Auf dem Weg zu einem interoperablen europäischen Cybersecurity-Standard

Towards a European interoperable cybersecurity standard

Markus A. Wischy

Die führenden Akteure der europäischen Bahnbetreiber und Lösungsanbieter (Bild 1) haben seit 2016 zusammengearbeitet, um die Grundlage für eine interoperable europäische Cybersecurity in der Bahnautomatisierungsbranche zu legen. Das EU- und industriefinanzierte Forschungsprojekt X2Rail-1 und 3 (Teil des Horizon 2020 EU-Innovationsprogramms) hat Leitlinien zu technischen Anforderungen und Prozessmethoden für Bahnautomatisierungssysteme herausgegeben. Diese erleichtern die weitere Standardisierung von Cybersecurity in der EU (ERA CCS TSI, UNISIG und EULYNX).

1 Auswahl eines internationalen Cybersecurity-Standards

Das Hauptergebnis nach drei Jahren Analysearbeit innerhalb des durch die EU- und industriefinanzierten Forschungsprojektes X2Rail-1 war die Übernahme des internationalen und industriellen Cybersecurity-Standards IEC 62443 für den EU-Bahnautomatisierungsmarkt. Die Analyse hat gezeigt, dass alle bisherigen Veröffentlichungen des Standards für die Bahnautomatisierung anwendbar sind. Insbesondere wurde kein Konflikt durch die Anwendung der IEC 62443-Serie mit den anzuwendenden CENELEC-Standards für Bahnautomation identifiziert.
Die detaillierte Analyse kam zu dem Ergebnis: Die IEC 62443-Serie ist vollständig anwendbar für die Bahnautomatisierungsbranche.

Key stakeholders from among European rail operators and solution providers (fig. 1) have been working together since 2016 to agree on the foundations for interoperable European cybersecurity in the rail automation domain. The X2Rail-1 and 3 research projects funded by the EU and industry (part of the Horizon 2020 EU innovation program) have provided guidance on the technical requirements and procedural methods for cybersecurity in rail automation systems. This is further facilitating the EU cybersecurity standardisation for ERA CCS TSI, UNISIG and EULYNX.

1 Selecting an international cybersecurity standard

Three years of analysis under the auspices of the EU and industry funded X2Rail-1 research project mainly resulted in the adoption of the IEC 62443 international series of industrial cybersecurity standards for the EU rail automation market. The analysis has shown that all existing publications are applicable to the rail automation domain. In particular, the application of the IEC 62443 series has not introduced any conflicts to the already applicable CENELEC standards for rail automation.
The detailed analysis has led to the conclusion that the IEC 62443 series is fully applicable to the rail automation domain.

Bild 1: Teilnehmerkreis der X2Rail-1 und 3 Cybersecurity-Arbeitsgruppe
Fig. 1: The key stakeholders in the X2Rail-1 and 3 cybersecurity working groups

Quelle aller Bilder / *Source all figures*: X2-Rail-3 WP8 / Horizon 2020 [3]

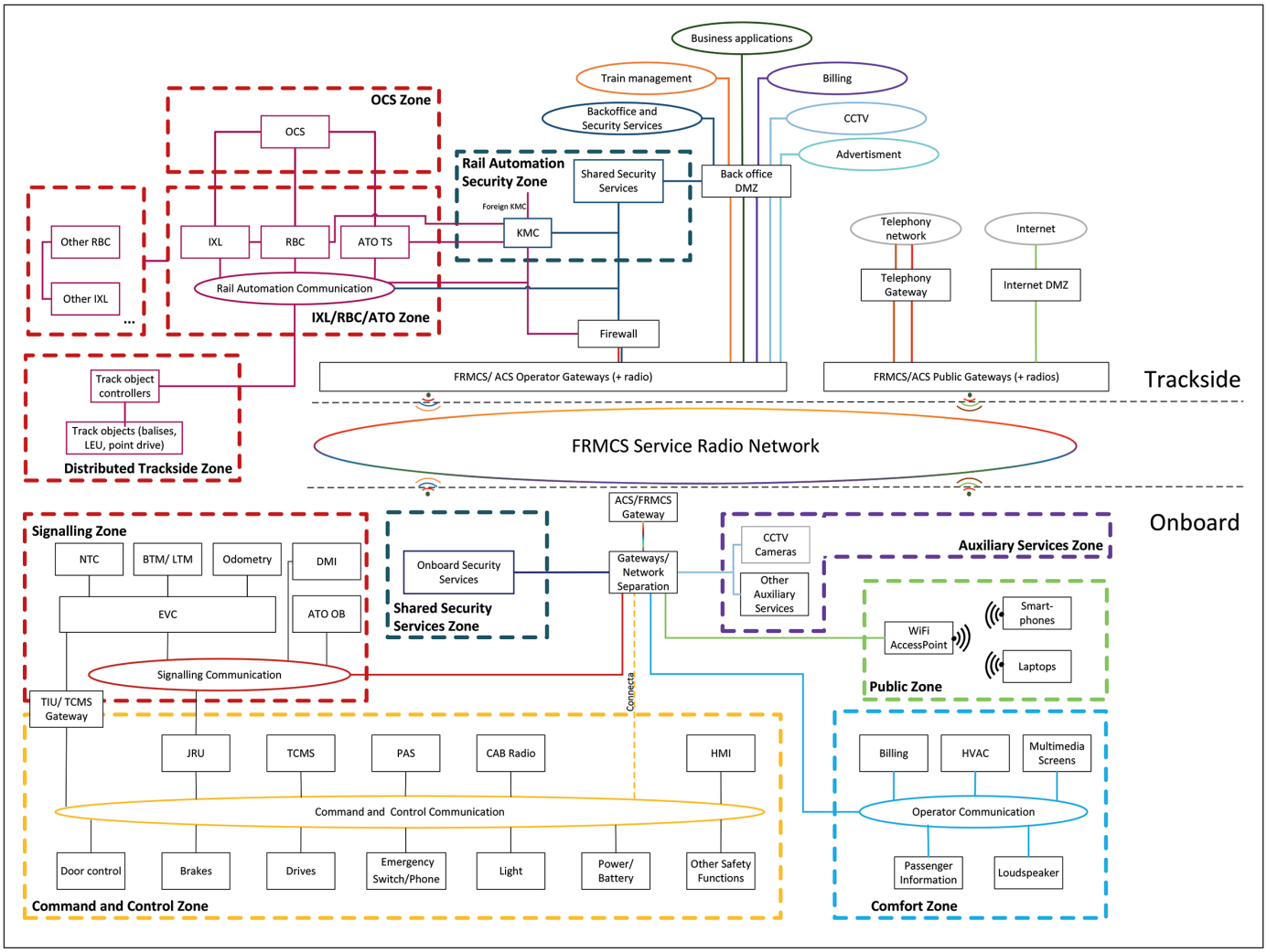

Bild 2: Allgemeine Cybersecurity-Dienste: die Cybersecurity-Umgebung für EU-weite Interoperabilität
Fig. 2: Shared security services: the security environment for EU interoperability

Ein weiteres Ergebnis von X2Rail-1 war die Definition eines Zonenmodells für eine Referenzarchitektur und der Security Levels der einzelnen Zonen nach initialen und detaillierten Risikoanalysen. Von 13 Zonen resultierten elf Zonen mit Security Level 3 und zwei Zonen mit Security Level 2 (siehe hierzu die Security-Architektur mit Zonen, Bild 28 in [1]).

2 EU-Cybersecurity-Interoperabilität für Bahnautomation

X2Rail-3 führte 2019 und 2020 die Arbeiten fort und definierte die Grundlage für technische Interoperabilität für Cybersecurity in der Bahnautomationsbranche. Dies resultierte in der Definition von obligatorischen und gemeinsamen Security-Diensten wie ein systemweiter Zeitsynchronisationsdienst (TIME), zentraler Loggingdienst (LOG), Security Information and Event Management System (SIEM), Angriffserkennungssystem (IDS), Identitäts- und Zugriffsmanagementsystem (IAM), Backupdienst (BKP) und ein Anlageinventursystem (INV) sowie zwei sehr empfohlene Dienste: eine Public Key Infrastruktur (PKI) und ein zentrales Softwareaktualisierungssystem (SWU) (Bild 3).
Nachdem die gemeinsamen Security-Dienste identifiziert wurden, konnte die generische Cybersecurity-Architektur für Bahnautomationssysteme definiert werden [3]. Diese Architektur beinhaltet auch Themen von anderen X2Rail-Arbeitsgruppen wie

Yet another result from X2Rail-1 involved the definition of the security level after initial and detailed risk assessments for the various security zones. Of the 13 zones, eleven resulted in security level 3 and two in security level 2 (see the high level security architecture with zones for more details: fig. 28 in [1]).

2 EU interoperability for rail automation cybersecurity

X2Rail-3 continued to define the basis for the technical interoperability of cybersecurity in the area of rail automation in 2019 and 2020. This resulted in the definition of mandatory shared security services such as the system-wide time service (TIME), central logging (LOG), security incident and event management (SIEM), intrusion detection (IDS), identity and access management (IAM) and backup (BKP) and asset inventory (INV), as well as two highly recommended services: a public key infrastructure (PKI) and a central software updating system (SWU) (fig. 3).
A generic cybersecurity architecture was defined for the rail automation system once the shared security services had been identified [3]. This architecture also includes topics from other X2Rail work groups such as automatic train operation (ATO), the unified train network (CONNECTA) and the fu-

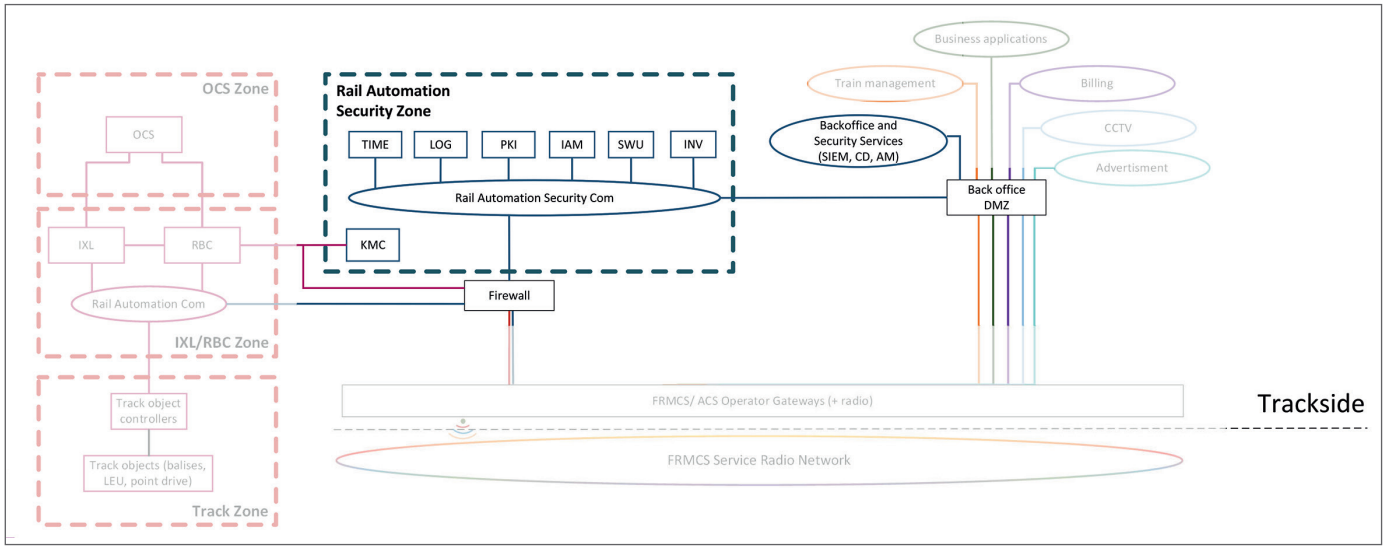

Bild 3: Allgemeine Cybersecurity-Architektur
Fig. 3: The generic cybersecurity architecture

automatische Zugbeeinflussung (ATO – Automatic Train Operation), einheitliches Zugkommunikationsnetz (CONNECTA) und die zukünftige mobile Zugkommunikation (FRMCS / 5G – Future Railway Mobile Communication System). Des Weiteren werden verschiedene Security-Zonen und Conduits für zugseitige als auch streckenseitige Geräte und Systeme dargestellt (Bild 2).

Die X2Rail-3-Cybersecurity-Arbeitsgruppe entwickelte des Weiteren die Basis für EU-Interoperabilität, indem die Protokolle zu den gemeinsamen Security-Diensten definiert wurden. In Frage kommende Protokolle wurde analysiert und evaluiert. Dazu wurden die folgenden Auswahlkriterien benutzt:

- Das Protokoll ist ein internationaler Standard (d. h. es gibt ein veröffentlichtes Dokument)
- Das Protokoll ist stabil
- Das Protokoll wird auf breiter Basis benutzt
- Open-Source-Implementierungen sind vorhanden
- Das Protokoll unterstützt Authentifikation und Integritätsschutz mit kryptografischen Mitteln
- Das Protokoll unterstützt Verschlüsselung (wenn Vertraulichkeit notwendig ist)
- historische Schwachstellen und Verfügbarkeit von Sicherheitsaktualisierungen.

Mit diesen Evaluationskriterien wurden die folgenden Protokolle ausgewählt:

- systemweite Zeitsynchronisation (TIME): NTPv4 (RFC 5905)
- zentrales Logging (LOG): syslog-ng (d. h. syslog over TLS) (RFC 5425)
- Security and Event Management System (SIEM): syslog-ng (RFC 5425)
- Zertifikatsmanagement (PKI): CMP (RFC 4210)
- Identitäts- und Zugriffsmanagement (IAM): SCIMv2 über TLS (RFC 7655)
- Backup (BKP): rsync über SSH
- zentrale Softwareaktualisierung (SWU): OPC UA SC & HTTPS
- zentrale Anlageinventur (INV): OPC UA SC (IEC 62541).

Das Hauptmotiv dieser Arbeit von X2Rail war, einen gemeinsamen europäischen Markt zu definieren. Die Definition einer vereinheitlichten Security-Umgebung kann technische länderspezifische Schnittstellen vermeiden. Lösungs- und Produkthersteller können damit ihre Produkte entwickeln und in zukünftige europäische Bahnautomationsprojekte integrieren. Ein gemeinsamer Standard senkt die Kosten für Bahnautomationsprodukte (weniture rail mobile communication system (FRMCS / 5G). Furthermore, it also depicts the various security zones and conduits from onboard as well as trackside equipment and systems (fig. 2).

The X2Rail-3 cybersecurity working group has further developed the basis for EU interoperability by defining the protocols for the shared security services. The possible protocols to the shared security services have been analysed and evaluated. The following evaluation criteria were used:

- the protocol is an international standard (e.g. a published document)
- the protocol's definition is stable
- widespread use of the protocol
- open source implementation is available
- the protocol supports authentication and integrity protection by cryptographic means
- the protocol supports encryption (where confidentiality is needed)
- historic vulnerabilities and the availability of patches.

The following protocols have been chosen based on the evaluation criteria:

- system-wide time synchronisation (TIME): NTPv4 (RFC 5905)
- central logging (LOG): syslog-ng (i.e. syslog over TLS) (RFC 5425)
- security and event management system (SIEM): syslog-ng (RFC 5425)
- certificate management (PKI): CMP (RFC 4210)
- identity and access management (IAM): SCIMv2 over TLS (RFC 7655)
- backup (BKP): rsync over SSH
- remote software update (SWU): OPC UA SC & HTTPS
- asset inventory (INV): OPC UA SC (IEC 62451).

The main motivation for the work undertaken by X2Rail was to define a common market in Europe. The definition of a security environment can eliminate any country-specific technical interfaces. Solution and product providers can use this to develop their product portfolio and integrate it into future European rail automation systems. A common standard lowers the costs for rail automation products (fewer customer-specific adapta-

ger länderspezifische Adaption ist notwendig), fördert somit eine größere Auswahl für die Bahnbetreiber und erleichtert den grenzüberschreitenden Bahnverkehr in Europa.
Dieser gemeinsame Standard wurde in X2Rail-3 mittels Schutzprofilen (eine Auflistung der technischen und Interoperabilitätsanforderungen) definiert. Die Arbeitsgruppe definierte drei Schutzprofile: für streckenseitige Komponenten [4], für zugseitige Komponenten [5] und für Komponenten des Adaptable Communication System (ACS) [6].
Die Dokumente der gemeinsamen Security-Dienste und der Schutzprofile sind öffentlich über die X2Rail3-Webseite [2] zugänglich.
Die generische Security-Architektur, die gemeinsamen Security-Dienste und die Schutzprofile werden in europäischen Standardisierungsgremien weiter detailliert (siehe hierzu Kapitel 4).

3 Weitere Ergebnisse

Die Anwendbarkeit von Cybersecurity auf Bestandsysteme wurde ebenfalls in X2Rail-3 analysiert und umfasste Themen wie Bedrohungsanalyse, Implementierung von IEC 62443 Anforderungen und ausgleichende Gegenmaßnahmen.
Die Risikobewertungsmethode, die in X2Rail-1 definiert und benutzt wurde, stellte sich als komplex und zeitaufwendig heraus. Daher hat X2Rail-3 eine vereinfachte Risikobewertungsmethode auf Basis des STRIDE-Modells definiert (STRIDE steht für die Bedrohungsszenarien Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Evelation of Privileges).
Weitere Berichte wurden zu IoT (Internet of Things)-Security and Security für hoch verfügbare Architekturen erstellt.
Die Ergebnisse dieser Themen sind ebenfalls auf der X2Rail-3-Webseite veröffentlicht [2].

4 Weiterverwendung

Die Verbreitung der X2Rail-3-Ergebnisse in EU-Standardisierungsgremien ist für 2021 geplant. Insbesondere werden die X2Rail-Ergebnisse ERA TSI CCS 2022, UNISIG subset 146 und EULYNX BL 4.x bereitgestellt und dort weiter detailliert.
Jedoch ist der komplette Anforderungskatalog aus den Schutzprofilen in Anbetracht der kurzen Frist für die Erstellung des ERA TSI CCS 2022 nicht umsetzbar. Darum werden die Anforderungen in zwei Gruppen zerlegt. Die erste Gruppe fokussiert sich auf den Authentifikation- und Integritätsschutz von Datenkommunikation mittels TLS (Transport Layer Security), die Benutzung einer PKI und Zeitsynchronisation. Die zweite Gruppe beinhaltet die verbleibenden Anforderungen aus den Schutzprofilen für eine aktualisierte TSI (Technical Specification for Interoperability) in den kommenden Jahren.

5 Ausblick

X2Rail hat nicht nur an technischen Themen gearbeitet. Prozessthemen wurden ebenfalls analysiert. X2Rail-1 hat die prozessbedingten Cybersecurity-Anforderungen auf die Anwendbarkeit in der Bahnautomatisierungsbranche hin evaluiert. Insbesondere beim Thema Security-Anforderungsnachweis konnten verschiedene Verbesserungen definiert werden (u. a. Klärung des Umfangs für Schwachstellentests).
X2Rail-3 D9.1 wird eine detailliertere und angepasste Sicht auf bewährte Techniken von Security-Anforderungsbewertungen und Validierung entlang des Produkt- und IACS-Lebenszyklus dokumentieren.

tions are needed), provides rail operators with a wider choice and simplifies the cross border rail traffic.
This common standard was created in X2Rail-3 by defining the protection profiles and listing the technical and interoperability requirements. The working group defined three protection profiles: trackside components [4], on-board components [5] and the components in the adaptable communication system (ACS) [6].
The documents defining the shared security services and the protection profiles are publicly available on the X2Rail-3 website [2].
The generic security architecture, the shared security services and the protection profiles will be given greater detail by the European standardisation bodies (see chapter 4).

3 Other results

The applicability of cybersecurity to legacy systems has also been analysed in X2Rail-3 with regard to areas such as threat analysis, the implementation of IEC 62443 requirements and compensating counter-measures.
The risk assessment method defined and used during X2Rail-1 was found to be complex and time consuming. Therefore, X2Rail-3 has defined a simplified risk assessment method using the STRIDE model (Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Evelation of Privileges).
Further reports on rail security topics have been created on IoT (Internet of Things) security and securing resilient architectures.
The results of these topics have also been published on the X2Rail-3 website [2].

4 Dissemination

The dissemination of the X2Rail-3 results to the EU standardisation groups is planned for 2021. The X2Rail results will especially be provided and further detailed by ERA TSI CCS 2022, UNSIG subset 146 and EULYNX BL 4.x.
However, the full set of requirements for the protection profiles is not feasible within the short timeframe of ERA TSI CCS 2022. The requirements have therefore been split into two sets. The initial set focuses on communication authentication and integrity protection using TLS (Transport Layer Security), the use of a PKI and time synchronisation. The second set contains the remaining requirements for an updated TSI (Technical Specification for Interoperability) in the years ahead.

5 Outlook

X2Rail has not only worked on technical topics, but has also analysed procedural topics. X2Rail-1 evaluated the procedural cybersecurity requirements with regard to their applicability in the rail automation domain. Several improvements were especially able to be defined in the area of security verification (e.g. scope clarification for vulnerability testing).
X2Rail-3 D9.1 will provide a more detailed and aligned view of the security verification and validation testing best practices along and across the product lifecycle and the IACS lifecycle.
This will constitute the basis for its further dissemination to ENISA (European Network and Information Security Agency) and CENELEC.
Additionally, X2Rail-3 WP9 has also addressed the emerging topic of railway supply-chain security, verification and the validation of X2Rail-3 demonstrators (as ACS).

Dies stellt dann die Basis dar für weitere Verwendung bei ENISA (European Network and Information Security Agency) und CENELEC (z. B. als Bestandteil von Zertifizierungsschemata). Zusätzlich adressiert X2Rail-3 WP9 die Themen Lieferkettensicherheit sowie Anforderungsbewertung und Validierung von X2Rail-3-Demonstratoren (u. a. beim ACS Demonstrator).

6 Zusammenfassung

X2Rail-1 und 3 haben Ergebnisse erstellt, die die Grundlagen für EU-Interoperabilität für Cybersecurity legen. Die Hauptergebnisse für technische Interoperabilität sind eine generische Cybersecurity-Architektur, gemeinsame Security-Dienste, Interoperabilitätsprotokolle und Schutzprofile für streckenseitige, zugseitige und Adaptable-Communication-System-Komponenten. ■

6 Summary

X2Rail-1 and 3 have created results that provide the foundation for EU cybersecurity interoperability. The main results for technical interoperability involve a generic cybersecurity architecture, shared security services, interoperability protocols and protection profiles for trackside, on-board and adaptable communication system components. ■

LITERATUR | LITERATURE

[1] X2Rail-1 D8.2 Security Assessment – available from "Results" section of following website: https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1, 15.2.2021 um 16:30
[2] X2Rail-3 Website https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3, 15.2.2021 um 16:30
[3] X2Rail-3: Deliverable 8.2-2 Generic cybersecurity architecture and shared security services, X2Rail-3 Website, 02-12-2020
[4] X2Rail-3: Deliverable 8.2-3b Protection profile trackside components, X2Rail-3 Website, 02-12-2020
[5] X2Rail-3: Deliverable 8.2-3c Protection profile onboard components, X2Rail-3 Website, 02-12-2020
[6] X2Rail-3: Deliverable 8.3 Protection profile adaptable communication system components, X2Rail-3 Website, 02-12-2020

AUTOR | AUTHOR

Dipl.-Inf. Markus A. Wischy
Head of Product and Solution Security (R&D)
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: markus.wischy@siemens.com