IT-Sicherheitsmaßnahmen für ATO over ETCS

IT security measures for ATO over ETCS

Martin Koop | Richard Poschinger

Eine erhöhte Bedrohungslage rückt die IT/OT-Sicherheit (kurz Security) als Bestandteil der Technischen Spezifikationen für Interoperabilität der transeuropäischen Hochgeschwindigkeitsbahnsysteme in den Vordergrund. Durch den verstärkten Einsatz digitaler Leit- und Sicherungstechnik (DLST) steigt der Bedarf, die bestehenden Security-Schwächen von ETCS (European Train Control System) zu reduzieren und gleichzeitig die Safety- und Security-Anforderungen für neue Systeme wie ATO zu definieren.

Die voranschreitende Ausrüstung von DLST bereitet den hoch- und vollautomatisierten Bahnbetrieb vor. Das Ziel, automatischen Zugbetrieb im Automatisierungsgrad 2 (Grade of Automation 2, GoA 2) umzusetzen, macht es notwendig, neue technische Lösungen zu entwickeln. Diese müssen in der Migrationsphase mit bestehenden Systemen verbunden werden.
Ein Beispiel ist das moderne Verkehrsmanagementsystem (Traffic Management System, TMS). Das TMS bezieht dabei Fahrplandaten aus dem bestehenden Leit- und Dispositionssystem sowie die Fahrerlaubnis aus dem digitalen Stellwerk (DSTW). Zukünftig werden die Daten dann in einem zentralen und georedundanten Rechenzentrum für Automatic Train Operation (ATO) aufbereitet und bereitgestellt. Zusammen mit dem Einsatz aktueller 5G Funktechnologie (Future Railway Mobile Communication System, FRMCS) soll damit eine 20-prozentige Steigerung der Kapazität für den Zugverkehr erreicht werden.
Grundlagen bilden das DSTW, das unter anderem eine verkürzte Zugfolge sicherstellt, ETCS, das für die automatische Bremskurvenüberwachung zuständig ist und ATO, welches das automatisierte Fahren übernimmt.
Die Herausforderungen sind das Zusammenspiel neuer und bestehender Systeme verschiedener Hersteller, die Nutzung gemeinsamer Schnittstellen auf der Seite des Betreibers und die Absicherung der Angriffsvektoren, die sich daraus ergeben. Hierzu zählen beispielsweise die Übergänge zwischen den verschiedenen Kommunikationsnetzen. Diese umfassen den Mobilfunk zur bahnbetrieblichen Kommunikation (GSM-R / FRMCS), die für ATO in der ersten Migrationsphase eingesetzten öffentlichen Mobilfunknetze sowie die Netzwerkinfrastruktur des Betreibers. Zusätzliche Schwachstellen können sich ergeben, wenn Betreiber und Hersteller Insellösungen für Security-Mechanismen schaffen, die keine systemübergreifende Angriffserkennung ermöglichen. Durch den Einsatz zentralisierter Dienste würde zusätzlich das Potenzial genutzt, Ressourcen einzusparen. Beispielsweise nach einem erkannten Angriff wird die Reaktion, sowohl in Form des Ausschlusses von kompromittierten Geräten als auch mittels fehlerbehebender Updates, durch eine zentrale Koordination erleichtert.
Die zonenübergreifenden Verbindungen erfordern deswegen eine sorgfältige Safety- und Security-Betrachtung des kompletten Systems nach etablierten Security-Normen, genauso wie den Einsatz unterschiedlicher IT/OT-Schutzmaßnahmen, wie sie teil-

An increased threat level has brought IT/OT security into focus as part of the Technical Specifications for the Interoperability of Trans-European High-Speed Rail Systems. The increased use of digital command and control systems has increased the need to reduce the existing ETCS (European Train Control system) security weaknesses and at the same time to define the safety and security requirements for any new systems, such as ATO.

The ongoing retrofitting of digital command and control technology is paving the way for highly and fully automated railway operations. The goal of implementing automatic train operations at Grade of Automation Level 2 (GoA 2) has made it necessary to develop new technical solutions. These must be linked to the existing systems during the migration phase.
One such example is the modern Traffic Management System (TMS). The TMS obtains timetable data from the existing control and dispatching system, as well as movement authorisations from the digital interlocking. The data is then processed and made available in a central, geo-redundant data centre for ATO (Automatic Train Operation). In conjunction with the use of current 5G radio technology (FRMCS: Future Railway Mobile Communication System), this is expected to achieve a 20 % increase in train traffic capacity.
The basis for this is the digital interlocking, which ensures shorter train headways, amongst other things, ETCS, which is responsible for automatic braking curve monitoring, and ATO, which handles automated driving.
The challenges lie in the interaction between the new and existing systems made by different manufacturers, the use of common interfaces by the operators and protection against the attack vectors that result from this. These include, for example, the transitions between the various communication networks. These networks are the mobile radio network for railway communications (GSM-R / FRMCS), the public mobile radio networks used for ATO in the first migration phase and the operator's network infrastructure. Additional vulnerabilities may arise, if operators and manufacturers create isolated solutions for security mechanisms that do not enable cross-system attack detection. The use of centralised services would additionally offer the potential to save resources. For example, the response after a detected attack, both in the form of the exclusion of any compromised devices and the provision of troubleshooting updates, would be facilitated by central coordination.
The inter-zone connections therefore require a careful safety and security assessment of the complete system according to the established security standards, as well as the use of different IT/OT protection measures, as partially discussed in the CYRAIL project [1]. In this article, we will focus on the selection of measures that will play a major role in the realisation of ATO over ETCS.

weise im Projekt CYRAIL diskutiert [1] wurden. In diesem Beitrag wollen wir uns besonders auf eine Auswahl von Maßnahmen konzentrieren, welche für die Realisierung von ATO over ETCS eine tragende Rolle spielen werden.

1 IT-Sicherheit in ATO over ETCS

Der EU-Richtlinie „96/48/EG" für Interoperabilität der transeuropäischen Hochgeschwindigkeitsbahnsysteme folgend, bildet die Technische Spezifikation für Interoperabilität der Zugsteuerung, Zugsicherung und Signalgebung (TSI ZZS) bereits seit den 1990er Jahren die Grundlage der Sicherheitsfunktionen mit Fokus auf Safety. Mit der Umsetzung der TSI ZZS wurde bislang als Voraussetzung eines (IT-)Sicherheitskonzepts die Anwendung der Normen EN 50126-1, EN 50126-2, EN 50128 sowie EN 50129 vorgegeben. Dabei behandeln die Normenreihen um EN 50126 „Sicherheit" grundsätzlich als Widerstandsfähigkeit des Eisenbahnsystems gegen Vandalismus, böswillige Handlungen und absichtlich schädliches menschliches Verhalten (Betriebssicherheit = Safety).
Für die Betrachtung von IT-Sicherheit (Security) stellt die EN 50126 jedoch wenig Anforderung und verweist auf die Anwendung weiterer etablierter Verfahren und Prozesse. Genau an dieser Stelle ist es essenziell, dass sowohl Hersteller, Integratoren sowie Betreiber grundsätzlich die Normen IEC 62443 bzw. CLC/TS 50701 zur Entwicklung von automatisierten Industrieprodukten nach bahnspezifischen IT-Security-Prozessen heranziehen.

1 IT security in ATO over ETCS

Following the adoption of EU Directive "96/48/EC" on the interoperability of trans-European high-speed rail systems, the Technical Specifications for the Interoperability of Control Command and Signalling (TSI CCS) have formed the basis for safety functions since the 1990s. The implementation of the TSI CCS resulted in the specified application of the EN 50126-1, EN 50126-2, EN 50128 and EN 50129 standards as a prerequisite for any safety and security concept. The series of standards around EN 50126 define "safety" as the resistance of the railway system to vandalism, malicious acts and deliberately harmful human behaviour (operational safety).
However, EN 50126 makes few demands in relation to the assessment of IT security and it refers to the application of other established procedures and processes. At this point, it is essential for manufacturers, integrators and operators to refer to the IEC 62443 and CLC/TS 50701 standards for the development of any automated industrial products in accordance with the railway-specific IT security processes.

2 Encryption and integrity protection in ETCS

The following threats to the data exchange between the train and trackside via GSM-R, amongst others, were identified by the initial ETCS specification in the 1990s: message delay / removal / masking or manipulation. The remedy to this was

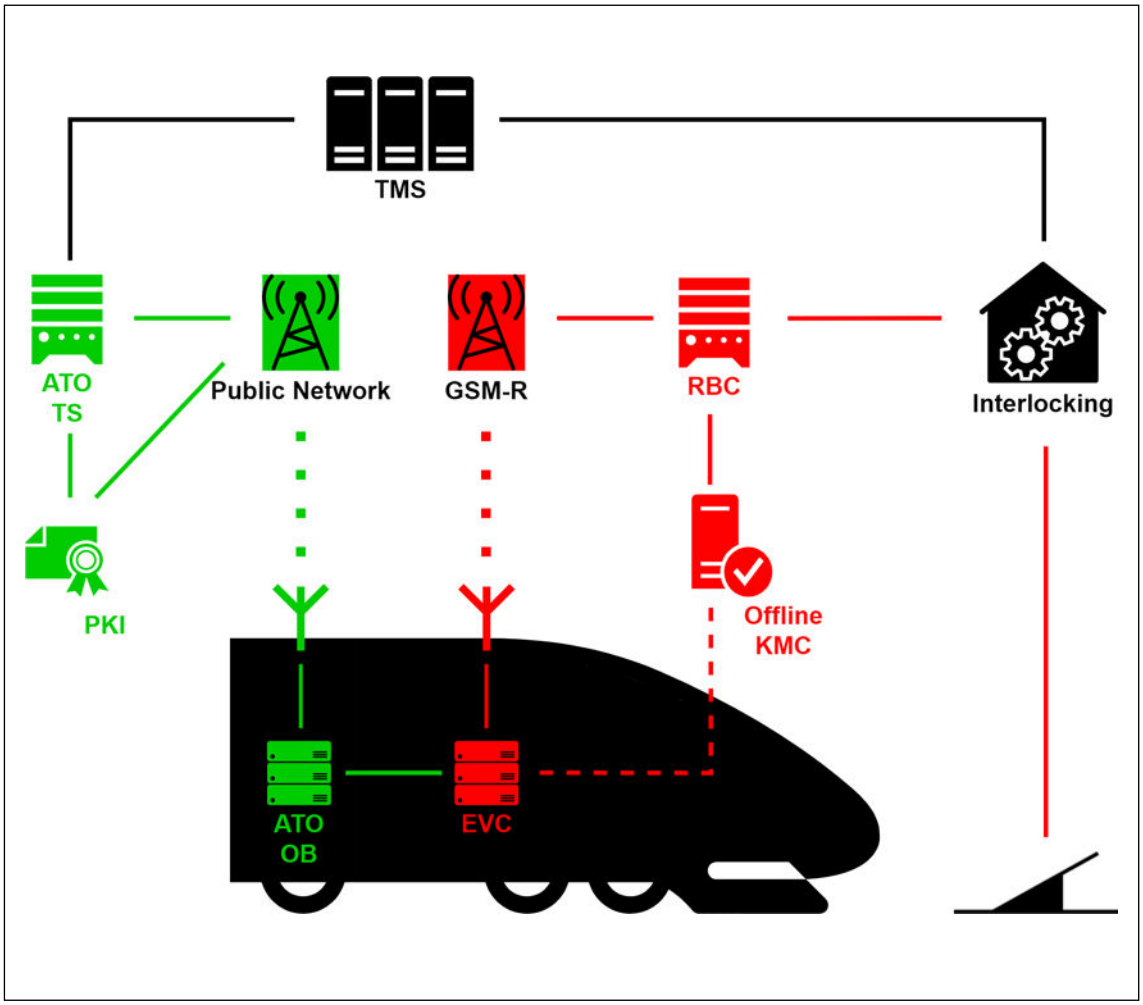

Bild 1: Aufbau von ATO over ETCS mit getrennten mobilen Netzen
Fig. 1: The structure of ATO over ETCS with separate mobile networks

2 Verschlüsselung und Integritätsschutz in ETCS

Mit der initialen Spezifikation von ETCS in den 1990ern wurden unter anderem folgende Bedrohungen beim Datenaustausch zwischen Zug und Streckenseite über GSM-R identifiziert: Nachrichtenverzögerung, -entfernung, -maskierung oder -manipulation. Die Behandlung wurde mit grundlegenden Maßnahmen in der Euroradio Spezifikation [2] dokumentiert.
Dazu gehörte das Einfügen von Zeitstempel, Seriennummern sowie des Integritäts- und Authentizitätsschutzes mittels MAC (Message Authentication Codes). Die Berechnung des MAC basiert dabei auf dem 3DES Algorithmus (Triple Data Encryption Standard). Dieser berechnet eine kryptografische Prüfsumme der Nachricht des Senders A, indem mittels symmetrischen Schlüssels die Eingabedaten blockweise chiffriert werden. Der letzte Block des Schlüsseltextes dient dann als Prüfsumme. Mit dem selben (symmetrischen) Schlüssel kann anschließend der Empfänger B auf dieselbe Weise die Prüfsumme errechnen und damit die Integrität der Nachricht prüfen. Ebenso wird durch die Ausstellung eindeutiger (symmetrischer) Schlüsselpaare zwischen einem bestimmten Sender A (z. B. Zug Nr. 1) und einem Empfänger B (z. B. Radio Block Centre (RBC) in Stuttgart) die Authentizität der Kommunikationspartner nachgewiesen. Anzumerken ist, dass dabei die Nachricht weiterhin unverschlüsselt zwischen A und B über GSM-R übermittelt wird, somit kein Schutz der Vertraulichkeit gegeben ist. Die Schlüsselgenerierung findet dabei zentral im Key Management Center (KMC) statt.
Der Vorteil dieses Verfahrens ist, das die Datenpakete weiterhin sehr klein sind und die Berechnung schnell durchgeführt wird. Dies ist in Anbetracht der geringen Datenkapazität von GSM-R und der geringen Rechenleistung bestehender ETCS-Zugsicherungssysteme (EVC: European Vital Computer) notwendig. Das Verfahren hat jedoch mehrere Probleme bzw. potenzielle Bedrohungen:

- Mit zunehmend größeren Datenpaketen kann die 3DES-Chiffrierung (Prüfsummenbildung) gebrochen werden [3, 4, 5], womit Angreifer Datenpakete fälschen und beispielsweise eine unerlaubte Fahrerlaubnis senden könnten.
- Durch die große Menge an notwendigen Schlüsseln (S) für alle Teilnehmer (T) (Gesamtanzahl: S=T*(T-1)/2) erhöht sich zum einen der Verwaltungsaufwand der Schlüssel und zum anderen das Risiko zum Schutz der zentral gespeicherten Schlüssel.
- Da die Auslieferung (Erneuerung) der Schlüssel aktuell noch manuell durchgeführt wird, ist neben dem enormen Zeit- und Kostenaufwand besonders der Transport der Schlüssel auf die Fahrzeuge und RBC ein potenzieller Angriffsvektor. Hierbei wird nach der Generierung der Schlüssel das Schlüsselmaterial mittels gesichertem Transportmedium (USB-Stick / Laptop) von Instandhaltungspersonal zu den Entitäten gebracht und installiert.
- Durch die hohen Aufwände bei der Auslieferung / Erneuerung der Schlüssel kommt es auch vor, das kleinere Eisenbahnverkehrsunternehmen nur einen gemeinsamen Schlüssel für die komplette Flotte verwenden. Dadurch wird nicht nur der Authentizitätsschutz aufgehoben, es steigt auch das Risiko der Kompromittierung eines Schlüssels.
- Außerdem können Angreifer die Schlüssel abgreifen und somit die Kommunikation zwischen den entsprechenden Kommunikationspartnern fälschen, wenn diese nicht sicher auf dem Zug bzw. im RBC gespeichert werden.

Um den Aufwand der manuellen Auslieferung der Schlüssel zu reduzieren, soll mittels zentralen online KMC die Übermittlung

documented with the basic measures in the Euroradio specification [2].
These included the insertion of timestamps, serial numbers and integrity as well as authenticity protection using MAC (Message Authentication Codes). The calculation of a MAC is based on the 3DES algorithm (Triple Data Encryption Standard). It computes a cryptographic checksum for sender A's message by encrypting the input data block by block using a symmetric key. The last block of the key text is then used as the checksum. Using the same (symmetric) key, recipient B can then compute the checksum in the same way and thus check the integrity of the message. Similarly, the issuance of unique (symmetric) key pairs between a specific sender A (e.g. train number 1) and receiver B (e.g. the Radio Block centre (RBC) in Stuttgart) proves the authenticity of the communication partners. It should be noted that the message is still transmitted in an unencrypted form between A and B using GSM-R, so there is no confidentiality protection. The key generation takes place centrally at the Key Management Centre (KMC).
The advantage of this procedure lies in the fact that the data packets remain very small and the computation can be performed quickly. This is necessary in view of the low data capacity offered by GSM-R and the low computing power of the existing ETCS train control systems (EVC: European Vital Computer). However, the method has several problems and / or potential threats:

der Schlüssel durch eine verschlüsselte Datenverbindung (TLS) realisiert werden – siehe Subset 137. Hierzu ist der Aufbau einer Public Key Infrastructure (PKI) vorausgesetzt, welche die notwendige Signierung der Zertifikate realisiert und den Vertrauensanker sicherstellt. Mittels TLS verschlüsselter Verbindung zum Zug sowie RBC kann damit der symmetrische Schlüssel sicher übertragen werden.
Anzumerken ist, dass nach der verschlüsselten Übermittlung der symmetrischen Schlüssel die Kommunikation weiterhin unverschlüsselt und nur integritätsgeschützt durch die Prüfsumme MAC mittels 3DES stattfindet. Die beschriebenen Bedrohungen bestehen weiterhin.

3 Erhöhung der Informationssicherheit in ATO

Die Kernkomponenten des ATO-Systems bilden die ATO-TS (Trackside) auf der Streckenseite und ATO-OB (Onboard) auf dem Fahrzeug sowie das Teilsystem TMS (Bild 1).
Dabei übernimmt das ATO-OB neben der Türsteuerung an Haltepunkten die automatische Antriebs- und Bremssteuerung des Fahrzeugs. Hierbei wird zu jeder Zeit das optimale Geschwindigkeitsprofil anhand der Daten der Infrastruktur (Segment- bzw. Streckenprofil) sowie Fahrplaninformationen (Journey-Profil) berechnet, welche von TMS verarbeitet, in der ATO-TS aggregiert und an die entsprechende ATO-OB übermittelt werden. Mit der Schnittstelle vom ATO-OB zum EVC sorgt ETCS für die sichere Einhaltung zulässiger Geschwindigkeitsprofile und Zugabstände (Bild 2).

- 3DES ciphering (checksum computation) can be broken with increasingly larger data packets [3, 4, 5]. This would allow attackers to forge data packets and send an unauthorised movement authority, for example.
- The large number of keys (K) required for all the subscribers (S) (total number: K=S*(S-1)/2) increases both the administrative effort required to manage the keys and the risk of protecting any centrally stored keys.
- Since the keys are currently delivered (renewed) manually, the transportation of the keys to the vehicles and the RBCs constitutes a potential attack vector, in addition to the enormous time and costs involved. Once the keys have been generated, the key material is transported to the entities and installed by maintenance personnel using a secure transport medium (a USB stick / laptop).
- Due to the high volumes involved in the delivery / renewal of the keys, smaller rail transport companies sometimes only use one common key for the entire fleet. This not only removes the authenticity protection, but it also increases the risk of a key being compromised.
- Furthermore, if the keys are not securely stored on the train or in the RBC, attackers can tap the keys and thus forge the communication between the corresponding communication partners.

In order to reduce the effort required for manual key delivery, a central online KMC is to be used to transmit the keys via an encrypted data connection (TLS) – see Subset 137. This

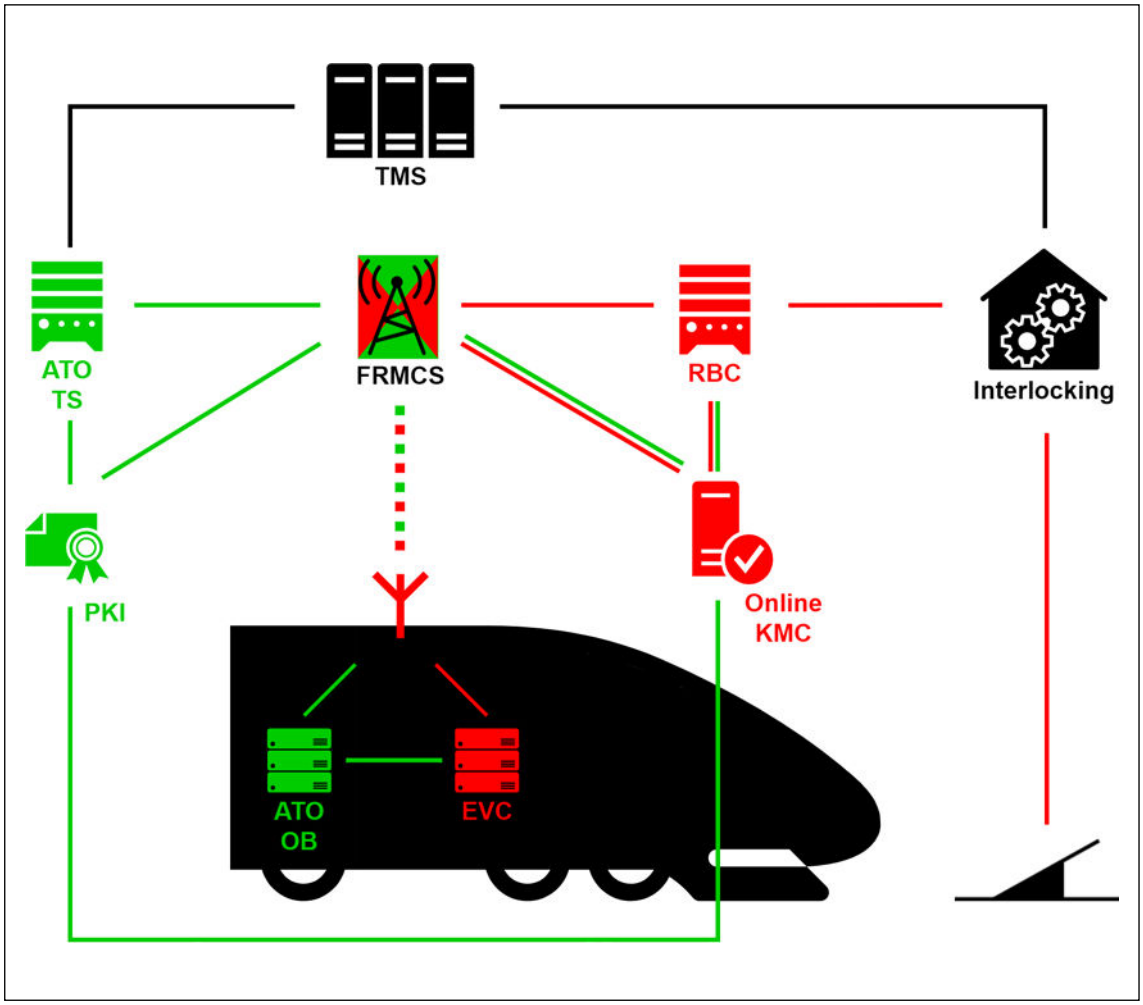

Bild 2: Aufbau von ATO over ETCS mit einem gemeinsamen mobilen Netz und PKI
Fig. 2: The setup of ATO over ETCS with a common mobile network and PKI

Mit der Inbetriebnahme von ATO sollen zukünftig, zusammen mit der TSI 2022, mehrere neue IT-Sicherheitsfunktionen umgesetzt werden, welche die Security-Schwächen aus ETCS lösen sollen. Die Aktualisierung der TSI bezieht sich dabei auf:

- Aktualisierung der Nachrichtenkonfiguration (z. B. Kopfdaten der Anwendungsdaten) aus dem Subset 126 in den neuen Subset 148
- Aktualisierte Spezifikation der verschlüsselten Kommunikation über TLS (inklusive PKI-Funktionen) aus dem Subset 126 Anhang A (Subset 137) in den neuen Subset 146 mit:
- Einsatz einer zentralen PKI mit Registration Authority (zur Prüfung der Authentizität der Teilnehmer) und Validation Authority (Validierung der Zertifikate) mittels OCSP (Online Certificate Status Protocol) bzw. CRL (Certificate Revocation List)
- Nutzung des aktuellen Verschlüsselungsprotokolls TLS 1.3 zur Verschlüsselung des kompletten Datenverkehrs (bzw. Schutz der Integrität und Authentizität)
- Generierung der Schlüssel im Endgerät (nicht zentral wie beim KMC)
- Speichern der Schlüssel im abgesicherten HSM (Hardware Secure Module)
- Einsatz sicherer Random Number Generator zur Erzeugung des Schlüsselmaterials
- Verwendung aktueller Algorithmen zum Verschlüsseln und Signieren der Nachrichten mittels SHA3, AES und Elliptischen Kurven.

requires the implementation of a Public Key Infrastructure (PKI), which provides the necessary signing of the certificates and ensures the trust anchor. The symmetric key can then be transmitted securely via a TLS-encrypted connection to the train and the RBC.
It should be noted that once the encrypted transmission of the symmetric keys has taken place, the communication still remains unencrypted and is only integrity-protected by the MAC checksum using 3DES. The described threats still exist.

3 Increasing information security in ATO

The core components of the ATO system are the ATO-TS (trackside) and ATO-OB (onboard) on the vehicle, as well as the TMS subsystem (fig. 1).
In addition to the door control at the stopping points, the ATO-OB also takes over the vehicle's automatic driving and brake control. The optimal speed profile is constantly computed based on infrastructure data (the route / segment profile) and the timetable information (the journey profile), which is processed by the TMS, aggregated in the ATO-TS and transmitted to the corresponding ATO-OB. ETCS ensures safe compliance with the permissible speed profiles and train headways by means of the interface from the ATO-OB to the EVC (fig. 2).

4 Schutz von Schlüsselmaterial

Die Geheimhaltung des sensiblen Schlüssels auf dem Fahrzeug sowie im Stellwerk / RBC wird erreicht, indem dieser nur auf dem zugehörigen Gerät selbst erstellt und gespeichert wird. Die Generierung des Schlüssels muss durch sichere Zufallsgeneratoren erfolgen, um einem Angreifer keinen Rückschluss auf die Beschaffenheit des Schlüssels zu gewähren. Der externe Zugriff auf den privaten Schlüssel muss darüber hinaus über die komplette Lebenszeit verhindert werden [6]. Der europäische Stellwerkstandard EULYNX sieht daher die Generierung und Speicherung der Schlüssel bevorzugt auf einem HSM vor. Die Nutzung eines Trusted Platform Modules (TPM) wird hierfür als nicht mehr ausreichend angesehen. Ein Export oder eine externe Erstellung der Schlüssel ist nicht zulässig. Im Falle einer erkannten Kompromittierung des Schlüssels ist eine sofortige Revozierung des zugehörigen Zertifikats erforderlich. Dies wird über die PKI durchgeführt und unterbindet eine weitere Nutzung des Zertifikats nebst Schlüssel [7].

The commissioning of ATO means that several new IT security functions are to be implemented in the future along with the TSI 2022. They are intended to solve the security weaknesses from ETCS. Within this context, the TSI update refers to:

- the updated message configuration (e.g. the application data's header data) from subset 126 to the new Subset 148
- the updated specification of the encrypted communication via TLS (including PKI functions) from Subset 126 Appendix A (subset 137) to the new subset 146 with:
- the use of a central PKI with a Registration Authority (for checking the authenticity of the subscribers) and a Validation Authority (the validation of the certificates) by means of OCSP (the Online Certificate Status Protocol) and CRL (Certificate Revocation List) respectively.
- the use of the current TLS 1.3 encryption protocol for the encryption of the complete data traffic (or the protection of integrity and authenticity)
- the generation of keys in the end device (not centrally as with the KMC)

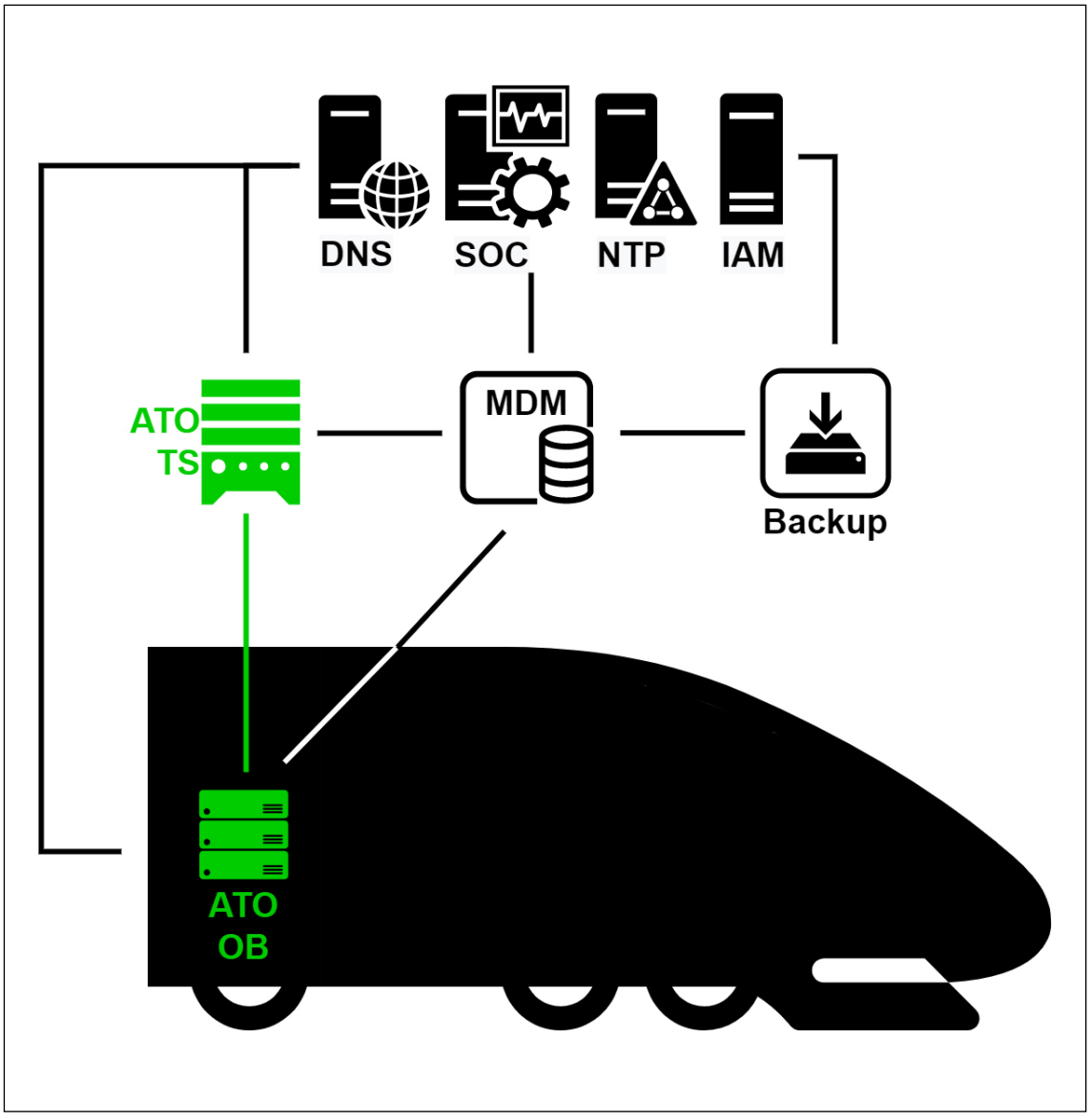

Bild 3: Integration eines MDM und zentraler Dienste in ATO
Fig. 3: The integration of an MDM and central services in ATO

5 Übergreifende Sicherheitsmechanismen

Neben der konkreten Umsetzung von IT-Sicherheitsfunktionen auf den Systemen gehört auch der Aufbau übergreifender (zentraler) Sicherheitsmechanismen zu den notwendigen IT-Security-Funktionen.

5.1 SOC

Zur Erkennung und Reaktion auf Cyber-Angriffe ist der Aufbau eines Security Operation Center (SOC) unumgänglich. Damit das SOC Angriffe erkennen kann, müssen Sensoren an den Netzübergängen wie Firewalls (sogenannte Intrusion Detection Systeme) implementiert sowie Log-Daten der Anwendungen gesammelt werden. Zu den Log-Daten zählen Anwendungs- bzw. Netzwerkereignisse wie, Verbindungsaufbau, Login-Versuche oder das Starten / Beenden von Diensten auf dem System.
Die Kernkomponente ist das Sicherheitsinformations- und Ereignis-Management (SIEM), welches z. B. durch Software wie Splunk oder Elastik realisiert wird. Diese analysieren die Daten auf Anomalien sowie Muster und sorgen durch Reaktoren (z. B. Firewalls und Inhaltsfilter) dafür, dass unerwünschtes Verhalten in Kommunikationsverbindungen und Programmabläufen blockiert oder durch konfigurierte Prozesse zuständiges Personal benachrichtigt wird.
Für das ATO-System ist dabei das Logging der Ereignisse auf Streckenseite wie auf dem Zug wichtig, da hierdurch die Aggregation beider Datenquellen die Angriffserkennung verbessert.

5.2 Maintenance Security

Angriffe auf IT-Systeme lassen sich häufig auf eine fehlende Wartung zurückführen. Während nach der Inbetriebnahme das System noch dem aktuellen Stand der Technik entspricht, können schon kurz danach erste Probleme mit Bezug auf die Security entstehen. Häufig wird hierdurch auf entdeckte Schwachstellen nicht rechtzeitig reagiert. Dies kann einerseits an einem fehlenden Überblick der Softwarestände eingesetzter Systeme liegen. Andererseits verhindern komplexe Wartungsprozesse häufig eine zeitnahe Problemlösung.
Abhilfe schafft die zentrale Verwaltung sämtlicher Softwarestände und Konfigurationen. Die Bündelung dieser und weiterer Aufgaben kann in einem Maintenance and Data Management (MDM)

- the storage of the keys in a secured HSM (Hardware Secure Module)
- the use of a secure random number generator to generate the key material
- the use of current algorithms for encrypting and signing the messages via SHA3, AES and elliptic curves.

4 The protection of key material

The confidentiality of the sensitive key on the vehicle and in the interlocking / RBC is achieved by generating and storing it only on the corresponding device itself. The key must be generated by secure random generators so that an attacker cannot draw any conclusions as to the nature of the key. Furthermore, external access to the private key must be prevented throughout its complete lifetime [6]. The European EULYNX interlocking standard therefore recommends the generation and storage of keys preferably on an HSM. The use of a Trusted Platform Module (TPM) is no longer considered sufficient for this purpose. The export or external generation of the keys is not permitted. If a compromised key is detected, the associated certificate must be revoked immediately. This is performed via the PKI and prevents the further use of the certificate and key [7].

5 Overarching security mechanisms

In addition to the specific implementation of the IT security functions on the systems, the establishment of overarching (central) security mechanisms is also part of the necessary IT security functions.

5.1 SOC

The establishment of a Security Operation Centre (SOC) is essential in order to detect and respond to any cyber-attacks. If the SOC is to detect attacks, sensors must have been implemented at network transitions such as firewalls (known as intrusion detection systems) and the log data from the applications must be collected. Log data includes application or network events such as the establishment of a connection, login attempts or the starting / stopping of services in the system.

erfolgen. Dieses wird bereits im europäischen Standard für Stellwerkstechnik EULYNX [8] eingesetzt und ermöglicht dort die Verwaltung sämtlicher zum Stellwerk gehöriger Elemente.
Die in Bild 3 visualisierte Architektur zeigt die direkte Anbindung von ATO-TS und ATO-OB, welche auch über das Mobilfunknetz erfolgen kann. Durch die Verteilung signierter Konfigurations- und Softwareupdates über verschlüsselte Datenverbindungen wird ein ausreichender Schutz vor Manipulation und Ausspähung gewährleistet. Die zentrale Verwaltung ermöglicht zusätzlich eine Absicherung der Zugänge für technisches Personal mittels eines Identity and Access Managements (IAM). Die Rechte können somit feingranular auf ein notwendiges Minimum beschränkt werden. Das MDM kann zusätzlich über standardisierte Schnittstellen auf die von Herstellern bereitgestellten Aktualisierungen zugreifen, ohne einen direkten Zugriff auf die Systeme zu ermöglichen. Eine Protokollierung der am MDM getätigten Zugriffe gewährleistet zusätzlich Nachverfolgbarkeit.
Mittels des Einsatzes eines Cyber Emergency Response Teams (CERT), welche Informationen über Schwachstellen genutzter Systeme auswertet, kann das MDM effizient zur Sicherheitssteigerung beitragen.

5.3 Europäische Security-Dienste

Die verstärkte Vernetzung der Bahntechnik verbessert die Steuerung des Verkehrsflusses und Effizienzerhöhungen. Zusätzlich erleichtern standardisierte Technologien den grenzüberschreitenden Verkehr erheblich. Grundvoraussetzung hierfür ist eine Etablierung übergreifender Standards, welche die vorgestellten Security Features realisieren. Die hierfür notwendigen Dienste umfassen unter anderem:

- PKI: Zentrale Verwaltung von Zertifikaten zur Etablierung einer sicheren Kommunikation
- Logging: Erfassung von Logdaten zur zentralen Analyse des aktuellen Sicherheitszustand des Gesamtsystems
- Zeitdienst (NTP: Network Time Protocol): Einheitliche Zeitquelle, welche eine Basis für das Logging und die Prüfung von Zertifikatsgültigkeiten darstellt
- DNS (Domain Name System): Verzeichnis zur Übersetzung von Domainnamen in IP-Adressen
- Identity and Access Management (IAM): Vergabe von Autorisierungen an menschliche Nutzer und für Maschine-zu-Maschine-Kommunikation

Die Grundlage für die sogenannten Shared Security Services hat Baseline 4 Release 1 des stellwerksseitigen Projekts EULYNX gelegt [7].
Um Doppelstrukturen bei Betreibern zu verhindern und eine europäische Standardisierung dieser Dienste zu ermöglichen, ist ein projektübergreifender Austausch notwendig. Aus diesem Grund arbeiten die Security-Gremien von EULYNX, RCA, OCORA und der ERTMS Security Core Group zusammen, um einheitliche Security-Services zu definieren. Essenziell ist hierbei die Berücksichtigung eines betreiber- und grenzübergreifenden Datenaustauschs. Hierdurch soll sowohl der intereuropäische Verkehr mittels ATO und ETCS als auch die Kommunikation von Fahrzeug- und Stellwerkssystemen vereinfacht werden. Diese Angleichung der notwendigen zentralen Dienste wird zusätzlich in einer Ressourceneinsparung durch die Beseitigung von Doppelstrukturen resultieren. Die Automatisierung des grenzüberschreitenden Zugverkehrs wird hierdurch angestrebt.
Shared Services auf europäischer Ebene helfen Vertrauensbeziehungen zwischen verschiedenen am automatischen Bahnverkehr beteiligten Unternehmen herzustellen. Die PKI kann zu-

The core component is the security information and event management (SIEM), which is implemented by software such as Splunk or Elastik. These analyse the data for any anomalies as well as patterns and ensure that any undesirable behaviour in the communication and program flows is blocked using reactors (e.g. firewalls and content filters) or that the responsible personnel are notified using the configured processes.
The logging of events trackside as well as on the train is important for the ATO system, because the aggregation of both data sources improves the attack detection.

5.2 Maintenance security

Attacks on IT systems can often be traced back to a lack of maintenance. While the system is still state of the art after commissioning, the first security problems can arise shortly thereafter. This often results in a lack of a timely reaction to any discovered vulnerabilities. On the one hand, this can be due to a lack of an overview of the software statuses in the deployed systems. On the other hand, complex maintenance processes often prevent timely problem resolution.
This can be remedied by means of the central administration of all the software statuses and configurations. These and other tasks can be bundled into a maintenance and data management (MDM) system. This is already used in the European EULYNX standard for interlocking technology [8], where it enables the management of all the elements belonging to the interlocking.
The architecture visualized in fig. 3 shows a direct connection between ATO-TS and ATO-OB, which can also take place via a mobile network. The distribution of signed configuration and software updates via encrypted data connections ensures sufficient protection against manipulation and spying. Central administration additionally secures the access of any technical personnel by means of identity and access management (IAM). The rights can thus be limited to a necessary minimum on a fine-granular basis. The MDM can additionally access updates provided by the manufacturers via standardised interfaces without providing any direct access to the systems. The logging of the accesses performed by the MDM ensures additional traceability.
The MDM can contribute to efficiently increasing security by establishing a Cyber Emergency Response Team (CERT) that evaluates the information about any vulnerabilities in the systems in use.

5.3 European security services

The increased interconnection of rail technology improves traffic flow management and efficiency gains. In addition, standardised technologies facilitate cross-border traffic considerably. The basic requirement for this is the establishment of overarching standards that implement the presented security features. The services required for this include:

- PKI: the central administration of certificates to establish secure communication
- logging: the collection of log data for the central analysis of the overall system's current security status
- a time service (NTP: Network Time Protocol): a uniform time source that provides the basis for logging and checking certificate validity
- a DNS (Domain Name System): a directory for translating the domain names into IP addresses
- Identity and Access Management (IAM): the allocation of authorisations to human users and for machine-to-machine communication.

künftig beispielsweise pro Betreiber digitale Zertifikate und kryptographische Schlüssel für ATO verwalten. Dies ermöglicht eine abgesicherte Kommunikation zwischen den fahrzeug- und infrastrukturseitigen Systemen. Im Umfang einzelner und regionaler ATO-Projekte kann hierbei noch eine zentralisierte Lösung eines Infrastrukturbetreibers angestrebt werden. Spätestens ab der Überschreitung der Landesgrenze müssen gegenseitige, digitale Vertrauensbeziehungen gewährleistet werden. Hierzu können PKI beispielsweise durch gegenseitige Akzeptanz eines Vertrauensankers (Cross-Signing) oder Schaffung gemeinsamer zentraler Stellen (Bridge-CA oder gemeinsame Root-CA) verknüpft werden [9].

Eine weitere Herausforderung, die eine europäische Standardisierung erfordert, ist die Auswertung von Logdaten. Dazu ist nicht nur eine Zusammenführung der Logdaten in einem gemeinsamen SIEM erforderlich. Zusätzlich müssen beim grenzübergreifenden Verkehr einheitliche Regeln zur Erfassung dieser Daten und eine jeweils verantwortliche zentrale Stelle definiert werden. Nur unter dieser Voraussetzung können Anomalien im Betrieb des ATO-Systems ermittelt und entsprechende Gegenmaßnahmen eingeleitet werden.

The basis for any so-called shared security services has been laid out by Baseline 4 Release 1 for the EULYNX interlocking-side project [7].

A cross-project exchange is necessary in order to prevent any duplicate structures at operators and to enable the European standardisation of these services. For this reason, the EULYNX, RCA and OCORA security groups and the ERTMS Security Core Group are working together to define uniform security services. It is essential to take into account both cross-operator and cross-border data exchange within this context. This is intended to simplify both inter-European traffic using ATO and ETCS and the communication between the vehicle and interlocking systems. This harmonisation of the necessary central services will additionally result in resource savings through the elimination of any duplicate structures. The aim is to automate cross-border train traffic.

Shared services at a European level will help establish trust relationships between the different companies involved in automated rail traffic. In the future, the PKI will be able to manage digital certificates and cryptographic keys for ATO per operator, for example. This will enable secure communication be-

6 Fazit

Die Umsetzung der aktualisierten Technischen Spezifikationen wie TLS-verschlüsselte Ende-zu-Ende-Kommunikation sowie die stetige Weiterentwicklung der Security-Anforderungen durch die ERTMS Security Core Group sichern das Bahnsystem vor den wachsenden Cyber-Bedrohungen ab. Die Etablierung moderner Sicherheitsmechanismen ist dabei entscheidend, um das IT-Security-Niveau auf dem aktuellen Stand der Technik zu halten. Dazu gehört der Einsatz standardisierter Schnittstellen, zentraler Dienste wie PKI, SOC und MDM sowie die grundlegende Entwicklung nach etablierten Security-Normen. ■

tween the vehicle and the infrastructure systems. A centralised solution from an infrastructure operator can still be envisaged here on the scale of individual and regional ATO projects. Mutual, digital trust relationships must have been secured by the time the national border is crossed at the latest. To this end, PKI can be linked, for example, through the mutual acceptance of a trust anchor (cross-signing) or the creation of common central authorities (bridge CA or common root CA) [9].
Another challenge that requires European standardisation is the evaluation of the log data. This not only requires the merging of log data into a common SIEM. In addition, uniform rules for the collection of this data and a responsible central authority in each case must also be defined in the case of cross-border traffic. Any anomalies in the ATO system's operations can only be identified and the appropriate countermeasures initiated under these conditions.

6 Conclusion

The implementation of updated technical specifications such as TLS-encrypted end-to-end communication, as well as the continuous development of security requirements by the ERTMS Security Core Group, secures the railway system against growing cyber threats. The establishment of modern security mechanisms is crucial in order to maintain the IT security level at the current state of the art. This includes the use of standardised interfaces, centralised services such as PKI, SOC and MDM and fundamental development according to established security standards. ■

LITERATUR | LITERATURE

[1] CYRAIL, „CYRail Recommendations on cybersecurity of rail signaling and communication," https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf, 2018
[2] ERTMS/ETCS, „EuroRadio FIS – SUBSET-037," UNISIG, 2015
[3] Chothia, T.; Ordean, M.; De Ruiter, J.; Thomas, R. J.: „An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols," Asia Conference on Computer and Communications Security, 2017
[4] Pépin, F.; Vigliotti, M. G.: „Risk Assessment of the 3Des in ERTMS," RSSRail, 2016
[5] De Ruiter, J.; Thomas, R. J.; Chothia, T.: „A Formal Security Analysis of ERTMS Train to Trackside Protocols," Lecture Notes in Computer Science, 2016
[6] Federal Office for Information Security, „Key Lifecycle Security Requirements, Version 1.0.3," 2021
[7] EULYNX Consortium, Eu.Doc.114 – EULYNX Security Specification, BL4R1 ed., 2022
[8] EULYNX Consortium, Eu.Doc.18 – Maintenance and data management specification, BL4R1 ed., 2022
[9] Drodt, M.; Heinrich, M.: „IT Security bei ETCS," AG CYSIS, 2019

AUTOREN | AUTHORS

Dr. Martin Koop
Senior Expert IT-Security
INCYDE GmbH
Anschrift / *Address*: Schaumainkai 91, D-60596 Frankfurt am Main
E-Mail: martin.koop@incyde.com

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

BIM-Software für LST-Planung

Automatisch sicherer ans Ziel

Die Highlights von ProVI LST

- **Vollständige Planung der Leit- und Sicherungstechnik:** Weichen, Signale, Gleisfreimeldung, Fahrstraßenlogik, Flankenschutz und punktförmige Zugbeeinflussung
- Automatische Generierung von Achszählpunkten, Gleismagneten und Fahrstraßen
- Integration der Leit- und Sicherungstechnik in den Gesamtkontext der Planung

Noch Fragen? Rufen Sie uns an +49 89 57 99 – 700

// ENTWICKELT VON INGENIEUREN FÜR INGENIEURE

„In der LST-Planung ist oft die Ausnahme die Regel – es gibt selten den einen, einheitlichen Weg. ProVI LST bietet dort, wo es geht, praktische Automatismen an. Das macht die Planung deutlich schneller und ist ein echtes Alleinstellungsmerkmal."

Matthias Frei, Principal Software Engineer bei ProVI

ProVI

Verkehr und Infrastruktur planen

www.provi-cad.de