Technologie- und Securityprognose System Bahn – Bedrohungen rechtzeitig erkennen

Technology and security forecast for the railway system – the timely identification of threats

Markus Heinrich | Lukas Iffländer | Dirk Scheuermann | Stefan Katzenbeisser | Simon Unger

Im Rahmen des Forschungsprojekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn" wurden Prognosen erstellt, wie digitale Technologien im System Bahn künftig eingesetzt werden und wie diese durch Angriffe missbraucht werden können. Die Beschreibungen der Angriffe wiederum erlaubten eine Abschätzung künftiger Bedrohungen, die durch Standards oder Normen behandelt werden müssen.

1 Einleitung

Die fortschreitende Digitalisierung und Vernetzung des Systems Bahn bringt neue Gefahren für die Informationstechnik (IT)-Sicherheit mit sich – dies gilt sowohl für den operativen Bahnbetrieb als auch für neuartige Anwendungen wie die dynamische und individuelle Reisendenlenkung. Für die IT-Sicherheit des Systems Bahn existiert seit 2021 die technische Spezifikation TS 50701 [5], die sich eng an die IEC 62443 [6] anlehnt und die ursprünglich im Kontext der Industrieautomatisierung entwickelt wurde. Die Normen und Standards bilden den aktuellen Stand der Technik ab.

Allerdings entwickelt sich das Feld der IT-Sicherheit sehr dynamisch – stets kommen neue Angriffstechniken hinzu, gegen die ein effektiver Schutz erforderlich ist. Daher muss geprüft werden, ob die normativ festgehaltenen Maßnahmen der IT-Sicherheit auch zu erwartende künftige Bedrohungen abwehren können.

Im Rahmen des vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) beim Eisenbahn-Bundesamt (EBA) finanzierten Projekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn" wurden daher Prognosen erstellt, wie digitale Technologien im System Bahn künftig eingesetzt werden und wie diese durch Angriffe missbraucht werden können – es entstanden sogenannte Abuse-Cases (Missbrauchsfällen). Diese wiederum erlaubten eine Abschätzung künftiger Bedrohungen, die durch Standards oder Normen behandelt werden müssen.

2 Einsatz digitaler Technologie bis ins Jahr 2050

Der künftige Bedarf an IT-Sicherheitskonzepten für das System Bahn kann nur anhand konkreter Einsatzszenarien digitaler Technologien abgeschätzt werden. Zu diesem Zweck wurde eine Technologieprognose angefertigt, die einen Blick bis in das Jahr 2050 wirft und in mehr als 20 Szenarien die Anwendung digitaler Technologien im Umfeld von Reisenden, Gütern, Schienenfahrzeugen, Infrastruktur und ihren Prozessen beschreibt. Hierbei wurde der Schienenverkehr nicht als geschlossenes System betrachtet, sondern mit dem Übergang auf Straße, Wasser und Luft (intermodaler Verkehr) sowie dem grenzüberschreitenden Verkehr in einen Gesamtkontext gebracht.

Prognoses pertaining to the application of digital technology in the railway system and its abuse through attacks have been undertaken as part of the „Security Requirements Forecast and Evaluation of Possible Security Concepts for the Railway System" research project. They in turn have allowed us to assess any future threats that have yet to be considered by the standards or norms.

1 Introduction

The advancing digitalisation and interconnection of the railway system poses new risks to the security of information technology (IT); this applies to both current railway operations and to new applications such as dynamic and individual passenger guidance. The TS 50701 technical specification [5], closely based on IEC 62443 [6] which was initially developed for industrial automation, has existed for railway cybersecurity since 2021. The norms and standards represent the current state of the art.

However, the field of cybersecurity is developing dynamically; newly emerging offensive techniques require the development of adequate protections. It is therefore necessary to question whether the normative cybersecurity measures can also ward off any expected future threats.

Prognoses pertaining to the digital technology applied in the railway system and its abuse through attacks (the creation of so-called abuse cases) have been undertaken as part of the "Security Requirements Forecast and Evaluation of Possible Security Concepts for the Railway System" project funded by the German Centre for Rail Traffic Research (DZSF) at the Federal Railway Authority (EBA). They in turn have allowed us to assess future threats that have yet to be considered by the standards or norms.

2 The use of digital technology up to 2050

The future need for cybersecurity concepts in the railway system relies on the specific application scenarios for the digital technologies. To this end, we have prepared a technology forecast for 2050 that describes the digital technology applications in the environments of passengers, goods, rail vehicles, and infrastructure and their processes in more than 20 scenarios. We did not consider rail transport to be a closed system here and took a broader view regarding intermodal traffic involving roads, water and airways, and cross-border transportation.

Numerous digital technologies find multiple potential applications in the railway system. Fig. 1 shows examples of this schematically. This applies to the communication between the peo-

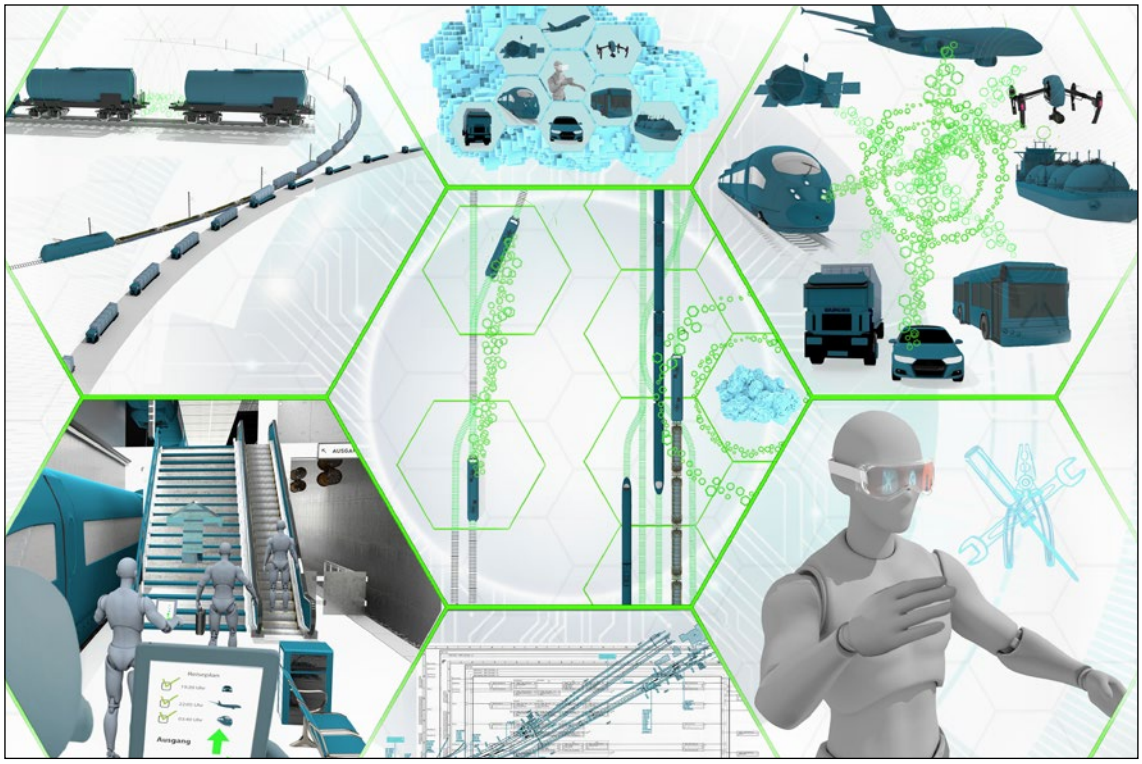

Bild 1: Illustration der unterschiedlichen Anwendungsbereiche digitaler Technologien
Fig. 1: Illustration of the different application areas of digital technologies

Es zeigt sich, dass zahlreiche digitale Technologien auf unterschiedliche Art und in verschiedener Ausprägung im System Bahn eingesetzt werden können. Bild 1 stellt Beispiele dafür schematisch dar. Dies betrifft besonders die Kommunikation der beteiligten Personen und Systeme. Funktechnologien wie das Future Railway Mobile Communication System (FRMCS) werden eine zentrale Rolle einnehmen, um den Datenaustausch für eine Vielzahl von Services des Bahnbetriebs (wie die Zugsicherung) und der Kundenkommunikation (etwa die Reisendenlenkung) bereitzustellen. Auch heute noch wenig bis gar nicht eingesetzte kabellose Übertragungsmöglichkeiten wie der Satellitenfunk stellen ein realistisches Szenario dar, um in Kombination aus verschiedenen Kommunikationstechnologien die Resilienz des Systems zu erhöhen.

Im Fokus vieler Anwendungsgebiete steht das Überwachen von Zustand und Bewegung aller Teilnehmer – Güter, Fahrzeuge – im Gesamtsystem. Hervorzuheben sind Themen wie das Internet of (Railway) Things, die Verfolgung und Parameterüberwachung bei Gütern, die Unterstützung der Instandhaltung der Infrastruktur oder das Verbessern des Reiseerlebnisses für die Fahrgäste (Bild 2). Um einen gesteigerten Mehrwert durch die Vernetzung und Interaktion erzielen zu können, muss diese Vernetzung auch aufseiten der Betreiber, Hersteller und Lieferanten des Systems Bahn abgebildet werden. Dies erfordert, dass Unternehmen ihre individuellen Datenbestände verknüpfen, was entsprechende Konzepte und Modelle zum digitalen Datenaustausch impliziert, die auch die Belange der IT-Sicherheit und Privatsphäre berücksichtigen müssen. Daraus ergibt sich auch die Möglichkeit, dem Kunden aus Personen- und Güterverkehr eine bessere Integration des intermodalen Transportes und einen reibungslosen Übergang zwischen den Verkehrsträgern zu bieten. Dafür müssen die relevanten Informationen unternehmensübergreifend zur Verfügung stehen, um so dem einzelnen Kunden individuell zugeschnittene Information, Vorschläge und Organisation zukommen zu lassen.

Weiterhin können sich Mobilitätsanbieter andere Lebensbereiche technisch erschließen und in ihr Geschäftsmodell integrieren, um

ple and the systems involved. Radio technologies such as the Future Railway Mobile Communication System (FRMCS) will play a central role in providing the data exchange for a variety of services in railway operations (such as train control) and customer communication (such as passenger guidance). Wireless transmissions such as satellite radio, which is currently used very little or not at all, also represent a realistic scenario for increasing the system's resilience with the combination of a range of communication technologies.

Many application areas focus on monitoring the status and movement of all the participants (goods and vehicles) in the overall system. Topics such as the Internet of (Railway) Things, the tracking and parameter monitoring of goods, support for infrastructure maintenance or improving the passenger travel experience (fig. 2) should be highlighted. If increased added value is to be created through networking and interaction, this networking must also be reproduced on the part of the railway system's operators, manufacturers, and suppliers. This requires companies to link their data stocks and as such to take into account the corresponding concepts and models for digital data exchange that also consider cybersecurity and privacy concerns. This also results in the possibility of offering passenger and freight transport customers better integration of intermodal transport and a smooth transition between the modes of transportation. The relevant information must be available across all the companies to provide individually tailored information, suggestions, and organisation to the individual customer.

Furthermore, mobility providers can develop other areas of life technically and then integrate them into their business model to ensure their future viability. This development can be achieved, for example, through comprehensive travel and life management that supports travellers with digital assistants already at home and accompanies them on their way to the train with timely reminders, route suggestions and tips on shopping opportunities (breakfast rolls at their favourite bakery). When travelling, the

Bild 2: Der digitale Assistent begleitet den Reisenden über alle Verkehrsmittel.
Fig. 2: The digital assistant accompanies the traveller across all means of transport.

ihre Zukunftsfähigkeit sicherzustellen. Dies kann beispielsweise durch ein umfassendes Reise- und Lebensmanagement erfolgen, das den Reisenden durch digitale Assistenten bereits zu Hause unterstützt und den Weg zum Zug durch rechtzeitige Erinnerungen, Routenvorschläge und Hinweise auf Einkaufsmöglichkeiten (Frühstücksbrötchen beim Lieblingsbäcker) begleitet. Beim Reisen kann der digitale Assistent Abteile im Zug für mobiles Arbeiten reservieren oder einen Besprechungsraum am (Umsteige-) Bahnhof für das Treffen mit Kollegen und Kunden organisieren. Über die vollständige Reise wird der Reisende bei der Routenwahl, Verkehrsmittelwahl und der benötigten Reisezeit unterstützt (Bild 2).

Aus diesen Anwendungsfällen sind einige zentrale Herausforderungen und Konflikte zwischen Anwendungsziel und Schutzziel bereits absehbar:

- Hohes Vertrauen in die Korrektheit von erhobenen Daten (z. B. Sensordaten), um auf ihrer Basis operative Entscheidungen treffen zu können bei gleichzeitig millionenfacher Sensorverteilung im Kleinstformat
- Integrität und Authentizität beim Austausch der Daten in den unterschiedlichsten Kommunikationsnetzen (Vehicle to Vehicle, Object to Object)
- Wahrung der Privatsphäre und des Datenschutzes bei der Erhebung und Speicherung personenbezogener Daten, auch bei einem Austausch über Unternehmensgrenzen hinweg, unter Erhalt der Nutzbarkeit (Auswertung) der Information
- räumlich und zeitlich uneingeschränkte Verfügbarkeit von Daten und Kommunikation und damit Resilienz der Übertragungsnetze gegen Ausfälle und gezielte Störungen
- Einfluss der Digitalisierung und damit der IT-Sicherheitskonzepte auf die funktionale Sicherheit des Bahnbetriebs
- flexible Weiterentwicklung der Algorithmen durch KI-Methoden auch im Bereich unüberwachten Lernens bei gleichzeitiger Beibehaltung einer Vorhersagbarkeit der Systemreaktion für Agieren im sicherheitsrelevanten Anwendungsbereich.

digital assistant can reserve compartments on the train for mobile work or organise a meeting room at a (transfer) station for meetings with colleagues and customers. Throughout the entire journey, the system supports the traveller in the choice of route, the means of transport and the required travel time (fig. 2).

Some key challenges and conflicts between the application goal and the protection goal are already foreseeable from these use cases:

- high confidence requirements for the correctness of the collected data (e.g., sensor data) for making operative decisions, while at the same time distributing millions of miniature sensors;
- integrity and authenticity during data exchanges in heterogeneous communication networks (vehicle to vehicle, object to object);
- the preservation of privacy and data protection when collecting, storing and sharing personal data, but also while maintaining the usability (analysis) of the information in question;
- the spatially and temporally unrestricted availability of the data and communication and the resilience of the transmission networks against failures and targeted disruptions;
- the influence of the digitalisation and thus the cybersecurity concepts on the safety of railway operations;
- the flexible further development of algorithms using AI methods, including unsupervised learning, while maintaining the predictability of the system response for actions in the safety-relevant application area.

The complete technology forecast has already been published in the first part of the research report on the project and is available online [1].

3 Abuse cases

The known and new threats to the railway system have been analysed based on the technology forecast use cases and described in the form of abuse cases to derive the future need for protection.

Die vollständige Technologieprognose wurde im ersten Teil des Forschungsberichtes zum Projekt bereits publiziert und ist online abrufbar [1].

3 Abuse-Cases

Zur Herleitung des zukünftigen Schutzbedarfs wurden, aufbauend auf den Anwendungsfällen der Technologieprognose, bekannte und neuartige Bedrohungen auf das System Bahn analysiert und in Form von Abuse-Cases (Missbrauchsfällen) beschrieben. Den identifizierten Abuse-Cases werden existierende Schutzmaßnahmen nach dem Stand der Technik und der Normung gegenübergestellt, um zu analysieren, welchen zukünftigen Bedrohungen noch keine angemessenen Schutzmaßnahmen gegenüberstehen. Für diese Analyse kommt die Methodik der Angriffsgraphen zum Einsatz (siehe z. B. Bild 3), die bereits in [2] vorgestellt wurde und für die ein Software-Werkzeug [3] verfügbar ist. Grundlage der hier durchgeführten Risikoanalysen sind die Risikobewertungsmethoden aus der TS 50701 (Cybersicherheit für Bahnanwendungen) [5] und der auf IEC 62443 basierenden Vornorm DIN VDE V 0831-104 für IT-Sicherheit für Bahn-Signalanlagen [6]. Die Methoden wurden hierfür analysiert und widerspruchsfrei implementiert.

Die Angriffsgraphen bieten einige Vorteile für die Risikoanalyse der Szenarien aus der Technologieprognose:

- Abschätzung der Angriffsfolgen: Angriffsgraphen bringen konkrete Angriffe mit den unterschiedlichen möglichen Konsequenzen in Verbindung.
- Nachvollziehbarkeit des Angriffsweges: Angriffsgraphen verfeinern die notwendigen Schritte und zeigen Verkettungen und Alternativen in der Durchführung auf.
- Ausgenutzte Schwachstellen: Angriffsgraphen zeigen die technischen Voraussetzungen für die Realisierung eines Angriffes auf.
- Risiko- bzw. Bedrohungsanalyse: Die Charakterisierung eines Angriffs inkl. seiner Konsequenzen wird durch die Angriffsgraphen dargestellt.
- Gegenmaßnahmen: Die risikomindernde Wirkung von Gegenmaßnahmen wird mit konkretem Bezug auf einen Angriff dargestellt.

Eine herkömmliche Dokumentation von Risikoanalysen basiert typischerweise auf einem Tabellenformat, bei dem es nur schwer möglich ist, die Zusammenhänge zwischen Angriffen / Bedrohungen, Schadensausmaß und wirksamen Gegenmaßnahmen intuitiv darzustellen und damit nachvollziehbar zu machen.

We compared the identified abuse cases with the existing protective measures according to the state of the art and the standards so as to analyse which future threats have not yet been countered by adequate protective measures. We employed the attack graph methodology for this analysis (e.g., see fig. 3) as presented in [2] and developed a software tool to this end [3]. The risk analyses carried out here are based on the risk assessment method from TS 50701 (cybersecurity for railway applications) [5] and the DIN VDE V 0831-104 pre-standard for the cybersecurity of railway signalling systems [6] based on IEC 62443. We have analysed and implemented the methods for this purpose without any contradictions.

The attack graphs offer some advantages in the risk analysis of the scenarios from the technology forecast:

- the assessment of the consequences of attacks: attack graphs relate specific attacks to different possible outcomes.
- the traceability of the attack path: attack graphs refine the necessary steps and show the chains and alternatives in the execution.
- the exploited vulnerabilities: attack graphs show the technical requirements for the realisation of an attack.
- the risk or threat analysis: attack graphs represent the characterisation of an attack, including its consequences
- countermeasures: attack graphs represent the risk-reducing effect of countermeasures with specific reference to an attack.

The conventional documentation of risk analyses typically relies on a table format where it is difficult to intuitively present the connections between the attacks and the threats, the extent of the damage and any effective countermeasures and thus to make them understandable.

Attack graphs, on the other hand, prepare the risk analysis graphically, facilitate the reader's understanding and are therefore predominantly suitable for the comprehensive discussion that the technology forecast intends to stimulate. The central challenge in analysing the technology forecast scenarios lies in the systems that have only been abstractly defined, since the system cannot yet be completely technically realised based on an outlook of the future. Therefore, the risk analysis is subject to uncertainty due to the choice of the given technical realisation, which is represented more comprehensibly by logically linking the sub-steps in the attack graphs.

Die Angriffsgraphen bereiten die Risikoanalyse dagegen grafisch auf, erleichtern das Verständnis für den Leser und eignen sich daher vorwiegend für die umfassende Diskussion, wie sie die Technologieprognose anregen soll. Die zentrale Herausforderung bei der Analyse der Szenarien der Technologieprognose sind die nur abstrakt definierten Systeme, da es aufgrund des Ausblicks auf die Zukunft noch keine vollständige technische Realisierung des Systems geben kann. Daher ist die Risikoanalyse der Unsicherheit durch die Wahl der konkreten technischen Umsetzung unterworfen, die sich durch die logische Verknüpfung von Teilschritten in den Angriffsgraphen nachvollziehbarer darstellen lässt.

4 Künftige Bedrohungen für das System Bahn

Aus der in den Angriffsgraphen dokumentierten Risikoanalyse für die Szenarien der Technologieprognose lassen sich Trends der zukünftigen IT-Sicherheits-Bedrohungen für das System Bahn ableiten und erste Handlungsempfehlungen entwickeln.

4.1 Resilienz der drahtlosen Kommunikation

Mit dem zunehmenden Einsatz digitaler Technologien steigt auch der Bedarf an Kommunikation und Vernetzung, um alle Vorteile der Digitalisierung ausnutzen zu können. Für viele Anwendungen ist eine drahtlose Kommunikation erforderlich, wofür neben dem bekannten FRMCS (5G) auch andere Übertragungssysteme, wie Bluetooth, Wireless Local Area Network (WLAN), Near Field Communication (NFC), Low Power Wide Area Networks (LPWAN) und Satellitenfunk in Frage kommen. Daher erhöht sich gleichzeitig auch die Angriffsfläche für Manipulationen und Störungen unterschiedlicher Art. Insbesondere Jamming-Angriffe (Störung der genutzten Funkfrequenzen) stellen eine Herausforderung dar, da mit einfachen Mitteln eine starke Einschränkung der Verfügbarkeit erzeugt werden kann. Nach dem Stand der Technik existiert heute keine geeignete Maßnahme, um Jamming vollständig und wirksam zu verhindern. Daher müssen Strategien entwickelt werden, um Anwendungen resilienter gegen den Einfluss von Jamming zu gestalten. Abhängig vom Einsatzszenario der drahtlosen Kommunikation kommen verschiedene Möglichkeiten in Frage, etwa die temporäre Tolerierung punktueller Ausfälle, die Bereitstellung redundanter Kommunikationskanäle über unterschiedliche Technologien oder die schnelle Ortung und Verfolgung dieser Aktivitäten zur Erhöhung der Eintrittsschwelle durch Abschreckung.

4.2 Absicherung der Sensorik des Internet of Railway Things

Der Schienenverkehr verlässt sich auf eine immer größer werdende Menge digitaler Daten unterschiedlichen Typs, die über Sensoren des Internet of Railway Things (IoRT) erfasst werden. Bereits ohne die Gegenwart von Angreifern stellt es heute eine Herausforderung dar, eine korrekte digitale Repräsentation der analogen Welt zu erstellen und aktuell zu halten. Dies wird verstärkt durch den Einsatz von digitalen Zwillingen, die ein System nahezu in Echtzeit auf Veränderungen überwachen müssen (bspw. Bewegung von Zügen oder Personen, Reaktion auf Veränderung der Umweltbedingungen). Durch Cyberangriffe kommt die Dimension der bewussten (gegebenenfalls verschleierten) Manipulation der digitalen Abbildung der analogen Welt in Echtzeit hinzu. Wenn etwa Sensordaten von automatisch fahrenden Zügen durch Manipulation die Realität nicht korrekt widerspiegeln, kann dies auch einen Einfluss auf die funktionale Sicherheit des Bahnbetriebs haben. Anwendungen wie automatisiertes oder gar autonomes Fahren sind in hohem Maße von der korrekten Erfassung der Umwelt und korrekten Erfassung der Position (sichere Ortung) sowie des Zustands (Abnutzungsvorrat) abhängig und somit besonders an-

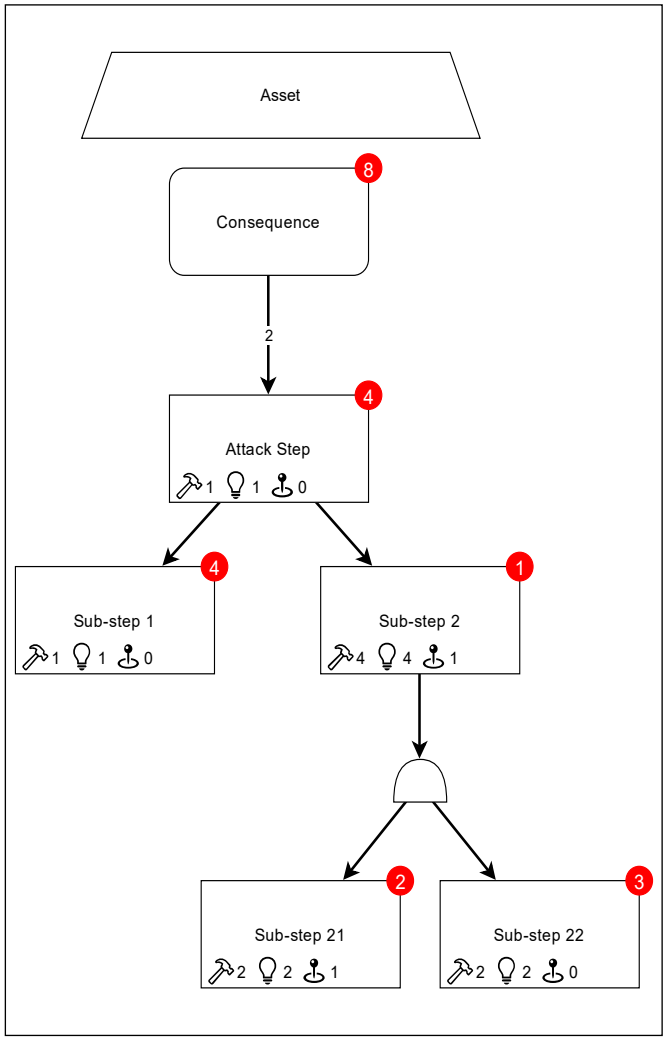

Bild 3: Beispiel eines Angriffsgraphen
Fig. 3: Attack Graph Example

4 Future threats to the railway system

The risk analysis documented in the attack graphs for the technology forecast scenarios enables trends in future cybersecurity threats to the railway system to be derived and initial recommendations for action to be developed.

4.1 The resilience of wireless communication

The increasing use of digital technologies means that the need for communication and networking also has to grow in order to take advantage of all the benefits of digitalisation. Many applications require wireless communication, for which other transmission systems such as Bluetooth, Wireless Local Area Network (WLAN), Near-Field Communication (NFC), Low-Power Wide Area Networks (LPWAN) and satellite radio are possible, in addition to the well-known FRMCS (5G). Therefore, the attack surface for manipulations and disruptions of various kinds also simultaneously increases. Jamming attacks (interference with the radio frequencies) pose a challenge, as a severe restriction of availability can be created using simple means. The state of the art currently provides no suitable measures to prevent jamming entirely and effectively. Therefore, this lack of defence requires the development of new strategies to increase the appli-

fällig. Die zukünftige Herausforderung wird es sein, ein hohes Vertrauen in die korrekte Erhebung und Vorhaltung unterschiedlicher Datensätze sicherzustellen. Technische Ansätze hierzu können die Validierung über die Historie der Messpunkte oder die Verknüpfung unterschiedlicher Messungen darstellen, sodass eine gegenseitige Plausibilitätsprüfung ermöglicht wird. Hinzu kommt eine Ende-zu-Ende-Authentifizierung beginnend an den Sensoren des IoRT unter Berücksichtigung der beschränkten Energie- und Prozessor-Ressourcen, die den Anforderungen an starke Authentifizierungsmechanismen auch unter physischem Zugriff des Angreifers auf den Sensor gerecht werden müssen. Hier stehen die technische Hochrüstung der Sensoren oder die Verwendung von leichtgewichtigen kryptographischen Authentifikationsprotokollen im Vordergrund. Beides sollte bereits jetzt für langfristig geplante Sensornetzwerke in Betracht gezogen werden.

4.3 Schutz und Nachvollziehbarkeit von maschinellem Lernen

Prominentestes Beispiel für den Einsatz von maschinellem Lernen in den Szenarien der Technologieprognose ist die intelligente Instandhaltung. Maschinelles Lernen und Künstliche Intelligenz (KI) werden aber auch in weiteren Szenarien eingesetzt, um – teilweise (sicherheits-)kritische – Funktionen zu erfüllen. Durch die vermehrte Übertragung menschlicher Entscheidungen auf eine KI sind solche Entscheidungen aber nicht in gleichem Maße transparent und nachvollziehbar. Angreifer können diesen Umstand ausnutzen, um die Entscheidungen zu ihren Gunsten zu manipulieren.

cation's jamming resilience. Various options, such as the temporary tolerance of delays, the provision of redundant communication channels using different technologies or the rapid location and tracking of these activities to increase the entry threshold through deterrence, are possible depending on the wireless communication deployment scenario.

4.2 Securing the sensor technology for the Internet of Railway Things

Rail transport relies on an ever-increasing amount of digital data collected via sensors on the Internet of Railway Things (IoRT). Even without the presence of attackers, it is currently a challenge to create and keep the correct digital representation of the analogue world up to date. Digital twins, which monitor a system for any changes in near real-time (e.g., the movement of trains or people, reactions to changes in environmental conditions), exacerbate this effect. Cyber-attacks add the dimension of deliberate (possibly disguised) manipulations of the digital image of the analogue world in real-time. If, for example, sensor data from automatically running trains does not correctly reflect reality due to any such manipulation, this can also impact the safety of railway operations. Applications such as automated or even autonomous driving are highly dependent on the correct detection of the environment, the accurate detection of the position (safe location) and the condition (wear stock) and are, therefore, particularly vulnerable. The future challenge lies in ensuring high confidence in the correct collection and retention of different

Die Forschung zu Adversarial Machine Learning (Angriffe auf maschinelles Lernen) hat gezeigt, dass Maschinelles Lernen durch geschickt (und für einen menschlichen Betrachter unbemerkt) manipulierte Eingaben in der Klassifikation getäuscht werden kann. Hierbei nutzt der Angreifer verfügbare Informationen über den Algorithmus und das KI-Modell aus. Dazu werden dem Modell speziell präparierte Eingaben präsentiert, um eine vom Angreifer bestimmte Ausgabe zu erzwingen. Angriffe können sowohl während der Trainingsphase als auch während der Nutzung erfolgen. Besonders in der Bilderkennung sind die zum Täuschen der KI erforderlichen Manipulationen so subtil, dass sie durch einen menschlichen Betrachter nicht erkannt werden können. Wird eine solche KI eingesetzt, um etwa eine Hinderniserkennung für automatisch fahrende Züge zu realisieren, kann ein Angreifer durch Manipulation der Daten falsche Reaktionen der Hinderniserkennung auslösen.

4.4 Schutz vor Angriffen durch Quantencomputer

Quantencomputer nutzen anstelle von Bits sogenannte Qubits, welche neben den Zuständen 0 und 1 auch kohärente Überlagerungen von beiden Zuständen darstellen können. Dies führt bei gewissen Berechnungen, wie sie etwa zum Brechen kryptographischer Verfahren genutzt werden, zu einem deutlichen Vorteil gegenüber klassischen Computern. Zum heutigen Zeitpunkt stellen Quantencomputer noch keine große Gefahr dar, da diese noch über sehr wenige Qubits verfügen. Jedoch arbeiten Forschungseinrichtungen und Industrie weltweit daran, die Technik der Quantencomputer zu verbessern, wodurch es in Zukunft zu einer Bedrohung der Sicherheit (Security) durch leistungsstärkere Quantencomputer kommen kann. Deswegen sollte bereits jetzt sichergestellt werden, kryptographische Verfahren zu verwenden, welche hinreichend stark sind, um auch zukünftig nicht durch Quantencomputer gefährdet zu sein. Nach aktuellem Stand der Technik können hierfür unter anderem die Empfehlungen zur Post-Quanten-Kryptografie des BSI herangezogen werden [7].

5 Ausblick

Für ausgewählte Abuse-Cases wird auf Basis der vorliegenden Bewertungsschemata und des vorhandenen Softwarewerkzeuges als nächstes eine detaillierte Risikoanalyse durchgeführt. Dabei werden zwei verschiedene Experten-Teams jeweils eine getrennte Untersuchung durchführen und ihre Ergebnisse gegeneinander abgleichen. Aus den Ergebnissen der Risikoanalyse wird ein genauerer Schutzbedarf für die einzelnen Anwendungsfälle abgeleitet.

Im abschließenden Schritt folgt die Erarbeitung und Evaluierung von Sicherheitsmaßnahmen zur Minderung der Risiken und zur Erfüllung des identifizierten Schutzbedarfs. Dabei sind zunächst bestehende, auf das System Bahn anwendbare Normen zu betrachten. Anschließend werden Lücken identifiziert und zielgerichtete Sicherheitsmaßnahmen zur Schließung dieser Lücken erarbeitet. Die Entwicklung von Sicherheitsmaßnahmen wird begleitet von einem iterativen Prozess der Risikoneubewertung unter Benutzung der vorhandenen Software-Werkzeuge.

6 Forschungsförderung

Die vorgestellte Arbeit entstand im Rahmen des vom Deutschen Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt beauftragten und finanzierten Projekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“.

data sets. Technical approaches can include validation based on measurement point history or the linking of other measurements to enable a mutual plausibility check. In addition, there is also end-to-end authentication, starting with the IoRT sensors, while taking into consideration the limited energy and processor resources, which must meet the requirements for solid authentication mechanisms, even if the attacker has physical access to the sensor. In this case, the technical upgrading of the sensors or the use of lightweight cryptographic authentication protocols have come to the foreground. Sensor network planning should consider them during the design phase.

4.3 The protection and traceability of machine learning

The most prominent example of the use of machine learning in the technology forecast scenarios involves predictive maintenance. However, machine learning and artificial intelligence (AI) are also used in other scenarios to fulfil critical functions (safety). These decisions are no longer as transparent and understandable to the same extent due to the increased transfer of human decisions to AI. Attackers can exploit this circumstance in order to manipulate the decisions in their favour.

Research on Adversarial Machine Learning has shown that machine learning can be fooled by cleverly manipulated (unnoticeable to a human observer) inputs to the classification. Here, the attacker exploits information about the algorithm and the AI model. In order to achieve this, the attacker presents specially prepared inputs to the model to force the output that the attacker desires. Attacks can occur both during the training phase and during use. The manipulations required to fool the AI are so subtle that a human observer cannot detect them, especially in the area of image recognition. For example, an attacker can trigger false obstacle detection reactions by manipulating the data, if the AI performs obstacle detection for automatically moving trains.

4.4 Protection against attacks by quantum computers

Instead of bits, quantum computers use so-called qubits, which, in addition to the states 0 and 1, can also represent coherent superpositions of both states. This gives them a clear advantage over classical computers in specific calculations, such as those used to break cryptographic procedures. At present, quantum computers do not yet pose a significant threat, because they still have very few qubits. However, research institutions and industries worldwide are working on improving quantum computer technology, which could lead to a security threat from more powerful quantum computers in the future. For this reason, system designers must ensure the use of sufficiently cryptographically solid procedures so that quantum computers do not endanger them in the future. The BSI‘s recommendations on post-quantum cryptography that are based on the current state of the art can be used for this purpose [7].

5 Outlook

A detailed risk analysis will subsequently be conducted for selected abuse cases based on the available assessment schemes and the existing software tool. In the process, two teams of experts will each perform separate investigations and compare their results against one another. We will derive more precise protection requirements for the individual use cases based on the risk analysis results.

The final step involves developing and evaluating safety measures to mitigate the risks and meet the identified need for protec-

AUTOREN | AUTHORS

Dr.-Ing. Markus Heinrich
Expert IT Security
Incyde GmbH
Anschrift / *Address*: Schaumainkai 91, D-60596 Frankfurt am Main
E-Mail: markus.heinrich@incyde.com

Dr. rer. nat. Lukas Iffländer
Scientific Consultant Cyber Security
Deutsches Zentrum für Schienenverkehrsforschung
Anschrift / *Address*: August-Bebel-Straße 10, D-01219 Dresden
E-Mail: ifflaenderL@dzsf.bund.de

Dr. rer. nat. Dirk Scheuermann
IT Security Researcher
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Anschrift / *Address*: Rheinstraße 75, D-64295 Darmstadt
E-Mail: dirk.scheuermann@sit.fraunhofer.de

Prof. Dipl.-Ing. Dr. Stefan Katzenbeisser
Chair of Computer Engineering
Universität Passau
Anschrift / *Address*: Innstraße 43, D-94032 Passau
E-Mail: stefan.katzenbeisser@uni-passau.de

Simon Unger
Research Associate IT Security for Critical Infrastructures
Universität Passau
Anschrift / *Address*: Innstraße 43, D-94032 Passau
E-Mail: simon.unger@uni-passau.de

tion. Thus, the existing standards that are applicable to the railway system must first be taken into account. Gaps will subsequently be identified and targeted safety measures will be developed in order to close these gaps. The development of the safety measures will be accompanied by an iterative risk reassessment process using existing software tools.

6 Research funding

The presented work is part of the „Security Requirements Forecast and Evaluation of Possible Security Concepts“ project, commissioned and financed by the German Centre for Rail Traffic Research at the Federal Railway Authority. ■

LITERATUR | LITERATURE

[1] https://doi.org/10.48755/dzsf.220008.06; 17.06.2022
[2] Heinrich, M.; Iffländer, L.: Softwaregestützte Bedrohungsanalyse durch Angriffsgraphen, SIGNAL+DRAHT, 05/2022
[3] https://github.com/incyde-gmbh/drawio-plugin-attackgraphs
[4] https://github.com/INCYDE-GmbH/attackgraphs
[5] CLC/TS 50701: Railway Applications – Cybersecurity. 2021
[6] DIN VDE V 0831-104 VDE V 0831-104: Elektrische Bahn-Signalanlagen - Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443. 2015.
[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1; 17.06.2022