ERTMS Security Core Group

Threat and Risk Analysis

23E059
1A
26.10.2023

Modification history

Version	Date	Modification / Description	Editor
1A	26.10.2022	Initial Release after EUG and CER Review	Jungo, Christof Kleine, Ernst Metz, Roger Poschinger, Richard Poyet, Nicolas Schubert, Max Yrjölä, Juhana

Table of Contents

1 Introduction

1.1 Scope

The purpose of this document is to provide an overview over the results of the threat and risk assessments which have been performed in the ERTMS Security Core Group (ESCG). These include the definition of the Security Level and a Risk Assessment which results in measures including System Requirements of the IEC 62443-3-3 [1].

1.2 References

[1] IEC 62443-3-3, 2020.

[2] RFC 2119, 1997.

[3] EULYNX, EUG, RCA, OCORA, Security Guideline, 2 ed., 2022: EUG.

[4] ERTMS Security Core Group / ERTMS Users Group, Security Concept, 1 ed., 2022.

[5] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz Compendium - Elementary Threats, 2022.

1.3 Abbreviations

ERORAT ..... *EULYNX EUG RCA OCORA Risk Assessment Tool*
ESCG ..... *ERTMS Security Core Group*
EUG ..... *ERTMS Users Group*
SL ..... *Security Level*
SR ..... *System Requirement*
SuC ..... *System under Consideration*

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)
  - Ernst Kleine
  - Max Schubert
  - Richard Poschinger
  - Roger Metz
- Fintraffic
  - Juhana Yrjölä
- SBB
  - Christof Jungo
- SNCF
  - Nicolas Poyet

1.5 Definition of requirement types

This document uses key words indicating requirement levels according to RFC 2119 [2].

For a better clarity requirement are tagged with

MUST

SHOULD

according to RFC 2119 [2].

To separate requirements from additional information informal texts can be tagged with

INFO

The tag is used as a prefix and is valid for the following text until the end of the chapter.

Texts without a tag do not constitute a requirement.

2 Threat and Risk Analysis

The analysis includes the definition of the security level based on a selected threat catalogue. Based on these prerequisites a full risk analysis is performed to define risks and corresponding mitigating measures as well as risk acceptance definitions.

2.1 Methodology

The ESCG used the EULYNX EUG RCA OCORA Risk Assessment Tool (ERORAT) to define the Security Level (SL) and preselect System Requirements (SRs) based on the SL-Vector. These SRs are selected as mitigating measures completed by additional measures which help to reduce the risk.

The full process implementing IEC 62443 and TS 50701 is defined in the Security Guideline [3], which is as well used by the European projects EULYNX, OCORA and RCA.

According to the Security Guideline the following inputs need to be provided to perform the ERORAT-based analysis:

- System under Consideration (SuC)
  Definition of all components which are part of the assessed system.
- Zoning Concept
  Zones based on a preliminary risk or protection requirements analysis.
- Attacker types
  Details on attacker types (including resources and knowledge available to this attacker type) which are considered.

These definitions are documented in the ESCG Security Concept [4].

ERORAT requires a threat catalogue to perform the analysis. The ESCG has selected the elementary threat catalogue of the BSI [5] (German Federal Office for Information Security) and not chosen not to add additional threats.

The detailed assessment (using ERORAT) is available to the EUG members.

2.2 Assessed Zones

The zones analysed in this document are based on the zoning concept [4]. The separation of zone in current and future standards is also addressed in the ESCG security concept [4]. Not every Zone has to be analysed (see Table 1) for a future release, as the corresponding components will not be part of ERTMS anymore. Furthermore, some systems with equal protection requirements and risks like the PKI are grouped to one assessment. The KMC is only analysed according to the current SoS, as it will not be used as a security feature anymore as soon as state of the art asymmetric cryptography is used to secure the ETCS connections.

Zone	SoS3	Future TSI
Eurobalise	✓	✓
Euroloop	✓	∅
RIU	✓	∅
RBC	✓	✓
KMC	✓	∅*
ETCS On-Board	✓	✓
PKI OKM	✓**	✓**
PKI Euroradio	∅	✓
GSM-R / FRMCS	✕	✕
Driver/Operator/User Voice	✕	✕
ATO-OB/TS	✕	✕

Table 1: Analyzed Zones

✓ = available

∅ = not required/applicable

✕ = postponed

* KMC security responsibilities are transferred to TLS / PKI Euroradio in the future TSI. The KMC will still be used.

** PKI OKM is analysed in the PKI Euroradio assessment

2.3 Security Levels

The definition of the target SL (SL-T) is necessary to have a documented basis for choosing the required measures to ensure security for the system. The vectors have been defined according to the EUG/EULYNX/OCORA (Cyber) Security Guideline in the corresponding Risk Assessment Excel Sheet (ERORAT). The result is the final target Security Level for each zone. In the following all SL-Vectors for each asset are shown for SoS 3 (Table 2) and Future TSI (Table 3).

According to the method described in the Security Guideline [3] these SLs define an initial selection of System Requirements (SR) per Foundational Requirement (FR). During the Risk Assessment Phase these preselected SRs can be used to mitigate existing risks. If SRs are not required according to the Risk Assessment, a reason is provided why they are not implemented. The result of the process is document in Chapter 3. Furthermore, selecting an SR in the assessment does not indicate that the requirement has to be applied to every aspect of the component. For example, requirements regarding confidentiality of data transfer might only be applied to maintenance and diagnostic connections and not be relevant for operational network traffic. Hence only a subset of the SL-based selection of SR is transferred to the specifications. The resulting SRs are achievable according to the technical assessments of the ESCG.

Zone\Foundational Requirement	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS On-Board	PKI OKM	PKI Euroradio
IAC (Identification and Authentication Control)	3	3	4	4	4	4	4	-
UC (Use Control)	4	4	4	4	4	4	4	-
SI (System Integrity)	3	3	4	4	4	4	4	-
DC (Data Confidentiality)	0	0	4	4	4	4	4	-
RDF (Restricted Data Flow)	3	3	4	4	4	4	4	-
TRE (Timely Response to Events)	3	3	4	4	4	4	4	-
RA (Resource Availability)	3	3	4	4	4	4	4	-
SL-T	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**-**

Table 2: SL Vectors for SoS 3

Zone\Foundational Requirement	Eurobalise	Euroloop	RIU	RBC	KMC*	ETCS On-Board	PKI OKM	PKI Euroradio
IAC (Identification and Authentication Control)	3	-	-	4	-	4	4	4
UC (Use Control)	4	-	-	4	-	4	4	4
SI (System Integrity)	3	-	-	4	-	4	4	4
DC (Data Confidentiality)	3	-	-	4	-	4	4	4
RDF (Restricted Data Flow)	3	-	-	4	-	4	4	4
TRE (Timely Response to Events)	3	-	-	4	-	4	4	4
RA (Resource Availability)	3	-	-	4	-	4	4	4
SL-T	**4**	**-**	**-**	**4**	**-**	**4**	**4**	**4**

Table 3: SL Vectors for Future TSI

* The KMC Assessment for Future TSI is based on the SL vector of the SoS3 assessment. The SRs and measures applied are adapted to the reduced security responsibility of the KMC in the Future TSI according to Table 1.

3 IEC 62443-3-3 Compliance Check

To meet the regulatory requirements, it is necessary to assure that all necessary SRs are considered and implemented. Most of the 62443-3-3 SRs have been selected during the risk assessment while others are not applicable. The SR must not be implemented if the SR cannot be applied to the zone (e.g., SR for radio connections if not radio connection exists) or if the SR is not required as proved by the risk assessment.

This check was only performed for the assets included in the analysis for future TSIs [1]. The reasons for not implementing specific requirements are provided in Risk Assessment Excel Sheet (ERORAT).) for each asset. The main reasons of performing this check are to ensure quality assurance and to reduce the requirements to the just needed and applicable ones.

✓ = available

✕ = not selected according to risk assessment or not applicable

○ = not required according to SL-T definition

System Requirement	FR	Lowest SL	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS-On Board	PKI OKM	PKI Euroradio
SR 1.1	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.1 RE 1	IAC	2	✓	-	-	✓	✓	✓	✓	✓
SR 1.1 RE 2	IAC	3	✓	-	-	✓	✓	✓	✓	✓
SR 1.1 RE 3	IAC	4	○	-	-	✓	✓	✓	✓	✓
SR 1.2,	IAC	2	✕	-	-	✓	✓	✓	✓	✓
SR 1.2 RE 1	IAC	3	✕	-	-	✓	✓	✓	✓	✓
SR 1.3	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.3 RE 1	IAC	3	✓	-	-	✓	✓	✓	✓	✓
SR 1.4	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.5	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.5 RE 1	IAC	3	✓	-	-	✓	✓	✓	✓	✓
SR 1.6	IAC	1	✕	-	-	✕	✕	✕	✕	✕
SR 1.6. RE 1	IAC	2	✕	-	-	✕	✕	✕	✕	✕
SR 1.7	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.7 RE 1	IAC	3	✓	-	-	✓	✓	✓	✓	✓
SR 1.7 RE 2	IAC	4	○	-	-	✓	✓	✓	✓	✓
SR 1.8	IAC	2	✕	-	-	✓	✓	✓	✓	✓
SR 1.9	IAC	2	✕	-	-	✓	✓	✓	✓	✓
SR 1.9 RE 1	IAC	3	✕	-	-	✓	✓	✓	✓	✓
SR 1.10	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.11	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.12	IAC	1	✓	-	-	✓	✓	✓	✓	✓
SR 1.13	IAC	1	✕	-	-	✓	✓	✓	✓	✓

System Requirement	FR	Lowest SL	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS-On Board	PKI OKM	PKI Euroradio
SR 1.13 RE 1	IAC	2	✗	-	-	✓	✓	✓	✓	✓
SR 2.1	UC	1	✗	-	-	✓	✓	✓	✓	✓
SR 2.1 RE 1	UC	2	✓	-	-	✓	✓	✓	✓	✓
SR 2.1 RE 2	UC	2	✓	-	-	✓	✓	✓	✓	✓
SR 2.1 RE 3	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.1 RE 4	UC	4	✓	-	-	✓	✓	✓	✓	✓
SR 2.2	UC	1	✗	-	-	✗	✗	✗	✗	✗
SR 2.2 RE 1	UC	3	✗	-	-	✗	✗	✗	✗	✗
SR 2.3	UC	1	✗	-	-	✗	✗	✓	✗	✗
SR 2.3 RE 1	UC	3	✗	-	-	✗	✗	✓	✗	✗
SR 2.4	UC	1	✗	-	-	✓	✓	✓	✓	✓
SR 2.4 RE 1	UC	3	✗	-	-	✗	✗	✓	✗	✗
SR 2.5	UC	1	✓	-	-	✓	✓	✓	✓	✓
SR 2.6	UC	2	✗	-	-	✓	✓	✓	✓	✓
SR 2.7	UC	3	✗	-	-	✓	✓	✓	✓	✓
SR 2.8	UC	1	✓	-	-	✓	✓	✓	✓	✓
SR 2.8 RE 1	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.9	UC	1	✓	-	-	✓	✓	✓	✓	✓
SR 2.9 RE 1	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.10	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.11	UC	2	✓	-	-	✓	✓	✓	✓	✓
SR 2.11 RE 1	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.11 RE 2	UC	4	✓	-	-	✓	✓	✓	✓	✓

System Requirement	FR	Lowest SL	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS-On Board	PKI OKM	PKI Euroradio
SR 2.12	UC	3	✓	-	-	✓	✓	✓	✓	✓
SR 2.12 RE 1	UC	4	✓	-	-	✓	✓	✓	✓	✓
SR 3.1	SI	1	✓	-	-	✓	✓	✓	✓	✓
SR 3.1 RE 1	SI	3	✓	-	-	✓	✓	✓	✓	✓
SR 3.2	SI	1	✕	-	-	✓	✓	✓	✓	✓
SR 3.2 RE 1	SI	2	✕	-	-	✓	✓	✓	✓	✓
SR 3.2 RE 2	SI	3	✕	-	-	✓	✓	✓	✓	✓
SR 3.3	SI	1	✓	-	-	✓	✓	✓	✓	✓
SR 3.3 RE 1	SI	3	✓	-	-	✓	✓	✓	✓	✓
SR 3.3 RE 2	SI	4	○	-	-	✓	✓	✓	✓	✓
SR 3.4	SI	2	✓	-	-	✓	✓	✓	✓	✓
SR 3.4 RE 1	SI	3	✓	-	-	✓	✓	✓	✓	✓
SR 3.5	SI	1	✕	-	-	✓	✓	✓	✓	✓
SR 3.6	SI	1	✕	-	-	✓	✓	✓	✓	✓
SR 3.7	SI	2	✕	-	-	✓	✓	✓	✓	✓
SR 3.8	SI	2	✕	-	-	✓	✓	✓	✓	✓
SR 3.8 RE 1	SI	3	✕	-	-	✓	✓	✓	✓	✓
SR 3.8 RE 2	SI	3	✕	-	-	✓	✓	✓	✓	✓
SR 3.8 RE 3	SI	4	○	-	-	✓	✓	✓	✓	✓
SR 3.9	SI	2	✕	-	-	✓	✓	✓	✓	✓
SR 3.9 RE 1	SI	4	○	-	-	✓	✓	✓	✓	✓
SR 4.1	DC	1	✕	-	-	✓	✓	✓	✓	✓
SR 4.1 RE 1	DC	2	✕	-	-	✓	✓	✓	✓	✓

System Requirement	FR	Lowest SL	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS-On Board	PKI OKM	PKI Euroradio
SR 4.1 RE 2	DC	4	○	-	-	✓	✓	✓	✓	✓
SR 4.2	DC	2	✕	-	-	✓	✓	✓	✓	✓
SR 4.2 RE 1	DC	3	✕	-	-	✓	✓	✓	✓	✓
SR 4.3	DC	1	✕	-	-	✓	✓	✓	✓	✓
SR 5.1	RDF	1	✕	-	-	✓	✓	✓	✓	✓
SR 5.1 RE 1	RDF	2	✕	-	-	✓	✓	✓	✓	✓
SR 5.1 RE 2	RDF	3	✕	-	-	✓	✓	✓	✓	✓
SR 5.1 RE 3	RDF	4	○	-	-	✓	✓	✓	✓	✓
SR 5.2	RDF	1	✕	-	-	✓	✓	✓	✓	✓
SR 5.2 RE 1	RDF	2	✕	-	-	✓	✓	✓	✓	✓
SR 5.2 RE 2	RDF	3	✕	-	-	✓	✓	✓	✓	✓
SR 5.2 RE 3	RDF	3	✕	-	-	✓	✓	✓	✓	✓
SR 5.3	RDF	1	✕	-	-	✓	✓	✓	✓	✓
SR 5.3 RE 1	RDF	3	✕	-	-	✓	✓	✓	✓	✓
SR 5.4	RDF	1	✕	-	-	✓	✓	✓	✓	✓
SR 6.1	TRE	1	✕	-	-	✓	✓	✓	✓	✓
SR 6.1 RE 1	TRE	3	✕	-	-	✓	✓	✓	✓	✓
SR 6.2	TRE	2	✕	-	-	✓	✓	✓	✓	✓
SR 7.1	RA	1	✕	-	-	✓	✓	✓	✓	✓
SR 7.1 RE 1	RA	2	✕	-	-	✓	✓	✓	✓	✓
SR 7.1 RE 2	RA	3	✕	-	-	✓	✓	✓	✓	✓
SR 7.2	RA	1	✕	-	-	✓	✓	✓	✓	✓
SR 7.3	RA	1	✕	-	-	✓	✓	✓	✓	✓

System Requirement	FR	Lowest SL	Eurobalise	Euroloop	RIU	RBC	KMC	ETCS-On Board	PKI OKM	PKI Euroradio
SR 7.3 RE 1	RA	2	✗	-	-	✓	✓	✓	✓	✓
SR 7.3 RE 2	RA	3	✗	-	-	✓	✓	✓	✓	✓
SR 7.4	RA	1	✗	-	-	✓	✓	✓	✓	✓
SR 7.5	RA	1	✗	-	-	✗	✓	✗	✗	✗
SR 7.6	RA	1	✗	-	-	✓	✓	✓	✓	✓
SR 7.6 RE 1	RA	3	✗	-	-	✓	✓	✓	✓	✓
SR 7.7	RA	1	✗	-	-	✓	✓	✓	✓	✓
SR 7.8	RA	2	✗	-	-	✓	✓	✓	✓	✓

Table 4: Compliance Check for System Requirements

End of Document