Automatisiertes Security-Risikomanagement für Züge

Automated security risk management for trains

Patric Birr | Stefan Karg

Security spielt bei der Entwicklung und Wartung von modernen, vernetzten Schienenfahrzeugen eine immer wichtigere Rolle. Digitale Zwillinge ermöglichen eine präzise und ganzheitliche Modellierung dieser Systeme und bilden die Grundlage für automatisierbare Security-Risikoanalysen. Diese Analysen identifizieren systematisch Sicherheitslücken und bewerten potenzielle Angriffspfade. Tägliche Aktualisierungen der Risikoanalysen und effiziente Maßnahmendefinition ermöglichen kontinuierliche Security und Zuverlässigkeit der Fahrzeuge über ihren gesamten Lebenszyklus hinweg.

1 Motivation

Moderne Schienenfahrzeugarchitekturen bestehen aus komplexen Netzwerken mit Komponenten aus dem OT- sowie zunehmend aus dem IT-Bereich. Neben den mechanischen und elektronischen Komponenten des Systems kommt so eine Ebene hinzu, die die Komplexität eines modernen Schienenfahrzeugs deutlich erhöht [1] und neue Risiken für die Security mit sich bringt. Des Weiteren erfordern zeitgemäße Technologien wie Predictive Maintenance eine Anbindung des Fahrzeugs an die Außenwelt, die gegenüber dem herkömmlichen Zugfunk neue Angriffsvektoren eröffnet.

Zeitgleich mit der zunehmenden Vernetzung und Komplexität von Schienenfahrzeugen nimmt auch die allgemeine Bedrohungslage zu. Auf beide Entwicklungen reagieren die Gesetzgeber mit regulatorischen Verschärfungen. Europäische Regulierungen wie NIS2 (Artikel 21, [2]) oder der CRA (Artikel 13, [3]) fordern von Betreibern und Herstellern die Durchführung von regelmäßigen Security-Risikoanalysen. Normativ werden Schienenfahrzeuge durch die CENELEC TS 50701 [4] abgedeckt, die jene bahnspezifischen Aspekte ergänzt, die dem zugrundeliegenden Standard IEC 62443 [5] fehlen, der allgemein für industrielle Automatisierungssysteme gilt. Auch hier steht die Ganzheitlichkeit der Security-Risikoanalyse im Fokus, siehe Fig. 5 in [4].

Um im Rahmen der Security-Risikoanalyse ein möglichst realistisches Gesamtbild der Risiken des Schienenfahrzeugs zu erhalten, müssen systematisch die Angriffsmöglichkeiten analysiert werden. Diese Bewertung muss über den Lebenszyklus des Schienenfahrzeugs kontinuierlich aktualisiert werden. Gründe für eine notwendige Aktualisierung können in Änderungen am Schienenfahrzeug begründet sein oder dadurch, dass sich die Bedrohungslage ändert, beispielsweise durch neue Angriffsmöglichkeiten auf eine bisher sicher geglaubte Technologie.

Zumeist wird dieser Schritt derzeit manuell vorgenommen, beispielsweise in Form einer Excel-Tabelle. Die sehr hohe Komplexität von Schienenfahrzeugen erschwert bis verunmöglicht hierbei die manuelle Betrachtung aller Angriffsszenarien auf alle Systeme in Fahrzeugen und bringt einen hohen Aufwand bei der Aktualisierung mit sich.

Security is playing an increasingly important role in the development and maintenance of modern, connected rail vehicles. Digital twins enable the precise and holistic modelling of these systems and form the basis for automatic Security Risk Assessments. These assessments systematically identify any security vulnerabilities and evaluate potential attack paths. Daily updates of the risk assessments and efficient countermeasure definition ensure the continuous security and reliability of the vehicles throughout their entire lifecycle.

1 Motivation

Modern rail vehicle architectures consist of complex networks with components from both OT and IT. In addition to the system's mechanical and electronic components, this also adds a layer that significantly increases the complexity of a modern rail vehicle [1] and introduces new security risks. Furthermore, contemporary technologies such as predictive maintenance require the vehicle to be connected to the outside world, which opens up new attack vectors when compared to conventional train radio.

The general threat landscape is also growing along with the increasing connectivity and complexity of rail vehicles. Legislators have responded to both developments with stricter regulations. European regulations such as NIS2 (Article 21, [2]) or the CRA (Article 13, [3]) require operators and manufacturers to conduct regular Security Risk Assessments. Rail vehicles are normatively covered by CENELEC TS 50701 [4], which complements the rail-specific aspects missing in the underlying IEC 62443 standard [5] that generally applies to industrial automation systems. Here, too, the focus is on the holistic nature of the Security Risk Assessment: see fig. 5 in [4].

The attack vectors must be systematically analysed in order to obtain a realistic overview of the rail vehicle's security risks within the Security Risk Assessment. This assessment must be continuously updated throughout the lifecycle of the rail vehicle. The reasons for a necessary update may include changes to the rail vehicle or to the threat landscape, such as new attack vectors pertaining to technology previously considered secure.

Currently, this step is mostly performed manually, for example in the form of an Excel spreadsheet. The very high complexity of the rail vehicle makes it difficult, if not impossible, to manually consider all the attack scenarios on all the vehicle's systems, resulting in high update efforts.

One possible approach is to simplify or generalise the considered attack scenarios to a manually manageable level. However, this generalisation carries the risk of underestimating the risks or overlooking attack vectors.

Eine mögliche Herangehensweise ist die Vereinfachung oder Verallgemeinerung der betrachteten Angriffsszenarien auf ein manuell handhabbares Maß. Diese Verallgemeinerung birgt allerdings die Gefahr, Risiken zu unterschätzen oder Angriffsvektoren zu übersehen.
Stattdessen ist sicherzustellen, dass durch einen ganzheitlich definierten Betrachtungsumfang die Security-Risikoanalyse alle relevanten Sicherheitslücken identifiziert und bewertet. Diese inkludieren neben technischen Schwachstellen auch organisatorische Mängel und Aspekte der physikalischen Infrastruktur.
Die Automatisierung der Risikoanalysen ist eine effiziente Möglichkeit, unzulässige Vereinfachungen zu vermeiden und konkrete Schwachstellen auch mit konkreten Maßnahmen zu adressieren.

2 Ganzheitliche Digitale Zwillinge

Ideale Grundlage für eine automatisierte Security-Risikoanalyse ist ein Digitaler Zwilling des Schienenfahrzeugs. Die Bedeutung Digitaler Zwillinge wächst kontinuierlich in der Bahnindustrie [6]. Unter einem Digitalen Zwilling wird im Rahmen dieses Beitrags ein digitales Modell des realen Systems verstanden. Dieses Modell geht weit über eine rein schematische Abbildung des Schienenfahrzeugs hinaus. Neben Komponenten und deren Verbindungen sind alle für die Security relevanten Eigenschaften aller Objekte im Digitalen Zwilling hinterlegt.
Diese möglichst vollständige digitale Modellierung des Schienenfahrzeugs beinhaltet zu jeder Komponente auch deren Verortung im Gesamtsystem. Dies erleichtert zwar die Orientierung im Digitalen Zwilling, denn die Komponenten sind so im Modell hinterlegt, wie sie in der Realität verbaut sind. Wichtiger ist jedoch der Einfluss des physikalischen Schutzes einer Komponente auf die Security-Risikoanalyse. Befindet sich beispielsweise ein Steuergerät in einem abschließbaren Schaltschrank im Führerstand, so wird sowohl der Schaltschrank als auch die Tür zum Führerstand mit den für die Security relevanten Eigenschaften modelliert. Dazu gehören insbesondere die verbauten Zutrittskontrollmechanismen. Durch diese Zuordnung ist es möglich, in der automatisierten Security-Risikoanalyse auch die physikalischen Schutzmaßnahmen mit einzubeziehen, die ein Angreifer überwinden muss, bevor er eine Komponente direkt manipulieren kann. Ein Beispiel für den Digitale Zwilling eines Schienenfahrzeugs ist in Bild 1 dargestellt.
Die initiale Erstellung des Modells kann auf unterschiedliche Arten erfolgen. Grundlage könnte beispielsweise ein durchgeführter Penetrationstest sein. Aus den Ergebnissen von Discovery Scans und Enumeration Scans können die Komponenten, deren Verbindungen und die für die Security relevanten Eigenschaften weitestgehend automatisch ausgelesen werden. Eine andere Grundlage könnte ein Assetmanagementsystem sein, in dem die Daten in strukturierter Form maschinenlesbar vorliegen. Aus diesen unterschiedlichen Quellen können Komponenten oder Verbindungen in den Digitalen Zwilling importiert werden.
Ist kein Assetmanagementsystem mit geeigneter Schnittstelle verfügbar und ein Discovery Scan oder Enumeration Scan nicht möglich, besteht auch die Möglichkeit, den Digitalen Zwilling auf Basis von importieren Excel-Dateien, Dokumenten oder in Zusammenarbeit mit Fachexperten zu modellieren. Dieser Ansatz ist insbesondere in Entwicklungsprojekten relevant, wo das reale System zum Zeitpunkt der Risikoanalyse noch nicht existiert. Im Vergleich zur schnittstellenbasierten Modellierung entstehen allerdings höhere manuelle Aufwände.
Lassen sich auch durch diesen Ansatz die Security-Eigenschaften von Bestandteilen des Schienenfahrzeugs nicht vollständig bestimmen, beispielsweise weil der Hersteller eine dieser Eigenschaften

Instead, it should be ensured that the Security Risk Assessment identifies and evaluates all the relevant security vulnerabilities using a holistically defined scope. These vulnerabilities include not only technical weaknesses, but also organisational deficiencies and aspects of the physical infrastructure.
Risk assessment automation is an efficient way of avoiding simplifications and of addressing specific vulnerabilities with specific countermeasures.

2 Holistic digital twins

A digital twin of the rail vehicle constitutes an ideal basis for an automated Security Risk Assessment. The importance of digital twins is continuously growing in the railway industry [6]. Within the context of this article, a digital twin is understood to mean a digital model of a real system. This model goes far beyond a purely schematic representation of the rail vehicle. In addition to the components and their connections, the digital twin also includes all the security-relevant properties of all the objects.
This digital modelling of the rail vehicle, which is as complete as possible, includes the location of each component within the overall system. On the one hand, this facilitates the orientation within the digital twin, as the components are located in the model as they are installed in reality. A more important factor, however, involves how the physical protection of a component influences the Security Risk Assessment. For example, if a control unit is located in a lockable cabinet in the driver's cab, both the cabinet and the door to the driver's cab are modelled with the security-relevant properties. This includes the installed access control mechanisms in particular. With this information integrated into the model, the automated Security Risk Assessment can now include the physical countermeasures that an attacker must overcome before being able to directly manipulate a component. Fig. 1 depicts an example of a digital twin of a rail vehicle.
The model can initially be created using various methods. One basis could involve a performed penetration test. The components, their connections and the security-relevant properties can be sorted automatically as far as possible based on the results of the discovery and enumeration scans. Another basis could involve an asset management system where the data is available in a structured, machine-readable form. The components or connections can be imported into the digital twin from these different sources.
If no asset management system with a suitable interface is available and a discovery scan or enumeration scan is not possible, it is also possible to model the digital twin on the basis of imported Excel files and documents or in collaboration with subject matter experts. This approach is particularly relevant in development projects, as the real system does not yet exist at the time of the risk assessment. However, higher manual efforts are required compared to interface-based modelling.
If the security properties of the rail vehicle's components cannot be fully determined even using this approach, for example because the manufacturer has not made one of these properties public, conservatively chosen standard values from a component library can be used at these points.
In addition to the components and systems installed in the rail vehicle, the connection of these systems to each other also plays a crucial role in the Security Risk Assessment. Interfaces

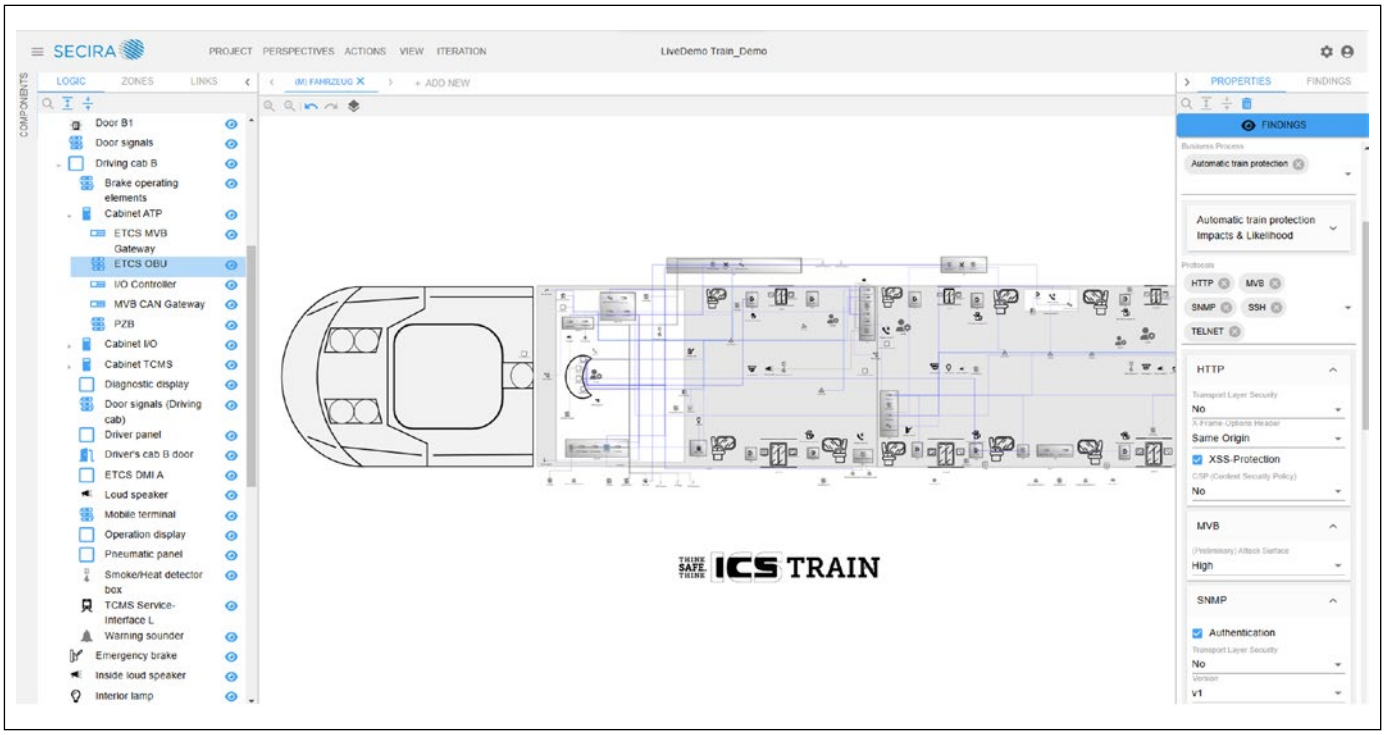

Bild 1: Digitaler Zwilling eines Schienenfahrzeugs
Fig. 1: A digital twin of a rail vehicle

nicht öffentlich macht, so können an diesen Stellen konservativ gewählte Standardwerte aus einer Komponentenbibliothek hinterlegt werden.

Neben den im Schienenfahrzeug verbauten Komponenten und Systemen spielt die Verbindung dieser Systeme untereinander für die Bewertung der Security eine entscheidende Rolle. Schnittstellen zwischen Systemen können unterschiedliche Formen annehmen, von analogen Signalen über Bussysteme bis hin zu einer Ethernetverbindung. Die verschiedenen Schnittstellen sind für Angreifer unterschiedlich gut manipulierbar. Die Verbindungen zwischen den Systemen sind unter Berücksichtigung dieser Vielfalt zu modellieren und in der Security-Risikoanalyse automatisiert zu bewerten. Hierzu gehören auch Netzwerkstrukturen und die Netzwerksegmentierung beispielsweise über unterschiedliche VLAN (Virtual Local Area Networks).

Moderne Schienenfahrzeuge werden üblicherweise auf Basis einer einheitlichen Plattform als Flotten oder Baureihen für die einzelnen Endkunden angepasst. Aus einem generischen Digitalen Zwilling der einheitlichen Plattform lassen sich durch adaptierte Vervielfältigungen des Modells alle konkreten Ausprägungen der kundenspezifischen Fahrzeuge ableiten. Im fahrzeugspezifischen Zwilling müssen dann nur noch die Komponenten angepasst oder ausgetauscht werden, die von der einheitlichen Plattform abweichen.

Entscheidend für die anhaltende Korrektheit von automatisierten Security-Risikoanalysen ist die regelmäßige Aktualisierung des Digitalen Zwillings und die darauffolgende Neubewertung. Durch einen schnittstellenbasierten Datenabgleich zwischen dem Digitalen Zwilling und dem Netzwerk des realen Systems lässt sich diese Aktualität sicherstellen. Ein direkt im Schienenfahrzeug integriertes Intrusion Detection System (IDS) oder eine Configuration Management Database (CMDB) sind hierfür die optimalen Lösungen.

Wird beispielsweise im realen Netzwerk durch das IDS eine neue Komponente oder ein neues Protokoll erkannt, das im aktuellen Digitalen Zwilling nicht modelliert ist, muss die Diskrepanz durch Ak-

between systems can take different forms, ranging from analogue signals to bus systems to an Ethernet connection. The various interfaces differ in how easily they can be manipulated by an attacker. The connections between the systems must be modelled while taking this diversity into consideration and they will be automatically evaluated in the Security Risk Assessment. This also includes network structures and network segmentation, for example, via different VLAN (Virtual Local Area Networks).

Modern rail vehicles are usually adapted as a fleet or class for individual end customers based on a uniform platform. All the specific manifestations of the customer-specific vehicles can be derived from a generic digital twin of the uniform platform using adapted duplications of the model. In the vehicle-specific twin, only those components that deviate from the uniform platform need to be adjusted or replaced.

The regular updating of the digital twin and the subsequent re-evaluation are crucial for the continued correctness of the automated Security Risk Assessments. This up-to-dateness can be ensured using interface-based data reconciliation between the digital twin and the real system network. An Intrusion Detection System (IDS) or a Configuration Management Database (CMDB) integrated directly into the rail vehicle are the optimal solutions for this purpose.

For example, if the IDS detects a new component or protocol in the real network that has not been modelled in the digital twin, the discrepancy must be resolved by updating the digital twin. Similarly, the digital twin and the associated risk assessment will align once the CMDB dataset reflects the updated software or firmware versions.

If the digital twin contains all the security-relevant information about the system, an automated Security Risk Assessment can generate a daily current assessment of the rail vehicle's security risks.

tualisierung im Digitalen Zwilling aufgelöst werden. Analog dazu würden sich gemäß des CMDB Datensatzes nach Aktualisierung von Software- oder Firmware-Versionen der Digitale Zwilling und die dazugehörige Risikobewertung angleichen.
Sofern alle für die Security relevanten Informationen zum System im Digitalen Zwilling enthalten sind, lässt sich durch Automatisierung der Security-Risikoanalyse täglich eine aktuelle Bewertung der Risiken des Schienenfahrzeugs generieren.

3 Automatisierte Security-Risikoanalyse

Security-Risikoanalysen lassen sich durch einen intelligenten Algorithmus automatisieren, der auf Basis aller im Digitalen Zwilling modellierten Objekteigenschaften und Sicherheitslücken die möglichen Angriffspfade identifiziert und in einer Angriffsbaumanalyse (Bild 2) zusammenführt. Die automatisiert hergeleiteten Angriffssequenzen sind dabei auf die sog. „essential functions" des Systems ausgerichtet, also Funktionen wie die Bremssteuerung und die Zugsicherung. Wie wichtig die jeweiligen Funktionen und Prozesse für die Sicherheit und den Betrieb des Schienenfahrzeugs sind und welche Komponenten durch ihren Beitrag zur Funktionalität als sog. „critical assets" zu deklarieren sind, ist vorab im Digitalen Zwilling zu dokumentieren. Diese Kritikalität von Komponenten wird entlang der Security-Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit differenziert, sodass im Angriffsbaum Manipulationsversuche, bewusst herbeigeführte Störungen und Vertraulichkeitsverletzungen separat bewertet werden können.
Die oberen Ebenen des automatisiert erstellten Angriffsbaums beschreiben auf Basis dieser Zuordnungen, welche „essential functions" durch Angriffe auf „critical assets" kompromittiert werden können und wie kritisch erfolgreiche Angriffe jeweils wären.
Die für eine Risikobewertung jeder Bedrohung notwendige Einschätzung der Eintrittswahrscheinlichkeit ist aus der Identifikation und Zusammenführung aller möglichen Angriffspfade zu ermitteln. Die einzelnen Angriffspfade ergeben sich dabei aus einer Sequenz von Angriffsschritten, die wiederum jeweils die Ausnutzung einer Sicherheitslücke repräsentieren.
Die Wahrscheinlichkeit eines erfolgreichen Angriffsschritts ist aus Angreiferperspektive durch erfahrene Offensive-Security-Experten zu definieren, und aktuelle Erkenntnisse aus dem „threat monitoring" (Überwachung der Bedrohungslandschaft) müssen berücksichtigt werden. Entscheidend ist bei der Bewertung, welche Tools und etablierten Methoden es gibt bzw. wie verfügbar diese für einen Angreifer sind. Oft ergibt sich aus dieser Betrachtung, wie komplex und aufwendig eine Angriffssequenz ist.
Wird beispielsweise in einschlägigen Deep-Web-Foren oder im Darknet ein Werkzeug angeboten, das neue Angriffsmöglichkeiten eröffnet oder bestehende deutlich erfolgsversprechender werden lässt, so müssen die Bewertungen der Eintrittswahrscheinlichkeiten angepasst werden. Dieses „threat monitoring" ist ein kontinuierlicher Prozess, der durch dedizierte Teams durchgeführt werden sollte. Die Erkenntnisse dieser Überwachung sollten in einem zentralen Bedrohungskatalog (engl. threat library) gepflegt werden, sodass künftige Risikobewertungen auf diesem Stand aufsetzen können.
Basis für die Herleitung möglicher Angriffsschritte ist einerseits ein Abgleich der Security-Eigenschaften von Objekten mit dem sogenannten „best practice", der beispielsweise durch internationale Standards wie [7], durch das BSI (unter anderem kryptographische Schlüssellängen in [8]) und durch das „Center for Internet Security" (CIS, [9]) definiert wird. Im Sinne der ganzheitlichen Bewertung inkludieren derartige Abgleiche sowohl den physikalischen Schutz von Komponenten als auch deren Konfiguration der Dienste und Protokolle.

3 Automated Security Risk Assessment

Security Risk Assessments can be automated using an intelligent algorithm that identifies any possible attack paths based on all the object properties and vulnerabilities modelled in the digital twin and consolidates them into an attack tree analysis (fig. 2). The automatically derived attack sequences are focused on the system's so-called "essential functions", such as brake control and train protection. The importance of the respective functions and processes for the safety and operation of the rail vehicle, in addition to the components that should be declared "critical assets" due to their contributions to the functionality, must be documented in the digital twin in advance. This component criticality is differentiated in line with the security protection goals of integrity, availability and confidentiality, so that any manipulation attempts, deliberately induced disruptions and confidentiality breaches can be evaluated separately in the attack tree.
The upper levels of the automatically created attack tree use these assignments to describe which "essential functions" can be compromised by attacks on "critical assets" and how critical any successful attacks would be.
The assessment of the likelihood necessary for a risk assessment of each threat is to be determined from the identification and consolidation of all the possible attack vectors. The individual attack vectors result from a sequence of attack steps, each representing the exploitation of a vulnerability.
The likelihood of a successful attack step has to be defined from the attacker's perspective by experienced offensive security experts and the current "threat monitoring" findings must be taken into account. The decisive factor in the assessment is which tools and established methods are available or how accessible they are to an attacker. This consideration often reveals how complex and time-consuming an attack sequence is. For example, if a tool is offered in relevant deep web forums or on the darknet, this opens up new attack possibilities or makes existing ones significantly more promising, meaning that the assessments of the likelihood of occurrence must be adjusted. This "threat monitoring" is a continuous process that should be carried out by dedicated teams. The findings from this monitoring should be maintained in a central threat library in order to support any future risk assessments with this knowledge.
The basis for deriving the possible attack steps involves a comparison of the security properties of objects with so-called "best practices" defined, for example, by international standards such as [7], by the BSI (including the cryptographic key lengths in [8]) and by the "Centre for Internet Security" (CIS, [9]). In the sense of a holistic assessment, such comparisons include both the physical protection of components and their service and protocol configurations.
The second essential aspect for identifying attack vectors is a comparison of the software used by each component with the established vulnerability databases, particularly the "National Vulnerability Database" (NVD, [10]) and the underlying CVE database [11] of the MITRE Corporation. Queries on any publicly known vulnerabilities can be generated from the information stored in the digital twin.
How relevant any inadequate security configurations, outdated locking mechanisms or identified vulnerabilities are for the security of the rail vehicle is determined by the Security Risk Assessment for the overall system. This can, for example, re-

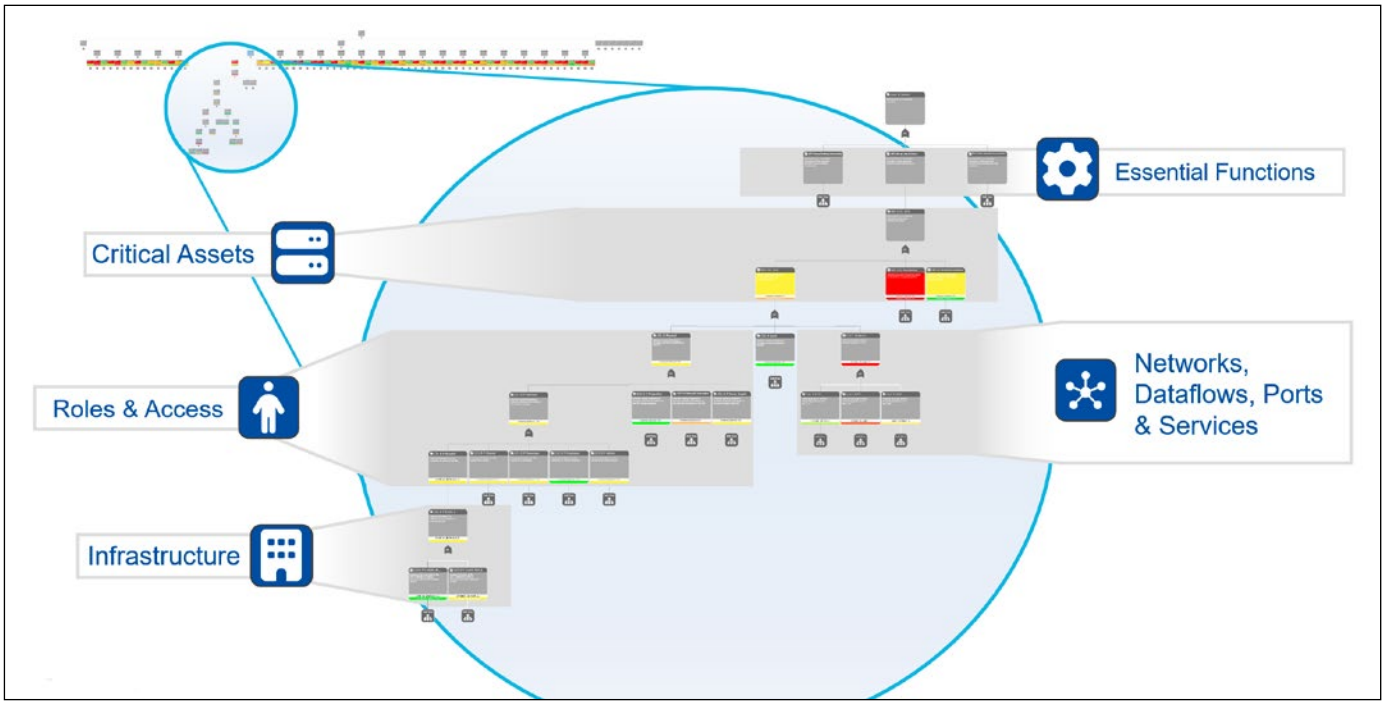

Bild 2: Ganzheitliche automatisierte Angriffsbäume
Fig. 2: Holistic automated attack trees

Der zweite wesentliche Aspekt für die Identifikation von Angriffsvektoren ist ein Abgleich der eingesetzten Software jeder Komponente mit etablierten Datenbanken für Schwachstellen (engl. vulnerabilities), insbesondere mit der „National Vulnerability Database" (NVD, [10]) und der zugrundeliegenden CVE-Datenbank [11] der MITRE Corporation. Aus den im Digitalen Zwilling hinterlegten Informationen lassen sich Abfragen erzeugen, die öffentlich bekannte Schwachstellen zurückliefern.
Wie relevant mangelhafte Security-Konfigurationen, veraltete Schließmechanismen oder identifizierte Schwachstellen für die Security des Schienenfahrzeugs sind, ergibt sich erst aus der Security-Risikoanalyse für das Gesamtsystem. Diese kann beispielsweise ergeben, dass eine ohne Kenntnis des Systemkontexts als kritisch bewertete Schwachstelle einer Komponente im realen System durch Netzwerksegmentierung gar nicht ausnutzbar wäre.
Auch der Angreifertyp ist für die Bewertung von Eintrittswahrscheinlichkeiten entscheidend. Eine Differenzierung der Angreifertypen sollte die Kategorisierung der ISA/IEC 62443 [5] nutzen, sodass die automatisierte Security-Risikoanalyse eine Aussagekraft zur Widerstandsfähigkeit des Schienenfahrzeugs z. B. gegen einen „Security Level 3 Angreifer" liefert.

4 Maßnahmen

Ergibt sich aus der automatisierten Security-Risikoanalyse auf Basis des aktuellen Systems Handlungsbedarf, da bestimmte Risiken über der definierten Akzeptanzschwelle liegen, so müssen Gegenmaßnahmen definiert werden.
Gegenmaßnahmen können unterschiedlich ausgestaltet sein. Zum einen können die für die Security relevanten Eigenschaften einer Komponente geändert werden. Beispielsweise wird anstelle einer unverschlüsselten http-Verbindung eine TLS-verschlüsselte https-Verbindung verwendet. Weitere Gegenmaßnahmen können in einem verbesserten physikalischen Schutz einer Komponente bestehen, indem beispielsweise die die Komponente schützende

veal that a vulnerability in a component rated as critical without any knowledge of the system context would not be exploitable in the real system due to the network segmentation.
The type of attacker is also crucial when assessing the likelihood. The differentiation of attacker types should use the ISA/IEC 62443 categorisation [5], so that the automated Security Risk Assessment can provide meaningful information on the resilience of the rail vehicle, e.g. against a "Security Level 3 attacker".

4 Countermeasures

If the automated Security Risk Assessment based on the current system indicates a need for any action, because certain risks exceed the tolerable risk, countermeasures must be defined.
Countermeasures can take various forms. On the one hand, the security-relevant properties of a component can be changed. For example, a TLS-encrypted HTTPS connection can be used instead of an unencrypted HTTP connection. Further countermeasures can consist of the improved physical protection of a component, for example, by protecting the maintenance flap that shields the component not only with a square key, but also with a lock with a locking cylinder. Additional so-called "compensating countermeasures" can be added if direct protective measures on the component itself are not possible. These are often organisational by nature.
The measures that most efficiently mitigate the overall risk to the system can be derived over the course of automated attack tree creation. Essentially, the countermeasure allocation priority results from the contribution of an object to many or to critical attack sequences.
Since the digital twin not only contains the components, but also their location in the rail vehicle (such as the control cabinets or the driver's cab), any protective measures on these el-

Wartungsklappe nicht nur durch einen Vierkant, sondern durch ein Schloss mit Schließzylinder geschützt wird. Weitere sogenannte „compensating countermeasures" können ergänzt werden, wenn direkte Schutzmaßnahmen an der Komponente selbst nicht möglich sind. Diese sind oft organisatorischer Natur.

Welche Maßnahmen möglichst effizient das Gesamtrisiko des Systems mitigieren, lässt sich im Zuge der automatisierten Angriffsbaumerstellung herleiten. Dabei ergibt sich im Wesentlichen aus dem Beitrag eines Objektes zu vielen oder kritischen Angriffssequenzen die Priorität der Maßnahmenzuordnung.

Da der Digitale Zwilling nicht nur die Komponenten, sondern auch deren Verortung im Schienenfahrzeug wie beispielsweise Schaltschränke oder den Führerstand abbildet, wirken sich Schutzmaßnahmen an diesen Elementen automatisch auf mehrere Komponenten aus. So senkt beispielsweise eine höhere Widerstandsklasse eines Schaltschranks das Risiko für sämtliche im Schaltschrank verbauten Komponenten. Analog dazu wirkt sich das Verbauen eines elektronischen Schlosses an der Tür zum Führerstand automatisch auf unberechtigte Zugriffe auf sämtliche im Führerstand zugänglichen Komponenten aus.

Gleiches gilt für die Analyse der Datenflüsse. Hieraus ergibt sich beispielsweise, dass eine schlecht konfigurierte Firewall, die selbst üblicherweise nicht als „critical asset" gesehen wird, durch Mitwirkung an wichtigen Datenflüssen das größte Risiko für mehrere „essential functions" darstellen wird. Die Rekonfiguration der Firewall würde folglich als Maßnahme priorisiert werden.

ements automatically affect multiple components. For example, a higher resistance class in a control cabinet reduces the risk for all the components installed in the cabinet. Similarly, installing an electronic lock on the door to the driver's cab automatically affects any unauthorised access to all the components accessible in the cab.

The same applies to the dataflow analysis. For example, analysis has revealed that a poorly configured firewall, which is usually not seen as a "critical asset", poses the greatest risk to several "essential functions" due to its involvement in important dataflows. Consequently, reconfiguring the firewall would be prioritised as a measure.

5 Simulating planned modifications

Rail vehicles are designed to have a long service life. Technical changes to the vehicle usually occur throughout that period, for example by means of the introduction of new interfaces into an existing vehicle in the future or by carrying out a retrofit.

In order to ensure holistic security management throughout the entire lifecycle of the rail vehicle, each planned modification of the vehicle during the respective development phase must be evaluated to ascertain whether it increases or decreases the risk of a successful attack on the vehicle's "essential functions".

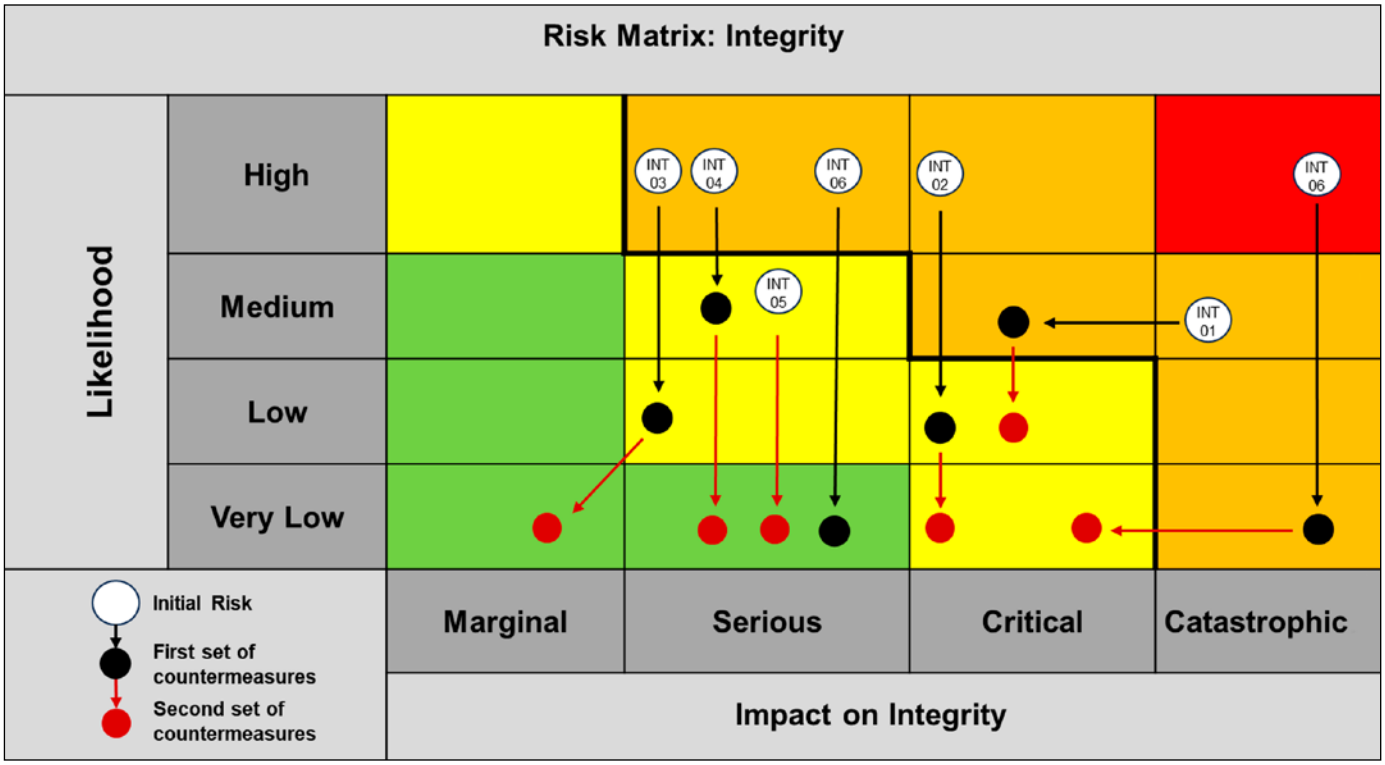

Bild 3: Beispiel einer Risikomatrix mit zwei Iterationen
Fig. 3: An example of a risk matrix with two iterations

5 Simulation von geplanten Änderungen

Schienenfahrzeuge sind auf eine lange Lebensdauer ausgelegt. Während dieser Zeit ergeben sich üblicherweise technische Veränderungen am Fahrzeug, beispielsweise indem in der Zukunft neue Schnittstellen in ein bestehendes Fahrzeug eingefügt werden oder eine Fahrzeugmodernisierung durchgeführt werden soll.

Um ein ganzheitlich taugliches Security-Management über den gesamten Lebenszyklus des Schienenfahrzeugs zu gewährleisten, muss für jede geplante Änderung am Fahrzeug in der Entwicklungsphase evaluiert werden, ob diese das Risiko für einen erfolgreichen Angriff auf die„essential functions" des Fahrzeugs erhöht oder senkt. Eine auf einen Digitalen Zwilling des Schienenfahrzeugs gestützte Security-Risikoanalyse ermöglicht es, eine Änderung am Fahrzeug durch Klonen und Adaptieren des Digitalen Zwillings zu simulieren und das resultierende Risiko mit dem aktuellen Risiko des Fahrzeugs ohne die geplante Veränderung zu vergleichen.

Zeigt die Analyse des Fahrzeugs mit der simulierten Änderung, dass das resultierende Security-Risiko das Akzeptanzniveau überschreitet, so lassen sich in den Entwicklungsprozess noch frühzeitig und dadurch kosteneffizient Anpassungen einbringen, um das Risiko wieder auf ein akzeptables Maß abzusenken. Sollte eine technische Mitigation des durch die Änderung erhöhten Risikos nicht möglich sein, so besteht alternativ die Möglichkeit, „compensating countermeasures" (beispielsweise organisatorische Maßnahmen) einzuführen.

Veranschaulicht werden soll die Bewertung einer geplanten Änderung an einem Schienenfahrzeug, das bisher bis auf den Zugfunk keinerlei Verbindung zur Streckenseite unterhält. Das beispielhafte Schienenfahrzeug ist als Digitaler Zwilling modelliert, und die automatisierte Security-Risikoanalyse hat für das unveränderte Fahrzeug ein akzeptables Risiko ergeben.

Um die Wartung zu vereinfachen, sollen durch das Fahrzeug Daten für eine zentrale Analyse bereitgestellt werden. Hierzu muss das

A Security Risk Assessment based on a digital twin of a rail vehicle allows a modification to the vehicle to be simulated by cloning and adapting the digital twin and comparing the resulting risk with the vehicle's current risk without the planned modification.

If the analysis of the vehicle with the simulated modification shows that the resulting security risk exceeds the tolerable risk, adjustments can be made early in the development process, thus reducing the risk to a tolerable level in a cost-effective manner. If the technical mitigation of the increased risk based on the modification is not possible, the alternative involves the option of introducing "compensating countermeasures" (e.g. organisational measures).

The evaluation of a planned modification to a rail vehicle that has so far had no connection to the trackside except for train radio is to be illustrated. The exemplary rail vehicle is modelled as a digital twin and the automated security risk assessment yields a tolerable risk for the unmodified vehicle.

The vehicle should provide data for central analysis in order to simplify maintenance. The vehicle must transmit the data to an operator's cloud solution via the public mobile network for this purpose. Accordingly, a mobile router is added to the digital twin and all the control units connected to this router in the vehicle are also connected in the digital twin. In this scenario, the risk assessment reveals how the overall risk changes and which new attack vectors arise from the functional extension by means of a before-and-after comparison.

6 Summary

A holistically modelled digital twin enables the automation of Security Risk Assessments. Attack paths can be identified and risks assessed via an automatically generated attack tree.

Fahrzeug Daten über das öffentliche Mobilfunknetz an eine Cloud-Lösung des Betreibers übermitteln. Im Digitalen Zwilling wird entsprechend ein Mobilfunkrouter ergänzt und werden alle an diesen Router angeschlossenen Steuergeräte im Fahrzeug verbunden.
Die Risikoanalyse offenbart in diesem Szenario durch einen Vorher-Nachher-Vergleich, wie sich das Gesamtrisiko verändert und welche neuen Angriffsmöglichkeiten sich durch die funktionale Erweiterung ergeben.

6 Zusammenfassung

Ein ganzheitlich modellierter Digitaler Zwilling ermöglicht die Automatisierung von Security-Risikoanalysen. Angriffspfade können über einen automatisch generierten Angriffsbaum identifiziert und Risiken bewertet werden.
Maßnahmen zur Risikominimierung sollten priorisiert und ganzheitlich effizient sein. Der Digitale Zwilling ermöglicht die Simulation und Bewertung der Wirksamkeit von Maßnahmen, bei Bedarf auch vor ihrer realen Umsetzung. Dies umfasst technische Anpassungen sowie physikalische und organisatorische Schutzmaßnahmen. Durch die Berücksichtigung aller Angriffspfade können Schutzmaßnahmen an zentralen Elementen wie Schaltschränken oder Führerständen das Risiko für mehrere Komponenten gleichzeitig senken.
Die Security-Risikoanalyse eines Schienenfahrzeugs muss kontinuierlich aktualisiert werden, um Änderungen am Fahrzeug oder in der Bedrohungslandschaft zu berücksichtigen. Gründe für notwendige Aktualisierungen können technische Änderungen am Fahrzeug oder neue Angriffsmöglichkeiten sein. Eine automatisierte Security-Risikoanalyse auf Basis eines Digitalen Zwillings ermöglicht damit eine effiziente regelmäßige Neubewertung aller Risiken und bietet eine wichtige Grundlage für sichere Schienenfahrzeuge. ■

Countermeasures to minimise risks should be prioritised and holistically efficient. The digital twin enables the simulation and evaluation of the effectiveness of the countermeasures, if necessary, even before their real implementation. This includes technical adjustments as well as physical and organisational countermeasures. Protective measures on central elements such as control cabinets or driver's cabs can reduce the risk for multiple components simultaneously by considering all the attack paths.
The Security Risk Assessment of a rail vehicle must be continuously updated to account for any modifications to the vehicle or the threat landscape. Reasons for necessary updates can include technical modifications to the vehicle or new attack vectors. An automated Security Risk Assessment based on a digital twin thus enables the efficient regular reassessment of all the risks and provides an important basis for secure rail vehicles. ■

AUTOREN | AUTHORS

Patric Birr, M.Sc.
Chief Operations Officer, Product Director SECIRA
ICS GmbH
Anschrift / *Address*: Wallstraße 27, D-10179 Berlin
E-Mail: patric.birr@ics-gmbh.de

Stefan Karg, CISSP, M.Sc.
Head of Competence Center Security, Team Lead Rail Security
ICS GmbH
Anschrift / *Address*: Sonnenbergstraße 13, D-70184 Stuttgart
E-Mail: stefan.karg@ics-gmbh.de

LITERATUR | LITERATURE

[1] Janicki, J.; Reinhard, H.; Rüffer, M.: Schienenfahrzeugtechnik, Berlin: Bahn Fachverlag GmbH in Kooperation mit DB Training, Learning & Consulting, 2020
[2] „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union", European Union, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555
[3] „Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements", European Union, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
[4] „Scope", in CLC/TS 50701:2023 Railway applications – Cybersecurity, CENELEC, 2023
[5] „IEC 62443-3-2 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design", IEC, 2020
[6] Härdi, R.: „Digital Twin: Ein Fundament für die Zukunft der Bahn", Deine Bahn 04/2021
[7] „IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components", IEC, 2019
[8] „BSI TR-02102-1 – Technische Richtlinie – Kryptographische Verfahren", Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2024
[9] „CIS Center for Internet Security", Center for Internet Security, 2025. [Online]. Available: https://www.cisecurity.org/
[10] „National Vulnerability Database", National Institute of Standards and Technology, [Online]. Available: https://nvd.nist.gov/
[11] „CVE: Common Vulnerabilities and Exposures", The MITRE Corporation, 2025. [Online]. Available: https://www.cve.org/