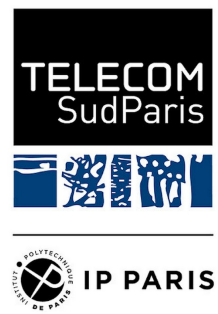
Systematic Risk Analysis of Multi-Stage Attacks in Zonal Automotive E/E Architectures

Ramakrishnan PITCHAIMANI Sébastien CANARD
Badis HAMMI Aurel Sorin SPORNIC

The 23rd IEEE International Symposium on Network Computing and Applications, Lisbon, Portugal.
5-7 November, 2025



Plan

Motivation

Architecture evolution

- **Shift:** Distributed → centralized
- **Enabler:** HPC + Ethernet backbone [1]
- **Effect:** Software Defined Vehicles [2]
- **Consequence:** Broader attack surface [3]

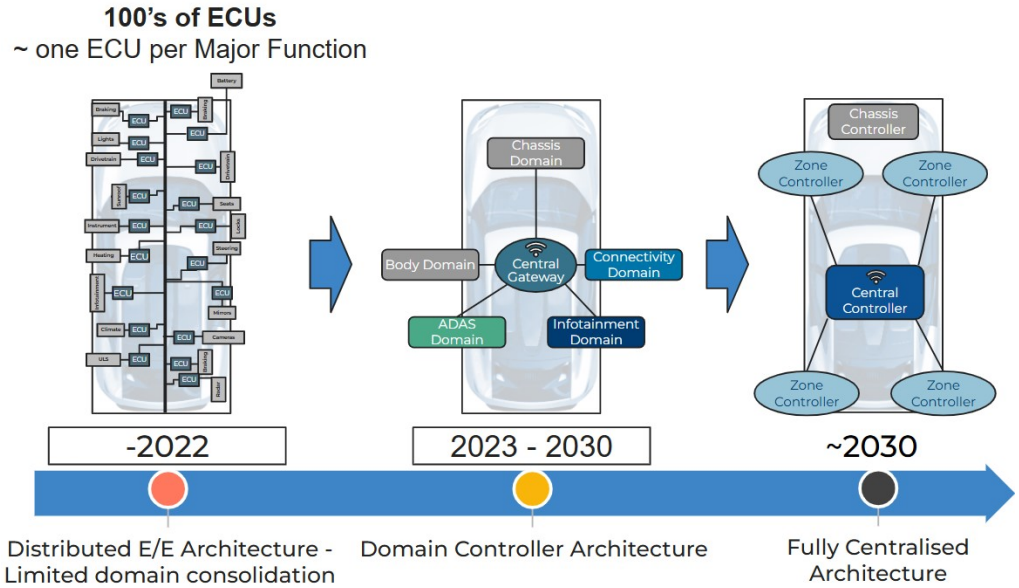


Figure: Shift to centralized zonal systems

Takeaway

Security perimeter has shifted from hardened ECUs to the internal network.

Multistage Attack

- Chained actions that escalate control over time.
- Multiple vulnerabilities across systems and layers.
- Steps often look benign alone — risk is cumulative.
- Nissan Leaf (2025 Black Hat demonstration) — remote infotainment compromise → lateral move to vehicle network [4].

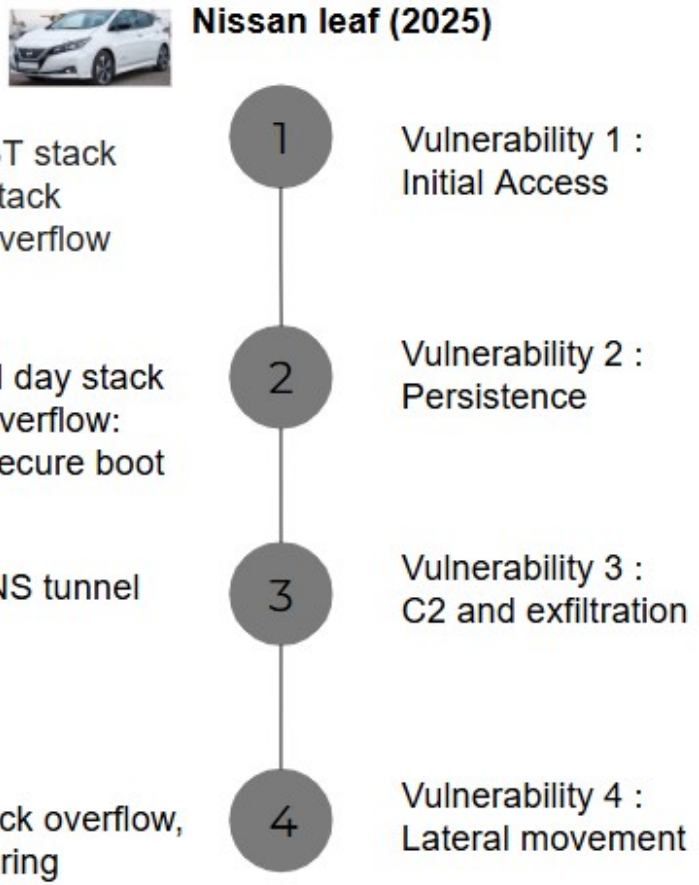


Illustration: chained actions → lateral

Scientific Problem

Limitations of Current Threat Analysis Frameworks

- Existing frameworks (e.g., EVITA [5], HEAVENS v2 [6]) focus on distributed CAN-based systems.
- Few incorporate multi-stage attack models[7] [8].
- Limited research on centralized architectures, lacking systematic or mature methodologies [9].
- No standardized mapping to known adversarial behaviors (e.g., MITRE ATT&CK, Automotive Threat Matrix (ATM) [10]).

Takeaway

Lack of a comprehensive, standardized framework for modeling and mitigating multi-stage cyber-attacks in automotive architectures.

Research Contributions

Key Contributions

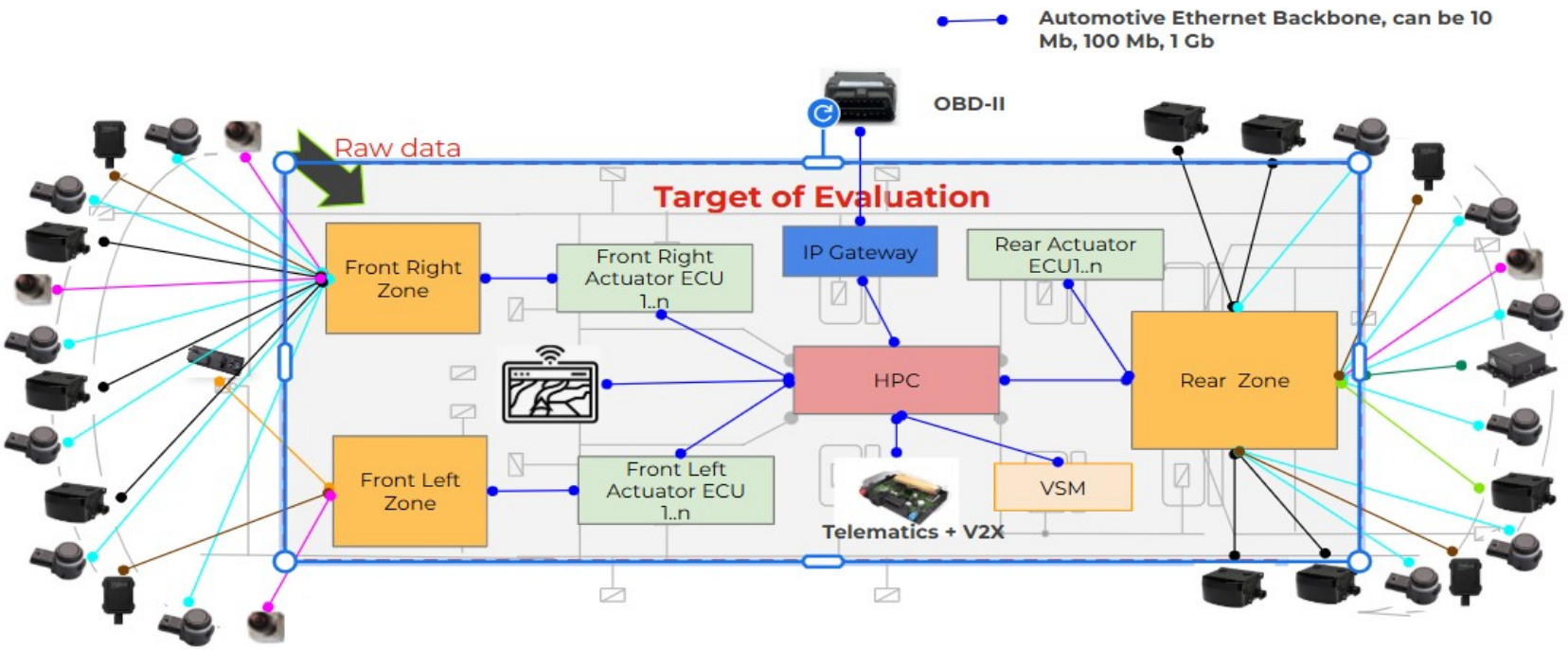
- **ISO 21434 [11] + ATM Integration [10]:** Adds standard adversary behavior to risk assessment process
- **UML-Based Attack Modeling:** Models multistage attack chains for better defense
- **Zonal E/E Architecture Application:** Targeted risk management in zonal systems
- **Path-based Detection Framework:** Correlation defense through attack path analysis

A risk analysis-based methodology

Methodological approach

- **Reference Architecture:** Define architecture, functionalities and data flow
- **Scope Identification (TOE):** Define system boundaries and assets
- **Damage Scenarios:** Identify potential risks
- **Threat Analysis (STRIDE [12] + ATM):** Link threats to attacker techniques
- **UML Modeling:** Model dynamic attack evolution and kill chains
- **Feasibility & Risk Calculation:** Estimate multi-stage attack feasibility and risk
- **Remediation:** Derive defense strategies based on kill chain progression

Derived Architecture (Zonal)



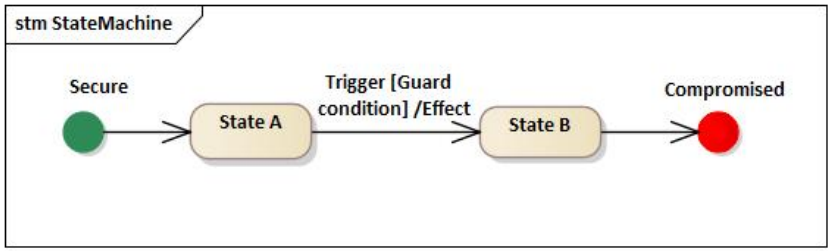
Summary

3 Zonal Controllers (ZCs) + central HPC over Ethernet backbone.
ECUs: Telematics, Infotainment, IP Gateway, Vehicle Security Master (VSM).

State Machine Modeling

UML Modeling of Multistage attacks

- **State**: Component security posture (e.g., “Modem compromised”).
- **Transition**: Adversary action on an asset (ATM [10])
- **Guard**: Pre-conditions (CWE, vehicle state).
- **Effect**: Privilege gain or impact (asset compromise).



Novelty

Asset compromise as UML transitions, dynamic and traceable to TARA

Feasibility & Risk Computation

Table: Feasibility (**Proprietary values**)

Feasibility	**Threat**
0-13	High
14-19	Medium
20-24	Low
$\geq$25	Very Low

Table: Risk Matrix

Feasibility/Impact	Negligible	Moderate	Major	Severe
High	1	3	4	5
Medium	1	2	3	4
Low	1	2	3	3
Very Low	1	1	2	2

Feasibility

Feasibility per step = f(time + knowledge + expertise + opportunity + equipment)

Path Feasibility and Risk

$$\text{Attack feasibility} = \frac{1}{N}\sum \text{step scores}$$

Risk = f(feasibility and end user impact)

Security Risk Assessment

Scope and Analysis

- **100+ assets**: Data, functional, and physical components analyzed.
- **138 damage scenarios**: Covering safety, financial, operational, and privacy impacts.
- **297 threats**: Includes both asset-targeted and 25+ multi-asset kill chains modeled in UML.
- Identified distinction between **vehicle-wide attacks** and **localized ECU attacks**.

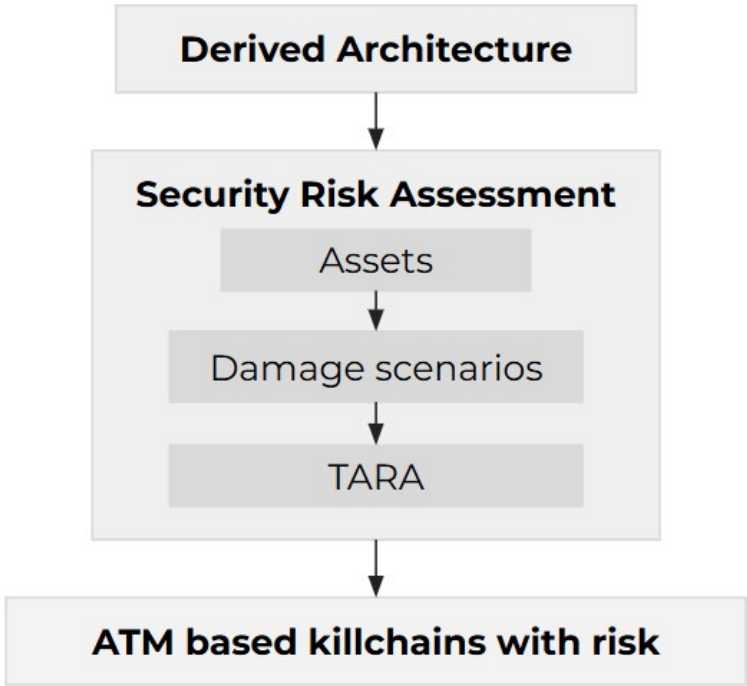


Illustration: ISO 21434 risk assessment process

Case Study - Remote Telematics Attack

Kill-chain Stages

- **Stage 1:** Exploit `T.TELE` radio port → payload execution.
- **Stage 2:** Privilege escalation (Linux → AUTOSAR).
- **Stage 3:** Lateral movement via SOME/IP → Zonal Controller (ZC).
- **Stage 4:** Impact — malicious braking command.

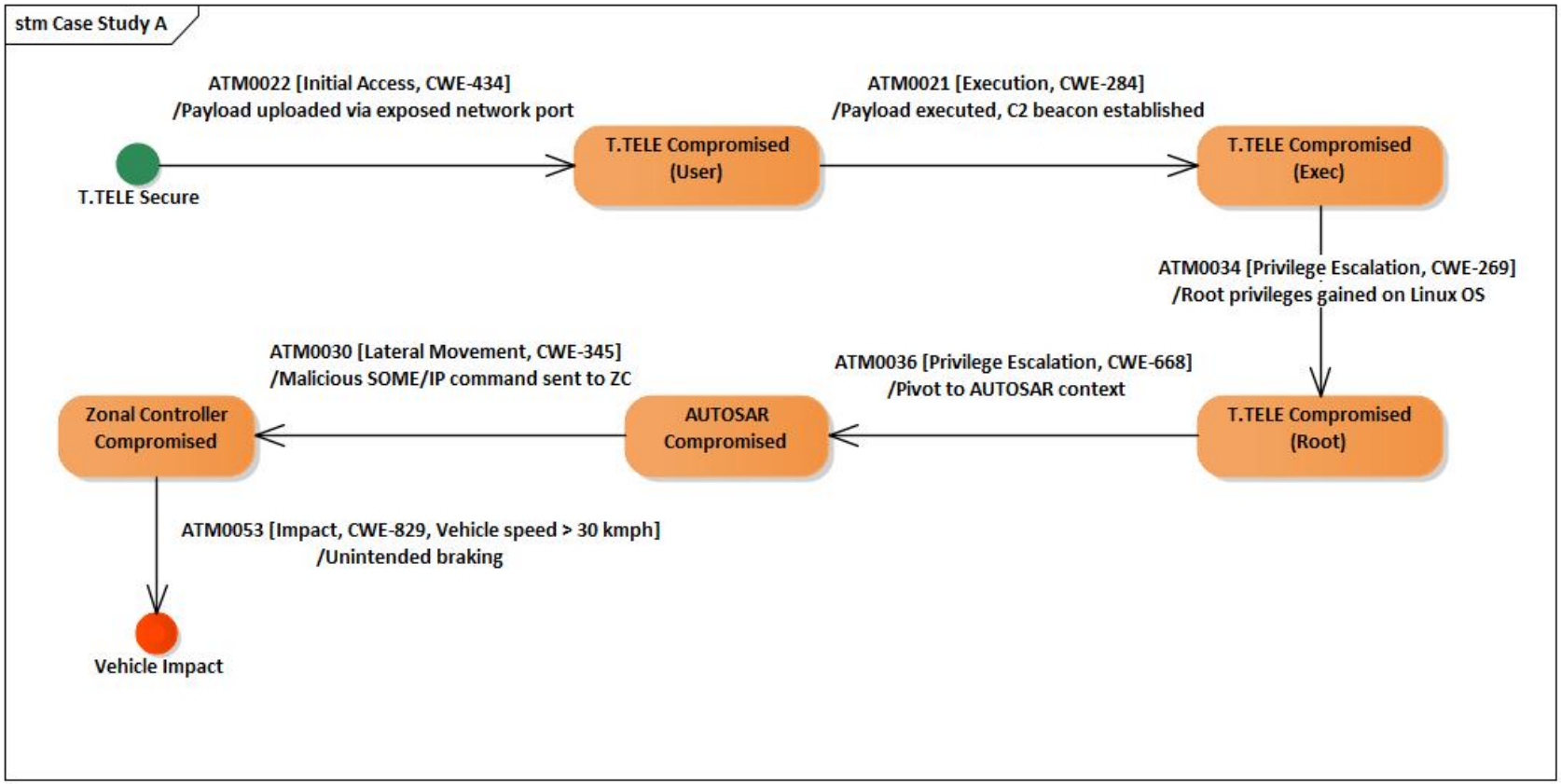
Risk Summary

Avg. difficulty: **15.7 (Medium)** → **Overall risk: High (4/4/4/4)**.

Main takeaway

Shared middleware (SOME/IP) collapses isolation boundaries — enables remote telematics to pivot to safety-critical zones.

Remote Telematics Attack - Kill chain



Kill-chain UML

Critical Inferences 1 & 2

Propagation Geometry

- **Distributed:** Linear bus segmentation limits spread.
- **Zonal:** Ethernet interlinks enable multi-path movement.
- **Inference:** Propagation topology shifts from isolated chains → interconnected graphs.

Risk Centralization

- **ZCs/HPCs:** Concentrate multiple functions.
- **Single points of failure:** A centralized structure increases risk.

Takeaway

Zonal systems enable broader attack spread and centralize risk.

Critical Inferences 3 & 4

Cross-Domain Impact Coupling

- **Shared compute and data paths:** Cascading effects across safety and non-safety domains.
- **Inference:** Cross-domain coupling amplifies impact.

Feasibility & Detection Shift

- Avg. attack difficulty: **Distributed** = 22–24, **Zonal** = 15–18.
- Local anomaly detection insufficient; requires cross-zone correlation.

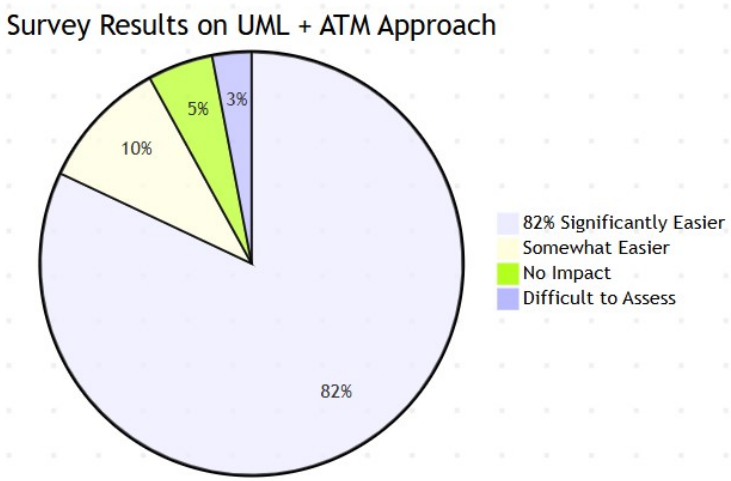
Takeaway

Zonal architectures don't introduce new attacks, but make them easier and more impactful.

Validation & Expert Feedback

Survey of 17 Automotive Cyber Professionals

- **82%** found UML + ATM approach "significantly easier" for attack-path validation.
- Highlighted benefits:
  - Clarity of multi-stage logic.
  - Better communication to non-experts.
  - Reusable analysis models.



AKCC Framework Overview

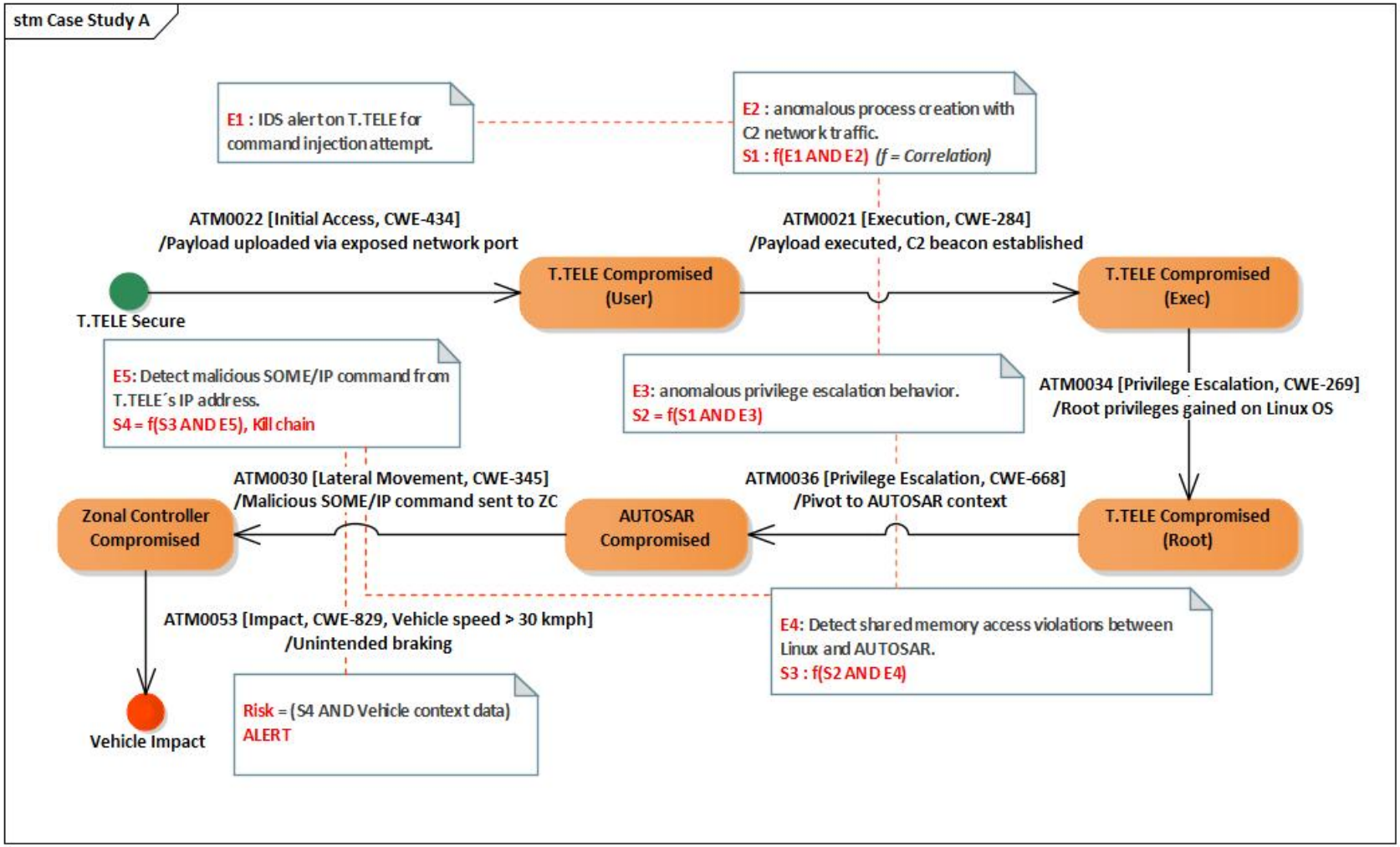
AKCC Framework

- **Automotive Kill Chain Correlation**
- AKCC detects multi-stage and lateral movement attacks across vehicle zones.
- **Key features:** Path correlation, risk analysis, early attack path detection.
- **Goal:** Identify high-risk attack paths early to prevent escalation.

AKCC Flow (UML)

- **State**: Tracks component security posture to assess attack paths.
- **Transition**: Event to monitor, such as an adversary's action
- **Guard**: Context for correlation (preconditions)
- **Effect**: Measures impact (e.g., asset compromise)
- AKCC correlates to trace attack progression

Remote Telematics Attack - AKCC



Conclusions & Future Work

Conclusions

- **Zonal E/E architectures:** Increase interconnectivity and risk centralization.
- **Integration of ISO 21434 + ATM + UML:** Provides systematic kill-chain analysis.
- **AKCC:** Delivers stateful multi-zone detection.

Future Work

- **AKCC framework validation:** Implementation and validation in NXP secure gateway.
- **Automated UML generation:** Enhance analysis efficiency.
- **AI-enhanced correlation:** Improve real-time detection and response.

[1] Ondrej Burkacky et al. *Getting ready for next-generation E/E architecture with zonal compute*. Online. Semiconductors Practice. June 2023. URL: https://www.mckinsey.com/industries/semiconductors/our-insights/getting-ready-for-next-generation-ee-architecture-with-zonal-compute.

[2] Meindert van den Beld. *How Zonal E/E Architectures with Ethernet Are Enabling Software-Defined Vehicles*. Feb. 2023. URL: https://www.nxp.com/company/about-nxp/smarter-world-blog/BL-HOW-ZONAL-EE-ARCHITECTURES.

[3] Florian Sagstetter et al. "Security challenges in automotive hardware/software architecture design". In: *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 2013, pp. 458–463. DOI: 10.7873/DATE.2013.102.

[4] Dmitry Evdokimov. *Remote Exploitation of Nissan Leaf*. Tech. rep. Singapore: Black Hat Asia, 2025. URL:

https://i.blackhat.com/Asia-25/Asia-25-Evdokimov-Remote-Exploitation-of-Nissan-Leaf.pdf.

[5] EVITA Project. *EVITA: An Evaluation and Validation Framework for Automotive Security*. https://www.evita-project.org/deliverables.html. Accessed: Date. Year Accessed.

[6] Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. "Proposing HEAVENS 2.0 – an automotive risk assessment model". In: *Proceedings of the 5th ACM Computer Science in Cars Symposium*. CSCS '21. Ingolstadt, Germany: Association for Computing Machinery, 2021. ISBN: 9781450391399. DOI: 10.1145/3488904.3493378. URL: https://doi.org/10.1145/3488904.3493378.

[7] Shah Khalid Khan et al. "Cybersecurity framework for connected and automated vehicles: A modelling perspective". In: *Transport Policy* 162 (2025), pp. 47–64. ISSN: 0967-070X. DOI: https://doi.org/10.1016/j.tranpol.2024.11.019.

URL: https://www.sciencedirect.com/science/article/pii/S0967070X24003561.

[8] Sunniva F. Meyer, Rune Elvik, and Espen Johnsson. "Risk analysis for forecasting cyberattacks against connected and autonomous vehicles". In: *Journal of Transportation Security* 14.3 (Dec. 2021), pp. 227–247. ISSN: 1938-775X. DOI: 10.1007/s12198-021-00236-4. URL: https://doi.org/10.1007/s12198-021-00236-4.

[9] K. Appajosyula. *Ethernet-Based IDS for Zonal Architecture*. SAE Technical Paper 2024-28-0121. SAE International, 2024. DOI: 10.4271/2024-28-0121.

[10] Automotive Information Sharing and Analysis Center. *Automotive Threat Matrix*. Apr. 2025. URL: https://atm.automotiveisac.com/home.

[11] International Organization for Standardization and Society of Automotive Engineers. *ISO/SAE 21434:2021, Road vehicles —*

Cybersecurity engineering. Aug. 2021. URL: https://www.iso.org/standard/70918.html.

[12] Microsoft Corporation. *STRIDE Threat Model*. Microsoft Security Development Lifecycle (SDL). Developed by Loren Kohnfelder and Praerit Garg; Accessed: 2025-08-27. 1999. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool.