IEEE Advancing Technology for Humanity

The 34th IEEE International Symposium on Industrial Electronics

June 20-23, 2025 | Toronto, Canada

IEEE Industrial Electronics Society

Cybersecurity for Intelligent Transportation Systems: Foundations, Trends, and Opportunities

Max Mauro Dias Santos

Federal Technological University of Paraná – Ponta Grossa

Paraná – Brazil

Friday, June 20, 3:45 PM – 5:15 PM

Room 302

INSTRUCTOR

Max Mauro Dias Santos, PhD

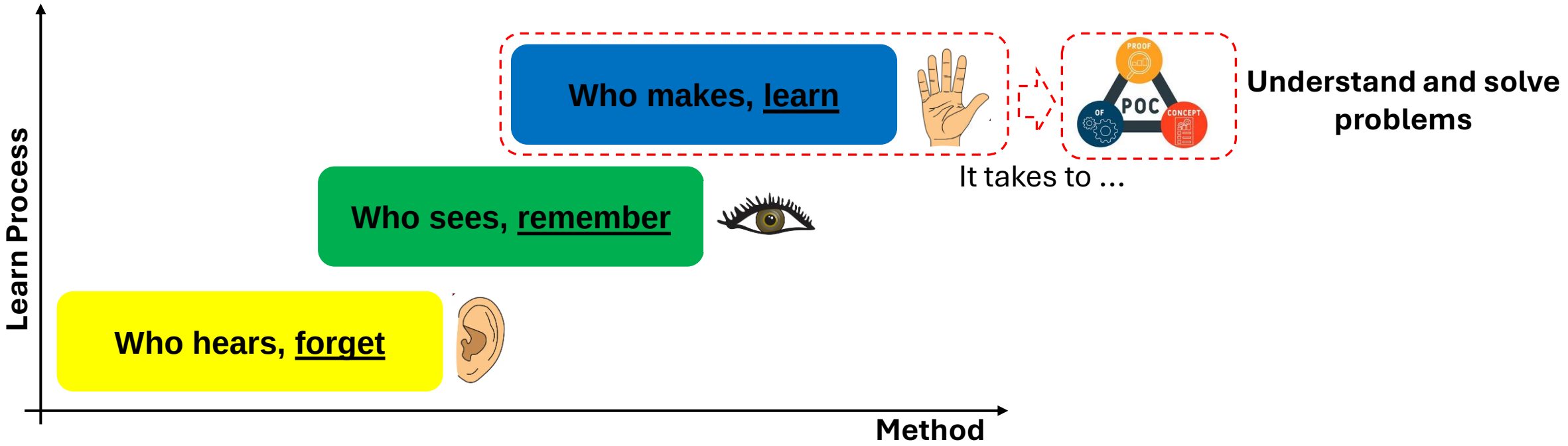
Department of Electronics
Federal Technological University of Paraná – Ponta Grossa
Paraná - Brazil

maxsantos@utfpr.edu.br

Responsabilities

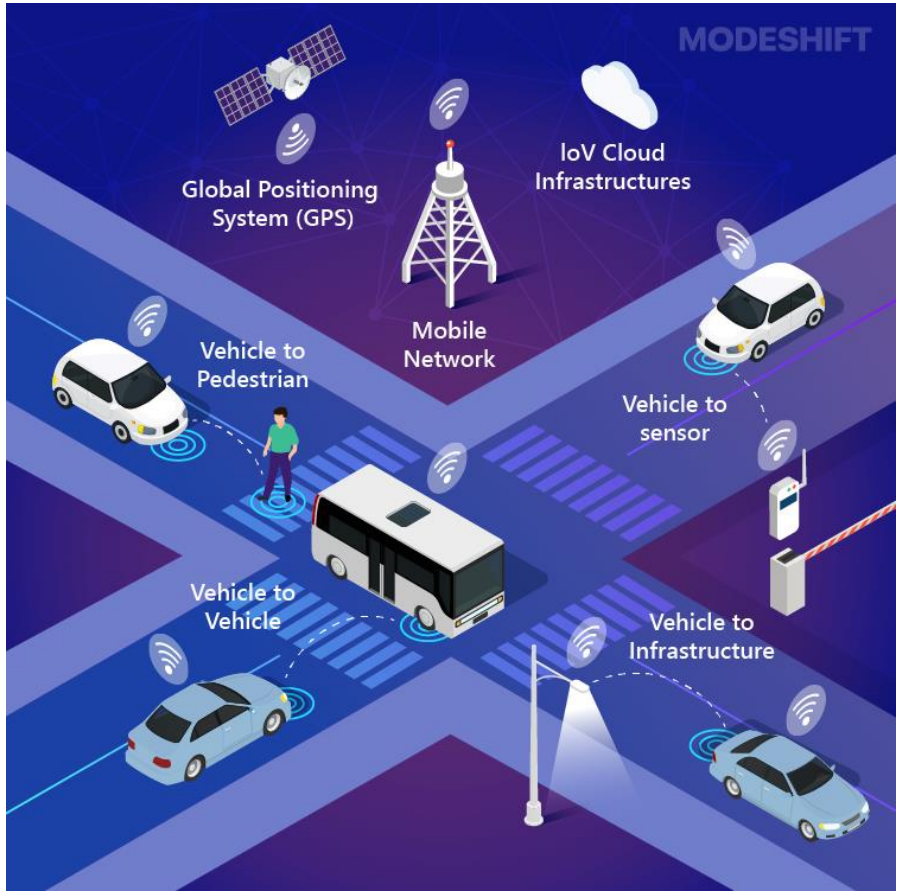
- **Associate Professor** – Teaching
- **Department Chair** – Management
- **Lab Director** – Research

We work based in PoC. Why?



SUMMARY

Transportation



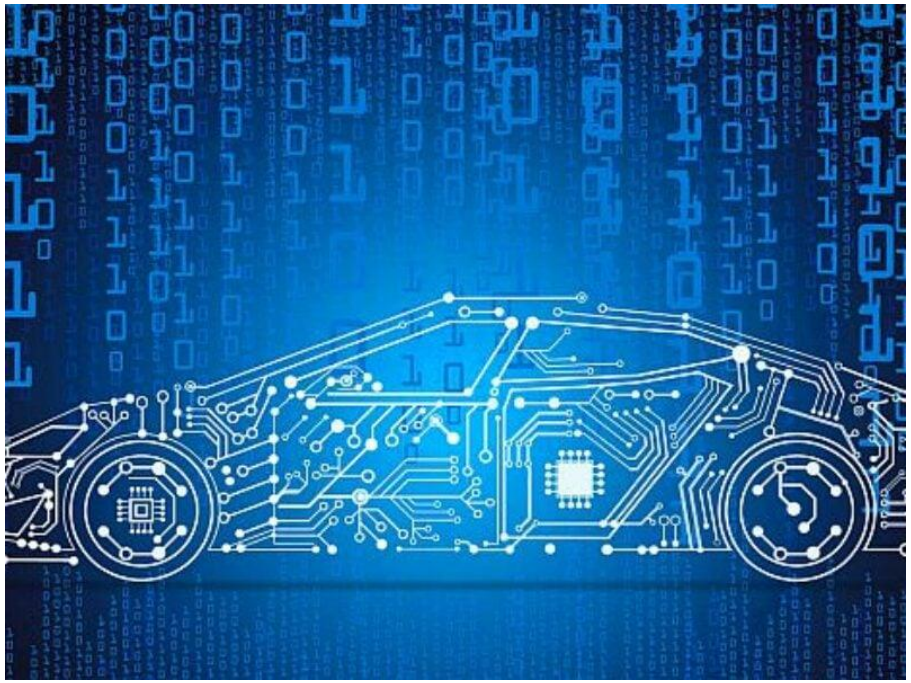
Intelligent

System

ITS

1. INTRODUCTION

Automotive Cybersecurity refers to use of technologies, processes, policies, and best practices to protect vehicle electronic systems, software, communications, and data against malicious attacks, unauthorized access, and manipulations.



1. INTRODUCTION

Automotive Cybersecurity involves safeguarding the entire automotive ecosystem, which includes:

a) Electronic Control Units (ECUs), complex hardware, and diagnostic interface
b) In-vehicle networks and communication buses (e.g., CAN, LIN, FlexRay, Automotive Ethernet…)
c) External interfaces (e.g., Bluetooth, G4/G5, Wi-Fi, V2X)
d) Cloud backends and mobile applications connected to the vehicle
e) Over-the-Air (OTA) update infrastructure

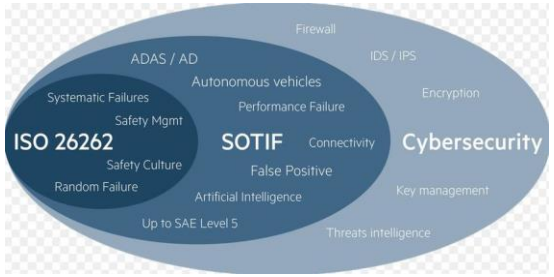
It focuses on detecting, preventing, and responding to attacks that could lead to:

a) Malicious attacks and unauthorized vehicle control
b) Data theft or privacy invasion (EV and EVSE)
c) Disruption of Advanced Driver Assistance System or Autonomous Driving features
d) Physical safety risks to passengers and surrounding traffic

1. INTRODUCTION

We experience nowadays cyber attacks on our devices like personal computer, mobile phone, and so on.

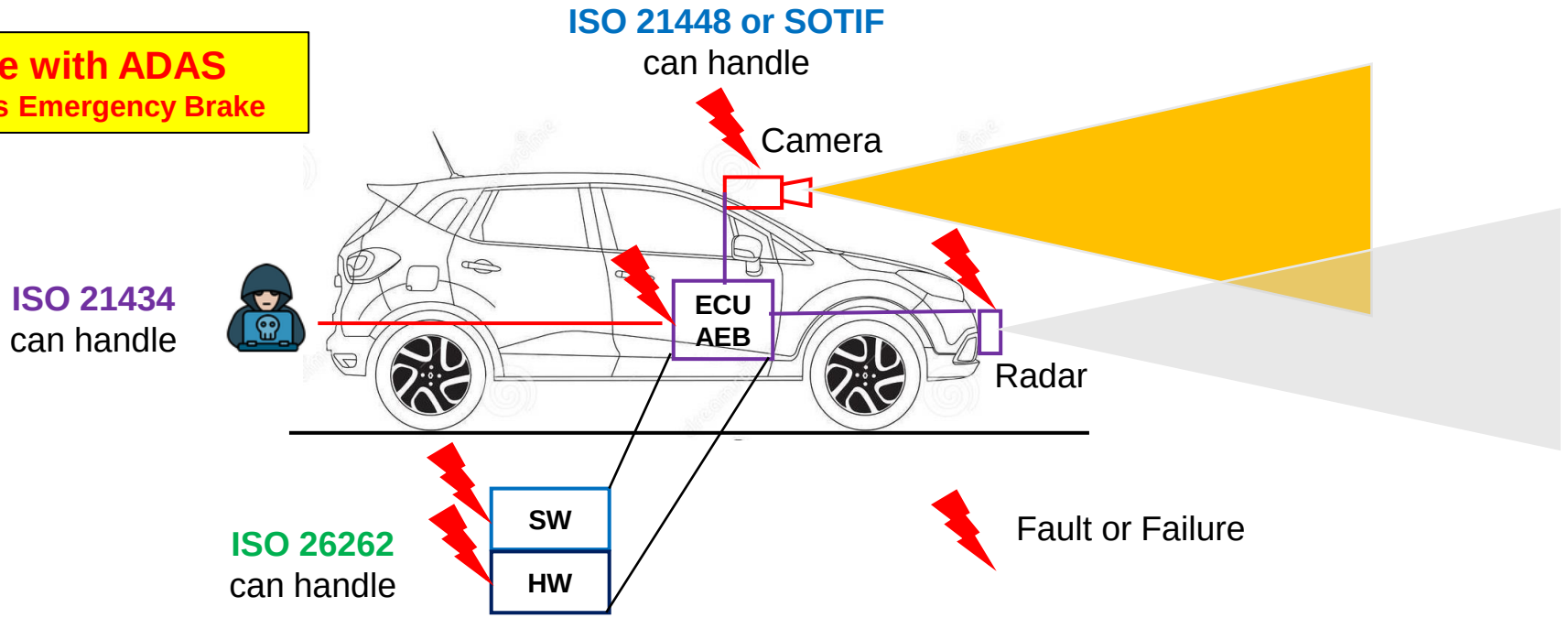
2. MOTIVATION



Fault	Type	Standard
HW & SW	Faults on IC wire or stack overload	ISO 26262
Functionality	Fails to detect a child crossing in poor lighting	ISO 21448
Cyber Attacks	Malicious attack or unautorized access	ISO 21434

Mitigation

Road Vehicle with ADAS
AEB – Autonomous Emergency Brake



2. Motivation

IEEE ISIE 2025

ATM

Money 

Cash withdrawal and banking services

≈

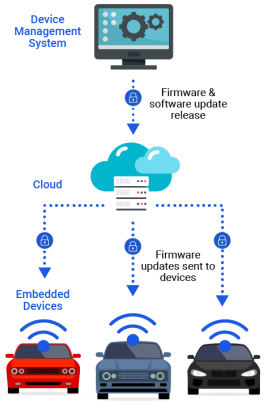
EVSE

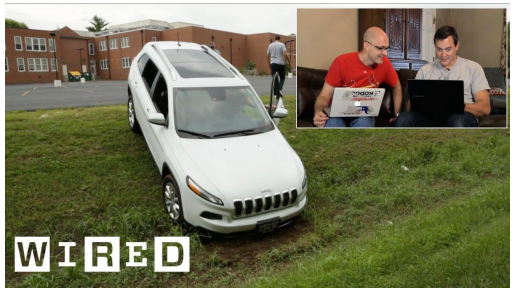
Power 

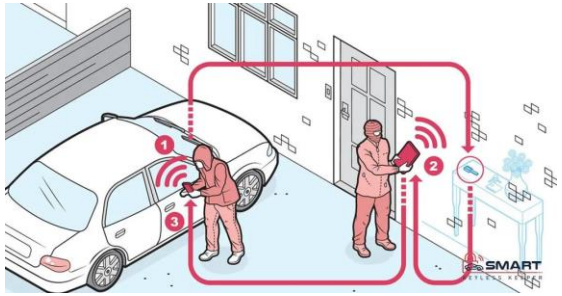
Electric vehicle charging and payment

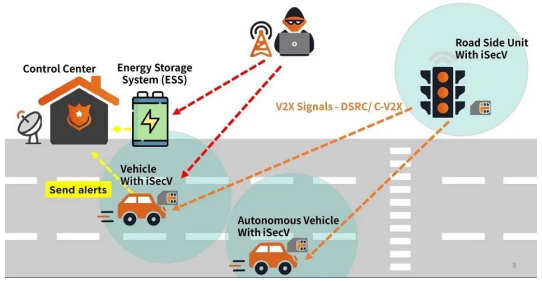
3. Real-World Problems

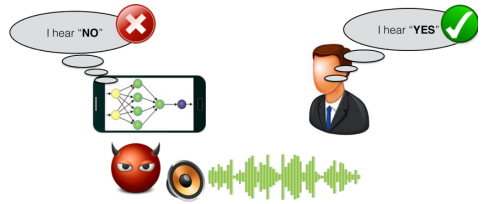
1. CAN Bus Spoofing and Injection Attacks
2. Over-the-Air (OTA) Software Update Vulnerabilities
3. Keyless Entry and Relay Attacks
4. V2X Communication Vulnerabilities (Fake Traffic Messages)
5. AI-Based Perception Systems under Adversarial Attacks











Problem → **Example** → **Mitigation**

3.1. CAN Bus Spoofing and Injection Attacks

- **Problem:**

The CAN Bus, still widely used in most vehicles, but the lack of inherent message **authentication** and **encryption**, make it vulnerable to spoofing, replay, and injection attacks.

- **Example:**

In recent security demonstrations (e.g., 2019 Tesla CAN Bus Hack and other research studies on Jeep and BMW), researchers successfully injected spoofed CAN messages to control vehicle functions like braking and steering.

- **Mitigation Strategies:**

Implement CAN Intrusion Detection Systems (IDS) with anomaly and behavior-based monitoring.

Use CAN message authentication protocols (e.g., SecOC from AUTOSAR).

Transition towards CAN-FD with enhanced security extensions or move to Automotive Ethernet where possible.

3.2. Over-the-Air (OTA) Software Update Vulnerability

- **Problem:**

Vehicles with OTA capabilities are vulnerable to Man-in-the-Middle (MitM) and firmware tampering attacks, where attackers may inject malicious code during update processes.

- **Example:**

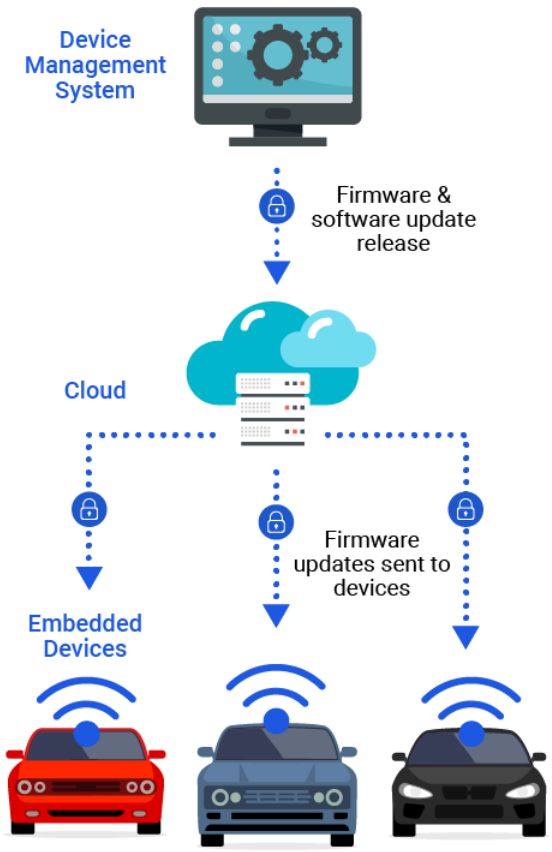
In 2021, researchers from Karamba Security highlighted vulnerabilities in OTA pipelines that could lead to remote exploitation in several OEMs if not properly secured.

- **Mitigation Strategies:**

Enforce End-to-End Cryptographic Signing and Verification of OTA packages.

Implement protection, ensuring vehicles only accept newer and verified firmware.

Deploy secure boot mechanisms.



3.3. Keyless Entry and Relay Attacks

- **Problem:**

Keyless entry systems are widely exploited through relay attacks, where attackers extend the communication range between the key fob and the vehicle.

- **Example:**

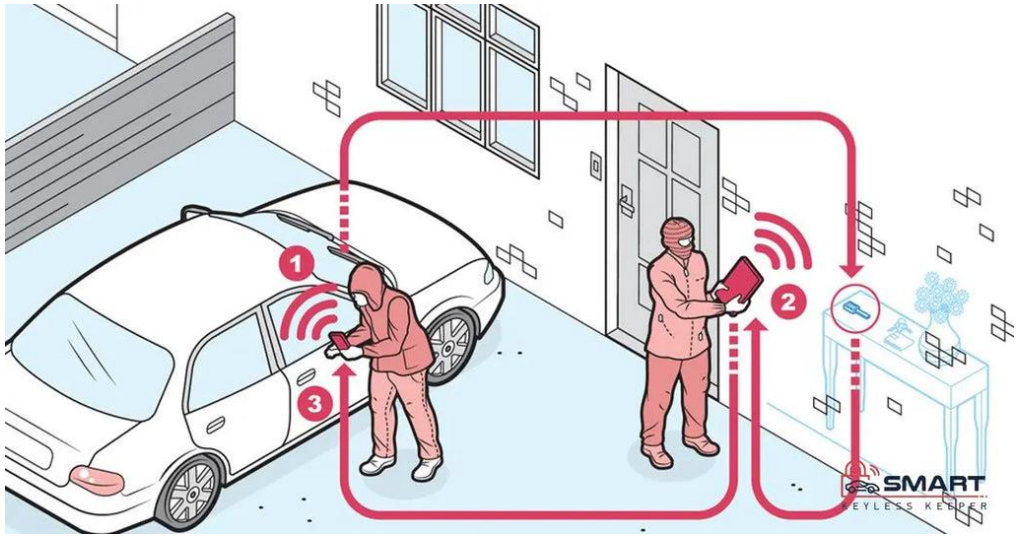
The "Relay Attack on Tesla Model S" (2020) and similar attacks on BMW, Audi, and Mercedes showed how criminals could open and start vehicles without physical access to the key.

- **Mitigation Strategies:**

Use Ultra-Wideband (UWB) technology for distance bounding and precise location verification.

Apply RF signal anomaly detection.

Implement motion sensors in key fobs (disable response when stationary for long periods).



3.4. V2X Communication Vulnerabilities

- **Problem:**

V2X communications (DSRC, C-V2X) open new cyberattack surfaces where fake messages (e.g., false collision warnings, fake traffic congestion alerts) can disrupt traffic safety.

- **Example:**

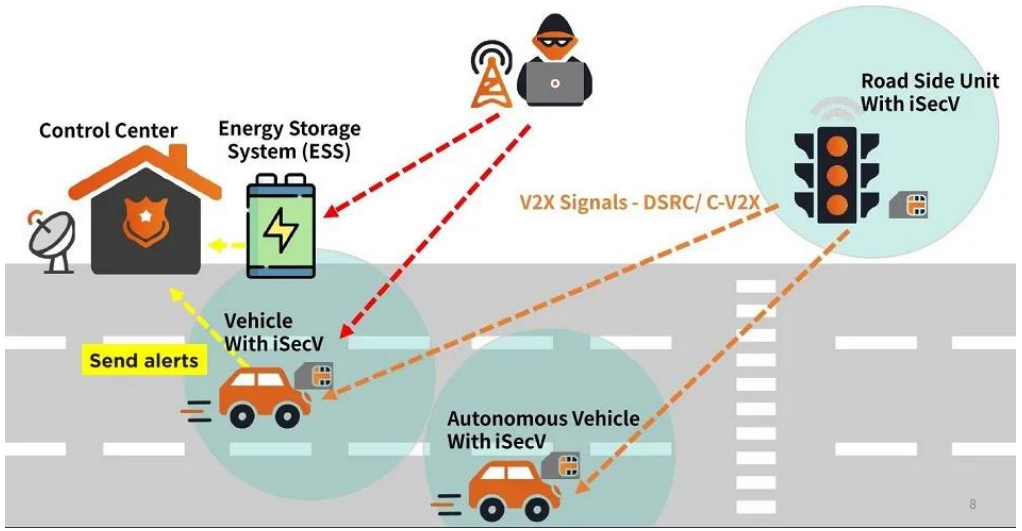
In 2022, researchers showed that malicious V2X broadcasts could force vehicles to apply emergency braking or cause route deviations.

- **Mitigation Strategies:**

Enforce PKI-based authentication and message signing (SCMS for DSRC, 5G-V2X PKI models).

Deploy V2X Intrusion Detection and Anomaly Filtering at the Onboard Unit (OBU) level.

Design robust misbehavior detection algorithms within V2X stacks.



3.5. AI-Based Perception under Adversarial Attacks

- **Problem:**

ADAS and Autonomous Vehicles increasingly rely on AI-based perception systems (e.g., YOLO, CNNs for object detection), making them vulnerable to adversarial perturbations like altered stop signs or lane markings.

- **Example:**

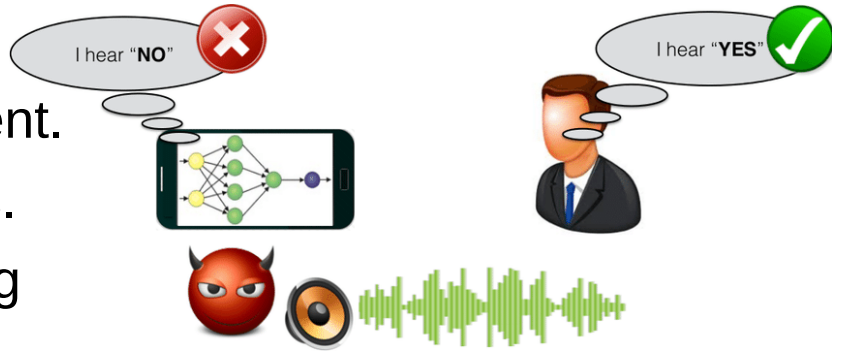
In 2020, academic studies showed that by applying small, imperceptible changes to stop signs (e.g., adversarial stickers), vehicles with AI-based detection systems could misclassify them, leading to safety risks.

- **Mitigation Strategies:**

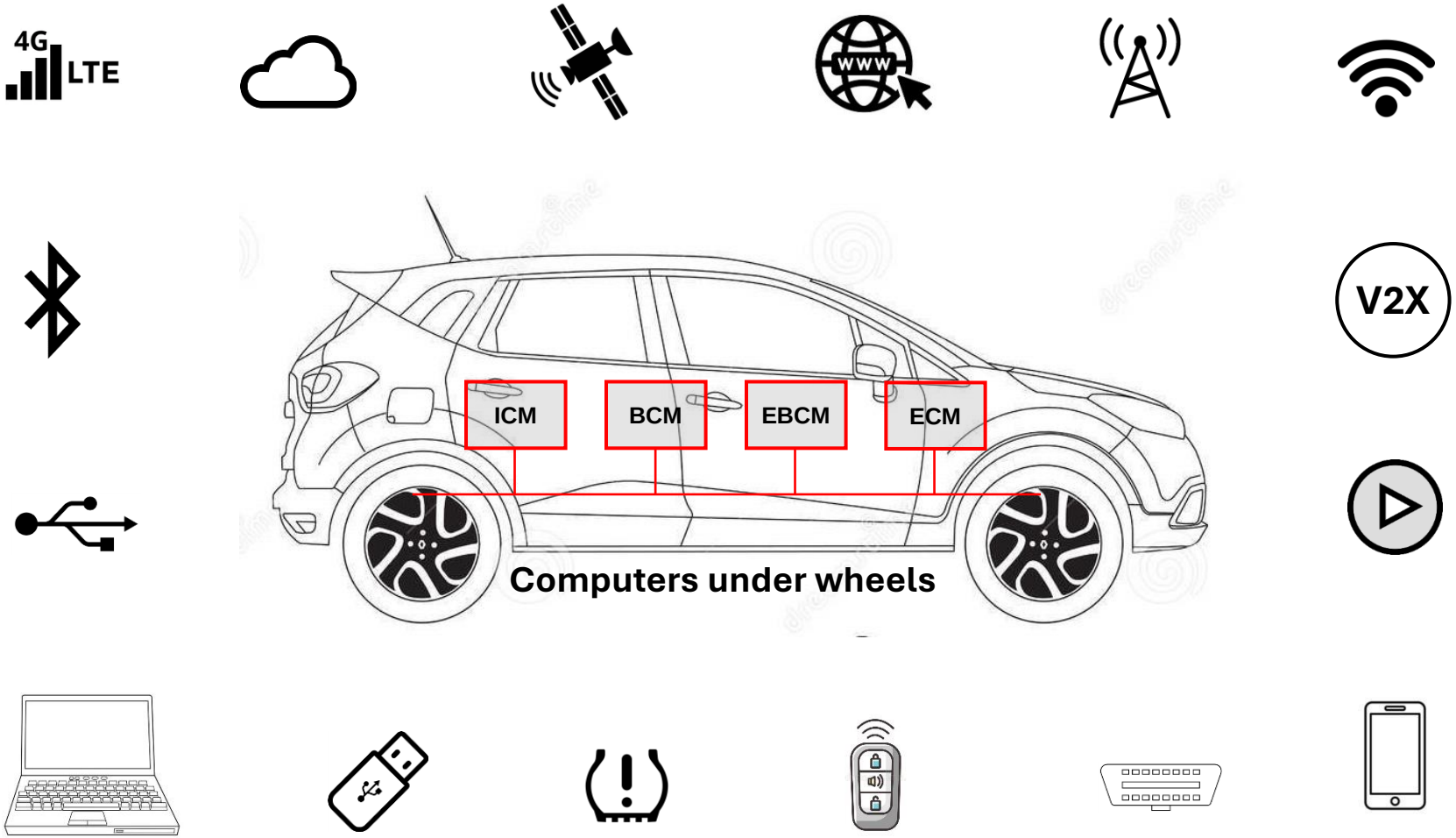
Integrate adversarial training techniques during AI model development.

Use sensor fusion (e.g., Radar + Camera) to cross-check detections.

Implement runtime monitoring and out-of-distribution detection to flag suspicious inputs.



5. Vulnerabilities and Attack Points



5. Vulnerabilities and Attack Points

IEEE ISIE 2025

Vehicle Dashboard

Wifi | LTE | TPMS | OBD | Keyless | USB | Bluetooth

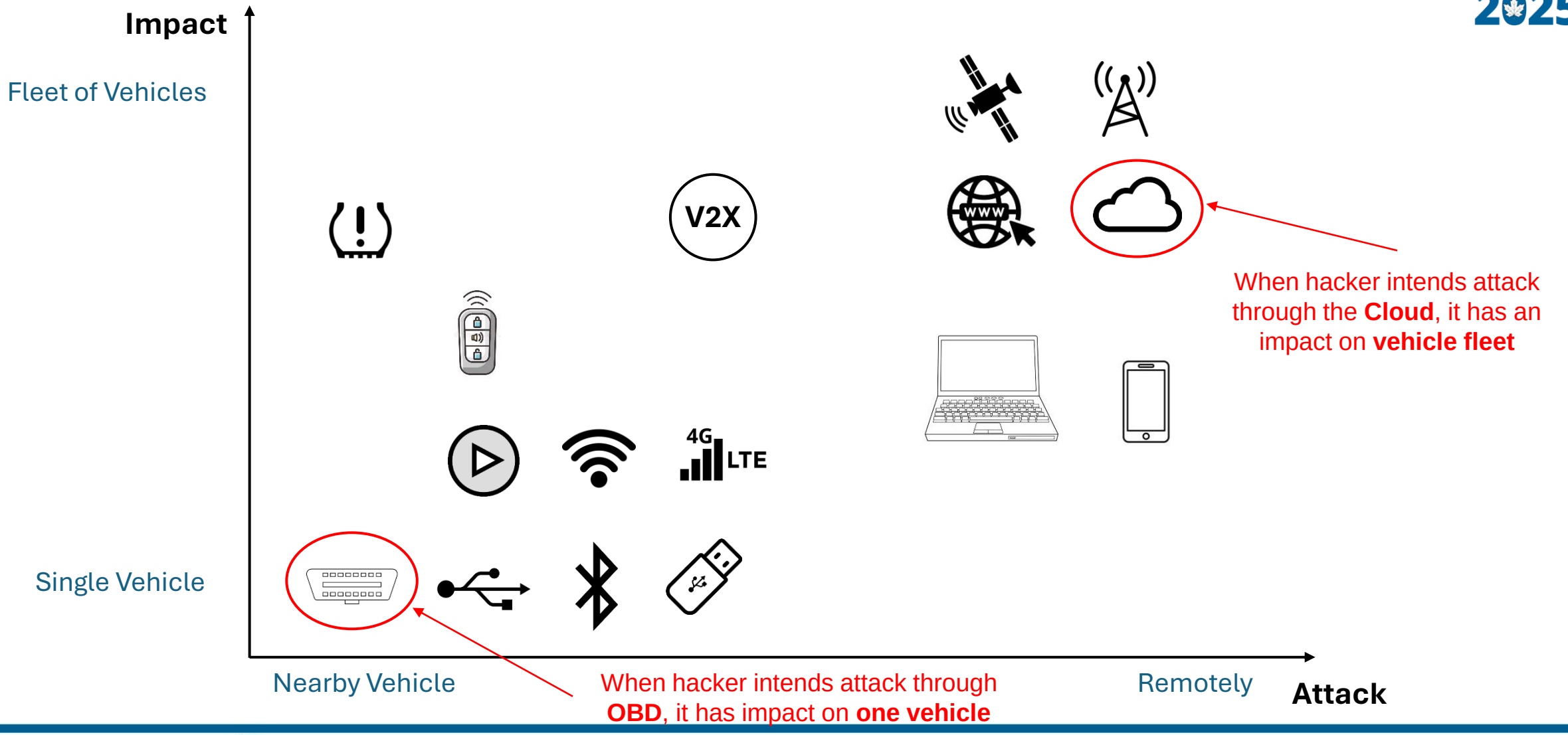
Motivations for hacking

a) Steal vehicle and goods
b) Vehicle control
c) Financial gain
d) Fame
e) Damage vehicle

Methods of hacking

a) Human hacking
b) Stealth malware
c) Unauthorized remote access
d) Insider threats
e) Personal information

5. Vulnerabilities and Attack Points



5. Vulnerabilities and Attack Points

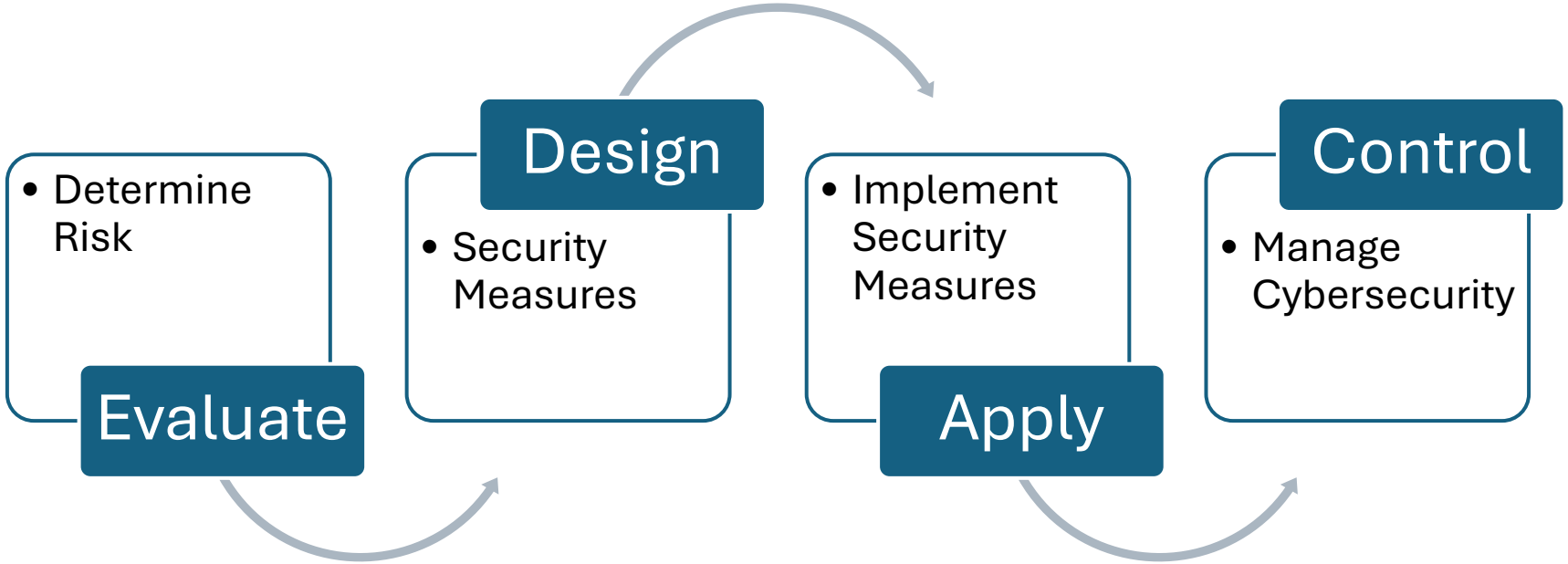
Attack Point	Vulnerability Type	Example Attack
In-Vehicle Networks	Message injection, Spoofing	Remote brake control
Telematics/Infotainment	Remote execution, Pivot attacks	Remote Jeep Hack
Keyless Entry	Relay attacks, Replay	Car theft without key
OTA Systems	MitM, Malicious firmware	ECU updates
V2X	Message spoofing, DoS	Fake emergency alerts
ADAS Sensors	Adversarial ML inputs	Stop sign misclassification
ECU Firmware	Flashing attacks	Engine remapping
OBD-II	Unauthorized access	Airbag disabling

6. Counter Measures

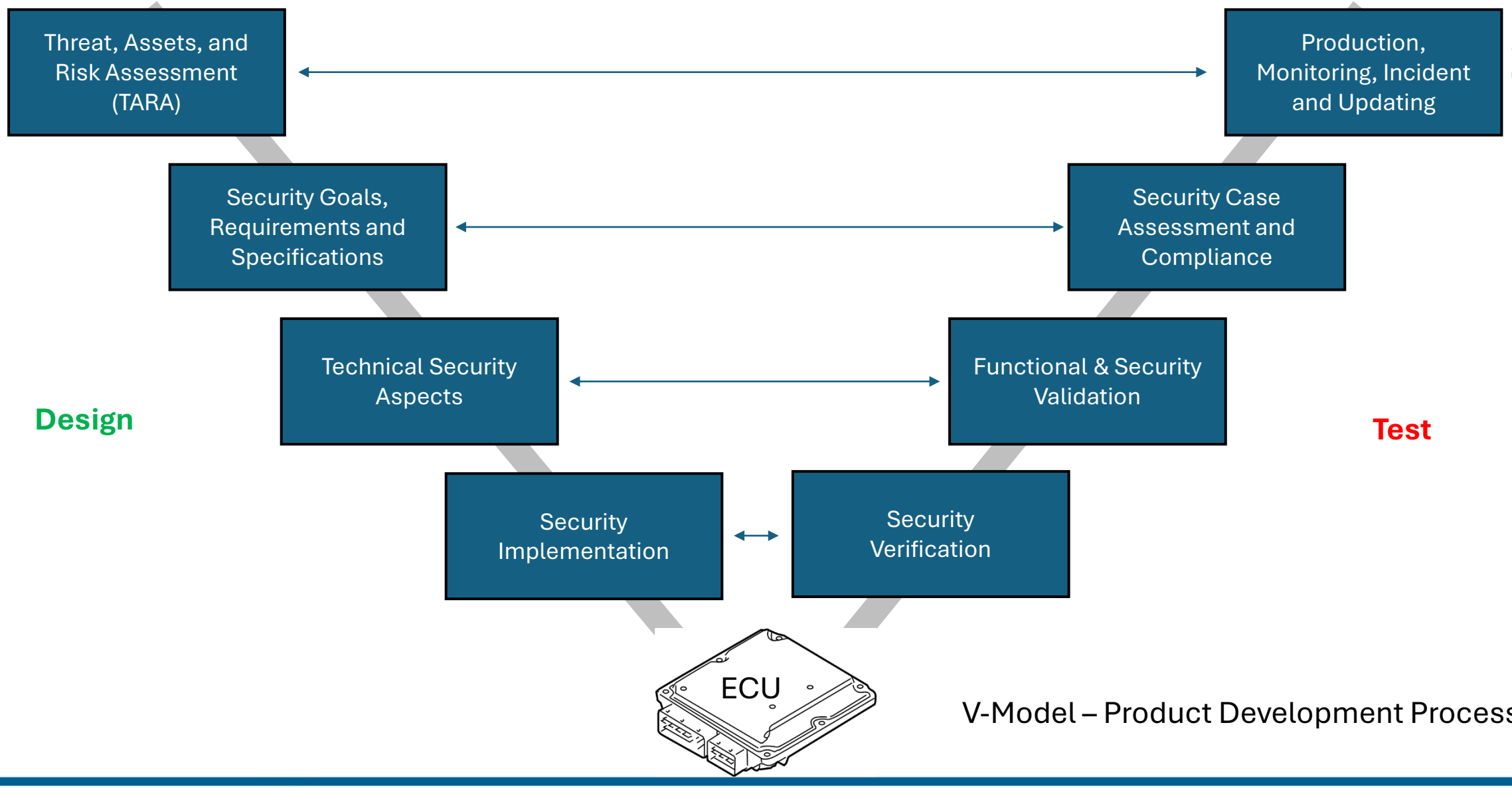
Attack Vector	Common Attack Types	Countermeasures / Defense Strategies
In-Vehicle Network (CAN, FlexRay, Ethernet)	Message spoofing, replay, injection	- Message Authentication (e.g., AUTOSAR SecOC) - Intrusion Detection Systems (IDS)
Telematics & Infotainment Units	Remote code execution, pivot to CAN	- Secure software development (SDL) - Hardened OS and sandboxing and secure OTA
Keyless Entry Systems	Relay attacks, replay attacks	- Ultra-Wideband (UWB) technology - Key fob motion sensors and RF detection
Over-the-Air (OTA) Updates	Man-in-the-Middle (MitM), firmware tampering	- Digital signature verification - Secure boot and rollback protection and encryption
Vehicle-to-Everything (V2X)	Message spoofing, Sybil, DoS	- PKI and digital certificates - Misbehavior Detection Systems (MDS)
ADAS / Autonomous AI Perception	Adversarial inputs, sensor spoofing	- Adversarial training of ML models - Sensor fusion (e.g., camera + radar + LiDAR)
ECU Firmware / Bootloaders	Flashing unauthorized firmware	- Secure boot - ECU-level cryptographic authentication
OBD-II / Diagnostic Interfaces	Unauthorized access, data theft	- Access control and authentication - Time-limited diagnostic sessions
GPS / GNSS Signals	Spoofing, jamming	- GNSS signal authentication (SBAS, RAIM) - Sensor fusion with IMU/map data

7. Methods and Processes

- Cybersecurity does not start and end with cryptography
- Cybersecurity needs to be an integral part of the whole development process
- Standards need to be applied to cybersecurity properties
- Cybersecurity needs to be deployed even after development is finished
- Cybersecurity is essential to protect assets, people and the environment

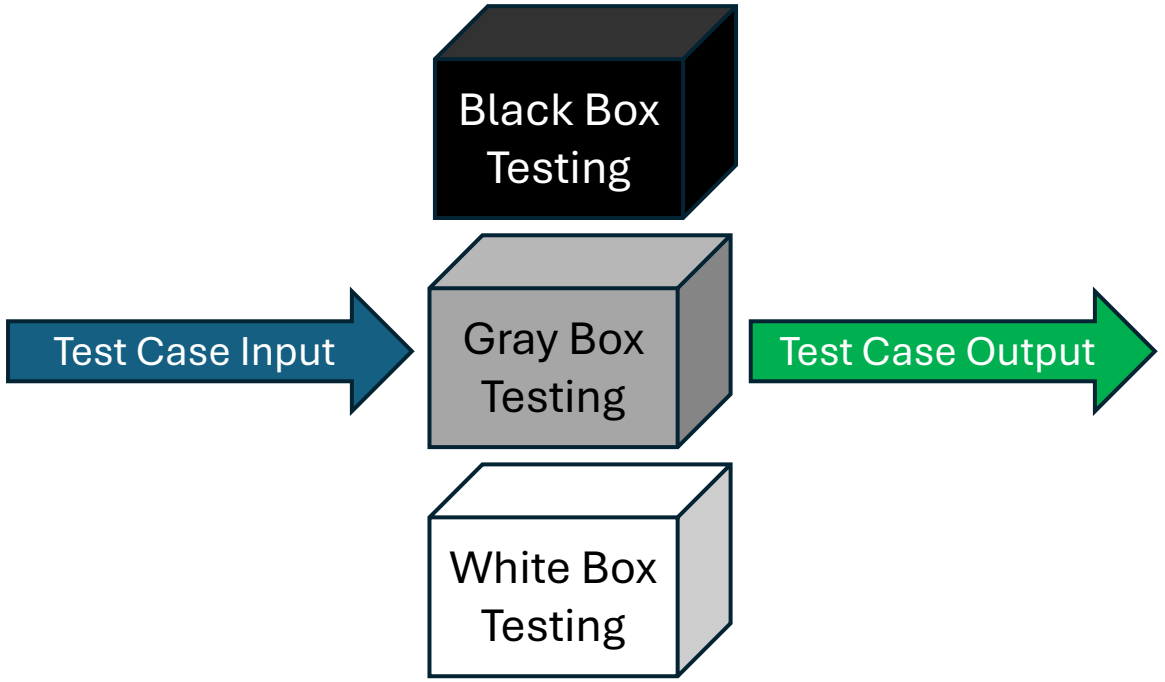


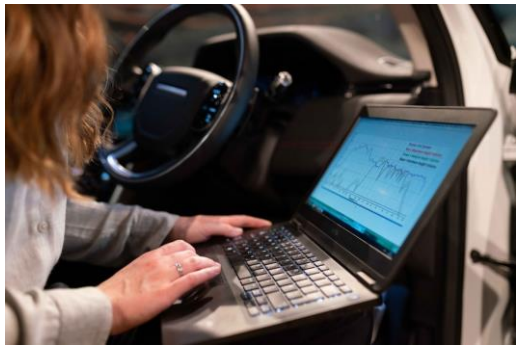
7. Methods and Processes



V-Model – Product Development Process

How to Test Vulnerabilities?





Setup for penetration testing

8. Case Studies

8.1. Jeep Cherokee Hack (2015)

8.2. Stop Sign Adversarial Attack (2020)

8.3. V2X Message Spoofing (2022)

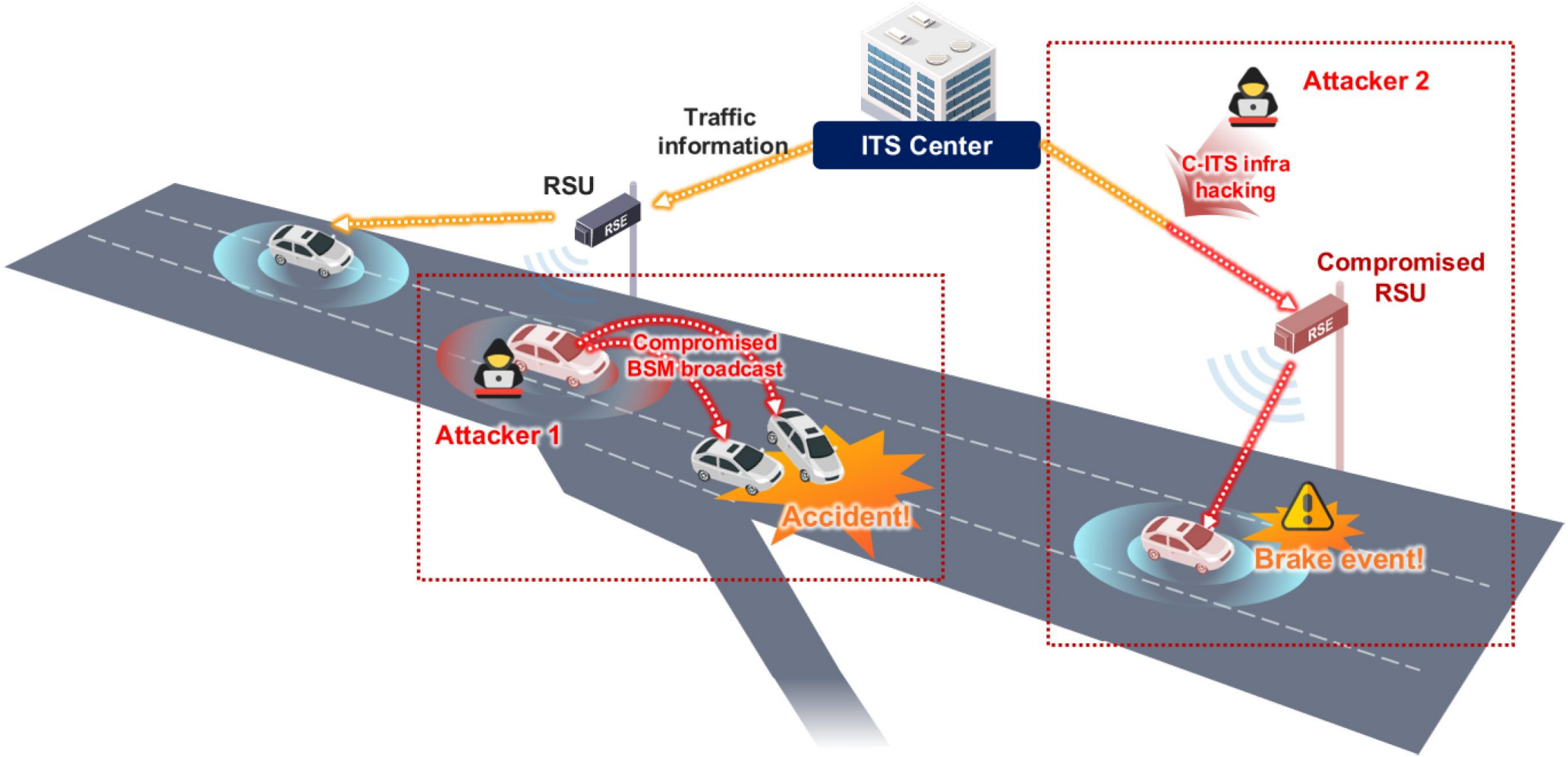
8.4. Kolmogorov-Arnold Network for EV Chargers

8.5. Analysis of The Most Hackable Vehicles

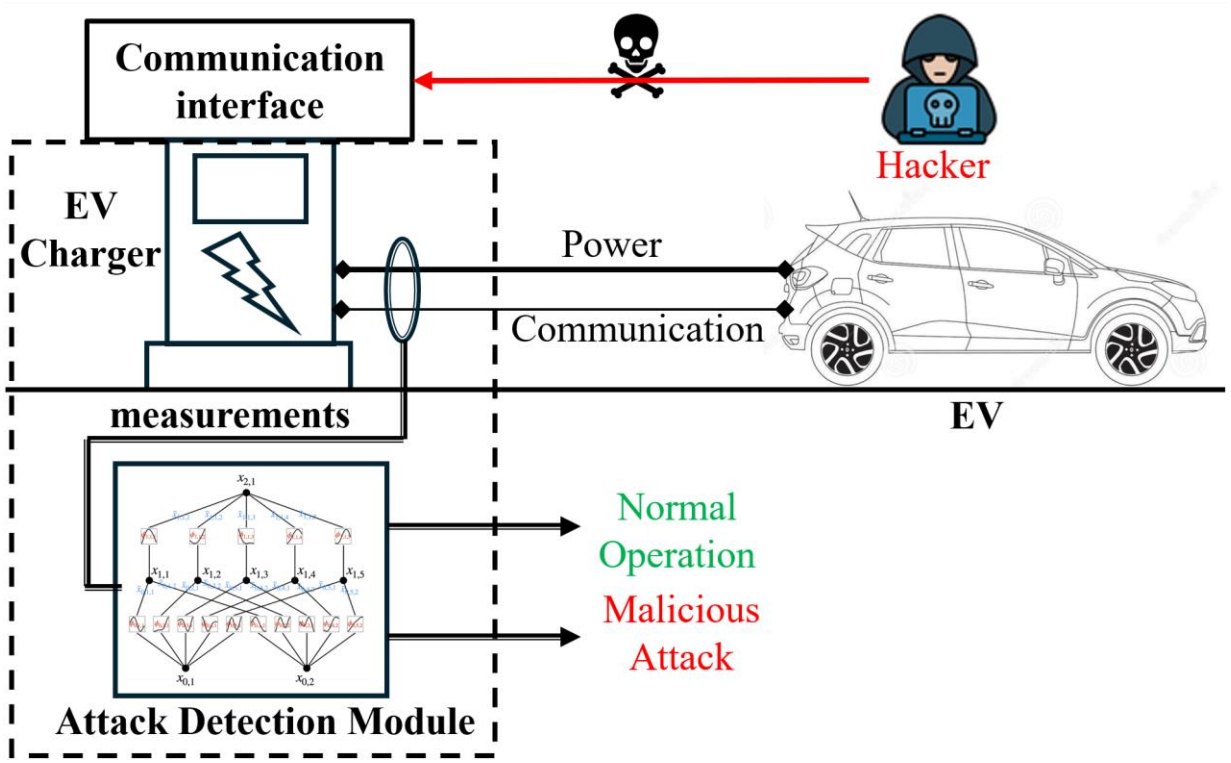
8.1. Jeep Cherokee Hack (2015)

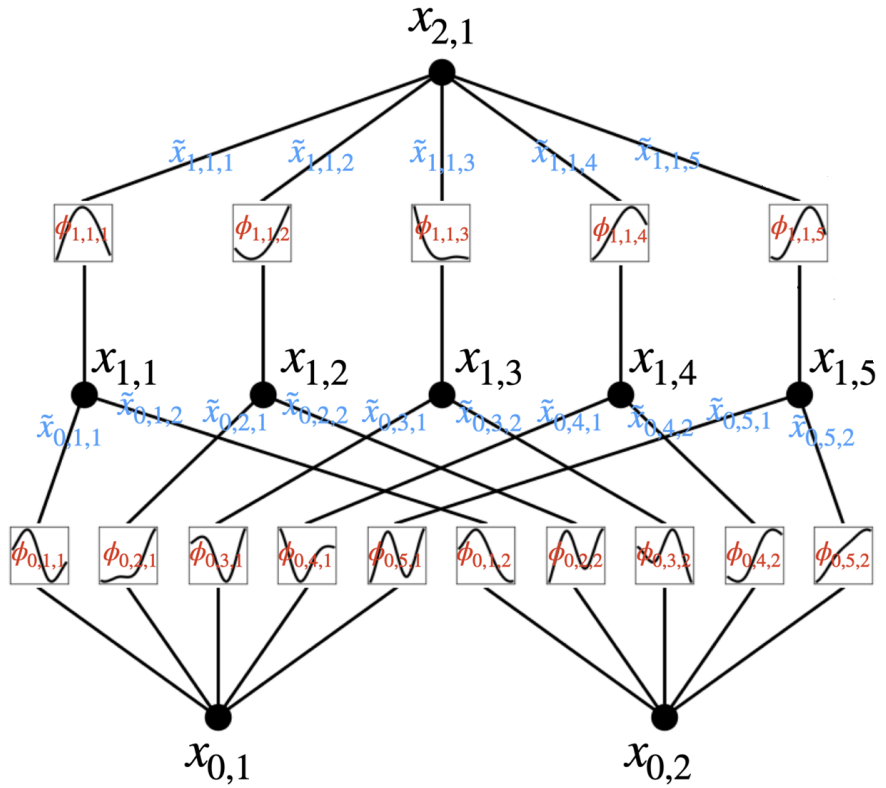
8.2. Stop Sign Adversarial Attack (2020)

8.3. V2X Message Spoofing (2022)



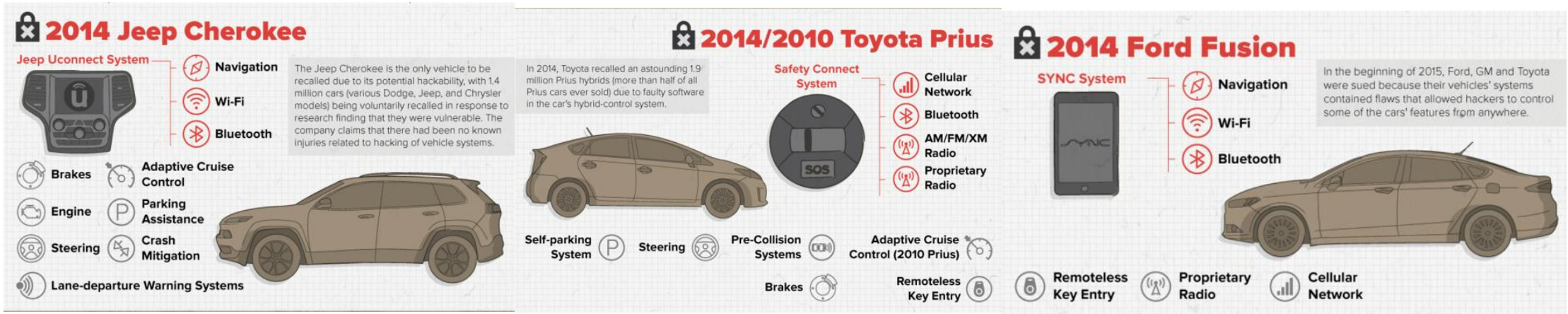
8.4. KAN Detection of Cyberattacks on EV Chargers



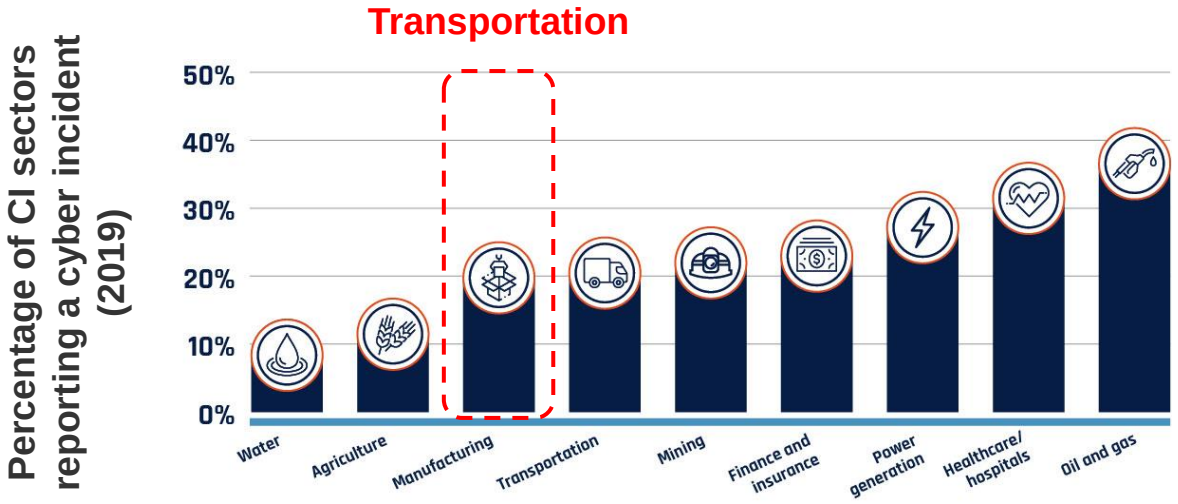


Kolmogorov and Arnold Network
We have updated the activation functions

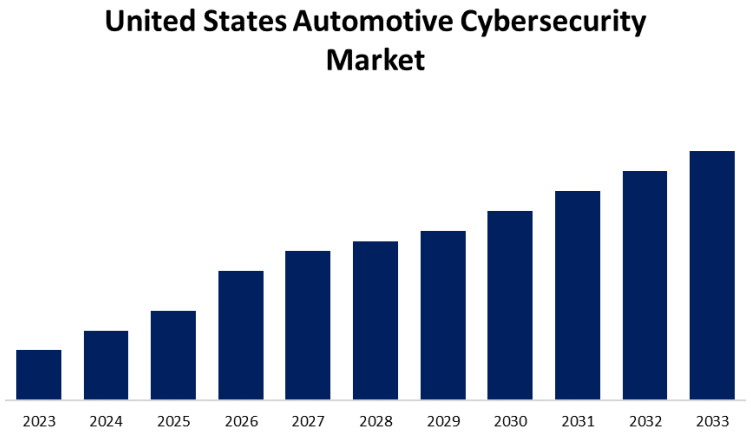
8.5. Analysis of The Most Hackable Vehicles



2014



2019



2033

https://www.csoonline.com/article/552765/study-names-the-five-most-hackable-vehicles.html

Automotive Cybersecurity Standards

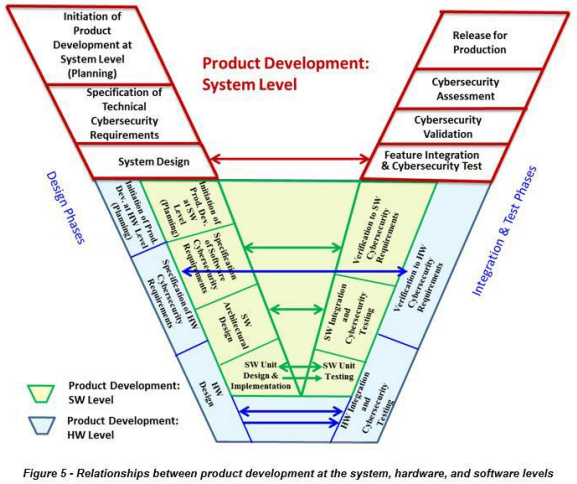
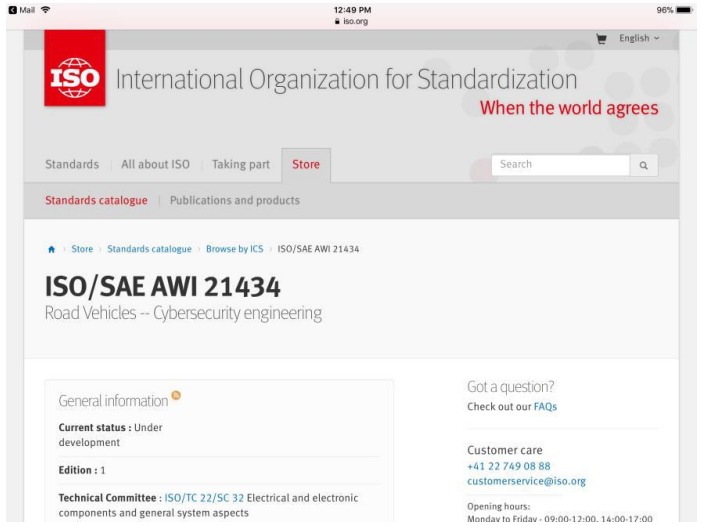


Figure 5 - Relationships between product development at the system, hardware, and software levels

SAE J3061

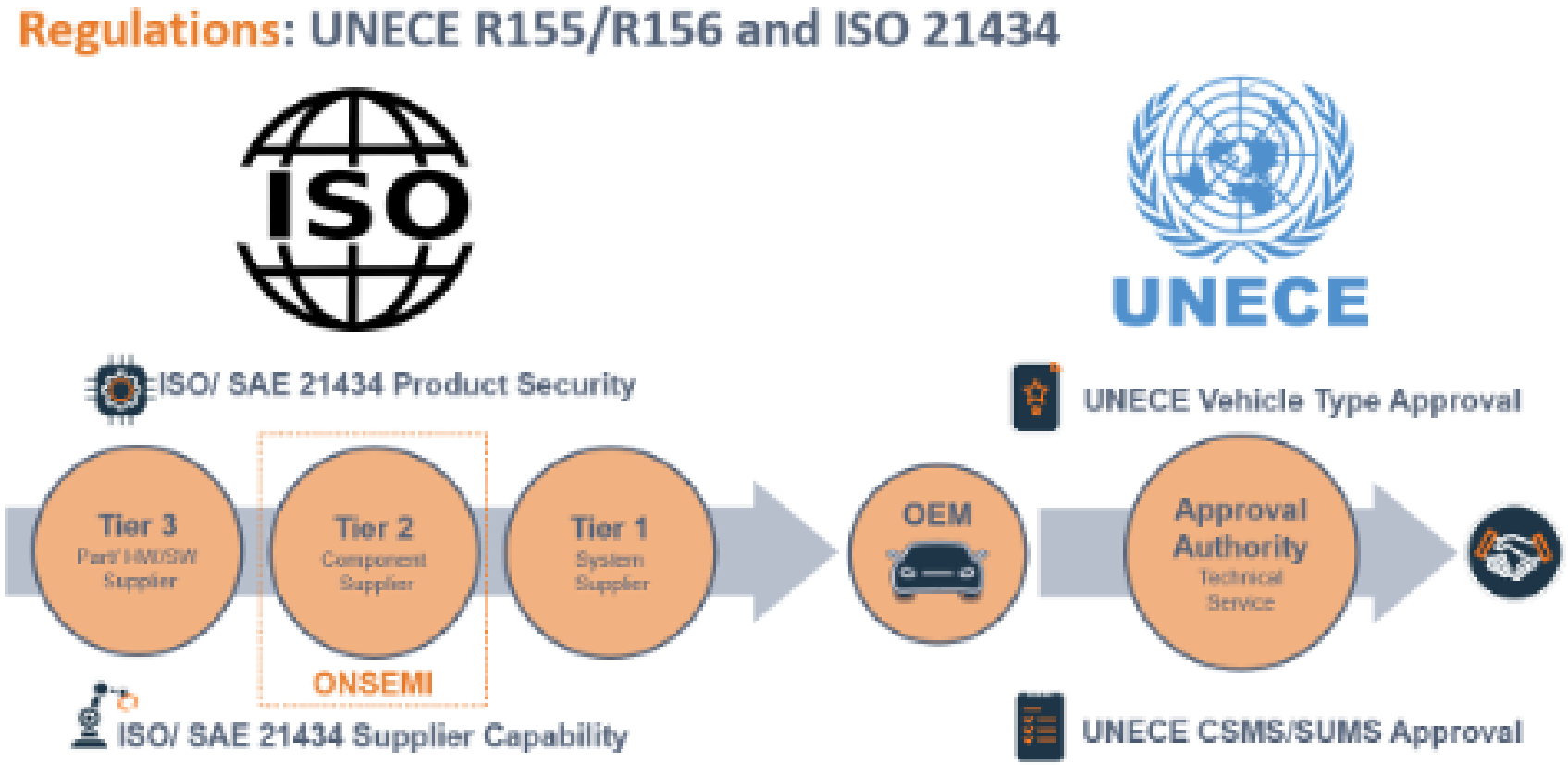
"Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"



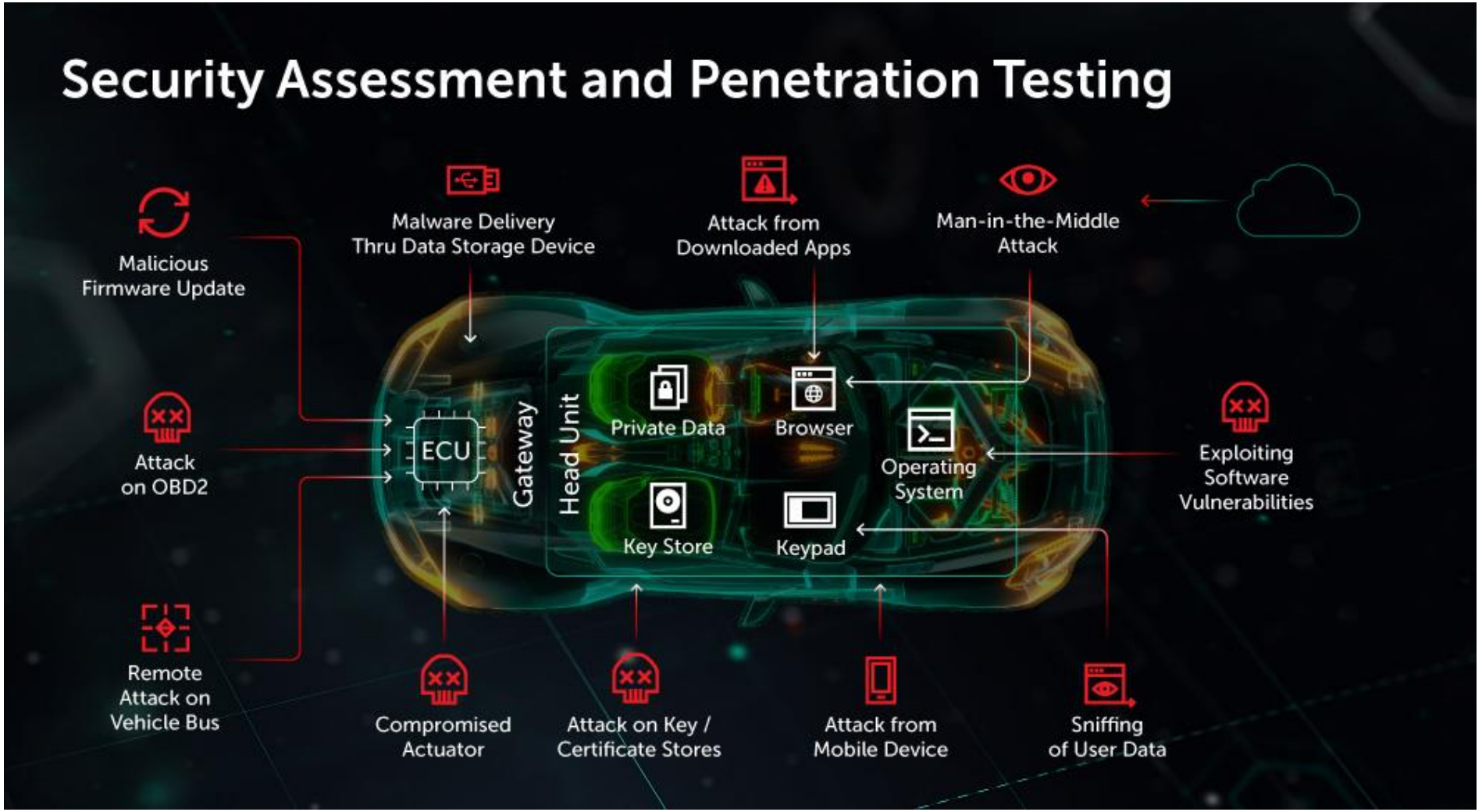
ISO/SAE 21434

IEEE ISIE 2025

There are regulations in Europe



9. Standards and Regulations



10. Research Opportunities

a) Real-Time Intrusion Detection (IDS) and Prevention for In-Vehicle Networks
b) Securing Over-the-Air (OTA) Updates and Software Lifecycle Management
c) AI Robustness and Adversarial Attack Protection in Perception Systems
d) V2X Security and Misbehavior Detection
e) Security of Autonomous Driving Decision-Making and Control Systems
f) Security Testing, Penetration Testing, and Dataset Generation for Automotive Systems

10. Research Opportunities

- **Blockchain** enhances integrity, trust, and decentralized validation across OTA processes, V2X communications, and forensic logs.
- **Quantum technologies**—from QRNG to QKD and PQC—enable vehicles to prepare for a future where classical encryption is broken by quantum computers.
- **Secure OTA** plays a central role, allowing automotive systems to evolve dynamically as new cryptographic standards emerge.

11. Final Considerations

The tutorial highlighted the growing importance of cybersecurity in Intelligent Transportation Systems (ITS), driven by the rise of Connected, Autonomous, Shared, and Electric (CASE) vehicles. Key topics included safety, regulatory compliance (ISO 21434, UNECE WP.29), financial risk, and brand reputation. Real-world incidents like the Jeep Cherokee Hack and V2X spoofing were discussed, along with critical attack points such as CAN Bus and ADAS systems. The session emphasized multi-layered defense strategies and outlined ongoing research challenges, reaffirming cybersecurity as essential for the safety and trust in future mobility.

12. References

[1] ISO/SAE 21434, Road Vehicles — Cybersecurity Engineering, 1st ed., International Organization for Standardization and SAE International, 2021.

[2] United Nations Economic Commission for Europe (UNECE), UN Regulation No. 155: Cyber Security and Cyber Security Management System (CSMS), WP.29, 2021.

[3] SAE International, SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, 2016.

[4] European Union Agency for Cybersecurity (ENISA), Cybersecurity and Resilience of Smart Cars, Dec. 2019.

[5] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in Proceedings of the USENIX Security Symposium, 2011.

[6] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," in Black Hat USA, Las Vegas, USA, 2015.

[7] Upstream Security, 2024 Global Automotive Cybersecurity Report, Upstream Security Ltd., 2024. [Online]. Available: https://www.upstream.auto/

[8] M. Petri, C. Törsleff, et al., Automotive Cybersecurity: An Introduction for the Engineering Community, Springer, 2021.

[9] O. Al-Jarrah et al., "Cyber-Physical Systems Security for Smart Cars: Challenges and Solutions," IEEE Communications Magazine, vol. 55, no. 8, pp. 98–104, Aug. 2017.

[10] National Highway Traffic Safety Administration (NHTSA), Cybersecurity Best Practices for the Safety of Modern Vehicles, DOT HS 812 333, 2022.

[11] R. S. Shrestha et al., "A Survey on Intrusion Detection Systems for In-Vehicle Networks," IEEE Access, vol. 8, pp. 185497–185511, 2020.

[12] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the Art: Automotive Security," EURASIP Journal on Embedded Systems, vol. 2007, Article ID 074706, 2007.

[13] M. Amoozadeh et al., "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," IEEE Communications Magazine, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[14] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired Magazine, Jul. 2015. [Online]. Available: https://www.wired.com

Q&A