Für den Laborbereich zeichnet sich ab, dass die gezeigten Grundkonfigurationen über einfache Modifikationen für FRMCS und 5G verwendet werden können. Entsprechende Aktivitäten dazu laufen bereits, und auf europäischer Ebene existiert eine Reihe von spannenden Forschungsprojekten unter anderem zum dynamischen Kanalverhalten [6]. ■

AUTOR | AUTHOR

Jens Köcher
Laborleiter / *Laboratory Supervisor*
Funkwerk Systems GmbH
Anschrift / *Address*: Im Funkwerk 5, D-99625 Kölleda
E-Mail: jens.koecher@funkwerk.com

LITERATUR | LITERATURE

[1] The National Guidelines for Transport System Management (NGTSM), 2015
[2] ETCS – Inner city project business case; cost benefit analysis summary, May 2016; https://www.statedevelopment.qld.gov.au/__data/assets/pdf_file/0023/54509/ETCS-Inner-City-Cost-Benefit-Analysis-Summary_web.pdf
[3] Advanced Train Management System (ATMS) - ARTC; https://www.artc.com.au/projects/atms/
[4] ETSI TS 102 933-2 V2.1.1 (2015-06); Railway Telecommunications (RT); GSM-R improved receiver parameters; Part 2: Radio conformance testing
[5] Akustische-Oberflächenwellen-Filter – Wikipedia; https://de.wikipedia.org/wiki/Akustische-Oberfl%C3%A4chenwellen-Filter
[6] EMMTES Projekt; EMMTES | Technische Universität Ilmenau (tu-ilmenau.de); https://www.tu-ilmenau.de/universitaet/fakultaeten/fakultaet-elektrotechnik-und-informationstechnik/profil/institute-und-fachgebiete/fachgebiet-elektronische-messtechnik-und-signalverarbeitung/projekte/emmtes

Cyber-Security-Maßnahmen für ERTMS aus Sicht der Bahnbetreiber

Cyber security measures for ERTMS from the rail operators' perspective

Richard Poschinger | Christof Jungo | Ernst Kleine | Martin Espenschied

Durch eine steigende digitale Gefährdungslage rückt die Cyber Security im Bahnbereich verstärkt in den Vordergrund. Die Anzahl der mit dem europäischen digitalen Zugbeeinflussungssystem ETCS betriebenen Strecken steigt. Der damit einhergehende Bedarf zur securityspezifischen Absicherung von ETCS resultierte innerhalb der ERTMS Users Group (EUG) in der Gründung der ERTMS Security Core Group (ESCG). Die Arbeit der ESCG resultierte in umfangreichen, praktisch anwendbaren Security-Maßnahmen und Vorschlägen für die zukünftige Entwicklung von ETCS.

1 Einleitung

Bei der Etablierung der verbindlichen europäischen Interoperabilitätsspezifikationen (TSI CCS) für ERTMS (European Railway Traffic Management System) wurde das Thema Security bisher nicht adressiert. Erst in der erst kürzlich vereinbarten TSI CCS 2023 wurde dieses Thema aufgenommen, allerdings nur auf generischer Ebene.

1.1 Gründung und Aufbau der ESCG

Die Entwicklung und Umsetzung des ERTMS ist eine der Maßnahmen zur Schaffung eines transeuropäischen Eisenbahnnetzes. Die EUG (www.ertms.be) bündelt das Wissen und die Erfahrung ihrer Mitglieder, um die Einführung des ERTMS zu unterstützen und sicherzustellen, dass es sich um ein sicheres, zuverlässiges und in-

The growing digital threat means that cyber security is assuming an increasingly prominent role in the railway sector. More lines are being operated with ETCS, the European digital train control system. The consequent need to provide ETCS with specific security protection was the impetus for establishing the ERTMS Security Core Group (ESCG) within the ERTMS Users Group (EUG). The work undertaken by the ESCG has resulted in comprehensive security measures with practical applications and proposals for the future development of ETCS.

1 Introduction

Security was not specifically addressed when the mandatory European interoperability specifications (TSI CCS) for ERTMS (the European Railway Traffic Management System) were drawn up. This subject has only been taken up in the recently agreed TSI CCS 2023 and even then only at a generic level.

1.1 The establishment and structure of the ESCG

The development and implementation of ERTMS are some of the measures behind the creation of a trans-European rail network. The EUG (www.ertms.be) pools the knowledge and experience of its members in order to support the introduction of ERTMS and ensure that it is a safe, reliable and interoper-

teroperables System zu angemessenen Kosten handelt. Innerhalb der EUG wurde Handlungsbedarf bezüglich der Security von ERTMS identifiziert. Dies ist sowohl für die bestehenden ERTMS-Systeme, aktuelle Ausschreibungen als auch für die zukünftigen Standardversionen relevant. Aus diesem Grund wurde die ESCG gegründet, um Security-Maßnahmen für die aktuelle Systemlandschaft und zukünftige ERTMS-Einführungen praktisch zu bewerten und vorzuschlagen. Die ESCG besteht aus Security-Experten der EUG, die sowohl über Wissen bezüglich ERTMS als auch über Security-Expertise verfügen.

1.2 Ziele der ESCG

Die ESCG setzt sich mit einer umfassenden ERTMS Security auseinander, die über das hinausgeht, was in den aktuellen TSI CCS-Spezifikationen und zugehörigen Subsets vorgeschrieben ist. Der Schwerpunkt (Bild 1) liegt sowohl auf ERTMS-Security-Richtlinien als auch auf der Mitarbeit an der Standardisierung von ERTMS Security (in zukünftigen TSI-Versionen), welche in den EU-Rail System Pillar einfließt.
Die ESCG zielt darauf ab, eine gemeinsame Austauschplattform hinsichtlich Security für ihre Mitglieder und andere Partner im Eisenbahnsektor bereitzustellen. Hierbei arbeitet sie mit anderen Initiativen wie OCORA und EULYNX zusammen, deren Ergebnisse ebenfalls in den EU-Rail System Pillar einfließen.

2 Prozesse und Analysen

Die ESCG hat sich zum Ziel gesetzt, durchgängige und nachvollziehbare Security-Anforderungen zu definieren, die europäische Bahnbetreiber dann als Grundlage für ihre bereits eingesetzten und zukünftigen Systeme anwenden können. Als Basis dient der Standard IEC 62443 und die TS 50701. Es wird eine Methodik definiert und eine Reihe von Analysen durchgeführt, welche in den nachstehenden Kapiteln erläutert werden.

2.1 Scope

Das betrachtete System (System under Consideration – SuC) besteht aus allen Systemen, die für den Eisenbahnbetrieb aus Sicht von ERTMS relevant sind. Bild 2 zeigt die für die ESCG-Analysen relevanten Systeme. Die fahrzeugseitigen und streckenseitigen

able system at a reasonable cost. The EUG has identified a need for action to ensure the security of the ERTMS. This is relevant for both the existing ERTMS systems and the ongoing tendering procedures, as well as for any future standard versions. Consequently, the ESCG was established in order to undertake a practical assessment and propose security measures both for existing systems and for those that might be introduced into ERTMS in the future. The ESCG is made up of EUG security experts with both ERTMS knowledge and expertise in the field of security.

1.2 Aims of the ESCG

The ESCG is primarily concerned with comprehensive ERTMS security beyond what is prescribed in the current TSI CCS specifications and their associated subsets. Its focus (fig. 1) is both on the ERTMS security guidelines and on contributing to the standardisation of ERTMS security (in future TSI versions), which will feed into the EU-Rail System Pillar.
The ESCG aims to provide a common security exchange platform both for its own members and for other partners in the railway sector. In doing so, it cooperates with other initiatives such as OCORA and EULYNX, the results of which are also fed into the EU-Rail System Pillar.

2 Processes and analyses

The ESCG has set itself the goal of defining consistent and comprehensible security requirements that European railway operators can use as the basis for their existing and future systems. The IEC 62443 standard and the TS 50701 form the baseline. A methodology will be defined and a series of analyses, which are explained in the following sections, will be implemented.

2.1 Scope

The System under Consideration (SuC) consists of all those systems that from the ERTMS point of view are of relevance to railway operations. Fig. 2 shows those systems that are of relevance to the ESCG analyses. The on-board and trackside sys-

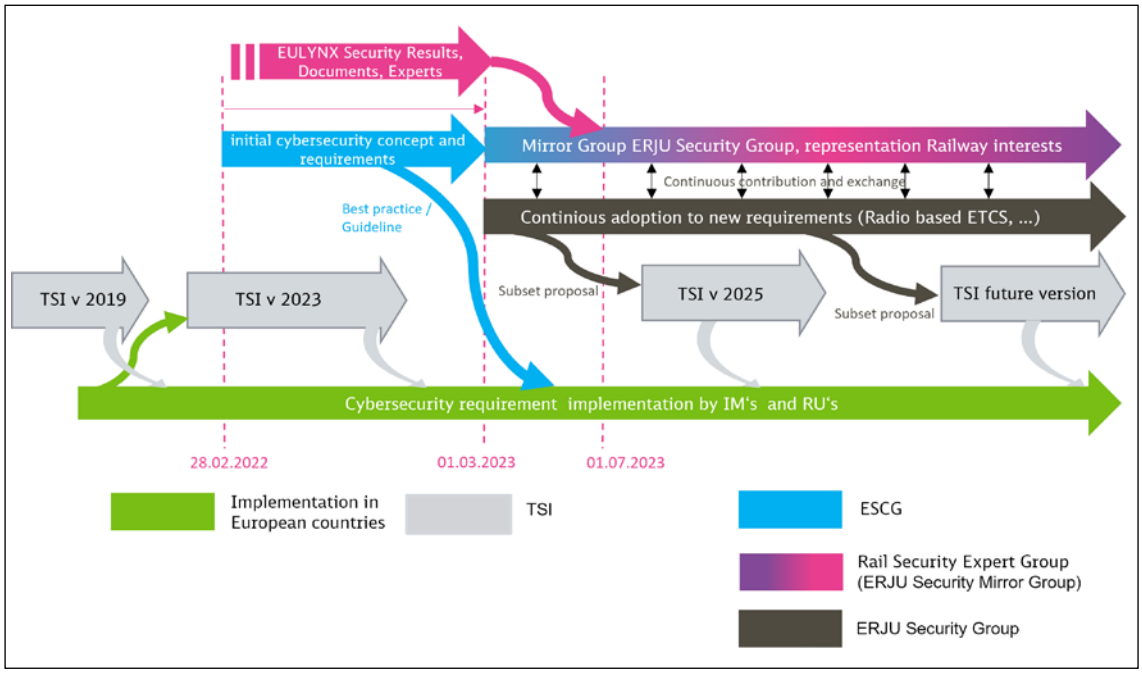

Bild 1: Prozess der Arbeit der ESCG
Fig. 1: The ESCG work process Quelle / *Source*: [1]

Systeme (Infrastruktur) sind nach dem für ihre Normung zuständigen Projekt gegliedert. Zusätzlich werden die Ergebnisse des EULYNX Security Clusters und anderer Standardisierungsgruppen berücksichtigt.

2.2 Bestandssysteme und zukünftige Standardisierung

Die Arbeit der ESCG orientiert sich an den Herausforderungen der Mitglieder der EUG in Bezug auf die Security der eingesetzten ERTMS-Systeme. Somit wird nicht nur an der Weiterentwicklung der Security von ETCS und dem bahnspezifischen Mobilfunk gearbeitet, sondern auch auf aktuell im Bestand oder in Planung befindliche Systeme eingegangen. Auf Basis von detaillierten Risikobetrachtungen, wird, wie in Bild 1 zu sehen, ein Satz an Maßnahmen in Form von Best Practices erstellt.

Basis für diese Anforderungen ist eine Risikoanalyse, welche initial je Zone durchgeführt wird. Diese bezieht sich auf das aktuell verfügbare Set of Specification (SoS) 3. Innerhalb der Analyse wird zwischen risikomindernden Maßnahmen unterschieden, welche bei bereits im Betrieb befindlichen Systemen im Sinne einer Nachrüstung anwendbar sind, und Maßnahmen, welche nur bei einer Neuausschreibung nach SoS 3 umsetzbar sind.

Für die zukünftigen Versionen der ETCS Subsets wurde auf Basis der bekannten Änderungen im Vergleich zu SoS 3 eine weitere Analyse durchgeführt. Somit konnte eine einheitliche und konsistente Risikosicht über die verschiedenen technischen Stände erzeugt werden. Die genannte Trennung wird in den resultierenden Maßnahmendokumenten fortgesetzt, um eine gut strukturierte Grundlage für Ausschreibungsdokumente zu generieren.

2.3 Arbeit auf Basis der aktualisierten Guideline

Die Analysen der ESCG wurden basierend auf der erstmals im Stellwerksstandard EULYNX angewendeten Security Guideline [2] durchgeführt. Diese legt eine einheitliche Anwendung der IEC 62443 und

tems (infrastructure) are grouped according to the project responsible for their standardisation. In addition, the results of the EULYNX Security Cluster and other standardisation groups will also be taken into account.

2.2 Existing systems and future standardisation

The work of the ESCG is oriented towards the challenges faced by the members of the EUG in ensuring that the ERTMS systems already in use are secure. Thus, its work not only involves the further development of ETCS security and security for the railway-specific mobile radio, but is also concerned with systems that are either currently in existence or being planned. A set of measures in the form of best practices is currently being created based on detailed risk assessments, as can be seen in fig. 1.

These requirements are based on a risk analysis that is initially carried out for each zone. The risk analysis relates to the currently available Set of Specifications (SoS) 3. The analysis distinguishes between risk-reducing measures that can be applied to systems already in operation in the form of a retrofit and measures that can only be implemented following a fresh tendering procedure in accordance with SoS 3.

A further analysis was carried out for future versions of the ETCS subsets based on known changes compared to SoS 3. In this way, it was possible to generate a uniform and consistent overview of the risk across the different technical statuses. The distinction mentioned above will be continued in the resulting documentation setting out the measures to be taken, so as to generate a well-structured basis for the production of tender documents.

2.3 Work based on the updated guideline

The ESCG analyses have been carried out on the basis of the Security Guideline [2] which was first applied in the EULYNX interlocking standard. This guideline specifies that IEC 62443

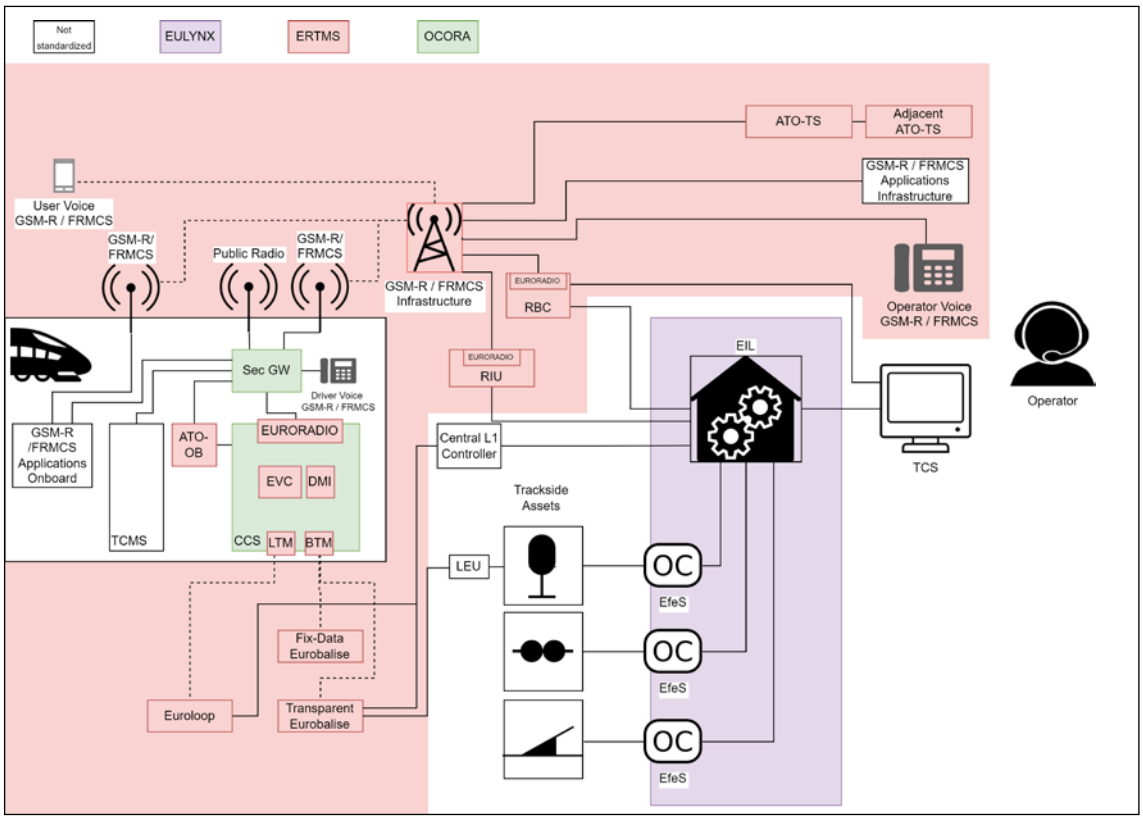

Bild 2: ERTMS System under Consideration
Fig. 2: The ERTMS System under Consideration
Quelle / *Source*: [1]

TS 50701 innerhalb der europäischen Standardisierungsprojekte EULYNX, EUG, RCA und OCORA fest. Der Prozess startet mit der Definition des SuC und erstreckt sich über die Festlegung von Gefährdungen und dem Security Level bis hin zur Risikoanalyse. Die Festlegung des Security Levels und die Risikoanalyse wird unterstützt durch ein Excel-Tool (ERORAT), welches auch die vollständige Umsetzung der System Requirements gemäß IEC 62443-3-3 sicherstellt. Auf Basis der Erfahrungen in der Erstellung der EULYNX-Dokumente wurde das Vorgehen in Version 2 der Guideline und ERORAT überarbeitet. Hierdurch konnten die automatisch erzeugte Nachvollziehbarkeit von Anforderungszuweisungen sowie die Dokumentation stark verbessert werden. Außerdem wurde durch detailliertere Beschreibungen der Zonierung die Grundlage für ein einheitliches Verständnis geschaffen. ERORAT wurde um eine automatisch generierte und aktualisierte Heatmap erweitert, welche die Zuordnung von System Requirements wesentlich erleichtert. Auf Basis der Ergebnisse und Erfahrungen der ESCG werden beide Dokumente weiter verbessert. Eine Anpassung an die zukünftige IEC 63452 (als Nachfolger der TS 50701) ist geplant.

3 Ergebnisdokumente

Die detaillierte und normengerechte Durchführung von Analysen und Erarbeitung von Maßnahmen wird in den folgenden, durch die ESCG veröffentlichten, Dokumente beschrieben.

3.1 Concept

Das Konzept [1] legt die Security-Anforderungen auf übergeordneter Ebene für die gesamte ERTMS-Architektur fest, einschließlich der Kommunikationsschnittstellen und der Systemkomponenten sowie der erforderlichen Prozesse. Es umfasst den gesamten Security-Lebenszyklus von der Systemdefinition bis zur Außerbetriebnahme des Systems. Zur Analyse der Risiken in der ERTMS-Architektur und zur Festlegung von Maßnahmen zur Risikominderung wird der gemeinsame Security-Leitfaden von EUG, RCA, OCORA und EULYNX [2] verwendet.
Die in der Leitlinie definierte Methode basiert auf der IEC 62443 und der damit verbundenen Erweiterung um bahnspezifische Aspekte in der TS 50701. Die bewertete Security-Architektur für bestehende Implementierungen basiert auf den ERA ERTMS-Spezifikationen (SoS 3). Als Grundlage für die Bildung von Zonen und Festlegung des Security Levels wurde die Schutzbedarfsbewertung für die Kategorien Vertraulichkeit, Integriät, Verfügbarkeit, Nichtabstreitbarkeit und Authentizität durchgeführt und im Konzept festgehalten. Anhand der Angreifertypen, welche in [2] definiert sind, wird der maximale Security Level (SL Max) für die einzelnen Zonen definiert.

3.2 Threat & Risk

Die durch die ESCG durchgeführte Risikoanalyse bildet die Basis für die Erstellung von risikomitigierenden Maßnahmen. Sie wurde auf Basis der bereits im Konzept eingeführten Zonierung und Schutzbedarfsfeststellung erstellt. Die Risikoanalyse (erstellt in ERORAT) steht den Security-Experten der Mitgliederorganisationen der EUG zur Verfügung. Eine Übersicht über die Ergebnisse der Risikoanalyse und deren Grundlagen bietet das veröffentlichte Dokument „Threat and Risk Analysis" [3]. Hierbei werden die erfassten und analysierten Zonen aufgeführt. Zusätzlich befinden sich hier die resultierenden Security-Level-Vektoren, welche die Basis für die Auswahl der System Requirements (SR) bilden. Die Vollständigkeitsprüfung der Umsetzung dieser SR beschreibt detailliert die Anwendung einzelner SR in den Maßnahmendokumenten der ESCG.

and TS 50701 are to be applied uniformly within the European EULYNX, EUG, RCA and OCORA standardisation projects. The process starts with defining the SuC, continues by specifying the risks and the security level and culminates with the risk analysis. The definition of the security level, as well as the risk analysis, is supported by an Excel tool (ERORAT), which also ensures complete implementation of the system requirements in accordance with IEC 62443-3-3.
The procedure set out in Version 2 of the Guideline and ERORAT has been revised based on experience gained when drawing up the EULYNX documents. This has greatly improved the automatically generated traceability of how requirements are assigned as well as the quality of the documentation itself. In addition, the more detailed zoning descriptions have created a basis for a uniform understanding. ERORAT has been expanded to include an automatically generated and updated heat map, which makes assigning system requirements significantly easier. Both documents will be subject to further improvements based on the lessons learned and experience gained by the ESCG. There are plans to adapt them to match the future IEC 63452 (as the successor to TS 50701).

3 Documenting the results

The detailed and standard-compliant conduct of the analyses and the drawing up of measures to be implemented are described in the following documents published by the ESCG.

3.1 Concept

The concept [1] specifies the higher level security requirements for the entire ERTMS architecture, including the communication interfaces and the system components, as well as the necessary processes. It covers the entire security lifecycle from system definition to system decommissioning. The joint EUG, RCA, OCORA and EULYNX Security Guideline [2] is used in order to analyse the risks in the ERTMS architecture and define any risk mitigation measures.
The method defined in the guideline is based on IEC 62443 and on the more detailed guidance covering specific railway-related aspects set out in TS 50701. The security architecture, which has been evaluated in the existing implementations, is based on the ERA ERTMS specifications (SoS 3). An assessment was undertaken of the extent to which confidentiality, integrity, availability, non-repudiation and authenticity were in need of protection as the basis for forming the zones and defining the security level and this was recorded in the concept. The potential types of attack, as defined in [2], were taken as the basis for defining the maximum security levels (SL Max) for the individual zones.

3.2 Threat & risk

The risk analysis carried out by the ESCG forms the basis for drawing up the risk mitigation measures. The analysis was based on the zoning and required protection assessment already introduced in the concept. The risk analysis (created in ERORAT) is available for use by the security experts employed by EUG member organisations. A summary of the risk analysis results and its foundation is provided in the already published "Threat and Risk Analysis" document [3]. It lists the recorded and analysed zones. In addition, it also contains the security level vectors that form the basis for selecting the system requirements (SR). The completeness check for implementing these SRs describes in detail the application of the individual SR in the ESCG documentation on the measures to be undertaken.

3.3 Security-Maßnahmen

Die Security-Maßnahmen wurden in einem Dokument für Bestandsysteme [4] und einem für die zukünftigen Versionen [5] der ETCS Subsets festgehalten. Als übergeordnete Kapitel werden die Kategorien Identification and Authentication, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events und Resource Availability der IEC 62443 herangezogen. Zusätzlich wurden die Kategorien Physical Protection und Organisational Security and Processes aufgenommen. Diese Kategorien sind nicht in der IEC 62443 abgebildet, werden jedoch als Voraussetzung in der TS 50701 genannt. Für jede Maßnahme, welche einer Kategorie zugewiesen wird, ist festgehalten, welche Zonen betroffen sind, welche Bedrohungen adressiert werden und welche Security Requirements aus der IEC 62443 referenziert wurden. Diese Vorgehensweise liefert dem Bahnbetreiber die notwendige Transparenz, um die Resultate nachzuvollziehen. Zudem kann er feststellen, welche Maßnahmen die meisten Risiken adressieren. Dem Bahnbetreiber steht es frei, die Maßnahmen seinen Bedürfnissen anzupassen. Es besteht keine Pflicht, die erarbeiteten Resultate anzuwenden.

4 Erkenntnisse

Durch die Maßnahmendefinitionen der ESCG wird ein umfassender Schutz innerhalb der ERTMS-Umgebung erzeugt. Hierbei wurden auch Vorschläge in den folgenden Themengebieten erarbeitet.

4.1 Zentrale Services

Aus Sicht der Security wird das funktionale Zusammenspiel der Komponenten untereinander betrachtet und gesichert. Um beispielsweise eine verschlüsselte Kommunikation zwischen mehreren Komponenten zu gewährleisten und über längere Zeit sicher zu betreiben, ist nicht nur die Fähigkeit der Komponenten, Verschlüsselung anzubieten, relevant, sondern auch deren Konfiguration und Wartung. Im Rahmen der ESCG werden, sowohl für die zentralen Services wie auch für die Schnittstellen der anzuschließenden Komponenten, Maßnahmen definiert.

4.1.1 Security

Zu den Security Services gehören eine Public Key Infrastructure (PKI), das Identity und Access Management (IAM) und das Security Monitoring und Logging System. Alle diese Security Services haben keinen direkten Einfluss auf die Funktionsweise des Gesamtsystems, sondern dienen der Aufrechterhaltung der Security. Dementsprechend wurden Maßnahmen definiert, um die Integrität der Services zu gewährleisten sowie deren Schnittstellen, als Weiterführung der EULYNX-Standardisierung, zu vereinheitlichen.

4.1.2 Maintenance

Das zentrale Maintenance und Data Management (MDM) ist für die Sicherung und Wiederherstellung der relevanten Daten (Basissoftware und Konfiguration) sämtlicher Komponenten zuständig. Die Komponente selbst benötigt keine Back-up-Funktionalität, da sie alle relevanten Daten aus der zentralen Verwaltung abruft. Im Rahmen der Arbeiten wurden die Maßnahmen für die Wartungsschnittstelle (Remote-Zugang) spezifiziert. Die ESCG plant, auf Basis der EULYNX-Schnittstellen und gemeinsam mit EU-Rail, ein zentralisiertes MDM im Eisenbahnbereich zu spezifizieren.

4.2 Euroradio over TLS

Die gestiegenen Anforderungen an die Security konnten durch die in Safety-Protokollen eingebetteten und meist veralteten Mechanismen nicht mehr erfüllt werden. Aus diesem Grund werden in

3.3 Security measures

The security measures have been set out in one document for the existing systems [4] and one for any future versions [5] of the ETCS subsets. The IEC 62443 categories covering identification and authentication, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability were added as higher-level sections. In addition, the categories of physical protection, organisational security and processes were also included. These categories are not included in IEC 62443, but are mentioned as a prerequisite in TS 50701. The affected zones, the addressed threats and the IEC 62443 security requirements are recorded for each measure assigned to a category. This approach provides the railway operator with the necessary transparency to understand the results. Railway operators are also able to identify which measures address the most risks and are at liberty to adapt the measures to their own needs. They are under no obligation to apply the obtained results.

4 Findings

The measures defined by the ESCG create comprehensive protection within the ERTMS environment. Suggestions covering the areas set out below have also been developed.

4.1 Central services

The functional interaction of each component has been considered from the security perspective. For example, both the ability of the components to offer the relevant encryption and their configuration and maintenance are relevant in order to ensure encrypted communications between several components and secure operations over longer periods of time. Measures have been defined for both the central services, as well as the interfaces between components that they are to be linked to as part of the work of the ESCG.

4.1.1 Security

The security services include a public key infrastructure (PKI), identity and access management (IAM) and the security monitoring and logging system. None of these security services has any direct influence on the functioning of the overall system, but they assist in maintaining its security. Accordingly, measures have been defined so as to ensure the integrity of the services as well as to standardise their interfaces in pursuit of EULYNX standardisation.

4.1.2 Maintenance

The central maintenance and data management (MDM) system is responsible for backing up and restoring the relevant data (basic software and configuration) held by every component. The component itself does not need any backup functionality, since it retrieves the relevant data from the central administration. The necessary measures for the maintenance interface (remote access) were specified as part of the work. The ESCG plans to produce a specification for a centralised MDM in the railway sector based on the EULYNX interfaces and in conjunction with EU-Rail.

4.2 Euroradio over TLS

The mostly outdated mechanisms embedded in the safety protocols were no longer capable of satisfying the enhanced security requirements. This is why existing protocols are being replaced or supplemented with state-of-the-art security protocols

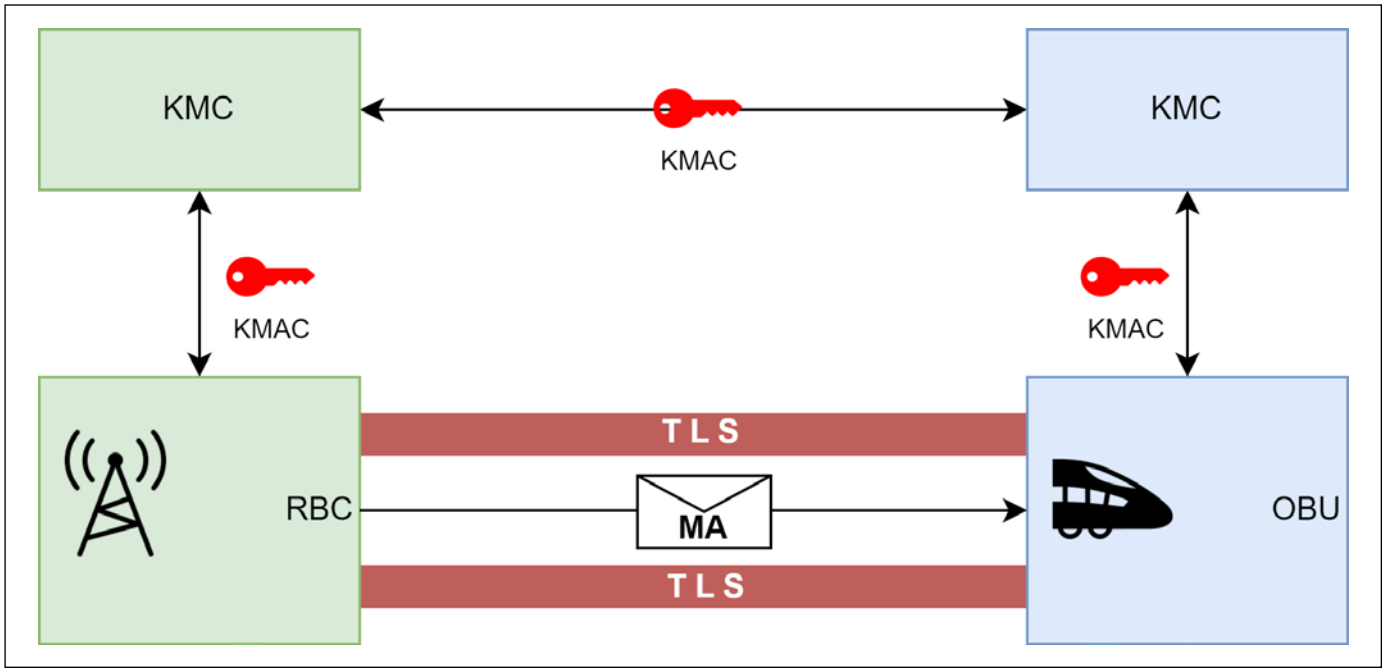

Bild 3: Euroradio over TLS
Fig. 3: Euroradio over TLS

zahlreichen Bereichen der Bahnindustrie, wie z. B. EULYNX, bestehende Protokolle durch Security-Protokolle nach aktuellem Stand der Technik ersetzt oder um sie ergänzt. Diesen Weg hat inzwischen auch die ERTMS-Umgebung erreicht. Erstmalig wurde Transport Layer Security (TLS) in ETCS durch Subset 137 [6] für die Übertragung von Schlüsseln innerhalb des Key Management eingeführt. Dieser Weg wird durch Subset 146 [7], welcher aktuell als Entwurf vorliegt, fortgeführt. In diesem Dokument werden die Anforderungen an TLS zukünftig gebündelt. Zusätzlich wird TLS auch für die Automatic-Train-Protection-(ATP)- Verbindungen verwendet. Somit wird, wie in Bild 3 zu sehen, der Euroradio Datenverkehr mittels TLS abgesichert und authentifiziert.

4.2.1 Geänderte Schutzbedarfe der ETCS-Schlüssel

In bisherigen ERTMS-Systemen übernimmt das Key Management Centre (KMC) eine essenzielle Funktionalität hinsichtlich der Erreichung von Security-Anforderungen. Auch wenn die technischen Maßnahmen zum Schutz der Euroradio-Verbindung veraltet und somit leicht angreifbar sind, ist die Absicherung mittels der durch das KMC verwalteten Schlüssel (KMAC) die einzige Möglichkeit einer Verhinderung von Manipulationen von beispielsweise Movement Authorities. Somit trägt das KMC wesentlich dazu bei, Kollisionen und Unfälle zu verhindern. Eine Absicherung nur über GSM-R-Mechanismen kann aufgrund der schon vor vielen Jahren als veraltet angesehenen und unsicheren Algorithmen nicht angenommen werden [8]. Der Schutzbedarf für das KMC und seine Übertragungsverfahren wurde daher bezüglich Integrität und Vertraulichkeit als „sehr hoch" angenommen. Auch der Schutzbedarf der Verfügbarkeit wurde als „hoch" angenommen, da der operative Betrieb hierdurch gestört werden kann.
Sobald die Absicherung von einer Euroradio-Verbindung, wie in Subset 146 spezifiziert, über eine aktuelle Version von TLS abgesichert wird, ändert sich diese Einschätzung. Die durch das KMC verwalteten Schlüssel tragen somit keine Verantwortung mehr für die Security des Gesamtsystems. Hierdurch wird der Schutzbedarf der Schlüssel gesenkt. Somit kann eine Manipulation von KMAC nur noch in eine gestörte Verbindung zwischen Radio Block Centre (RBC) und Zug re-

in many areas of the railway industry, such as EULYNX. The ERTMS environment has now reached this stage too. Transport Layer Security (TLS) was introduced to ETCS for the first time with Subset 137 [6] for transmitting keys within the Key Management System. This approach has been continued by Subset 146 [7], which is currently available as a draft. In the future, the TLS requirements will all be contained in this document. In addition, TLS will also be used for Automatic Train Protection (ATP) communications. Thus, as can be seen in fig. 3, Euroradio data traffic will be secured and authenticated through TLS.

4.2.1 Modified protection requirements for ETCS Keys

In the present ERTMS systems, the Key Management Centre (KMC) assumes an essential functionality when it comes to satisfying the security requirements. Even though the technical measures for protecting the Euroradio link may be outdated and therefore vulnerable, the only way, for example, to prevent movement authorities from being tampered with is to minimise the risk by using the keys managed by the KMC (KMAC). In this way, the KMC makes a significant contribution to preventing any collisions and accidents. It cannot be assumed that the risks can be minimised by using GSM-R mechanisms alone, because their algorithms have been regarded as outdated and unsafe for many years [8]. Consequently, the need to protect the KMC and its transmission procedures was rated as "very high" with regard to integrity and confidentiality. The need to protect availability was also rated as "high" since it is possible that railway operations could be disrupted.
This assessment will change as soon as the risk to the Euroradio link, as specified in Subset 146, is minimised through the use of a state-of-the art version of TLS. The keys managed by the KMC will thus no longer bear any responsibility for the security of the entire system. This will reduce the requirement to protect the keys. Consequently, any tampering with the KMACs will only result in disruption to the communications between the Radio Block Centre (RBC) and the train. Therefore, any re-

sultieren. Verbleibende Aspekte des Schutzbedarfs beziehen sich somit nur noch auf die betriebliche Verfügbarkeit der Euroradio-Verbindung. Im Falle von Strecken ohne andere Zugsicherungssysteme und Signale wird daher eine starke Verminderung der Streckenkapazität bis hin zum Ausfall von Zügen angenommen.

4.2.2 PKI-Strukturen in föderierten Systemen

Zum Aufbau der in Subset 137 für Online Key Management spezifizierten und mittels Subset 146 auf weitere Verbindung ausgeweiteten Absicherung über TLS sind Zertifikate auf allen beteiligten Entitäten erforderlich. Diese Zertifikate werden durch eine PKI ausgestellt, welche auch die Überprüfung der Validität der Zertifikate ermöglicht. Das bisherige Online Key Management erfordert hierbei eine interne PKI für den Austausch zwischen KMC und den zugehörigen Entitäten. Für den Austausch zwischen KMC unterschiedlicher Betreiber sind die erforderlichen Zertifikate organisationsübergreifend zu verwalten. Dies kann initial durch einen manuellen Austausch oder eine zusätzliche PKI nur für den inter-KMC Datenverkehr erfolgen.

Mit Blick auf die Verwendung von Zertifikaten für die Euroradio-Verbindung werden diese Verfahren verwaltungstechnisch jedoch als zu komplex angesehen. Daher ist eine Verknüpfung der betreiberspezifischen PKI erforderlich. Eine komplette Zentralisierung der PKI erscheint aufgrund nationaler Anforderungen an die Eigenständigkeit der Betreiber unwahrscheinlich resp. nicht zielführend. Zwei Lösungsmöglichkeiten für das technische Prozedere sind in den Abbildungen zu finden. Bild 4 zeigt die Verknüpfung zweier getrennter PKI mittels einer zentralen Root PKI. Dies mindert den administrativen Aufwand drastisch, sorgt jedoch für eine verstärkte Abhängigkeit zu der zentralen PKI-Instanz. Aus diesem Grund wird innerhalb der ESCG auch der Einsatz eines Bridge-Zertifikats verfolgt. Dieses, in Bild 5 gezeigte, Verfahren mindert die zentralen Abhängigkeiten und stellt durch gegenseitige Signierung eines Bridge-Zertifikats eine feste Vertrauensverknüpfung zwischen den beiden betreiberseitigen PKI her. Die ESCG evaluiert aktuell die unterschiedlichen Varianten im tieferen Detail und plant einen Proof of Concept zur technischen und operativen Analyse. Hierdurch sollen auch die Grundlagen für die Entscheidung bzgl. des möglichen Betriebs der zentralen Systeme geschaffen werden.

maining elements of the requirement to provide protection will only relate to the operational availability of the Euroradio link. With regard to lines that do not possess any alternative train control systems and signals, it is assumed that there will be a severe reduction in line capacity, possibly extending to the cancellation of train services.

4.2.2 PKI structures in federated systems

Certificates are required for all the involved entities in order to establish risk minimisation via TLS as specified in Subset 137 for online key management and as extended to further communication via Subset 146. These certificates will be issued by a PKI, which will also allow the validity of the certificates to be checked. The present online key management system needs an internal PKI for the exchange between the KMC and its associated entities. Switching between the KMCs of different operators requires the certificates to be managed across all the organisations. This can initially be achieved either by means of a manual switchover or by means of an additional PKI for inter-KMC data traffic only.

However, these procedures are considered too complex from an administrative point of view with regard to the use of certificates for the Euroradio link. It is therefore essential to link the PKIs that are specific to each operator. Complete PKI centralisation would appear unlikely and would not achieve the desired outcome because of each country's requirements for its rail operators to retain some autonomy. Two solutions for a possible technical procedure can be seen in the illustrations. Fig. 4 shows two separate PKIs linked by a central root PKI. This drastically reduces the administrative effort, but increases the dependency on the central PKI entity. That is why the ESCG is pursuing the use of a bridge certificate. This procedure, illustrated in fig. 5, reduces the dependence on the central entity and establishes a firm trust-based link between two operators' PKIs by means of the mutual signing of a bridge certificate. The ESCG is currently evaluating the different variants in more detail and intends to produce a Proof of Concept for technical and operations analysis. This should also provide the basis for a decision regarding the possible operation of central systems.

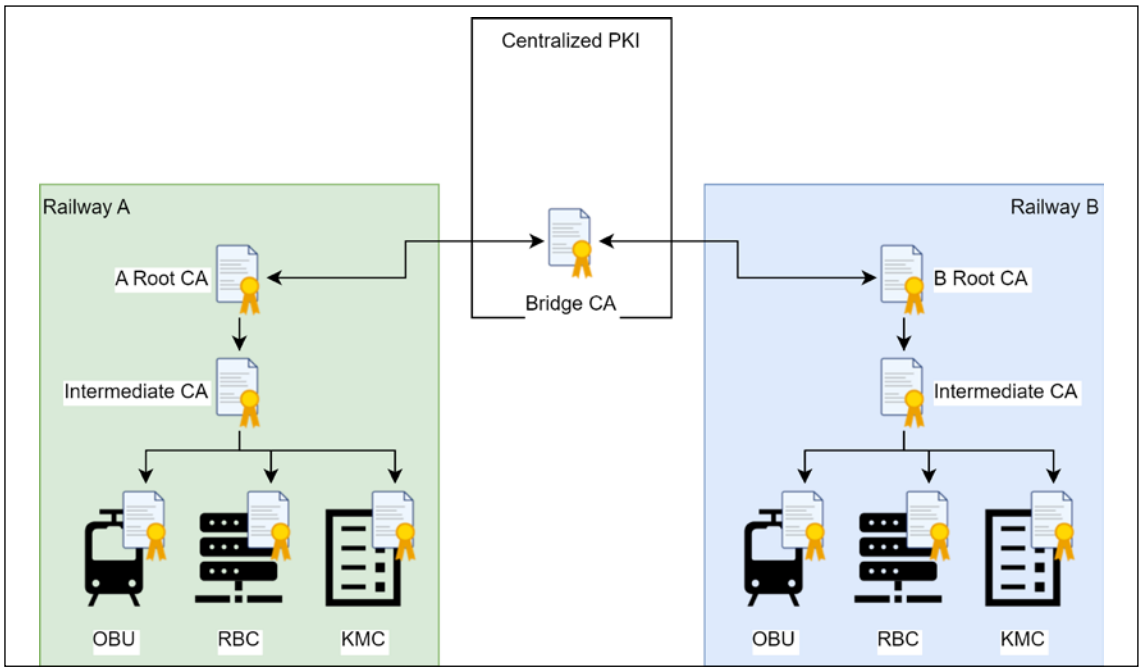

Bild 4: Bridge PKI-Struktur
Fig. 4: The Bridge PKI structure

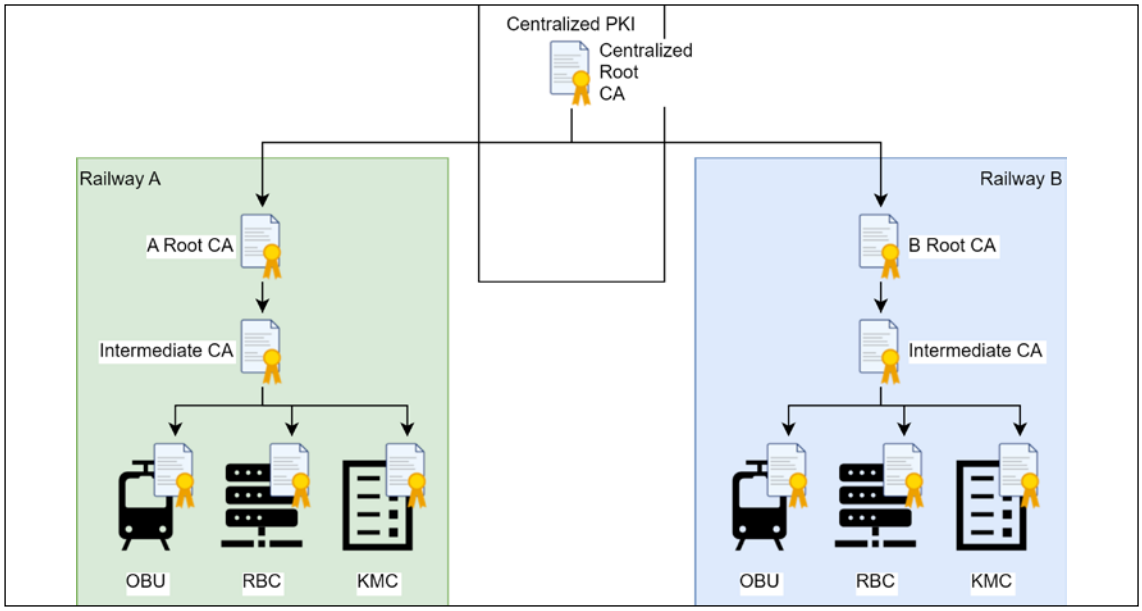

Bild 5: Zentralisierte PKI-Struktur
Fig. 5: The centralised PKI structure

4.3 ERTMS ohne KMC

Der geänderte Schutzbedarf der für Euroradio erforderlichen Schlüssel (KMAC) resultiert in reduzierten Security-Maßnahmen des KMC. Dies ermöglicht eine ressourcenschonendere Umsetzung von On- und Off-Line Key Management. Zusätzlich zur Vereinfachung des Key Managements ist jedoch auch ein vollständiger Verzicht auf diese technische Lösung möglich. Der als unsicher geltende KMAC [9] kann aus Sicht der Security vollständig entfallen. Der aus Sicht der Safety notwendige Safety Code kann ohne kryptographische Eigenschaften umgesetzt werden, da der kryptographische Integritätsschutz schon mittels TLS umgesetzt wird [10]. Der Safety Code muss somit nur noch gegen zufällige Fehler bei der Übertragung schützen. Die hierdurch entfallene Notwendigkeit, Schlüssel vor Verbindungsaufbau auszutauschen, resultiert in einem möglichen Verzicht auf das KMC. Der Safety Code kann durch einen alternativen Algorithmus umgesetzt werden, was eine Änderung im Euroradio Protokoll erforderlich machen würde. Alternativ kann der Austausch der KMAC vereinfacht oder der Einsatz von vorkonfigurierten KMAC erwogen werden. Dies erleichtert auch die Migration zu ERTMS ohne KMC. Durch den Wegfall der Verwaltung und technischer Infrastrukturen eines zentralen Key Managements wird eine drastische Kostensenkung für den Betrieb von ETCS erwartet. Die ESCG wird die unterschiedlichen Lösungskonzepte in ihrer zukünftigen Arbeit detailliert evaluieren.

4.4 Eurobalise Telegram Protection

Neben der leicht angreifbaren Übertragung von Euroradiodaten über den bahnbetrieblichen Mobilfunk waren auch sämtliche anderen Schnittstellen der ERTMS-Systeme Betrachtungsgegenstand der ESCG. Aus diesem Grund wurden auch die Übertragung von Telegrammen von Eurobalisen zum Zug (Balise Transmission Module – BTM) und deren Speicherung analysiert. Aufgrund fehlender kryptographischer Absicherung können Telegramme, wie in Bild 6 zu sehen, manipuliert an den Zug übertragen werden. Diese sind entweder in der Balise fix festgelegt oder werden transparent von einer Datenquelle (z. B. Lineside Electronic Unit) über die Balise an den Zug übertragen. Eine Manipulation kann somit sowohl durch falsche Programmierung der Balise als auch durch falsche Eingangsdaten erfolgen. Somit könnten beispielsweise innerhalb von ETCS Level 1 gefälscht Movement Authorities oder ab ETCS Level 2 verfälschte Positionsdaten gesendet werden, welche unter anderem in

4.3 ERTMS without the KMC

Modifying the need to protect the keys (KMAC) required for Euroradio results in fewer security measures being required for the KMC. This enables a more resource-efficient implementation of the on- and off-line key management. However, in addition to simplifying key management, it is also possible to do without this technical solution altogether. KMAC [9] is considered insecure and can be phased out from a security perspective. The safety code, regarded as essential from a safety perspective, can be implemented without any cryptographic properties, since cryptographic integrity protection has already been implemented via TLS [10]. The safety code now only needs to provide protection against any random errors during transmission. This eliminates the need to exchange keys before establishing a connection, which means that the KMC can be dispensed with. The safety code can be implemented by an alternative algorithm, something which would require an amendment to the Euroradio protocol. Alternatively, the replacement of the KMACs can be simplified or consideration can be given to the use of pre-configured KMACs. This will also make it easier to migrate to ERTMS without the KMC. By eliminating the administration and technical infrastructures inherent in central key management, a drastic reduction in the cost of operating ETCS can be expected. The ESCG will evaluate the different solutions in detail as part of its further work.

4.4 Eurobalise Telegram Protection

In addition to the Euroradio data, which is vulnerable to attack when transmitted via the railway mobile radio, the ESCG also considered all the other ERTMS system interfaces. The way telegrams are transmitted from Eurobalises to the train (the Balise Transmission Module - BTM) and how these telegrams are stored was also analysed. The lack of cryptographic protection means that the telegrams can be tampered with and then transmitted to the train, as illustrated in fig. 6. These telegrams are either pre-set in the balise or are transparently transmitted from a data source (e.g. a Lineside Electronic Unit) via the balise to the train. Tampering can therefore occur both through the incorrect programming of the balise and incorrect input data. For example, phoney movement authorities could be transmitted within ETCS Level 1 or falsified position data could be sent from ETCS Level 2 upwards; either of which could result in a colli-

einer Kollision resultieren könnten. Die ESCG schlägt daher die kryptographische Signierung der Telegramme vor, um eine Prüfung der Authentizität der Daten zu ermöglichen. So kann geprüft werden, ob das Telegramm vom jeweiligen Betreiber der befahrenen Strecke ausgestellt wurde. Telegramme können jedoch, sofern aus Sicht der Safety erforderlich, ohne eine (gültige) Signatur verarbeitet werden. Die ESCG wird hierfür einen technischen Vorschlag erarbeiten.

5 Weitere Arbeit der EUG

Aufgrund der produzierten Ergebnisse wird die ESCG ein Teil der EUG Security Expert Group, welche als Mirror Group der EU-Rail System Pillar Cybersecurity Group ihre Arbeit verrichtet. Dies ist ein weiterer wichtiger Schritt in Richtung Standardisierung der Security für Bahnsysteme. Die ESCG arbeitet unter anderem an folgenden Fokusthemen für dieses Jahr: Aufbau eines PKI-Prototyps, Security von Automatic Train Operation (ATO), Erstellen einer Vorlage des Project Security Management Plans (PSMP) und von Anwendungsrichtlinien für Bestandssysteme.

6 Fazit

Die ESCG hat wertvolle Erkenntnisse, Hilfsmittel und Richtlinien für ihre Mitglieder erstellt, um heutigen und zukünftigen Security-Bedrohungen im Einsatz von ERTMS zu begegnen.

sion. Consequently, the ESCG has proposed that the telegrams be cryptographically signed so as to enable the verification of the data's authenticity. This will check whether the telegram has actually been issued by the relevant operator of the train travelling on the route. If deemed necessary from a safety perspective, however, the telegrams can also be processed without a (valid) signature. The ESCG will develop a technical proposal for this option.

5 Further work for the EUG

Based on the produced results, the ESCG is set to become part of the EUG Security Expert Group working as a mirror group to the EU-Rail System Pillar Cybersecurity Group. This is another important step towards standardising railway system security. The topics on which the ESCG is focussing this year include establishing a PKI prototype, Automatic Train Operation (ATO) security, producing a Project Security Management Plan (PSMP) template and application guidelines for existing systems.

6 Conclusion

The ESCG has produced valuable insights, tools and guidelines for its members in order to address current and future security threats to ERTMS.

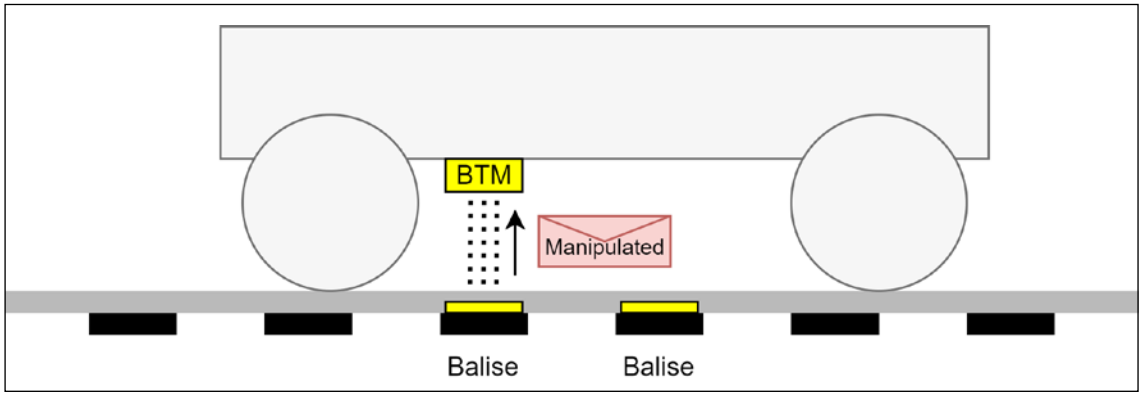

Bild 6: Manipulation Eurobalise Telegram
Fig. 6: Eurobalise telegram manipulation

6.1 Ergebnisse der ESCG

Das Ergebnis nach einem Jahr Arbeit der ESCG ist eine gemeinsame Security-Leitlinie, ein klar definiertes Security-Konzept, eine gemeinsame Bedrohungs- und Risikoanalyse und eine umfassende Liste von Security-Maßnahmen sowohl für den heutigen als auch für den zukünftigen ERTMS-Einsatz. Darüber hinaus hat sich nun eine gut etablierte Gruppe internationaler ERTMS-Security-Experten gebildet, die in den kommenden Jahren weiter zusammenarbeiten wird.

6.2 Anwendung bei der SBB

Die Schweizerische Bundesbahnen AG (SBB) setzt auf einen integrierten Security-Ansatz, d. h. die Sicherstellung respektive Aufrechterhaltung der Integrität und Verfügbarkeit zur Gewährleistung der Safety und RAM (Reliability, Availability, Maintainability) des Gesamtsystems ERTMS. Die Mitarbeit in der ESCG erachtet die SBB dementsprechend als wichtigen Beitrag. Die Ergebnisse aus der Arbeitsgruppe wurden bereits übernommen und adaptiert. Verwendet wurden z. B. die Ergebnisse der „Threat and Risk Analysis" [3] sowie die Security-Maßnahmen mit Blick auf das Bestandsystem [4] und dessen Erweiterung. Zudem wendet die SBB die Security-Maßnahmen zukünftig für Bestandssysteme sowie bei Beschaffung und Integration von neuen Systemen an. ■

6.1 Results from the ESCG's work

One year of work by the ESCG has resulted in a common security guideline, a clearly defined security concept, a common threat and risk analysis and a comprehensive list of security measures for both current and future ERTMS deployment. In addition, a well-established group of international ERTMS security experts has now been set up and will continue its collaborative work in the years to come.

6.2 Applying these results at SBB

Swiss Federal Railways AG (SBB) relies on an integrated security approach, i.e. ensuring and / or maintaining system integrity and availability so as to guarantee the safety and the RAM (Reliability, Availability, Maintainability) of the overall ERTMS system. Accordingly, SBB considers its participation in the ESCG to constitute an important contribution. The results from the working group have already been adopted and adapted. For example, the results of the "Threat and Risk Analysis" [3] and the application of the security measures to the existing system [4] and its further expansion have already been used. In addition, SBB will also apply the security measures to its existing systems in the future, as well as when procuring and integrating any new systems. ■

LITERATUR | LITERATURE

[1] ERTMS Security Core Group, Security Concept (23E060), EEIG ERTMS Users Group, 2023
[2] EULYNX/RCA Security Cluster, ERTMS Security Core Group, OCORA TWS 06 (Cyber-) Security, Security Guideline, 2.01 ed., EEIG ERTMS Users Group, 2023
[3] ERTMS Security Core Group, Threat and Risk Analysis (23E059), EEIG ERTMS Users Group, 2023
[4] ERTMS Security Core Group, Security Measures SoS3 (23E058), EEIG ERTMS Users Group, 2023
[5] ERTMS Security Core Group, Security Measures Future TSI (23E057), EEIG ERTMS Users Group, 2023
[6] UNISIG, SUBSET 137 – On-line Key Management FFFIS, 1.0.0 ed., 2015
[7] UNISIG, SUBSET 146 – ERTMS/ETCS End-to-End Security, 0.1.0 ed., 2022
[8] Dunkelman, O.; Keller, N.; Shamir, A.: A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, 2010
[9] Barker, E.; Roginky, A.: Transitioning the Use of Cryptographic Algorithms and Key Lengths, USA: U.S. National Institute of Standard and Technology, 2019
[10] CENELEC, EN 50159 – Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems, 2010

AUTOREN | AUTHORS

Richard Frhr. Poschinger von Frauenau, M. Sc.
Senior Expert IT-Security, Member of ERTMS Security Core Group
Incyde GmbH
Anschrift / *Address*: Herzog-Wilhelm-Straße 19, D-80331 München
E-Mail: richard.poschinger@incyde.com

Christof Jungo, Ingenieur HTL
Senior Expert IT-Security, Member of ERTMS Security Core Group
SBB AG
Anschrift / *Address*: Hilfikerstraße 3, CH-3000 Bern 65
E-Mail: christof.jungo@sbb.ch

Ernst Kleine, M. Sc.
Technical Manager
EEIG ERTMS Users Group
Anschrift / *Address*: Rue Froissart 123-133, B-1040 Brüssel
E-Mail: ekleine@ertms.be

Martin Espenschied
Head of Security CCS
SBB AG
Anschrift / *Address*: Hilfikerstraße 3, CH-3000 Bern 65
E-Mail: martin.espenschied2@sbb.ch