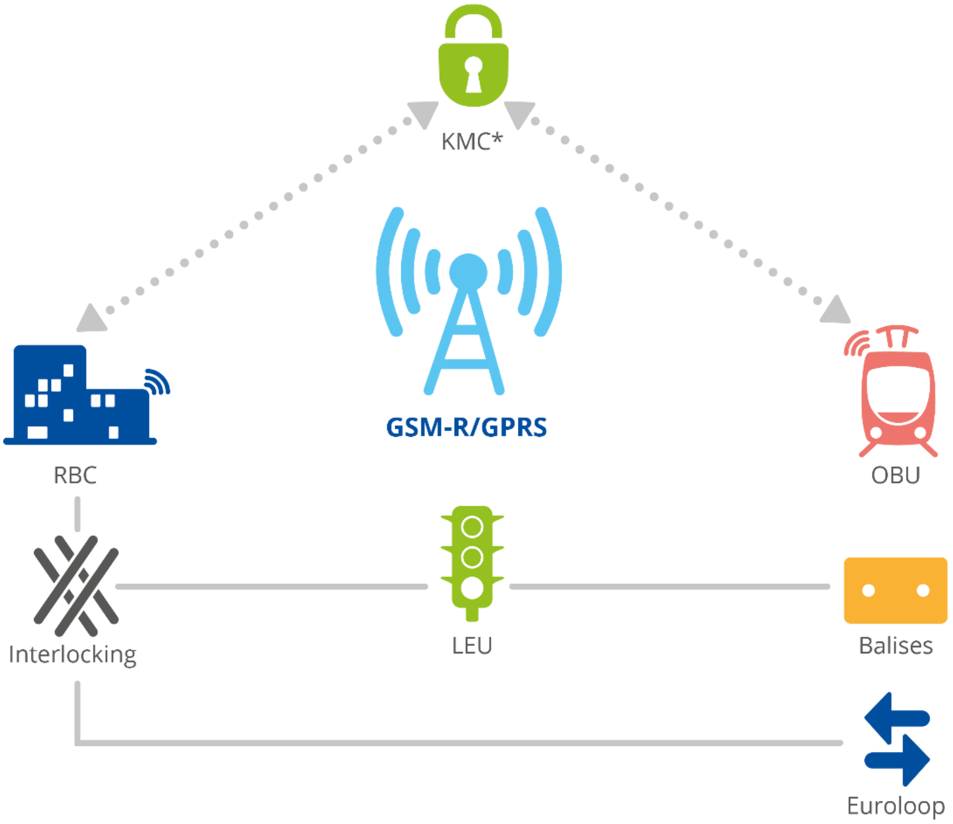


Figure Note:

Radio Block Centre (RBC), On-Board Unit (OBU), Lineside Electronic Unit (LEU), Key Management Centre (KMC): *keys can also be distributed offline to the vehicles, e.g. via USB keys

Source: Adapted by an illustration of the CYSIS Working Group

The following communication subsystems and functions require protection:

- **balise interfaces** (yellow marks in the above figure)
  - programming of balises
  - balise – infrastructure interface (train, interlocking, LEU, and/or field elements)
- **on-board unit (OBU) interfaces**
  - OBU – RBC via GSM-R or – in future – further data circuits according to the Future Railway Mobile Communication System (FRMCS)
  - OBU – vehicle bus system(s) (not ETCS-specific)
- **radio block centre (RBC) interfaces**
  - RBC – OBU via GSM-R or – in future – further data circuits
  - RBC operator interface
  - RBC – interlocking
- **key management centre (KMC) for the ETCS**[46]
  - operator interfaces, i.e. set-up keys and access authorisation
  - transmission of the keys to the operative subsystems, i.e. OBU and RBC
  - KMC-ETCS entities via GSM-R
  - KMC-KMC via different networks

[46] At present, the keys are mainly transmitted off-line. In future, they will be more and more transmitted on-line.

4.2 CYBERSECURITY ON ERTMS

ERTMS is a standardised solution with an architecture defined in the Control Command and Signalling Technical Specifications for Interoperability (CCS TSI)[47]. However, maintenance tools and the external interfaces (interlocking, maintenance system, traffic management system (TMS), etc.) are open and depend on the chosen system supplier. More and more systems allow remote access through maintenance tools to the radio block centre (RBC), GSM-R, etc., increasing the associated risks and widening the attack vector. More and more information management systems (IMS) require global connected systems to improve the performance and provide new services to passengers.

As any signalling and command and control system, ERTMS has high availability and safety integrity requirements, as these are related to service provision and safety. If we consider cybersecurity, these are reflected on availability and integrity requirements for the ICT systems. Confidentiality requirements refer mainly to the protection of information needed for access control in relevant systems or to the protection of cryptographic keys. For example, there is high need for protection of the radio block centre (RBC) in respect of its availability and integrity for the following two reasons:

- If it fails, and especially if it fails on lines without conventional signalling, it would:
  - make the line nearly inoperable; trains would have to be re-directed, which would overload other lines;
  - mean that the trains on the line in question would have to clear the relevant section, i.e. measures that would reduce the operational safety would inevitably have to be taken.
- It is, of course, of decisive importance for signalling and control-command systems that the data are collected, transmitted and processed correctly as corrupted, untimely or suppressed data could have consequences to operational safety.

As any signalling and command and control system, ERTMS has high availability and safety integrity requirements, as these are related to service provision and safety.

If we consider cybersecurity, these are reflected on high availability and integrity requirements for the ICT systems.

Moreover, the communication interfaces, such as communication between the vehicle and the track, should be protected against attacks. An attack on communication via a few manipulated balises and their telegrams seems to be very disproportionate in view of the short effective radius, but that does not mean that the likelihood of such an attack could be ignored. An attack on the communication via the radio interface is more critical because it can be made at a remote workstation and, thus, affect several vehicles at the same time resulting into a large scale crisis (possibly DDoS attack), impacting both safety and availability. Securing communication interfaces should become a priority for the Railway community and ERA.

This is also relevant for the other trackside elements (radio infill, euroloop, balises, LEUs), and for the OBU: when those elements fail, it may have a negative safety consequence or it may not allow the train to continue its trip.

The development of ETCS is according to European standards (including EN50128, EN50129) and complies with safety integrity level 4 (SIL4) requirements. If an internal failure occurs, the train should be stopped by the system. However, threats can impact operations and some safety functions, such as speed restrictions. Some cybersecurity measures are already available, but an in-depth analysis of threats, attack vectors and measures to be derived in this context has not been conducted yet. A detailed analysis is needed to assess which cybersecurity requirements for railway systems including ERTMS should be mandatory or optional features, and which minimum specifications for such controls should be offered by ERTMS suppliers. For instance, up-to-date cryptographic requirements should be specified.

[47] See https://www.era.europa.eu/activities/technical-specifications-interoperability_en

A recent analysis by CYSIS Working Group (Subgroup: ETCS and Security) works towards this direction. It reveals that it is very unlikely that an attack on the balises will be successful due to the implemented security functions, in case these are active. Man-in-the-middle attacks are at least in principle possible, but only if the symmetric keys in use are attacked simultaneously with purposively tapping of the communication. Moreover, an attack in the form of purposive manipulation and copying of the GSM-R infrastructure is possible, but only at extremely high efforts.

Several cybersecurity measures for rail systems like the one analysed in the previous section, are also needed for ERTMS. Implementation of cybersecurity measures, however, face challenges in ERTMS:

- Several measures are directly dependent on ERTMS supply chain and it is difficult to implement/enhance these measures in legacy systems.
- Software updates are complex, expensive, time consuming and dependent on the intervention of ERTMS suppliers. In some cases, those updates could even require a review of vehicle authorisation.
- Lack of rigorous tender specifications to be shared amongst OES make any implementation even more cumbersome.

Examples of types of cybersecurity measures for ERTMS would include:

- measures for the balises/loop to verify the authenticity of data, i.e. by signing the data;
- measures to minimise the effect of reduced availability on the communication between the OBU and the RBC;
- measures for integrity and authenticity of the communication, especially from and to the RBC;
- event logging and analysis;
- access control measures, such as “Administrative accounts” and “Authentication and identification” security measures;
- an update/patching policy for key components, e.g. GSM-R, RBC etc.;
- ensuring network controls are implemented (network segregation, no direct internet connection, no remote access by administrators, ensuring unnecessary services, interfaces, protocols and port numbers are not activated, etc.);
- state-of-the-art key and certification management and distribution; and
- a scalable key management centre (KMC) and the related public key infrastructure (PKI).

These measures are mere examples and need to be assessed for feasibility after a threat assessment of the ERTMS is conducted.

5. CONCLUSIONS

For the Railway sector the introduction of IP networks in signalling and power systems is a key issue to be assessed and further understood. The implementation of the NIS Directive in the railway sector varies between the MS and the OES. Concerning the transposition of the NIS Directive, each MS has adopted its own way of defining essential services, identifying Operators of Essential Services (OES), assigning national or sectorial competent authorities and defining the acceptable means for compliance with the Directive.

Furthermore, each OES has its own way of implementing security measures, according to its cybersecurity maturity, digital skills, size, business challenges, suppliers and the resources allocated to cybersecurity.

The overall trend shows that the security measures identified by the Cooperation Group for the NIS Directive are relevant to the railway stakeholders who responded to the study, and that the majority of security measures appear to have been in place.

5.1 SECURITY MEASURES

The security measures most widely implemented by OES are the following:

- cybersecurity basics (e.g. administrative accounts, security policy, logging, traffic filtering),
- measures beyond the requirements of cybersecurity (particularly for railway operations, such as business continuity),
- legal requirements such as safety and physical security (e.g. physical and environmental safety, crisis management, incident reporting).

5.2 CONSIDERATIONS

Security measures requiring special cybersecurity expertise and strict cybersecurity governance are more complex to implement (e.g. cryptography, industrial control systems, log correlation and analysis). This must be adapted according to the type of system (IT or OT). It is often impossible to fully enforce even the simplest security measures on OT systems. When OES in the railway sector enforce the NIS Directive, they have to deal with the following challenges:

- an overall low digital and cybersecurity awareness in the railway sector in the railway sector, coupled with conflicts between safety and security mind-sets,
- the characteristics of railway infrastructure and the OT environment (dependence on the supply chain, geographic spread of railway infrastructure, legacy systems),
- a growing need in the transport sector to strike a balance between cybersecurity, competiveness and operational efficiency, combined with the on-going digital transformation of railway, and
- the complexity and lack of harmonization of cybersecurity regulations, which must be fully understood to be put into practice.

5.3 NEXT STEPS

Trying to address some of the challenges described above, several European initiatives take place.

Standardization

At the standardization front, CENELEC’s Technical Committee 9X “Electrical and electronic applications for railways” is finalising the European technical specification TS 50701, which aims to introduce the requirements as well as provide recommendations for addressing cybersecurity within the railway sector. ERTMS technical specifications update is been considered to include stronger cybersecurity, taking as a priority enhancing the security of communication interfaces between different components.

Policy

On the policy side, the NIS Directive and national implementations are undergoing continuous review. The European Commission and the Member states, with the assistance of ENISA, are working towards addressing the challenges identified above, especially those that relate to the policy and regulatory context. At the same time, the implementation of minimum security measures by OES is monitored by the Member states with the aim to identify potential improvements and areas where OES require further support. This report supports this activity and highlights rail-specific sectorial challenges.

Change of mind-set

Cybersecurity practices in the rail sector are evolving. Cybersecurity is slowly being integrated into the design of IT and OT for transport systems. Cybersecurity culture builds up among rail stakeholders, both OES and their suppliers. This is an indication of the way forward and of a grand change of mind-set; cybersecurity becomes a vital requirement for the rail transport sector.

APPENDIX

Table 5: Main EU Directives and Railway Packages

Year	Name	Description
February 2001	First Railway Package[48]	Three directives (2001/12/EC[49], 2001/13/EC[50] and 2001/14/EC[51]) known as the "railway infrastructure package", were adopted to give railway operators access to the trans-European network on a non-discriminatory basis. These Directives concern the development of the Community's railways, the licensing of railway undertakings, the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification.
2002-2004	Second Railway Package[52]	Based on the "White Paper: a strategy for revitalising the Community's railways"[53], this second package (Directives 2004/49/EC[54], 2004/50/EC[55] and 2004/51/EC[56] and Regulation (EC) No 881/2004[57]) presented new measures to improve and accelerate safety, interoperability and open up the rail freight market. It introduced common procedures for accident investigation and established safety authorities in each member state.
April 2004	Regulation (EC) No 881/2004[58]	Through this regulation, the European Commission established a European railway agency ("Agency Regulation")[59]. Its objective is "to contribute, on technical matters, to the implementation of the European Union's legislation aimed at improving the competitive position of the railway sector, by enhancing the level of interoperability of railway systems and developing a common approach to safety on the European railway system".
October 2007	Third Railway Package[60]	This third package (Directives 2007/58/EC[61], 2007/59/EC[62], Regulations (EC) No 1370/2007[63], No 1371/2007[64] and No 1372/2007[65]) introduced open access rights for international rail passenger services, regulated passenger rights and the certification of train crews, introducing a European driving licence that allows train drivers to circulate on the entire European network.
December 2013	TEN-T Core Network Corridors[66]	Regulations (EU) 1315/2013[67] and 13/16/2013[68] revised the guidelines for the TEN-T (Trans European Network for Transport)[69] to define a core network of infrastructure for all means of transport, with a specific focus on railways.
April and December 2016	Fourth Railway Package[70]	This fourth package established the Single European Railway Area to revitalise the railway sector and to improve its competitiveness, divided into two pillars:

[48] See https://ec.europa.eu/transport/modes/rail/packages/2001_en
[49] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001L0012
[50] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0013
[51] See https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32001L0014
[52] See https://ec.europa.eu/transport/modes/rail/packages/2004_en
[53] See https://op.europa.eu/en/publication-detail/-/publication/59802bc4-5957-4c0a-adb8-de8fb346af7a
[54] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004L0049
[55] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0050
[56] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0051
[57] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R0881
[58] See https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1445259097536&uri=CELEX:02004R0881-20090101
[59] See https://www.era.europa.eu/
[60] See https://ec.europa.eu/transport/modes/rail/packages/2007_en
[61] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007L0058
[62] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32007L0059
[63] See https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32007R1370
[64] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007R1371
[65] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007R1372
[66] See https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/en/maps.html
[67] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R1315&from=FR
[68] See https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1575297145263&uri=CELEX:32013R1316
[69] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2013.348.01.0001.01.ENG
[70] See https://ec.europa.eu/transport/modes/rail/packages/2013_en

Year	Name	Description
		- the ‘technical pillar’ in April 2016 (Directive (EU) 2016/797[71] and 2016/798[72] and Regulation (EU) 2016/796[73]), designed to ‘boost the competitiveness of the European railway sector by significantly reducing the costs and the administrative burden for cross-border railway services’ through different technical projects (ERTMS, ‘one-stop-shop’ IT tool, etc.), - the ‘market pillar’ in December 2016 (Regulation (EU) 2016/2338[74], Directive 2016/2370/EU[75] and Regulation (EU) 2016/2337[76]), completing the process of opening up the market by establishing a general right for railway undertakings, and introducing measures to improve the independence and impartiality of infrastructure managers.

Table 6: Main EU Directives and Regulations regarding cybersecurity

Year	Name	Description
2013	First EU Cybersecurity Strategy[77]	This first EU Cybersecurity Strategy set out “strategic objectives and concrete actions to achieve resilience, reduce cybercrime, develop cyber defence policy and capabilities, develop industrial and technological resources and establish a coherent international cyberspace policy for the EU”.
2016	Regulation (EU) 2016/679[78]	This Directive, also called the General Data Protection Regulation (GDPR), addressed the protection of natural persons regarding the processing and the free movement of personal data, defined requirements for the protection of personal data in all sectors including railways.
2016	Directive 2016/1148[79]	The NIS Directive is an EU-wide cybersecurity legislation harmonizing national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU.
2017	Regulation (EU) 526/2013[80]	This Regulation established the "EU Cybersecurity Agency", also called ENISA (European Union Agency for Network and Information Security).
2019	EU Cybersecurity Act[81]	The EU Cybersecurity Act strengthened the position of ENISA for cybersecurity matters in EU member states and defined an EU-wide cybersecurity certification framework for ICT products, services and processes. This framework will provide a comprehensive set of rules, technical requirements, standards and procedures in order to attest that ICT products and services can be trusted, based on EU requirements.

[71] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0797
[72] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0798
[73] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.138.01.0001.01.ENG
[74] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R2338
[75] See https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L2370
[76] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R2337
[77] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001
[78] See https://eur-lex.europa.eu/eli/reg/2016/679/oj
[79] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=FR
[80] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526
[81] See https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

Table 7: List of standards

Standard	Description
ANSI/EIA 649B	American National Standards Institute/Electronic Industries Alliance
APTA	Security and Emergency Management Standards (USA) Part 1: Elements, Organization and Risk Assessment/Management Part 2: Defining a Security Zone Architecture for Rail Transit & Protection of Critical Zones Part 3a: Attack Modelling Security Analysis White Paper Part 3b: Protecting the Operationally Critical Security Zone Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure
COBIT 2019	Control Objectives for Information and Related Technologies framework (ISACA)
C2M2	CYBERSECURITY CAPABILITY MATURITY MODEL (DOE, USA)
DIN VDE V 0831-104	Electric signalling systems for railways — Part 104: IT Security Guideline based on IEC 62443
EN 50125	Railway Applications — Environmental conditions for Equipment – Part 1: Rolling Stock and On-board equipment
EN 50126-1	Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
EN 50126-2	Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
EN 50128	Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems
EN 50129	Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling
EN 50159	Railway applications — Communication, signalling and processing systems — Safety-related communication in transmission systems
EN 60447	Basic and safety principles for man-machine interface, marking and identification - Actuating principles
EN 61508	Functional safety of electrical, electronic and programmable electronic systems
ERA	Common Safety Methods 2016 (2016/413) (EU)
ETSI TS 102 165	Telecommunications and Internet converged Services and Protocols (EU) Part 1: Method and proforma for Threat, Vulnerability, Risk, Analysis (TVRA) Part 2: Protocol Framework Definition; Security Counter Measures
ISA/IEC 62443	Security for Industrial Automation and Control Systems
ISO 22301	Business continuity and disaster recovery for critical infrastructure (International)
ISO 27000	Information technology — Security techniques — Information security Management Systems – Overview and Vocabulary
ISO 27001	Information technology — Security techniques — Information security Management Systems - Requirements
ISO 27002	Information technology — Security techniques — Code of Practice for Information Security Controls
ISO 27003	Information technology — Security techniques — Information security Management Systems - Guidance
ISO 27004	Information technology — Security techniques — Information security Management – Monitoring, Measurement, Analysis and Evaluation
ISO 27005	Information technology — Security techniques — Information security risk management
ISO 27032	Information technology — Security techniques — Guidelines for cybersecurity
ISO 27102	Information security management — Guidelines for cyber-insurance
ISO 31001	Risk management system
ISO/IEC 12207	Systems and software engineering — Software life cycle processes

Standard	Description
ISO/IEC/IEEE 15288	Systems and software engineering — Systems life cycle processes
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
NIST SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
NIST Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
TS 50701	Railway applications - Cybersecurity
UIC - 5-18005E	Guidelines for Cyber-Security in Railways
UL 2900	Software cybersecurity standards for network-connectable devices
UL 2900-1	General software cyber security requirements
UL 2900-2-2	Cyber security requirements for industrial control systems
UL 2900-2-3	Cyber security requirements for security and life safety signalling systems

Table 8: List of security measures[82]

Security Domain	Security Subdomain	Security Measure	Description
Defence	Computer Security Incident Management	Incident Reporting	The operator creates and keeps up-to-date and implements procedures for incidents' reporting.
		Communication with competent authorities and CSIRTs	The operator implements a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of Critical Information Systems (CIS), interconnections of CIS with third-party networks, etc.).
		Information system security incident response	The operator creates and keeps up-to-date and implements a procedure for handling, response to and analyses of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.
	Detection	Logging	The operator sets up a logging system on each CIS in order 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.
		Logs 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 in order to detect events that affects CIS security.
		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 in order to seek out events likely to affect the security of CIS.
Governance and Ecosystem	Ecosystem Management	Ecosystem mapping	The operator establishes a mapping of its ecosystem, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.
		Ecosystem relations	The operator establishes a policy towards its relations with its ecosystem in order to mitigate the potential risks identified. This includes in particular but is not limited to interfaces between the CIS and third parties.
	Information System Security Governance & Risk Management	Human resource security	The established information system security policies set up a CIS security awareness raising program for all staff and a security training program for employees with CIS related responsibilities.
		Information system 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 organization's performance, the maintaining of resources in secure conditions, users' access rights, authenticating access to resources, and resource administration.
		Information system 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 OES and identifies the main risks to these CIS.
		Information system 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 risks analysis.
		Information system 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.
		Information system security policy	Building upon the risks analysis, the operator establishes, maintains up-to-date and implements an information system security policy (ISSP) approved by senior management, guaranteeing high level endorsement of the policy.
Protection	Identity and access management	Authentication and identification	For identification, the operator sets up unique accounts for users or for automated processes that need to access resources of its CIS. Unused or no longer needed accounts

[82] See NIS Directive Cooperation Group Publication 01/2018 - Reference document on security measures for Operators of Essential Services http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

Security Domain	Security Subdomain	Security Measure	Description
			are to be deactivated. A regular review process should be established.
	Identity and access management	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.
	IT Security Administration	Administration accounts	The operator sets up specific accounts for the administration, to be used only for administrators that are carrying out administration operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list.
	IT Security Administration	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.
	IT Security Architecture	System segregation	The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems.
	IT Security Architecture	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.
	IT Security Architecture	Traffic filtering	The operator filters traffic flows circulating in its Critical Information Systems (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.
	IT Security Architecture	Systems configuration	The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS.
	IT Security Maintenance	IT security maintenance procedure	The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources.
	IT Security Maintenance	Industrial control systems	The operator takes the particular security requirements for ICS (control systems, SCADA systems, etc.) into account.
	Physical and environmental security		The operator prevents unauthorized physical access, damage and interference to the organization's information and information processing facilities.
Resilience	Continuity of operations	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.
		Business continuity management	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of IT security incident.
	Crisis management	Crisis management organisation	The operator defines in its ISSP the organization for crisis management in case of IT security incidents and the continuity of organization's activities.
		Crisis management process	The operator defines in its ISSP the processes for crisis management which the crisis management organization will implement in case of IT security incidents and the continuity of an organization's activities.

TP-01-20-709-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. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-412-1
DOI 10.2824/235164