Multi-modales Intrusion Detection System: Angriffserkennung für Mobilitätssysteme

Multi-modal intrusion detection system: attack detection for mobility systems

Dominik Spychalski | Markus Heinrich | Ali Recai Yekta | Jens Gramm | Andreas Isbarn

Cyber-Angriffe auf vernetzte Straßen- und Schienenfahrzeuge stellen eine zunehmende Gefahr für Mensch und Maschine dar. Die Vernetzung dieser Fahrzeuge sowie der Einsatz externer Technologien erweitern die potenziellen Angriffsflächen erheblich [2]. Ein zentrales Element einer Sicherheitsarchitektur sind Intrusion-Detection-Systeme (IDS), um Angriffe frühzeitig erkennen und darauf reagieren zu können. Sie erkennen verdächtige Aktivitäten und Anomalien, überwachen potenzielle Schwachstellen und liefern wichtige Daten zur Analyse und Meldung von Vorfällen. Damit tragen solche Systeme nicht nur zur Absicherung kritischer Systeme wie der Verkehrsinfrastruktur bei, sondern auch zur Einhaltung regulatorischer Anforderungen.

1 Einleitung

Trotz der Unterschiede zwischen Straßen- und Schienenverkehr weisen die IT- und OT-Systeme beider Sektoren aus einer Sicherheits- und Architektursicht viele Gemeinsamkeiten auf. Dies eröffnet die Möglichkeit, ganzheitliche, multi-modale Sicherheitslösungen zu entwickeln, die sowohl hersteller- als auch flottenübergreifende Analysen und Schutzmaßnahmen unterstützen [1].
Das BMBF-geförderte Projekt FINESSE (Cyber Schutzsysteme für Fahrzeuge und Infrastruktur im Straßen- und Schienenverkehr) stärkt die IT / OT-Sicherheit im Personen- und Güterverkehr. Partner wie DB Systemtechnik, ETAS GmbH, Fraunhofer SIT, Incyde GmbH, die Universität Passau und Yekta IT GmbH entwickeln Technologien für Security-Monitoring und Sicherheitsanalysen. Fokus liegt auf On-board-Detektionsmechanismen, einem Vehicle-Security-Operations-Centre (VSOC) sowie der Integration von IDS in Bestandsfahrzeuge. Untersucht werden Ethernet- und Feldbus-Kommunikation sowie host-basierte Sensoren. Ein Schwerpunkt ist die sichere Datenübertragung zwischen Fahrzeugen und VSOC. Als bahnseitiger Versuchsträger dient das „advanced Train Lab" (aTL) der Deutschen Bahn AG (DB). Das Projekt legt die Grundlage für praxisnahe Sicherheitslösungen in der modernen Mobilität.

2 Vergleich: Automotive vs Rail

Security-Überwachung ist in der Bahnwelt noch Neuland, während sie bei Straßenfahrzeugen bereits etabliert ist und erste Standardisierungsansätze existieren. Ein Vergleich der Domänen zeigt, welche Automotive-Erfahrungen übertragbar sind und wo Unterschiede bestehen. Im Folgenden werden drei Themenbereiche analysiert.

Cyber-attacks on networked road and rail vehicles pose an increasing threat to people and machines. The networking of these vehicles and the use of external technologies have significantly expanded the potential attack surfaces [2]. Intrusion detection systems (IDS) are a central element in the security architecture used to detect and respond to attacks at an early stage. They detect suspicious activities and anomalies, monitor any potential vulnerabilities and provide important data for analysing and reporting incidents. In this way, such systems not only help to secure critical systems such as the transport infrastructure, but also to ensure compliance with the regulatory requirements.

1 Introduction

Despite the differences between road and rail transportation, the IT and OT systems of both sectors have many similarities from a security and architectural perspective. This opens up the possibility of developing holistic, multi-modal security solutions that support both cross-manufacturer and cross-fleet analyses and protective measures [1]. The BMBF-funded FINESSE project is strengthening IT / OT security in passenger and freight transport. Partners such as DB Systemtechnik, ETAS GmbH, Fraunhofer SIT, Incyde GmbH, the University of Passau and Yekta IT GmbH are developing technologies for security monitoring and analysis. The focus is on on-board detection mechanisms, the Vehicle Security Operations Centre (VSOC) and the integration of IDS into existing vehicles. Ethernet and fieldbus communication as well as host-based sensors are being investigated. One focus is on secure data transmissions between vehicles and the VSOC. Deutsche Bahn AG's (DB) "advanced Train Lab" (aTL) serves as a test vehicle for railroad operations. The project is laying the foundation for practical safety solutions in modern mobility.

2 A comparison: automotive vs rail

Security monitoring is still uncharted territory in the railroad world, whereas it has already become established in road vehicles and initial standardisation approaches now exist. A comparison of these domains shows which automotive experiences are transferable and where there are differences. Three subject areas are analysed below.

2.1 Fahrzeugzulassung und Anforderungen an Sensoren

In Straßenfahrzeugen sind IDS-Sensoren eine schon heute eingesetzte Technologie. IDS-Sensoren werden in Form von Softwarekomponenten angeboten, die in die Steuergerätesoftware integriert werden. So ist oft auch ein Nachrüsten von IDS-Sensoren über Software-Updates möglich.

Für die IDS-Sensor-Komponente ist in der Regel keine spezifische Safety-Klassifikation notwendig – die relevante Safety-Norm im Fahrzeugbereich ist die ISO 26262. Da es sich bei einem IDS-Sensor um eine rein passiv beobachtende Komponente handelt, ist der IDS-Sensor kein "Aktor" im System und ist in der Regel auch nicht in eine Funktionskette eingebunden, die eine spezielle Safety-Klassifikation erfordert. Die IDS-Sensoren erhalten Datenpakete parallel zum eigentlichen Nachrichtenstrom zur Prüfung und führen somit zu keiner Latenz der Nachrichten.

Auch eine mögliche Busüberlastung durch IDS-Nachrichten führt zu keinen spezifischen Anforderungen an die Safety-Klassifikation – im Allgemeinen müssen Fahrzeugbusse Überlastszenarien tolerieren können. In der Praxis wird dieser Fall durch die Netzwerkkonfiguration verhindert. So kann z. B. festgelegt werden, dass der Sensor auf einem CAN-Bus Nachrichten nur in einem zugewiesenen zyklischen Raster senden kann. Zudem können IDS-Management-Komponenten die über den Bus gesendete Datenmenge konfigurierbar beschränken.

Schienenfahrzeuge stellen höhere Anforderungen an IDS-Sensoren, da sicherheitsrelevante Feldbusse nicht beeinflussbar sein dürfen. Oft werden zertifiziert rückwirkungsfreie Geräte verwendet. Die Integration von IDS-Software in bestehende Komponenten ist aufwendig und erfordert eine Neuzulassung, was zeitnahe Updates erschwert. Daher werden meist parallele, nicht sicherheitsrelevante Security-Architekturen genutzt.

2.2 Ebenen der IDS-Integration

Die Integration von IDS in moderne Fahrzeuge erfolgt über vier Ebenen (Bild 1), die eine umfassende Sicherheitsüberwachung von der einzelnen Komponente bis zur gesamten Flotte ermöglichen. Diese Struktur ist sowohl für Straßen- als auch für Schienenfahrzeuge anwendbar.

2.1 Vehicle approvals and sensor requirements

IDS sensors involve technology that is already used in road vehicles today. They are offered in the form of software components that are integrated into the control unit software. This means that IDS sensors can often be retrofitted during software updates.

As a rule, no specific safety classification is required for the IDS sensor component – the relevant safety standard in the vehicle sector is ISO 26262. Given that an IDS sensor is a purely passive monitoring component, it is not an "actuator" in the system and is generally not integrated into a function chain that requires a special safety classification. The IDS sensors receive data packets for testing in parallel to the actual message stream and therefore do not lead to any latency in the messages.

Even a possible bus overload due to IDS messages will not lead to any specific requirements for the safety classification – in general, vehicle buses must be able to tolerate overload scenarios. In practice, this case is prevented by the network configuration. For example, it can be specified that the sensor on a CAN bus can only send messages in an assigned cyclical grid. IDS management components can also limit the amount of data sent via the bus in a configurable manner.

Rail vehicles place higher demands on IDS sensors, as safety-relevant fieldbuses must not be able to be influenced. Certified non-reactive devices are often used. The integration of IDS software into existing components is complex and requires new approval, which makes timely updates difficult. For this reason, parallel, non-safety-relevant security architectures are usually used.

2.2 Levels of IDS integration

IDS is integrated into modern vehicles via four levels (fig. 1), which enable comprehensive safety monitoring ranging from an individual component through to the entire fleet. This structure can be used for both road and rail vehicles.

The monitoring at the level of the electronic control unit (ECU) is carried out by host-based IDS (HIDS), which analyse system states and behaviour.

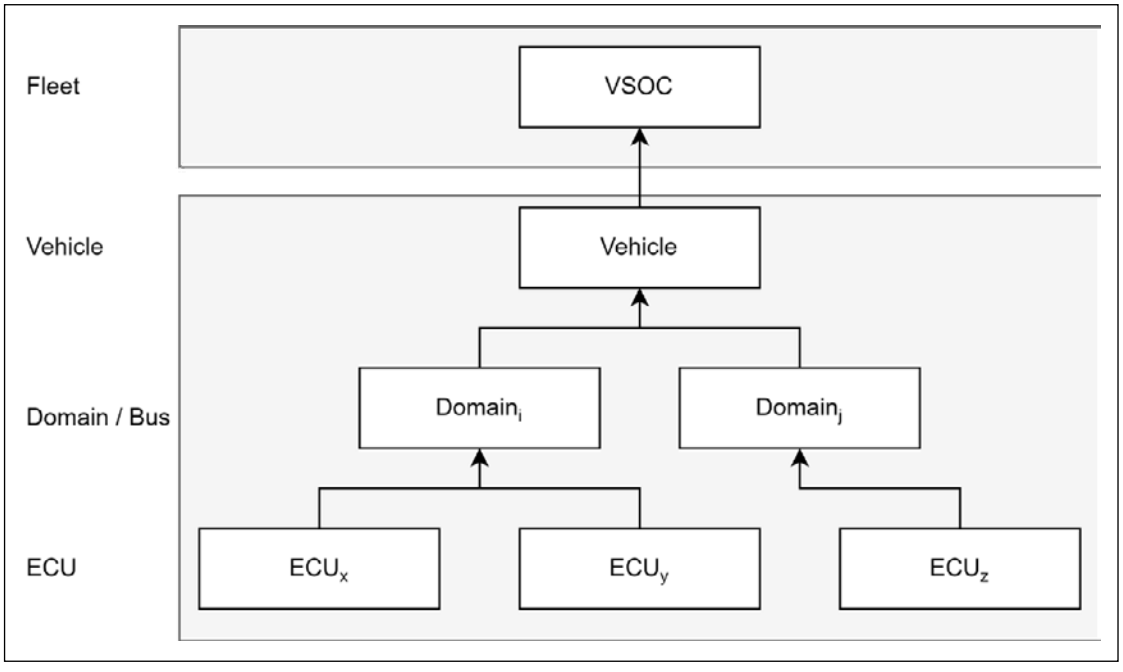

Bild 1: Übersicht der IDS-Integrationsebenen
Fig. 1: An overview of the IDS integration levels

Auf der Steuergerätebene (Electronic Control Units – ECU) erfolgt die Überwachung durch host-basierte IDS (HIDS), die Systemzustände und Verhalten analysieren.
Die Domain / Bus-Ebene erweitert die Überwachung auf ganze Domänen und Bussysteme mittels netzwerkbasiertem IDS (NIDS). Im Automotive-Bereich steht dabei die Überwachung der CAN-Bus-Kommunikation und zunehmend auch Ethernet-basierter Netzwerke im Fokus, während im Schienenverkehr der Multifunction Vehicle Bus (MVB) sowie ebenfalls Ethernet-basierte Systeme überwacht werden.
Auf Fahrzeugebene werden Daten verschiedener Domains und Bussysteme korreliert, was eine domänenübergreifende Analyse von Sicherheitsereignissen ermöglicht. Die Flottenebene ermöglicht das Monitoring ganzer Fahrzeugflotten und die Durchführung fahrzeugübergreifender Analysen. Hier können koordinierte Angriffe auf mehrere Fahrzeuge und die verwendete Infrastruktur (Straße, Schiene) erkannt und systematische Schwachstellen identifiziert werden.

2.3 Standardisierung von IDS-Architekturen und Security Events

Im Automobilbereich existieren proprietäre Security-Monitoring-Lösungen von Anbietern, und Hersteller entwickeln eigene Spezifikationen, was hohe Kosten für alle Beteiligten verursacht.
Aus diesem Grund wurde eine Standardisierung von IDS für Fahrzeuge begonnen. Als Forum zur Standardisierung wurde hier AUTOSAR gewählt, ein Konsortium von Industriepartnern zur Architektur-Standardisierung von Steuergerätesoftware, das allgemein anerkannt ist und jährliche Ergänzungen der Standards erlaubt. Als Ausgangspunkt spezifiziert AUTOSAR mit dem IDS-Manager eine Komponente zur Sammlung und Vorverarbeitung von Security Events auf einem Steuergerät. Verteilte IDS-Manager in den ECU und Gateways sammeln die Security Events der ihnen zugewiesenen lokalen Sensoren ein, filtern nicht-relevante Events bzw. Rauschen heraus, um die Buslast zu minimieren, und übermitteln sie weiter an den IDS-Reporter in der Telematik-Einheit, der sie schließlich – nach weiterer Vorabanalyse – an das VSOC überträgt.
Das "Qualified Security Events"-Format (QSEV) spezifiziert einen einheitlichen Rahmen für Security-Events aus Fahrzeugen. Es erlaubt auch, komplexere Events von proprietären Sensoren in einer einheitlichen Weise zu kapseln. Auf Basis des QSEV-Formats werden auch konkrete Events spezifiziert, mit Details wie Trigger-Bedingungen und zu erhebenden Kontextdaten. Diese Event-Spezifikation wird derzeit jährlich erweitert.
Die Erfahrung zeigt Vorteile einer standardisierten Basis, weshalb auch für die Bahnwelt eine Standardisierung sinnvoll erscheint.

3 Multi-modales und holistisches IDS für Straße und Schiene

Die Cybersicherheitsüberwachung von Fahrzeugen erfordert eine Balance zwischen zentraler Analyse und dezentraler Erkennung. Ein VSOC koordiniert Sicherheitsvorfälle, doch die Datenmengen moderner Fahrzeuge stellen Herausforderungen dar. Effiziente Datenübertragung, oft über öffentliche Netze, und on-board Erkennung, besonders bei Angriffen, die große Datenmengen erzeugen, sind entscheidend. Durch lokale Verarbeitung können Bedrohungen schnell erkannt und kann die Datenübertragung entlastet werden. Dieses Zusammenspiel aus fahrzeugseitiger Erkennung und zentraler Koordination schützt vernetzte Fahrzeugsysteme effektiv.

The domain / bus level extends the monitoring to entire domains and bus systems using network-based IDS (NIDS). In the automotive sector, the focus is on monitoring CAN bus communication and, increasingly, Ethernet-based networks, while in rail transportation the multifunction vehicle bus (MVB) and Ethernet-based systems are also monitored.
At the vehicle level, the data from the different domains and bus systems is correlated, thereby enabling a cross-domain analysis of any security events. The fleet level enables the monitoring of entire vehicle fleets and the performance of cross-vehicle analyses. Here, coordinated attacks on several vehicles and the used infrastructure (road, rail) can be detected and any systematic vulnerabilities identified.

2.3 The standardisation of IDS architectures and security events

In the automotive sector, providers have proprietary security monitoring solutions and manufacturers have developed their own specifications, resulting in high costs for all the parties involved
As such, the standardisation of IDS for vehicles was started for this reason. AUTOSAR, a consortium of industry partners for the architectural standardisation of ECU software which is generally recognised and allows annual additions to the standards, was chosen as the standardisation forum. AUTOSAR specifies the IDS manager, i.e. a component for collecting and pre-processing security events on an ECU, as the starting point. The distributed IDS managers in the ECU and gateways collect the security events from the local sensors assigned to them, filter out any non-relevant events or noise in order to minimise the bus load and forward them to the IDS reporter in the telematics unit, which finally transmits them – after further preliminary analysis – to the VSOC.
The "Qualified Security Events" format (QSEV) specifies a standardised framework for security events from vehicles. This also allows more complex events from proprietary sensors to be encapsulated in a standardised manner. Specific events are also specified on the basis of the QSEV format with details such as trigger conditions and context data to be collected. This event specification is currently being expanded annually.
Experience has shown the advantages of a standardised basis, which is why standardisation also makes sense for the rail world.

3 Multi-modal and holistic IDS for road and rail

The cybersecurity monitoring of vehicles requires a balance between centralised analysis and decentralised detection. A VSOC coordinates security incidents, but the data volumes of modern vehicles pose challenges. Efficient data transmission, often over public networks, and on-board detection are critical, especially for attacks that generate large amounts of data. Local processing can quickly identify threats and reduce the burden on data transmission. This combination of on-board detection and central coordination effectively protects networked vehicle systems.

3.1 On-board

The IDS architecture within a vehicle is hierarchically structured and consists of two central components:
- the smart sensors and
- the Security Event Centre (SEC).

These components work together to ensure comprehensive and efficient monitoring and attack detection.

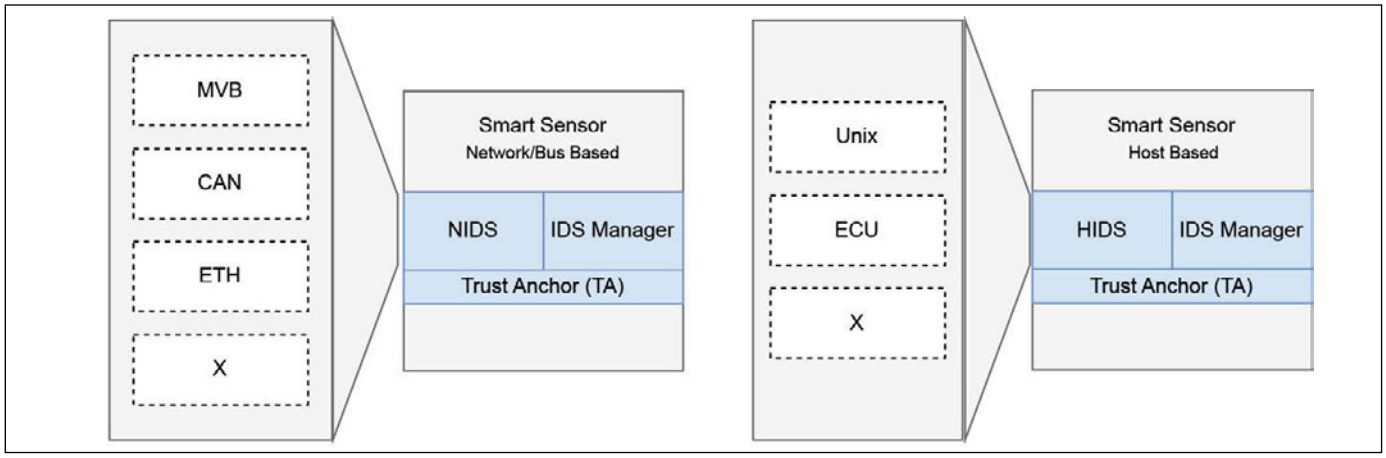

Bild 2: Grobarchitektur einer Smart-Sensor-Komponente. Links: NIDS, rechts: HIDS
Fig. 2: The rough architecture of a smart sensor component. Left: NIDS, right: HIDS

3.1 On-Board

Die IDS-Architektur innerhalb eines Fahrzeugs ist hierarchisch strukturiert und besteht aus zwei zentralen Komponenten:

- den Smart Sensors und
- dem Security Event Centre (SEC).

Diese Komponenten arbeiten zusammen, um eine umfassende und effiziente Überwachung sowie Angriffserkennung zu gewährleisten.

3.1.1 Smart Sensors: technologiespezifische Überwachung

Die Smart Sensors konzentrieren sich auf spezifische Technologien im Fahrzeug, wie z. B. Netzwerke oder Host-Systeme. Sie bestehen aus zwei Hauptkomponenten:

- Sensorkomponente: Diese sammelt relevante Daten aus dem überwachten System, sei es aus dem Fahrzeugnetzwerk oder direkt von Host-Systemen.
- Technologiespezifisches IDS: Dieses System filtert die erfassten Daten, führt Voranalysen durch und erkennt potenzielle Angriffe auf Basis der jeweiligen Technologie.

Durch diesen spezialisierten Ansatz kann der Smart Sensor gezielt Bedrohungen in einem klar definierten Bereich eines Fahrzeugs identifizieren. Es existieren zwei grundlegende Ausprägungen (Bild 2).

Netzwerk- / Busbasierte Smart Sensors überwachen die Kommunikation in fahrzeugspezifischen Netzwerken wie CAN-Bus im Automobilbereich oder MVB in Schienenfahrzeugen sowie zunehmend Ethernet-basierte Systeme in beiden Domänen. Die NIDS-Komponente realisiert dabei das passive Abhören des Netzwerk- und Feldbusverkehrs sowie die Angriffserkennung. Letztere basiert auf vordefinierten Regeln für bekannte Angriffsmuster und der Analyse von Anomalien im Kommunikationsverhalten.

Host-basierte Smart Sensors fokussieren sich auf die Überwachung einzelner Komponenten wie ECU oder Unix-basierte Systeme. Die HIDS-Komponente erkennt dabei ungewöhnliche Systemzustände, verdächtige Prozessaktivitäten oder Manipulationsversuche durch die kontinuierliche Analyse von System- und Anwendungslogs sowie Verhaltensmustern.

Beide Smart-Sensor-Varianten verfügen über einen IDS-Manager für die Ereignisverarbeitung und einen Trust Anchor (TA). Der TA implementiert grundlegende Sicherheitsfunktionen zum Schutz der Sensoren selbst, wie sichere Kommunikation und Integritätsschutz.

Ethernet-basierte Kommunikation kann über dedizierte Ports eines Switches, über dedizierte TAP, oder über Software direkt auf

3.1.1 Smart sensors: technology-specific monitoring

Smart sensors focus on specific technologies in the vehicle, such as networks or host systems. They consist of two main components:

- The sensor component: this collects any relevant data from the monitored system, whether from the vehicle network or directly from the host systems.
- The technology-specific IDS: this system filters the collected data, carries out preliminary analyses and recognises any potential attacks based on the respective technology.

This specialised approach enables the smart sensor to identify specific threats in a clearly defined area of a vehicle. There are two basic versions (fig. 2).

Network / bus-based smart sensors monitor the communication in vehicle-specific networks such as the CAN bus in the automotive sector or MVB in rail vehicles, as well as increasingly Ethernet-based systems in both domains. The NIDS component implements the passive interception of network and fieldbus traffic as well as attack detection. The latter is based on predefined rules for known attack patterns and an analysis of any anomalies in the communication behaviour.

Host-based smart sensors focus on monitoring individual components such as ECU or Unix-based systems. The HIDS component detects unusual system states, suspicious process activities or manipulation attempts through the continuous analysis of system and application logs as well as behavioural patterns.

Both smart sensor variants have an IDS Manager for event processing and a Trust Anchor (TA). The TA implements the basic security functions to protect the sensors themselves, such as secure communication and integrity protection.

Ethernet-based communication can be intercepted via dedicated ports on a switch, via dedicated TAP or via software directly on the switch in order to passively monitor the network traffic. This usually involves a unidirectional transmission in which the IDS only analyses the incoming data.

Automotive Ethernet switches used in the automotive sector often offer a dedicated computing core (switch core) on which the software components of an intrusion detection system can run. The tests carried out in the hardware (switch fabric), which an automotive Ethernet switch supports for speed reasons, can be taken into account as a basis.

On rail vehicles, attacks on the control technology can be detected by monitoring their communications via the Train Commu-

dem Switch abgehört werden, um den Netzwerkverkehr passiv zu überwachen. Dabei handelt es sich in der Regel um eine unidirektionale Übertragung, bei der das IDS nur die eingehenden Daten analysiert.
Im Automotive-Bereich eingesetzte Automotive Ethernet Switches bieten häufig einen dedizierten Rechenkern (Switch Core), auf dem die Softwareanteile eines Intrusion Detection Systems ablaufen können. Dabei können die in Hardware (Switch Fabric) durchgeführten Prüfungen, die ein Automotive Ethernet Switch aus Geschwindigkeitsgründen unterstützt, als Basis mitberücksichtigt werden.
Auf Schienenfahrzeugen werden Angriffe auf die Leittechnik u. a. erkennbar durch die Beobachtung ihrer Kommunikation über das Train Communication Network (TCN). Diese erfolgt über Feldbusse, wie z. B. MVB, CAN oder Ethernet.
Host-basierte Überwachung erfolgt durch Protokollierung relevanter Ereignisse wie Dateizugriffe, Systemaufrufe und Benutzeraktivitäten. Die Überwachung wird durch Audit-Regeln gesteuert, die festlegen, welche Ereignisse erfasst werden sollen.
Die gesammelten Audit Events werden im Systemlog gespeichert und können mit verschiedenen Analyse-Tools ausgewertet werden. Die Integration in ein übergeordnetes Monitoring-System erfolgt in der Regel über Syslog, wodurch die Ereignisse zentral gesammelt und analysiert werden können.

3.1.2 Security Event Centre (SEC): Konsolidierte Fahrzeugüberwachung

Das SEC aggregiert die von Smart Sensors gesammelten Daten und Security Events, um eine konsolidierte Sicht auf das gesamte Fahrzeug zu bieten. Im Gegensatz zu den technologiespezifischen Smart Sensors führt das SEC technologieübergreifende Analysen und Korrelationen durch. Dies ermöglicht eine ganzheitliche Bewertung von Sicherheitsvorfällen, die über die Grenzen einzelner Technologien hinausgehen.
Das SEC bildet die zentrale Einheit zur konsolidierten Fahrzeugüberwachung (Bild 3). Im Input-Modul werden Logs aus verschiedenen Quellen wie Smart Sensors und Syslog-Agenten gesammelt und über Komponenten wie den IDS-Manager und den Syslog-Server integriert.
Der Managementbereich verarbeitet, normalisiert und speichert die Logs dauerhaft. Diese Persistenz gewährleistet, dass die Daten auch bei einer unterbrochenen Verbindung zum VSOC für Analysen und forensische Zwecke verfügbar bleiben. Zusätzlich erlaubt das Sensor Management die Verwaltung der angebundenen Smart Sensors durch das Deployment und die Aktualisierung von Regeln und Modellen.

nication Network (TCN). This takes place via fieldbuses such as MVB, CAN or the Ethernet.
Host-based monitoring is performed by logging relevant events such as file access, system calls and user activities. The monitoring is controlled by audit rules that define which events are to be recorded.
The collected audit events are stored in the system log and can be evaluated using various analysis tools. Integration into a higher-level monitoring system usually takes place via syslog, thereby allowing the events to be collected and analysed centrally.

3.1.2 The Security Event Centre (SEC): consolidated vehicle monitoring

The SEC aggregates the data and security events collected by smart sensors to provide a consolidated view of the entire vehicle. In contrast to the technology-specific smart sensors, the SEC performs cross-technology analyses and correlations. This enables a holistic assessment of any security incidents that goes beyond the boundaries of the individual technologies.
The SEC forms the central unit for consolidated vehicle monitoring (fig. 3). Logs from various sources such as smart sensors and syslog agents are collected in the input module and integrated via components such as the IDS Manager and the syslog server.
The management area processes, normalises and saves the logs permanently. This persistence ensures that the data remains available for analysis and forensic purposes even if the connection to the VSOC is interrupted. In addition, sensor management allows the connected smart sensors to be managed by deploying and updating the rules and models.
The analytics component enables cross-technology and cross-bus analyses to identify security incidents that affect multiple subsystems. Responders and alerters ensure that there is a rapid response to any detected security events and that relevant stakeholders are alerted in real time.
The logs can be enriched with additional information in post-processing before they are forwarded to a VSOC via the connector. In this way, the SEC creates the basis for comprehensive security monitoring that supports both local vehicle analyses and global security operations.

3.2 The Vehicle Security Operations Centre (VSOC)

A VSOC is a centralised system for monitoring, detecting and responding to security threats in vehicle fleets. A VSOC platform pools data from multiple sources and vehicles, continuously analyses it and detects any patterns or anomalies that indicate

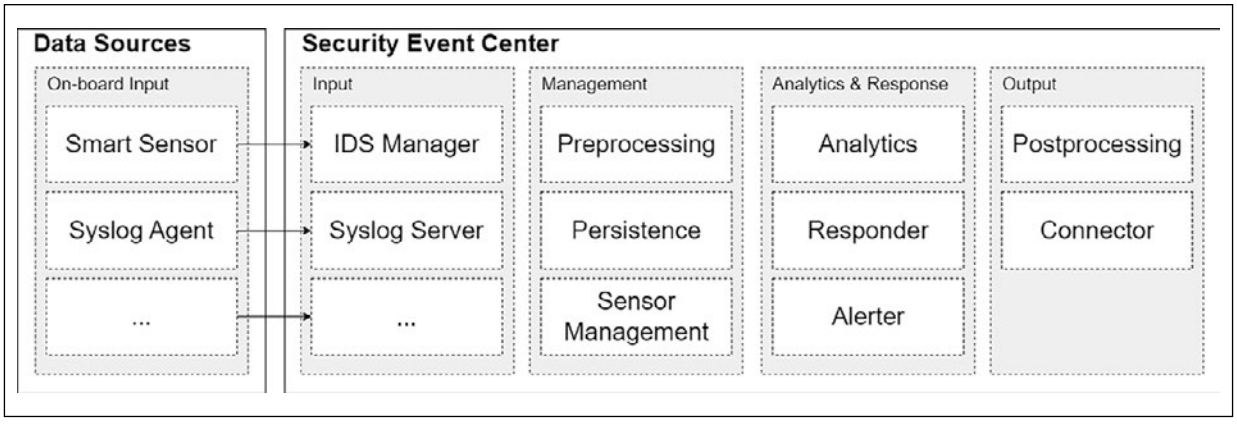

Bild 3: Architektur der SEC-Komponente
Fig. 3: The architecture of the SEC component

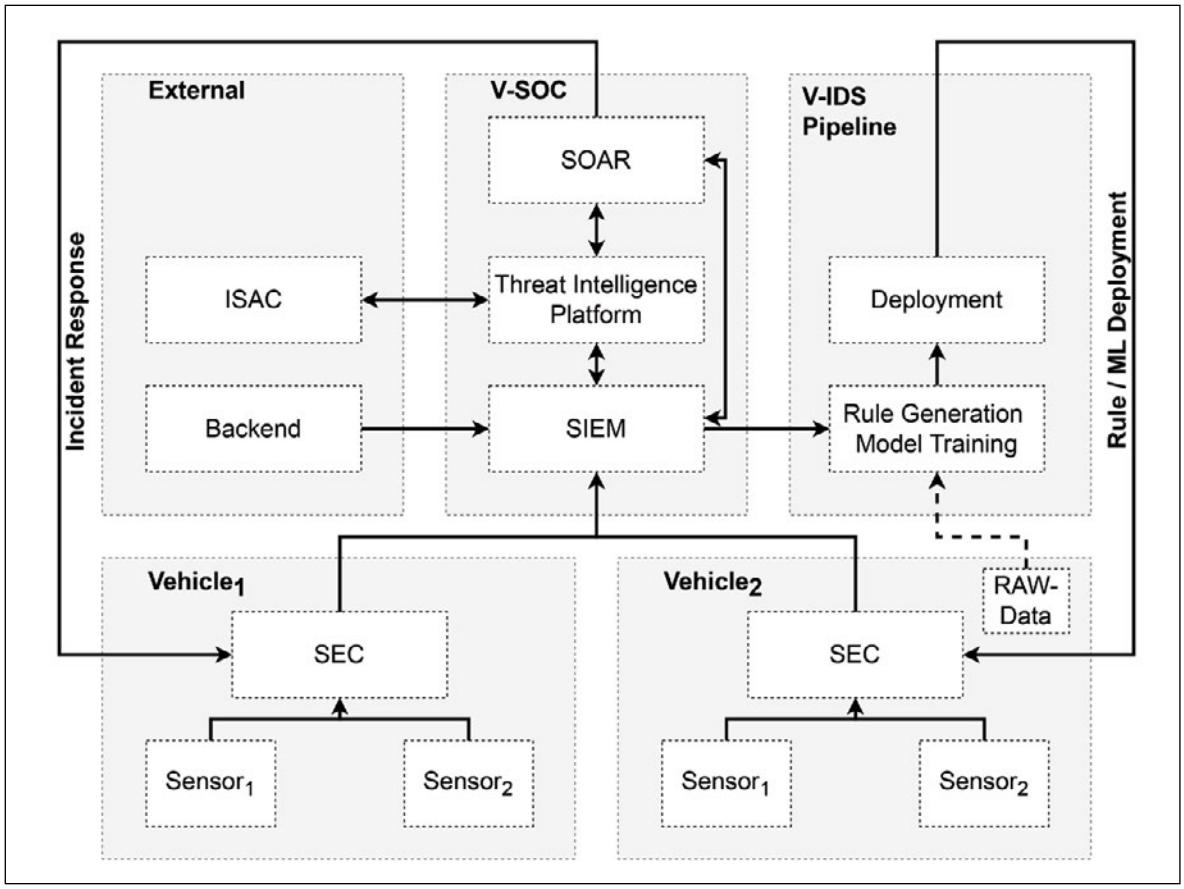

Bild 4: Gesamtarchitektur des multi-modalen IDS mit Fahrzeugen und zentralem VSOC
Fig. 4: The overall architecture of the multi-modal IDS with vehicles and a central VSOC
Quelle (Bilder 1-4)/ *Source (Fig. 1-4)*: Ali Recai Yekta / Yekta IT GmbH

Die Analytics-Komponente ermöglicht technologie- und busübergreifende Analysen, um Sicherheitsvorfälle zu identifizieren, die mehrere Subsysteme betreffen. Responder und Alerter sorgen dafür, dass auf erkannte Sicherheitsereignisse schnell reagiert wird und relevante Akteure in Echtzeit alarmiert werden.
Im Postprocessing können die Logs mit Zusatzinformationen angereichert werden, bevor sie über den Connector an ein VSOC weitergeleitet werden. Dadurch schafft das SEC die Grundlage für eine umfassende Sicherheitsüberwachung, die sowohl lokale Fahrzeuganalysen als auch globale Sicherheitsoperationen unterstützt.

3.2 Vehicle Security Operations Centre (VSOC)

Ein VSOC ist ein zentrales System zur Überwachung, Erkennung und Reaktion auf Sicherheitsbedrohungen in Fahrzeugflotten. Eine VSOC-Plattform bündelt Daten aus verschiedenen Quellen und Fahrzeugen, analysiert diese kontinuierlich und erkennt Muster oder Anomalien, die auf Cyberangriffe hindeuten. Durch die Integration von Daten über mehrere Fahrzeuge oder Betreiber hinweg ermöglicht ein VSOC eine umfassende Perspektive, um Bedrohungen auf Flottenebene zu identifizieren und abzuwehren. Dadurch trägt es entscheidend zur Minimierung von Risiken und zur Aufrechterhaltung eines sicheren Betriebs moderner Fahrzeugflotten bei (Bild 4).
Ein Security Information and Event Management (SIEM) sammelt Log-Daten von verschiedenen Fahrzeugen und bildet die zentrale Komponente eines VSOC. Sämtliche von den Fahrzeugen übermittelten Events und Alarme werden hierbei erfasst. Um die enorme Datenmenge zu bewältigen, erfolgt bereits an Bord der Fahrzeuge eine Vorverarbeitung und Filterung. Smart Sensors erzeugen relevante Meldungen und reduzieren gleichzeitig die Anzahl

cyberattacks. A VSOC provides a comprehensive perspective to identify and defend against any threats at the fleet level by integrating data across multiple vehicles or operators. This makes a decisive contribution to minimising risks and maintaining the safe operation of modern vehicle fleets (fig. 4).
The Security Information and Event Management (SIEM) collects log data from various vehicles and forms the central component of a VSOC. All the events and alarms transmitted by the vehicles are recorded. Pre-processing and filtering take place on board the vehicles in order to cope with the enormous amount of data. Smart sensors generate the relevant messages and simultaneously reduce the number of transmitted messages so that only essential logs are received. The VSOC then integrates these data sets with additional information from the OEM and third-party sources, thereby making it possible to determine whether certain incidents have occurred simultaneously in several vehicles.
A Threat Intelligence Platform supplements the VSOC with up-to-date information on attack methods and vulnerabilities, e.g. from Information Sharing and Analysis Centres (ISAC). The SIEM automatically compares the incoming events with these indicators in order to quickly identify any threats. Security Orchestration, Automation and Response (SOAR) supports the work of the analysts with automated analyses. Asset Management enriches the events with additional information and facilitates incident analysis. Direct responses to vehicles are not possible and the final decisions remain with humans in safety-critical areas such as the rail sector in order to avoid disrupting operations. Optionally, over-the-air (OTA) updates can also be managed centrally to efficiently provide sensors with new rules and machine learning models.

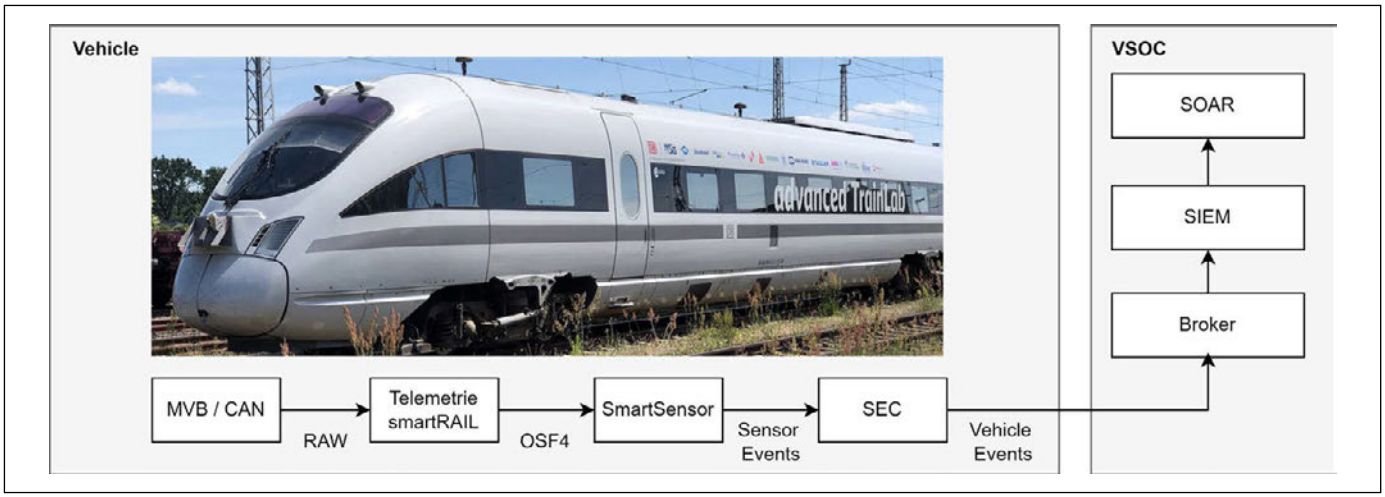

Bild 5: Verarbeitungskette auf dem aTL
Fig. 5: The processing chain on the aTL

Quelle / *Source*: Andreas Isbarn / DB Systemtechnik GmbH

der übertragenen Nachrichten, sodass nur essenzielle Logs empfangen werden. Anschließend integriert das VSOC diese Datensätze mit zusätzlichen Informationen aus OEM- und Drittanbieter-Quellen, wodurch festgestellt werden kann, ob bestimmte Vorfälle gleichzeitig in mehreren Fahrzeugen auftreten.
Eine Threat Intelligence Platform ergänzt das VSOC mit aktuellen Informationen zu Angriffsmethoden und Schwachstellen, z. B. von Information Sharing and Analysis Centres (ISAC). Das SIEM vergleicht eingehende Events automatisch mit diesen Indikatoren, um Bedrohungen schnell zu erkennen. Security Orchestration, Automation and Response (SOAR) unterstützt durch automatisierte Analysen die Arbeit der Analysten. Asset Management bereichert SIEM-Events mit zusätzlichen Informationen und erleichtert die Vorfallsanalyse. Direkte Reaktionen auf Fahrzeuge sind nicht möglich, und in sicherheitskritischen Bereichen wie dem Bahnsektor bleiben finale Entscheidungen beim Menschen, um den Betrieb nicht zu stören. Optional können Over-the-Air (OTA) Updates zentral verwaltet werden, um Sensoren effizient mit neuen Regeln und Machine-Learning-Modellen zu versorgen.

4 Versuchsträger „advanced TrainLab“

Das aTL der DB dient als Versuchsplattform, um das FINESSE IDS für die Bahndomäne zu demonstrieren (Bild 5).
Die Kommunikation über MVB und CAN wird direkt an Bord abgegriffen und als Rohdaten erfasst.
Zum Mitlesen des weit verbreiteten MVB-Busses wird ein kapazitiv abtastendes Klasse 0-Gerät (DIN EN 61375-3-1:2015-10) eingesetzt (Telematics Control Unit, TCU).
Die TCU wandelt die Signale in OSF4-Format um und überträgt sie per User Datagram Protocol (UDP) an einen RailPC. Auf diesem läuft je ein MVB und CAN Smart Sensor, welche die ankommenden OSF4-Daten weiter normalisieren und nach potenziellen Manipulationen untersuchen. Wird eine Anomalie erkannt, erstellt er einen Alarm und leitet diesen an das SEC weiter, das ebenfalls auf der FINESSE-Box angesiedelt ist. Das SEC fasst sämtliche relevanten Ereignisse und Alarme zusammen und sendet sie mittels des Message-Queuing-Telemetry-Transport (MQTT)-Protokolls an das zentrale VSOC. Dort werden sie in einem SIEM erfasst und weiter analysiert. Durch diese abgestimmte Prozesskette lassen sich mögliche Angriffe frühzeitig erkennen, ohne den laufenden Bahnbetrieb zu beeinträchtigen.

4 Test vehicle “advances TrainLab”

DB’s aTL serves as the test platform for demonstrating the FINESSE IDS for the rail domain (fig. 5).
Communication via the MVB and the CAN is tapped directly on board and recorded as raw data.
A capacitive scanning class 0 device (DIN EN 61375-3-1:2015-10) (Telematics Control Unit, TCU) is used to read the widely used MVB bus.
The TCU converts the signals into the OSF4 format and transmits them to a RailPC via User Datagram Protocol (UDP). An MVB and CAN smart sensor run on this, which further normalises the incoming OSF4 data and checks it for potential manipulation. If an anomaly is detected, it generates an alarm and forwards it to the SEC, which is also located on the FINESSE box. The SEC summarises all the relevant events and alarms and sends them to the central VSOC via Message Queuing Telemetry Transport (MQTT). There they are recorded in a SIEM and analysed further. This coordinated process chain allows potential attacks to be detected at an early stage without disrupting any ongoing rail operations.

5 Conclusion and outlook

The development of multi-modal IDS for vehicles and infrastructure shows great potential to significantly improve cyber security in transportation systems. Evaluation runs with the aTL have confirmed the feasibility of the developed approaches and proven the effectiveness of attack detection in real scenarios. The processing chain from the fieldbus to the VSOC makes it possible to detect potential attacks at an early stage and to respond to them efficiently without affecting operations. An important prospect lies in the greater involvement of vehicle and component manufacturers. They must be proactively engaged in order to ensure that the assets can already provide the relevant data for the IDS natively. The standardised and comprehensive provision of this data is essential in order to seamlessly integrate the security solutions into the existing and future vehicle architectures. Transport infrastructure operators also play a central role. They must not only ensure the technical integration of the IDS solutions, but also implement sustainable security management that addresses attacks across the entire lifecycle of the vehicle fleets.

5 Fazit und Ausblick

Der Aufbau eines multi-modalen IDS für Fahrzeuge und Infrastruktur zeigt großes Potenzial, die Cybersicherheit in Transportsystemen entscheidend zu verbessern. Durch Evaluationsfahrten mit dem aTL wird die Machbarkeit der entwickelten Ansätze bestätigt und die Wirksamkeit der Angriffserkennung in realen Szenarien belegt. Die Verarbeitungskette vom Feldbus bis zum VSOC ermöglicht es, potenzielle Angriffe frühzeitig zu erkennen und effizient darauf zu reagieren, ohne den Betrieb zu beeinträchtigen. Ein wichtiger Ausblick liegt in der stärkeren Einbindung von Fahrzeug- und Komponentenherstellern. Diese müssen proaktiv in die Pflicht genommen werden, um sicherzustellen, dass Assets bereits nativ relevante Daten für IDS bereitstellen können. Eine standardisierte und umfassende Bereitstellung dieser Daten ist essenziell, um Sicherheitslösungen nahtlos in bestehende und zukünftige Fahrzeugarchitekturen integrieren zu können. Auch die Betreiber von Verkehrsinfrastrukturen spielen eine zentrale Rolle. Sie müssen nicht nur die technische Integration der IDS-Lösungen sicherstellen, sondern auch ein nachhaltiges Sicherheitsmanagement implementieren, das Angriffe über den gesamten Lebenszyklus von Fahrzeugflotten hinweg adressiert. Dies umfasst den Aufbau eines robusten Incident-Response-Systems, die regelmäßige Überprüfung der Sicherheitsinfrastruktur und die Schulung von Personal. Zukünftige Arbeiten sollten sich auf die Weiterentwicklung von IDS-Lösungen konzentrieren, die sowohl herstellerübergreifend als auch interoperabel zwischen den Domänen einsetzbar sind. Mit zunehmender Vernetzung und technologischer Komplexität wird die Fähigkeit zur adaptiven Bedrohungserkennung und -abwehr unverzichtbar. Die gewonnenen Erkenntnisse aus dem FINESSE-Projekt bilden dabei eine solide Grundlage, um die Mobilität der Zukunft sicher und resilient zu gestalten. ■

This includes building a robust incident response system, regularly reviewing the security infrastructure and training staff. Future work should focus on the further development of IDS solutions that are both multi-vendor and interoperable between domains. Increasing networking and technological complexity mean that the ability to adaptively detect and defend against threats is becoming indispensable. The knowledge gained from the FINESSE project forms a solid basis for making the mobility of the future secure and resilient. ■

LITERATUR | LITERATURE

[1] Spychalski, D.; Heinrich, M.; Krauß, C.: Rail meets Automotive: Gemeinsamkeiten in der fahrzeugseitigen IT/OT-Sicherheitsbetrachtung, SIGNAL+DRAHT (114) 11/2022, S. 51–57

[2] Yekta, A. R.; Spychalski, D.; Yekta, E.; Yekta, C.; Katzenbeisser, S.: VATT&EK: Formalization of Cyber Attacks on Intelligent Transport Systems – a TTP based approach for Automotive and Rail. Proceedings of the 7th ACM Computer Science in Cars Symposium, Association for Computing Machinery, 2023

AUTOREN | AUTHORS

Dominik Spychalski
Senior Security Expert & Manager Strategy and Business Development
INCYDE GmbH
Anschrift / *Address*: Rheinstraße 16a, D-64283 Darmstadt
E-Mail: dominik.spychalski@incyde.com

Dr.-Ing. Markus Heinrich
Senior Security Expert
INCYDE GmbH
Anschrift / *Address*: Rheinstraße 16a, D-64283 Darmstadt
E-Mail: markus.heinrich@incyde.com

Ali Recai Yekta
CTO & Head of Cyber Security
Yekta IT GmbH
Anschrift / *Address*: Ruhrallee 9, D-44139 Dortmund
E-Mail: info@yekta-it.de

Dr. Jens Gramm
Product Manager Offboard Security
ETAS GmbH
Anschrift / *Address*: Borsigstraße 24, D-70469 Stuttgart
E-Mail: jens.gramm@etas.com

Andreas Isbarn
Senior Technical Expert
DB Systemtechnik GmbH
Anschrift / *Address*: Weilburger Str. 22, D-60326 Frankfurt a. M.
E-Mail: andreas.isbarn@deutschebahn.com