FINESSE

cyber protection systems
for vehicles and infrastructure
in road and rail transport

Fraunhofer SIT

DB

YEKTA IT

eTAS

UNIVERSITÄT PASSAU

INCYDE

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

PUBLISHING NOTES

Layout and Typesetting

Carolin-Isabel Kaiser

Contakt

National Research Center for Applied Cybersecurity
ATHENE
c/o Fraunhofer Institute for
Secure Information Technology SIT
Rheinstraße 75
64295 Darmstadt

Contakt: info@sit.fraunhofer.de

Darmstadt, 2026

AUTHORS & INSTITUTIONS

INCYDE industrial cyber defense GmbH (INCYDE):
Christoph Krauß
Sofian Beyer
Dominik Spychalski

ETAS GmbH:
Jens Gramm
Ramona Jung
Nicolas Loza
Michael Peter Schneider

Universität Passau, Fakultät für Informatik und Mathematik:
Stefan Katzenbeisser
Simon Unger

YEKTA IT GmbH:
Ali Recai Yekta
Cenk Yekta
Moritz Reichelt
Clara Eggers
Erhan Yekta
Marco Gren
Max Randhahn

DB Systemtechnik (DBS):
Andreas Isbarn

Fraunhofer Institute for Secure Information Technology SIT:
Christian Plappert
Florian Fenzl

The FINESSE project (Cyber Schutzsysteme für Fahrzeuge und Infrastruktur im Straßen- und Schienenverkehr) was funded by the Federal Ministry of Research, Technology and Space.

Critical transportation infrastructures are at risk of cyberattacks. This is true for both road and rail transport. Road vehicles have repeatedly been the target of cyberattacks. For example, remote attackers managed to get access to the core vehicle bus, physical attackers were able to tamper with messages exchanged between vital vehicular components, or a weakness in an entertainment system allowed them to control a car. Likewise, a few incidents have been reported in the railway sector, showing that a compromise of the network in the train can potentially cause safety-relevant incidents. Besides proper security engineering during the design phase, as mandated nowadays both in road and rail vehicles, constant security monitoring is important to spot an ongoing attack.

Monitoring approaches have been developed for both the road and the rail sector. Nevertheless, these developments mainly happened independently, without exchange of knowledge and solutions between the sectors. For the first time, the FINESSE project aimed to overcome this separation by designing a unified framework for security monitoring of both road and rail vehicles. By piloting the architecture both in a car and in the Advanced Train Lab of Deutsche Bahn, FINESSE demonstrated that a strong collaboration between the sectors can be highly beneficial.

This brochure provides insights into the main achievements of the FINESSE project, which ran from July 2022 to December 2025. We hope that the results of the project stimulate further research in this important area.

Stefan Katzenbeisser, Autor

Christoph Krauß, Autor

PREFACE

1

Introduction

1.1 Project Mission

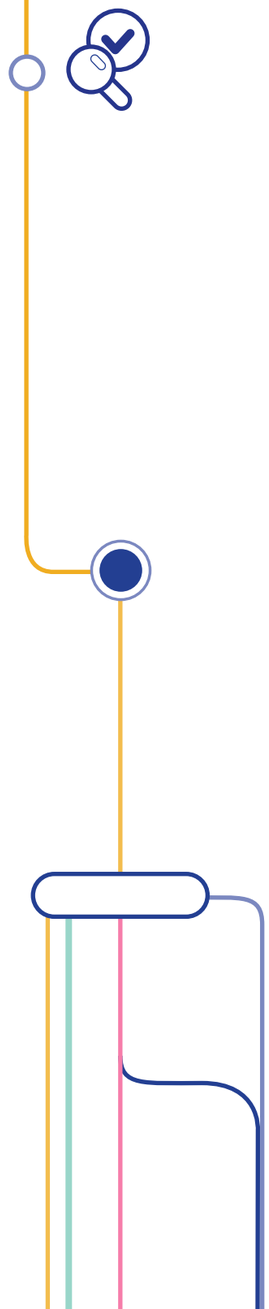
Digitalization in transportation is a major trend and aims for intermodal transport, higher efficiency, and increased capacity. However, this growing connectivity – within vehicles, between vehicles, and with central systems for digital services and traffic control – introduces new cyber threats. Scalable attacks on the integrity and availability of transport systems, and the confidentiality of user data (privacy), become possible.

IT security is crucial in both road and rail transport. For road vehicles, the UN R155 regulation, relevant for the European market, expands vehicle type approval to include cybersecurity. Similar regulations are emerging globally. These standards mandate vehicle manufacturers to detect and respond to cybersecurity incidents across their entire fleet, with security monitoring being a key measure.

Continuous monitoring of potential attacks is also essential for rail vehicles. Rail is considered as critical infrastructure. Digitalization in rail led to standardization efforts, aiming for unified IT security standards.

The FINESSE project focuses on technologies for secure, reliable, and efficient security monitoring of vehicle fleets and appropriate, (semi-)automated responses. It considers all system layers – component security within vehicles, transmission paths, and fleet monitoring in a Vehicle Security Operation Center (SOC) – to detect and mitigate attacks on vehicles. For example, smart sensors in vehicles and novel analysis methods in the SOC enable efficient fleet security monitoring.

A unique aspect of FINESSE is its dual focus on road and rail domains, aiming to create a multimodal security infrastructure applicable to both domains.



1.2 Project Scope

The topic of the FINESSE project is comprehensive security monitoring for automotive and train fleets. As starting point, it identifies commonalities and differences between rail and street vehicles for fleet security monitoring. A generic vehicle model forms the basis for „multi-modal“ threat analysis and security monitoring, covering both domains.

FINESSE provides a multi-modal threat model and, with Vehicle Adversarial Tactics, Techniques & Expert Knowledge (VATT&EK), a vehicle-specific adaptation of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. These frameworks formalize cyberattacks using a Tactics, Techniques, and Procedures (TTP) approach, which is, e.g., applied to derive a comprehensive threat taxonomy for the automotive UDS diagnostic protocol.

The project's security monitoring architecture considers both on-board and off-board technologies. On-board, novel Intrusion Detection System (IDS) sensors, so-called smart sensors, such as for the train-specific Multifunction Vehicle Bus (MVB) bus, are studied. A Security Event Center (SEC) is proposed as a central component in a distributed vehicle security monitoring system. FINESSE leverages Artificial Intelligence (AI) for rule generation in rule-based IDS sensors and improves the standardization of security events for distributed intrusion detection systems.

On the off-board side, FINESSE proposes an architecture for a multi-modal Vehicle Security Operation Center (VSOC), defining key components and data sources. Vehicle-specific characteristics of security monitoring are considered, e.g. by proposing to use asset management to link data sources. Security monitoring strategies are exemplified for the case of the Unified Diagnostic Services (UDS) protocol.

To protect the integrity of its security monitoring mechanisms, FINESSE proposes a strong Hardware Security-based platform concept, centered on a Trusted Platform Module (TPM) within the vehicle architecture. This enables secure firmware and IDS rule distribution, alongside a hybrid, lightweight integrity verification system.

Finally, FINESSE has developed a series of demonstrators and evaluation platforms to illustrate and assess its results, covering both automotive and train networks. Its concepts have been evaluated on the Advanced Train Lab, a real-world train platform.

1.3 Project Framework and Partners

The FINESSE project „Cyber protection systems for vehicles and infrastructure in the automotive and rail domains“ is funded by the Federal Ministry for Research, Technology and Space („Bundesministerium für Forschung, Technologie und Raumfahrt“, BMFTR). The project is part of the funding program „Security on All IT System Layers,“ which is included in the research framework program on IT security titled „Self-Determined and Secure in the Digital World 2015-2020.“

The project term is July 2022 – December 2025.

The project consortium consists of the following partners:

Systemtechnik

DB Systemtechnik. DB Systemtechnik is a service provider for vehicle and infrastructure testing and approvals and operates throughout Europe for rail transport and infrastructure companies.

ETAS. ETAS GmbH is a wholly owned subsidiary of Robert Bosch GmbH. The ETAS portfolio includes automotive cybersecurity solutions, as well as software development tools, software testing solutions, automotive middleware, data acquisition & processing tools, and authoring & diagnostic solutions. ETAS products and services contribute to the realization of software-defined vehicles.

Fraunhofer Institute for Secure Information Technology SIT. The Fraunhofer Institute for Secure Information Technology SIT is one of the world's leading research institutions for cyber security and privacy protection. The institute deals with the central security challenges in economy, administration, and society and conducts practice-oriented top-level research and innovation development. Numerous prizes and awards prove the high quality of the results and developments.

1.3

INCYDE (Consortium Leader)
INCYDE INdustrial CYber DEfense GmbH are IT/OT experts, specialized in the analysis, solution development and implementation of security requirements in the field of operational technologies in the railroad, automotive, maritime, and energy technology sectors. Clients are accompanied through the entire life cycle and benefit from Incyde GmbH's industry and cybersecurity experts who act as sparring partners and consultants. With Incyde GmbH, companies can develop and achieve their cyberse curity goals for lasting success.

University of Passau. The University of Passau enjoys visibility and a high reputation as an academic address in the heart of Europe thanks to its excellent research, outstanding study conditions and dense international network. The Chair of Computer Engineering of Prof. Dr. Stefan Katzenbeisser deals with practical questions of IT security with a focus on hardware-oriented security, critical infrastructures and data protection.

Yekta IT is a 15-year established cybersecurity company from Dortmund, specializing in critical infrastructure (KRITIS) and Operations Technology (OT) for SMEs to large corporations. With extensive experience in building and operating Security Operations Centers in KRITIS environments, YIT combines offensive and defensive expertise in penetration testing, SOC and OT Security.

2 Vehicle Architectures and Technologies

2.1 Automotive Systems – E/E Architectures and Communication Protocols

In the rapidly evolving landscape of automotive technology, improved vehicle electronic architectures and communication protocols play a crucial role in enhancing the functionality, safety, and security of modern vehicles.

Vehicles feature numerous computing nodes, so-called Electronic Control Units (ECUs), interconnected through various communication systems. Electrical / Electronic (E/E) architectures define the structured design and integration of these ECUs and automotive bus systems. Key automotive bus systems include:

- **Controller Area Network (CAN)**: A widely used protocol that allows multiple ECUs to communicate without a host computer.
- **Local Interconnect Network (LIN)**: A simpler, lowercost alternative to CAN, often used for less critical applications.
- **FlexRay**: A high-speed protocol designed for safety-critical applications, providing redundancy and fault tolerance.
- **Automotive Ethernet**: Increasingly used in modern vehicles for high-bandwidth applications, such as infotainment and advanced driver assistance systems (ADAS).

Automotive networks are well-structured into domains and/or zones. We give some examples:

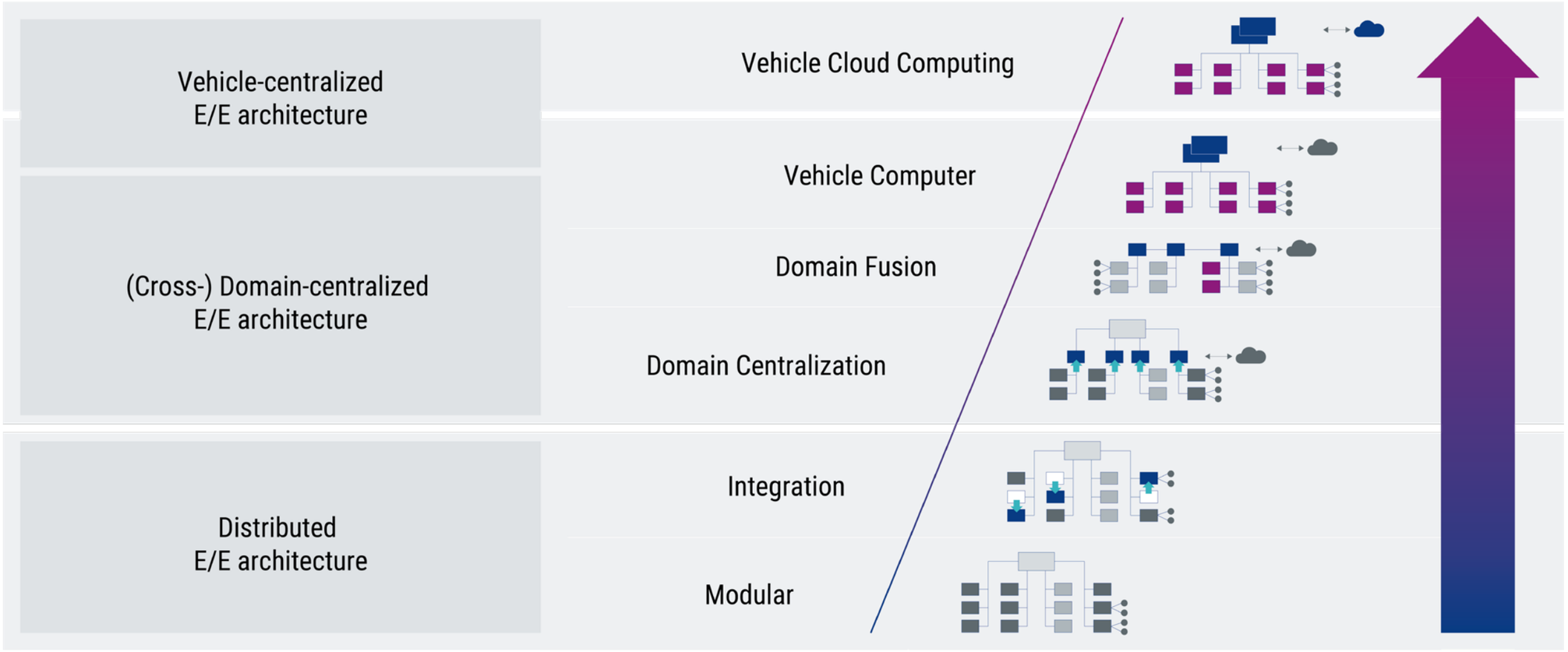
Domain Controllers are centralized units that manage specific domains of vehicle functionality (e.g., powertrain, chassis, infotainment), to reduce complexity and improve efficiency.

Gateways act as intermediaries, facilitating communication between different network domains or bus systems (e.g., CAN, LIN, Ethernet) by translating protocols and managing data flow.

Zone architectures group ECUs by vehicle location (e.g., front, rear), allowing specific functions (e.g., braking) to be defined by software rather than hardware.

2.1

E/E architectures are evolving to incorporate vehicle computers and cloud-based functionalities, blurring the lines between on-board and off-board functions. For fleet security monitoring, as explored in the FINESSE project, understanding vehicle network structures is essential. Given their complexity, security monitoring systems will be distributed, utilizing multiple sensors to monitor various locations inside and outside the vehicle.



Authors: Jens Gramm (ETAS), Ramona Jung (ETAS)

2.2 Automotive Systems – Software-defined Vehicles (SDV)

SUMMARY

In the Software-defined Vehicle (SDV), a software middleware provides an abstraction layer over physical control units. As this also weakens the security-relevant physical separation of functions, new concepts for protection against cyber attacks are needed.

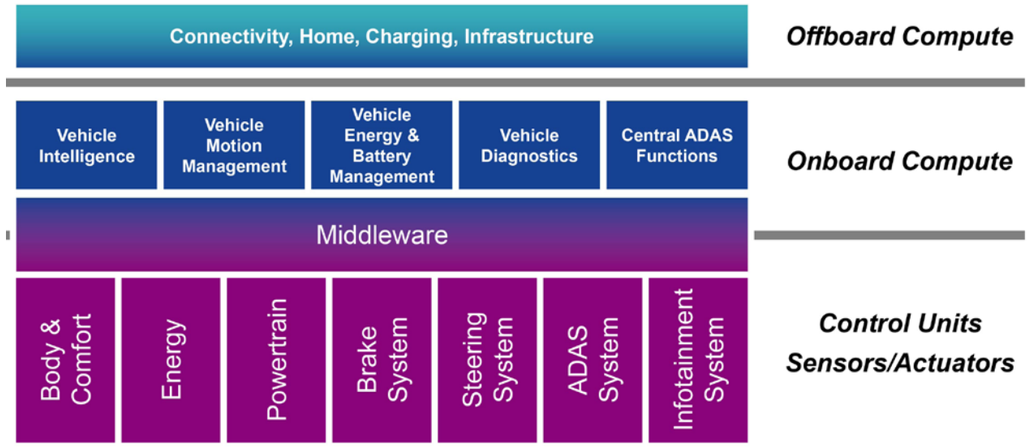
Traditional onboard network architectures were functionally rather monolithic and defined by control units. They were characterized by predominantly static signal-based communication over physically separated bus systems with different functions.

The SDV of the near future requires efficient, broadband, and dynamic data transmission for the implementation of various use cases as, e.g., remote diagnostics or optimized engine and battery management.

E/E architectures of SDVs utilize middleware that acts as a logical, software-based overlay across multiple control units, abstracting the hardware and thereby facilitating extended crossfunctional communication.

SDV E/E architectures allow implementing new functions independent of bus systems and hardware. This brings new stakeholders to the market: In addition to traditional vehicle manufacturers, IT software development companies and mobile app developers can now provide new customer functions for the vehicle.

Regarding cybersecurity, future vehicle architectures present new challenges, but they also offer opportunities. For instance, identified vulnerabilities can be addressed through remote security updates, and established security measures from traditional IT can be adapted and applied to the vehicle. This underlines the relevance of security monitoring for vehicle fleets which is the main topic of the FINESSE project.



Authors: Jens Gramm (ETAS), Ramona Jung (ETAS)

2.3 Rail Technologies

Rail vehicles have evolved over the past decades from simple mechanical-electrical systems to complex, networked, and digitally controlled units. Modern train architectures increasingly rely on the intelligent interconnection of electronic components, significantly enhancing safety, reliability, and efficiency.

Historically, rail vehicles consisted of separate mechanical and electrical components controlled by simple relays and analog circuits. Today's architecture is characterized by digital control systems where ECUs and bus systems communicate seamlessly. Standardized protocols such as the MVB and Wire Train Bus (WTB) collectively form the Train Communication Network (TCN), defined by IEC standard 61375. MVB ensures fast and reliable communication within individual vehicles, while WTB facilitates data transmission between different cars in a train set.

Modern rail vehicles increasingly utilize Ethernet-based communication protocols, such as the Train Real-time Data Protocol (TRDP) and Time-Sensitive Networking (TSN). These technologies guarantee real-time communication, enabling applications like video surveillance, diagnostic systems, and predictive maintenance.

In addition to in-vehicle communication, standardized train control and protection systems play a crucial role. The European Train Control System (ETCS) provides unified and secure communication between trains and infrastructure, replacing national legacy systems and enhancing interoperability and operational safety across rail networks. Automatic Train Operation (ATO) is increasingly integrated alongside ETCS.

ATO enables various degrees of automation, known as Grades of Automation (GoA), ranging from assisted operation (GoA1) to fully autonomous operation without a driver (GoA4). ETCS supplies essential safety data utilized by ATO systems for controlling train movements, aiming to boost capacity, efficiency, and punctuality in rail transport.

Despite numerous advantages, modern rail vehicle architectures also present specific challenges. Integration and standardization of heterogeneous systems, as well as long-term maintainability, are critical for ensuring reliable operation. Diverse technologies and manufacturers necessitate clearly defined interfaces and interoperability standards to guarantee stable systems over the long term.

Additionally, the increased digitization and networking of rail vehicles elevate the importance of cybersecurity. Regulatory frameworks such as the Cyber Resilience Act (CRA) classify rail control systems as critical products requiring mandatory intrusion detection capabilities and continuous monitoring of system activities. Every component update or retrofit triggers new compliance requirements, creating additional complexity for the typical 30-40 year vehicle lifecycle. Networked systems pose potential targets for cyber-attacks, necessitating integrated security architectures that combine functional safety with cybersecurity requirements.

Authors: Ali Recai Yekta (Yekta IT), Andreas Isbarn (DB Systemtechnik)

2.4 Automotive vs Rail — Communication Paths and Control

SUMMARY

In both the automotive and train domains, effective communication paths and control systems are crucial for ensuring safety, efficiency, and reliability. These sectors share commonalities in their reliance on advanced technologies, and common security goals exist for vehicles of both domains.

Both vehicle types implement ECUs for control tasks, e.g., engine control. Certain ECUs are safety-relevant and therefore require special protection within the vehicle network.

Similarities can be identified in used technologies and communication principles. Field bus systems are the traditional way to implement communication networks, and they remain dominant until today. For trains, this includes the Wire Train Bus/Multifunction Vehicle Bus (WTB/MVB), in automotive CAN, LIN or MOST. In modern automotive vehicles, these bus technologies are increasingly replaced by Automotive Ethernet. Ethernet also started to be used in train networks – examples are Real-Time Ethernet (RTE) related standards such as Ethernet Train Backbone (ETB) or Ethernet Consist Network (ECN).

External communication exists in both domains, digital mobile radio networks are used for communication between vehicles and the infrastructure. In the railway sector, this includes GSM-R, in the automotive sector LTE. In trains, passengers can use internet services via Wi-Fi. Communication with infrastructure is in place in both domains.

A common focus of security considerations in both domains is primarily on the aspects of network separation and zoning. Access to safety-relevant components from external-facing units, for example the infotainment segment or interfaces available to passengers, must be controlled - this is a universal requirement for all types of vehicles. Subsystem-specific protection goals include their availability and the integrity, authenticity and confidentiality of their communication. Such security requirements are usually generally valid for comparable (e.g., safety-relevant) subsystems, regardless of the system context (railway or automotive).

2.5 Automotive vs Rail — Drivers, Implementation State and Standardization

Fleet security monitoring still varies between automotive and rail vehicles, with three key differences highlighted below.

Fleet Security Monitoring Drivers.

Fleet security monitoring is essential for vehicle security architectures, mandated by standards and regulations in both sectors. Since July 2022, car manufacturers must comply with UN ECE Regulation 155 to obtain type approval and establish a Cyber Security Management System (CSMS). This involves adhering to ISO/SAE 21434, which emphasizes integrating security from the vehicle development phase. Security monitoring plays a crucial role in meeting these regulatory requirements.

In the rail sector, initiatives like the Open CCS On-Board Reference Architecture (OCORA) are standardizing safety architectures, which will increasingly influence vehicle operators' specifications, enhancing train safety levels.

Implementation Status of In-Vehicle IDS Sensors.

In road vehicles, in-vehicle IDS sensors are already in use today. These sensors, often software-based, can be integrated into control unit software and retrofitted via updates. Passive monitoring components typically do not require specific safety classifications, following ISO 26262 standards.

Conversely, rail vehicles demand higher standards for IDS sensors, ensuring that safety-relevant field buses remain unaffected. Certified non-reactive devices are employed, and integrating IDS software into existing systems is complex, necessitating new approvals, which complicates timely updates.

Standardization of Solutions

In the automotive sector, standardization of IDS has begun, led by AUTOSAR, a consortium focused on ECU software architecture. AUTOSAR specifies the IDS manager for collecting and processing security events. It introduces the Qualified Security Event (QSEV) format for standardized vehicle security events. Standardization facilitates integration of proprietary components, making it a valuable approach for the rail industry as well.

Interested to learn more? See Dominik Spychalski et al., „Multi-modal Intrusion Detection System: Attack Detection for Mobility Systems", Signal + Draht (117) 3, 2025

2.6 Generic Vehicle Model

The increasing complexity of modern vehicles, driven by integrated Information Technology (IT) and Operational Technology (OT) systems, demands robust cybersecurity strategies. A generic vehicle model emerges as a promising solution, abstracting critical components and communication structures across road and rail systems to enable standardized security approaches.

Despite domain-specific differences, road and rail vehicles share fundamental technological similarities. For example, both systems rely on modular subsystems, function-specific control units (like ECUs), and field buses like Controller Area Network (CAN) or MVB for on-board communication. The increasing adoption of IP-based protocols like Scalable service-Oriented Middleware over IP (SOME/IP) and RTE further highlights the common ground. Their system architectures exhibit comparable logical constructs, translating into similar security requirements. Connections to infrastructure systems and passenger interfaces present similar functional requirements. This convergence allows for technology-agnostic solutions applicable to both domains.

A **Generic Vehicle Model** introduces an abstract representation. Systems, components and communication technologies are grouped together based on their functional purpose, application scenarios or basic technical characteristics. It classifies components based on functionality (driving, communication, comfort, diagnosis), user roles (owner, driver, passenger, unrelated actor), and surrounding environment systems. The vehicle model is embedded in land-based (fixed) surrounding systems, such as traffic control.

A joint and generalized view of the railway system and the automotive system not only offers opportunities in terms of interactive learning and synergy effects. It serves as a basis for risk considerations and for the development of holistic and cross-domain safety technologies. The mixture of sector-specific knowledge from road and rail transport enables new perspectives on common and different challenges in order to develop better solutions through diversity.

The FINESSE project exemplifies the practical application of the generic vehicle model. By leveraging this model, cross-domain intrusion detection systems are developed, enabling threat intelligence sharing and improving response times.

Interested to learn more? See Dominik Spychalski, Markus Heinrich, and Christoph Krauß, „Rail meets Automotive: Commonalities in Vehicleside IT/OT Security Considerations“, Signal + Draht (114) 11, 2022.

Author: Sofian Beyer (INCYDE GmbH)

3

Threat Landscape

3.1 VATT&EK: A Framework for Transport System Cybersecurity

SUMMARY

Current cybersecurity frameworks like MITRE ATT&CK were designed for traditional IT environments but struggle with Intelligent Transport Systems (ITS). Vehicles contain dozens of Electronic Control Units communicating over specialized protocols like CAN bus while connecting to external networks. The convergence of IT and operational technology in transport has created new attack surfaces where security failures can have immediate physical consequences.

VATT&EK`S key innovation lies in its multi-modal approach, enabling systematic threat modeling across both automotive and rail domains. This recognizes technological convergence in transport systems – service-oriented architectures, Ethernet-based communications, and standardized protocols appearing across both sectors, often creating similar vulnerabilities.

The TTP Approach

The framework breaks down complex attacks into analyzable components:

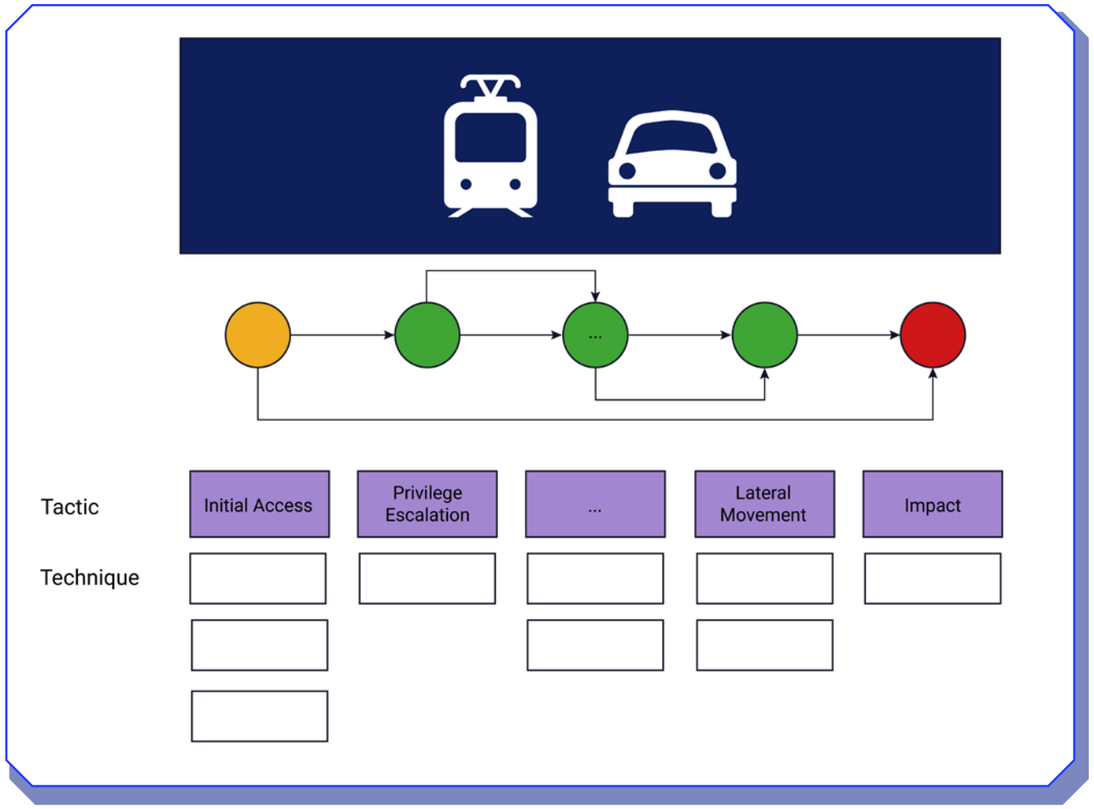
Tactics identify adversary objectives – whether gaining initial access, maintaining persistence, or affecting vehicle functions.

Techniques describe specific methods like exploiting OBD dongles, manipulating CAN messages, or spoofing GNSS signals.

Procedures document implementation details from real attacks, providing concrete examples for defensive measures.

3.1

VATT&EK organizes adversarial activities into 14 tactic classes, from environment manipulation through initial access to final impact, demonstrating effectiveness through analysis of significant real-world attacks including remote vehicle compromises and infrastructure disruptions.



Interested to see more? See Ali Recai Yekta et al., „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 (CSCS), 2023, https://doi.org/10.1145/3631204.3631867. See also the accompanying „Vehicle Threat Matrix" website https://vehicle-threat-matrix.com/.

Authors: Ali Recai Yekta (Yekta IT), Dominik Spychalski (INCYDE), Erhan Yekta (Yekta IT), Cenk Yekta (Yekta IT), Stefan Katzenbeisser (University of Passau)

3.2 UDS Attack Taxonomy: Systematic Classification of Vehicle Diagnostic Threats

SUMMARY

A taxonomy of attack techniques for UDS, the most widely used diagnostic protocol in the automotive domain, provides a structured approach for security assessments, incident response, and the development of security monitoring strategies for UDS.

UDS protocol

The UDS protocol, serving as the primary standard for vehicle diagnostics throughout the entire lifecycle, represents a critical attack surface. However, existing security analyses remain fragmented, focusing predominantly on individual UDS services, particularly Security Access (0x27), thereby lacking a systematic assessment of the comprehensive threat landscape.

To address this gap, a comprehensive attack taxonomy for the entire UDS protocol has been developed. Through systematic threat modeling, each of the 27 UDS services was analyzed using STRIDE methodology to identify potential attack vectors. The resulting threats were integrated into the VATT&EK framework, yielding 50 UDS-specific attack techniques categorized across nine tactics, ranging from Resource Development and Privilege Escalation to Vehicle Function Manipulation.

Validation against 33 published vulnerability reports demonstrates practical relevance: two-thirds of the identified techniques are already documented in real-world attacks, while simultaneously revealing previously unexplored attack vectors, particularly for newer services such as Authentication (0x29). The taxonomy enables comprehensive end-to-end attack chain modeling for the first time.

This work contributes to the field by providing a systematic foundation for UDS threat assessment through structured knowledge representation. The taxonomy supports methodical threat assessments aligned with ISO/SAE 21434 requirements, enables systematic security testing approaches, and facilitates evidence-based development of monitoring strategies for VSOCs. Furthermore, it establishes a common terminology for the automotive security community, thereby enhancing the scientific basis for security decision-making in vehicle development.

In scope of the FINESSE project, the UDS attack taxonomy serves as the basis for the development of security monitoring strategies for a concrete automotive use case, both guiding onboard logging of security events as well as the backend analysis in a VSOC infrastructure.

ID	Technique
Resource Development	
AT-RD-1	Firmware Reverse-Engineering
AT-RD-2	Leak secrets
Persistence	
AT-PS-1	Download Custom Package
Privilege Escalation	
AT-PE-1	Change to Privileged Session
AT-PE-2	Valid Credentials
AT-PE-3	Replay Attack on SA
AT-PE-4	Brute-Force on SA
AT-PE-5	Weak Auth29 configurations
Defence Evasion	
AT-DE-1	Block DTCs Generation
AT-DE-2	Remove Attack Traces in DTCs
AT-DE-3	Replay Download
AT-DE-4	Bypass Checks
AT-DE-5	Bypass Read Protections using DDDID
Credential Access	
AT-CA-1	Extract Secrets from ECU
Discovery	
AT-DS-1	Service Discovery
AT-DS-2	Subfunction Discovery
AT-DS-3	Diagnostic Sessions Discovery
AT-DS-4	UDS Fuzzing
AT-DS-5	Check seed entropy in SA (0x27)
AT-DS-6	Reverse-engineer SA (0x27) algorithm
AT-DS-7	Identify Auth29 (0x29) configuration
AT-DS-8	Enumerate algorithms, Auth29
AT-DS-9	Check challenge entropy, Auth29
AT-DS-10	Identify Configurations for SDT
AT-DS-11	DID Enumeration
AT-DS-12	Routine Enumeration
AT-DS-13	File System Discovery
AT-DS-14	Eavesdropping
Lateral Movement	
AT-LM-1	Man-in-the-Middle
Collection	
AT-CL-1	Event-Based Data Extraction
AT-CL-2	Periodic Data Extraction
AT-CL-3	DID Data Extraction
AT-CL-4	Memory Extraction
AT-CL-5	File Extraction
AT-CL-6	Read DTCs
Affect Vehicle Function	
AT-AF-1	Request Flooding
AT-AF-2	Request Blocking
AT-AF-3	Interrupt Operations, DSC
AT-AF-4	Impede Usage of SA
AT-AF-5.1	Resource Overload via ROE
AT-AF-5.2	Resource Overload via RDBPI
AT-AF-6	Interrupt Periodic Data Readout
AT-AF-7	Change IO Configuration
AT-AF-8	Routine Misuse
AT-AF-9	Early Transfer Termination
AT-AF-10	Interrupt Routine
AT-AF-11	Keep Session Open
AT-AF-12	I/O Control
AT-AF-13	Disrupt ECU Communication
AT-AF-14	Reset ECU
AT-AF-15	DID Manipulation
AT-AF-16	File Manipulation
AT-AF-17	Memory Manipulation

Interested to see more? See Ali Recai Yekta et al., „UDS Attack Taxonomy: Systematic Classification of Vehicle Diagnostic Threats“, Proceedings of the IEEE Conference on Communications and Network Security (CNS), 2025, https://doi.org/10.1109/CNS66487.2025.11195020.

Authors: Ali Recai Yekta (Yekta IT), Nicolas Loza (ETAS), Jens Gramm (ETAS), Michael Peter Schneider (ETAS), Stefan Katzenbeisser (University of Passau)

4

Multi-modal Fleet Security Monitoring On-Board

4.1 Intrusion Detection Systems (IDS)

IDS are essential components in modern cybersecurity, designed to monitor network or system activities for malicious actions or policy violations. Their primary goal is to detect potential threats in real time or near real time, alert administrators, and help prevent damage to digital infrastructure. With increasing connectivity in modern vehicles, IDS are becoming a crucial part of automotive networks.

There are several types of IDS:

Network-based IDS (NIDS) monitor entire network segments, analyzing traffic to identify suspicious patterns.

Host-based IDS (HIDS) operate on individual devices, examining internal system activities such as file access and process behavior.

Hybrid IDS combine both approaches, aiming to deliver more comprehensive protection in one sensor.

Anomaly-based IDS detect deviations from established behavioral baselines, while signature-based IDS identify threats based on known attack patterns.

In safety-critical environments, such as vehicle networks, IDS must meet several important requirements. Explainability is crucial, as decisions made by the system must be transparent and understandable to system operators and auditors. This is particularly important for gaining trust and enabling corrective actions. Safety coexistence refers to the IDS operating without interfering with the core safety functions of the system. It must function passively or in a carefully controlled active manner to ensure it does not introduce new risks. Lastly, certifiability involves the ability to formally verify and certify the IDS as part of a larger system, ensuring compliance with regulatory and industry standards. These requirements are essential to integrate IDS effectively into both conventional IT systems and critical infrastructure environments.

In FINESSE, we explore various means of integrating different types of IDS in an overall system architecture and explore ways to utilize the data effectively. We have also explored different types of sensors and other data sources on how we can use them to improve classification performance, safety, and security.

4.2 Y-MVB-IDS: Vendor-Agnostic Intrusion Detection for Railway Systems

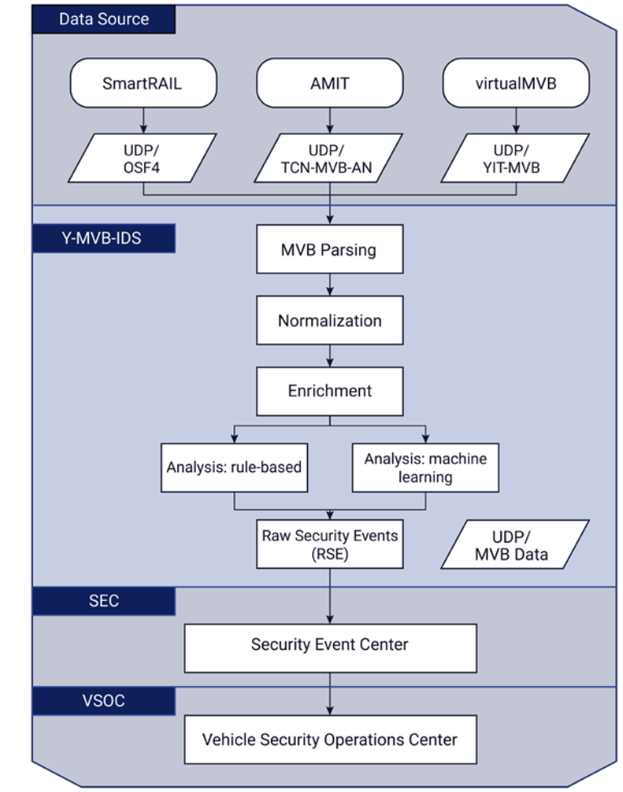
The increasing digitalization of rail vehicles expands the cyberattack surface of critical communication systems. The MVB according to IEC 61375 requires continuous security monitoring, while heterogeneous vendor implementations complicate unified monitoring strategies.

Yekta IT conducted real train recordings using AMIT and smartRAIL systems to capture authentic MVB communication patterns. These recordings were analyzed to understand protocol behaviors and communication characteristics. Based on this analysis, a virtualMVB test environment was developed that simulates realistic MVB fieldbus communication via UDP/YITMVB, enabling controlled testing scenarios.

System Architecture: The Y-MVB-IDS implements an adapter-based architecture for integrating diverse MVB data sources: AMIT (UDP/TCNMVB-AN), smartRAIL (UDP/OSF4), and the developed virtual MVB (UDP/YIT-MVB). All protocol variants are transformed through lightweight adapters into a canonical MVB data model.

PROCESSING PIPELINE:

- Protocol Parsing: Decoding of the three MVB implementations
- Normalization: Transformation into IEC 61375-compliant data model
- Enrichment: Contextual metadata enhancement



Detection Methods: Hybrid approach combining rule-based detection and machine learning-based anomaly detection. Validation: The system was validated using real train recordings from AMIT and smartRAIL as well as virtualMVB simulation data. The solution combines empirical field data analysis with vendor-neutral data modeling and enables unified security policies in heterogeneous MVB environments while maintaining IEC 61375 compliance.

Authors: Ali Recai Yekta (Yekta IT), Cenk Yekta (Yekta IT), Moritz Reichelt (Yekta IT)

4.3 MVB-IDS

Cyber threats targeting rail and road vehicles require robust, adaptable security strategies. Most of the communication technologies currently used in these sectors lack security in terms of cybersecurity. INCYDE GmbH considers an IDS component to be an essential part of a solution for this problem in real-life applications, as it is not feasible to switch to newer, more secure technologies anytime soon.

As part of the FINESSE Project, INCYDE GmbH developed an IDS to present a solution for this problem. This was showcased with the INCYDE-Rail-Demonstrator at InnoTrans 2024 and National Conference on IT Security Research 2025. The developed IDS demonstrated its capability of monitoring not just abstracted, but actual MVB communication and successfully detected real-world MVB attacks in a live setting. Thus, a successful attack on MVB was publicly demonstrated for the first time using the INCYDE-MVB-Attacker, more on that in section “INCYDE Rail Demonstrator”. Both, DoS and spoofing attacks were carried out and detected by the developed IDS.

These were then reported to the installed SEC.

INCYDE-MVB-IDS

is not limited to the MVB protocol or Master-Slave schemed buses. Its multimodal, holistic, and generic approach is suitable for other field buses as well. Understanding the content of the messages is not mandatory, as the IDS considers numerous other data points for its threat detection. The used Machine Learning (ML) techniques utilize multimodal input sources, such as messages and their characteristics, as well as other electrical properties of the network. These features are used to evaluate a comprehensive assessment of the ground truth and form the basis for detecting anomalies.

Upcoming iterations of the INCYDE GmbH’s IDS will show that the approach is not limited to MVB protocol or Master-Slave schemed buses, but to all kinds of field buses.

Author: Sofian Beyer (INCYDE GmbH)

4.4 Y-UDS-IDS

UDS (ISO 14229) implements standardized diagnostic services for automotive ECU communication. Conventional CAN-IDS systems analyze exclusively CAN frame structures without understanding protocol semantics. UDS-IDS implementations interpret the diagnostic protocols and extract service parameters, session states, and security access levels for contextual attack detection.

ARCHITECTURE

Phase 1 Data Acquisition - Passive UDS traffic capture via ISO-TP and DoIP transport with precise timestamping and multi-ECU coverage for comprehensive vehicle diagnostic monitoring.

Phase 2 Protocol Processing - Multi-frame reassembly for segmented ISO-TP messages, UDS message parsing with service ID extraction, parameter normalization, and session context tracking for structured event generation.

Phase 3 Security Analysis - Pattern-based detection engine with configurable ECU-specific thresholds, session state validation, and sliding window analysis for attack pattern recognition.

Phase 4 Event Generation - Structured security event output with diagnostic context, priority classification, and deduplication for SIEM integration and downstream systems.

DETECTIONS

Phase 1 Data Acquisition - Passive UDS traffic capture via ISO-TP and DoIP Enumeration Detection: DiagnosticSessionControl (0x10), ReadDataByIdentifier (0x22), and RoutineControl (0x31) monitoring for systematic parameter scanning patterns with high negative response rates.

Phase 2 Security Access Monitoring: SecurityAccess (0x27) seed/key cycles for brute-force patterns and XOR-key probing through characteristic generation patterns.

Phase 3 Memory & Data Access Control: ReadMemoryByAddress (0x23) for systematic address scanning patterns and access to protected memory ranges, ReadDataByIdentifier (0x22) DID discovery through sequential identifier enumeration, WriteDataByIdentifier (0x2E) session validation against security access levels, protected DID access control for safety-critical identifiers outside authorized sessions.

Phase 4 DoS: ECUReset (0x11) for abnormal reset frequencies and reset-after-attack patterns.

Limitations: Individual service requests and complex multistep attacks often remain undetected. Firmware upgrade/downgrade attacks, cross-ECU attacks, and long-term behavioral anomalies require advanced correlation in the Vehicle VSOC through multi-source fusion and vehicle context integration.

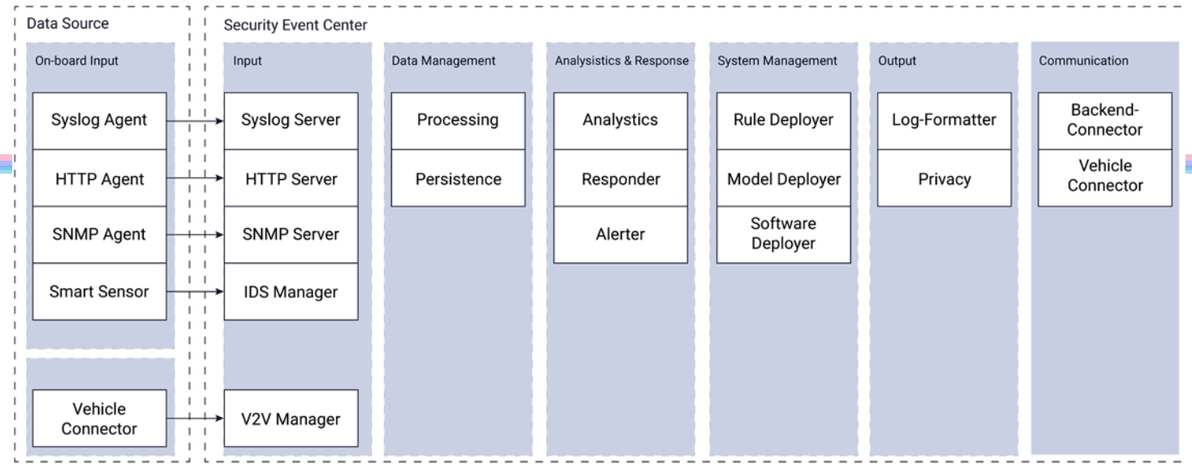
Authors: Ali Recai Yekta (Yekta IT), Cenk Yekta (Yekta IT), Clara Eggers (Yekta IT)

4.5 On-board Security Event Center

The increasing connectivity of vehicles in automotive and rail domains results in a fragmented security landscape where isolated IDS can only detect domain-specific threats. Traditional approaches monitor specific technologies such as CAN-Bus, Ethernet, or host systems separately, rendering complex, crosstechnology attack chains invisible.

The SEC addresses these limitations through a centralized architecture for vehicle security monitoring. Unlike passive solutions, the SEC provides a centralized view of vehicle security by aggregating, analyzing, and correlating security events from heterogeneous sources.

The SEC architecture comprises four functional modules: The Input module integrates various data sources through Syslog, HTTP, and SNMP servers as well as specialized sensor interfaces. The Data Management module normalizes heterogeneous input data and ensures persistent storage for forensic analyses. The Analytics & Response module implements correlation algorithms to detect cross-technology attack patterns and coordinates alert mechanisms. The System Management module enables bidirectional control of connected Smart Sensors through central distribution of detection rules and behavioral models. The primary contribution of the SEC lies in establishing a comprehensive security view of the vehicle system. This capability enables reconstruction of complete attack chains, supports security analysis procedures, and provides extended forensic analysis capabilities. As an interface to the Vehicle Security Operations Center, the SEC establishes the foundation for fleet-wide security monitoring and represents a transition from isolated to centralized security architectures.



Authors: Ali Recai Yekta (Yekta IT), Cenk Yekta (Yekta IT), Clara Eggers (Yekta IT)

4.6 RulEth: Genetic Programming-Driven Derivation of Security Rules for Automotive Ethernet

The increasing connectivity required for modern driver assistance systems and autonomous vehicles presents a significant security challenge. Traditional rule-based intrusion detection systems often fail to identify sophisticated attacks due to the complexity of underlying behaviors. Meanwhile, machine learning systems, particularly those using artificial neural networks, struggle with interpretability, often making their decisions very hard to trace back to their actual cause.

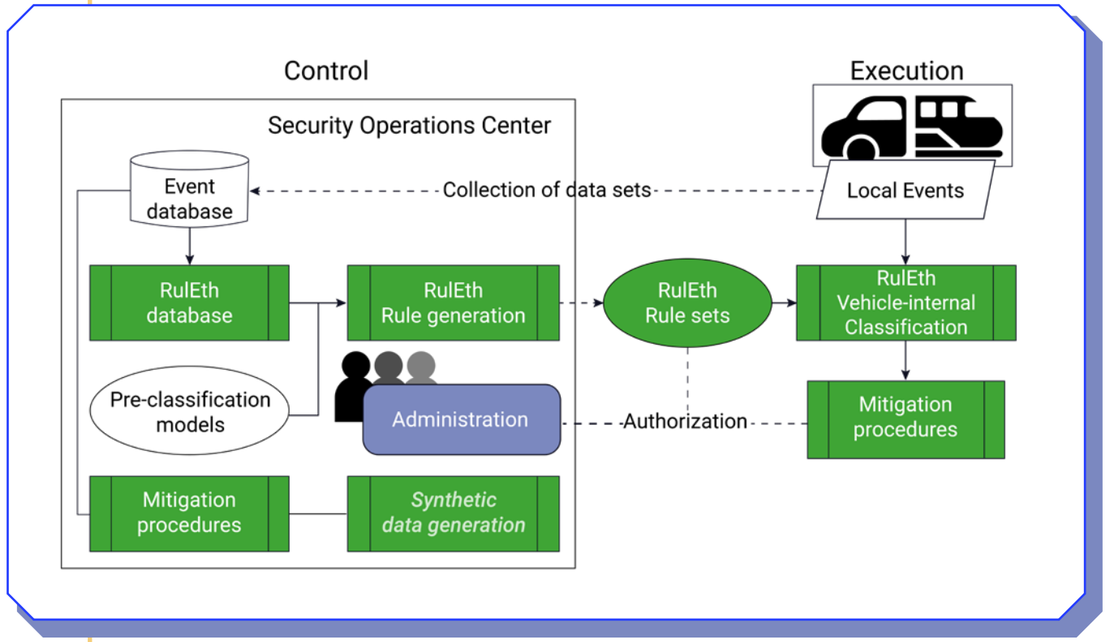
In **FINESSE**, we therefore explored various different approaches for explainable rule generation with common automotive protocols. Our work introduces RulEth, a novel approach that utilizes genetic programming **to generate human-understandable, verifiable security rules for Automotive Ethernet systems.** It is built on a previous system we developed using decision trees.

Using RulEth, operators can generate rules that can identify anomalies in packet flows, that may then be used to enrich alerts with information about the root cause of detected threats. This allows for timely and informed responses to potential intrusions and easier detection and filtering of incoming reports. This directly interacts with a different system developed in the context of FINESSE (see 'SecPol: Enabling Security Policy Control in Vehicle Networks using Intrusion Detection and Hardware Trust'). Here we supply a special access control system with detailed reports from various sources within the vehicle, such as a RulEth-equipped sensor. The system's effectiveness lies in its ability for operators to evaluate each generated rule without sophisticated knowledge, enabling the filtration of ineffective rules, thereby bolstering overall system robustness. The proposed rules language, RulEth, is specifically designed to address cyber threats inherent in automotive environments, facilitating the detection of complex attack patterns, but rules may also be compiled in other formats for rule-based detection systems that are already in use. The implementation of RulEth was tested against different attack scenarios, showing a high level of accuracy in identifying both single and multi-packet attacks. The results indicate a significant improvement over other methods, especially in terms of interpretability and human oversight, which is an important requirement according to EU ethical guidelines for trustworthy AI.

Author: Florian Fenzl (Fraunhofer SIT)

4.6

The RulEth approach not only enhances the security posture of automotive systems but also ensures that the generated rules comply with ethical standards, emphasizing transparency and accountability in AI-driven security solutions. In addition to that, with minor effort, the generated rules can be compiled to different formats for existing rule-based detection systems, such as Snort. The generated reports can also be configured to adhere to different common formats, such as the one used by AUTOSAR (see chapter 'Standardization of Vehicle Security Events in AUTOSAR').



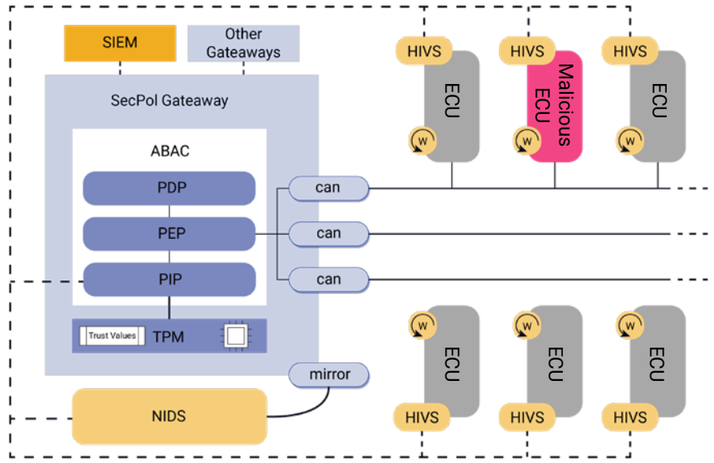
Interested to learn more? See Felix Clemens Gail, Roland Rieke, and Florian Fenzl, „RulEth: Genetic Programming-Driven Derivation of Security Rules for Automotive Ethernet", Proceedings of the European Conference on Machine Learning and Knowledge Discovery in Databases (ECML PKDD), 2023, https://doi.org/10.1007/978-3-031-43430-3_12.

Author: Florian Fenzl (Fraunhofer SIT)

4.7 SecPol: Enabling Security Policy Control in Vehicle Networks using Intrusion Detection and Hardware Trust

As vehicles become increasingly interconnected through the Internet of Vehicles (IoV), the complexity of their networks escalates, raising the potential for cyberattacks. This necessitates advanced security measures to protect these systems. Our work introduces SecPol, a security policy control architecture designed to enhance the adaptability and security of vehicle networks by integrating IDS and Hardware Trust Anchors (HTAs).

The SecPol architecture connects existing security systems to ensure that access control decisions from Attribute-based access control (ABAC) systems on each relevant gateway are informed by real-time data from IDS and HTA components. This allows for dynamic response to security incidents, facilitating the implementation of countermeasures against various intrusion scenarios. For instance, when malicious activity is detected, SecPol can adapt its policies accordingly, ensuring robust protection against attacks.



We evaluated SecPol using two primary communication protocols in automotive settings: CAN and Automotive Ethernet (AE). By developing reference implementations that integrate SecPol with these protocols, we demonstrated its effectiveness in detecting and mitigating attacks, such as denial-of-service and integrity violations. The architecture can be extended beyond automotive applications, making it applicable to other resource-constrained IoT networks. Our findings indicate that SecPol significantly enhances the security posture of vehicular networks by enabling flexible, policy-driven usage control while maintaining compliance with legal requirements, such as UN Regulation No. 155.

Interested to learn more? See Florian Fenzl et al., „SecPol: Enabling Security Policy Control in Vehicle Networks using Intrusion Detection and Hardware Trust“, Proceedings of the 1st Cyber Security in CarS Workshop (CSCS), 2024, https://doi.org/10.1145/3689936.3694697.

Authors: Florian Fenzl (Fraunhofer SIT), Christian Plappert (Fraunhofer SIT)

4.8 Standardization of Vehicle Security Events in AUTOSAR

SUMMARY

The AUTOSAR standarization of security events in the automotive domain provides a common data language for distributed vehicle intrusion detection systems, in particular for the exchange of security events between on-board and off-board sides.

IDS for vehicles are complex, involving components from various manufacturers. Proprietary specifications can lead to increased costs for vehicle integrators. To address this, the AUTOSAR consortium, which focuses on standardizing ECU software architecture, has initiated steps toward standardizing vehicle IDS. AUTOSAR defines the IDS Manager, responsible for collecting and pre-processing security events, and introduces the QSEV format for vehicle security events.

As part of the **FINESSE** project, efforts were made to improve the standardization of security events in AUTOSAR, with the goal to enhance the effectiveness of fleet security monitoring systems. A dedicated working group was formed to improve the standardization process, achieving several key advancements:

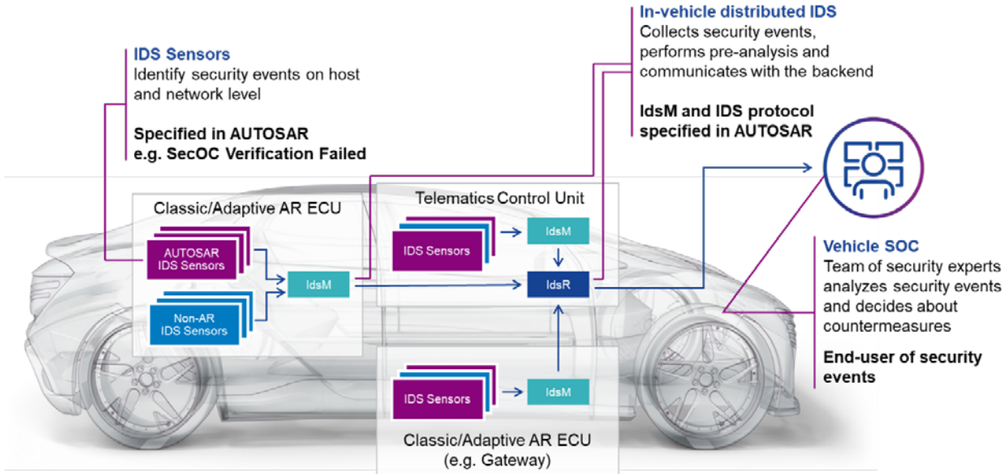
Flexibility: Introduction of versioning for context data formats, allowing for future advancements. Event specifications are provided in an XML format which allows automated processing of new specifications.

Structure: A central AUTOSAR document was created to compile all standardized security events, along with new guidelines for event specification.

New Events: Standardization of new security events across areas such as UDS, Transport Layer Security (TLS), Media Access Control Security (MACsec), software updates, secure boot, certificate management, and Diagnostics over Internet Protocol (DoIP).

Improved Event Quality: Establishment of quality criteria for security events, including specifications for trigger conditions and relevant context data.

These developments lead to a comprehensive set of standardized vehicle security events, enhancing intrusion detection capabilities in fleet security monitoring. The results are included in AUTOSAR releases 23-11, 24-11, and 25-11. The automotive sector's experience highlights the benefits of standardization, which is also recommended for intrusion detection systems in the rail domain.



Interested to learn more? See AUTOSAR, „Technical Report on Security Events Specification", AUTOSAR FO Release R25-11, 2025, https://www.autosar.org/fileadmin/standards/R25-11/FO/AUTOSAR_FO_TR_SecurityEventsSpecification.pdf

Authors: Jens Gramm (ETAS), Nicolas Loza (ETAS), Michael Peter Schneider (ETAS)

5

Multi-modal Fleet Security Monitoring Off-Board

5.1 VSOC Architecture

A VSOC is a centralized system for monitoring, detecting and responding to security threats in vehicle fleets. A VSOC platform pools data from multiple sources and vehicles, continuously analyzes it and detects patterns or anomalies that indicate cyberattacks. By integrating data across multiple vehicles or operators, a VSOC provides a comprehensive perspective to identify and defend against threats at fleet level. This makes a decisive contribution to minimizing risks and maintaining the safe operation of modern vehicle fleets.

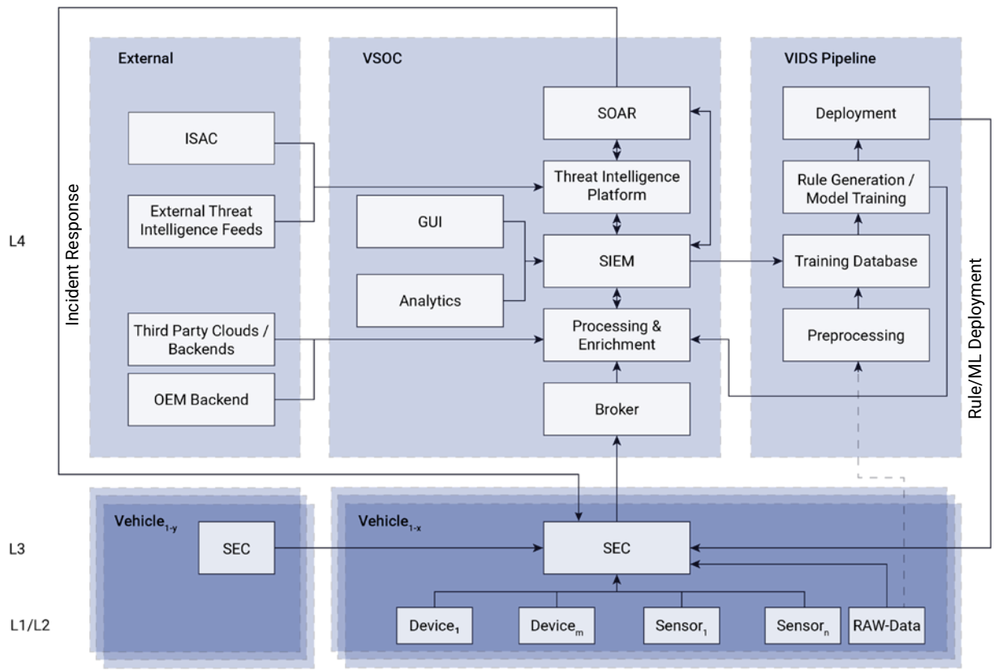
VSOC

- A Security Information & Event Management (SIEM) collects log data from various vehicles and forms the central component of a VSOC. The VSOC then integrates these data sets with additional information from automotive manufacturers and third-party sources.
- Security Orchestration, Automation and Response (SOAR) supports the work of analysts with case management, integration of various data sources and automated analyses.
- A Threat Intelligence Platform supplements the VSOC with up-to-date information on attack methods and vulnerabilities, e.g. from Information Sharing and Analysis Center (ISAC).

The specific nature of event data and the organization and architecture of data endpoints — vehicles — are unique characteristics of a VSOC for vehicle fleets, in comparison to a classical Enterprise IT SOC.

Asset Management enriches a VSOC platform with data about fleets, vehicles and their components, e.g., vehicle model information, E/E architectures, ECUs, rolled-out software and hardware versions. Asset Management is the basis to connect security-relevant information from various sources.

Direct responses to vehicles are not possible, and in safety critical areas such as the rail sector, final decisions remain with humans to avoid disrupting operations. Optionally, Over-the- Air (OTA) updates can be managed centrally to efficiently provide sensors with new rules and machine learning models.



Authors: Ali Recai Yekta (Yekta IT), Jens Gramm (ETAS), Nicolas Loza (ETAS)

5.2 Multi-Modal Data Model

The architecture implements a five-level hierarchical structure based on the Data-Information-Knowledge-Wisdom (DIKW) framework. It systematically transforms raw sensor data into actionable security insights and addresses multi-vendor complexity while enabling immediate local response and comprehensive fleet-wide threat correlation.

Hierarchical Data Processing (Level 0-4)

Level 0

Bits: Raw data collection in ECUs and network components without active security analysis.

Level 1

ECU: HIDS monitor individual control units for unauthorized access and anomalous memory/syscall patterns. HTAs ensure cryptographic authenticity of events.

Level 2

Domain: NIDS monitor specific vehicle domains (powertrain, infotainment) with protocol-specific communication (CAN/CAN-FD, UDS, automotive Ethernet; MVB, TRDP for railway).

Level 3

Vehicle/SEC: Security Event Center aggregates and correlates ECU and domain-specific events for immediate local security responses.

Level 4

Fleet/VSOC: Cross-vehicle analysis integrates data from multiple vehicles, OEM backends, and external threat intelligence. VATT&EK framework integration enables standardized threat classification and comprehensive incident response strategies.

Standardized Event Formats

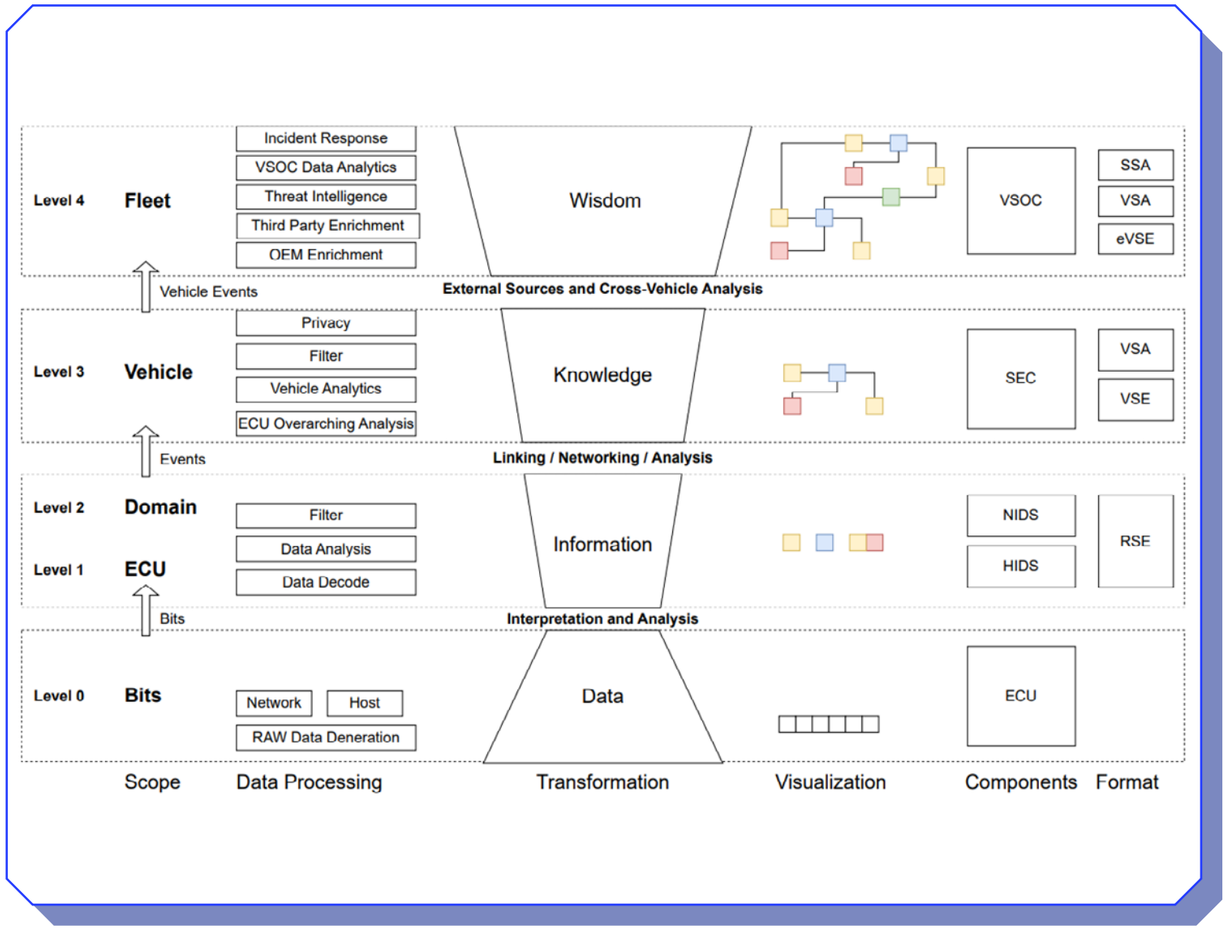
The architecture extends AUTOSAR SEv/QSEv standards with additional security-relevant fields: rule_id, rule_version, severity, and context_data_version. These Raw Security Events (RSEs) combine protocol-agnostic meta-fields with domain-specific context data. The SEC generates Vehicle Security Event (VSE) through enrichment with vehicle state and correlation context. The VSOC produces Enhanced Vehicle Security Event (eVSE) with fleet-wide metadata and VATT&EK classification. GDPR-compliant pseudonymization and multi-level anonymization protect personal data. For railway domains, analogous formats are defined that ensure structural compatibility with automotive standards. Advanced Security Alert Formats (VSA/SSA): Vehicle Security Alerts (VSAs) and SOC Security Alerts (SSAs) extend the event formats with structured notifications including VATT&EK classification, severity assessment, and recommended response actions. The specific nature of event data and the organization and architecture of data endpoints — vehicles — are unique characteristics of a VSOC for vehicle fleets, in comparison to a classical Enterprise IT SOC.

5.2

Multi-Modal Adaptation Mechanisms

Unified Event Processing Pipeline: All transport domains use the same three-stage transformation from RSEs via VSEs to eVSEs.

Protocol-Independent Smart Sensors: A generic sensor framework is adapted to different protocols through interchangeable modules (CAN, Ethernet, MVB, TRDP). Adaptable SEC/VSOC Components: Unified correlation and analysis components configurable for automotive OEMs and railway operators without architectural modifications. The standardized multi-modal architecture enables cross vendor cybersecurity in connected transport systems through proven interoperability and systematic threat detection.

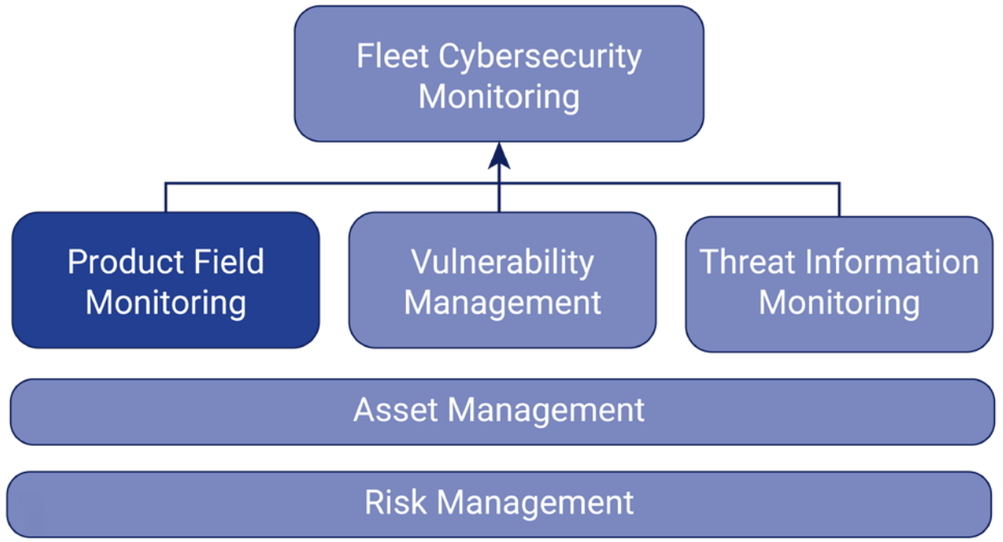


5.3 Offboard Contextualization of Vehicle Security Events

Vehicle security event monitoring is a crucial aspect of comprehensive fleet cybersecurity, encompassing the entire lifecycle of vehicles. Enhanced insights emerge from integrating various data sources and monitoring techniques. For instance, a vulnerability in ECU software may be documented in public databases, discussed in news articles, and reflected in logs from vehicle intrusion detection systems.
Within the FINESSE project, we explored and prototyped the contextualization of vehicle security events with diverse data sources:

- Vulnerability Management: By utilizing a Bill of Materials (BoM) for vehicle software alongside public vulnerability databases, security vulnerabilities relevant to specific products are identified.
- Threat Information Monitoring: Potential threat vectors for specific products are identified using both public and private information sources, including open-source intelligence and closed communities.
- Risk Management: Conducting vehicle risk analyses helps pinpoint critical monitoring areas and assess the significance of security events.
- Asset Management: Effective linkage of these data sources relies on asset management, which provides details on vehicle product lines, electronic architectures, and software bills of materials for specific ECUs.

Contextualization of vehicle security events with these information sources supports their analysis and assessment. For each data source, examples, use cases and detection strategies are available. This leads to generalizable methods for identifying vehicle security attacks. A holistic approach to fleet cybersecurity monitoring necessitates the integration of various information sources to ensure a reliable assessment of vehicle security.



Authors: Jens Gramm (ETAS), Nicolas Loza (ETAS), Michael Peter Schneider (ETAS)

5.4 Security Monitoring Strategies on the Example of the UDS Protocol

SUMMARY

Detection strategies for UDS protocol guide the implementation of UDS security monitoring, from deriving vehicle-side logging requirements to the backend-side log processing in a VSOC.

As contribution of the FINESSE project, strategies for the security monitoring of the UDS protocol are provided. The approach involves specifying security event logging requirements, contextual data collection, and the development of detection strategies aimed at identifying UDS attack scenarios. Detection strategies fall into **three categories**:

- Monitoring for the occurrence of suspicious patterns in logs collected in the vehicle.
- Assessment of the (successful or failed) execution of UDS services in context of additional information, e.g. vehicle state or maintenance services, typically available in a fleet backend.
- Assessment of threat intelligence information about the vehicle and its components to identify attack patterns, e.g. from publicly available information as CVEs and security news feeds.

The relevance of the presented monitoring strategies is shown by applying them to a comprehensive taxonomy of UDS attack techniques. Results show that presented detection strategies cover almost all the attack techniques in this taxonomy. Among others, results show which attack techniques require correlation of data sources in a fleet backend.

It is also shown to which extent the security events standardized by a current industry standard, AUTOSAR, are already suited to support the detection of UDS attack techniques, and we identify corresponding gaps in the standard.

In scope of the FINESSE project, the UDS security monitoring strategies provide a concrete example for the implementation of security monitoring for a widely used automotive protocol.

Interested to learn more? See Ali Recai Yekta et al., „From ECU to VSOC: UDS Security Monitoring Strategies“, Proceedings of the 19th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2025, https://doi.org/10.48550/arXiv.2510.25375.

Authors: Ali Recai Yekta (Yekta IT), Jens Gramm (ETAS), Nicolas Loza (ETAS), Michael Peter Schneider (ETAS), Stefan Katzenbeisser (University of Passau)

6 Security Architecture and Integration

6.1 The Role of Hardware-Based Security in Modern Systems

In an increasingly digital world, where data breaches and cyberattacks grow both in frequency and sophistication, the need for robust security mechanisms is more critical than ever. While software-based solutions provide flexibility and adaptability, they are often not enough to ensure the integrity and confidentiality of sensitive operations. This is where hardware-based security steps in, offering a foundational layer of protection rooted in physical components that are much harder to tamper with or bypass.

Hardware-based security solutions operate independently of the main processor and operating system, making them more resilient against software-level attacks. They provide strong isolation, secure storage, and tamper resistance, which are vital for protecting cryptographic keys, sensitive data, and the integrity of critical computations. This physical isolation significantly decreases the attacker's possibility of penetrating the system. Even if a system is compromised at the software level, hardware-based protections can limit the scope of the breach and maintain the confidentiality of high-value assets.

One of the most prominent hardware-based security technologies is the Trusted Execution Environment (TEE). TEEs, such as Intel SGX, ARM TrustZone, or AMD SEV, provide a secure enclave within the processor where code and data can be processed in isolation from the rest of the system. This isolation ensures that even if the operating system or a hypervisor is compromised, the data and operations within the TEE remain protected. TEEs offer key security properties, including code integrity (only verified code can run in the enclave), data confidentiality (encrypted memory and secure key storage prevent data leakage), and isolation (access to enclave memory is tightly controlled).

However, TEEs are not without drawbacks.

They introduce additional complexity in software design and can suffer from side-channel attacks if not carefully implemented. Also, their size and performance overhead limit the amount of computation that can realistically be performed inside them.

Another cornerstone of hardware-based security is the TPM. A TPM is a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. It can be used for platform integrity checks (such as secure boot), secure credential storage, and attestation.

Unlike TEEs, which are designed for secure execution, TPMs primarily focus on secure storage and attestation. They are essential for establishing trust in devices, particularly in remote or distributed environments.

Hardware-based security provides a robust defense against a growing landscape of threats. Technologies like TEEs and TPMs significantly enhance the security posture of modern systems by adding hardware-enforced guarantees.

In FINESSE, we developed a framework, which is used to evaluate different Hardware-based security technologies regarding their suitability to be deployed on different components in the vehicle E/E architecture. The developed security concepts are detailed in this chapter.

Interested to learn more? See Christian Plappert et al., „Evaluating the Applicability of Hardware Trust Anchors for Automotive Applications", Computers & Security (135), 2023, https://doi.org/10.1016/j.cose.2023.103514.

Authors: Simon Unger (University of Passau), Christian Plappert (Fraunhofer SIT)

6.2 Secure and Lightweight Over-the-Air Software Updates for Adaptive Automotive IDS

Connected vehicles face increasing cyberattack threats during their lifecycle. To keep IDS rules continuously up-to-date with the changing of cyberattack landscape, secure OTA software updates are essential.

In **FINESSE**, we developed a novel OTA update mechanism tailored to the Trusted Platform Module 2.0 (TPM) capabilities, serving as a hardware trust anchor in the vehicle's telematics unit. The approach addresses recent automotive security standards and regulations, e.g., ISO 21434 and UNECE regulations 155 and 156, providing unique security guarantees compared to existing methods.

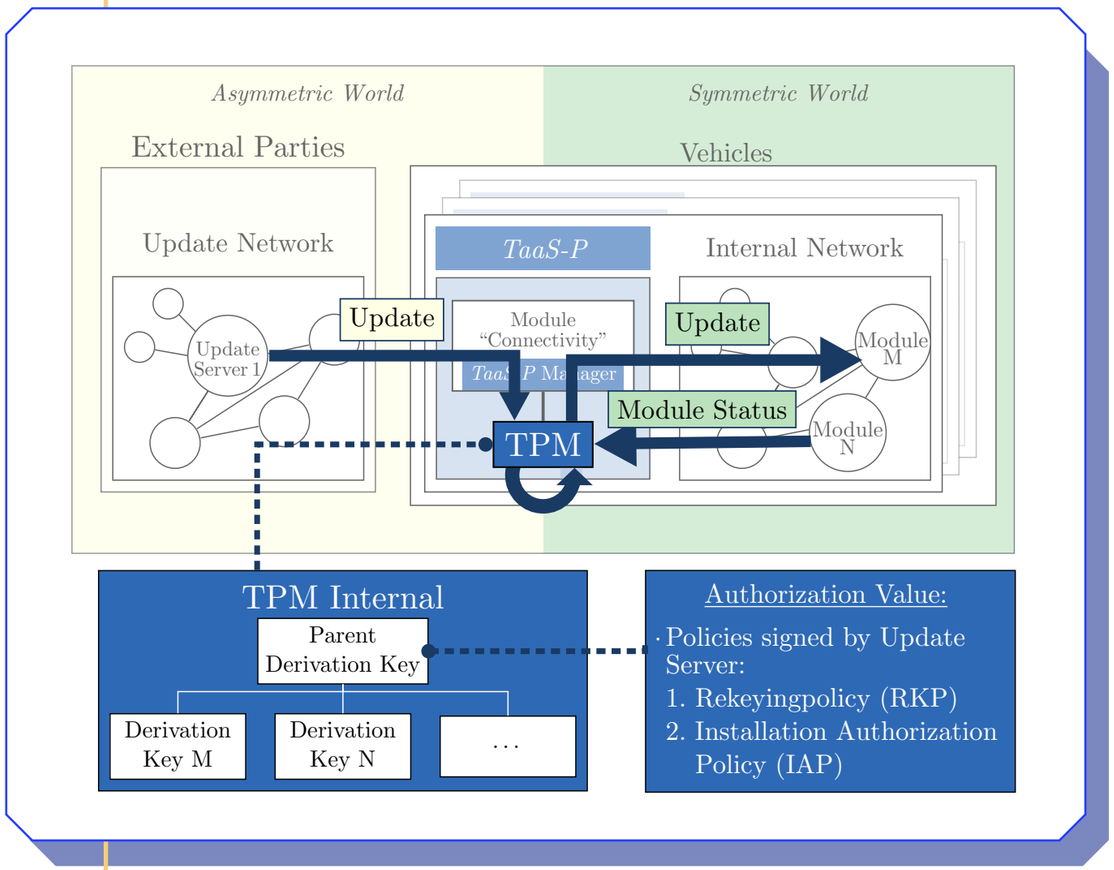
In our concept, the TPM acts as a trusted update distribution point, translating asymmetric backend cryptography to symmetric in-vehicle cryptography. It also serves as an update authorization point, coordinating installation based on vehicle state. This is enforced within the TPM's shielded location, representing a minimal trusted computing base. Unlike other solutions, our approach does not depend on boot time integrity mechanisms, thus mitigating advanced runtime and physical cyberattacks.

Our evaluation demonstrates the solution's feasibility via prototypical implementation on an automotive evaluation platform (cf. chapter "Security Evaluation Platform for Autonomous Driving (SEPAD)"). The TPM significantly reduces security overhead in the vehicle's ECUs, limiting critical cryptographic keys to a single asymmetric update signing key. This design minimizes complexity and enhances security by reducing potential attack surfaces.

By leveraging TPM's advanced features, our system ensures secure transmission of updates from the backend to the vehicle, followed by a safe update installation process. This setup addresses existing requirements and provides a robust security framework for connected vehicles. Our contributions include designing a system with minimal Trusted Computing Base (TCB), tailored to automotive architectures with minimal interference, and ensuring compliance with TPM 2.0 specification. The TPM 2.0's security capabilities are fully utilized, enhancing the overall security framework for connected vehicles.

6.2

In summary, our solution presents a secure, lightweight OTA update distribution mechanism, combining strong security guarantees with practical applicability in the automotive domain. It stands out by uniquely addressing all critical requirements and features for secure OTA updates.



Interested to learn more? See Christian Plappert and Andreas Fuchs, „Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles“, Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC), 2023, https://doi.org/10.1145/3627106.3627135.

Authors: Christian Plappert (Fraunhofer SIT), Florian Fenzl (Fraunhofer SIT)

6.3 Lightweight ECU Attestations for Securing Smart Sensors

The increasing connectivity of modern vehicles presents significant cybersecurity challenges. As vehicles incorporate more advanced driving assistance systems, the complexity of their electronic architectures grows, leading to a larger cyberattack surface. The IDS has become a promising mitigation technology to secure against runtime attacks. However, their efficiency relies on secure operation of smart sensors.

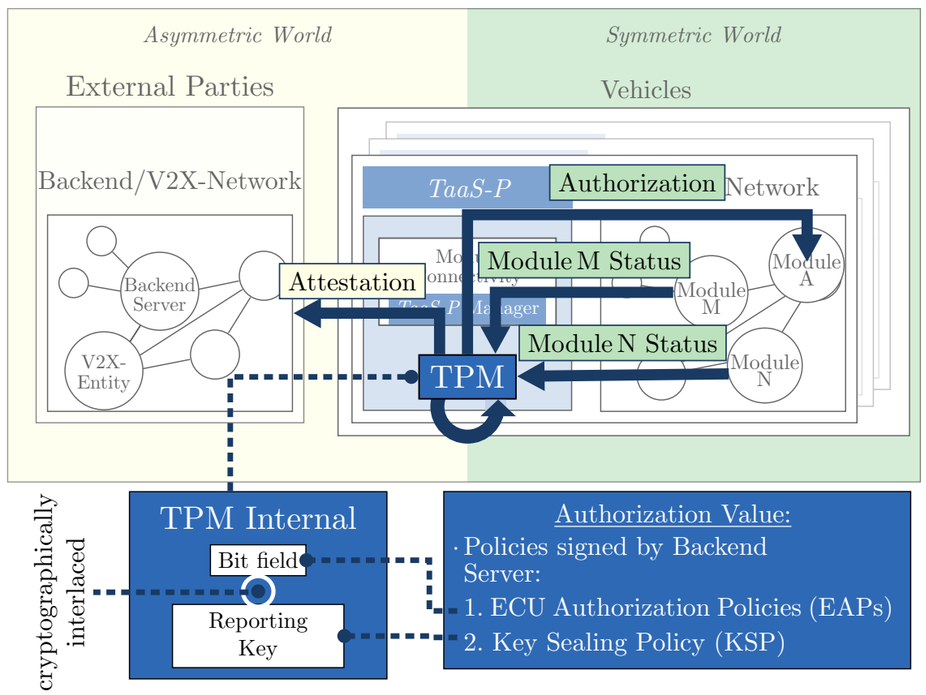
To secure the operation of smart sensors, we developed a novel security concept that enhances the security of in-vehicle processes. The foundation of our security mechanism lies in the integration of two trusted computing technologies: the TPM and the Device Identifier Composition Engine (DICE). The TPM, installed within the vehicle's telematics unit, serves as a central hardware trust anchor. It securely verifies the current software state of the vehicle's ECUs, ensuring authenticity and integrity. DICE provides a lightweight root of trust, ideal for resource-constrained controllers, enabling secure bootstrapping and reporting of software states.

Our approach allows the ECUs to report their running software versions to the TPM securely. If an ECU's software state is verified as authentic, the TPM can authorize the vehicle's transition from an update-ready state back to its fully functional mode. This mechanism ensures that any updates are installed safely, maintaining the vehicle's operational integrity.

By implementing this security concept, we provide a comprehensive solution that addresses the critical requirements for secure OTA updates. Our system is designed to be seamlessly integrated with existing update distribution mechanisms, providing a robust framework for maintaining vehicle security.

6.3

In conclusion, as the automotive industry continues to evolve, ensuring the security of connected vehicles becomes paramount. Our solution offers a secure and lightweight method for ECU attestations, fortifying the overall security architecture of modern vehicles.



Interested to learn more? See Christian Plappert and Andreas Fuchs, „Secure and Lightweight ECU Attestations for Resilient Over-the-Air Updates in Connected Vehicles“, Proceedings of the 39th Annual Computer Security Applications Conference (ACSAC), 2023, https://doi.org/10.1145/3627106.3627202.

Authors: Christian Plappert (Fraunhofer SIT), Florian Fenzl (Fraunhofer SIT)

6.4 Architectural Strategies for Secure Execution of Railway Intrusion Detection Systems

Systems, like an IDS, need to operate in a secure execution environment where sensitive data, logic, and communication remain secure, even under adversarial conditions. We explored three architectural strategies to achieve this goal: container-based isolation, separation kernels, and secure, measured boot.

Containers, like Docker, offer a lightweight and flexible method to isolate the IDS from other onboard applications. The IDS runs inside a sandboxed environment, separated from the underlying host system, which itself is considered untrusted. Sensitive data such as detection rules, cryptographic keys, and logs are stored in TPM-backed secure storage.

To ensure trust in the IDS container, its integrity is verified using attestation, either locally or remotely from a backend. This process confirms that the container has not been tampered with before sensitive operations or communication take place. Communication between the container and backend systems is encrypted, with keys protected inside the container's secure storage.

This approach benefits from ease of deployment and compatibility with existing infrastructure, making it suitable for gradual integration into vehicle fleets. However, because the host operating system remains outside the Trusted Computing Base (TCB), it is crucial to perform regular attestations to detect any compromise.

A more robust approach uses a **separation kernel** to enforce strong partitioning between trusted and untrusted components. The IDS runs in its own secure partition, separate from other vehicle software. Each partition has restricted access to resources and communication channels, enforced at the kernel level.

This architecture reduces the TCB and prevents attacks from compromising the IDS via other software components. Secure storage is implemented within the trusted partition, again using TPM functionality. The separation kernel supports both spatial and temporal isolation, which is crucial for real-time applications in embedded environments.

Attestation is integrated at the partition level and can be performed either locally by a dedicated verification partition or remotely. This architecture provides high assurance against lateral attacks and is particularly well-suited for safety-critical systems with stringent isolation requirements.

Secure and measured boot ensures that the IDS environment starts in a trusted state. Each stage of the boot process is measured, i.e., cryptographically hashed, and recorded in TPM registers. Any unauthorized modification to the bootloader, operating system, or application stack is detected before execution.

In this setup, trust is anchored in the boot process itself. If all boot stages match known-good measurements, the system is deemed trustworthy. Extending the boot process with rollback protection ensures that older, vulnerable configurations cannot be reloaded.

While this method offers strong guarantees at startup, it lacks runtime isolation and cannot detect modifications after the system has booted. It is therefore best used in combination with runtime protections or regular re-attestation cycles to maintain integrity over time.

Each of these strategies provides a different balance of flexibility, security, and complexity. Containers are easy to deploy and manage but offer weaker isolation. Separation kernels deliver strong security boundaries at the cost of integration effort. Measured boot establishes system integrity but requires additional mechanisms for runtime assurance.

Authors: Simon Unger (University of Passau), Stefan Katzenbeisser (University of Passau)

6.5 Non-Restrictive Hardware-Based Trust in Embedded High-Level Operating Systems

Embedded systems often rely on restrictive mechanisms to enforce software integrity. While secure, such mechanisms can limit flexibility, hinder repairability, and reduce control for device owners. An alternative architecture demonstrates that strong protection can also be achieved through non-restrictive methods that monitor and verify system state without enforcing execution restrictions.

The design focuses on four main goals: preventing rollback to outdated or vulnerable software versions, supporting safe system updates, securing sensitive data, and enabling remote attestation of device integrity. It builds on capabilities offered by a TPM, which acts as an independent security component within the device.

To prevent rollback attacks, we introduce a version tracking mechanism that recognizes whether the software running on the device is current or outdated (inside or outside a pre-defined rollback window). Therefore, we use non-volatile (NV) extend-indices and signed TPM policies.

Updates follow a two-partition A/B update scheme that maintains two OS slots, each with its own bootable image. Updates are installed to the inactive slot, and only switches fully to the new version once it confirms successful startup, reducing the risk of failed updates. This mechanism allows updates to move forward securely while still permitting a controlled fallback in case an update fails, ensuring devices remain functional even during recovery.

Sensitive information, such as encryption keys, is tightly bound to the trusted state of the system. Access to this data is granted only if the system's configuration matches expected conditions, ensuring that unauthorized changes or attempts to revert to older software render the data inaccessible. A built-in check detects attempts to replay or restore outdated data, blocking these actions automatically.

The architecture also includes the ability for remote systems to verify that a device is running the expected software. This allows network administrators or service providers to assess the trustworthiness of devices in the field without direct physical access.

We implemented a boot process that realizes these mechanism with manageable overhead. Overall, the system shows how embedded devices can be both secure and flexible. By avoiding restrictive mechanisms and instead relying on verifiable evidence of integrity, it supports sustainable, repairable, and usercontrolled deployments while maintaining strong protection against tampering and misuse.

Interested to learn more? See Simon Unger, Sven Gebauer, and Stefan Katzenbeisser, „Non-Restrictive Hardware-Based Trust in Embedded High-Level Operating Systems“, Proceedings of the IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2025, https://doi.org/10.1109/Trustcom66490.2025.00066.

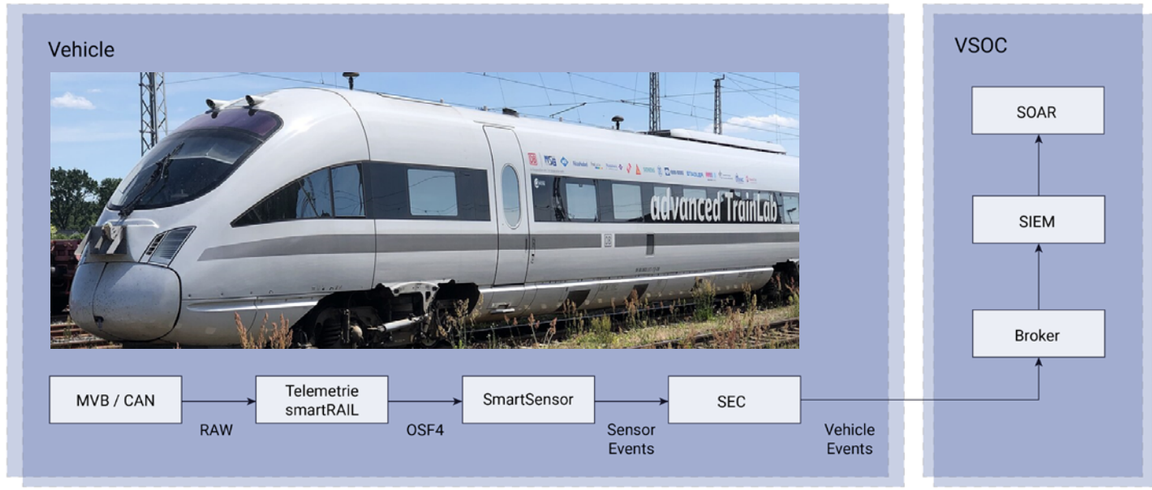
Authors: Simon Unger (University of Passau), Stefan Katzenbeisser (University of Passau)

7 Test Platforms and Evaluation

7.1 aTL Integration: Technical Implementation of Rail Cybersecurity

Advanced Train Laboratory (aTL) of DB Systemtechnik serves as a test platform for the practical implementation of the FINESSE IDS in the rail domain. The train enables testing of cybersecurity systems under real operational conditions. The aTL integration is based on a multi-stage data processing architecture. MVB and CAN buses are directly tapped on board and already provided in OSF4 format. Transmission occurs via UDP to a RailPC equipped with a TPM. MVB and CAN smart sensors run in Docker-based containers and normalize incoming OSF4 data while checking for manipulations. To address bandwidth limitations, smart sensors implement intelligent data filtering that reduces transmission volume by forwarding only security-relevant events, suspicious activities, and anomalies to the VSOC, ensuring efficient use of available mobile connectivity. Anomaly detection is performed through a combination of signature-based methods for known attack patterns and behavior-based algorithms that identify statistical deviations in protocol communication. When anomalies are detected, an alarm is generated and forwarded to the SEC. The SEC collects and analyzes all relevant events from various IDS systems within the vehicle and buffers them locally during VSOC outages. The architecture enables both distributed and centralized deployment scenarios depending on available hardware and system requirements. The consolidated security events are transmitted to the central VSOC via MQTT protocol. A critical requirement is the non-intrusive implementation of all IDS components, which operate exclusively in read-only mode to prevent any interference with safety-critical vehicle systems. In the VSOC, entire vehicle fleets can be centrally monitored, enabling fleetwide threat analysis and coordinated security measures.

The functionality of the overall architecture has been successfully demonstrated on a real rail vehicle through the ATL demonstrator. Initial simulated attacks on the train are detected and handled by the system, validating the effectiveness of the integrated security approach. aTL of DB Systemtechnik serves as a test platform for the practical implementation of the comprehensive FINESSE IDS in the rail domain.



Authors: Ali Recai Yekta (Yekta IT), Andreas Isbarn (DB Systemtechnik), Dominik Spychalski (INCYDE), Simon Unger (University of Passau)

7.2 Fraunhofer Security Evaluation Platform for Autonomous Driving (SEPAD)

The development and evaluation of security solutions for autonomous vehicles is a challenging task. Many researchers have no access to real vehicles to implement and test their solutions. In addition, vehicle E/E architectures of different brands or even model series of one car manufacturer differ significantly. Also, vehicles may be the source of physical hazards, e.g., an exploding airbag. To enable researchers to develop, implement, and evaluate new security solutions for autonomous vehicles, we propose a new security evaluation platform called Security Evaluation Platform for Autonomous Driving (SEPAD) and a dedicated development process for testing security mechanisms with it. SEPAD allows modeling realistic E/E architectures where the developed security solutions can be integrated and evaluated without causing safety risks for the researcher or other road users.

For FINESSE, we instantiated SEPAD for the IDS use case and deployed our developed security solutions. Figure 10 shows the relevant components. In particular, the vehicle network is based on modern zonal E/E architectures (cf. chapter "Vehicle Architectures and Technologies") and comprises three interconnected Raspberry Pi single-board computers with multiple sensors used for the sensor fusion process for its autonomous driving ability. The sensors consist of a depth camera, lidar, ultrasonic sensor, and gyroscope. Data communication is done over Automotive Ethernet and SOME/IP services.

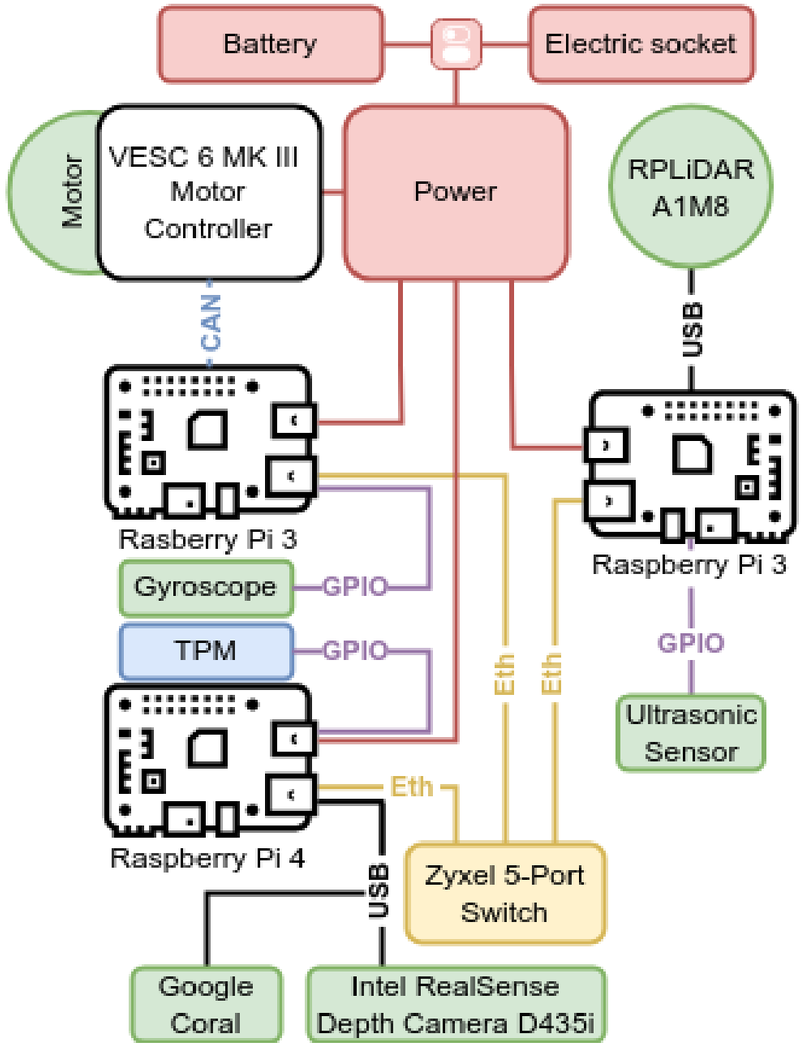


Figure 10: Robocar Architecture

Authors: Florian Fenzl (Fraunhofer SIT), Christian Plappert (Fraunhofer SIT)

7.2

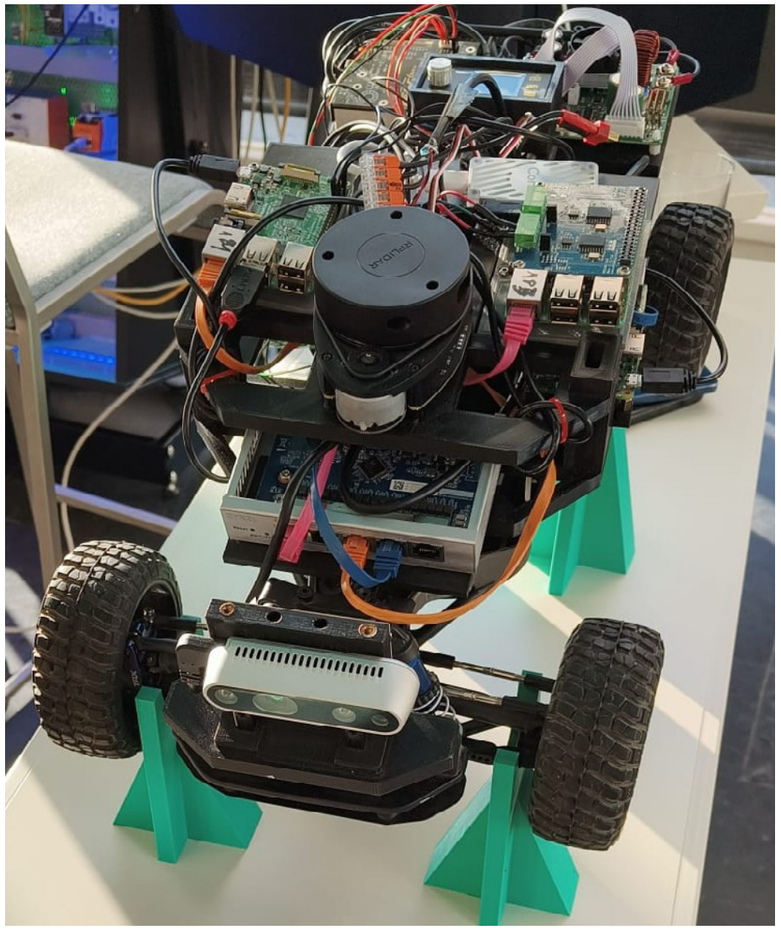


Figure 11: Security Evaluation Platform for Autonomous Driving (SEPAD)

Interested to learn more? Daniel Zelle et al. “SEPAD – Security Evaluation Platform for Autonomous Driving.” In: 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). 2020, pp. 413–420. doi: 10.1109/PDP50117.2020.00070

Authors: Florian Fenzl (Fraunhofer SIT), Christian Plappert (Fraunhofer SIT)

7.3 Yekta IT Automotive Demonstrator

System Architecture

The demonstrator is designed as a portable case and emulates the security architecture of connected vehicles. The system comprises Electronic Control Units (ECUs) with CAN communication, a vehicle network with CAN-Bus and Unified Diagnostic Services (UDS), and an OBD-II interface for real diagnostic devices.

YekCar - Yekta IT Automotive Security Demonstrator

The multi-layered dashboard system consists of three components: The vehicle dashboard displays real-time parameters such as speed, RPM, and temperature. The attacker dashboard enables CAN message injection, speed manipulation, and UDS attacks, while providing comprehensive message logging capabilities. The IDS monitor supervises CAN-Bus and UDS traffic in real-time and visualizes suspicious activities. The CARLA 3D simulation environment represents cyberattack effects on autonomous vehicles, controllable via Xbox controller. A keyless entry system demonstrates replay attacks on keyless access systems.

Security Analysis and Monitoring

The system implements dedicated intrusion detection capabilities through CAN-IDS and UDS-IDS components that monitor respective protocol traffic for anomalous patterns. The integrated Vehicle Security Operations Center (VSOC) collects and correlates these detection logs from the various monitoring systems. Security Information and Event Management (SIEM) aggregates the collected data for comprehensive threat analysis. Detected attacks are mapped to the Vehicle Adversarial Tactics, Techniques, and Expert Knowledge (VATT&EK) framework, an automotive-specific adaptation of MITRE ATT&CK for systematic categorization of attack vectors.

This comprehensive setup provides researchers with a realistic testbed for investigating automotive cybersecurity threats and developing defensive strategies. The system facilitates controlled experimentation with attack scenarios while enabling real-time observation of detection mechanisms and their effectiveness.

Authors: Ali Recai Yekta, Cenk Yekta, Clara Eggers, Erhan Yekta, Marco Gren, Max Randhahn, Moritz Reichelt (all Yekta IT)

7.4 Yekta IT Rail Demonstrator

The increasing digitalization of rail vehicles makes them attractive targets for cyberattacks. To develop realistic attack and detection methods for the Multifunction Vehicle Bus (MVB), we pursued a systematic approach from analyzing real trains to integration into a Rail Security Operations Center.

Analysis of Real Rail Vehicles

Our research began with detailed analysis of real trains. The Advanced TrainLab (ATL) of DB Systemtechnik provided insights into real MVB implementations according to IEC 61375. The Class 605 (ICE TD) served as reference for complex MVB topologies with numerous networked control units. This analysis enabled extraction of authentic signal definitions and timing parameters as foundation for our simulators.

Development of Train Simulators

Based on these findings, we developed two complementary approaches. The physical YekTrain simulator serves as a demonstration platform replicating critical vehicle systems and features an interactive dashboard for manual control and haptic interaction with the simulated systems. The virtual MVB simulator implements the complete MVB protocol in master-slave architecture, encompassing all nine critical vehicle systems from HVAC and door control through traction and braking to safety systems and drivermachine interface. This virtual environment serves as the primary platform for attack execution and detection.

Attack Simulation and Detection

To create realistic threat scenarios, we implemented a compromised DMI component capable of spoofing telegrams from other vehicle components. This performs targeted attacks: triggering unplanned emergency braking and false fire alarm system alerts by spoofing the corresponding safety telegrams. In parallel, we developed an MVB-IDS for detecting spoofing attacks. All components were integrated into a dedicated Rail Security Operations Center that centrally collects security events, visualizes threats in real-time, and enables live monitoring of the YekTrain simulator with geographical representation of security events.

7.4

The developed test environment successfully demonstrates the integration of all components from physical YekTrain simulation through virtual MVB implementation to the Rail Security Operations Center. The compromised DMI component can successfully forge safety telegrams, while the MVB-IDS detects these activities and forwards them to the Security Operations Center. The platform confirms fundamental vulnerabilities in MVB systems and highlights the need for improved authentication and monitoring.

Conclusion

Our systematic approach from analyzing real trains through simulator development to SOC integration demonstrates the feasibility of a comprehensive cybersecurity test environment for rail vehicles. The combination of physical and virtual simulators, realistic attack simulations, and specialized detection creates a unique research platform. Next steps include comprehensive experimental evaluations, extension to additional protocols, and machine learning-based anomaly detection. The developed test environment contributes to improving cybersecurity in critical rail infrastructures.

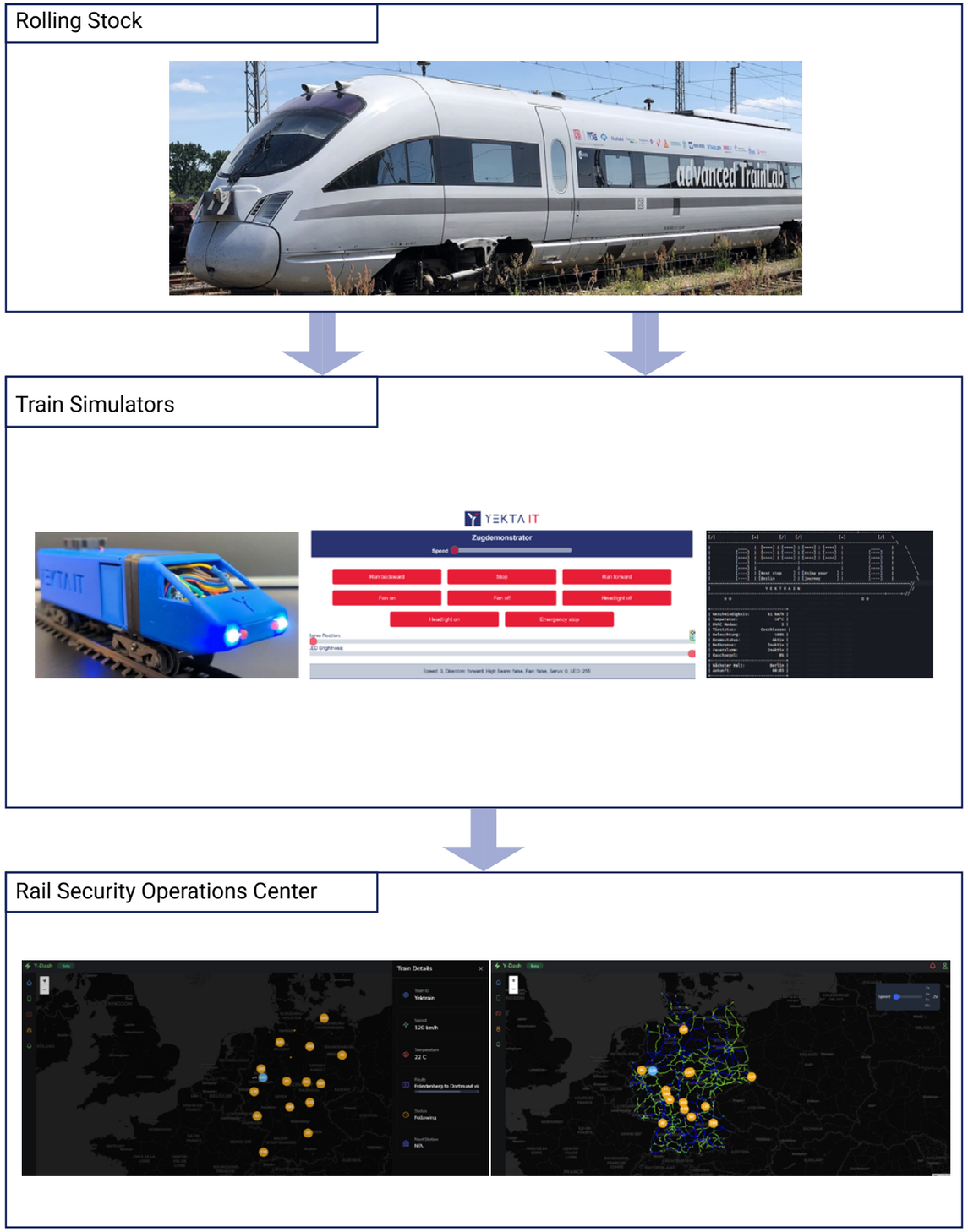


Figure 12: Yektrain - Yekta IT Rail Demonstrator

Authors: Ali Recai Yekta (Yekta IT), Cenk Yekta (Yekta IT), Marco Gren (Yekta IT), Max Randhahn (Yekta IT)

7.5 INCYDE Rail Demonstrator

To demonstrate the learning and findings of INCYDE GmbH within the FINESSE project, a rail demonstrator was built, which abstracts a railway architecture, commonly used field technologies, and their potential cyber threats. The demonstrator design consists primarily of the control module and the logic module.

The control module represents the driver's cab and houses various inputs such as the accelerator/brake lever, direction, and door control buttons. Additionally, various displays are available to show the overall vehicle status, including speed, door status, and cybersecurity status, with the potential to monitor the demonstrated train.

The logic module is the heart of the demonstrator and is intended to represent the technical train system. It contains several control units that communicate with each other via actual MVB.

- DMI: read, write driver input/output on MVB
- Door control unit: simulates doors I/O
- ECU: simulates Motor I/O
- TCU: connects the vehicle system with external environmental components, a SIEM in our case.

An IDS developed by INCYDE continuously analyzes the MVB communication within the vehicle. It is capable of successfully detecting attacks, using ML approaches. Whenever an attack is detected, a message is sent to the installed SEC, and the demonstrators' blue and green color theme is switched to red, signaling a potential threat.

Particularly noteworthy in this context is the INCYDE-MVB-Attacker, a microcontroller developed by INCYDE, which enables MVB attacks, thereby allowing the testing of the IDS accuracy. This microcontroller was specially developed to meet the electrical specifications of the MVB and provide the necessary functionality to support it. More on that in article "MVB-IDS".

7.5

The Attacker remains unnoticed in the first phase of collecting information. Once sufficient information has been collected, the INCYDEMVB-Attacker can remotely switch to attack mode. Therefore, the INCYDE Rail Demonstrator is capable of showcasing a complete, real-world MVB attack and detection chain, starting from the attack (INCYDE-MVB-Attacker) through detection (IDS) to countermeasures (SEC) and further notification (SIEM).

INCYDE-MVB-Attacker
Easily plugged into existing MVB networks with its standard D-Sub connectors. It is then able to listen to the MVB, as well as intercept and block messages, and infiltrate its data. The microcontroller is controlled wirelessly over Bluetooth. Combined with a celluar module, the INCYDE-MVB-Attacker can be secretly installed into a system and remain undetected, while being remotely manageable by an attacker from anywhere in the world.

Author: Sofian Beyer (INCYDE GmbH)

8

FINESSE Project Contributions to Fleet Security

8 FINESSE
Project Contributions to Fleet Security Monitoring

The FINESSE Project has made significant strides in enhancing fleet security monitoring solutions for both rail and street vehicles. Below are key contributions and innovations introduced by the project:

Multimodal Approach

FINESSE has developed solutions that cater to both rail and street vehicles, carefully analyzing the commonalities and distinctions between these two domains. Notable advancements include the design of intrusion detection sensors and event processing components applicable to both rail and automotive contexts.

From On-board to Off-Board

FINESSE provides new concepts for the vehicle side as well as for the backend "Security Operation Center" side of fleet security monitoring systems. This includes on-board security event processing and the integration of asset management, which are critical components of effective fleet security monitoring systems.

Over all system layers

FINESSE addresses fleet security monitoring across all system layers, from high-level architectures to software components and hardware trustanchor mechanisms. A prime example is the implementation of a robust Hardware-Security-based platform security concept, which is based on a central Trusted Platform Module (TPM) placed within the vehicle E/E architecture.

VATT&EK

FINESSE has developed VATT&EK (Vehicle Adversarial Tactics, Techniques & Expert Knowledge), a specialized framework that employs the TTP approach to systematically analyze cyber threats in Intelligent Transportation Systems. This framework is tailored specifically for automotive and rail systems, providing structured methodology for developing targeted cybersecurity countermeasures.

8

Analytics and Artificial Intelligence

The project leverages advanced analytics and AI techniques to generate and analyze vehicle security events. A specific highlight is the use of genetic programming to derive security rules tailored for Automotive Ethernet.

Demonstrators

To showcase its concepts, FINESSE has developed tangible physical prototypes, including Automotive Security and Rail Security Demonstrators, which have been presented at various trade fairs and research events.

Influencing Standardization

The outcomes of the FINESSE Project are actively contributing to standardization efforts in fleet security monitoring systems, exemplified by the standardization of automotive security events within the AUTOSAR framework.

Live in Trains

The Advanced Train Lab (ATL) served as a practical environment for evaluating FINESSE technologies, providing insights into their real-world applicability.

All FINESSE contributions integrate into a common view on cross-domain fleet security monitoring.

Acronyms

ABAC	Attribute-based access control
AE	Automotive Ethernet
AI	Artificial Intelligence
aTL	Advanced Train Laboratory
ATO	Automatic Train Operation
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BoM	Bill of Materials
CAN	Controller Area Network
CRA	Cyber Resilience Act
CSMS	Cyber Security Management System
DICE	Device Identifier Composition Engine
DoIP	Diagnostics over Internet Protocol
E/E	Electrical / Electronic
ECN	Ethernet Consist Network
ECU	Electronic Control Unit
ETB	Ethernet Train Backbone
ETCS	European Train Control System
eVSE	Enhanced Vehicle Security Event
GoA	Grades of Automation
HIDS	Host-based IDS
HTA	Hardware Trust Anchor
IDS	Intrusion Detection System
IoV	Internet of Vehicles
ISAC	Information Sharing and Analysis Center
IT	Information Technology
ITS	Intelligent Transport Systems
MACsec	Media Access Control Security
ML	Machine Learning
MVB	Multifunction Vehicle Bus
NIDS	Network-based IDS
NV	non-volatile
OBD	On-board Diagnostics
OCORA	Open CCS On-Board Reference Architecture
OT	Operational Technology
OTA	Over-the-Air
QSEV	Qualified Security Event
RSE	Raw Security Event
RTE	Real-Time Ethernet
SDV	Software-defined Vehicle
SEC	Security Event Center
SEPAD	Security Evaluation Platform for Autonomous Driving
SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Center
SOME/IP	Scalable service- Oriented Middleware over IP
SSA SOC	Security Alert
TCB	Trusted Computing Base
TCN	Train Communication Network
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRDP	Train Real-time Data Protocol
TSN	Time-Sensitive Networking
TTP	Tactics, Techniques, and Procedures
UDS	Unified Diagnostic Services
VATT&EK	Vehicle Adversarial Tactics, Techniques & Expert Knowledge
VSA	Vehicle Security Alert
VSE	Vehicle Security Event
VSOC	Vehicle Security Operation Center
WTB	Wire Train Bus