KI auf Schienen – Beschleunigung der digitalen Transformation des Bahnbetriebs

AI on rails – steering the digital transformation of railway operations

Dominik Spychalski | Nicolai Erbs | Ali Recai Yekta

Im digitalen Zeitalter sind Daten ein zentrales Gut, das mit jeder Anwendung an Wert gewinnt. Dies gilt insbesondere für den Bahnsektor, wo die verschiedenen Formen und Interpretationen von Daten Erkenntnisse ermöglichen, die für die Verbesserung des Betriebs entscheidend sind. Die Integration von Künstlicher Intelligenz (KI) stellt einen bedeutenden Sprung in diesem Bereich dar und verändert den Bahnbetrieb von der Planung über das Asset Management bis hin zum Kundenerlebnis. Der Einsatz von KI und Daten im Bahnbetrieb ist jedoch ein Balanceakt zwischen Effizienz und Sicherheit.

1 Einsatz von KI im Schienenverkehr: Balance zwischen Effizienz und Sicherheit

Die riesigen Datenbestände, die in KI-Systemen verwendet werden und für maschinelle Lernmodelle (ML) unerlässlich sind, bergen auch Sicherheitsimplikationen. Die anpassungsfähigen und leistungsfähigen Modelle können durch Datenmanipulationen beeinträchtigt werden, was Risiken für die betriebliche Integrität und Sicherheit mit sich bringt. In dem Maße, in dem wir KI nutzen, um den Bahnbetrieb zu revolutionieren, müssen wir auch unsere Abwehrmaßnahmen gegen potenzielle Verstöße verstärken. Dieser Beitrag befasst sich mit dem dynamischen Zusammenspiel von KI, Daten und Sicherheit in der Bahnindustrie. Er soll Fachleuten und Entscheidungsträgern einen Überblick geben, um sich in dieser Landschaft zurechtzufinden und sicherzustellen, dass das Streben nach Effizienz durch KI nicht die Notwendigkeit der Aufrechterhaltung robuster Sicherheitsmaßnahmen überschattet. Auf dem Weg des Eisenbahnsektors zur digitalen Transformation ist KI sowohl ein mächtiger Verbündeter als auch eine Herausforderung, die mit äußerster Vorsicht zu bewältigen ist.

2 Technologieintegration in das Eisenbahnökosystem

Die Eisenbahnindustrie ist ein Ökosystem, das eine Vielzahl von Akteuren und technischen Elementen umfasst. Im Mittelpunkt stehen die Bahnbetreiber, die für einen reibungslosen Zugbetrieb sorgen, unterstützt von den Infrastrukturbetreibern, die die wichtigen Gleise, Signale und Bahnhöfe warten. Dieses Netzwerk erstreckt sich auf Hersteller von Rollmaterial, staatliche Regulierungsbehörden und eine Vielzahl von Dienstleistern, die alle zur Funktionalität des Ökosystems beitragen. Technologisch gesehen ist das Eisenbahnsystem ein hochentwickeltes Netzwerk, in dem die Züge als dynamische Datendrehscheiben fungieren. Ausgestattet mit fortschrittlichen Sensoren und Kommunikationsmitteln sind die Züge für die Aufrechterhaltung der Betriebssicherheit und Effizienz von zentraler

Data is emerging in the digital era as a pivotal asset that is gaining in value with each application. This is particularly true in the railway sector, where data's diverse forms and interpretations unlock patterns and insights that are crucial for enhancing operations. The integration of artificial intelligence (AI) marks a significant leap in this domain that will transform rail operations from scheduling and asset management through to the customer experience. However, the power of AI and data in the railways is a balancing act between efficiency and security.

1 Harnessing AI in rail traffic: balancing efficiency and security

The vast data pools that are used in AI systems and are essential for machine learning (ML) models also present security vulnerabilities. These adaptable and potent models can be compromised by data manipulation that poses risks to operating integrity and security. Thus, as we leverage AI to revolutionise railway operations, we must also fortify our defences against any potential breaches. This article delves into the dynamic interplay of AI, data and security in the railway industry. It aims to provide an overview for professionals and policymakers to navigate this landscape, thereby ensuring that the pursuit of efficiency through AI does not overshadow the imperative of maintaining robust security measures. AI stands as both a powerful ally and a challenge to be managed with the utmost caution in the railway sector's journey towards digital transformation.

2 Integrating technology into the railway ecosystem

The railway industry is a multifaceted ecosystem that encompasses a diverse range of stakeholders and technical elements. At its heart are railway operators, who ensure seamless train operations, with support from the infrastructure managers, who maintain the essential tracks, signals and stations. This network extends to rolling stock manufacturers, governmental regulatory bodies and a variety of service providers, each contributing to the ecosystem's functionality. Technologically, the railway system is a sophisticated network where trains act as dynamic data hubs. Equipped with advanced sensors and communication tools, trains are pivotal to maintaining operating safety and efficiency. The infrastructure, including the tracks and signals, provides the real-time data that is crucial for optimal train navigation. Control centres, functioning

Bedeutung. Die Infrastruktur, einschließlich der Gleise und Signale, liefert Echtzeitdaten, die für eine optimale Zugnavigation entscheidend sind. Leitstellen, die als Nervenzentrum des Systems fungieren, steuern die Zugbewegungen durch kontinuierlichen Datenaustausch. Die Wartungsteams nutzen diese Daten für eine proaktive Instandhaltung, die die Sicherheit erhöht und die Lebensdauer der Anlagen verlängert. Fahrgäste und Fracht, die in diesem Ökosystem eine zentrale Rolle spielen, interagieren über digitale Plattformen und bereichern so das Reiseerlebnis sowie die Frachtverfolgung und -zustellung. Drittangebote, von Unterhaltung bis zum Catering, lassen sich nahtlos in die Zugsysteme integrieren und verbessern so die Dienstleistungen an Bord. Eingebettete Sicherheitssysteme, die Überwachung und Zugangskontrolle umfassen, erhöhen die Sicherheit von Fahrgästen und Anlagen. Das Bahnökosystem wird dadurch ein komplexes, miteinander verbundenes Netzwerk. Züge werden zu zentralen Knotenpunkten in diesem datengesteuerten Netz, die die Kommunikation und die betriebliche Effizienz im gesamten Ökosystem erleichtern.

3 Datengesteuerte Dynamik im Eisenbahn-Ökosystem

Das Bahnökosystem lebt von einer Vielzahl von Daten, von denen jeder einzelne zu einem umfassenden Betriebsbild beiträgt. Betriebsdaten, die Zugsteuerungsmetriken wie Geschwindigkeit, Standort und Beschleunigung sowie Wartungs- und Infrastrukturzustandsberichte umfassen, bilden das Rückgrat des täglichen Eisenbahnmanagements. Diese Daten sind entscheidend für die Entscheidungsfindung in Echtzeit und für vorausschauende Wartungsstrategien. Fahrgastdaten, von Fahrscheindetails bis hin zu Feedback und Unterhaltungsnutzung, bieten wertvolle Einblicke in die Vorlieben der Kunden, die das Fahrgasterlebnis prägen. Sicherheitsdaten, einschließlich IT/OT-Security-Daten und Überwachungsdaten, stellen eine Schutzbarriere gegen physische und digitale Bedrohungen dar und gewährleisten die Sicherheit des Eisenbahnnetzes. Im Zeitalter ausgefeilter Cyberbedrohungen kommt diesem Aspekt der Daten eine besondere Bedeutung zu, wobei ihre kontinuierliche Überwachung und Analyse der Schlüssel zum Schutz der Integrität der Bahn ist. Kommunikationsdaten, die die Wi-Fi-Nutzung verfolgen und die Kommunikation zwischen den Zügen erleichtern, spielen eine entscheidende Rolle bei der Aufrechterhaltung der Konnektivität und

as the system's nerve centre, manage the train movements by means of a continuous data exchange. Maintenance teams leverage this data for proactive repairs, thereby enhancing safety and extending asset lifecycles. Passengers and cargo, central aspects of this ecosystem, engage through digital platforms that enrich their travel experience, as well as freight tracking and delivery. Service providers, ranging from entertainment to catering, seamlessly integrate with train systems, thereby elevating onboard services. Embedded security systems, including surveillance and access control, reinforce passenger and asset safety. In summary, the railway ecosystem is a complex, interconnected network where each participant, from the vehicles to the passengers, plays a vital role. Trains are transcending their traditional role and have emerged as central nodes in this data-driven network that facilitate communication and operating efficiency across the ecosystem.

3 Data-driven dynamics in the railway ecosystem

The railway ecosystem thrives on a rich tapestry of data, each strand contributing to a comprehensive picture of operations. Operating data that encompasses train control metrics such as speed, location and acceleration, as well as maintenance and infrastructure condition reports, forms the backbone of the day-to-day railway management. This data is crucial for real-time decision-making and predictive maintenance strategies. Passenger data, ranging from ticketing details to feedback and entertainment use, offers valuable insights into customer preferences that shape the passenger experience. Security data, including IT/OT security logs and surveillance feeds, stands as a protective barrier against physical and digital threats, thereby ensuring safety in the railway network. This data aspect has assumed heightened importance in an age of sophisticated cyber threats with continuous monitoring and analysis being key to safeguarding the railway's integrity. Communication data that tracks Wi-Fi usage and facilitates inter-train communication plays a vital role in maintaining connectivity and operational harmony. All this is complemented with additional data sources such as object metadata, HR information and external environmental readings, which provide contex-

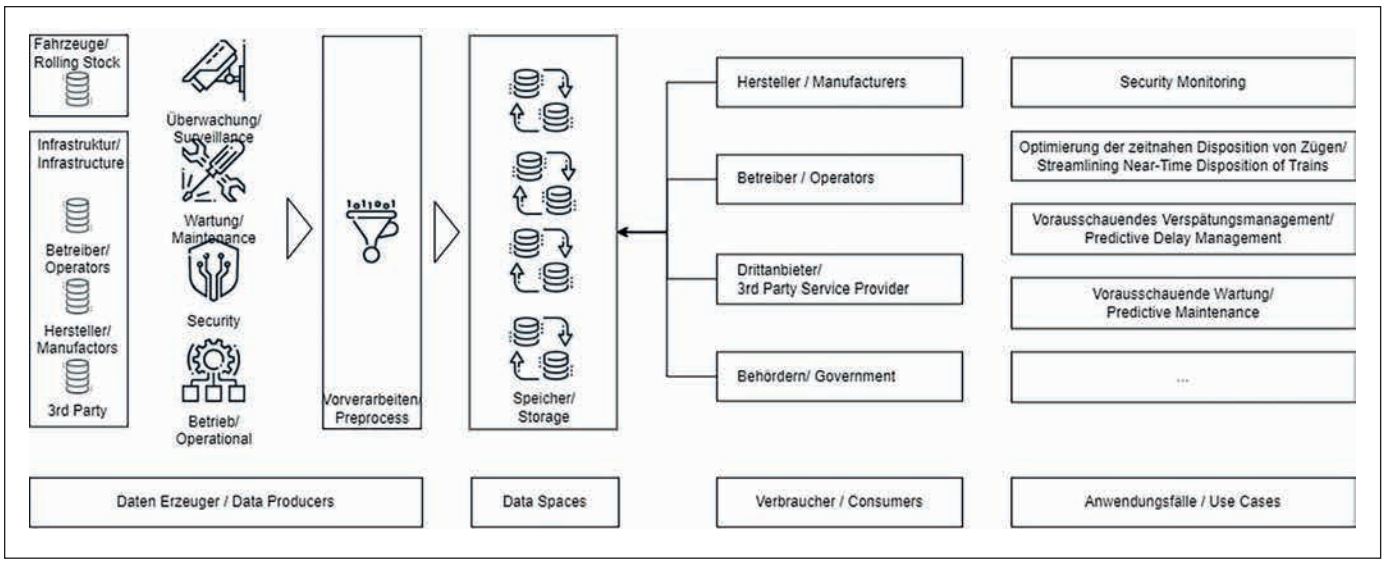

Bild 1: Die Daten-Pipeline eines facettenreichen Datenökosystems
Fig. 1: The data pipeline of a multi-faceted data ecosystem

Quelle / *Source*: eigene Darstellung / *own figure*

der betrieblichen Harmonie. Hinzu kommen zusätzliche Datenquellen wie Objekt-Metadaten, Personalinformationen und externe Umgebungsdaten, die ein kontextbezogenes Verständnis für die strategische Planung und das Personalmanagement liefern.
Die Rolle der KI und des maschinellen Lernens in diesem datenreichen Umfeld ist transformativ. Durch die Analyse der verschiedenen Datenströme können KI-Algorithmen den Wartungsbedarf vorhersehen, Betriebsrouten verfeinern, Sicherheitsmaßnahmen verstärken und Passagierdienste anpassen. Im Bereich der IT/OT-Sicherheit ist die Fähigkeit der KI, große Datensätze zur Erkennung von Bedrohungen zu analysieren, von unschätzbarem Wert und bietet einen proaktiven Schutz vor potenziellen Cyberangriffen. Da sich die Bahnindustrie weiter digitalisiert, ist die Synergie von KI mit diesem facettenreichen Datenökosystem nicht nur vorteilhaft, sondern unerlässlich, um einen reibungslosen, sicheren und effizienten Bahnbetrieb zu gewährleisten.

4 KI-Anwendungen mit Betriebsdaten ausstatten

4.1 Nutzung von Betriebsdaten zur Optimierung des Zugbetriebs

Die Vorhersage von Zugverspätungen ist eine komplexe Herausforderung, die durch die Nutzung von Betriebsdaten erreicht werden kann. Für Zugbetreiber liegt der Schlüssel zur Minimierung von Störungen darin, diese Daten zu nutzen, um Verspätungen vorherzusehen und zu managen, bevor sie auftreten. Der erste Schritt zur Vorhersage von Zugverspätungen ist die Integration von Betriebsdaten. Dazu gehören Echtzeit-Telemetriedaten von Zügen, die Aufschluss über Geschwindigkeit, Standort und Beschleunigung geben. Signal- und Streckendaten sind ebenfalls von entscheidender Bedeutung, da sie Informationen über die Streckennutzung und die Fahrplanung liefern. Durch die Analyse von Mustern in diesen Daten können die Betreiber potenzielle Engpässe erkennen, die zu Störungen führen können. Maschinelle Lernmodelle können auf historischen Daten trainiert werden, um Fahrtzeiten vorherzusagen. Diese Modelle berücksichtigen eine Vielzahl von Faktoren, wie z. B. die Dichte des Zugverkehrs, die Pünktlichkeit in der Vergangenheit, die Wetterbedingungen und bekannte Infrastrukturbeschränkungen. Durch die Verarbeitung dieser Daten können die Modelle potenzielle Verspätungen und deren wahrscheinliche Ursachen vorhersagen. Da die Betreiber den Zustand des Netzes kennen, können sie die Fahrpläne in Echtzeit anpassen, um mögliche Verspätungen zu vermeiden. Wenn beispielsweise ein Zug Verspätung hat, können nachfolgende Züge umdisponiert werden, um einen optimalen Verkehrsfluss zu gewährleisten und die Auswirkungen auf das gesamte System zu minimieren. Dieser proaktive Ansatz verbessert nicht nur den Fahrgastkomfort, sondern trägt auch zur wirtschaftlichen Leistungsfähigkeit des Eisenbahnnetzes bei.

4.2 Automatisierung der kurzfristigen Disposition von Zügen

Im schnelllebigen Umfeld des Zugbetriebs ist die Disposition von Zügen – insbesondere unter dem Einfluss von Störungen wie z. B. Bauarbeiten – ein sinnvoller Anwendungsfall für die Nutzung von Betriebsdaten. KI-Algorithmen können diese Informationen schnell analysieren, um zeitnahe Anpassungen vorzunehmen, die bei solchen unvorhergesehenen Ereignissen entscheidend sind. Diese Algorithmen können Routen dynamisch optimieren, indem sie aktuelle und historische Telemetriedaten, Signalzustände und Routendetails verarbeiten und so die effizientesten Pfade um etwaige Langsamfahrstellen herum ermitteln. Zugfolgen können nahezu in Echtzeit angepasst werden, um die Ausbreitung von Verzögerungen im gesamten Netz zu minimieren. Auch die Ressourcenzuweisung wird mithilfe von Betriebsdaten intelligenter und reaktionsschneller. Durch das Verständnis der aktuellen Disposition der Züge und die Vorhersage potenzieller Engpässe können Ressourtual understanding for strategic planning and workforce management.
The role of AI and machine learning in this data-rich environment is transformative. By analysing the diverse data streams, AI algorithms can anticipate maintenance needs, refine operating routes, bolster security measures and tailor passenger services. In the realm of IT/OT security, AI's capability to parse vast datasets for threat detection is invaluable, thereby offering a proactive shield against any potential cyber incursions. As the railway industry continues to evolve digitally, the synergy of AI with this multifaceted data ecosystem is not just beneficial, but essential, as it ensures the smooth, safe and efficient running of railway operations.

4 Empowering AI applications with operating data

4.1 Leveraging operating data to optimise train operations

Predicting train delays is a complex challenge that can be addressed through the strategic use of operating data. For train operators, the key to minimising disruptions lies in harnessing this data so as to anticipate and manage any delays before they occur. The first step in predicting train delays involves the integration of comprehensive operating data. This includes real-time telemetry data from trains that provides insights into train speed, location and acceleration. Signal and route data is also critical, as it offers information on track usage and scheduling. Operators can analyse the patterns within this data to identify any potential bottlenecks and constraints that may lead to disruptions. Advanced machine learning models can be trained on historical data to predict train movements. These models consider a multitude of factors such as train traffic density, historical punctuality, weather conditions and any known infrastructure constraints. Processing this data enables the models to forecast any potential delays and their probable causes. This understanding of the network status enables operators to adjust their schedules in real-time in order to avoid any potential delays. For example, if a train is running late, the subsequent trains can be rescheduled in order to maintain an optimal flow and minimise any system-wide impacts. Operating data from different sources is key for train operators when predicting and managing train delays. This proactive approach not only enhances the passenger experience, but also contributes to the railway network's economic performance.

4.2 Streamlining the short-term disposition of trains

In the fast-paced environment of train operations, the disposition of trains – especially given the strain of disruptions such as construction events – is a testament to the power of operating data. AI-driven algorithms fuelled by the aggregated data within data spaces can swiftly analyse and interpret this information to orchestrate timely adjustments that are critical during any such unforeseen events. These AI algorithms can dynamically optimise routes by processing the current and historical telemetry data, signal statuses and route details, thus identifying the most efficient paths around any obstructions. Schedules can be recalibrated in near real-time, thereby leveraging the interconnected data streams to minimise any delay propagation throughout the network. Resource allocation also becomes more intelligent and responsive with the aid of operating data. An understanding of the current disposition of the trains and predictions of potential bottlenecks enable re-

cen wie Fahrzeuge, Personal und Hilfskräfte strategisch dort eingesetzt werden, wo sie am dringendsten benötigt werden, um die Zufriedenheit der Fahrgäste zu gewährleisten.

5 Security Monitoring und On-Board-Systeme: Verbesserung der Cybersicherheit im Schienenverkehr

Im Zeitalter des digitalen Wandels sind Fahrzeuge und Eisenbahninfrastruktur zunehmend miteinander vernetzt, was die betriebliche Effizienz und das Erlebnis für die Fahrgäste verbessert. Diese Konnektivität birgt jedoch auch Schwachstellen, die sie zu potenziellen Zielen für Cyberangriffe machen. Cyberangriffe auf Fahrzeuge lassen sich grob in zwei Klassen unterteilen. Die erste Klasse konzentriert sich auf einzelne Fahrzeuge und nutzt spezifische Schwachstellen des jeweiligen Fahrzeugs aus. Diese Angriffe können zwar den Betrieb des anvisierten Fahrzeugs stören, ihre Auswirkungen sind jedoch oft lokal begrenzt. Umgekehrt ist die zweite Klasse von Angriffen heimtückischer. Indem sie auf öffentliche Schnittstellen oder Ökosystemschnittstellen abzielen, können Angreifer diese Angriffe so gestalten, dass sie skalierbar sind, sodass sie mehrere Fahrzeuge einer Flotte gleichzeitig angreifen können. Die Auswirkungen solcher Angriffe sind weitreichend und stellen nicht nur eine erhebliche Bedrohung für die betriebliche Integrität des Eisenbahnsystems, sondern auch für die Sicherheit der Fahrgäste dar. Angesichts der kritischen Natur dieser Bedrohungen besteht ein dringender Bedarf an fortschrittlichen Security Monitoring Lösungen. Zusätzlich zu den klassischen Klassifizierungsmechanismen, z. B. durch Schwellenwerte, erweisen sich KI und ML in dieser Hinsicht als wirksames Instrument, das Fähigkeiten zur Erkennung, Abschwächung und Verhinderung potenzieller Cyberbedrohungen und abnormalen Verhaltens in Echtzeit bietet und so die Sicherheit und Zuverlässigkeit des modernen Eisenbahnbetriebs gewährleisten kann. Sicherheits- und betriebliche Bahnsysteme, die traditionell auf deterministische Feldbuskommunikation angewiesen sind, liegen in der KI- und ML-basierten Sicherheitsforschung hinter dem Automobilsektor zurück. Das vom Bundesministerium für Bildung und Forschung geförderte Projekt FINESSE (Förderkennzeichen 16KIS1584K) widmet sich dieser Problematik durch die Entwicklung von Security Monitoring Ansätzen und Sensoren für z. B. den Multifunction Vehicle Bus (MVB). Das Projekt stellt ein modulares und anpassungsfähiges System zur Erkennung von Cyberangriffen vor, das sowohl für die Eisenbahn- als auch für die Automobilindustrie geeignet ist. Durch die Analyse, Anpassung und Weiterentwicklung von Ansätzen wie X-CANIDS [1] zu X-MVBIDS demonstriert FINESSE [2, 3] eine effektive Erkennung von Masquerade- und unbemerkten Fabrikationsangriffen auf MVB und den Controller-Area-Network (CAN)-Bus auf der Grundlage von Autoencodern. Die Evaluierung erfolgte unter Verwendung des ROAD-Datensatzes (Automobil) und proprietärer MVB-Datensätze, die von europäischen Bahnbetreibern und Zugherstellern bereitgestellt wurden. Die Erkennung von Angriffen wie Suspensionsangriffen und Fabrikationsangriffen stellt jedoch eine Herausforderung dar und verdeutlicht die Komplexität der Sicherheit von Eisenbahnsystemen. Die Forschungs- und Entwicklungsarbeiten in diesem Projekt und auf diesem Gebiet werden fortgesetzt, um die Grenzen der KI-basierten Sicherheitslösungen für Eisenbahnsysteme kontinuierlich zu erweitern.

5.1 Vehicle Security Operations Centers (VSOC): Der Cybersecurity-Hub

Vehicle Security Operations Centers (VSOC) sind ein integraler Bestandteil einer modernen Cyberverteidigungsstrategie im Schienenverkehr. Bei diesen Zentren handelt es sich um spezialisierte

sources such as rolling stock, crew and support personnel to be strategically deployed to where they are needed most, thus ensuring service continuity and passenger satisfaction.

5 Security monitoring and on-board systems: Enhancing railway cybersecurity

Vehicles and railway infrastructure have become increasingly interconnected in the age of digital transformation, thereby enhancing operating efficiency and the passenger experience. However, this connectivity also presents vulnerabilities and makes them potential targets for cyber-attacks. Cyber-attacks on vehicles can be broadly categorised in two types. The first focuses on individual vehicles and exploits the specific vulnerabilities that are unique to that vehicle. While these attacks can disrupt the operations of the targeted vehicle, their impact is often localised. On the other hand, the second type of attack is more insidious. By targeting public or ecosystem interfaces, adversaries design these attacks to be scalable, thereby allowing them to compromise multiple vehicles across a fleet simultaneously. The implications of such attacks are far-reaching and pose significant threats not only to the operational integrity of the railway system, but also to passenger safety. Given the critical nature of these threats, there is an imperative need for advanced security monitoring solutions. In addition to classical classification mechanisms such as thresholding, AI and ML have emerged as potent tools in this regard, as they offer capabilities to detect, mitigate and prevent potential cyber threats and abnormal behaviour in real-time to ensure the security and reliability of modern railway operations. Safety and operational railway systems, which have traditionally been reliant on deterministic fieldbus communication, are lagging behind the automotive sector in AI and ML based security research. The FINESSE project, funded by the German Ministry of Education and Research (funding code: 16KIS1584K), is addressing this by developing security monitoring approaches and sensors for the Multifunction Vehicle Bus (MVB) amongst other things. The project has introduced a modular, adaptable intrusion detection system that is applicable to both the railway and automotive industries. Analysing, adapting and evolving approaches such as X-CANIDS [1] to X-MVBIDS and FINESSE [2, 3] has demonstrated effective detection of masquerade and non-stealthy fabrication attacks on the MVB and CAN (Controller Area Network) buses based on autoencoders with evaluations conducted using the ROAD (automotive) dataset and proprietary MVB datasets provided by European rail operators and train manufacturers. However, it faces challenges when detecting attacks such as suspension and stealthy fabrication attacks, thereby highlighting the complexity of railway system security. The research and development in this project and field are ongoing, continually advancing the frontier of AI-based security solutions in railway systems.

5.1 Vehicle Security Operations Centres (VSOCs): the cybersecurity hub

Vehicle Security Operations Centres (VSOCs) represent a critical component in the modern railway cyber defence strategy. These centres are specialised units dedicated to monitoring, detecting and responding to security threats targeting railway vehicles and infrastructure. Operating around the clock, VSOCs employ a combination of advanced technologies and

Einheiten, die sich der Überwachung, Erkennung und Reaktion auf Sicherheitsbedrohungen widmen, die auf Schienenfahrzeuge und Infrastruktur abzielen. VSOC arbeiten rund um die Uhr und setzen eine Kombination aus fortschrittlichen Technologien und fachkundigem Personal ein, um große Datenmengen zu analysieren, potenzielle Schwachstellen zu erkennen und rechtzeitig Gegenmaßnahmen gegen Cyberbedrohungen einzuleiten. Ein besonderes Merkmal der VSOC ist ihre Fähigkeit, Daten aus verschiedenen Quellen und mehreren Fahrzeugen zusammenzuführen. Diese umfassende Perspektive ermöglicht es ihnen, Muster und Anomalien zu erkennen, die auf Cyberbedrohungen hinweisen, die nicht nur auf einzelne Fahrzeuge, sondern auf eine ganze Flotte abzielen. Wenn Angriffsdaten zwischen Betreibern ausgetauscht werden, kann das VSOC außerdem Bedrohungen erkennen und abwehren, die sich über die Flotten mehrerer Betreiber erstrecken. Durch die kontinuierliche Überwachung des Datenverkehrs und der Systemaktivitäten können VSOC Anomalien, unbefugte Zugriffsversuche und andere Anzeichen für potenzielle Cyberangriffe erkennen. Sobald eine Bedrohung erkannt wird, kann das Zentrum schnell mit den zuständigen Teams koordinieren, um das Risiko zu mindern und so eine minimale Störung des Bahnbetriebs und der Sicherheit der Fahrgäste zu gewährleisten.

5.2 Überwachung der Sicherheit an Bord: Die Frontlinie der Cyberverteidigung im Schienenverkehr

VSOC spielen zwar eine unverzichtbare Rolle bei der Cyberabwehr im Bahnverkehr, doch die Menge der von modernen Bahnsystemen erzeugten Daten stellt eine Herausforderung dar. Aufgrund

expert personnel to analyse vast amounts of data, identify potential vulnerabilities and initiate timely countermeasures against any cyber threats. A distinguishing feature of VSOCs is their ability to aggregate data from diverse sources and multiple vehicles. VSOCs obtain a holistic security view of the entire railway ecosystem by consolidating this data. This comprehensive perspective allows them to detect patterns and anomalies that might indicate cyber threats targeting not just individual vehicles, but also an entire fleet. Furthermore, when attack data is shared among operators, the VSOC can identify and counteract any threats that span multiple operators' fleets, thereby enhancing the collective security posture of the railway industry. The primary purpose of a VSOC is to ensure the digital integrity and security of railway operations. By continuously monitoring data traffic and system activities, VSOCs can detect anomalies, unauthorised access attempts and other signs of potential cyber-attacks. Once a threat has been identified, the centre can quickly coordinate with the relevant teams to mitigate the risk, thereby ensuring minimal disruption to railway operations and passenger safety.

5.2 On-board security monitoring: the frontline of railway cyber defence

While VSOCs play an indispensable role in railway cyber defence, the sheer volume of data generated by modern railway systems presents a challenge. Data rate limitations and the need for efficiency mean that it is impractical to transport all

der begrenzten Datenrate und der Notwendigkeit der Effizienz ist es unpraktisch, all diese Daten zur Analyse an das Backend-VSOC zu übertragen. Diese Einschränkung macht eine Änderung der Strategie erforderlich. Ein Teil der Überwachung und Erkennung der Fahrzeugsicherheit muss daher in den Fahrzeugen selbst erfolgen. Die Erkennung von Denial of Service (DoS)-Angriffen, die Kommunikations- oder Betriebsfunktionen eines Fahrzeugs schnell lahmlegen können, erfordert beispielsweise eine große Menge an zu analysierenden Netzwerkdaten. Darüber hinaus würde die Übertragung von DoS-Angriffsdaten an ein VSOC keinen zusätzlichen Nutzen für die Analyse oder Erkennung bringen. Durch die Implementierung von On-Board-Sicherheitssystemen können potenzielle Bedrohungen wie diese direkt an der Quelle identifiziert und entschärft werden, bevor sie eskalieren oder sich auf andere Teile des Netzes ausbreiten. Während das Backend-VSOC einen umfassenden Überblick über die Sicherheitsmaßnahmen bietet und diese koordiniert, fungiert die fahrzeugseitige Überwachung als erste Verteidigungslinie, die eine unmittelbare Reaktion auf Bedrohungen gewährleistet und die digitale Grenze des Eisenbahnökosystems schützt.

6 Stärkung der Cybersicherheit im Eisenbahnbetrieb

Betriebsdaten, die für einen effizienten Betrieb unverzichtbar sind, stellen ein Ziel für Cyberbedrohungen dar. Verletzungen können zu unbefugtem Systemzugriff, Unterbrechungen des Dienstes und Beeinträchtigungen der Sicherheit und Privatsphäre der Fahrgäste führen. In der Vergangenheit gab es verschiedene Cyberangriffe auf Bahnsysteme, die vom Eindringen in Signalsysteme bis hin zur Unterbrechung von Fahrkartenverkauf und Fahrplandienst reichten. Beispiele sind die Manipulation von Betriebsdaten durch Angreifer, um Verspätungen zu verursachen, Datendiebstahl und sogar die Erpressung von Lösegeld für Systeme (Ransomware). Um diese Risiken zu mindern, ist die Implementierung robuster Verschlüsselungsstandards zum Schutz der Daten sowohl im Ruhezustand als auch bei der Übertragung von entscheidender Bedeutung. Regelmäßige Sicherheitsprüfungen (Audits) spielen eine wichtige Rolle bei der Ermittlung und Behebung von Schwachstellen und stellen sicher, dass sich die Maßnahmen zur Cybersicherheit mit den neuen Bedrohungen weiterentwickeln. Im Zuge des digitalen Wandels in der Bahnindustrie muss die Komplexität der Cyberabwehr mit der Komplexität der potenziellen Bedrohungen Schritt halten. Dies gewährleistet die Integrität und Widerstandsfähigkeit kritischer Verkehrsinfrastrukturen und schützt die Daten, die die Grundlage des Bahnbetriebs bilden.

7 Schlussfolgerung: Balance zwischen Innovation und Verantwortung

Das Bahnökosystem mit seinen verschiedenen Akteuren und komplexen Datenarten steht vor der doppelten Aufgabe, die transformative Kraft der KI zu nutzen und die damit verbundenen Herausforderungen zu bewältigen. Der Weg der Eisenbahnindustrie zur Nutzung von Betriebsdaten für mehr Effizienz und Sicherheit führt durch eine Landschaft voller Herausforderungen und Zukunftsüberlegungen:

7.1 Anpassung von KI an dynamische Eisenbahnumgebungen

KI-Lösungen, die von Natur aus transformativ sind, müssen sich an das sich ständig verändernde Bahnumfeld anpassen. Dazu gehören schwankende Fahrgastzahlen, unterschiedliche Wartungspläne und sich verändernde Infrastrukturbedingungen.

this data to the backend VSOC for analysis. This limitation necessitates a shift in strategy. A portion of the vehicle security monitoring and detection must occur on-board the vehicles themselves in order to address this. For instance, detecting Denial of Service (DoS) attacks, which can quickly incapacitate a vehicle's communication or operating capabilities, requires a lot of network data to analyse. Furthermore, transferring DoS-attack related data to a VSOC would not add any further value to the analysis or detection. Implementing on-board security systems means that potential threats such as these can be identified and mitigated directly at the source before they escalate or spread to any other parts of the network. In essence, the on-board monitoring acts as the first line of defence that ensures an immediate response to any threats and safeguards the railway ecosystem's digital frontier, while the backend VSOC provides a comprehensive overview and coordination of security measures.

6 Fortifying cybersecurity in railway operations

The critical need for data protection in railway operations is highlighted by the vulnerabilities inherent in the operating data. This data, which is essential for efficient operations, constitutes a target for cyber threats with breaches potentially leading to unauthorised system access, service disruptions and compromises in passenger safety and privacy. Historical cyber-attacks on rail systems have varied from the infiltration of signalling systems to the disruption of ticketing and scheduling services. These incidents have resulted in financial losses, eroded public trust and, most critically, risked safety. Examples include attackers manipulating operating data to cause delays, data theft and even the holding of systems for ransom. The implementation of robust encryption standards is crucial to mitigate these risks and protect the data when both at rest and in transit. Access controls are equally vital, as limiting the data access to authorised personnel reduces the risk of internal threats and accidental breaches. Regular security audits play a key role in identifying and addressing any vulnerabilities, thereby ensuring that the cybersecurity measures evolve alongside any emerging threats. The development and enforcement of comprehensive cybersecurity policies are essential in order to align all the stakeholders in the effort to protect the operating data. This approach to cybersecurity is dynamic and requires constant attention, the integration of advanced technology and a strong culture of security awareness. As the railway industry continues its digital transformation, the sophistication of its cyber defences must also match the complexity of the potential threats. This will ensure the integrity and resilience of critical transportation infrastructures and safeguard the data that underpins the railway operations.

7 Conclusion: balancing innovation and responsibility

The railway industry's journey towards leveraging its operating data for enhanced efficiency and safety is currently navigating a landscape filled with challenges and future considerations.

7.1 Adapting AI to dynamic railway environments

AI solutions, which are transformative by nature, must be able to adapt to the ever-changing railway environment. This includes fluctuating passenger loads, varying maintenance

7.2 Kontinuierliche Investitionen in die Cybersicherheit

Mit zunehmender Integration von KI sind kontinuierliche Investitionen in die Cybersicherheit unerlässlich. Der Schutz dieser fortschrittlichen, vernetzten Systeme vor Cyberbedrohungen erfordert kontinuierliche Investitionen in modernste Sicherheitstechnologien, professionelle Schulungen und die Bereitschaft zur Reaktion auf Vorfälle.

7.3 Einhaltung der DSGVO

Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) ist sowohl eine Herausforderung als auch eine Chance. Bahnbetreiber müssen sicherstellen, dass ihre Datenpraktiken transparent und sicher sind und die DSGVO-Vorgaben für Datenzugriff, -verarbeitung und -löschung einhalten.

Die Bahnindustrie muss diese Herausforderungen mit einer vorausschauenden Denkweise angehen. Es ist von entscheidender Bedeutung, ein Gleichgewicht zwischen der Nutzung der Vorteile datengesteuerter KI-Anwendungen und dem Schutz vor potenziellen Risiken zu finden. Die wichtigsten Voraussetzungen für den erfolgreichen Einsatz von KI sind:

- Ein offener, kooperativer und vielseitiger Ansatz für die Daten und Lösungen.
- Frühzeitige (jetzt) Systementwicklung und -integration, die eine flexible Verbesserung der Datenerfassung, der Datenverwaltung, des Datenschutzes und der Integration von KI-Algorithmen ermöglicht.

Die Zukunft des Bahnbetriebs hängt von der Fähigkeit der Branche ab, KI verantwortungsvoll zu nutzen, die Effizienz und das Kundenerlebnis zu verbessern und gleichzeitig ihre digitalen und physischen Vermögenswerte zu schützen. Da KI für die Entwicklung der Bahnindustrie von zentraler Bedeutung ist, wird ihr Weg zur digitalen Transformation durch ihr Engagement für die Wahrung dieses Gleichgewichts bestimmt. Dieses Engagement ist der Schlüssel zur Gewährleistung eines sicheren, effizienten und nachhaltigen Eisenbahnsystems für die Zukunft. ■

LITERATUR | LITERATURE

[1] Jeong, S.; Lee, S.; Lee, H.; Kim, H. K.: X-CANIDS: Signal Aware Explainable Intrusion Detection System for Controller Area Network-Based In-Vehicle Network. arXiv:2303.12278 [cs.CR], 2023
[2] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/finesse
[3] https://www.linkedin.com/showcase/finesse-bmbf

AUTOREN | AUTHORS

Dominik Spychalski, M.Sc.
Security Expert
Incyde industrial cyber defense GmbH
Anschrift / *Address*: Rheinstraße 16a, D-64283 Darmstadt
E-Mail: dominik.spychalski@incyde.com

Dr. Nicolai Erbs
AI Solutions Product Owner
T-Systems International GmbH
Anschrift / *Address*: Hahnstraße 43, D-60528 Frankfurt am Main
E-Mail: nicolai.erbs@t-systems.com

Ali Recai Yekta, M.Sc.
Head of Cybersecurity
Yekta IT GmbH
Anschrift / *Address*: Ruhrallee 9, D-44139 Dortmund
E-Mail: ali-recai@yekta-it.de

schedules and evolving infrastructure conditions. AI systems need the flexibility to learn and adapt in real-time, so as to provide operators with accurate and actionable insights.

7.2 Continuous investments in cybersecurity

As AI integration deepens, continuous investments in cybersecurity are essential. Protecting these advanced, interconnected systems from cyber threats requires ongoing investments in cutting-edge security technologies, professional training and incident response preparedness.

7.3 Compliance with GDPR

Compliance with General Data Protection Regulation (GDPR) constitutes both a challenge and an opportunity. It sets a high standard for data protection that emphasises individual control over personal data and imposes strict penalties for non-compliance. Railway operators must ensure that their data practices are transparent and secure while adhering to the GDPR mandates pertaining to data access, processing and deletion.

The railway industry must approach these challenges with a forward-thinking mindset that embraces technological advancements while strictly adhering to data protection and cybersecurity standards. This approach will secure the benefits of AI and data analytics, thereby ensuring a future for rail travel that is not only smarter and more efficient, but also safer and more respectful of passenger privacy.

The integration of AI into the railway industry presents a landscape filled with opportunities and responsibilities. As data becomes central to innovation and operating excellence, it also necessitates rigorous data protection, advanced cybersecurity and adherence to regulations such as GDPR. The railway ecosystem, with its diverse stakeholders and complex data types, faces the dual task of harnessing AI's transformative power and addressing the challenges it brings. This involves ensuring privacy, adapting AI to ever-changing operating conditions and sustaining continuous investment in cybersecurity. Achieving a balance between reaping the benefits of data-driven AI applications and protecting against their potential risks is crucial. The key requirements for the successful use of AI will be:

- an open, collaborative and multifaceted approach to data and solutions
- early (now) system design and integration that allows flexible improvement in data gathering, data management and data protection and the integration of AI algorithms.

The future of rail operations hinges on the industry's ability to responsibly leverage AI, thereby enhancing efficiency and the customer experience while securing its digital and physical assets. As AI becomes central to the railway industry's evolution, its journey towards digital transformation will be defined by its commitment to maintaining this balance. This commitment is key to ensuring a safe, efficient and sustainable railway system for the future. ■