Rail Security Expert Group

Legacy Mitigating Security Measures

25E157
1A
11.02.2026

Modification history

Version	Date	Modification / Description	Editor
1A	11.02.2026	Initial Release published after internal and external (CER/EIM) review	Klas Andren, Oliver Lovric, Katharina Mader Richard Poschinger, Patrick Rozijn, Saku Salo Valerio Salustri Andreas Schröpfer Max Schubert Erika Valletta

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

1.1.1.0 The purpose of this document is to provide comprehensive guidance on implementing appropriate and proportionate technical, operational, and organisational measures to effectively manage the risks posed to the security of network and information systems. This guidance aligns with the requirements set forth in the NIS2 Directive (EU) 2022/2555 [1], which mandates enhanced cybersecurity resilience across essential entities, such as signalling systems.

1.1.1.1 Key components of this approach include:

- Conducting thorough risk analyses to systematically identify, evaluate, and understand cybersecurity threats and vulnerabilities.
- Developing and implementing robust security policies and procedures designed to mitigate identified risks and ensure ongoing protection of critical digital assets.
- By adhering to these principles, organisations can strengthen their cybersecurity posture, ensure compliance with NIS2, and enhance their ability to prevent, detect, and respond to emerging cyber threats.

1.1.1.2 The document is structured in general chapters and in system specific chapters.

1.1.1.3 The general chapters explain fundamentals, the process and system wide valid definitions. These are chapters 1 to 3.

1.1.1.4 The system specific chapters present the recommendations based on system specific analysis. These chapters are presented in Chapter 4.

1.1.1.5 Chapter 5 provides the management summary.

1.2 References

1.2.1.0 Subsets and EUG publication are referenced directly with their corresponding ID.

Other referenced documents:[1]

[1] E. Commission, NIS2 Directive (EU) 2022/2555, Brussels, 2022.

[2] EU-Rail System Pillar CyberSecurity Group, „Taxonomy and References 1.00,“ 2025.

[3] EU-Rail System Pillar CyberSecurity Group, „Secure Component Specification V1.00,“ 2025.

[4] EU-Rail System Pillar CyberSecurity Group, Secure Communication Specification V1.00, 2025.

[5] EU-Rail System Pillar CyberSecurity Group, Security Program Requirements Specification V1.00, 2025.

[6] EU-Rail System Pillar CyberSecurity Group, Shared Cybersecurity Services Specification V1.00, 2025.

[1] EU-Rail CyberSecurity Publications are available at https://rail-research.europa.eu/horizontal-tasks/

1.3 Abbreviations

ERTMS Abbreviations are listed in Subset-023.

EU-Rail Abbreviations are listed in [2]

1.4 Disclaimer

1.4.1.0 This guideline is purely advisory and does not have any legal binding effect. It is not meant to substitute the frameworks, guidance, tools, or other mechanisms established by Railways at the national level.

1.4.1.1 It should be emphasised that Railways maintain full discretion in deciding how to supervise compliance with the requirements when implementing the NIS2 regulation, by choosing the methods or processes that work best for them.

1.4.1.2 Nevertheless, the guideline provides a Railway’s agreed approach to fulfil the relevant EU regulations for legacy systems.

1.5 Authors

1.5.1.0 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.5.1.1 The following members of the Rail Security Expert Group were involved in creating this document:

- DB InfraGO
  - Katharina Mader
  - Andreas Schröpfer
- ERTMS User Group (EUG) / EULYNX
  - Richard Poschinger
  - Max Schubert
- SBB
  - Oliver Lovric
- Trafikverket
  - Jorge Gamelas
  - Klas Andrén
- NS
  - Patrick Rozijn
- RFI
  - Valerio Salustri
  - Erika Valletta

1.6 Applicability and Document Status

1.6.1.0 The document has the status of a guideline. It provides recommendations but is not binding.

2 Introduction

2.1.1.0 Legacy systems are outdated yet mission-critical platforms that have been in operation for many years within railway infrastructure. They impose unique and significant cybersecurity challenges, since they are commonly designed and developed long before the emergence of today's complex threat landscape and modern security standards. As a consequence, these systems typically lack the architectural resilience required to defend against sophisticated cyberattacks. Moreover, they frequently fall short of current regulatory requirements.

2.1.1.1 As a result, legacy systems constitute an attractive target for malicious actors, who exploit inherent vulnerabilities that are often difficult, costly, or even impossible to remediate through conventional patching or upgrades. Their continued use increases the risk of security breaches and operational disruptions, and their non-compliance highlights the urgent need for specialised risk management and mitigation strategies tailored to these systems.

2.1.1.2 Given the intensification and increased sophistication of cyber threats, the European regulatory landscape has also evolved to better regulate the field of cybersecurity. For this purpose, it is of importance to mention Directive (EU) 2022/2555 (NIS 2), among others. NIS 2 applies to essential and important entities listed in Annex I or II of the Directive, among which is the railway sector. NIS 2 requires a risk-based implementation of security measures to all railway systems, including existing installations.

2.1.1.3 The implementation of cybersecurity mitigating measures for legacy systems is not simply a matter of compliance or best practice; it is a strategic necessity. These measures are designed to reduce the risk of exploitation, safeguard sensitive data, and ensure continuity of operations, even when direct system upgrades or replacements are not feasible due to cost, complexity, or operational dependencies.

2.1.1.4 This document presents a comprehensive set of mitigation strategies developed through a risk-based approach that takes into account the unique characteristics and constraints of rail legacy systems. By adopting these measures, railways can securely extend the operational life of their legacy assets, bridge the security gap between past and present technologies, and maintain resilience in the ongoing challenge of meeting evolving cyber threats.

2.1.1.5 The recommendations are presented per system type, e.g. RBC, interlocking or level crossing to allow most suitable recommendations as the conditions per system type differ.

2.1.1.6 The purpose of this guideline is to provide railways across Europe with clear guidance on implementing effective counter measures aimed at preserving and strengthening trust both within individual railway organisations and between different railway operators.

3 Process

3.1 Check of side conditions

3.1.1.0 First, the side conditions have been checked to ensure regulatory compliance.

3.1.1.1 Check of regulatory requirements:

Regulation	Applicability
NIS 2	Use of the EU directive as the national adaption differs and is not available yet in every country
CRA	not applicable for installed base and spare parts. The applicability for new installations after 11/12/2027 is discussed in the upcoming guideline of the Cybersecurity Rail Sector Group (CRSG).
CSA	not applicable at the moment. Pointing to ENISA which should provide a certification level for railways first
Data Act	Not applicable at the moment but relevant to new products. Not taken into consideration in this document.
RED	Radio equipment only and with the application of the CRA the RED will be withdrawn.
TSI CCS	The TSI CCS 2023 applies to newly installed systems (with the 2023 requirements effective from 2025) and mandates backwards compatibility with the existing installed base

3.1.1.2 Check of standards requirements:

Standard	Applicability
IEC 62443-2-1	Applies to asset owner in general – independent if for legacy or new installations. It is used for the cybersecurity program.
ISO 27001	It is required to have an ISMS by NIS 2. ISO 27001 is referenced in this context. Can be used as a framework to comply with NIS 2 on company level.
IEC 63452 (TS 50701)	Not required, but can be used as input to comply with the regulations
EULYNX BL4R1 and newer	Required through tenders for new EULYNX installations
ERJU SP CyberSecurity Requirements	Starting to be required in tenders. Interoperability relevant requirements are going to be integrated in the next TSI CCS and further TSI (Energy, TAF/TAP, …)

3.2 Definition of Legacy

3.2.1.0 In railway cybersecurity, the term “legacy” describes systems that may not have the cybersecurity capabilities required from today’s perspective and as a consequence need mitigating counter measures, regardless of how long they have been in operation. This includes systems that are newly delivered and/or installed but have not been developed, integrated, and/or are not maintained according to cybersecurity regulations, standards, and specifications like EULYNX BL4R2 or newer, ERJU SP Cybersecurity Requirements, CLC/TS 50701, and/or EN IEC 62443.

3.2.1.1 That means, only systems developed according to the applicable and relevant regulations are treated as non-legacy.

3.3 Approach

3.3.1.0 First, Input documents have been checked for available compensating counter measures. The following inputs have been considered:

1. X2R3-WP08-T8.4 D8.2-5 “Security of legacy systems”
2. ERJU SP Cybersecurity Migration Guideline
3. IEC 63452 draft
4. NIS2

3.3.1.1 Second, an example cybersecurity risk analysis has been performed to identify the right methodology to derive the compensating counter measures.

3.3.1.2 The proposed security measures have then been evaluated based on their risk reduction benefits, implementation costs, and integration complexity to enable effective prioritisation

3.3.1.3 As a result, a list of cybersecurity compensating measures with indication of mandatory, recommended and not recommended has been provided (see chapter 3.7).

3.3.1.4 Finally, the residual risk has been presented to allow comparison with the targeted cybersecurity level for newly developed systems and the actual residual risk that has to be accepted by the railway (asset owner).

3.4 Risk Assessment Overview

3.4.1.0 The standard ERORAT risk assessment process has been used, which complies with IEC 62443 and TS 50701.

3.4.1.1 To effectively compare the identified risks and the suggested compensating cybersecurity measures with the ERJU System Pillar Cybersecurity Requirements (SPCR), the output of the risk assessment and the definition of compensating measures serve as the foundational basis.

3.4.1.2 Based on the available cybersecurity requirements, a decision has been made whether to apply the measure or choose an alternative mitigation.

3.4.1.3 At the end the residual risk based on the chosen measures has been evaluated.

3.4.1.4 In brief, the process looks as follows:

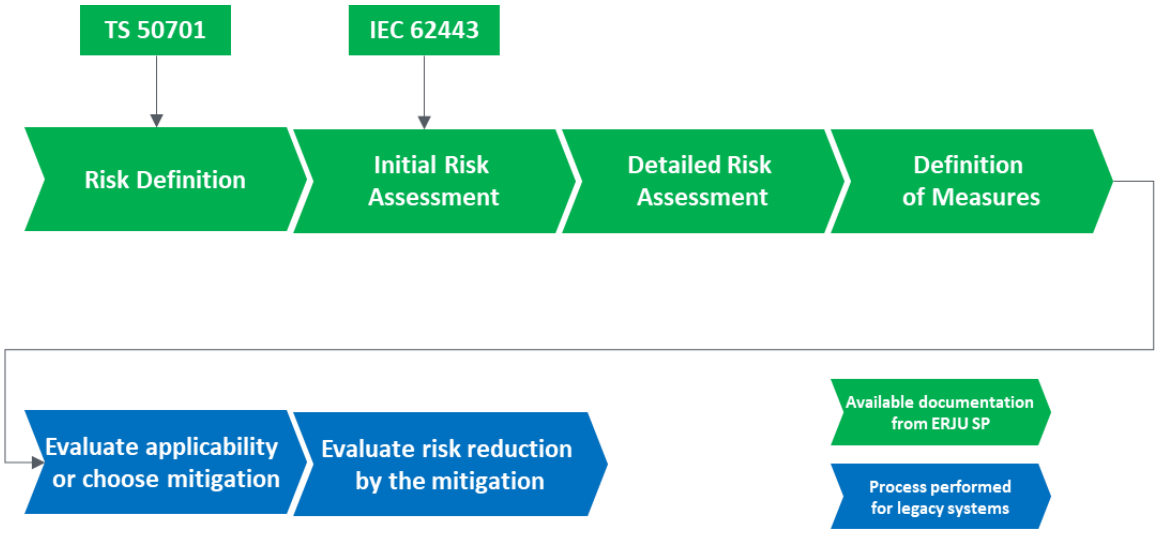


Figure 1 - Risk process

3.5 Risk Assessment and counter measure evaluation detailed

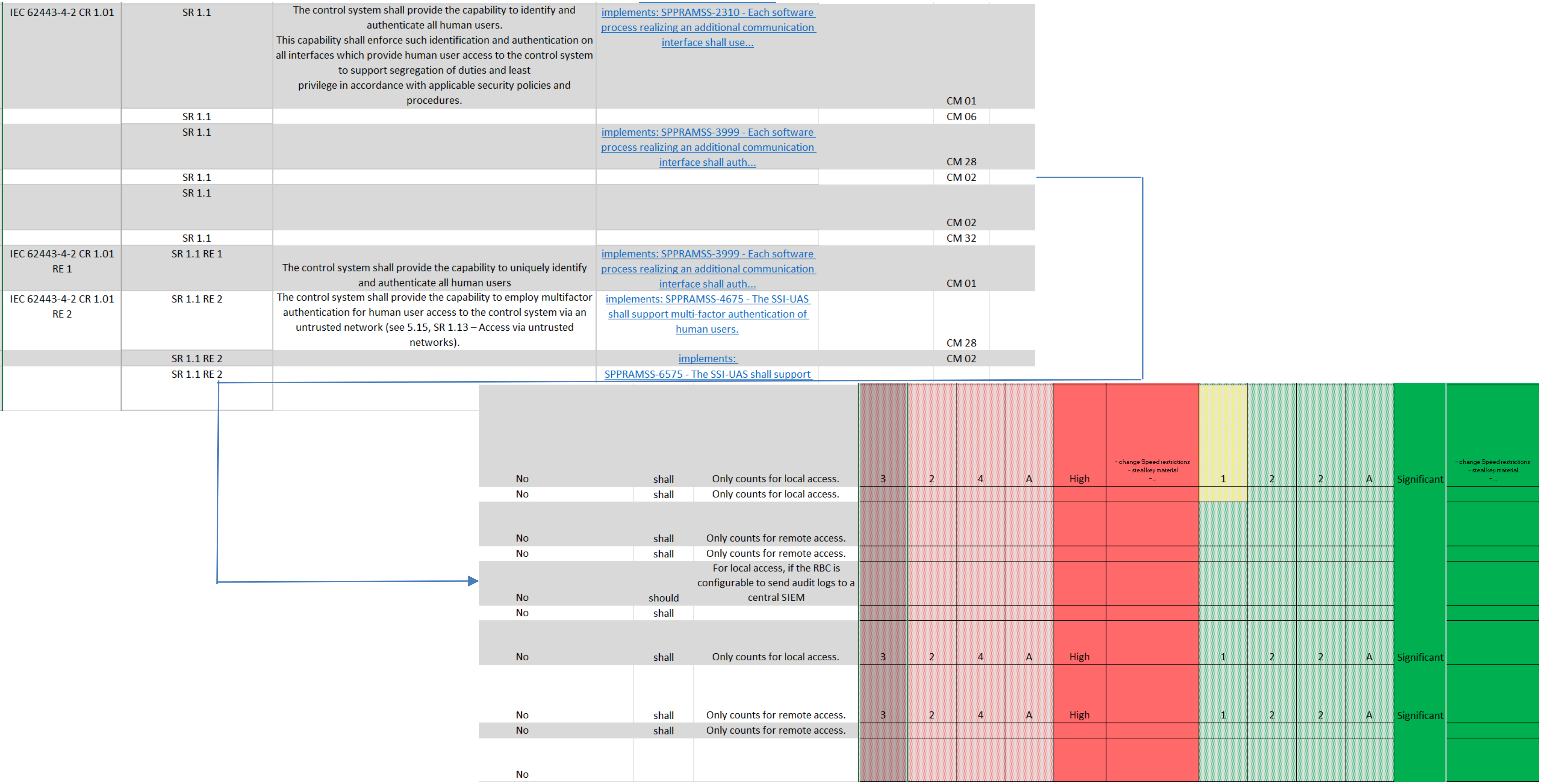
3.5.1.0 The following steps provide a detailed description of the evaluation process that will be used to assess risks and select the appropriate counter measures.

3.5.1.1 Starting with the System Pillar Secure Component Specification [3] (part of the SPCR) , a list of relevant System Requirements (SR) has been identified. This list serves as the foundational input for the assessment process, ensuring that all important cybersecurity criteria are considered.

3.5.1.2 For each SR it has been analysed if the cyber security measure could be applied to the legacy system or if an alternative counter measure must be applied.

3.5.1.3 Based on the chosen measure, the residual risk after implementation has been analysed (green)

3.5.1.4 Figure 2 shows this process.



IEC 62443-4-2 CR 1.01	SR 1.1	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	implements: SPPRAMSS-2310 - Each software process realizing an additional communication interface shall use...	CM 01
	SR 1.1			CM 06
	SR 1.1		implements: SPPRAMSS-3999 - Each software process realizing an additional communication interface shall auth...	CM 28
	SR 1.1			CM 02
	SR 1.1			CM 02
	SR 1.1			CM 32
IEC 62443-4-2 CR 1.01 RE 1	SR 1.1 RE 1	The control system shall provide the capability to uniquely identify and authenticate all human users	implements: SPPRAMSS-3999 - Each software process realizing an additional communication interface shall auth...	CM 01
IEC 62443-4-2 CR 1.01 RE 2	SR 1.1 RE 2	The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).	implements: SPPRAMSS-4675 - The SSI-UAS shall support multi-factor authentication of human users.	CM 28
	SR 1.1 RE 2		implements:	CM 02
	SR 1.1 RE 2		SPPRAMSS-6575 - The SSI-UAS shall support	

No	shall	Only counts for local access.	3	2	4	A	High	- change Speed restrictions - steal key material - ...	1	2	2	A	Significant	- change Speed restrictions - steal key material - ...
No	shall	Only counts for local access.												
No	shall	Only counts for remote access.												
No	shall	Only counts for remote access.												
No	should	For local access, if the RBC is configurable to send audit logs to a central SIEM												
No	shall													
No	shall	Only counts for local access.	3	2	4	A	High		1	2	2	A	Significant	
No	shall	Only counts for remote access.	3	2	4	A	High		1	2	2	A	Significant	
No	shall	Only counts for remote access.												
No														

Figure 2 - Risk Analysis SP input and counter measures

3.5.1.5 As a result of the detailed risk assessment and evaluation process described above, a comprehensive list of all possible counter measures has been compiled. The full range of these counter measures is presented and demonstrated in the following list providing a clear overview of the options available to address the identified risks.

CM 01 **Physical user access control**

Implement user identification mechanisms at critical physical access points such as building or room entrances. Examples include the use of personal key cards combined with magnetic locks, ensuring that only authorised personnel can enter sensitive areas. This measure enhances physical security by controlling and tracking access, thereby reducing the risk of unauthorised entry

CM 02 **Security Monitoring**

Deploy security monitoring capabilities to monitor network traffic and detect potential security breaches. This can be achieved through IDS, network taps or by other monitoring tools that provide continuous, real-time detection capabilities. This measure enhances situational awareness (observability), enables timely detection of unauthorised access attempts, and as a result supports rapid incident response.

The effectiveness of this measure is dependent on the implementation of CM 03.

CM 03 **Security Information and Event Management**

Install a Security Information and Event Management (SIEM) system to aggregate, correlate, and analyse security events and anomalies in the network. This includes setting up clear procedures for handling alarms and alerts to enable timely and effective incident response.

Additionally, existing log information, including from Physical user access control (CM 01), IT infrastructure (IAM, IDS, etc), system and maintenance logs shall be collected and aggregated, to support security event management, forensic analysis and incident response.

The SIEM infrastructure should be designed with scalability and future integration in mind, following relevant standards such as those outlined in the EUG 23E177 document (EUG Rail Security Expert Group Security Logging and SIEM Guideline).

CM 04 **Identity and Access Management (IAM)**

Deploy an Identity and Access Management (IAM**)** solution to centrally manage user identities, roles, and access permissions across the system. This includes integration with relevant subsystems such as authentication servers, directory services, and other supporting infrastructure. The IAM ensures that only authorised users with unique identities have access to specific systems and functions, based on defined roles and responsibilities. For the application of the requirement Authentication Gateway functionality for the relevant asset is required (CM 21).

CM 05 **Enhanced Physical Security**

Deploy Enhanced Physical Security Measures to strengthen physical security by implementing a layered approach that includes:

- Surveillance cameras with recording capabilities, and optionally active analysis triggered by events (e.g. motion detection, unauthorised access attempts),
- Physical barriers such as fences and secure perimeters to deter unauthorised access,
- Reinforced doors and access-controlled entry points (e.g. biometric or card-based systems) for high-security zones.

These measures help protect critical infrastructure from physical threats and support forensic investigations following any incidents.

CM 06 **Encryption**

Ensure integrity and, if needed, confidentiality of data exchanged between communication partners (e.g. between subsystems, control centres, or external stakeholders) by applying end-to-end encryption. This includes the use of modern cryptographic protocols (e.g. TLS, IPSec) to protect data in transit from eavesdropping, tampering, or man-in-the-middle attacks. Encryption shall be applied in line with current industry standards. If confidentiality is not required, the TLS 1.3 integrity only cipher may be used.

CM 07 **Firewalls**

Implement firewalls and filtering mechanisms to control and monitor traffic between communication partners. This includes:

- Network firewalls to enforce access control policies at the network perimeter or between internal zones,
- Application-layer filters to block unwanted traffic or payloads based on protocol behaviour or application content,
- Whitelisting/blacklisting of IP addresses, ports, and services.
- Such measures help prevent unauthorised access, reduce attack surfaces, and limit the spread of potential intrusions across interconnected systems.

CM 08 **Network Segmentation**

Introduce network segmentation to divide the overall system into logically or physically separated zones based on security levels, functions, or criticality. This measure reduces the attack surface and helps to enforce the principle of least privilege at the network level.

CM 09 **Hardening**

Apply hardening practices to systems, devices, and software components wherever possible. This includes but is not limited to the following activities:

- Disabling unused services and ports,
- Removing default accounts or credentials,
- Applying secure configuration baselines,
- Ensuring up-to-date patching and vulnerability management.

Hardening reduces the number of potential entry-points that attackers can exploit and strengthens the overall resilience of the system against both external and internal threats.

Where applicable, the CIS Benchmarks should be applied.[2]

CM 10 **Security Program**

Establish a structured Security Program (SP), see IEC62443-2-1 and IEC 63452/TS 50701) that encompasses all cybersecurity activities and ensures coordination with any existing Information Security Management System (ISMS)**.** This program shall, amongst other things, define roles, responsibilities, processes, for cybersecurity governance, awareness, incident response, and continuous improvement. If an ISMS is already in place, the security program should be aligned and integrated with it to promote consistency and strategic oversight.

CM 11 **ISMS**

In case of absence of an existing ISMS, initiate development of one to enable structured risk management, policy enforcement, and business continuity planning. An ISMS aligned with international standards such as ISO/IEC 27001, provides a systematic framework to manage sensitive information, define security controls, and monitor their effectiveness.

Additionally, establish formal coordination and communication channels between IT and OT security teams to ensure alignment across traditionally separated domains. This cross-domain collaboration is essential for addressing the unique challenges of managing control systems in railway operations and achieving a unified holistic security posture.

CM 12 **Asset Management**

Develop and maintain a comprehensive Asset Inventory through a dedicated Asset Management System. This system shall accurately record, classify, and organise all hardware, software, network components, and other critical assets within the system solution. Proper asset management enables better visibility and control, facilitating risk assessments, vulnerability management, and informed decision-making regarding system protection, security incident handling and lifecycle management.

[2] https://www.cisecurity.org/cis-benchmarks

CM 13 **Use Control Guidelines**

Establish clear, documented guidelines and rules governing personnel access to systems, data, and physical facilities. These policies shall define who is authorised to access which resources, under what conditions, using which authentication methods. Clear access rules help enforce the principle of least privilege, reduce insider threats, and ensure that access is regularly reviewed and updated in response to organisational changes.

CM 14 **Background Checks**

Implement background checks procedure for personnel involved in sensitive roles or with access to critical systems, following applicable national laws and regulations. These checks help mitigate insider risks by verifying the trustworthiness and reliability of employees. This includes but is not limited to contractors and third-party vendors before granting access.

CM 15 **Removable devices management**

Control the use of removable devices (e.g., USB drives, external hard disks) through strict procedures designed to prevent malware introduction or data leakage. This may include scanning devices in a secure, isolated environment (sanitised area) before using removable media for each operation or system change. These methods minimise the risk of infection and protect the sensitive systems from accidental compromise.

CM 16 **Disaster recovery process**

Develop and implement a comprehensive Disaster Recovery (DR) strategy encompassing clear processes for data backup, system restoration and full recovery. DR procedures often involve manual steps such as cleaning or replacing compromised systems and reinstalling software from verified clean images. Having a robust backup and restore plan maintains business continuity by ensuring rapid recovery from incidents such as cyberattacks, hardware failure, or natural disasters.

Aligned with the DR strategy an adequate stockpile of hardware spare parts shall be maintained to enable swift replacement of faulty or damaged equipment. This readiness reduces downtime by ensuring that critical components are readily available when needed, supporting timely restoration of operations.

CM 17 **Incident response team**

Introduce a process to form and activate a dedicated Security Incident Response Team (SIRT) that brings together representatives from both Operational Technology (OT), such as operators, maintenance personnel, and domain experts, and Information Technology (IT) teams, including SIEM/SOC analysts and Identity and Access Management (IAM) specialists.

The SIRT’s structure and activation procedures shall be based on predefined incident severity levels and clear rules of engagement. The team is activated only when necessary, ensuring efficient use of resources. The SIRT’s working process must be supported by

detailed logs and alerts from Intrusion Detection Systems (IDS) and other identified and relevant technical information systems, enabling timely detection, analysis, and response to security events. Thus, this CM is dependent on CM 2 and CM 3.

Management representatives, such as Safety and Security Managers or Officers and members of the board, should also be involved.

CM 18 **Incident reporting**

Create clear, documented processes and rules for reporting security breaches, including detailed guidelines on the immediate and follow-up actions to be taken.

These processes should be formally linked and agreed upon with the SIRT process to ensure coordinated and effective incident management. By implementing a **"**no fear, uncertainty, or doubt**"** policy to encourage personnel to report incidents or suspicious activities promptly and honestly, rather than hiding them. This culture of transparency is vital for early detection and mitigation of threats, ultimately strengthening the railway's security posture.

CM 19 **Security Awareness Training**

Conduct regular security awareness training tailored to the needs of various personnel groups, such as maintenance workers, system operators, and administrative staff. Training should cover cybersecurity best practices, recognising social engineering attempts, safe handling of sensitive information, and organisational policies. Well-informed personnel is a critical line of defence against cyber threats, as they are often the first to encounter and recognise potential security issues.

CM 20 **Knowledge management**

Develop and maintain a robust knowledge management system to ensure that critical system knowledge, including technical documentation, operational procedures, and security protocols, is preserved and accessible throughout the entire lifecycle of the systems.

This continuity safeguards railway staff turnover and supports consistent operation, maintenance, and security of the systems.

CM 21 **Authentication Server**

Implement a robust Authentication Server system to manage secure remote access. This solution typically includes a central authentication system responsible for verifying user credentials and enforcing access policies, along with an authentication gateway (e.g. realised by an existing firewall) that handles authentication requests at the entry to the security zone of the relevant asset.

Together, these security measures ensure that only authorised personnel can securely access systems remotely, reducing the risk of unauthorised access and potential cyber threats.

This CM is dependent on CM 04.

CM 22 **Public Key Infrastructure**

Implement a Public Key Infrastructure (PKI) system to manage digital certificates essential for authentication and encryption services across the railway organisation.

By adopting a PKI, railways ensure strong cryptographic trust relationships between systems and users, supporting secure access and data protection across system platforms and services.

CM 23 **Decommissioning process**

Establish a formalised process for the decommissioning and secure destruction of devices at the end of their operational lifecycle. This process should include steps to securely erase all sensitive data, physically destroy storage media if necessary, and properly dispose of hardware to prevent any potential data leakage or misuse. Adhering to strict decommissioning procedures helps mitigate risks related to data breaches.

CM 24 **Deactivation of interfaces**

Implement procedures to deactivate physical interfaces such as USB ports by default on all relevant systems to reduce the risk of malware introduction and data exfiltration. Access to enable these sensitive interfaces should be governed by a strict Dual Control process, where activation is only permitted for specific, documented operational needs.

CM 25 **Supply Chain Security**

The asset owner shall have policies and procedures that specify requirements for suppliers of products and services addressing cybersecurity risks to the system. The asset owner policies and procedures shall consider recursive requirements on the suppliers, where feasible (IEC 62443-2-1 ORG 1.6). The obligations arise from NIS 2. Nevertheless, it is a challenge to request the measures from existing contracts. The recommended application is to remind the suppliers on their obligations and make them accept these in every new and renewed contract.

3.5.1.6 The mapping between the IEC62443-3-3 System Requirements (SR) and corresponding counter measures has been established to create a linking of suggested Counter measures to the original System Pillar Cybersecurity Specifications [3] [4] [5] [6].

3.5.1.7 The following example in Figure 4 shows how the linking has been accomplished. By using the respective SR to address the threats in the original risk analysis, the link between Counter measures and threat mitigation is made.

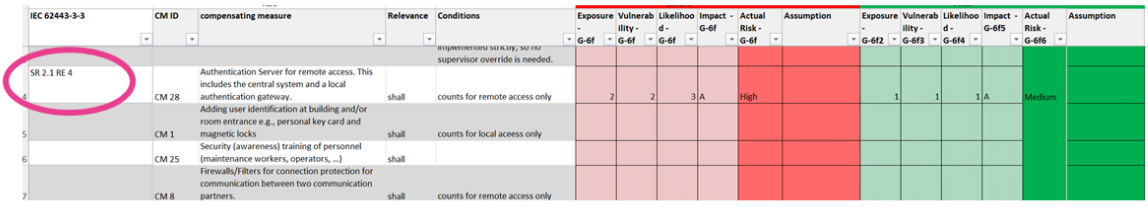
3.5.1.8 Following, the risk reduction has been analysed by using identified counter measures instead of the original measures used for a newly designed system.

3.5.1.9 Finally, the risk reduction has been demonstrated by a simple value expressing the number of reduced steps (very high, high, significant, medium, low). The maximum risk reduction is four (4). The maximum risk reduction reached is three (3).

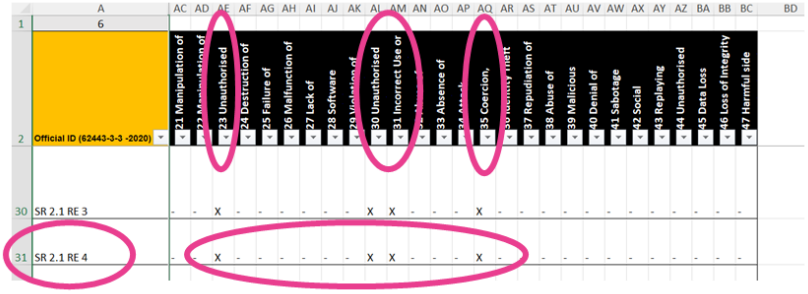
3.5.1.10 The effectiveness of each counter measure has then been evaluated. The risk reduction value (1,2,3) per threat has been divided by the number of used counter measures to calculate the actual risk reduction. The overall procedure is displayed in Figure 3.

3.5.1.11 Finally, the calculated impact value for each counter measure on threat is summed up over all threats providing one effect evaluation vale for each counter measure based on the effect it drives for risk reduction of the threats. This leads to the final comparable effectiveness value according to the direct effect on threat and thus risk reduction.

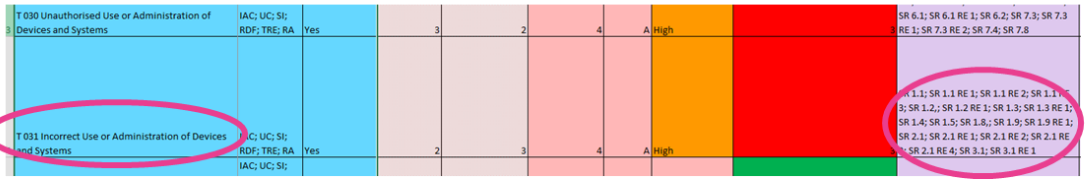
Integration of ERJU SP Security Requirements and provision of mitigating measure, if not directly applicable for legacy.



Use of EUG Security Risk Analysis to evaluate which Threats are managed by the security mitigating measure.



Integration of all security mitigating measures in the threat and risk analysis provided by EUG.



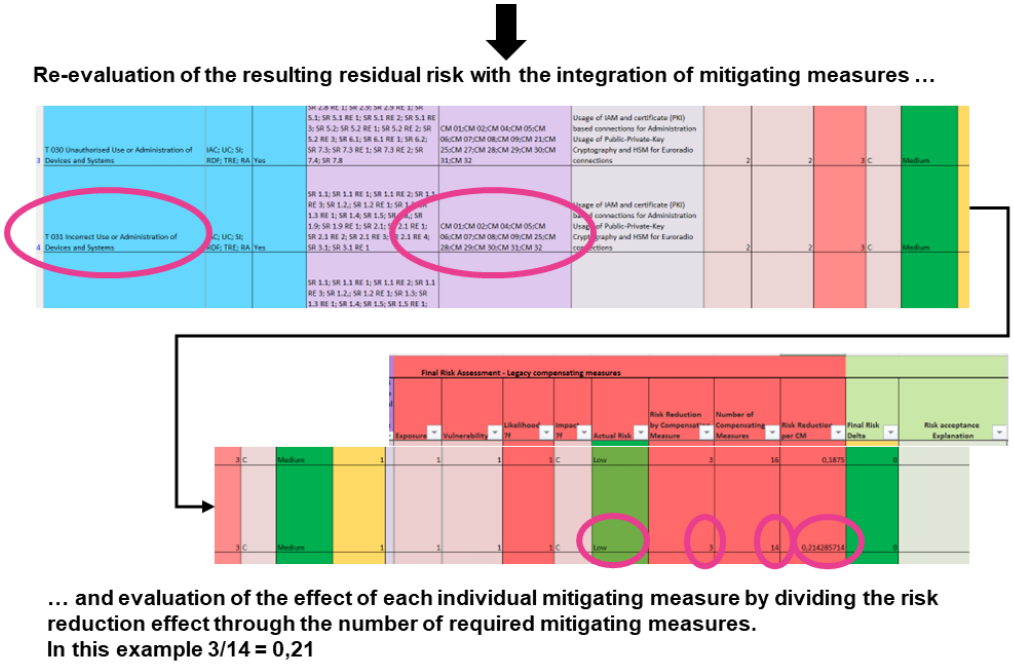


Figure 3 - Flow-Chart Risk Evaluation and Effectiveness Mitigating Measures

Target Risk:	Low																										
Threats			System Requirements - 7c			Risk Assessment - New development					Risk Delta		Final Risk Assessment - Legacy compensating measures														
Threat Catalogue	FR	Relevance	Measure (SR) from 62443	CM	Explanations for SRs	Exposure - 7d	Vulnerability -	Likelihood -	Impact - 7d	Actual Risk -	Risk Delta -	Spare	Exposure -	Vulnerability -	Likelihood -	Impact - 7f	Actual Risk -	Risk Reduction by Compensating Measure	Number of Compensating Measures	Risk Reduction per CM	Final Risk Delta							
T 014 Interception of Information / Espionage	DC;	Yes	SR 1.8,; SR 1.9; SR 1.9 RE 1; SR 3.1 RE 1; SR 4.1; SR 4.2; SR 4.2 RE 1	CM 01;CM 07;CM 08;CM 19;CM 28;CM 33		1	1	1	A	Medium	1		1	2	2	A	Significant	1	6	0,166666667	1							
T 018 Bad Planning or Lack of Adaption	SI; DC; RA	Yes	SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2	CM 08	e.g. Firewalls for remote administration and diagnostics	2	2	3	A	High	3		1	1	1	A	Medium	2	1	2	1							
T 020 Information or Products from an Unreliable Source	SI;	Yes	SR 2.4; SR 3.1; SR 3.1 RE 1; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.3; SR 3.3 RE 1; SR 3.3 RE 2; SR 3.4; SR 3.4 RE 1; SR 6.2	CM 02;CM 04;CM 07;CM 08;CM 10	SR 3.1 and SR 3.1 RE 1 only affects update files, SR 6.2 = SIEM, IDS-functionality	2	2	3	C	Medium	1		1	1	1	D	Low	3	5	0,6	0							
T 021 Manipulation of Hardware or Software	SI; TRE;	Yes	SR 3.1 RE 1; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.3; SR 3.3 RE 1; SR 3.3 RE 2; SR 3.4; SR 3.4 RE 1; SR 3.5; SR 3.6; SR 3.7; SR 3.9; SR 3.9 RE 1; SR 4.3; SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2; SR 5.1 RE 3; SR 5.2; SR 5.2 RE 1; SR 5.2 RE 2; SR 5.2 RE 3; SR 5.4; SR 6.1; SR 6.1 RE 1; SR 6.2; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.6; SR 7.6 RE 1; SR 7.7; SR 7.8	CM 02;CM 04;CM 07;CM 08;CM 21;CM 27		2	1	2	A	Significant	2		1	1	1	A	Medium	2	6	0,333333333	1							
T 022 Manipulation of Information	SI; TRE;	Yes	SR 1.8,; SR 1.9; SR 1.9 RE 1; SR 3.1; SR 3.1 RE 1; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.8; SR 3.8 RE 1; SR 3.8 RE 2; SR 3.8 RE 3; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.7; SR 7.8	CM 01;CM 07;CM 08;CM 21;CM 27;CM 28;CM 32	Implementations of encrypted connections (e.g. Variant A of EULYNX) between EIL and RBC Usage of TLS for Euroradio and in RBC to RBC connections (if possible, otherwise encryption tunnel)	1	2	2	A	Significant	2		1	1	1	A	Medium	2	7	0,285714286	1							

Figure 4 - Risk analysis resulting reduction and effectiveness

3.5.1.12 As a result, an evaluation of the effectiveness of each counter measure has been made available and is demonstrated below.

3.5.1.13 Overarching measures that form the foundation for the overall implementation of cybersecurity controls have been excluded from individual evaluation and have instead been designated as default (mandatory) measures. Every mandatory requirement is based on a legal (EU-)obligation to implement it.

3.5.1.14 The following list shows the mandatory overarching railway organisation measures.

- CM 10 - Security Program
- CM 11 - ISMS
- CM 12 - Asset Management
- CM 13 - Use Control Guidelines
- CM 17 - Incident response team
- CM 18 - Incident reporting
- CM 19 - Security Awareness Training
- CM 20 - Knowledge management
- CM 25 - Supply Chain Security

3.5.1.15 The following figure illustrates the evaluated technical measures as example, presented by their respective calculated evaluation value representing the effectiveness. The mandatory measures are not demonstrated in this chart.

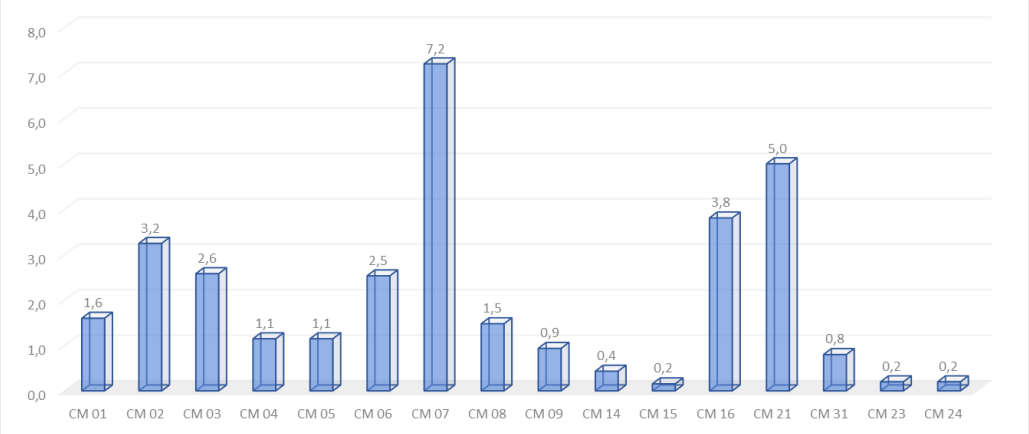


Figure 5 - Evaluation of technical measures example

3.6 Counter measure complexity

3.6.1.0 As a following step, each counter measure (CM) is evaluated concerning the complexity of its implementation.

3.6.1.1 The evaluation factors include time and cost.

3.6.1.2 Time for implementation of each counter measure is categorised in up to one year, up to three years, up to five years, more than five years.

3.6.1.3 Costs are defined as both initial (one-time) expenses and recurring annual expenses. These costs are categorized into three levels based on a best practice approach:

- low (under €10,000),
- medium (under €100,000), and
- high (over €100,000).

3.7 Prioritized counter measure list

3.7.1.0 Finally, an expert committee combines the complexity and effectiveness evaluation factors to classify each counter measure as follows:

- Mandatory – This measure has to be implemented
- Highly recommended – This measure should be implemented as it brings very high value and is relatively cost effective
- Recommended – This measure is strongly recommended but with a lower priority, either because the effectiveness is lower or the cost is relatively high
- Not recommended – This measure is not recommended to be used.

3.7.1.1 The following table shows an evaluation result example of the RBC. The measures with evaluation value 5,0 represent the overarching measures referred to in 3.5.1.14.

ID	Evaluation result *mandatory, highly recommend, not recommended*	Overall Evaluation explanation	Evaluation value	Time *< 1y, < 3y, < 5y, > 5y*	Cost result *low, medium, high*
CM 01	mandatory	Reduces the risk of unauthorised entry with relatively low effort and helps to implement NIS Article 21.2 human resources security, access control policies and asset management (i)	1,6	1	medium
CM 02	highly recommended	Introduces observability into the network and supports incident response. Low effort to implement with high benefits.	3,2	1	medium
CM 03	mandatory	Expected by ENISA, see NIS2 Technical Implementation Guidance. Installation of SIEM comes with a high initial cost.	2,6	3	high
CM 07	mandatory	NIS2 Article 21.2: basic cyber hygiene practices (g) access control policies (i). Furthermore, the implementation comes with a significant evaluation value.	7,2	1	medium
CM 11	mandatory	Overarching requirement. NIS2 Article 20 NIS2 Article 21.1	5,0	3	high
CM 17	mandatory	Overarching requirement. NIS2 Article 21.2 Incident handling (b)	5,0	3	high

4 System specific requirements

4.1 RBC

4.1.1 Measure evaluation

4.1.1.0 Following the evaluation result for the legacy RBC is presented.

4.1.1.1 The following figure illustrates the evaluated technical measures for the RBC, presented by their respective calculated evaluation value representing the effectiveness. The mandatory measures are not demonstrated in this chart.

4.1.1.2 The overarching measures (mandatory) from ID 3.5.1.14 apply in addition.

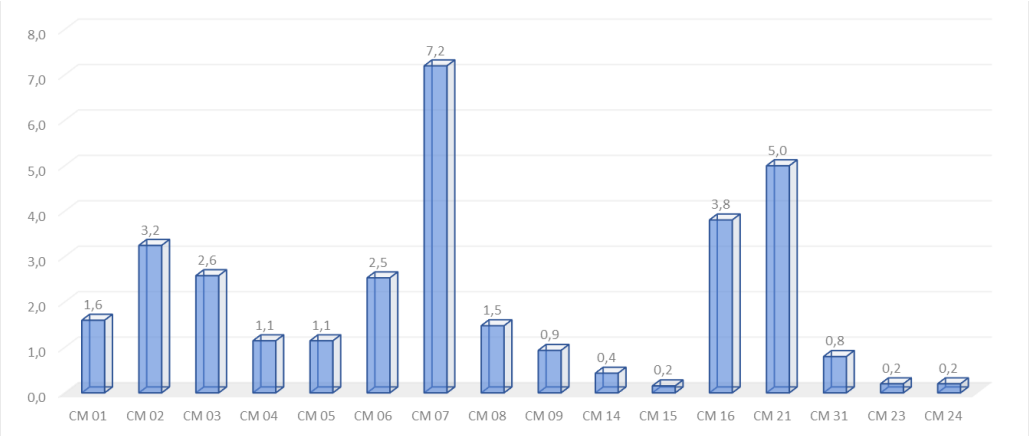


Figure 6 - Evaluation of technical measures RBC

Table 1 - Legacy RBC measure evaluation

ID	Evaluation result *mandatory, highly recommend, not recommended*	Overall Evaluation explanation	Evaluation value	Time *< 1y, < 3y, < 5y, > 5y*	Cost result *low, medium, high*
CM 01	mandatory	Reduces the risk of unauthorised entry with relatively low effort and helps to implement NIS Article 21.2 human resources security, access control policies and asset management (i)	1,6	1	medium
CM 02	highly recommended	Introduces observability into the network and supports incident response. Low effort to implement with high benefits.	3,2	1	medium
CM 03	mandatory	Expected by ENISA, see NIS2 Technical Implementation Guidance. Installation of SIEM comes with a high initial cost.	2,6	3	high
CM 04	mandatory	NIS2 Article 21.2 human resources security, access control policies and asset management (i)	1,1	3	high
CM 05	recommended	Relatively Low effort to implement and strengthens the implementation of NIS2 Article 21.2 human resources security, access control policies and asset management (i) Also strengthens the implementation of CM 01.	1,1	1	medium
CM 06	highly recommended	NIS2 Article 21.2 policies and procedures regarding the use of cryptography and, where appropriate, encryption (h) For Category 3 networks encryption is essential to guarantee the integrity of messages.	2,5	1	medium

ID	Evaluation result *mandatory, highly recommend, not recommended*	Overall Evaluation explanation	Evaluation value	Time *< 1y, < 3y, < 5y, > 5y*	Cost result *low, medium, high*
CM 07	mandatory	NIS2 Article 21.2: basic cyber hygiene practices (g) access control policies (i). Furthermore, the implementation comes with a significant evaluation value.	7,2	1	medium
CM 08	highly recommended	NIS2 Article 21.1 This could be considered as an appropriate and proportionate technical measure. Specifically mentioned in an own section in ENISA NIS2 Technical Implementation Guideline.	1,5	1	medium
CM 09	not recommended	Hardening of legacy systems can affect operation. Low determined evaluation value.	0,9	1	low
CM 10	mandatory	Overarching requirement. NIS2 Article 20 NIS2 Article 21.1	5,0	3	high
CM 11	mandatory	Overarching requirement. NIS2 Article 20 NIS2 Article 21.1	5,0	3	high
CM 12	mandatory	Overarching requirement. NIS2 Article 21.2 human resources security, access control policies and asset management (i)	5,0	1	low
CM 13	mandatory	Overarching requirement. NIS2 Article 21.2 human resources security, access control policies and asset management (i)	5,0	1	high

ID	Evaluation result *mandatory, highly recommend, not recommended*	Overall Evaluation explanation	Evaluation value	Time *< 1y, < 3y, < 5y, > 5y*	Cost result *low, medium, high*
CM 14	not recommended	High cost and a Low evaluation value. NIS2 Article 21.2 human resources security, access control policies and asset management (i)	0,4	1	high
CM 15	recommended	Low implementation effort (cost and time) but also Low evaluation value. Good cyber hygiene.	0,2	1	low
CM 16	mandatory	NIS2 Article 21.2 business continuity, such as backup management and disaster recovery, and crisis management (c)	3,8	3	high
CM 17	mandatory	Overarching requirement. NIS2 Article 21.2 Incident handling (b)	5,0	3	high
CM 18	mandatory	Overarching requirement. Extends CM 23. NIS2 Article 21.2 Incident handling (b)	5,0	1	high
CM 19	mandatory	Overarching requirement. NIS2 Article 20.2 NIS2 Article 21.1 basic cyber hygiene practices and cybersecurity training (g)	5,0	1	low
CM 20	mandatory	Overarching requirement. NIS2 Article 21.2: business continuity, such as backup management and disaster recovery, and crisis management (c)	5,0	3	high

ID	Evaluation result *mandatory, highly recommend, not recommended*	Overall Evaluation explanation	Evaluation value	Time *< 1y, < 3y, < 5y, > 5y*	Cost result *low, medium, high*
CM 21	mandatory	Supports NIS2 Article 21.2 (j) human resources security, access control policies and asset management (i) Access Control is a separate chapter in ENISA NIS2 Technical Implementation Guideline.	1,6	3	high
CM 22	highly recommended	Effectuates strong identities and hence supports NIS2 Article 21.2 human resources security, access control policies and asset management (i)	5,0	5	high
CM 23	mandatory	NIS2 Article 21.2 human resources security, access control policies and asset management (i) Proper lifecycle management of KMAC keys is essential.	0,2	1	low
CM 24	not recommended	Low evaluation value. For legacy systems, deactivating interfaces is not proportionate if it may undermine system Availability, especially in critical infrastructure like Railway application.	0,2	5	high
CM 25	Mandatory	Overarching requirement. Manages risks in the supply chain and hence supports NIS2 Article 21.2 (d) Managing trust through contracts	5,0	1	low

4.1.2 Implementation guide

4.1.2.0 The following two figures illustrate in an architectural way how the installed base usually is connected (Figure 7) and how the technical security counter measures (CM) could be implemented (Figure 8). The procedural security CM are not shown as they are implemented as policies and procedures in the organisation.

4.1.2.1 The introduction of the central services, like SIEM, PKI (if not present yet) and IAM are not for the use of legacy systems. These central services are required from newly developed and deployed systems already following TSI 2023 (PKI) and the EULYNX / ERJU System Pillar Cybersecurity Specifications (IAM, SIEM). So, the introduction of these services supports the smooth integration of EULYNX, System Pillar and TSI 2023 products.

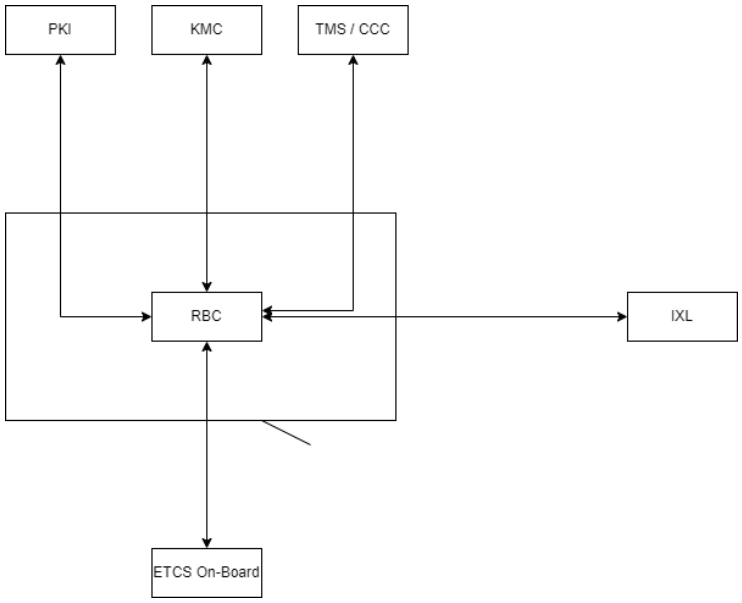


Figure 7 - Legacy Architecture RBC

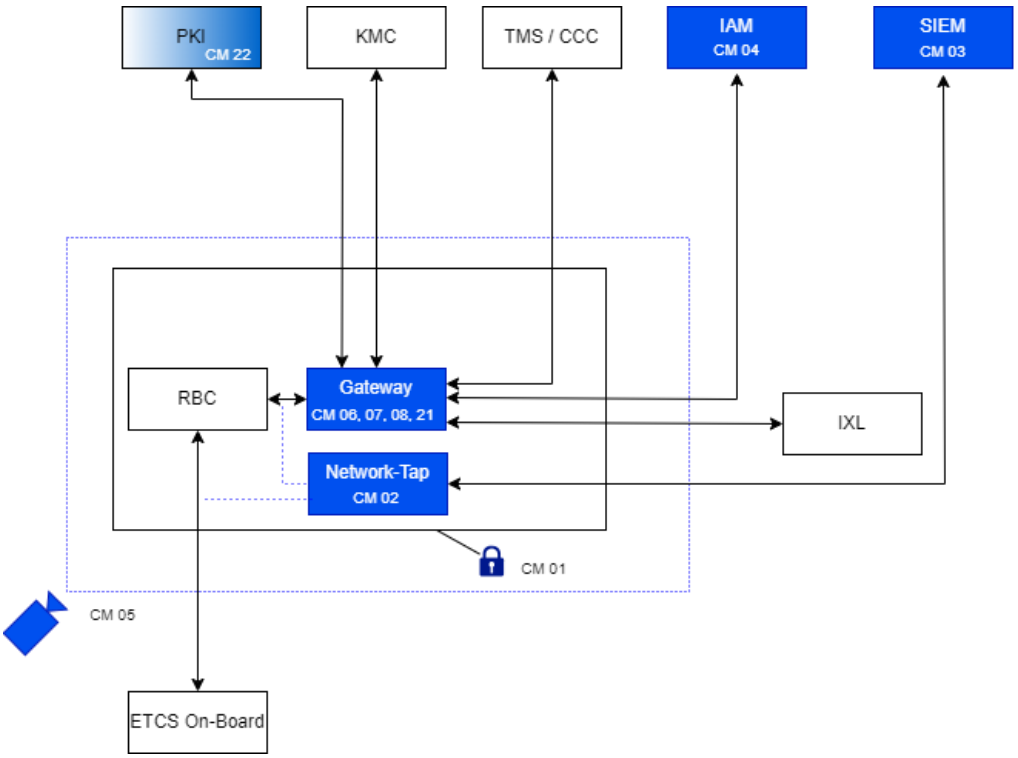


Figure 8 - Legacy Architecture RBC with CM

4.1.2.2 The illustration of the integration of the mitigating measures in Figure 8 reflects an example. Different integration and distribution of the suggested counter measures is fully possible.

4.1.2.3 The gateway in the illustrated example integrates the functionality of CM 06 - Encryption, CM 07 - Firewalls, CM 08 - Network Segmentation and CM 21 - Authentication Server in one Gateway. The integration of these capabilities may utilise existing hardware or alternatively multiple devices may be deployed to provide the corresponding functionalities. These security capabilities are intended to ensure protection at the boundaries between security zones. Consequently, it is not a strict requirement to position the protective devices directly in front of the legacy asset to protect. They may instead be located at the corresponding defined security zone boundary in accordance with the zoning definition, specified in the overall security concept. This approach enables other devices within the same security zone to benefit from the same protective measures.

4.1.2.4 In general, all illustrated security measures are feedback free to existing safety related railway installations, and hence do not interfere with, modify, or affect the functioning or safety integrity. That's why – in addition to their analysed effectiveness considering risk reduction – they have been identified as recommended or highly recommended as they may be integrated without requiring adaptions of safety approval.

4.2 Interlocking

4.2.1 Measure evaluation

4.2.1.0 Intentionally left blank

4.2.2 Implementation guide

4.2.2.0 Intentionally left blank

4.3 Field element controller

4.3.1 Measure evaluation

4.3.1.0 Intentionally left blank

4.3.2 Implementation guide

4.3.2.0 Intentionally left blank

4.4 Traffic Management System / Command and Control Centre

4.4.1 Measure evaluation

4.4.1.0 Intentionally left blank

4.4.2 Implementation guide

4.4.2.0 Intentionally left blank

4.5 Key Management System

4.5.1 Measure evaluation

4.5.1.0 Intentionally left blank

4.5.2 Implementation guide

4.5.2.0 Intentionally left blank

4.6 Onboard System

4.6.1 Measure evaluation

4.6.1.0 Intentionally left blank

4.6.2 Implementation guide

4.6.2.0 Intentionally left blank

5 Management summary

5.1.1.0 The implementation of cybersecurity measures is an essential and fundamental requirement since the introduction of the Network and Information Systems Directive (NIS).

5.1.1.1 These obligations are further elaborated and emphasised under the updated NIS 2 framework, which applies comprehensively across the entire railway sector.

5.1.1.2 The scope of NIS applies to legacy (installed base) signalling systems as well as any future systems yet to be deployed.

5.1.1.3 Although each supplier for essential systems (as defined in NIS 2) is also required to fulfil NIS 2 requirements, it is the asset owner who retains the primary responsibility and ultimate authority over the security measures and procedures actually applied. In contrast, the Cyber Resilience Act (CRA) promotes the implementation of built-in security by obliging manufacturers to provide technical and organisational safeguards for all new products with digital elements placed on the EU market, regardless of when the product was designed.

5.1.1.4 Basic security measures consisting of mainly processes, controls to address known vulnerabilities and other technical safeguards, are applicable to the legacy systems as well as future systems. If they are not implemented yet, they have to be now as they are mandatory.

5.1.1.5 When deploying the cybersecurity compensatory measures, it is essential to adopt a risk-based and strategic approach to ensure that resources are effectively allocated while still maintaining a robust protection. The process must begin with a thorough risk assessment with the purpose to identify vulnerabilities and threats specific to the operational signalling environment. Based on the assessment, compensatory measures are selected, not only for their ability to reduce risk, but also considering their cost-effectiveness, implementation complexity, and potential impact on existing systems.

5.1.1.6 Management must prioritise measures that provide the greatest risk reduction relative to their costs and potential operational impact. Clear categorisation of counter measures into mandatory, highly recommended, recommended, or non-recommended helps streamline decision-making and compliance tracking. Additionally, residual risks after implementation of the selected counter measure should be transparently reported to management and be evaluated against the organisational risk tolerance and regulatory requirements.

5.1.1.7 It is critical that compensatory measures are aligned with overarching security policies, industry standards, and regulatory frameworks to maintain trust and to ensure continuous business operation. Ongoing monitoring, regular review, and staff engagement form essential and integral parts of sustaining these security controls over the signalling system lifetime.

5.1.1.8 By embracing this structured approach, management can confidently support the deployment of targeted compensatory measures that safeguard signalling assets, ensure operational continuity, and fulfil compliance obligations.