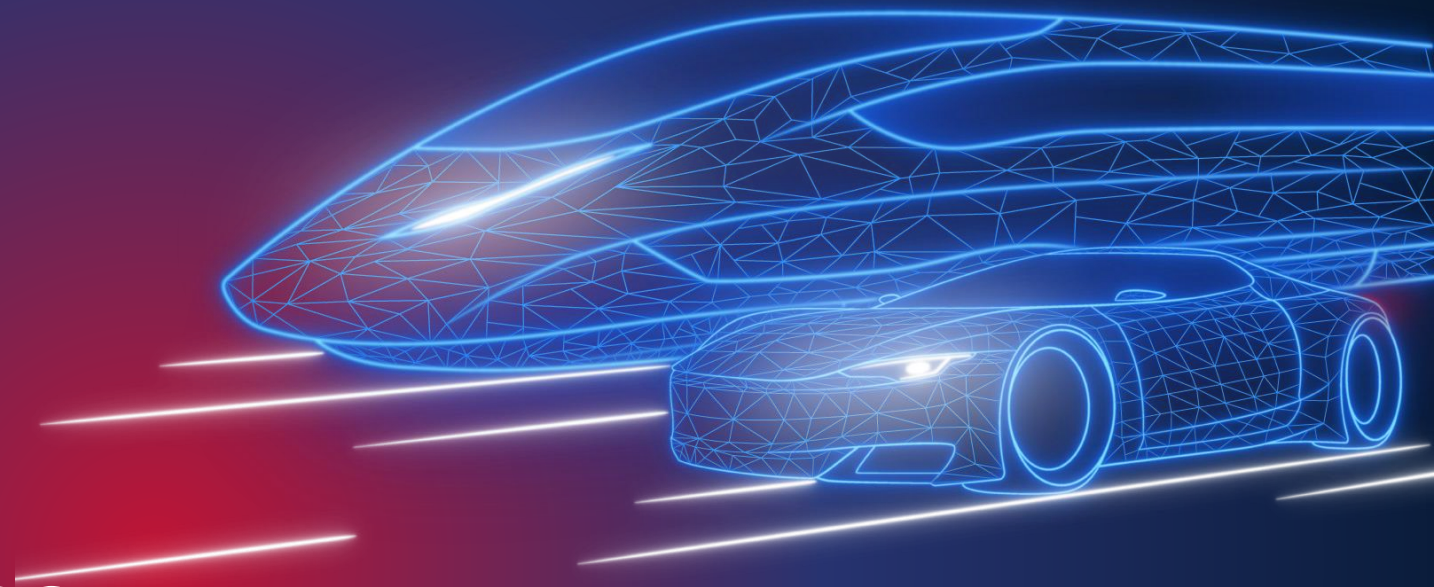


From ECU to VSOC: UDS Security Monitoring Strategies

The 19th International Conference on

Emerging Security Information, Systems and Technologies

Ali Recai Yekta[1] (ali@yekta-it.de), Nicolas Loza[2], Jens Gramm[2], Michael Peter Schneider[2], Stefan Katzenbeisser[3]

[1]Yekta IT GmbH, [2]ETAS GmbH, [3]University of Passau

whoami

Ali Recai Yekta

CTO & Head of Cybersecurity

- 15+ years of cybersecurity experience in IT and OT systems
- Red and Blue Team specialist
- Building and operating SOCs for critical infrastructure
- Extensive experience in railway, automotive, and energy sectors
- Co-founder and Head of Cybersecurity at Yekta IT GmbH
- Research focus on OT security
- Master's degree in IT Security (Ruhr University Bochum)
- OSCP, OSWE, OSEP, CRTO Certifications

FINESSE – Research Project

FINESSE Project Objectives:

- Multi-modal security monitoring for road and rail vehicles with synergy effects identification
- Unified security architecture across all system layers
- On-board components for vehicle-specific attack detection and system-wide analysis
- Fleet-scale attack detection and backend analytics

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/finesse

This research was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) within the project "FINESSE" (FKZ 16KIS1584K).

Federal Ministry of Research, Technology and Space

Motivation

Modern Vehicles

- Increasing complexity
- Connectivity and wireless interfaces
- Vulnerable to cyberattacks

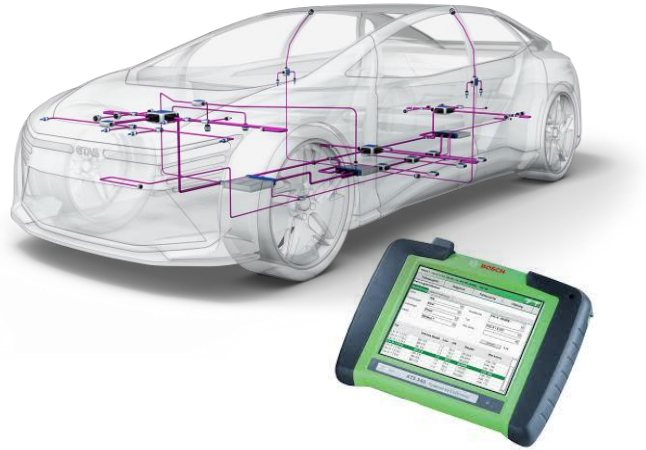
UN R155 Regulation

- Mandatory cybersecurity requirements
- Detection & response required
- Fleet security monitoring is a technical measure to satisfy certain regulation requirements

- Vehicle security monitoring for vehicle fleets has been established
- Still not well understood how to detect higher-level attack techniques from low-level security events
- We consider a widely used vehicle diagnostic protocol (UDS) as an example

Research Gap: Security monitoring for the UDS protocol has not been studied systematically before

Unified Diagnostic Services (UDS) Security



Unified Diagnostic Services (UDS) Protocol [ISO 14229]: **The Critical Entry Point**

- **Most widely used** automotive diagnostic protocol
- **Entry door** to Electronic Control Units (ECUs)
- Used during **all lifecycle phases**: development, testing, operation, maintenance
- **High level of control** over ECU functionality

- UDS security investigated in **isolated cases**
- Focus mainly on **Security Access Service**

- **Comprehensive taxonomy of attack techniques for UDS** [1]
- 53 UDS attack techniques along 9 tactics of known attack frameworks

Persistence (PS)
Resource Development (RD)
Lateral Movement
Privilege Escalation (PE)
Affect Vehicle Function (AF)
...

[1] A. Yekta, et al, “UDS attack taxonomy: Systematic classification of vehicle diagnostic threats,” CPS-Sec 2025, IEEE, 2025.

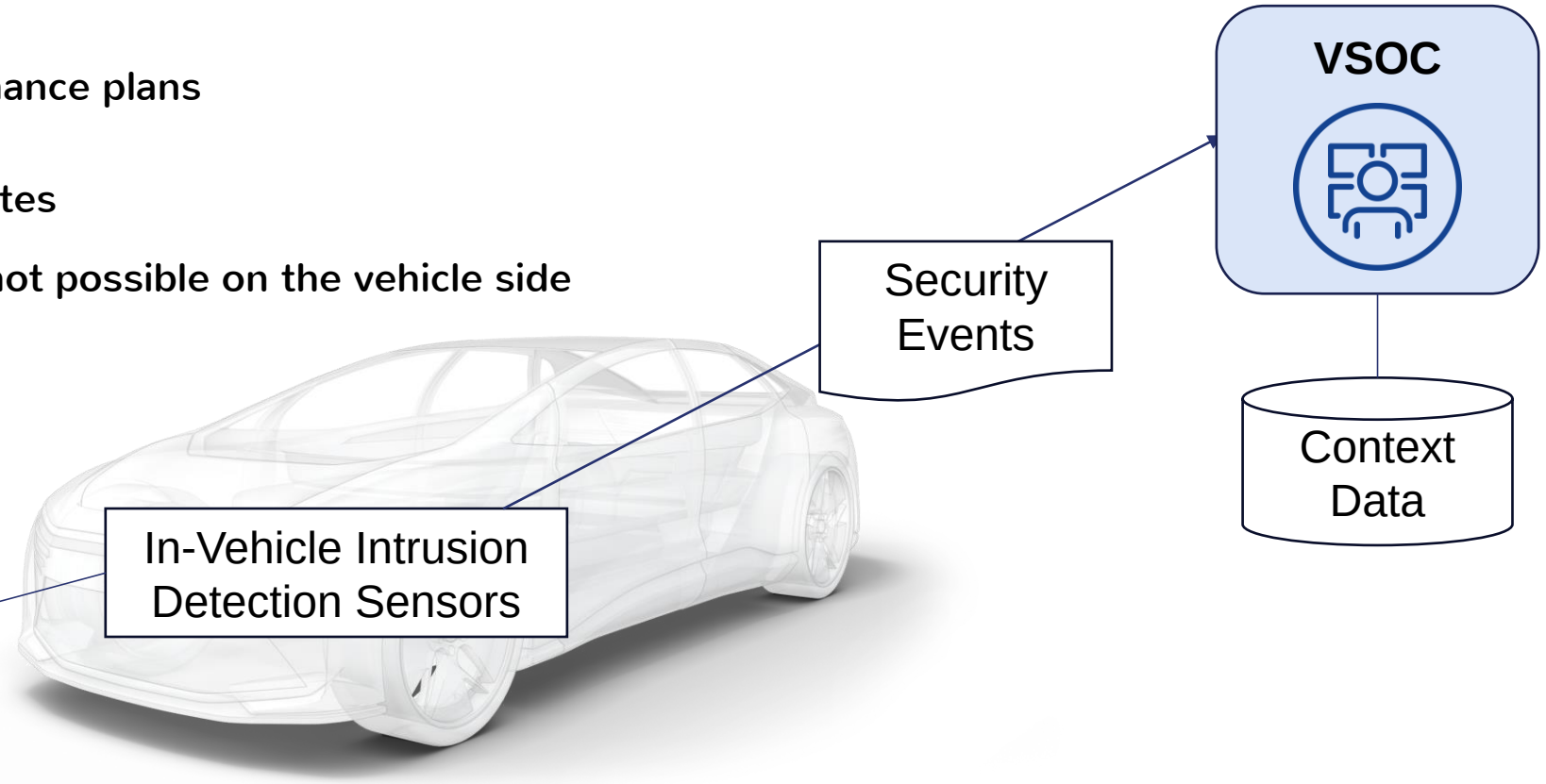
UDS Protocol Overview [ISO 14229]

- Communication standard between **diagnostic testers** and **ECUs**
- Request-response protocol with **Service IDs (SIDs)**
- Many services provide **powerful ECU control**

Service ID	Service Name	Purpose
0x10	DiagnosticSessionControl	Change diagnostic sessions
0x22	ReadDataByIdentifier	Read ECU data
0x27	SecurityAccess	Authentication & authorization
0x2E	WriteDataByIdentifier	Write ECU data
0x31	RoutineControl	Execute ECU routines
0x34/36	RequestDownload/TransferData	Software updates
...	...	...

VSOC: Vehicle Security Operations Center

- Collects security events from **entire vehicle fleet**
- Correlates with **context data**:
  - Vehicle records & maintenance plans
  - Threat intelligence feeds
  - Authorized firmware updates
- Enables **advanced detection** not possible on the vehicle side



- CAN IDS
- Ethernet IDS
- Host-Based IDS
- …

AUTOSAR Security Events

Industry Standard for Automotive Software

- Widely adopted **firmware specification**
- Native support for **Security Events (SEvs)**
- Standardized logging Formats

Example: AUTOSAR Security Event 103

SEV_UDS_SECURITY_ACCESS_FAILED

Triggered when SecurityAccess (0x27) authentication fails

Evaluation Focus: Assess how well current AUTOSAR standard supports UDS attack detection

Methodology

Methodology: Three-Layer Strategy

1. **Logging Strategies:** Define **which events** to log in vehicles
2. **Context Data Strategy:** Specify **which context information** to capture with logs
3. **Detection Strategies:** Develop rules to **identify attack scenarios** from logs

Logging Strategies

IR: Invalid Request: Log UDS requests that are invalid due to:

- Input validation failures (format, parameters, payload)
- Unexpected circumstances (e.g., vehicle driving, missing authorization)

FE: Function Execution: Log execution of **critical UDS services**

- Memory modifications
- Routine executions
- Authentication attempts

MFI: Message Flow Inconsistency: Log messages with routing anomalies:

- Unexpected source
- Modified during routing
- Unexpected sequence

Context Data Strategy

Basic Context

Service ID (SID)

Subfunction (SF)

Negative Response Code (NRC)

Timestamp

Service-Specific Context

Data Identifiers (DIDs)

Memory addresses & sizes

Routine IDs

Hashes over transferred data

Context Data: Examples

SID	Service	Context Data to Log
0x27	SecurityAccess	SID, Subfunction, NRC
0x2E	WriteDataByIdentifier	SID, DID, **hash over data**, NRC
0x31	RoutineControl	SID, Subfunction, RoutineID, NRC
0x34	RequestDownload	SID, memAddr, memSize, NRC
0x37	RequestTransferExit	SID, NRC, **hash over transferred data**

Detection Strategies

SLP: Suspicious Log Patterns

- Pattern matching with **threshold-based counting**
- Monitor for failed/rejected **UDS** operations
- Trigger alert when threshold exceeded

PTI: Product Threat Intelligence

- Use **threat intelligence feeds**
- CVE databases, forums, research papers
- Supplier vulnerability disclosures

CLC: Contextualized Log Checks

- Validate against **additional context information**
- Vehicle state & configuration
- Maintenance plans & service records
- Authorized firmware databases

Evaluation

AUTOSAR Logging Coverage

Question: ***How useful are current AUTOSAR standardized security events in UDS attack detection?***

Observations:

- AUTOSAR specifies Security Events for **13 out of 26 UDS services**.
- For UDS **attack technique taxomony with 53 attacks:**
  - **full logging support for 20 attacks**
  - **partial logging support for 10 attacks**

38-56%

Conclusions:

➔ AUTOSAR provides a good basis for UDS attack logging but it fails at providing complete coverage

➔ AUTOSAR does not support MFI (Message Flow Inconsistency) logging strategy

Example 1: **Brute-Force Security Access**

- **Attack:** Attacker tries to brute-force all possible "key" values for SA (0x27)
- **Detection:** Can be detected using
  - AUTOSAR Event 103:
  - SEV_UDS_SECURITY_ACCESS_FAILED

✓

Example 2: **Data Extraction**

- **Attack:** Attacker uses ReadDataByIdentifier (0x22) to extract confidential data (e.g., cryptographic keys)
- **Detection:** No AUTOSAR security event is available for 0x22

✗

Applicability of Detection Methods

Question: ***How well do the proposed detection strategies cover realistic attack scenarios?***

Reference: Comprehensive UDS Attack Taxonomy containing 53 attack techniques for UDS

Attack ID	Attack Name	SIDs	Logging Strategies	AUTOSAR Support	Detection Strategies
AT-RD-1	Firmware Reverse-Engineering	-	NA	No	PTI
AT-RD-2	Leak Secrets		NA	No	PTI
AT-PS-1	Download Custom Package	0x34, 0x36, 0x37	IR, FE	Only 0x34	SLP, CLC, PTI
AT-PE-1	Change to Privileged Session	0x10	FE, MFI	No	CLC
AT-PE-2	Valid Credentials	0x27, 0x29	FE	✓	CLC, PTI
AT-PE-3	Replay Attack SA	0x27	IR, FE, MFI	✓	SLP, CLC, PTI
AT-PE-4	Brute-Force SA	0x27	IR, FE	✓	SLP, CLC
AT-PE-5	Weak Auth29 configurations	0x29	IR, FE	✓	CLC
AT-DE-1	Block DTCs Generation	0x85	FE	✓	CLC
AT-DE-2	Remove Attack Traces in DTCs	0x14	FE	✓	CLC
AT-DE-3	Replay Download	0x34, 0x36, 0x37	FE	Only 0x34	CLC
					CLC, PTI
					CLC, PTI
				31	CLC
					SLP, CLC

Detection strategies
can be mapped to 52 attack techniques

Applicability of Detection Methods – Example 1

Brute-Force Security Access

Attack: Attacker tries to brute-force all possible "key" values for SA (0x27)

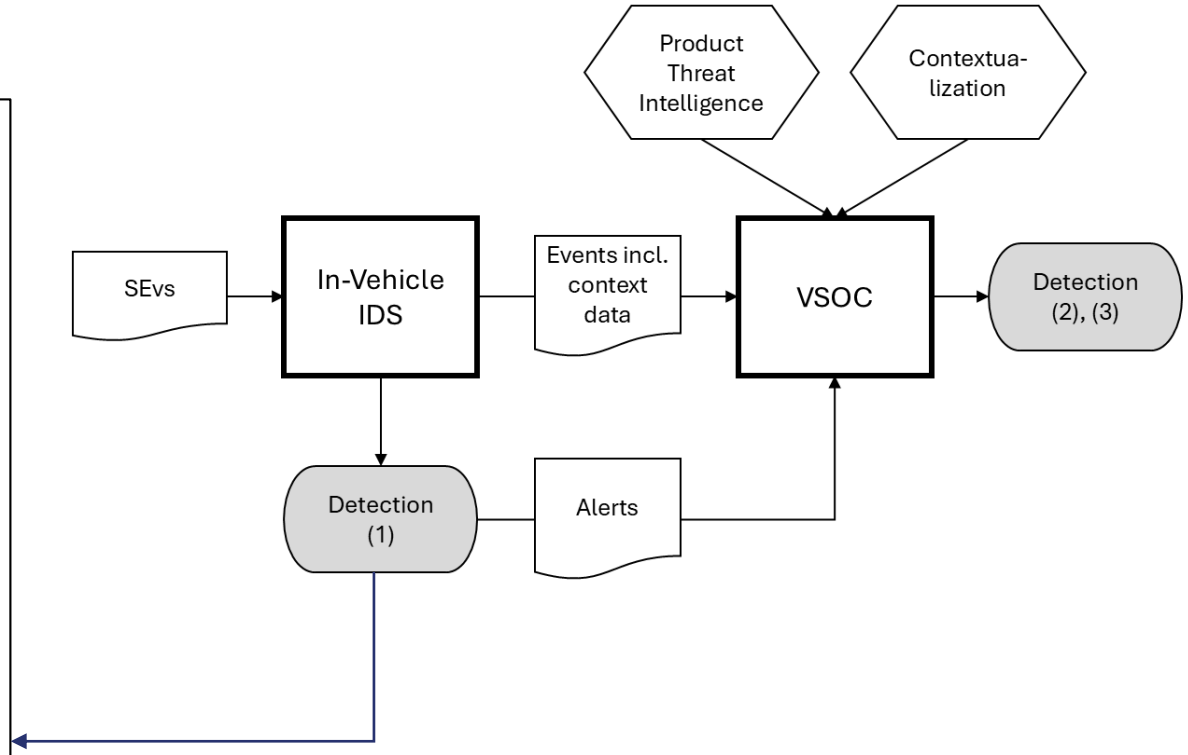
Detection Approach

Logging: IR strategy

- Use AUTOSAR Event 103: SEV_UDS_SECURITY_ACCESS_FAILED

Detection: SLP strategy

- Count failed 0x27 attempts within time window
- Alert when threshold exceeded



Applicability of Detection Methods – Example 2

Data Extraction

Attack: Attacker uses ReadDataByIdentifier (0x22) to extract confidential data (e.g., cryptographic keys)

Detection Approach

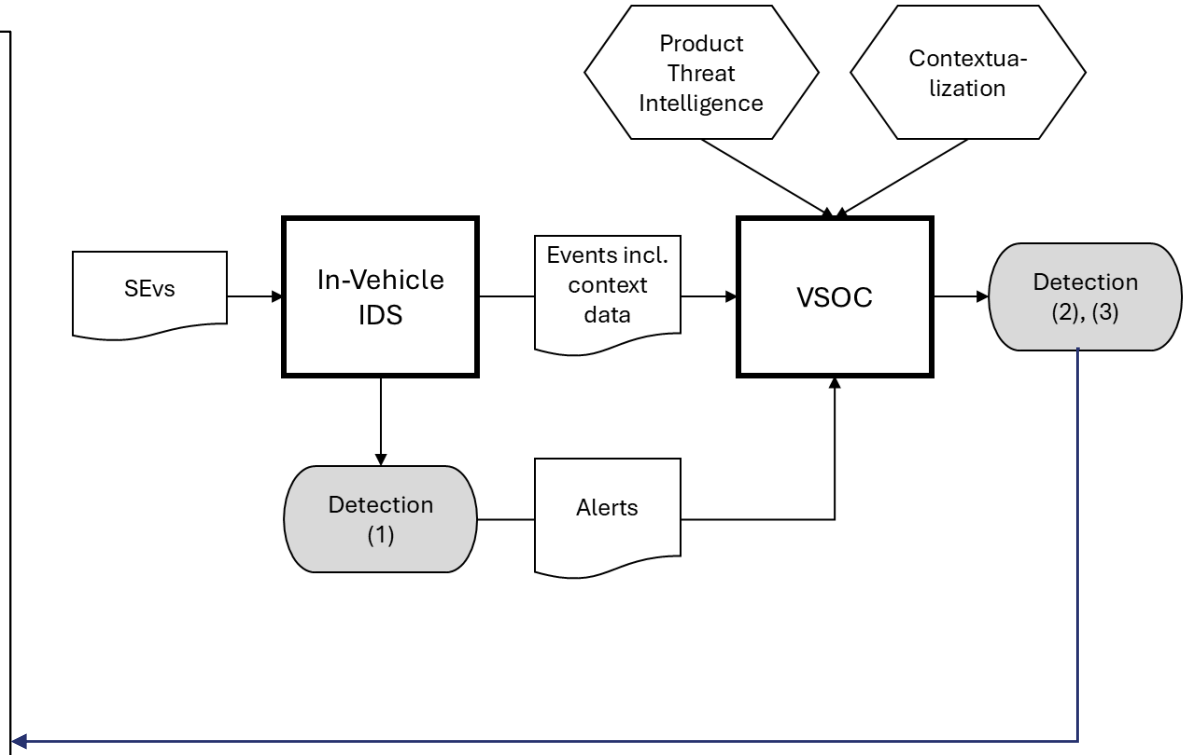
Problem: No AUTOSAR security events for 0x22

Logging: IR + FE strategies

- Log all accesses to **sensitive DIDs**
- Context: DID + NRC (for failed attempts)

Detection: CLC strategy in VSOC

- Filter: Only critical DIDs (e.g., crypto material)
- Validate against authorized access patterns



Applicability of Detection Methods – Example 3

Download Custom Package

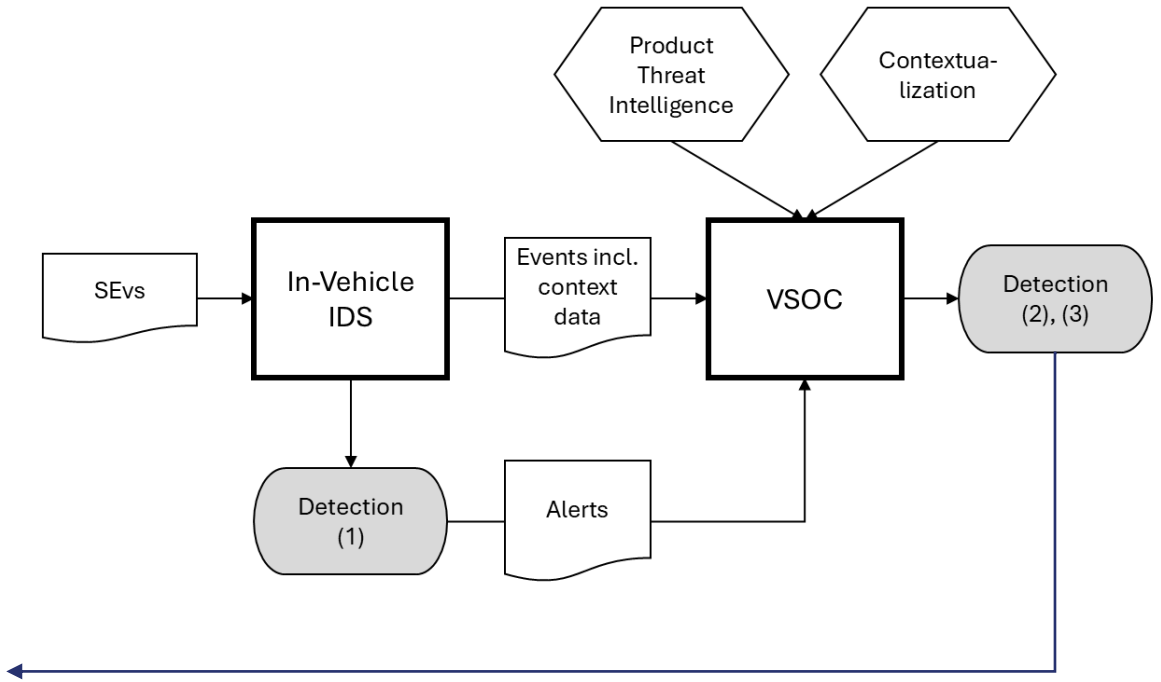
Attack: Attacker downloads malicious firmware using RequestDownload (0x34), TransferData (0x36), RequestTransferExit (0x37)

Logging: FE + IR strategies

- Log download operations (0x34, 0x36, 0x37)
- Context: **Firmware hash** on completion (0x37)

Detection: By detection strategy CLC

- **Detection strategy CLC: Correlate firmware hashes with those of authorized firmware databases**
- Detection strategy PTI: Look for published exploit patterns to install firmware
- Detection strategy SLP: Detect failed software update attempts in the operation



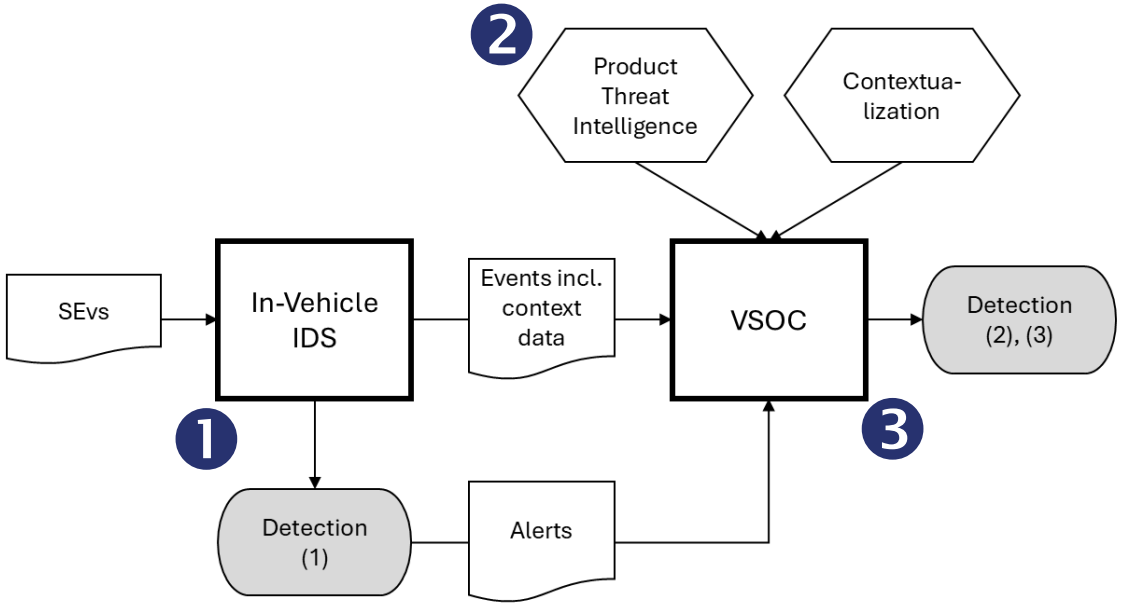
used additionally to raise reliability

Applicability of Detection Methods – Key Take-Aways

1. **Vehicle-side detection** can only cover a subset of UDS attack techniques.

2. **Product Threat Intelligence** is needed as part of a VSOC infrastructure

3. A **combination of detection strategies** as well as **backend processing in a VSOC** are needed for a maximum coverage and reliable detection of UDS attack techniques.



Conclusion

Contributions & Future Work

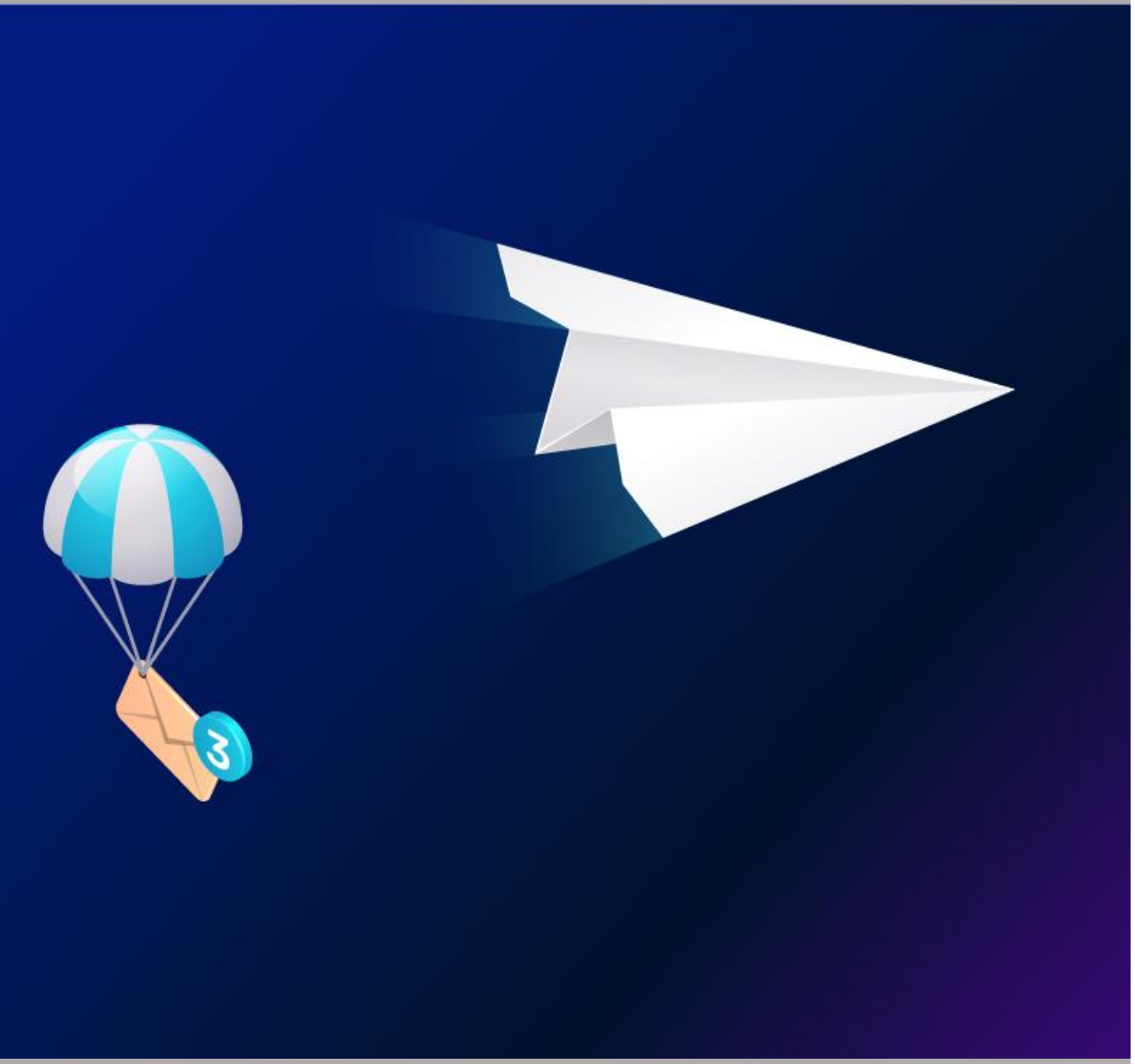
- ☑ Overview on detection strategies for attack techniques misusing the UDS protocol.
- ☑ Example for developing security monitoring strategies for an automotive communication protocol.
- ☑ VSOC detection scenarios: End-to-end monitoring strategies to detect the occurrence of higher-level attack techniques based on low-level security events.
- ☑ Guidance for vehicle-side logging and backend-side log processing in a VSOC.

Outlook:

- ☐ Experimental evaluation with real vehicles
- ☐ Monitoring scenarios for other automotive use cases (beyond UDS)

Thank you

YEKTA IT ETAS UNIVERSITÄT PASSAU



Contact

Ali Recai Yekta

ali@yekta-it.de

Yekta IT GmbH

www.yekta-it.de