ERTMS Security Core Group

Security Concept

23E060
1A
26.10.2023

Modification history

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

Table of Contents

1 Introduction

1.1 Scope

The purpose of this document is to define the security requirements 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 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] EULYNX, EUG, RCA, OCORA, Security Guideline, 2 ed., 2022: EUG.

[3] IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

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

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

[6] ERA, *ERA_ERTMS_015560,* 3.6.0 ed., 2016.

[7] EUROPEAN INTEGRATED RAILWAY RADIO; GSM-R Functional Group, *Functional Requirements Specification,* 8.0.0 (0.0.2) red.

[8] OCORA, *OCORA-TWS01-030,* 2.0.1 ed., vol. R1, 2021.

[9] EULYNX Consortium, *Eu.Doc.7,* 3.5 ed., 2020.

[10] EULYNX Consortium, *Eu.Doc.15,* 4.1 ed., 2022.

[11] OCORA, *OCORA-BWS03-010,* 5.0 ed., vol. R1, 2021.

[12] *RCA.Doc.35,* 0.2 ed., 2020.

Subset are referenced directly with their corresponding ID.

1.3 Abbreviations

APR ..... *Assessment of the Protection Requirements*
ATO ..... *Automatic Train Operation*
CCS ..... *Command Control and Signalling*, *Command, Control and Signaling*
CMP ..... *Certificate Management Protocol*
CMS ..... *Configuration Management System*
EfeS ..... *EULYNX Field Element Subsystem*
EIL ..... *Electronic Interlocking*
ERTMS ..... *European Rail Traffic Management System*
ESCG ..... *ERTMS Security Core Group*
EUG ..... *ERTMS Users Group*
FRMCS ..... *Future Rail Mobile Communication System*
FVA ..... *Functional Vehicle Adapter*
IACS ..... *Industrial Information and Control Systems*
IAM ..... *Identity and Access Management*
IM ..... *Infrastructure Manager*
OC ..... *Object Controller*
OCORA ..... *Open CCS On-Board Reference Architecture*
OCSP ..... *Online Certificate Status Protocol*
OKM ..... *Online Key Management*
PKI ..... *Public Key Infrastructure*
RU ..... *Railway Undertaking*
SIEM ..... *Security Incident and Event Management*
SoS ..... *Set of Specifications*
SuC ..... *System Under Consideration*
TCMS ..... *Train Control Management System*
TCS ..... *Traffic Control System*
TS ..... *Trackside*

Note: ERTMS Abbreviations are listed in SUBSET-023

1.4 Authors

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

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

1.5 Definition of requirement types

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

For a better clarity requirement are tagged with

MUST

SHOULD

according to RFC 2119 [1].

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 Security for Railway Operations

2.1 Legal requirements from NIS directive

Since July 2016 the [NIS Directive] is in force for countries of the European Union and has an impact on the Critical Infrastructures of these countries as it poses several requirements on these.

As an operator of essential services (if classified as such) the railway operator shall:

- Prevent risks by taking technical and organisational measures that are appropriate and proportionate to the risk.
- Ensure security of network and information systems. The measures should ensure a level of security of network and information systems appropriate to the risks
- Handle incidents, which means that he prevents and minimises the impact of incidents on the IT systems used.
- Reports notifiable incidents according to the number of affected users, duration of the incident and the geographic spread.

2.2 Security principles

The security principles applied in the concept and related specification documents are listed in the following chapters.

2.2.1 Secure by Design

Make security part of requirements, and not an afterthought.

Rationale

Protect a business application or information system against attacks by considering security requirements as part of its overall requirements.

- Experience has shown it is both costly and difficult to implement security measures after a system has been developed
- Avoid unnecessary development efforts by considering security requirements early on
- as security interferes with safety (e.g., timings, fail behaviour) they must be a holistic approach

Implications

- Understand the resulting security requirements in the engineering, design, implementation, and disposal of the system
- Security should treat the root cause of a problem, not its symptom

2.2.2 Defence in Depth

Avoid reliance on a single type of security control

Rationale

Implementing security on multiple layers is better than relying on a single defence layer. If one security control fails or is bypassed, an additional layer can help preventing the attack.

- Identify and secure the weakest links first
- Use multiple security layers to increases effort for an attacker to compromise a system or application

Implications

- Create a security architecture that documents the different layers of protection
- Balance defence in depth against simplicity and business needs
- Each deeper security layer should not trust the previous layers
- Compartmentalize the system by defining security boundaries for information flows
- Prepare for the worst possible compromise scenario

2.2.3 Secure by Default

Set secure default options to limit inherent security vulnerabilities

Rationale

System or application configurations should favour security over not being secure. The default setting for a security control should be to deny access to a resource and require a configuration to specifically grant access. When the system goes into an error or exception state, these states must favour security over not being secure.

Implication

- Security should not require extensive configuration to work and should just work reliably where it is implemented
- Establish secure defaults when system starts or goes in error or exception states
- Provide least privilege or make only necessary services and features available
- Use integrity protection and encryption by default for both data at rest and in transit. Omit encryption only if confidentiality protection is not required.

2.2.4 Simplicity over Complexity

Complexity is the worst enemy of security

Rationale

Complexity in systems leads to increased human confusion, errors, vulnerabilities, automation failures, and difficulty of recovering from an issue. Favour simple and consistent architectures,

designs, and implementations. Avoid unnecessary complexity. The more complex the system, the more likely it may possess exploitable flaws

Implication

- Simplicity should be a key objective in design of systems and security
- DRY - do not repeat yourself (Do not implement functions multiple times)
- Reduce the variety and types of hardware and software types and versions
- Design systems that use the least hardware and software resources possible
- Favour convention over configuration
- Do not implement unnecessary security mechanisms
- Complexity makes vulnerabilities harder for developers and testers to uncover. Each feature, function, and interaction are a potential threat vector
- Complexity makes vulnerabilities harder to fix once we find them

Notes

- Do not over-simplify
- Balance reduced complexity against diversity required to achieve resiliency and reduced single-point-of-failures

2.2.5 Assume Failure & Compromise

Complex distributed systems lead to unpredictability and cascading failures

Rationale

We build and operate highly coupled and interactively complex systems. Even when all the individual components of complex system are functioning properly, the interactions between those components can cause unpredictable outcomes and vulnerabilities. Rare or surprising combinations of events, vulnerabilities, and creative user interactions make such systems difficult to predict. Prediction, complete testing, and modelling of all states is not possible in such systems, we therefore must assume and account for failures and compromise.

Implications

- Our systems are too complex to anticipate all potential interactions or vulnerabilities
- Assume that critical parts of the infrastructure can be compromised during the life cycle of the components and systems
- Embrace principles of resilient engineering and testing - facilitate real and repeated tests to uncover systemic weaknesses
- Design system for automated testability
- Establish continuous and comprehensive monitoring of vital parameters to determine system health and security
- Security shall be actively managed over the IACS and product life cycle

2.2.6 Fail Safe and Secure

Failures should lead to a safe and secure state. Risk does not hurt - the impact does

Rationale

If a security control fails, it should maintain a state of deny access. Design security mechanisms so that a failure will follow the same execution path as disallowing the operation. Prevent unauthorized access in case of errors, failures, exceptions, system degradation, or compromise**.**

Implication

- Design to minimize the impact of component or control failures or compromise
- Confidentiality and integrity assurance top availability assurance
- Security methods like `isAuthorized()`, `isAuthenticated()`, and `validate()` should all return false if there is an exception during processing
- Assume system failure & compromise in design decisions

Examples

- Dead man’s switch is automatically operated if the human operator becomes incapacitated
- Traffic light controllers use a Conflict Monitor Unit to detect faults or conflicting signals and switch an intersection to an all-flashing error signal, rather than displaying potentially dangerous conflicting signals.

2.2.7 Zero Trust

Assume everything to be insecure until a level of trust is established

Rationale

The historic concept of trust that is based on a perimeter separating the inside from the outside does no longer hold in today’s rapidly changing environment. Assuming no trust is a security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, apps, and data wherever they are located

Implication

- Trust is not granted until the user, system, or component can be authenticated and authorized first
- Context and evolutions of threats: should be taken in consideration (malwares, new vulnerabilities, etc.) and the system must adapt in consequence
- Verify anything and everything trying to connect to its systems before granting access
- Workforce: Authenticate users (and potential processes) and continuously monitor and govern their access and privileges
- Workloads: Enforce controls across the entire application stack, especially connections between containers or hypervisors in the public cloud

- Data: Secure and manage data, categorize, and develop data classification schema, and encrypt data at rest and in transit
- Supply Chain: Question and assess the integrity and security of suppliers and the delivered products, systems, and services

2.2.8 Least Privilege

Only grant the minimal set of permissions that are necessary for a required/given operation/action - and no more

Rationale

Systems and users should operate while invoking as few privileges as possible. Granting permissions beyond the scope of the necessary rights of an action can allow a user or system to obtain or change information in unwanted ways. This principle limits the damage that can result from an attack, accident, or error. It also reduces the number of potential interactions among privileged systems to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.

Implication

- Minimize the system elements to be trusted
- This principle restricts how privileges are granted and revoked, and time out

2.2.9 Usability & Manageability

Balance of security and usability - make secure behaviour easy instead of complex

Rationale

Make it easy to do the right thing, make it difficult to do the wrong thing, and make it impossible to do the catastrophic thing. Security controls should not obstruct users in performing their work and should not be difficult to manage. User interface must be easy to use, so that users routinely and automatically apply the mechanisms correctly. Relates to the paradigm of Least Astonishment in UI design and Simplicity Principles

Implications

- A component or system should be designed to behave in a manner consistent with how users of that component are likely to expect it to behave
- Design security interfaces and functions for ease of use, so that users routinely and automatically apply the protection mechanisms correctly

Note

- If security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security

2.2.10 Design for Automation

Design for Automation to control complexity

Rationale

Manual security tasks are inefficient, expensive, and prone to inconsistencies and human error. It is no longer possible to deploy, operate, and secure complex applications and infrastructures without automation. Security, agility, scalability, and control are a direct function of automation in today's complex and rapidly changing technology and threat environment

Implications

- Automation reduces complexity and ensures consistency
- Reduces the talent gap by freeing scarce expertise form mundane tasks
- automated testing
- requires discipline and design

2.2.11 Open Design

The security of a mechanism should not depend on the secrecy of the details of its design or implementation

Rationale

Assume outsiders and attackers will have access to source code (also for closed source software) and complete design and network topologies. Assume sensitive information regarding security measurements are leaked or sold. Encourage proactive reporting of security issues or vulnerabilities and act on such reports.

Implications

- Never store secrets in code, documentation, or configurations
- Open security design promotes faster improvement cycles
- Security measurements should be open and transparent

Examples

- Shannon's Maxim: The enemy knows the system

2.3 Process definition

To analyse the risks in the ERTMS architecture and define mitigating measures the Common Security Guideline of the EUG, RCA, OCORA and EULYNX is used [2]. The method defined in the guideline is based on IEC 62443 and the associated extension regarding railway-specific aspects in the standard TS 50701. This implements Phase 3 (risk assessment) of the CENELEC process.

The process defined in the guideline is started by defining the systems under consideration. Thus, the scope of the assessment is determined. Based on this the zones and conduits can be defined, giving a structured overview over the scope.

To set basic assumptions on possible attack vectors an attacker type is defined. Furthermore, based on threats mapped to foundational requirements defined in IEC 62443 and an evaluation of the capabilities and resources required for these attacks. Thus, a security level can be defined for each zone.

As part of the risk assessment based on a predefined target security level the risk can be analysed based on the exposure and vulnerability as well as the likelihood of a threat. Measures based on the IEC 62443 and new compensating measures can or have to be defined depending on the delta between current and target risk. This process is documented in detail to allow later adjustments.

The operational process for analysing threats and risks to derive the suitable measures is defined and explained with an example in the Security Guideline [2].

The process is supported by an Excel tool (ERORAT v2).

2.4 Conformity to IEC 62443

Conformity for products and operators is possible. Therefore, it is recommended to apply IEC 62443-4-1 [3], -4-2 [4] and -3-3 [5] as conformity.

2.5 Assumption on available or to be established security services

The ERTMS environment currently consists of the following security services:

- Public Key Infrastructure (PKI) for Online Key Management

The following security services should be considered as solutions for current implementations and future standards:

- PKI (for other connections where required and compliant)
- Identity and Access Management (IAM)
- Security Logging
- Security Incident and Event Management (SIEM)

These services can be synchronized with the specifications defined by EUG, EULYNX, OCORA, RCA and the results of S2R.

Furthermore, security depends on additional services which provide the management of devices:

- Configuration Management System (CMS)
- Software and Configuration Repository
- Backup
- Asset Inventory

3 System under Consideration

The system under consideration (SuC) consists of all the systems relevant for railway operations from ERTMS perspective. Additional components used to provide security (e.g., KMC, PKI) are not addressed in Figure 1 to provide a focus on operational aspects.

Figure 1 shows the relevant systems in the railway domain for the ESCG analyses. Onboard systems and systems which are located trackside (infrastructure) are grouped according to the project responsible for its standardization.

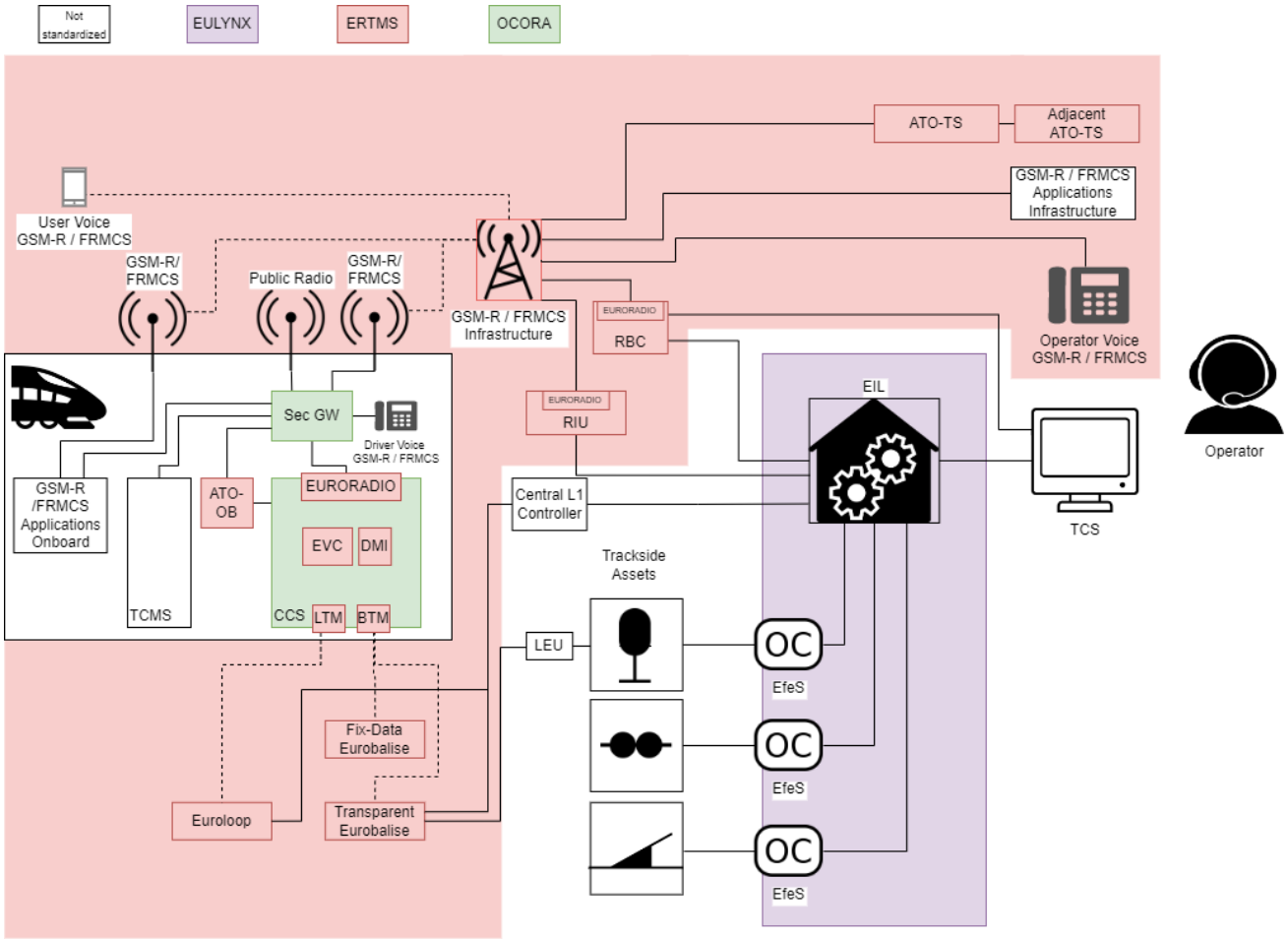

Figure 1: System under Consideration

Systems with a red background are part of the systems under consideration of this document and are defined in the ERTMS projects.

The GSM-R/FRMCS Applications on infrastructure side are excluded, as they are not standardized but their connection to the GSM-R infrastructure is included partly.

The on-board architecture is standardized by OCORA (green background). Thus, is it not taken into consideration by ESCG. Only the central EVC and the DMI as well as components connecting the train to the infrastructure (BTM, LTM, EURORADIO) are part of the SuC.

The interlocking and connected controllers of trackside are defined in EULYNX. Furthermore, EULYNX defines the interfaces from the Interlocking (EIL) to the RBC and the Central L1 Controller.

Systems without any coloured background are not standardized and are implemented by the supplier as proprietary systems. Only the interfaces to these systems are partly standardized.

3.1 ERTMS Scope

The ERTMS Scope defines systems which are assessed and analysed in the ESCG.

3.1.1 ETCS On-board

The ERTMS/ETCS on-board equipment is a computer-based system that supervises the movement of the train to which it belongs, on basis of information exchanged with the trackside subsystem [Subset 026].

The ETCS On-board consist of the following subcomponents:

- EVC (European Vital Computer)
  Safe vehicle computer and core of the ETCS vehicle equipment.
- DMI (Driver Machine Interface)
  The DMI is used to harmonize “the presentation of displayed information and the driver’s interactions with the equipment (…)”. It “(…) contributes to a unified operation of the trains regardless of which supplier’s products they are fitted with”. [3]
- LTM (Loop Transmission Module)
  The LTM is the combination “of Loop Receiver (LR) Function and Loop Decoder (LD) Function.”. It is used to connect the EVC to the trackside Euroloop. [Subset 044]
- BTM (Balise Transmission Module)
  The BTM is an “On-board module for intermittent transmission between track and train, which processes Up-link signals and telegrams from a Balise. It interfaces the ERTMS/ETCS Kernel and the Antenna Unit.” [Subset 036]

3.1.2 Euroradio On-board

The GSM-R on-board radio system is used for the bi-directional exchange of messages between on-board subsystem and RBC or radio infill unit [Subset 026].

3.1.3 RBC

“The RBC is a computer-based system that elaborates messages to be sent to the train on basis of information received from external trackside systems and on basis of information exchanged with the on-board subsystems” [Subset 026]. Furthermore, the RBC needs to be able to perform the handover to another RBC for a train passing the RBC borders.

3.1.4 RIU

“The RADIO INFILL subsystem operates on Level 1 lines, providing signalling information in advance as regard to the next main signal in the train running direction” [Subset 026]. It uses a mobile communication network (GSM-R/FRMCS) to transmit the information to the train.

3.1.5 Eurobalise

“The balise is a transmission device that can send telegrams to the on-board Subsystem” [Subset 026]. “A wayside Transmission Unit that uses the Magnetic Transponder Technology. Its main function is to transmit and/or receive signals through the air gap. The Balise is a single device mounted

on the track, which communicates with a train passing over it. In this specification, Balise is used as a short word for Eurobalise, unless otherwise stated.” [Subset 036]

3.1.6 Euroloop

“The Euroloop subsystem operates on Level 1 lines, providing signalling information in advance as regard to the next main signal in the train running direction [Subset 026]. The Euroloop Subsystem is a semi-continuous, intermittent transmission system. It transmits in-fill information from the trackside infrastructure to a train (up-link) at standstill or movement along a section of the track. (…) It uses a leaky cable as a trackside transmission antenna. The Euroloop system is composed of an On-board Equipment and one or several Trackside Equipments.” [Subset 044]

3.1.7 GSM-R / FRMCS and subsystems

The GSM-R radio communication network is used for the bi-directional exchange of messages between on-board subsystems and RBC or radio infill units [Subset 026].

The Future Rail Mobile Communication System (FRMCS) will be the successor of GSM-R.

3.1.8 KMC

A KMC is responsible for the generation of the key entries needed to establish safe connections between trackside entities belonging to its domain and any on-board entity [Subset 0139].

3.1.9 PKI OKM

The PKI ensures the creation, renewal, and validation of Euroradio's digital certificates which are used to establish a secure connection from the RBC (and RIU) and on-board Euroradio module to the KMC.

3.1.10 PKI Euroradio

The PKI ensures the creation, renewal, and validation of Euroradio's digital certificates and provides them to the Euroradio modules. The certificates are used to establish a secure hybrid encrypted connection from the RBC to the on-board Euroradio module.

3.1.11 Operator, Driver, and User Voice

Voice connections used by operators, drivers and other users are provided based on GSM-R and FRMCS. The infrastructure side of the mobile connections also includes a local connectivity infrastructure.

- “point-to-point voice calls;
- public emergency calls;
- broadcast voice calls;
- group voice calls;
- multi-party voice calls Radio Application” [4]

3.1.12 ATO-OB

ATO-OB “is a non-safe application for Automatic train operations. A safe extension is needed for GoA3 and GoA4 operations.” [5] “It shall drive the train so as to respect the time table provided by ATO-TS without infringing the safe limits imposed by ETCS-OB.“It “shall drive the train automatically while it is engaged [Subset 125].

3.1.13 ATO-TS

ATO-TS sends journey profiles, segment profiles and stopping points to ATO-OB [Subset 125].

3.2 Out of Scope

3.2.1 GSM-R / FRMCS Application Infrastructure and On-Board

Different applications can use the mobile connection infrastructure (GSM-R/FRMCS) connecting On Board systems to the infrastructure. These include:

- “text message bearer service;
- bearer service for general data applications;
- bearer service for automatic fax;
- bearer service for train control applications;” [4]

“The FRMCS On-Board System implements the required functionalities and services providing the connectivity for the CCS Systems with the RBC (for ETCS L2/L3 networks), with ATO trackside (ATO-AT) and with the RCA compliant CCS Data Centres respectively.” [5]

3.2.2 Central L1 Controller

“The Centralised ETCS L1 Controller communicates variable signalling data to balise drivers, based on the information from the subsystem Electronic Interlocking. The balise driver controls switchable balises.” [6]

System specified in: - (Supplier specific)

3.2.3 LEU

“The lineside electronic units are electronic devices, that generate telegrams to be sent by balises, on basis of information received from external trackside systems” [Subset 026].

System specified in: - (Supplier specific)

3.2.4 EfeS (OC)

“The EULYNX field element Subsystem provides the link between EIL and Trackside Asset. It represents the boundary between EULYNX-scope and vendor-specific standards for the trackside asset. (…) It provides interfaces for the control of field element subsystems (…)” [7]

System specified in: EULYNX (interface and security)

3.2.5 EIL

The Electronic Interlocking establishes safety relevant dependencies and processes commands to and from the subsystems and adjacent systems. [6]

System specified in: EULYNX (interface and security)

3.2.6 Trackside Assets

Following components controlled by the interlocking are categorized as trackside assets:

- Points
- Light Signals
- Level Crossings
- Train Detection Systems

Following ERTMS systems are part of the EULYNX definition of trackside assets:

- Central L1 Controller

[7] [6]

System specified in: - (Supplier specific)

3.2.7 OCORA Security Gateway

The OCORA Security Gateway is the central component that enables and secures a connection of the on-board components to the outside. It will be added in release 2 of the OCORA.

System specified in: OCORA

3.2.8 OCORA CCS Architecture and FVA

The OCORA projects “aims to reduce life-cycle costs and facilitate the introduction of innovation and digital technologies beyond the current proprietary interfaces, by establishing a modular, upgradeable, reliable and secure CCS on-board architecture.” [8]

System specified in: OCORA

3.2.9 TCS

“In EULYNX System architecture, the Command Control System is considered as part of the Traffic Control System (…)” [6] “The Command Control System serves as the human-machine-interface between the signaller and the connected systems.” [6]

System specified in: - (Supplier specific)

3.3 Involved Staff

To address authorisation and access management the following staff (human users) definitions are provided.

3.3.1 Maintenance Staff

Maintenance staff is responsible “for the technical operation and maintenance” of “systems, including Software, Hardware, and communication systems.

Provides and uses data with respect to the status of Software, Hardware, and communications systems.” [9]

3.3.2 Driver

“A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible, and safe manner.” [9]

3.3.3 Operator

“The Railway Operator manages, directs, and facilitates the movement of trains over an assigned area.” [9]

4 Assumptions and Definitions

4.1 Set of Specification

The assessed security architecture for existing implementations is based on ERA ERTMS set of specifications #3.

4.2 SUBSET Drafts

For future standardisation all drafts of subsets available to the ESCG are considered. These drafts are referenced in the respective chapters.

4.3 Assumptions for Protection Requirements

Non-repudiation is set to middle if health damage is (very) high in other Assessment of the Protection Requirements (APR) categories. It is set to middle as juridical consequences and nationwide reporting can be expected if the cause of an accident cannot be identified.

4.4 Definition of Protection Requirements

To provide a basis for the creation of zones, an assessment of the protection requirement is used. This assessment provides the protection requirements for the following categories:

- Confidentiality
- Integrity
- Availability
- Non-Repudiation
- Authenticity (only Human-Machine-Interaction)

For the classification of the protection requirements a scheme was used, which is available to the EUG members.

4.5 Mapping of APR to Risk Assessment

The ERORAT-based risk assessment is using the impact as part of the risk calculation. Furthermore, the impact is used to define the Security Level. This impact is in both cases assessed for each threat. As the maximum impact has already assessed in the APR to define the protection requirements these results can be reused to verify the ERORAT impact values.

However, the impact definition varies in both approaches. ERORAT is using the method based on TS 50701 and the APR is using a more fine-grained approach. Both methods are based on four different levels. Based on the comparison of the methods for each level the following mapping is used:

APR	ERORAT
Low	D
Middle	C
High	B
Very High	A

Table 1: Impact Mapping

The definitions of the levels per protection requirement matches and can be directly mapped for the following categories (APR / ERORAT):

- Health damage / Human health and safety
- Financial impact / Financial impact

If high values in the APR result from the following categories, detailed evaluation may be required:

- Disruption of business activity / Operational availability

The following categories are only available in the APR definition:

- Loss of reputation
- Privacy Violations
- Violation of laws, regulations, and rules

This mapping is used to check if the maximum impact in the ERORAT tool is valid according to the APR.

4.6 Processual Security

Security cannot be established just using technical measures. To establish secure operation of a product during the whole lifecycle, corresponding security processes must be established. These processes must be used to handle e.g., the supply chain, updates/configuration changes and maintenance. These processes are required by established security standards like IEC 62443.

These processes must be defined by the Railway Undertaking (RU) and Infrastructure Manager (IM). International standards can support the definition of these processes. Furthermore, they can provide a harmonized basis which increases the process quality as well as the effectiveness.

Security processes must be perfectly tailored to the system. Hence, technical standardisations projects like EULYNX already provide process templates in terms of security. In the ERTMS domain

this has not been addressed yet, which results in the mission of the ESCG to define technical as well as processual measures.

As no European standards for ERTMS security processes exist, all assessments are initially performed without considering these processes, even if some IMs and RUs might have already partially addressed this issue internally.

5 Zones

The following drawing presents the grouping of the assets into zones and conduits. A zone or a conduit shares common cybersecurity requirements.

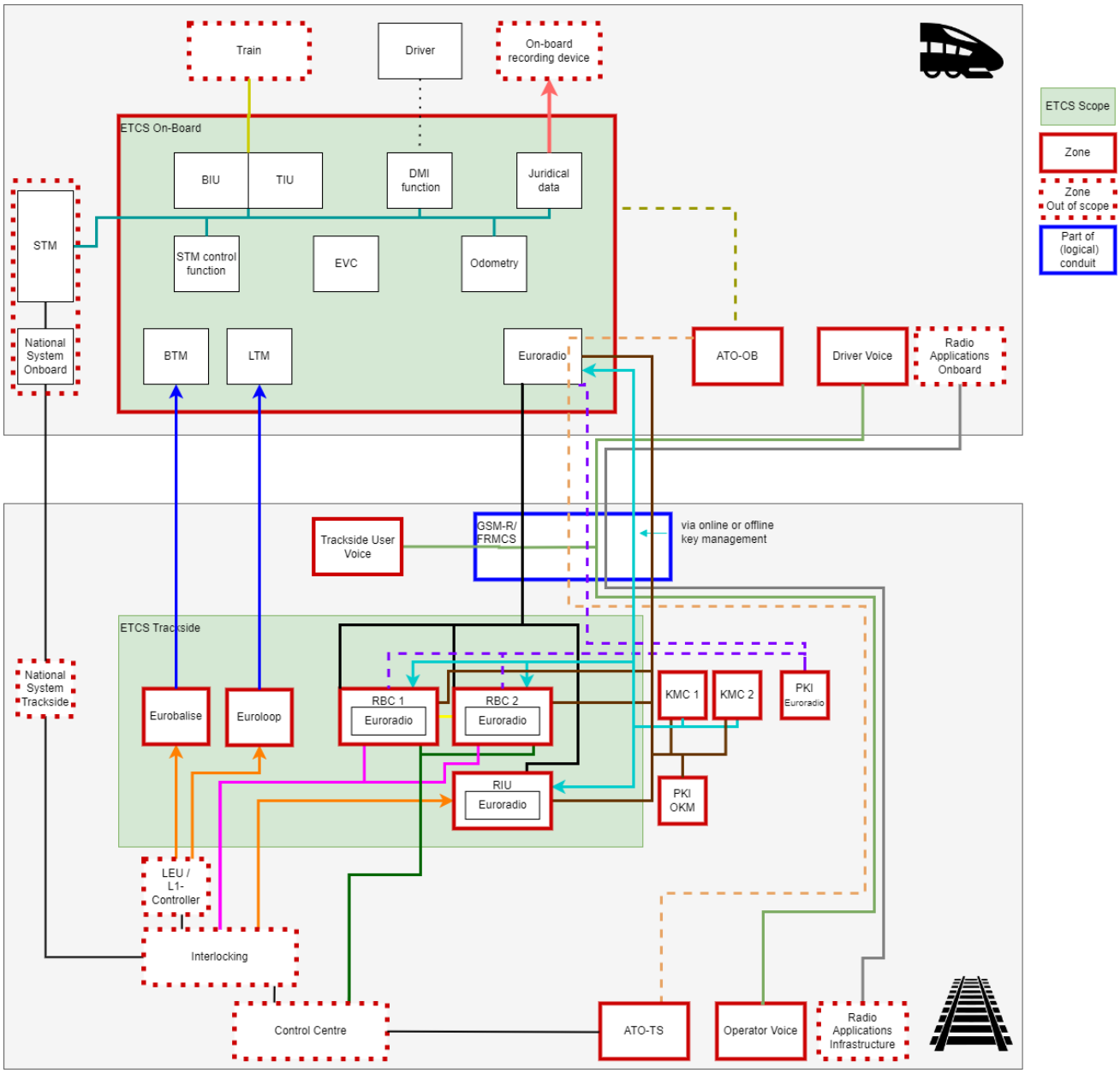

Figure 2: Zones and Conduits

5.1 Trackside

In the following Chapter all the Trackside Elements are described.

5.1.1 In Scope

All Trackside elements in Figure 2 which we are observing for ERTMS.

5.1.1.1 RBC

Zone description:

Described in Section 3.1.3

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L2	Very High	Very High	High	Middle	Not relevant
L3	Very High	Very High	High	Middle	Not relevant

5.1.1.2 RIU

Zone description:

Described in Section 3.1.4

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Very High	Very High	Low	Middle	Not relevant
L2	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L3	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant

5.1.1.3 Euroloop

Zone description:

Described in Section 3.1.6

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Very High	Low	Middle	Not relevant
L2	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L3	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant

5.1.1.4 Eurobalise

Zone description:

Described in Section 3.1.5

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Very High	Low	Middle	Not relevant
L2	Not relevant	Very High	Low	Middle	Not relevant
L3	Not relevant	Very High	Low	Middle	Not relevant

5.1.1.5 KMC

Zone description:

Described in Section 3.1.8

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L2	Very High	Very High	High	Middle	Very High
L3	Very High	Very High	High	Middle	Very High

5.1.1.6 PKI OKM

Zone description:

Described in Section 3.1.9

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L2	Very High	Very High	Middle	Middle	Very High
L3	Very High	Very High	Middle	Middle	Very High

5.1.1.7 PKI Euroradio

Zone description:

Described in Section 3.1.10

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
L2	Very High	Very High	Middle	Middle	Very High
L3	Very High	Very High	Middle	Middle	Very High

5.1.1.8 Operator Voice

Zone description:

Described in Section 3.1.11

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Low	Very High	Very High	Middle	Not relevant
L2	Low	Very High	Very High	Middle	Not relevant
L3	Low	Very High	Very High	Middle	Not relevant

5.1.1.9 Trackside User Voice

Zone description:

Described in Section 3.1.11

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Low	Very High	Very High	Middle	Low
L2	Low	Very High	Very High	Middle	Low
L3	Low	Very High	Very High	Middle	Low

5.1.1.10 ATO-TS

Zone description:

Described in Section 3.1.13

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	High	High	High	Middle	Not relevant
L2	High	High	High	Middle	Not relevant
L3	High	High	High	Middle	Not relevant

5.1.1.11 GSM-R / FRMCS

Zone description:

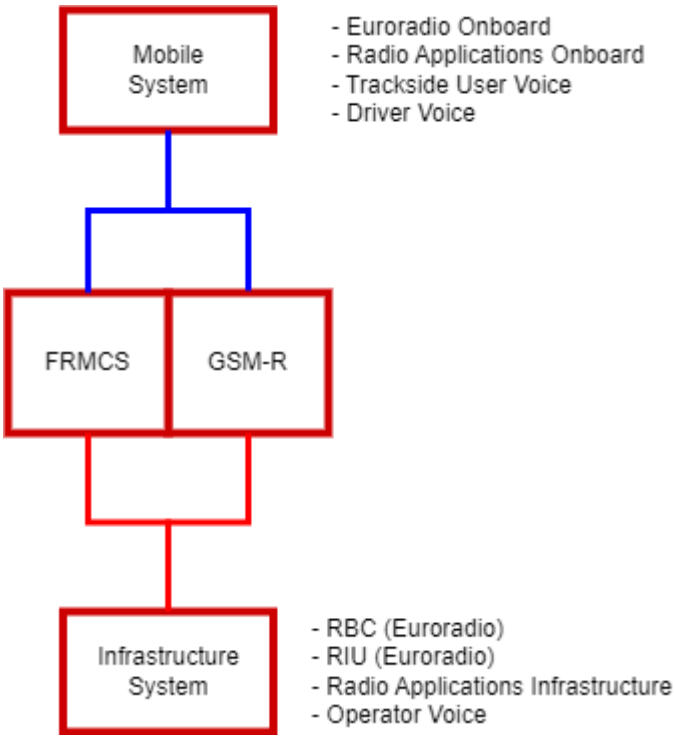

Figure 3: GSM-R / FRMCS Zoning

Protection requirements:

The GSM-R and FRMCS mobile network is assessed separately. The overall zoning is not addressing these mobile networks directly. Conduits like the Euroradio connections are using the mobile networks but these conduits are assessed on the transport and application layer. These conduits only generate requirements for the mobile network layers below.

As both mobile network technologies (GSM-R and FRMCS) are also in the scope of the ESCG, it is necessary to evaluate the protection requirements of them as well. The assessment of this subzones is based on the maximum protection requirements of the application layer conduits.

The protection requirements for this zone assume, that the transport and application layer are already protected according to the assigned protection requirements. Hence protection requirements for integrity and confidentiality are not transferred to the mobile network layer.

5.1.1.11.1 Mobile System

Zone description:

Describes the collected communication of the systems Euroradio Onboard, Radio Applications Onboard, Trackside User Voice and Driver Voice via GSM-R/ FRMCS with the Infrastructure System.

Protection requirements:

Assessed in the specific protection requirements assessments of the referenced zones.

5.1.1.11.2 GSM-R/FRMCS

Zone description:

Described in Section 3.1.7

Protection requirements:

	Confidentiality	**Integrity**	**Availability**	**Non-Repudiation**	**Authenticity (only Human-Machine-Interaction)**
Protection Requirement (Without Voice)	Not relevant	Not relevant	High	Middle	Not relevant
Protection Requirement (With Voice)	Not relevant	Very High	Very High	Middle	Not relevant

5.1.1.11.3 Infrastructure System

Zone description:

Described in Section Describes the collected communication of the RBC, RIU, Radio Applications Infrastructure and Operator Voice via GSM-R/ FRMCS with the Mobile System.

Protection requirements:

Assessed in the specific protection requirements assessments of the referenced zones.

5.1.2 Out of Scope

All Elements of the Trackside which do not have to be considered for ERTMS.

5.1.2.1 Radio Application

Described in Section 3.2.1

5.1.2.2 Interlocking

Described in Section 3.2.5

5.1.2.3 Control Centre

Described in Section 3.2.9

5.1.2.4 National System Trackside

The National system trackside is the trackside part of a train protection system in railway with technical installations to ensure safe operation in the event of human error. The National system trackside can consist of different ATP solutions (LZP, PZB etc.).

ATP is a system which continually checks that the speed of a train is compatible with the permitted speed allowed by signalling, including automatic stop at certain signal aspects.

5.1.2.5 LEU / L1-Controller

The LEU is described in Chapter 3.2.3 and the L1-Controller is explained in Chapter 3.2.1.

5.2 Onboard

In the following Chapter all the Onboard Elements are described.

5.2.1 In Scope

All Onboard elements in Figure 2 which are considered for ERTMS.

5.2.1.1 ETCS Onboard

Zone description:

Described in Section 3.1.1

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Very High	Very High	Low	Middle	Not relevant
L2	Very High	Very High	Low	Middle	Not relevant
L3	Very High	Very High	Low	Middle	Not relevant

5.2.1.2 Driver Voice

Zone description:

Described in Section 3.1.11

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Low	Very High	Very High	Middle	Low
L2	Low	Very High	Very High	Middle	Low
L3	Low	Very High	Very High	Middle	Low

5.2.1.3 ATO-OB

Zone description:

Described in Section 3.1.12

Protection requirements:

Protection Requirement / ETCS Level	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
L1	Low	Very High	Low	Middle	Not relevant
L2	Low	Very High	Low	Middle	Not relevant
L3	Low	Very High	Low	Middle	Not relevant

5.2.2 Out of Scope

All Onboard Elements which do not have to be considered for ERTMS.

5.2.2.1 Radio Applications Onboard

Described in Section 3.2.1

5.2.2.2 Driver

The Driver only got a non-technical connection to the DMI Device which don't count as conduit in the ETCS-Scope.

5.2.2.3 On-board recording device

The On-board recording device receives and saves juridical data provided by ETCS On-Board, STM and the TCMS.

5.2.2.4 Train (TCMS)

The Train Control Management System is responsible to control and connect safety relevant sensors and actors in the train.

5.2.2.5 STM/ National System Onboard

The Specific Transmission Module controls national ATP (Class B) systems.

6 Conduits

The Conduits give an insight in the different connections internal (inside the ERTMS scope) and external (connection between the ERTMS scope to external systems) which must be secured. The defined protection requirements are based on the highest classification of all connected zones. In the following subchapters all internal and external conduits are described in detail.

6.1 Internal

6.1.1 PKI Euroradio

Label:

Participants	Content/Purpose	Technology	Existing Security
• PKI Euroradio • RBC • Euroradio (On -Board)	Manage and distribute digital certificates between Euroradio instances which are used for the protection of Euroradio connections.	CMP OCSP	CMP (Secure Protocol) OCSP (Secure Protocol)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Middle	Middle	Not relevant

6.1.2 RBC - RBC

Label:

Participants	Content/Purpose	Technology	Existing Security
• RBC 1 • RBC 2	Handover Information between the RBC Areas	Euroradio Safety protocol according to SUBSET-098	None (currently) TLS in the future according to Subset 146

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Middle	Middle	Not relevant

6.1.3 Euroradio (RBC/RIU – Euroradio Onboard)

Label:

Participants	Content/Purpose	Technology	Existing Security
• RBC • RIU • Euroradio Onboard	Message exchange between on-board and trackside equipment	Euroradio Safety Protocol	None (currently) TLS in the future according to Subset 146

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	High	Middle	Not relevant

6.1.4 BTM / LTM

Label:

Participants	Content/Purpose	Technology	Existing Security
• Euroloop • Eurobalise • BTM • LTM	Handover interlocking and driver information from the trackside to the train	Eurobalise Telegrams via Magnetic Transponder Technology Euroloop Telegrams via Magnetic coupling or Direct Sequence Spread Spectrum (DSSS) modulation	None

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Low	Middle	Not relevant

6.1.5 Key Management

Label:

Participants	Content/Purpose	Technology	Existing Security
• RBC • KMC • RIU • Euroradio on ETC Onboard	Manage cryptographic keys to secure Euroradio communications between ERTMS/ECTS entities	Offline management via procedures and measures defined in SUBSET-038 Online management via procedures and measures defined in SUBSET-137	None for Offline Management TLS for Online Management

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Very High	Very High	High	Middle	Not relevant

6.1.6 Key Management PKI

Label:

Participants	Content/Purpose	Technology	Existing Security
• KMC • RBC • RIU • PKI	Manage and on-line distribution of cryptographic keys between KMCs and to the ERTMS/ETCS entities	TCP according to definition in SUBSET-037	TLS

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Middle	Middle	Not relevant

6.1.7 Voice connection

Label:

Participants	Content/Purpose	Technology	Existing Security
• Operator Voice • Driver Voice • Trackside User Voice	communication between operator, trackside User and driver voice trough network connections	GSM-R FRMCS	GSM-R: None (Security outdated) FRMCS: Not defined yet

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Low	Very High	Very High	Middle	Not relevant

6.1.8 Radio Applications

Label:

Participants	Content/Purpose	Technology	Existing Security
• Radio Applications Infrastructure • Radio Applications On-board	Information exchange between the onboard and Infrastructure Radio	Undefined radio connection	None (no security measures defined on European level)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Not relevant	Low	Not relevant	Not relevant

6.1.9 GSM-R / FRMCS

Described in Section 3.1.7

6.1.9.1 Mobile GSM-R / FRMCS

Label: (Figure 3)

Participants	Content/Purpose	Technology	Existing Security
• Mobile System • GSM-R/FRMCS	Mobile data transfer	GSM-R / FRMCS	GSM-R: None (Security outdated) FRMCS: Not defined yet

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement (Without Voice)	Not relevant	Not relevant	High	Middle	Not relevant
Protection Requirement (With Voice)	Not relevant	Very High	Very High	Middle	Not relevant

6.1.9.2 Internal GSM-R / FRMCS

Label: (Figure 3)

Participants	Content/Purpose	Technology	Existing Security
• GSM-R/FRMCS • Infrastructure System	Infrastructure-side transfer of mobile data	Depending on implementation / supplier	None (no security measures defined on European level)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement (Without Voice)	Not relevant	Not relevant	High	Middle	Not relevant
Protection Requirement (With Voice)	Not relevant	Very High	Very High	Middle	Not relevant

6.1.10 ATO-OB - ETCS On-Board

Label:

Participants	Content/Purpose	Technology	Existing Security
• ATO-OB • ETCS On-Board	Transfer of the status of the vehicle and all relevant information regarding ATO	UDP/TCP	TLS

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Low	Low	Low	Not relevant

6.1.11 ATO-OB - ATO-TS

Label:

Participants	Content/Purpose	Technology	Existing Security
• ATO-OB • ATO-TS	Transfer of data regarding journey profiles and additional information.	Euroradio Safety Protocol	TLS

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	High	High	Middle	Not relevant

6.2 External

6.2.1 Trackside ETCS Component Control

Label:

Participants	Content/Purpose	Technology	Existing Security
• Eurobalise • Euroloop • LEU/L1 Controller • Interlocking • RIU	Handover information from the Interlocking to the ETCS Trackside	Depending on implementation / supplier	None (no security measures defined on European level)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Low	Middle	Not relevant

6.2.2 RBC – Control Centre

Label:

Participants	Content/Purpose	Technology	Existing Security
• RBC • Control Centre	Information exchange containing e.g., temporary speed restrictions	Implementation specific	None (Implementation specific)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	High	Middle	Not relevant

6.2.3 RBC - Interlocking

Label:

Participants	Content/Purpose	Technology	Existing Security
• RBC • Interlocking	Information exchange containing e.g., train position, pre-set routes	Implementation specific or SCI-RBC (EULYNX)	None (Implementation specific or EULYNX Security)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	High	Middle	Not relevant

6.2.4 STM – ETCS Onboard

Label:

Participants	Content/Purpose	Technology	Existing Security
• STM • STM control function	Information exchange within the train parts in the ETCS On Board and the STM	Implementation specific or defined in OCORA	None (Implementation specific or OCORA Security)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Low	Middle	Not relevant

6.2.5 Train Control

Label:

Participants	Content/Purpose	Technology	Existing Security
• TIU • BIU • Train (TCMS)	Communication between onboard components	Implementation specific or defined in OCORA	None (Implementation specific or OCORA Security)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Not relevant	Very High	Low	Middle	Not relevant

6.2.6 On-board Juridical Recording

Label:

Participants	Content/Purpose	Technology	Existing Security
• Juridical data • On-board recording device	Provide protected juridical recording	Implementation specific or defined in OCORA	None (Implementation specific or OCORA Security)

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
Protection Requirement	Low	Middle	Middle	Middle	Not relevant

7 Attacker Type

7.1 Definition of Attackers

The following attacker types are used based on the definition of the Security Guideline [2].

7.1.1 A.Int.TerrorOrg

These organizations are made up of radicalized persons, who are drawn from political or religious motives (right-wing, left-wing, Islamism, Christianism, etc.) carry out targeted attacks and can have extensive possibilities if they have appropriate supporters. Attacks on rail transport may be carried out by terrorism, which is aimed at unsettling the population.

K4

R4

iSL4

7.1.2 A.Int.CriminalOrg

A criminal organization consists of persons who have made it their goal to achieve financial goals through illegal actions such as fraud or extortion. They range from small gangs to large, organized crime organisations (e.g., the mafia). The primary goal is to obtain money. Actions that are designed to simply causing damage are rare for this type of attacker.

K3

R3

iSL3

7.1.3 A.Int.GovOrg

These attackers are organized by the state and therefore have both, very high financial resources and enormous technical capabilities and skills. Governmental criminal organization can have different goals. They can either try to make profit using e.g., ransomware or get involved in cyber wars against other countries.

K4

R4

iSL4

7.1.4 A.Int.Comp

There are different Command, Control and Signaling (CCS) supplier companies that compete. It is therefore conceivable that an CCS system supplier could disrupt or manipulate the systems of the competitor, to damage the image of the competitor. It is not assumed that one railway operator attacks another one.

K4

R3

iSL4

7.1.5 A.Int.Activist

Activists are primarily politically motivated attackers who oppose political parties, who want to enforce their interests. The railway undertaker or the Rail transport can become the focus of activists, e.g., the transport of Castor containers case.

It is assumed that these are external persons or organizations who do not have detailed information on the internal structure of the railway. Availability attacks (achieving a blockade) are conceivable, causing security-critical situations (accidents) in which persons are injured do not correspond to their motivation.

K2

R3

iSL3

7.1.6 A.Int.Hacker

A hacker is generally a technically skilled computer user who has a large knowledge of current attack techniques. Black-hat hackers are using weaknesses identified in the reconnaissance phase to enrich themselves financially.

K3

R2

iSL3

7.1.7 A.Int.Internal

Internal attackers are persons who, as employees or suppliers, have internal knowledge and potentially have access to IT-systems and use them to carry out deliberately damaging actions, such as sabotage, betrayal of secrets or infidelity. Internal attackers must be treated in a different way, since the standard approach does not apply, since part of the security measures, following the IEC 62443 are not valid anymore, considering that access can be easily granted to internal attackers.

K4

R2

iSL3

7.2 Exclusion of Attackers

Within the ESCG the decision was made to not exclude any attacker types. Therefore, all attack types are considered during the risk assessment process. This decision was made during the initial attacker type definition workshop together with all members.
The main reason for not excluding any attacker type is the actual political situation in Europe and the threat landscape generated through military activities and a rising number of state-driven cyberattacks.

8 Separation of Safety and Security

In the following drawing the development paths for security and safety aspects are shown. The paths need to be separated to ensure that changes on the security relevant components or subsystems do not require a recertification of the safety relevant components.

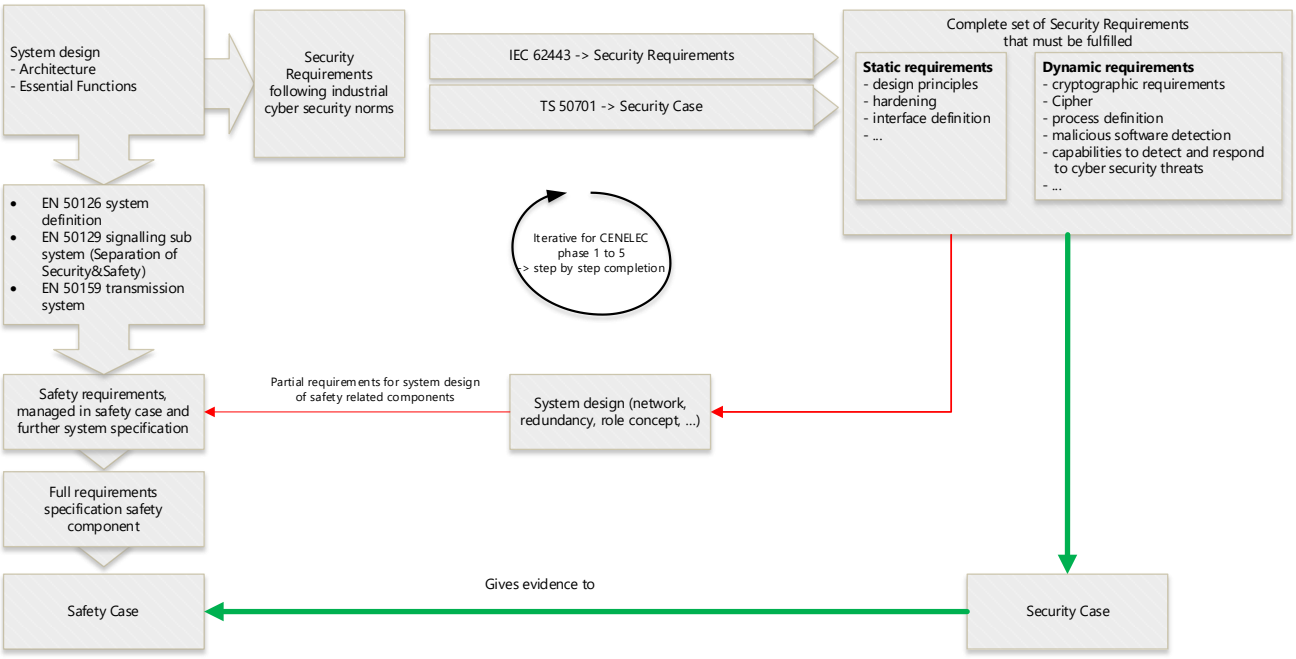

Figure 4: Safety and Security Case

Starting from the system as shown in Figure 4 design the path of safety and security is separated. Safety is addressed in the standards EN 50126, EN50129 and 50159 and results in requirements managed in the safety case and further system specification. During the same project phase, the security requirements are developed based on the standards IEC 62443 and its railway-specific implementation TS 50701. It results in static like safety requirements which will stay consistent over the lifetime of a product. Additionally dynamic requirements are developed, which might change during the lifetime of a product due to changing and evolving threats. All requirements are an input to the system design and thus result into partial requirements for safety. Furthermore, the security requirements and corresponding documents become a part of the security case which will give evidence to the safety case.

Security influences the design of components, its connections, and the whole system architecture. Hence it also affects aspects of systems categorized as safety-critical in the railway domain. As the treat landscape can change during the lifetime of a system, the security measures need to be regularly adapted to the current situation. However, the safety-critical system would lose its approval as a result, which results into high efforts for a new approval phase which is practically not possible in most of the cases. That's why it's necessary that the approval of the safety-critical system stays valid if security components are replaced or updated. This can be assured it is completely free from any possible negative influences on the safety-relevant component and its functionality. This absence of possible negative effects must be assured and can be implemented by separating security from safety. This

can be implemented on component level by physically separating the safety and security component and connecting it via a safe interface. An alternative to the physical separation is the implementation of virtual separation using e.g., safety-approved separation kernel. This way the safety and security applications can both run on the same hardware. Furthermore, the separation affects the communication as well, as safety-communication needs to be preserved, even if the security communication might fail. Thus, the separation of safety and security can be applied by implementing different communication layers for both purposes.

9 Handling of Existing and Future Standardisation

The ESCG is focusing on securing ERTMS in all aspects relevant to the EUG members. This includes the security of the current implementations as well as the design of future standards. Figure 5 shows the process used to accomplish this mission. The blue arrows indicate how the work of the ESCG will enrich future TSIs with cybersecurity. Furthermore, the ESCG will provide best practice and guideline documents to the IM and RU.

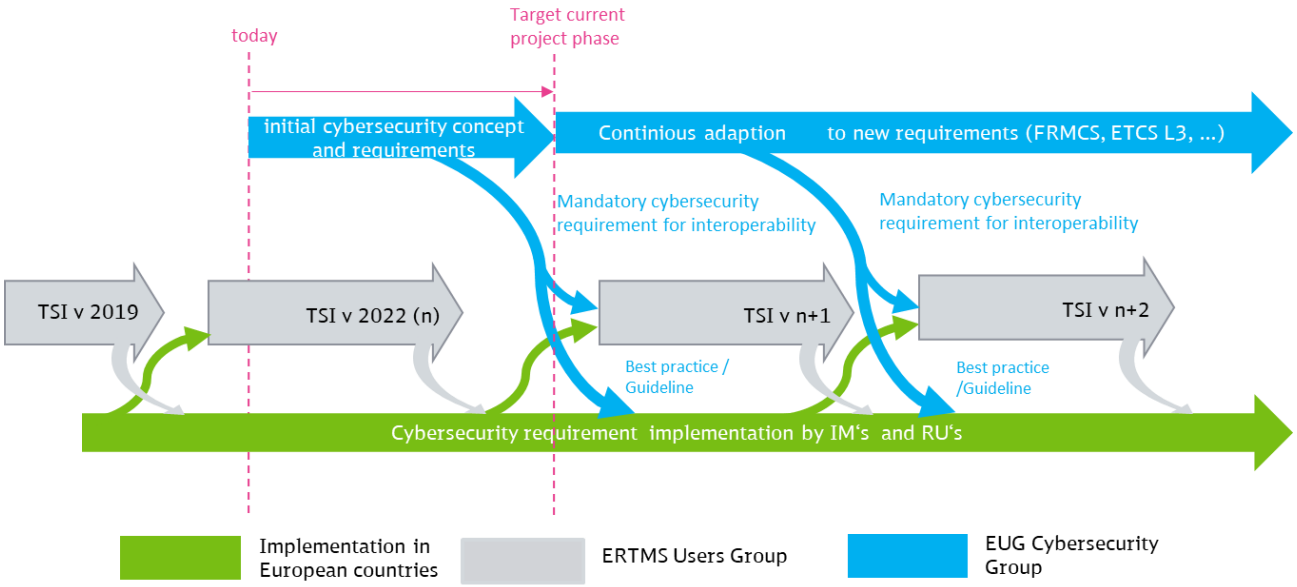

Figure 5: Continuous Process of ESCG

9.1 Synchronisation of Security Analysis

The risks of each zones differ depending on the specifications of the zone and the system architecture. Hence, the risk assessment might have different results if the current TSI or if a future release is analysed. The mitigating measures that can be defined also vary depending on the version taken into consideration. A combined analysis of both versions would therefore lead to inconsistent results or require extensive documentation and changes to ERORAT (v2).

The current release used in this document is defined in Chapter 4. By default, only existing implementations are assessed. If risks can be mitigated for new implementations of the current release, this is addressed in the comments of the risk assessment. If older sets of specifications contain relevant changes regarding the security analysis, it will be documented in the analysis of the current version.

The following approaches are defined to assure high quality of the security analysis results.

9.1.1 Document Management

If a system exists on both, the current and a future TSI release, a risk assessment will be created separately for every version.

The ERORAT document names are standardized as follows:

`ESCG_<Zone_Version/>_<Zone_Name/>_vX.XX.xlsx`

The Zone_Version is defined based on baseline and release:

`Zone_Version = SoSX`

As the assessment of future releases depends on current drafts of other organizations or groups, the draft version is added to the Assumptions in the ERORAT file.

9.1.2 Work procedure:

The risk assessment working group is defining the following informal process for zones, which are available in both, the current and a future release:

1. Application of the Security Guideline (and ERORAT) for the current release selected.
2. Summary of relevant changes included in current drafts
3. Modification of the work results for the current version based on the change summary to create the assessment for the future version.

9.2 Separation of Requirement Definition

According to the definition for synchronisation and separation of the security analysis in Chapter 9.1 the resulting requirements need to be split into two categories:

- Requirements for the current TSI
- Requirements for the future development of the next TSI

The specification will therefore contain a version number for every requirement or measure, which indicates for which version it can be applied. Furthermore, measures can be subdivided into requirement sections for different versions to improve clarity of the document.

9.3 Challenges and Limitations

The requirement definition based on detailed risk assessments for both, the current and future TSI, will result partly in different requirements.

9.3.1 Existing Implementation

Existing implementations are considered not to be updatable to a new SoS. Additionally changes to the systems must not have a negative influence on interoperability and existing approvals. Hence, the requirements selected must be feasible concerning these limitations. They must additionally fit the expected resources and implementation time which are available for existing implementations.

9.3.2 Future Standardisation

Future TSIs offer a broader scope for requirements compared to existing versions of the Subsets and drafts for TSI 2023. As the whole standard can be adapted to fulfil security needs, the set of eligible requirements is more extensive. Hence, vulnerabilities and architectural flaws which cannot be

addressed for existing implementations can be solved in future TSI release (after TSI 2023). These measures are defined as initial proposals.

End of Document