ERTMS Security Core Group

Recommended Security Measures Future TSI

Future Systems

23E057
1A
26.10.2023

Modification history

Version	Date	Modification / Description	Editor
1A	26.10.2023	Initial Release after EUG and CER Review	Jungo, Christof Metz, Roger Ötzekin, Samet Bahadir Poschinger, Richard Poyet, Nicolas Schubert, Max Yrjola, Juhana

Table of Contents

1 Introduction

1.1 Scope

The purpose of this document is the definition of the security requirements for future TSI releases on concept level for the whole ERTMS architecture, including communication interfaces and system components themselves as well as required processes. This includes the whole security life cycle from system definition up to decommissioning of the system. The document was created based on drafts available in 2022 for TSI 2023 and furthermore includes measures for future sets of specification.

The documents of the ESCG need to be regarded as a single framework, which is only valid as a compendium of documents.

1.2 References

[1] *RFC 2119,* 1997.

[2] „IEC 62443-3-3:2019 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels".

[3] „IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components".

[4] *EN 50159,* 2011.

[5] E. Barker and A. Roginsky, *Transitioning the Use of Cryptographic Algorithms and Key Lengths,* Gaithersburg, USA: U.S. National Institute of Standard and Technology, 2019.

Subset are referenced directly with their corresponding ID.

1.3 Abbreviations

ESCG	*ERTMS Security Core Group*

ERTMS Abbreviations are listed in SUBSET-023

1.4 Authors

The following members of the ERMTS Security Core Group (ESCG) were involved in creating this document:

- ERTMS User Group (EUG)
    - Roger Metz
    - Richard Poschinger
    - Max Schubert
- DB Netz AG
    - Samet Bahadir Öztekin
- Fintraffic
    - Juhana Yrjola
- SBB
    - Christof Jungo
- SNCF
    - Nicolas Poyet

1.5 Applicability and Document Status

In order to ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.6 Definition of Requirement Types

This document uses key words indicating requirement levels according to RFC 2119 [1].

Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified (Classification as optional input to a tender according to Chapter 1.5)
O	Optional	not mandatory, must be as specified if implemented (Classification as optional input to a tender according to Chapter 1.5)
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

A zone consists of systems and a system consists of components.

The key word “system” includes all components which are part of the zone.

The zones are defined in the measure header. Specific zones can be addressed using a limitation of scope subchapter.

Note: The requirement IDs are represented by clauses in the format a.b.c.d.f. These clauses do not represent chapters. Nevertheless, the clauses follow the chapter structure to allow relocation. (Example: Clause 2.1.1.1.1 in chapter 2.1.1 and sub-chapter 2.1.1.1.)

1.7 Implementation of IEC 62443

The requirements mentioned in each measure ensure the correct and complete implementation of IEC 62443-3-3 [2] (System Requirements) referenced in the measure header.

Additional aspects of the Component Requirements (IEC 62443-4-2 [3]) are referenced and used to provide detailed measure definition. That does not imply that the complete implementation and distribution to components is assured. The CR distribution to the component level is still task of the supplier.

1.8 Structure

The whole document is organised in multiple chapters with identic structure. Following this structure is explained.

1.8.1 Affected Zones

“Affected Zones” defines the zones for which the according chapter’s requirements are relevant. The zone definition is synchronised with the security concept and threat and risk analysis. If the zone “PKI” is mentioned, the requirements are valid for every PKI which is used in the context of the defined system under consideration.

1.8.2 Threats

“Threats” defines the mitigated or managed threats by the according chapter’s requirements.

1.8.3 References to IEC 62443

The references show on which IEC 62443 SR and CR the according requirements are based on. The requirements in this document either detail the application of the IEC 62443 requirements or simply reference to require the application.

1.8.4 Measure Definition and Proposals

This document contains measures defined for the TSI 2023. These measures are described in Chapter 2 and are referenced using the ID scheme M_XXX. They only provide a preliminary basis for tenders for TSI 2023.

As the ESCG identified unmitigated risks in its assessments, additional measures are proposed for upcoming releases which are currently not covered according to the drafts for TSI 2023 available to the EUG in 2022. Measures are provided as proposals in Chapter 3 and referenced using the ID scheme P_XXX. These cannot be applied in tenders as they are not conformant to the available and officially proposed ERTMS standards.

2 Cyber Security Measure Definition

2.1 Identification and Authentication (IAC)

2.1.1 M_018 Identity and Access Management

Measure ID: M_018
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 018 Bad Planning or Lack of Adaption
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 037 Repudiation of Actions
- T 039 Malicious Software
- T 041 Sabotage

Reference to IEC 62443:

- SR 1.1, SR 1.1 RE 1, SR 1.1 RE 2, SR 1.1 RE 3 (CR 1.1, CR 1.1 RE 1, CR 1.1 RE 2)
- SR 1.2, SR 1.2 RE 1 (CR 1.2, CR 1.2 RE 1)
- SR 1.3, SR 1.3 RE 1 (CR 1.3)
- SR 1.4 (CR 1.4)
- SR 1.5 (CR 1.5)
- SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE1, CR 1.7 RE 2)
- SR 1.10 (CR 1.10)
- SR 1.11 (CR 1.11)
- SR 1.12 (CR 1.12)
- SR 1.13, SR 1.13 RE 1 (NDR 2.13, NDR 2.13 RE 1)
- SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2, SR 2.1 RE 4 (CR 2.1, CR 2.1 RE 1, CR 2.1 RE 2, CR 2.1 RE 4)

2.1.1.1 Generic

2.1.1.1.1 The system shall limit unsuccessful login attempts according to SR 1.11 (CR 1.11). **(M)**

2.1.1.1.2 The operator shall define an IAM policy establishing the least privilege principle. **(M)**

2.1.1.1.3 The operator shall define an IAM policy establishing roles. **(M)**

2.1.1.1.4 The IAM shall enforce IAM policy. **(M)**

2.1.1.1.5 The IAM shall provide the operator with the ability to manage identifiers. **(M)**

2.1.1.1.6 The IAM shall provide the operator with the ability to assign groups for identifiers. **(M)**

2.1.1.1.7 The IAM shall provide the operator with the ability to assign roles for identifiers. **(M)**

2.1.1.1.8 The IAM shall provide the operator with the ability to assign permissions to roles. **(M)**

2.1.1.1.9 If the system is in operation, then the system shall not use pre-installed authenticators. **(M)**

2.1.1.1.10 The system shall block access based on the deny-by-default principle. **(M)**

2.1.1.2 Human to Machine

2.1.1.2.1 The IAM providing access for human users and the IAM used for machine-to-machine authorization shall be separated. **(M)**

2.1.1.2.2 The component shall establish password rules according to SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE 1, CR 1.7 RE 2). **(M)**

2.1.1.2.3 If a human-to-machine connection is established, then the system shall ensure unique human user authentication. **(M)**

2.1.1.2.4 If a human-to-machine connection is established, then the system shall ensure unique human user authorisation. **(M)**

2.1.1.2.5 If a human-to-machine connection is established, then the system shall ensure multi-factor-authentication. **(M)**

2.1.1.2.6 If a human-to-machine remote connection is established, then the system shall check authentication by connecting to the IAM using OpenID Connect 1.0. **(M)**

2.1.1.2.7 If a human-to-machine remote connection is established, then the system shall check authorizations by connecting to the IAM using OpenID Connect 1.0. **(M)**

2.1.1.2.8 The IAM shall provide the operator with the ability to assign identifiers to human users. **(M)**

2.1.1.2.9 The component shall display system use notifications according to SR 1.12 (CR 1.12). **(M)**

2.1.1.2.10 The component shall obscure feedback of authentication information. **(M)**

2.1.1.2.11 The IAM shall provide the operator with the ability to assign dual control principles separately for all rights. **(M)**

2.1.1.3 Machine to Machine

2.1.1.3.1 Machine-to-Machine connections do not include communication interfaces specified in the ETCS Subsets and the RBC to EIL interface specified in EULYNX. **(I)**

2.1.1.3.2 Furthermore, this chapter is not applicable to PKI connections via CMP, CRL over HTTP and OCSP. **(I)**

2.1.1.3.3 Aspects of IAM for Euroradio over TLS are addressed in Chapter 3.4.1. **(I)**

2.1.1.3.4 If a machine-to-machine connection is established, then the system shall ensure unique authentication for all software processes. **(M)**

2.1.1.3.5 If a machine-to-machine connection is established, then the system shall ensure unique authentications for all devices. **(M)**

2.1.1.3.6 If a machine-to-machine connection is established, then the system shall ensure unique authorisation for all software processes. **(M)**

2.1.1.3.7 If a machine-to-machine connection is established, then the system shall ensure unique authorisations for all devices. **(M)**

2.1.1.3.8 If a machine-to-machine connection is established, then the system shall check authorizations by connecting to the IAM using OpenID Connect 1.0. **(M)**

2.1.1.3.9 The IAM shall provide the operator with the ability to assign identifiers to component interfaces. **(M)**

2.1.2 M_020 Public Key Infrastructure

Measure ID: M_020
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 1.5 (CR 1.5)
- SR 1.8 (CR 1.8)
- SR 1.9 (CR 1.9)

2.1.2.1 Generic

2.1.2.1.1 The authentication and authorization of human users to the Euroradio PKI shall not depend on certificates issued by the Euroradio PKI. **(M)**

2.1.2.1.2 The authentication and authorization of human users to the KMS PKI shall not depend on certificates issued by the KMS PKI. **(M)**

2.1.2.1.3 The PKI shall map each signed certificate to a user. **(M)**

2.1.2.1.4 A certificate user is either a human, a software process, or a device. **(I)**

2.1.2.1.5 All the following PKI requirements in this measure (M_020) do not affect SUBSET-137 (On-line Key Management FFFIS) and SUBSET-146 (ERTMS/ETCS End-to-End Security) interfaces. **(I)**

2.1.2.1.6 The PKI shall sign X509v3 certificates using sha512WithRSAEncryption. **(M)**

2.1.2.1.7 The ESCG plans to specify a centralized shared security services specification including PKI in the railway domain together with EULYNX and ER JU. This specification will be based on the EULYNX SSI (Eu.Doc.117), SSP (Eu.Doc.121) and ESCG requirements. **(I)**

2.1.2.2 Certificate Revocation

2.1.2.2.1 The PKI shall provide Certificate Revocation Lists (CRL) **(M)**

2.1.2.2.2 The PKI shall provide an Online Certificate Status Protocol (OCSP) endpoint. **(M)**

2.1.2.2.3 The Certificate Authority shall add the CRL distribution point extension to every certificate issued. **(M)**

2.1.2.2.4 The CRL distribution point extension shall reference the OCSP endpoint. **(M)**

2.1.2.2.5 The CRL distribution point extension shall reference the CRL endpoint. **(M)**

2.1.2.3 Certificate Management

2.1.2.3.1 The PKI shall provide a Certificate Management Protocol (CMP) endpoint. **(M)**

2.1.2.3.2 The PKI shall provide an Enrolment over Secure Transport (EST) endpoint **(M)**

2.1.2.3.3 The component shall manage certificates via the CMP endpoint. **(M)**

2.1.2.3.4 The component shall acquire certificate via the EST endpoint. **(M)**

2.2 Use Control (UC)

2.2.1 M_006 Dual Control Principle

Measure ID: M_006
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 018 Bad Planning or Lack of Adaption
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 023 Unauthorised Intrusion into IT Systems
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 041 Sabotage
- T 042 Social Engineering

Reference to IEC 62443:

- SR 2.1 RE 4 (CR 2.1. RE 4)

2.2.1.1 Generic

2.2.1.1.1 The operator shall establish organisational processes which enforce the dual control principle for critical operations. **(M)**

2.2.1.1.2 Critical operations are amongst others: **(I)**

- Manual integrity checks of software updates (if not done automatically)
- Rollout of software updates
- Configuration changes
- Rollout of configuration changes
- Certificate issuing
- Key distribution

2.2.1.1.3 The system shall enforce the dual control principle for critical operations. **(M)**

2.2.2 M_021 Protection of Local Maintenance Access

Measure ID: M_021
Affected Zones:

- RBC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 023 Unauthorised Intrusion into IT Systems
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption

Reference to IEC 62443:

- SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE 1, CR 1.7 RE 2)
- SR 2.3, SR 2.3 RE 1 (CR 2.3, CR 2.3 RE 1)
- SR 2.5 (CR 2.5)

2.2.2.1 Generic

2.2.2.1.1 The portable maintenance device shall enforce authentications for all users. **(M)**

2.2.2.1.2 The portable maintenance device shall enforce security policies. **(M)**

2.2.2.1.3 The portable maintenance device shall establish password rules according to SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE 1, CR 1.7 RE 2). **(M)**

2.2.2.1.4 The system shall enforce authentication on all local maintenance connections. **(M)**

2.2.2.1.5 The system shall enforce a session lock based on a configurable time. **(M)**

2.3 System Integrity (SI)

2.3.1 M_008 Integrity Protection of Software

Measure ID: M_008
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 3.1, SR 3.1 RE 1 (CR 3.1, CR 3.1 RE 1)

2.3.1.1 Generic

2.3.1.1.1 The system shall check the signature including the hash of software installation packages before installation. **(M)**

2.3.1.1.2 The system shall check if the software installation packages has been signed by the supplier. **(M)**

2.3.1.1.3 The system shall reject software installation packages without a valid signature. **(M)**

2.3.1.1.4 The supplier shall provide a secure hash of software installation packages. **(M)**

2.3.1.1.5 The supplier shall sign the secure hash of software installation packages. **(M)**

2.3.1.1.6 The supplier shall attach the signature to the corresponding software installation packages. **(M)**

2.3.1.1.7 The supplier shall use X509v3 certificates including extended key usage code signing for software installation packages signatures. **(M)**

2.3.1.1.8 The supplier shall sign software installation packages using sha512WithRSAEncryption. **(M)**

2.3.2 M_010 Supply Chain Security

Measure ID: M_010
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- Eurobalise
- PKI

Threats:

- T 020 Information or Products from an Unreliable Source
- T 041 Sabotage

Reference to IEC 62443:

- -

2.3.2.1 Generic

2.3.2.1.1 The supplier shall establish a secure traceable supply chain. **(M)**

2.3.2.1.2 The supplier shall establish a secure traceable production process. **(M)**

2.3.2.1.3 The supplier shall provide evidence of the application of the secure traceable supply chain process. **(M)**

2.3.2.2 Physical Security Label

2.3.2.2.1 The system shall provide a physical tamper-protected label. **(M)**

2.3.2.2.2 The physical label shall contain the device number. **(M)**

2.3.2.2.3 The physical label shall contain the device type. **(M)**

2.3.2.2.4 The physical label shall contain the operator’s name. **(M)**

2.3.3 M_011 Protection against Malicious Software

Measure ID: M_011
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 028 Software Vulnerabilities or Errors
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 3.2, SR 3.2 RE 1, SR 3.2 RE 2 (SAR 3.2, EDR 3.2, HDR 3.2, HDR 3.2 RE 1, NDR 3.2)

2.3.3.1 PKI Requirements

2.3.3.1.1 These requirements apply only to the PKI. **(I)**

2.3.3.1.2 The technical personnel shall check software update packages regarding malicious code. **(M)**

2.3.3.1.3 The technical personnel shall reject the rollout of software update packages with detected malicious packages. **(M)**

2.3.3.2 Non-PKI Requirements

2.3.3.2.1 These requirements apply to all affected zones except the PKI. **(I)**

2.3.3.2.2 The software repository of the centralized data management shall check software update packages regarding malicious code. **(M)**

2.3.3.2.3 The software repository of the centralized data management shall report detected malicious code to technical personnel. **(M)**

2.3.3.2.4 The software repository of the centralized data management shall reject the rollout of software update packages with detected malicious packages. **(M)**

2.3.4 M_012 Security Verification

Measure ID: M_012
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage¨
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 028 Software Vulnerabilities or Errors
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 3.3, SR 3.3 RE 1, SR 3.3 RE 2 (CR 3.3, CR 3.3 RE 1)

2.3.4.1 Generic

2.3.4.1.1 The supplier shall implement security verification according to SR 3.3 and CR 3.3. **(M)**

2.3.4.1.2 The supplier shall implement automatic security verification according to SR 3.3 RE1 and CR 3.3 RE 1. **(M)**

2.3.4.1.3 The supplier shall implement automatic security verification during operation according to SR 3.3 RE2. **(M)**

2.3.5 M_013 System Integrity

Measure ID: M_013
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 041 Sabotage

Reference to IEC 62443:

- SR 3.4, SR 3.4 RE 1 (CR 3.4, CR 3.4 RE 1, CR 3.4 RE 2)
- SR 3.9 (CR 3.9)

2.3.5.1 Generic

2.3.5.1.1 The system shall check its integrity using Secure Boot. **(M)**

2.3.5.1.2 The system shall establish Secure Boot using HSM, TPM or TEE. **(M)**

2.3.5.1.3 The system shall encrypt data on persistent memory. **(M)**

2.3.5.1.4 The system shall block encryption of data if integrity violations are detected by Secure Boot. **(M)**

2.3.5.2 Signatures

2.3.5.2.1 The system shall reject software without a valid signature. **(M)**

2.3.5.2.2 The supplier shall provide a secure hash of software. **(M)**

2.3.5.2.3 The supplier shall sign the secure hash of software. **(M)**

2.3.5.2.4 The supplier shall attach the signature to the corresponding software. **(M)**

2.3.5.2.5 The supplier shall use X509v3 certificates including extended key usage code signing for software signatures. **(M)**

2.3.5.2.6 The supplier shall sign software using sha512WithRSAEncryption. **(M)**

2.3.6 M_014 Secure Development

Measure ID: M_014
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 028 Software Vulnerabilities or Errors
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 039 Malicious Software
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 3.5 (CR 3.5)
- SR 3.6 (CR 3.6)
- SR 3.7 (CR 3.7)
- SR 5.4

2.3.6.1 Generic

2.3.6.1.1 The system shall ensure input validation according to SR 3.5 (and CR 3.5). **(M)**

2.3.6.1.2 The system shall provide log data about detected input validation violations to the SIEM. **(M)**

2.3.6.1.3 The system shall ensure deterministic output according to SR 3.6 (and CR 3.6). **(M)**

2.3.6.1.4 The system shall ensure error handling according to SR 3.7 (and CR 3.7). **(M)**

2.3.6.1.5 The system shall ensure a secure state after switching from or to an emergency power supply. **(M)**

2.3.6.1.6 The system shall ensure partitioning of data according to the zoning model. **(M)**

2.3.6.1.7 The system shall ensure partitioning of applications according to the zoning model. **(M)**

2.3.6.1.8 The system shall ensure partitioning of services according to the zoning model. **(M)**

2.3.7 M_015 Integrity Protection of Data in Transit

Measure ID: M_015
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 1.1, SR 1.1 RE 1, SR 1.1 RE 2, SR 1.1 RE 3 (CR 1.1, CR 1.1 RE 1, CR 1.1 RE 2)
- SR 1.2, SR 1.2 RE 1 (CR 1.2, CR 1.2 RE 1)
- SR 1.9 (CR 1.9)
- SR 3.1, SR 3.1 RE 1 (CR 3.1, CR 3.1 RE 1)
- SR 3.8, SR 3.8 RE 1, SR 3.8 RE 2, SR 3.8 RE 3 (CR 3.8)
- SR 4.3 (CR 4.3)

2.3.7.1 Generic

2.3.7.1.1 The communication from RBC to EIL shall be secured according to EULYNX BL4 R1. **(M)**

2.3.7.1.2 The communication from RBC to RBC shall be cryptographically integrity protected by transferring the data through a TLS tunnel. **(M)**

2.3.7.1.3 The communication from RBC to Control Centre shall be cryptographically integrity protected using TLS. **(M)**

2.3.7.1.4 The maintenance communication shall be cryptographically integrity protected using TLS. **(M)**

2.3.7.1.5 The diagnostic communication shall be cryptographically integrity protected using TLS. **(M)**

2.3.7.1.6 The requirements for TLS are defined in Chapter 4.1. **(I)**

2.3.7.1.7 The requirements for protection of communication sessions are defined in Chapter 4.2. **(I)**

2.4 Data Confidentiality (DC)

2.4.1 M_001 Protection of Secret Keys

Measure ID: M_001
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 016 Theft of Devices, Storage Media and Documents
- T 017 Loss of Devices, Storage Media and Documents
- T 019 Disclosure of Sensitive Information
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 1.5, SR 1.5 RE 1 (CR 1.5, CR 1.5 RE 1)
- SR 1.9, SR 1.9 RE 1 (CR 1.9, CR 1.9 RE 1)
- SR 3.1, SR 3.1 RE 1 (CR 3.1, CR 3.1 RE 1)
- SR 4.1, SR 4.1 RE 1 (CR 4.1)
- SR 4.3 (CR 4.3)

2.4.1.1 Generic

2.4.1.1.1 Secret keys addressed in this measure are: **(I)**

- Asymmetric private keys

2.4.1.1.2 Secret keys <u>not</u> addressed in this measure are: **(I)**

- KMAC (EURORADIO and RBC-RBC)
- KTRANS
- KKMC

2.4.1.1.3 If ETCS Level 2 or 3 is used, the ERTMS system should use Online Key Management. **(R)**

2.4.1.1.4 The system shall use a Hardware Security Module (HSM) to protect secret keys. **(M)**

2.4.1.1.5 The system shall generate asymmetric private keys using secure key generators. **(M)**

2.4.1.1.6 The system shall prevent access to secret keys. **(M)**

2.4.1.1.7 The PKI shall physically isolate private keys of the root certificates from networks. **(M)**

2.4.1.1.8 The PKI shall physically protect private keys of the root certificates from unauthorized human access. **(M)**

2.4.2 M_002 Protection of Remote Maintenance Connections

Measure ID: M_002
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 018 Bad Planning or Lack of Adaption
- T 020 Information or Products from an Unreliable Source
- T 023 Unauthorised Intrusion into IT Systems
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 035 Coercion, Extortion or Corruption
- T 041 Sabotage

Reference to IEC 62443:

- SR 2.5 (CR 2.5)
- SR 2.6 (CR 2.6)

2.4.2.1 Generic

2.4.2.1.1 The system shall enforce a session lock based on a configurable time. **(M)**

2.4.2.1.2 The system shall terminate an idle session after a configurable time. **(M)**

2.4.2.2 Non-PKI requirements

2.4.2.2.1 These requirements apply to all zones except the PKI. **(I)**

2.4.2.2.2 The system shall only allow remote maintenance connections to or from the centralized data management. **(M)**

2.4.2.2.3 The operator shall define and implement a Remote Maintenance Connection policy for the connection to the centralized data management. **(M)**

2.4.2.2.4 The operator shall define and implement a secure Remote Maintenance process for the connection to the centralized data management. **(M)**

2.4.2.2.5 Further information on Remote Maintenance Connection will be released in the ESCG Third Party Policy Template. **(I)**

2.4.2.2.6 The connection to the centralized and secure management of configuration data (M_027) is encrypted using TLS (M_016). **(I)**

2.4.3 M_016 Confidentiality Protection of Data in Transit

Measure ID: M_016
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 018 Bad Planning or Lack of Adaption
- T 019 Disclosure of Sensitive Information
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 1.1, SR 1.1 RE 1, SR 1.1 RE 2, SR 1.1 RE 3 (CR 1.1, CR 1.1 RE 1, CR 1.1 RE 2)
- SR 1.9 (CR 1.9)
- SR 3.8, SR 3.8 RE 1, SR 3.8 RE 2, SR 3.8 RE 3 (CR 3.8)
- SR 4.1, SR 4.1 RE 1, SR 4.1 RE 2 (CR 4.1)
- SR 4.3 (CR 4.3)

2.4.3.1 Generic

2.4.3.1.1 The maintenance communication shall be cryptographically encrypted using TLS. **(M)**

2.4.3.1.2 The diagnostic communication shall be cryptographically encrypted using TLS. **(M)**

2.4.3.1.3 The communication used for key transfer shall be confidentiality protected using cryptographic methods. **(M)**

2.4.3.1.4 The requirements for TLS are defined in Chapter 4.1. **(I)**

2.4.3.1.5 The requirements for protection of communication sessions are defined in Chapter 4.2. **(I)**

2.4.4 M_026 Protection of Data at Rest

Measure ID: M_026
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 013 Intercepting Compromising Emissions
- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 016 Theft of Devices, Storage Media and Documents
- T 017 Loss of Devices, Storage Media and Documents
- T 019 Disclosure of Sensitive Information

Reference to IEC 62443:

- SR 4.2, SR 4.2 RE 1 (CR 4.2, CR 4.2 RE 1, CR 4.2 RE 2)

2.4.4.1 Generic

2.4.4.1.1 The encryption of data at rest is defined in Chapter 2.3.5. **(I)**

2.4.4.1.2 During decommissioning, the component shall purge information to which read access is restricted. **(M)**

2.4.4.1.3 During decommissioning, the component shall verify the successful completion of the memory purging process. **(M)**

2.4.4.1.4 The component shall prevent unauthorized information transfer via shared memory. **(M)**

2.5 Restricted Data Flow (RDF)

2.5.1 M_004 Network Segmentation

Measure ID: M_004
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 018 Bad Planning or Lack of Adaption
- T 019 Disclosure of Sensitive Information
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 040 Denial of Service
- T 041 Sabotage
- T 043 Replaying Messages
- T 045 Data Loss
- T 046 Loss of Integrity of Sensitive Information
- T 047 Harmful side effects of IT-based attacks

Reference to IEC 62443:

- SR 1.13, SR 1.13 RE 1 (NDR 1.13)
- SR 5.1, SR 5.1 RE 1, SR 5.1 RE 2, SR 5.1 RE 3 (CR 5.1)
- SR 5.2, SR 5.2 RE 1, SR 5.2 RE 2, SR 5.2 RE 3 (NDR 5.2, NDR 5.2 RE 1, NDR 5.2 RE 2, NDR 5.2 RE 3)

2.5.1.1 Traffic Flow Information

2.5.1.1.1 The supplier shall provide a complete traffic matrix for the supplied application. **(M)**

2.5.1.1.2 The supplier shall provide a complete protocol description including optional parameter for the supplied application. **(M)**

2.5.1.1.3 The supplier shall provide the complete valid communication sequences between applications. **(M)**

2.5.1.2 Network Segmentation

2.5.1.2.1 The network segment shall provide a separate appliance as network filter for the network traffic at its zone borders. **(M)**

2.5.1.2.2 The network filter shall block illegitimate network traffic on ISO OSI layers 2 to 7 based on the definition of valid traffic flow information. **(M)**

2.5.1.2.3 Network filters can also be applied to all IP-based traffic. This also includes the GPRS-based GSM-R and FRMCS traffic. **(I)**

2.5.1.2.4 The network filter shall block traffic based on the deny-by-default principle. **(M)**

2.5.1.2.5 The supplier shall provide the rule set required for blocking illegitimate network traffic on ISO OSI layers 2 to 7. **(M)**

2.5.1.2.6 The network filter shall send information regarding blocked traffic to a centralized logging system. **(M)**

2.5.1.2.7 The network filter shall provide the operator with the ability to block connections to allow island mode. **(M)**

2.5.1.2.8 The network filter shall provide the operator with ability to block single connections to allow partial island mode to specific communication partners only. **(M)**

2.5.1.2.9 The network filter shall automatically block connections (fail close) during a failure of the network filter mechanisms. **(M)**

2.5.1.2.10 The system shall provide physical or logical network segmentation. **(M)**

2.5.1.2.11 The system shall at least provide a separate network segment for maintenance data traffic. **(M)**

2.5.1.2.12 The system shall at least provide a separate network segment for monitoring data traffic. **(M)**

2.5.1.2.13 The system shall at least provide a separate network segment for operational data traffic. **(M)**

2.5.1.2.14 The system shall at least provide a separate network segment for security data traffic. **(M)**

2.5.2 M_028 Restrictions on Person-to-Person Communication

Measure ID: M_028
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 039 Malicious Software
- T 040 Denial of Service
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 5.3, SR 5.3 RE 1 (NDR 5.3)

2.5.2.1 Off-Line KMC

2.5.2.1.1 The system shall prevent non-KMS-related person-to-person communication. **(M)**

2.5.2.1.2 Person-to-Person communication cannot be completely avoided in Off-Line KMCs but can be reduced to communication only related to key management tasks only. **(I)**

2.5.2.2 On-Line KMC

2.5.2.2.1 The system shall prevent person-to-person communication. **(M)**

2.5.2.3 Non-KMC Zones

2.5.2.3.1 The system shall prevent person-to-person communication. **(M)**

2.6 Timely Response to Events (TRE)

2.6.1 M_007 Computer Emergency Response Team (CERT)

Measure ID: M_007
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 018 Bad Planning or Lack of Adaption
- T 028 Software Vulnerabilities or Errors
- T 047 Harmful side effects of IT-based attacks

Reference to IEC 62443:

- -

2.6.1.1 Generic

2.6.1.1.1 The operator shall establish a Computer Emergency Response Team (CERT). **(M)**

2.6.1.1.2 The supplier shall establish a Computer Emergency Response Team (CERT). **(M)**

2.6.1.1.3 The supplier shall provide information about vulnerabilities to the CERT of the operator. **(M)**

2.6.1.1.4 The supplier shall provide information regarding vulnerability handling to the CERT of the operator. **(M)**

2.6.1.1.5 The operator shall disclose vulnerability information according to ISO 29147. **(M)**

2.6.1.1.6 The supplier shall disclose vulnerability information according to ISO 29147. **(M)**

2.6.2 M_009 Logging and SIEM (Security Incident and Event Management)

Measure ID: M_009
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 035 Coercion, Extortion or Corruption
- T 036 Identity Theft
- T 037 Repudiation of Actions
- T 038 Abuse of Personal Data
- T 039 Malicious Software
- T 041 Sabotage
- T 042 Social Engineering

Reference to IEC 62443:

- SR 2.8, SR 2.8 RE 1 (CR 2.8)
- SR 2.9, SR 2.9 RE 1 (CR 2.9)
- SR 2.10 (CR 2.10)
- SR 2.11, SR 2.11 RE 1, SR 2.11 RE 2 (CR 2.11, CR 2.11 RE 1, CR 2.11 RE 2)
- SR 2.12, SR 2.12 RE 1 (CR 2.12, CR 2.12 RE 1)
- SR 3.9, SR 3.9 RE 1 (CR 3.9, CR 3.9 RE 1)
- SR 6.1, SR 6.1 RE 1 (CR 6.1, CR 6.1 RE 1)
- SR 6.2 (CR 6.2)

2.6.2.1 Generic

2.6.2.1.1 The ESCG plans to specify a centralized shared security services specification including security logging and time synchronisation in the railway domain together with EULYNX and ER JU. This specification will be based on the EULYNX SSI (Eu.Doc.117), SSP (Eu.Doc.121) and ESCG requirements. **(I)**

2.6.2.1.2 The operator shall establish a Security Incident and Event Management (SIEM). **(M)**

2.6.2.1.3 The network system shall provide relevant traffic data to the SIEM. **(M)**

2.6.2.1.4 The SIEM shall use system specific use cases to detect security incidents. **(M)**

2.6.2.1.5 The SIEM shall provide warnings to technical personnel regarding incidents in a timely manner. **(M)**

2.6.2.1.6 The SIEM shall provide related information of each warning to the technical personnel. **(M)**

2.6.2.1.7 The system shall provide log data to a centralized logging server. **(M)**

2.6.2.1.8 The system shall provide log data via Syslog-Ng over TLS. **(M)**

2.6.2.1.9 The centralized logging server shall provide relevant log data to the SIEM. **(M)**

2.6.2.1.10 The centralized logging server shall be able to provide exports of logging data. **(M)**

2.6.2.1.11 The centralized logging server shall be able to export logging data to write-once media. **(M)**

2.6.2.1.12 The centralized logging server shall check authorisations for log data access. **(M)**

2.6.2.1.13 The centralized logging server shall provide read only access only. **(M)**

2.6.2.1.14 The centralized logging server shall provide programmatic access to audit records. **(M)**

2.6.2.1.15 The system shall store log data locally until the successful transmission to a centralized logging server. **(M)**

2.6.2.1.16 The system shall be able to store local log data for at least 48h. **(M)**

2.6.2.1.17 The system shall warn when the record storage capacity reached a defined threshold. **(M)**

2.6.2.1.18 The centralized logging server shall warn when the record storage capacity reached a defined threshold. **(M)**

2.6.2.1.19 The centralized logging server shall warn when an audit processing failure is detected. **(M)**

2.6.2.2 Log time synchronisation

2.6.2.2.1 The system shall protect essential functions in case of an audit processing failure. **(M)**

2.6.2.2.2 The system shall synchronize its time with a centralized time source using NTP. **(M)**

2.6.2.2.3 The system shall synchronize its time in a configurable interval. **(M)**

2.6.2.2.4 The system shall use timestamp based on synchronized time for logging purposes. **(M)**

2.6.2.2.5 The system shall check the time deviation of local and synchronized time during synchronization with a centralized time source. **(M)**

2.6.2.2.6 If the time deviation of local and synchronized time is higher than a configurable among of time, system shall provide a log warning. **(M)**

2.6.2.3 Log requirements

2.6.2.3.1 The system shall provide log data for all user actions based on the user authentication. **(M)**

2.6.2.3.2 The operator shall define log data according to privacy regulations. **(M)**

2.7 Resource Availability (RA)

2.7.1 M_022 Denial of Service Protection

Measure ID: M_022
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 023 Unauthorised Intrusion into IT System
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 040 Denial of Service

Reference to IEC 62443:

- SR 2.7 (CR 2.7)
- SR 7.1 RE 1, SR 7.1 RE 2 (CR 7.1 RE 1)
- SR 7.2 (CR 7.2)

2.7.1.1 Generic

2.7.1.1.1 If the system detects a Denial of Service (DoS) attack, the system shall reduce the data processing priority of the affected connection. **(M)**

2.7.1.1.2 The system shall prevent users (connected humans or other systems) from using the systems functionalities to generate DoS attacks. **(M)**

2.7.1.1.3 The system shall limit the resource usage of security functionality to prevent resource exhaustion. **(M)**

2.7.1.1.4 The system shall limit the number of concurrent sessions to a configurable number. **(M)**

2.7.2 M_023 Backup

Measure ID: M_023
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 041 Sabotage
- T 043 Replaying Messages
- T 045 Data Loss
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 7.3, SR 7.3 RE 1, SR 7.3 RE 2, SR 7.3 RE 3 (CR 7.3, CR 7.3 RE 1)
- SR 7.4 (CR 7.4)

2.7.2.1 Generic

2.7.2.1.1 The ESCG plans to specify a centralized shared security services specification including backup in the railway domain together with EULYNX and ER JU. This specification will be based on the EULYNX SSI (Eu.Doc.117), SSP (Eu.Doc.121) and ESCG requirements. **(I)**

2.7.2.2 PKI Requirements for Config, Certificates and Software

2.7.2.2.1 These requirements apply only to the PKI. **(I)**

2.7.2.2.2 The operator shall establish a backup process for software data which is relevant for operational availability of the component. **(M)**

2.7.2.2.3 The operator shall establish a backup process for configuration data which is relevant for operational availability of the component. **(M)**

2.7.2.2.4 The operator shall establish a backup process for certificate data which is relevant for operational availability of the component. **(M)**

2.7.2.2.5 The operator shall backup the current version of relevant data. **(M)**

2.7.2.2.6 The operator shall backup at least the last version of relevant data. **(M)**

2.7.2.2.7 The operator shall backup at least the versions of relevant data of the last three months. **(M)**

2.7.2.2.8 The operator shall ensure the reliability of backups using verification mechanisms. **(M)**

2.7.2.2.9 The operator shall ensure the reliability of the backup recovery mechanism. **(M)**

2.7.2.2.10 The operator shall test the backup recovery mechanism regularly. **(M)**

2.7.2.2.11 The operator shall ensure that the last known secure state is recovered after a security incident. **(M)**

2.7.2.3 Non-PKI Requirements for Config and Software

2.7.2.3.1 These requirements apply to all affected zones except the PKI. **(I)**

2.7.2.3.2 The centralized data management (e.g., MDM in future specifications) is responsible for the backup of relevant data. Hence, the component itself does not need any backup functionality if it fetches all relevant data from the centralized management. **(I)**

2.7.2.3.3 The component shall backup software data which is relevant for operational availability of the component via a centralized data management. **(M)**

2.7.2.3.4 The component shall backup configuration data which is relevant for operational availability of the component via a centralized data management. **(M)**

2.7.2.3.5 The centralized data management shall automatically backup the current version of relevant data. **(M)**

2.7.2.3.6 The centralized data management shall automatically backup at least the last three versions of relevant data. **(M)**

2.7.2.3.7 The centralized data management shall automatically backup at least the versions of relevant data of the last three months. **(M)**

2.7.2.3.8 The centralized data management shall ensure the reliability of backups using verification mechanisms. **(M)**

2.7.2.3.9 The centralized data management shall ensure the reliability of the backup recovery mechanism. **(M)**

2.7.2.3.10 The operator shall test the backup recovery mechanism regularly. **(M)**

2.7.2.3.11 The component shall ensure that the last known secure state provided by the centralized data management is used after a failure. **(M)**

2.7.2.3.12 The component shall ensure that the last known secure state provided by the centralized data management is used after a disruption. **(M)**

2.7.2.4 Secret Keys

2.7.2.4.1 The KMC shall backup the current version of the encrypted secret keys. **(M)**

2.7.2.4.2 Backups of secret keys are protected according to M_001. **(I)**

2.7.2.4.3 The operator shall create a recovery key for the encrypted secret keys. **(M)**

2.7.2.4.4 The operator shall store the recovery key in a physically protected environment. **(M)**

2.7.2.4.5 The physically protected environment of the recovery key shall prevent data transfer. **(M)**

2.7.2.4.6 The operator shall limit the physical access to the recovery key. **(M)**

2.7.2.4.7 The KMC shall backup at least the last version of the encrypted secret keys. **(M)**

2.7.2.4.8 The KMC shall backup at least the versions of the encrypted secret keys of the last three months. **(M)**

2.7.2.4.9 The KMC shall ensure the reliability of backups using verification mechanisms. **(M)**

2.7.2.4.10 The KMC shall ensure the reliability of the backup recovery mechanism. **(M)**

2.7.2.4.11 The KMC shall test the backup recovery mechanism regularly. **(M)**

2.7.2.4.12 The KMC shall ensure that the last known secure state is recovered after a security incident. **(M)**

2.7.3 M_024 System Hardening

Measure ID: M_024
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 039 Malicious Software
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 2.4 (SAR 2.4, EDR 2.4, HDR 2.4, NDR 2.4)
- SR 7.6 (CR 7.6)
- SR 7.7 (CR 7.7)

2.7.3.1 Generic

2.7.3.1.1 The system shall only provide necessary functions. **(M)**

2.7.3.1.2 The system shall only allow connections on necessary ports. **(M)**

2.7.3.1.3 The system shall only provide necessary services. **(M)**

2.7.3.1.4 The supplier should remove mobile code functionalities. **(R)**

2.7.3.1.5 If the mobile code functionalities cannot be removed, then the supplier should disable mobile code functionalities. **(R)**

2.7.3.1.6 The system shall prevent the execution of mobile code. **(M)**

2.7.3.1.7 The supplier shall provide best practice guidelines for network configuration of the system. **(M)**

2.7.3.1.8 The supplier shall provide best practice guidelines for security configuration of the system. **(M)**

2.7.3.1.9 The operator shall configure the system according to guidelines provided by the supplier. **(M)**

2.7.4 M_027 Secure Configuration

Measure ID: M_027
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 018 Bad Planning or Lack of Adaption
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 037 Repudiation of Actions
- T 041 Sabotage
- T 043 Replaying Messages
- T 045 Data Loss
- T 046 Loss of Integrity of Sensitive Information
- T 047 Harmful side effects of IT-based attacks

Reference to IEC 62443:

- SR 7.6, SR 7.6 RE 1 (CR 7.6, CR 7.6 RE 1)
- SR 7.8 (CR 7.8)

2.7.4.1 Generic

2.7.4.1.1 The system shall provide the operator with the ability to change the network configuration. **(M)**

2.7.4.1.2 The system shall provide the operator with the ability to change the security configuration. **(M)**

2.7.4.1.3 The system shall provide associated properties to an asset inventory **(M)**

2.7.4.2 Non-PKI Requirements

2.7.4.2.1 These requirements apply to all affected zones except the PKI. **(I)**

2.7.4.2.2 The system shall use a centralized and secure management of configuration data. **(M)**

2.7.4.2.3 The system shall use a centralized and secure management of software updates. **(M)**

2.7.4.2.4 The ESCG plans to specify a centralized Maintenance and Data Management (MDM) in the railway domain together with EULYNX and ER JU. **(I)**

2.7.4.2.5 The centralized data management shall provide an interface to export a machine-readable report of the current network configuration. **(M)**

2.7.4.2.6 The centralized data management shall provide an interface to export a machine-readable report of the current security configuration. **(M)**

2.7.4.2.7 The centralized data management shall provide a complete asset inventory. **(M)**

2.7.4.2.8 The centralized data management shall provide associated properties in the asset inventory. **(M)**

2.8 Physical Protection (PHY)

2.8.1 M_003 Protection of Data Centres and Cabinets

Measure ID: M_003
Affected Zones:

- RBC
- KMC
- PKI

Threats:

- T 016 Theft of Devices, Storage Media and Documents
- T 017 Loss of Devices, Storage Media and Documents
- T 021 Manipulation of Hardware or Software
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 041 Sabotage

Reference to IEC 62443:

- -

2.8.1.1 Generic

2.8.1.1.1 This measure is only addressing IT-Security aspects of physical protection. Only the IT-Security of the physical access management is covered. **(I)**

2.8.1.1.2 The component shall be protected by a digital physical access management system. **(M)**

2.8.1.1.3 The physical access management system shall provide a fine-grained rights management. **(M)**

2.8.1.1.4 The physical access management system shall require a second authentication factor. **(M)**

2.8.1.1.5 The physical access management system shall use state of the art security for authentication. **(M)**

2.8.1.1.6 The physical access management system shall be centrally managed. **(M)**

2.8.1.1.7 The physical access management system shall provide log data regarding the authentication process. **(M)**

2.8.2 M_025 Protection of On-Board Cabinets

Measure ID: M_025
Affected Zones:

- ETCS On-Board

Threats:

- T 013 Intercepting Compromising Emissions
- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 021 Manipulation of Hardware or Software
- T 022 Manipulation of Information
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 035 Coercion, Extortion or Corruption
- T 039 Malicious Software
- T 041 Sabotage
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information
- T 047 Harmful side effects of IT-based attacks

Reference to IEC 62443:

- -

2.8.2.1 Generic

2.8.2.1.1 The component shall be protected against unauthorized physical access. **(M)**

2.9 Organisational Security and Processes (OSP)

2.9.1 M_005 Training and Education of Technical Personnel

Measure ID: M_005
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- Eurobalise
- PKI

Threats:

- T 018 Bad Planning or Lack of Adaption
- T 020 Information or Products from an Unreliable Source
- T 027 Lack of Resources
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 033 Absence of Personnel
- T 035 Coercion, Extortion or Corruption
- T 036 Identity Theft
- T 041 Sabotage
- T 042 Social Engineering

Reference to IEC 62443:

- -

2.9.1.1 Generic

2.9.1.1.1 The operator shall assure that technical personnel (internal and external) is sufficiently trained regarding security related technical aspects of the system. **(M)**

2.9.1.1.2 After trainings participants need to be able to operate and manage system in a cyber secure way. **(I)**

2.9.1.1.3 The supplier shall provide sufficient training for the suppliers' personnel regarding security related technical aspects of the system. **(M)**

2.9.1.1.4 The supplier shall provide sufficient training for the operators' personnel regarding security related technical aspects of the system. **(M)**

2.9.1.1.5 The supplier shall assure that prerequisites regarding knowledge and certifications are fulfilled for personnel attending a training. **(M)**

2.9.1.1.6 Security related aspects necessary for a training include amongst others: **(I)**

- Configuration (maintenance and commissioning) of security features
- Aspects of basic hardening regarding security
- Network configuration
- Commissioning and decommissioning processes
- Maintenance processes

2.9.2 M_017 Human Resource Planning

Measure ID: M_017
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 027 Lack of Resources
- T 031 Incorrect Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations
- T 033 Absence of Personnel
- T 035 Coercion, Extortion or Corruption
- T 036 Identity Theft
- T 042 Social Engineering

Reference to IEC 62443:

- -

2.9.2.1 Generic

2.9.2.1.1 The operator shall assure that a sufficient number of qualified security personnel is available to fulfil security processes. **(M)**

2.9.2.1.2 The security processes include the PDCA (Plan, Do, Check, Act) cycle. **(I)**

2.9.2.1.3 The operator shall assure that every security role can be fulfilled by at least two people. **(M)**

2.9.2.1.4 The operator shall ensure that the personnel is checked according to the required security clearance for the role. **(M)**

2.9.2.1.5 Security clearance can be based on background checks performed by the operator or public institutions. **(I)**

2.9.3 M_019 Security Management

Measure ID: M_019
Affected Zones:

- RBC
- KMC
- ETCS On-Board
- PKI

Threats:

- T 028 Software Vulnerabilities or Errors
- T 029 Violation of Laws or Regulations

Reference to IEC 62443:

- -

2.9.3.1 Generic

2.9.3.1.1 The operator shall implement an Information Security Management System (ISMS). **(M)**

2.9.3.1.2 The operator shall perform a security risk assessment for the system. **(M)**

2.9.3.1.3 The operator shall update the security risk assessments regularly. **(M)**

2.9.3.1.4 The operator shall update the security risk assessments after changes that affect security. **(M)**

2.9.3.1.5 The operator shall implement a security audit process for the system. **(M)**

2.9.3.1.6 The operator shall establish a process to assure regular penetration tests. **(M)**

3 Input to Future Measures

3.1.1.1.1 The following chapters contain preliminary measure proposals for currently existing threats and risks. However due to limitations in the TSI CCS currently in force, there are for the moment no mitigating measures possible. Therefore, these preliminary measure proposals can only be implemented with a future TSI CCS. These require more detailed assessment and technical considerations which will be included in upcoming versions. These proposals should not be included in tender documents.**(I)**

3.2 Identification and Authentication (IAC)

3.2.1 P_018 Identity and Access Management for Eurobalise Signing Devices

Measure Proposal ID: P_018
Affected Zones:

- Eurobalise

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations

Reference to IEC 62443:

- SR 1.1, SR 1.1 RE 1, SR 1.1 RE 2, SR 1.1 RE 3 (CR 1.1, CR 1.1 RE 1, CR 1.1 RE 2)
- SR 1.2, SR 1.2 RE 1 (CR 1.2, CR 1.2 RE 1)
- SR 1.3, SR 1.3 RE 1 (CR 1.3)
- SR 1.4 (CR 1.4)
- SR 1.5 (CR 1.5)
- SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE1, CR 1.7 RE 2)
- SR 1.10 (CR 1.10)
- SR 1.11 (CR 1.11)
- SR 1.12 (CR 1.12)
- SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2, SR 2.1 RE 4 (CR 2.1, CR 2.1 RE 1, CR 2.1 RE 2, CR 2.1 RE 4)

3.2.1.1 Generic

3.2.1.1.1 This Measure requires the implementation of P_015_2. **(I)**

3.2.1.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_018. **(M)**

3.2.2 P_020 Public Key Infrastructure for Eurobalise Signing Devices

Measure Proposal ID: P_020
Affected Zones:

- Eurobalise
- ETCS On-Board

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems
- T 032 Abuse of Authorisations

Reference to IEC 62443:

- SR 1.5 (CR 1.5)

3.2.2.1 Generic

3.2.2.1.1 This Measure requires the implementation of P_015_2. **(I)**

3.2.2.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_020. **(M)**

3.3 Use Control (UC)

3.3.1 P_006 Dual Control Principle for Eurobalise Signing Devices

Measure Proposal ID: P_006
Affected Zones:

- Eurobalise

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems

Reference to IEC 62443:

- SR 2.1 RE 4 (CR 2.1. RE 4)

3.3.1.1 Generic

3.3.1.1.1 This Measure requires the implementation of P_015_2 **(I)**

3.3.1.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_006. **(M)**

3.3.2 P_021 Protection of Local Maintenance Access for Eurobalise Signing Devices

Measure Proposal ID: P_021
Affected Zones:

- Eurobalise

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems

Reference to IEC 62443:

- SR 1.7, SR 1.7 RE 1, SR 1.7 RE 2 (CR 1.7, CR 1.7 RE 1, CR 1.7 RE 2)
- SR 2.5 (CR 2.5)

3.3.2.1 Generic

3.3.2.1.1 This Measure requires the implementation of P_015_2 **(I)**

3.3.2.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_021. **(M)**

3.4 System Integrity (SI)

3.4.1 P_015_1 Integrity Protection of Data in Transit for Euroradio Traffic

Measure Proposal ID: P_015_1
Affected Zones:

- RBC
- KMC

Threats:

- T 022 Manipulation of Information
- T 043 Replaying Messages
- T 046 Loss of Integrity of Sensitive Information

Reference to IEC 62443:

- SR 3.1, SR 3.1 RE 1 (CR 3.1, CR 3.1 RE 1)

3.4.1.1 Generic

3.4.1.1.1 The protection of the data traffic in the Euroradio protocol will be secured by an underlying TLS layer according to Subset 146.[1] **(I)**

3.4.1.1.2 If Subset 146 is applied for the Euroradio connection, the cryptographic integrity protection is applied via TLS and ensures protection categorized as either an additional cryptographic code or additional enciphering of the Euroradio data according to EN 50159 [2]. **(I)**

3.4.1.1.3 If Subset 146 is applied for the Euroradio connection, the MAC (Subset 037) can be reduced from a (unsecure [3]) cryptographic safety code to a non-cryptographic safety code detecting message corruption according to EN 50159 [2]. **(I)**

3.4.1.1.4 If Subset 146 is applied for the Euroradio connection, the MAC (Subset 037) does not require any pre-shared keys (KMAC) to establish a non-cryptographic safety code according to EN 50159 [2]. **(I)**

3.4.1.1.5 Based on these assumptions, the implementation of one of the following options for ETCS without KMC is proposed: **(I)**

a) Replace the MAC with a safety code not requiring a pre-shared key (KMAC).

b) Keep the MAC for migration reasons but replace the currently required previous exchange of KMACs with an automatic session key (KSMAC) determination on Euroradio connection setup.

c) Keep the MAC for migration reasons but use preconfigured KMACs.

3.4.1.1.6 If one of the proposed options for ETCS without KMC is applied, the KMC is obsolete.[2] **(I)**

3.4.1.1.7 If one of the proposed options for ETCS without KMC is applied, a PKI exclusively used for the On-Line KMS is obsolete.[3] **(I)**

[1] In Subset 146 the term Automatic Train Protection (ATP) is used to address the Euroradio connection used for ETCS.

[2] The certificates specified and used by Subset 146 compliant communication are distributed via a Public Key Infrastructure (PKI).

[3] A migration path from a PKI used for On-Line KMS to an PKI used for Euroradio via TLS might be implemented.

3.4.1.1.8 If Subset 146 is applied for the Euroradio connection, a PKI needs to be implemented to provide certificates to the RBC and EVC. **(I)**

3.4.2 P_015_2 Integrity Protection of Data in Transit for Eurobalise Telegrams

Measure Proposal ID: P_015_2
Affected Zones:

- Eurobalise
- ETCS On-Board

Threats:

- T 013 Intercepting Compromising Emissions
- T 014 Interception of Information / Espionage
- T 015 Eavesdropping
- T 019 Disclosure of Sensitive Information
- T 020 Information or Products from an Unreliable Source
- T 021 Manipulation of Hardware or Software
- T 023 Unauthorised Intrusion into IT Systems
- T 028 Software Vulnerabilities or Errors
- T 030 Unauthorised Use or Administration of Devices and Systems
- T 041 Sabotage
- T 043 Replaying Messages

Reference to IEC 62443:

- SR 3.1, SR 3.1 RE 1 (CR 3.1, CR 3.1 RE 1)
- SR 3.8, SR 3.8 RE 1, SR 3.8 RE 2, SR 3.8 RE 3 (CR 3.8)

3.4.2.1 Generic

3.4.2.1.1 The operator shall cryptographically sign Eurobalise telegrams. **(M)**

3.4.2.1.2 Technical proposals for signatures in Eurobalise telegrams are not available yet. **(I)**

3.4.2.1.3 The ETCS On-Board system shall check if the signature issuer matches the expected data for the track. **(M)**

3.4.2.1.4 If the received Eurobalise telegram does not contain a valid signature signed by the operator and if the Eurobalise telegram requires a signature, the ETCS On-Board system shall reject Eurobalise telegrams. **(M)**

3.4.2.1.5 Eurobalise telegrams might be accepted for safety reasons, even if the signature is not valid or not available. **(I)**

3.4.2.1.6 The system used to sign the Eurobalise telegrams is referred to as Eurobalise Telegram Signing Device in this document. **(I)**

3.5 Data Confidentiality (DC)

3.5.1 P_001 Protection of Secret Keys for Eurobalise Signing Devices

Measure Proposal ID: P_001
Affected Zones:

- Eurobalise

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems

Reference to IEC 62443:

- SR 1.5, SR 1.5 RE 1 (CR 1.5, CR 1.5 RE 1)

3.5.1.1 Generic

3.5.1.1.1 This Measure requires the implementation of P_015_2. **(I)**

3.5.1.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_001. **(M)**

3.6 Restricted Data Flow (RDF)

-Intentionally left blank-

3.7 Timely Response to Events (TRE)

3.7.1 P_009 Logging and SIEM (Security Incident and Event Management) for Eurobalise Signing Devices

Measure Proposal ID: P_009
Affected Zones:

- Eurobalise

Threats:

- T 030 Unauthorised Use or Administration of Devices and Systems
- T 035 Coercion, Extortion or Corruption
- T 037 Repudiation of Actions

Reference to IEC 62443:

- SR 2.8, SR 2.8 RE 1 (CR 2.8)
- SR 2.9, SR 2.9 RE 1 (CR 2.9)
- SR 2.10 (CR 2.10)
- SR 2.11, SR 2.11 RE 1, SR 2.11 RE 2 (CR 2.11, CR 2.11 RE 1, CR 2.11 RE 2)
- SR 2.12, SR 2.12 RE 1 (CR 2.12, CR 2.12 RE 1)

3.7.1.1 Generic

3.7.1.1.1 This Measure requires the implementation of P_015_2. **(I)**

3.7.1.1.2 The Eurobalise Telegram Signing Device shall be protected according to M_009. **(M)**

3.8 Resource Availability (RA)

-Intentionally left blank-

3.9 Physical Protection (PHY)

-Intentionally left blank-

3.10 Organisational Security and Processes (OSP)

-Intentionally left blank-

4 Annex

4.1 TLS Requirements

4.1.1.1.1 These TLS requirements do not affect SUBSET-146 (ERTMS/ETCS End-to-End Security). **(I)**

4.1.1.1.2 The TLS endpoint shall use TLS 1.3. **(M)**

4.1.1.1.3 The TLS endpoint shall enforce mutual authentication. **(M)**

4.1.1.1.4 The TLS endpoint shall validate the certificate using a certification path to a trusted CA. **(M)**

4.1.1.1.5 If confidentiality protection is not required, the TLS endpoint shall use the cipher TLS_SHA384_SHA384. **(M)**

4.1.1.1.6 If confidentiality protection is required, the TLS endpoint shall provide the cipher TLS_AES_256_GCM_SHA384. **(M)**

4.1.1.1.7 If confidentiality protection is required, the TLS endpoint shall provide the cipher TLS_CHACHA20_POLY1305_SHA256. **(M)**

4.1.1.1.8 If confidentiality protection is required, the TLS endpoint shall provide the cipher TLS_AES_128_GCM_SHA256. **(M)**

4.1.1.1.9 If confidentiality protection is required, the TLS endpoint shall prohibit the use of integrity-only ciphers. **(M)**

4.1.1.1.10 The TLS endpoint shall use X509v3 certificates to authenticate. **(M)**

4.1.1.1.11 The TLS endpoint shall check the validity of certificates using OCSP. **(M)**

4.1.1.1.12 If the OCSP endpoint is not available, the TLS endpoint shall check the validity of certificates using CRLs. **(M)**

4.1.1.1.13 The TLS endpoint shall perform the key agreement using x25519. **(M)**

4.2 Protection of Communication Sessions

4.2.1.1.1 The system shall reject invalid session IDs. **(M)**

4.2.1.1.2 The system shall invalidate session IDs upon user logout. **(M)**

4.2.1.1.3 The system shall invalidate sessions IDs upon session termination. **(M)**

4.2.1.1.4 The system shall generate unique secure random session IDs. **(M)**

End of Document