Securing the Future of Mobility

Cybersecurity, Privacy, and Quantum-ready Strategies for Software-Defined Vehicles
Venue: IEEE Vehicle Technology Society Webinar 2025

Dr. Sheikh Mahbub Habib

About me

Dr. Sheikh M. Habib

Head of Product
Cybersecurity and Privacy
Innovation

Oct. 2022

Education

- Doctoral degree (Dr. rer. nat) in Computer Science, TU Darmstadt (2013), Germany
- Master in Networks and Distributed Systems, Chalmers University of Technology (2009), Sweden
- Bachelor of Computer Science and Engineering, Khulna University of Engineering and Technology (2003), Bangladesh

Roles

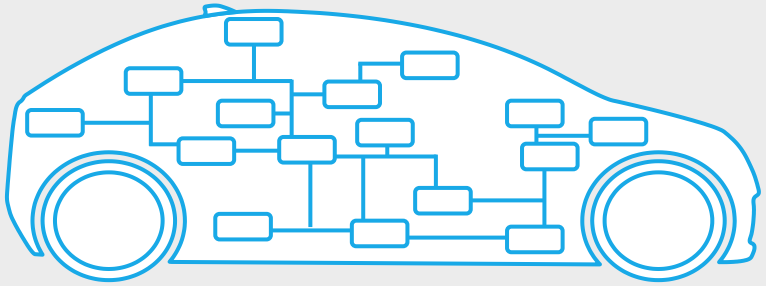
- Growth Field Leader, Security and Privacy Technologies Continental Automotive, Germany
- Manager, Automotive Security and Privacy Innovation, Continental AG, Germany
- Project Lead Automotive Security and Privacy, Continental AG, Germany
- Research Area Head, Telecooperation Division, TU Darmstadt, Germany
- Research Area Coordinator, Center for Advanced Security Research Darmstadt, Germany
- Visiting Scholar, Macquarie University, Australia

Personal Highlights

- More than 7 years industry experience in Automotive Cybersecurity and Privacy
- More than 9 years academic research experience in IT Security and Privacy
- Principal Investigator in various national and international Cybersecurity projects
- Public Speaker, Author, Program Committee members at Automotive/IT Cybersecurity events

Paradigm Shift
Complexity & functional growth reaching its limits

Up2now

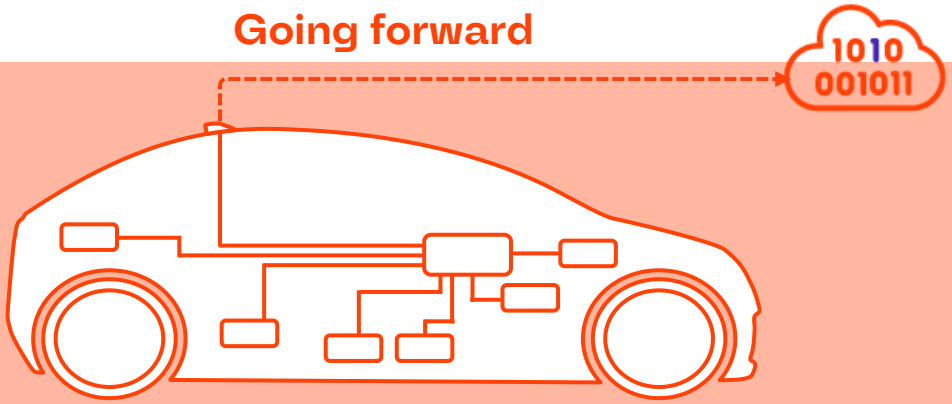


Patchwork Architecture

- Up to ~100 ECUs
- Limited compute power
- Functionality isolated in ECUs
- Lots of wires
- Limited cloud-based functionality

User Expectation: Pleasure, Safety & Comfort

Going forward



Function-defined / Service-oriented Architecture

- Few high-performance computers & zones
- Significant compute power (more processor cores)
- Functions defined by software (hardware abstraction)
- Less deterministic
- Always connected

User Expectation: Smart IoT device

Navigating the future
Leveraging key trends to drive the transformation

Demographic Shifts

Empowered Society

Next-Gen Mobility

Exponential Innovation

- **Urbanization**
  Smart traffic management, urban telematics, vehicle-to-infrastructure
- **Individualization**
  Differentiation, tailored solutions, flexibility, biometrics
- **Digital Lifestyle**
  Connectivity standards, seamless device integration, real-time data
- **Software-defined Vehicle**
  Server-Zone architecture, Edge computing, SW updates, services
- **Computing Power & Connectivity**
  Cloud computing, robust networking, Cybersecurity
- **AI and Virtualization**
  Big data, machine learning, HPC, digital twins

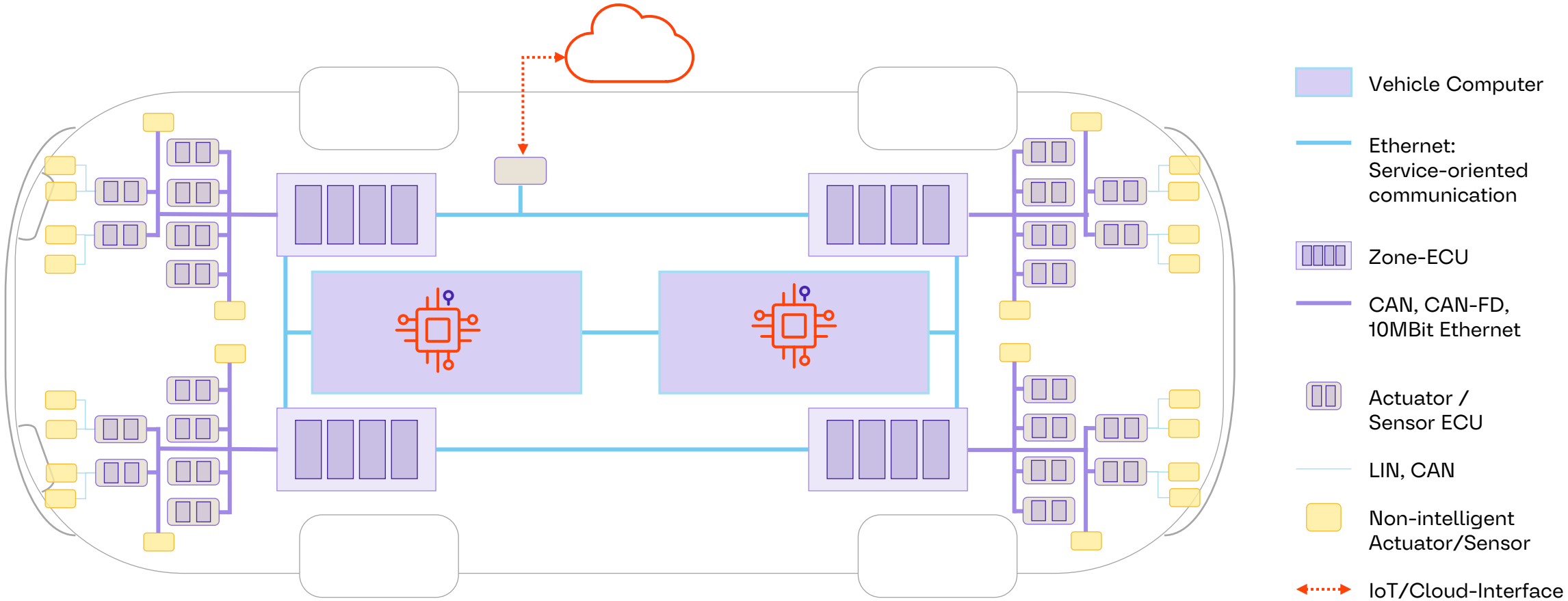
The vehicle is no longer a closed system but a part of a complex software-centric ecosystem – the IoT

Software Defined Vehicles (SDVs)
Definition

In a Software-defined Vehicle, functions are enabled by software. Decoupling software from hardware enables swift and continuous development & implementation of new functions and software updates throughout vehicle lifetime.

The vehicle is no longer a closed system but a part of a complex software-centric ecosystem – the IoT

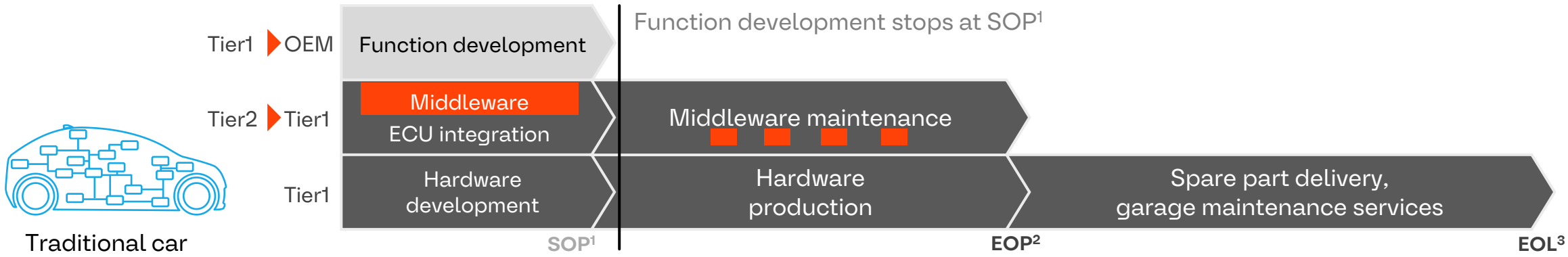
Complex Software Bundled in a few HPCs
Server / Zone Architecture, Networking & Connectivity



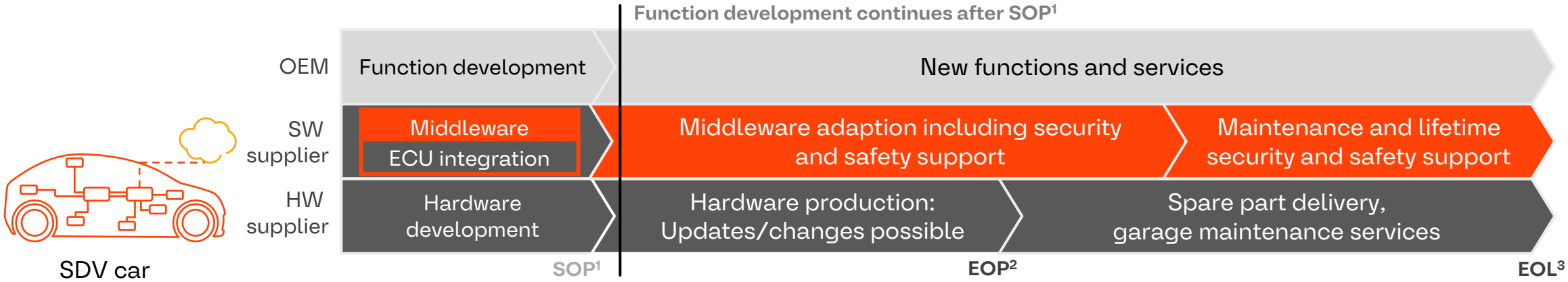
Example: 2 Vehicle Computers / 4 Zone-ECUs

Architecture Transformation
Trust-based collaboration & partnership models

Hardware and function coupling – Software treated like hardware



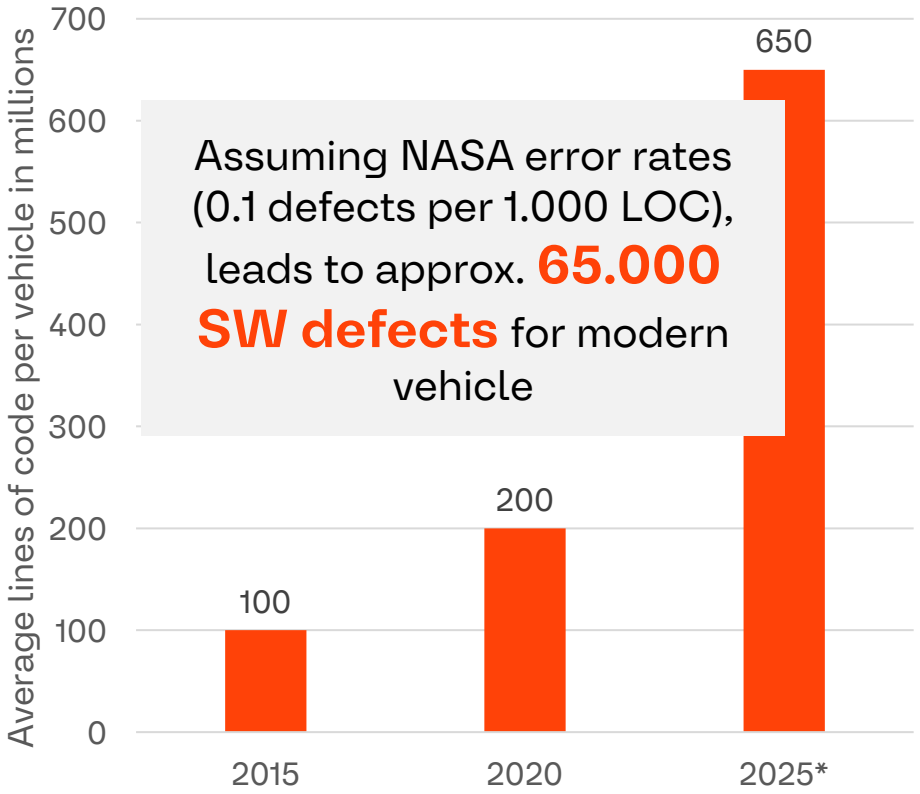
Software-defined vehicle needs a software platform partner throughout vehicle lifecycle



[1] SOP: Start of production, [2] EOP: End of production, [3] EOL: End of life

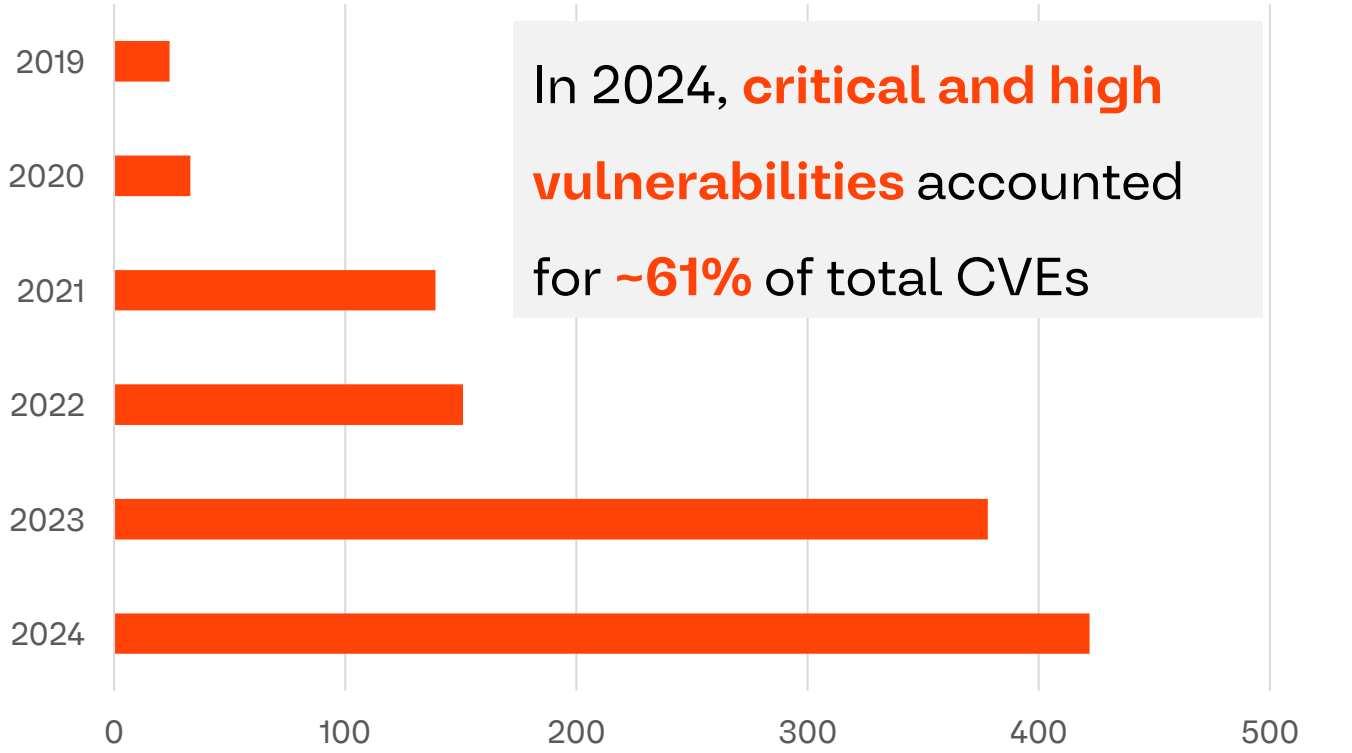
Number of Lines of Code is significantly Increasing
Leads to an increasing number of critical and high CVEs

Average lines of code per vehicle in millions



Source: Goldman Sachs. (November 8, 2022). Average number of lines of codes per vehicle globally in 2015 and 2020, with a forecast for 2025 (in millions)

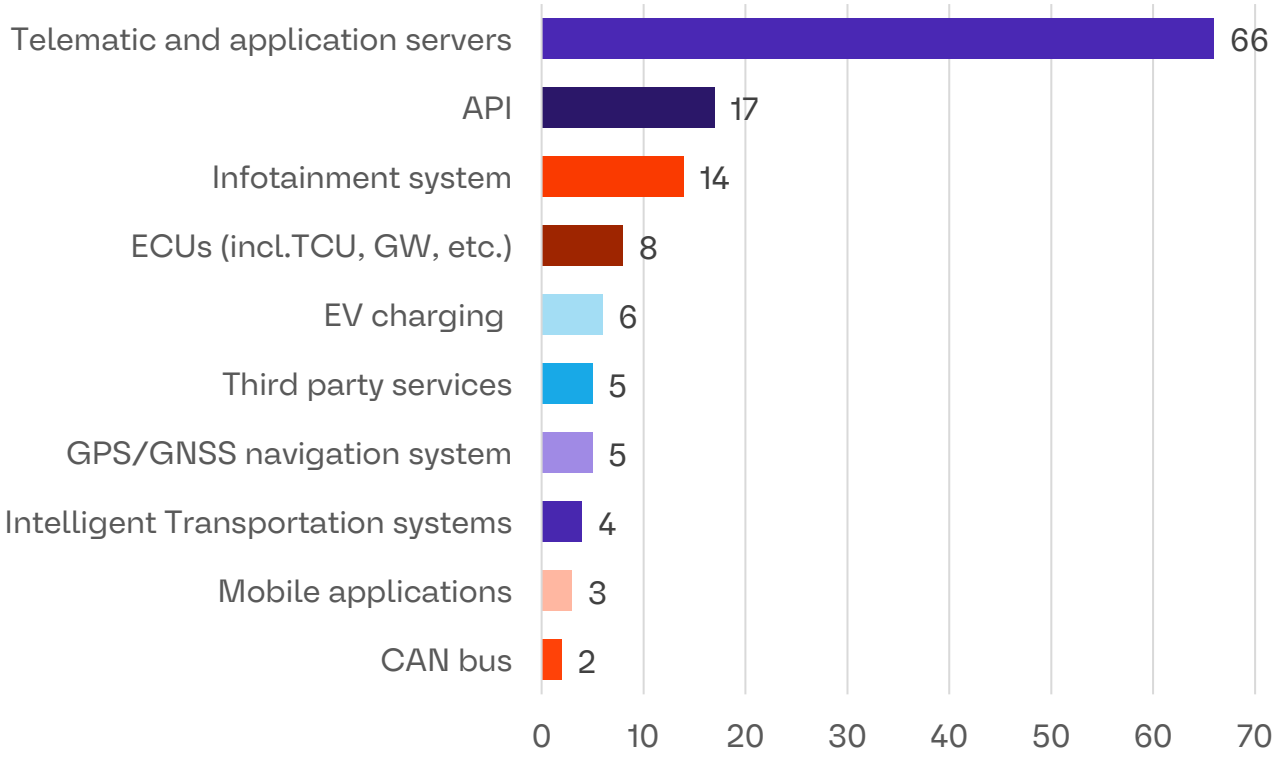
Number of automotive-related CVEs found in 2019-2024



CVE = Common Vulnerabilities and Exposures | LOC = Line of Code | Source: Upstream Global Automotive Cybersecurity Report 2025

Security Attacks in Automotive Industry
~92% of all attacks were remote in 2024

Illustration highlights the **key attack vectors** and their percentage of total Incidents in 2024



- The proportion of incidents with a **“high” or “massive” impact** increased to **over 60%** of all incidents
- Telematics and application server attacks increased from **43% in 2023** to **66% in 2024**
- In 2024, increase of **~41%** in **critical automotive – related vulnerabilities**
- Increase in **Black Hat Hackers each year**
  - 65% Black Hat (+1%),
  - 35% White Hat (-1%),
- **~92% (-3%)** of all attacks were **remote** in 2024, whereas 84% of those were long-range

Source: Upstream Global Automotive Cybersecurity Report 2025

What does SDV mean for Cybersecurity?

Risks

Increased complexity
► number of suppliers, lines of code, new protocols

Increased attack surface
► more interfaces, extension to infrastructure

More data collection
► privacy risks

Attacks on AI systems
► malfunctions

Skill and mindset of people
► 28% - of cybersecurity jobs worldwide unfilled

Opportunities

Advanced Sec. Architectures
►novel alg. and protocols

Novel fail-safe mode
► in case of cyber sec. attack

Security in SW vs. HW
► easier crypto agility

Virtualization ► new testing capabilities

Update cycle ►faster, frequent, cost-efficient

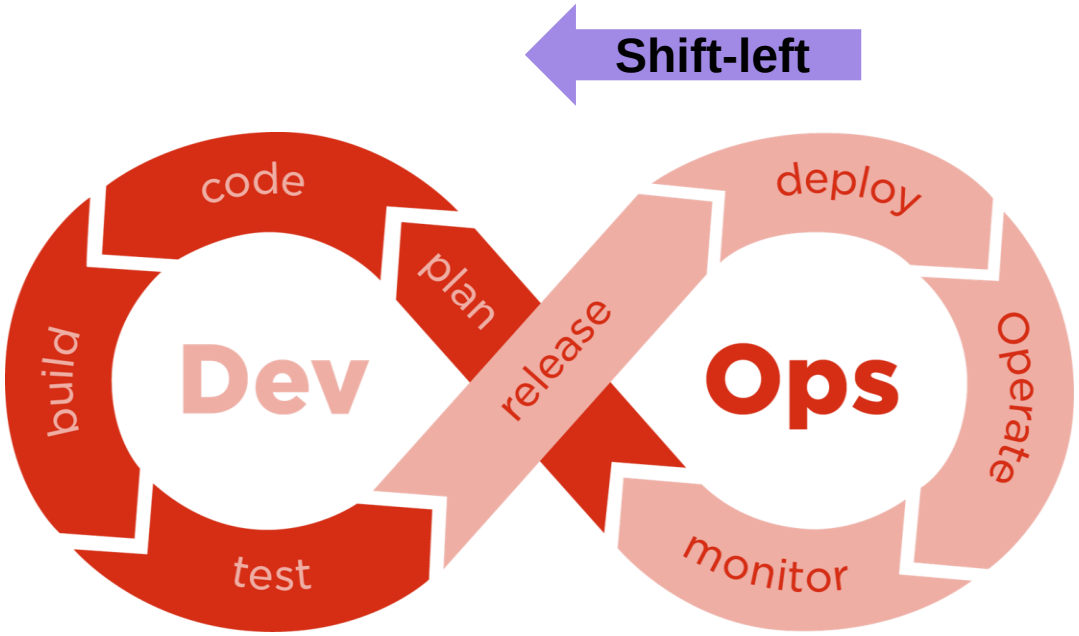
From SDLC → DevSecOps
► security operations included

Shift-left approach
► early mitigations

SDLC – SW Development Lifecycle | DevSeOps – Development Security Operations

Novel Development Cycle
Shift-left approach essential to manage complexity

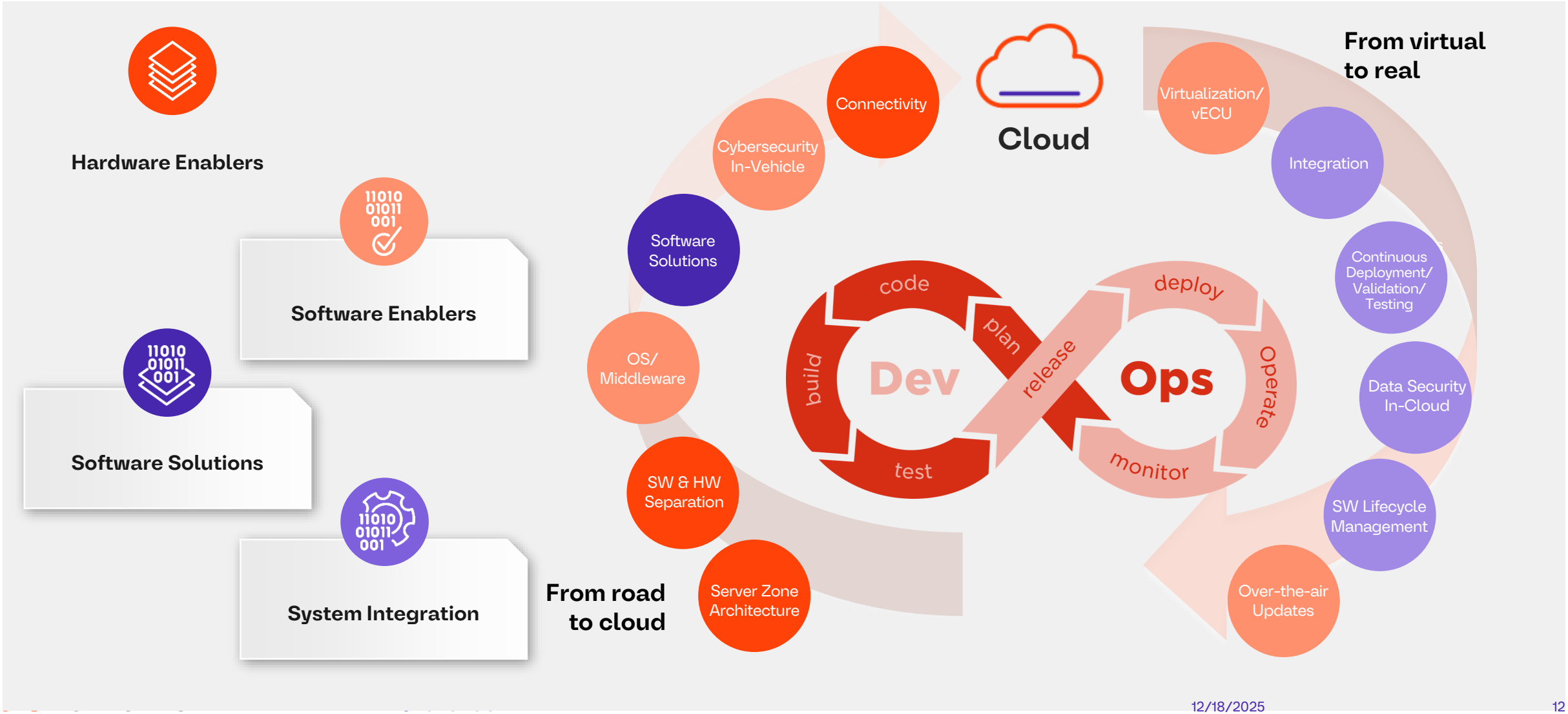
- **Early Integration:** Security practices integrated into the earliest stages of the SDLC
- **Proactive Measures:** Identifies and mitigates potential security vulnerabilities early in the development
- **Automated Testing:** Utilizes automated security testing tools to catch vulnerabilities early and often
- **Cost Efficiency:** Fixing security issues early in the development process
- **Improved Software Quality:** Leads to higher quality software that is more secure and resilient to cyberattacks



AUMOVIO

Novel Development Cycle Possible
Solutions for the software-defined vehicle

SW = Software | HW = Hardware | OS = Operating System

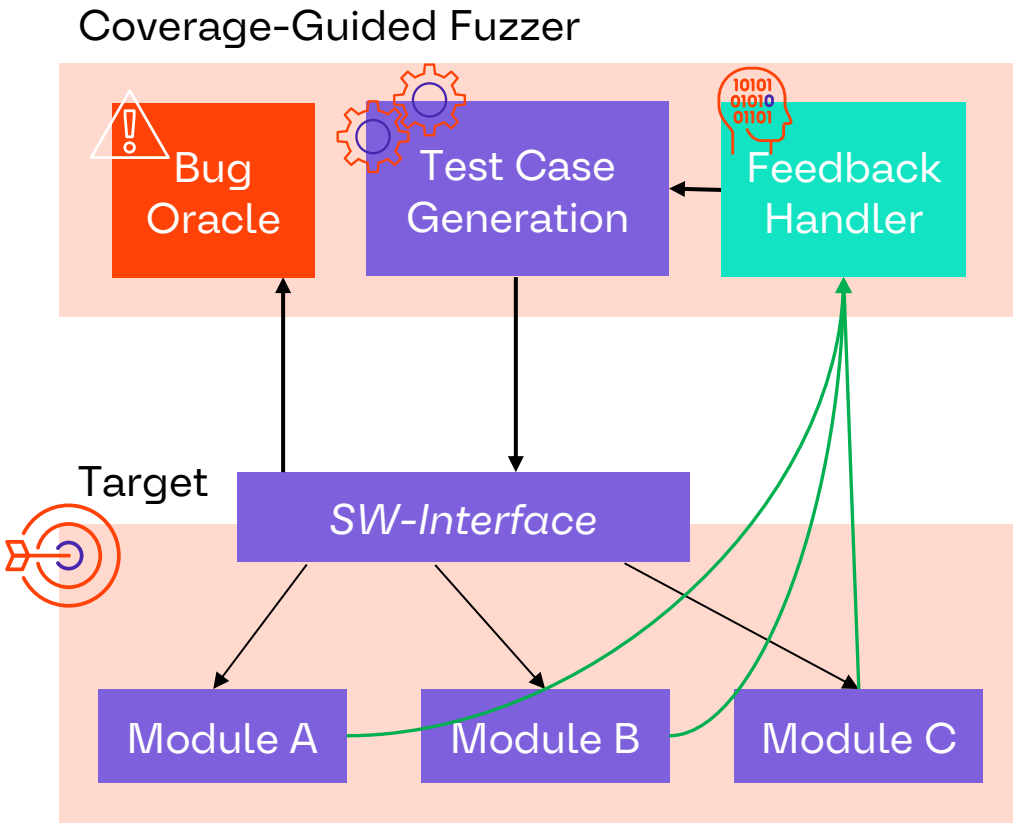


Securing the Future of Mobility

AUMOVIO

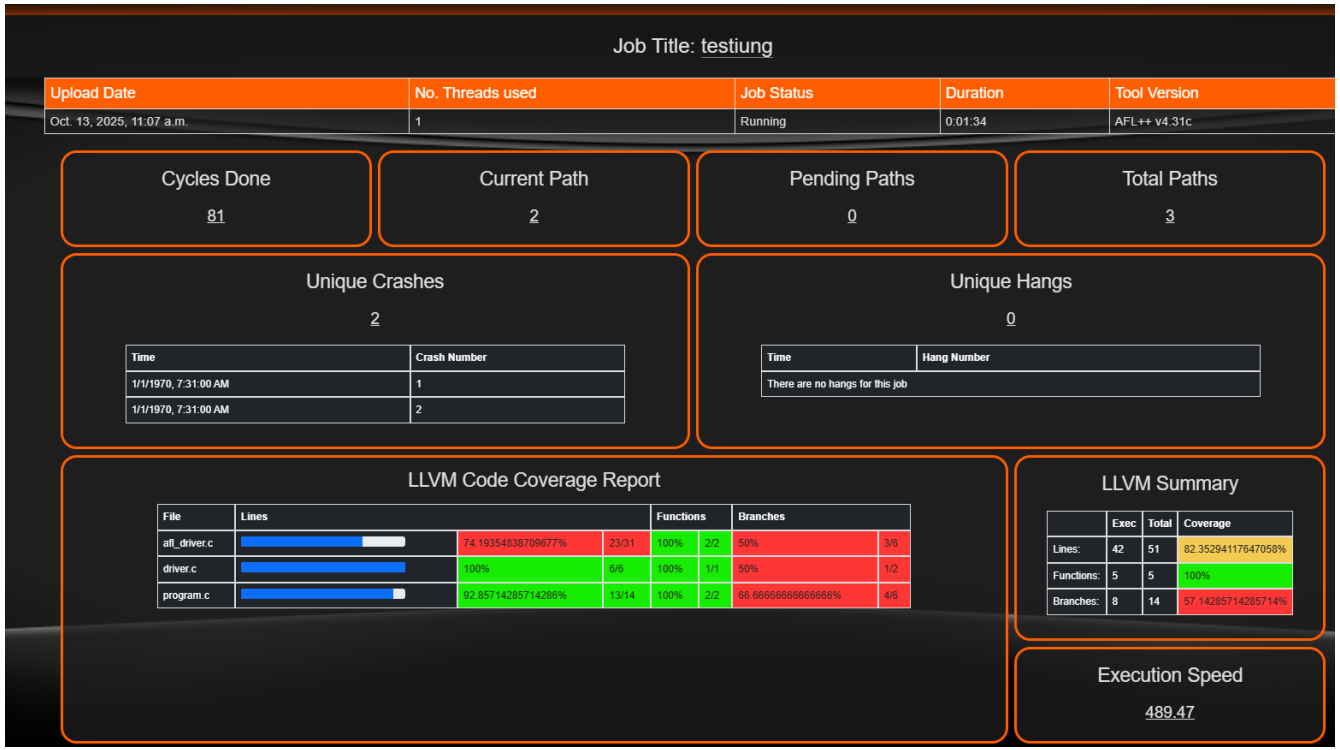
Novel Development Cycle Possible
Advanced Software Testing

- Software fuzzing is a testing technique that **inputs invalid or random data** into the software system to **discover memory errors and security loopholes**
- Coverage-Guided Fuzzing uses *instrumentation* to see what happens inside target
  - Focus on SW-level testing
  - “Smart” input generation
  - Feedback channel between target and Fuzzer
  - After data input the **system is monitored for** code coverage and various **exceptions**: crashing, failing built-in code, irregular behavior
  - Allows to **find more complex bugs in less time**



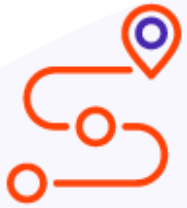
Advanced Software testing
AUMOVIO-EB Fuzz Framework – SW level test

- **OVERVIEW**
  - AFL based fuzzing
  - Easily setup and run fuzz tests
  - Supports C/C++ based applications
  - Currently works on linux based machines
- **FEATURES**
  - Root Cause analysis(RCA)
  - Full system emulation-based fuzzing
  - Generate coverage reports



Data collection in smart vehicles
Examples

Location information
- Starting position
- Destination
- Route
- Time
- Speed



User recognition
- Physical/ Biometrics
- Fingerprint
- Face
- Eye movement
- Seat configuration

In-Cabin information
- Microphone
- Camera
- Infotainment
- Vehicle Occupants

Applications
- Contacts
- Call logs & messages
- Payment
- Subscriptions

PERSONAL DATA IN YOUR CAR, National Automobile Dealers Association and the Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf

Categories of sensitive data
Examples

Data Type	Example	Sensitivity
Location	GPS tracking, route history	Can reveal habits, workplaces, private visits
Biometrics	Face recognition, driver fatigue detection	Identifies individuals
Behavioral	Driving style, braking habits	Used in insurance or employee monitoring
Communications	Voice commands, phone syncs	Contains private conversations
Multimedia	Cameras, microphones	Potentially records people without consent

Data access
Involved parties

OEMs
(Original Equipment Manufacturers)

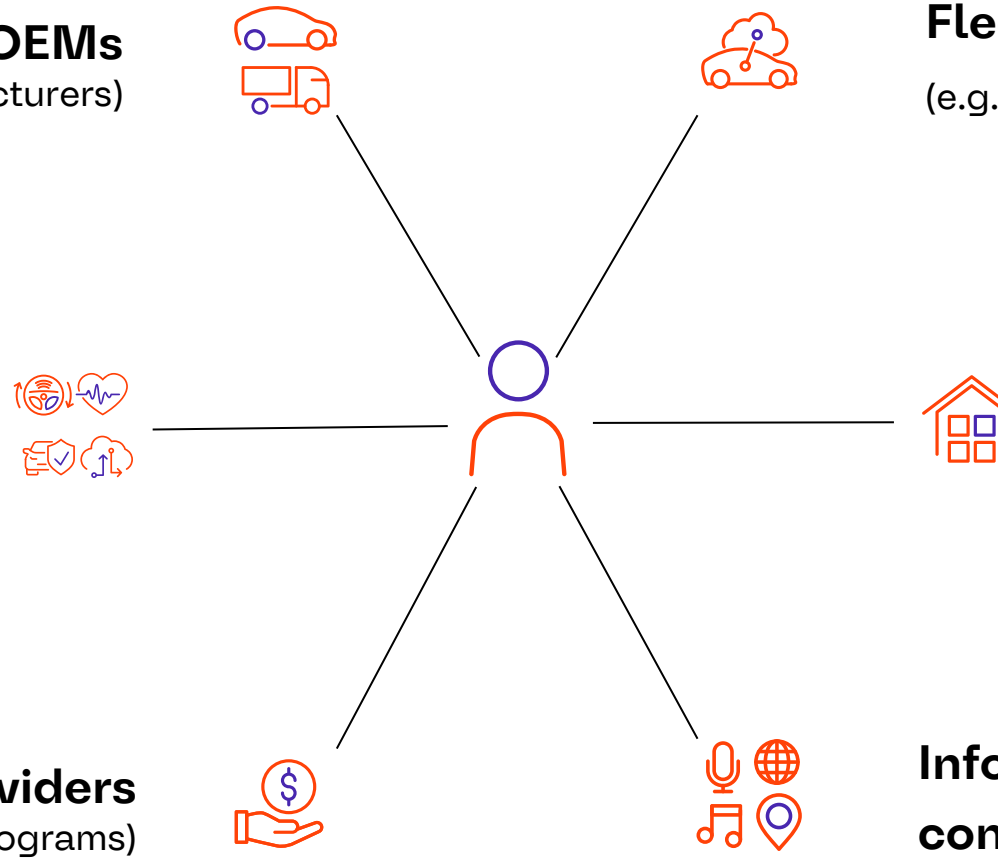
Fleet managers
(e.g., in corporate cars)

Tier 1 suppliers

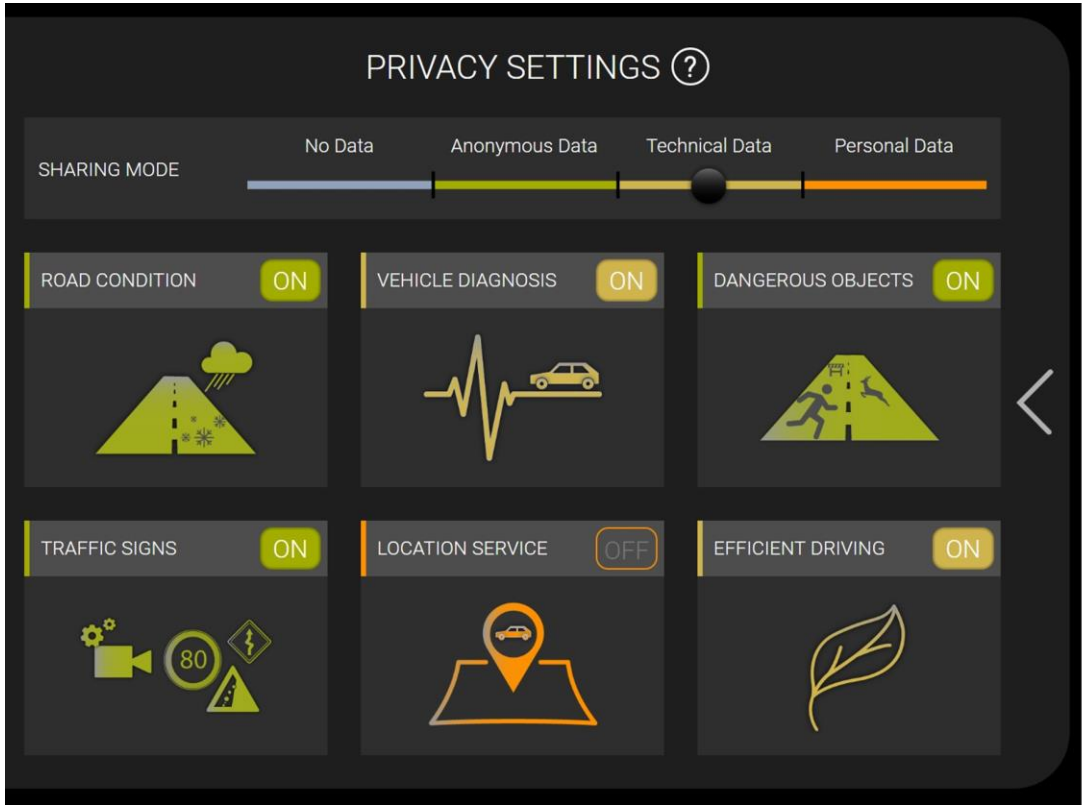
Law enforcement
(under certain conditions)

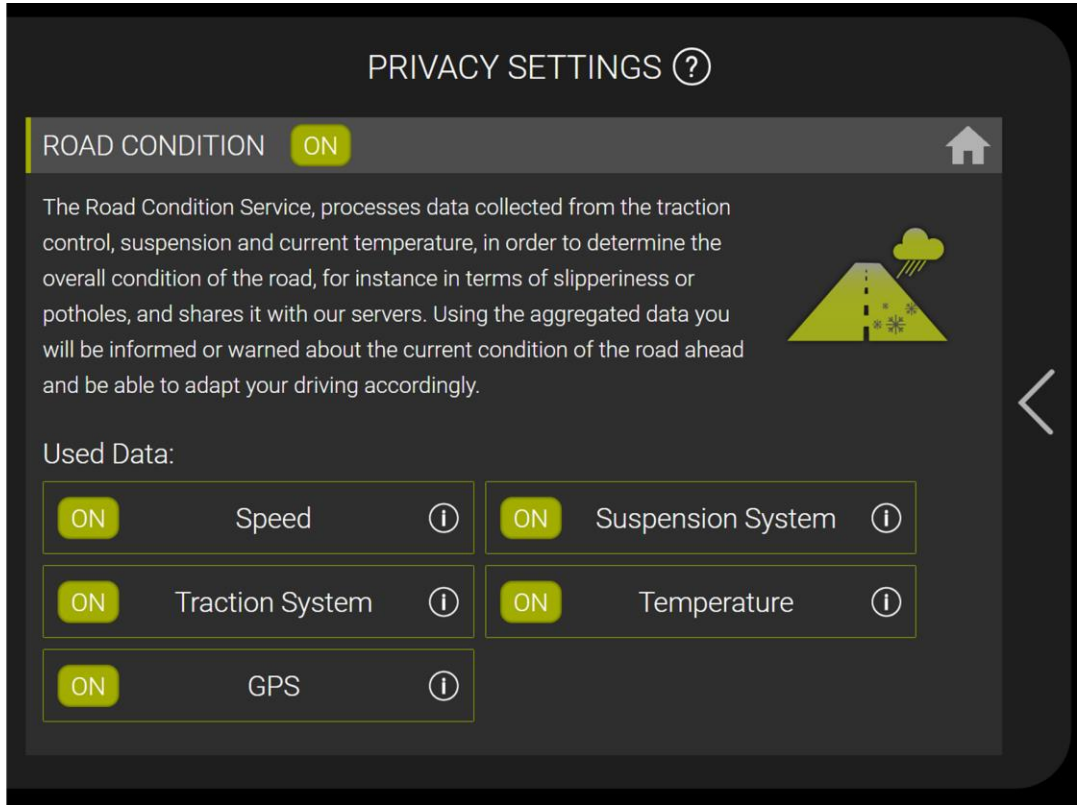
Insurance providers
(e.g., telematics programs)

Infotainment and connectivity providers



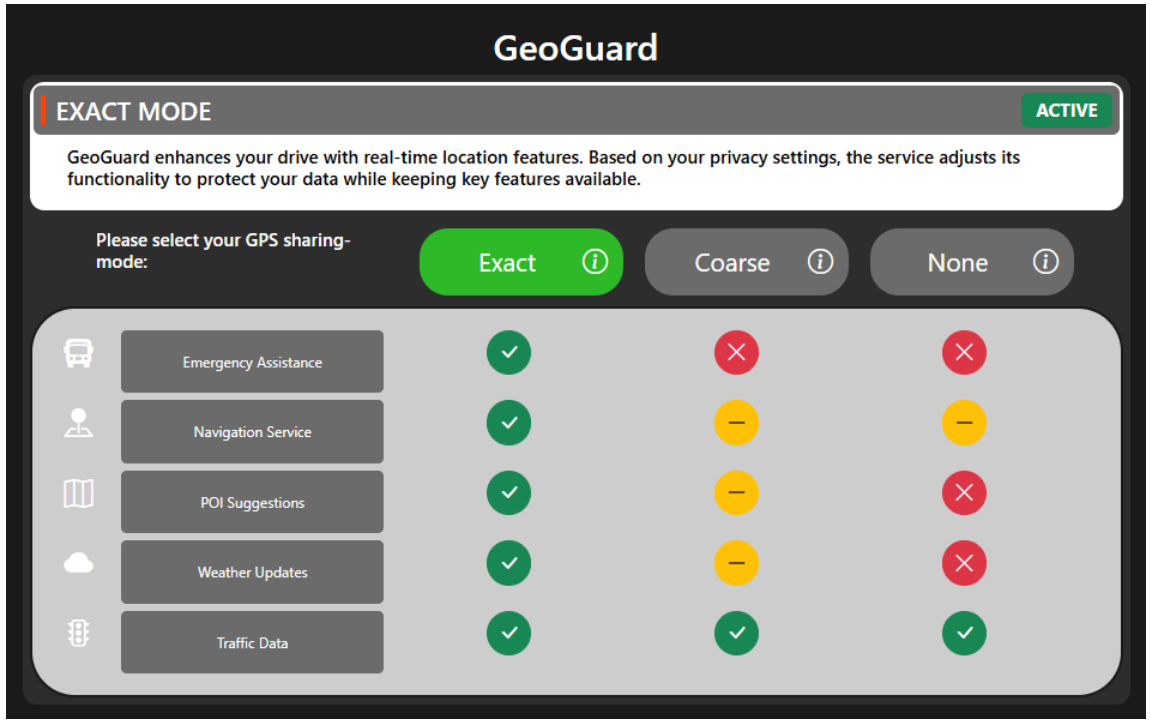
Solutions & technologies
Privacy Human-Machine Interface

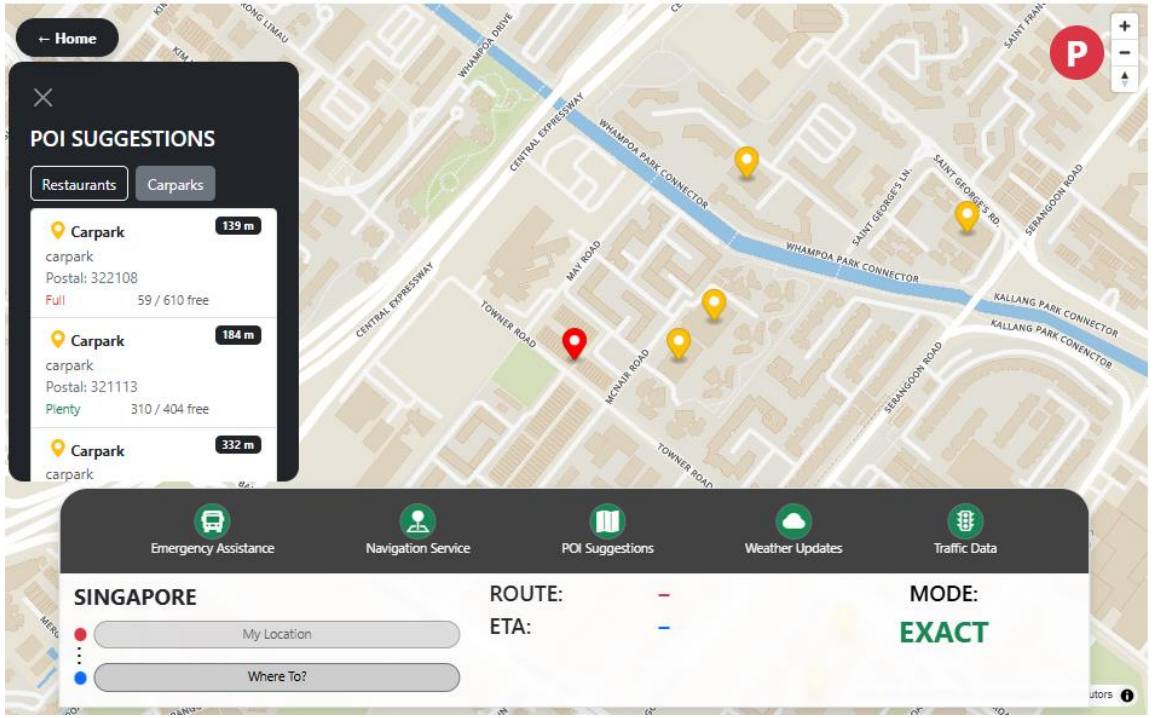




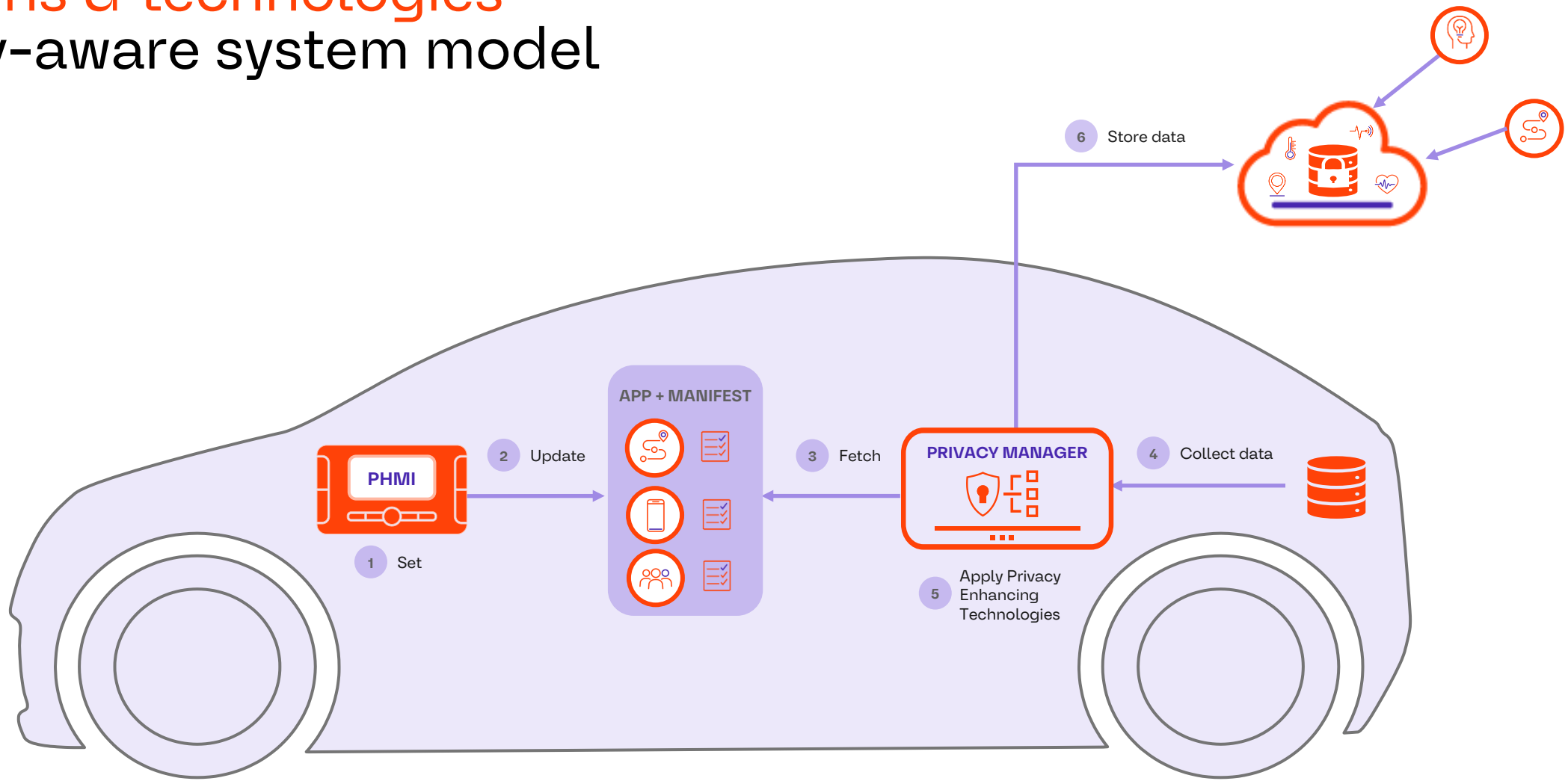
Solutions & technologies
Privacy Demonstrator

Conceptual product that embodies:
- **Privacy-by-design architecture** for location-based services
- A **configurable privacy interface (PHMI)**
- A **simulation of service provider perspectives** under different data-sharing modes





Solutions & technologies
Privacy-aware system model



[1] Syed-Winkler et al., “A Data Protection-Oriented System Model Enforcing Purpose Limitation for Connected Mobility”, 2022
[2] Pape et al., “A Systematic Approach for Automotive Privacy Management”, 2023
[3] Pape et al., “AUTOPSY: A Framework for Tackling Privacy Challenges in the Automotive Industry”, 2025

Regulatory landscape
Milestones 2012-2022

2012

› **General Data Protection Regulation**
Draft passed the EU Parliament

The Privacy Principles ISO/IEC 29100 (2011)

2013

Edward Snowden

2016

› **European General Data Protection Regulation**
Published

2018

› **EU GDPR**
Enforced

2020

› **Tesla Data Protection Study**

2021

› **Expert Study**
"GDPR application in the context of car connectivity "

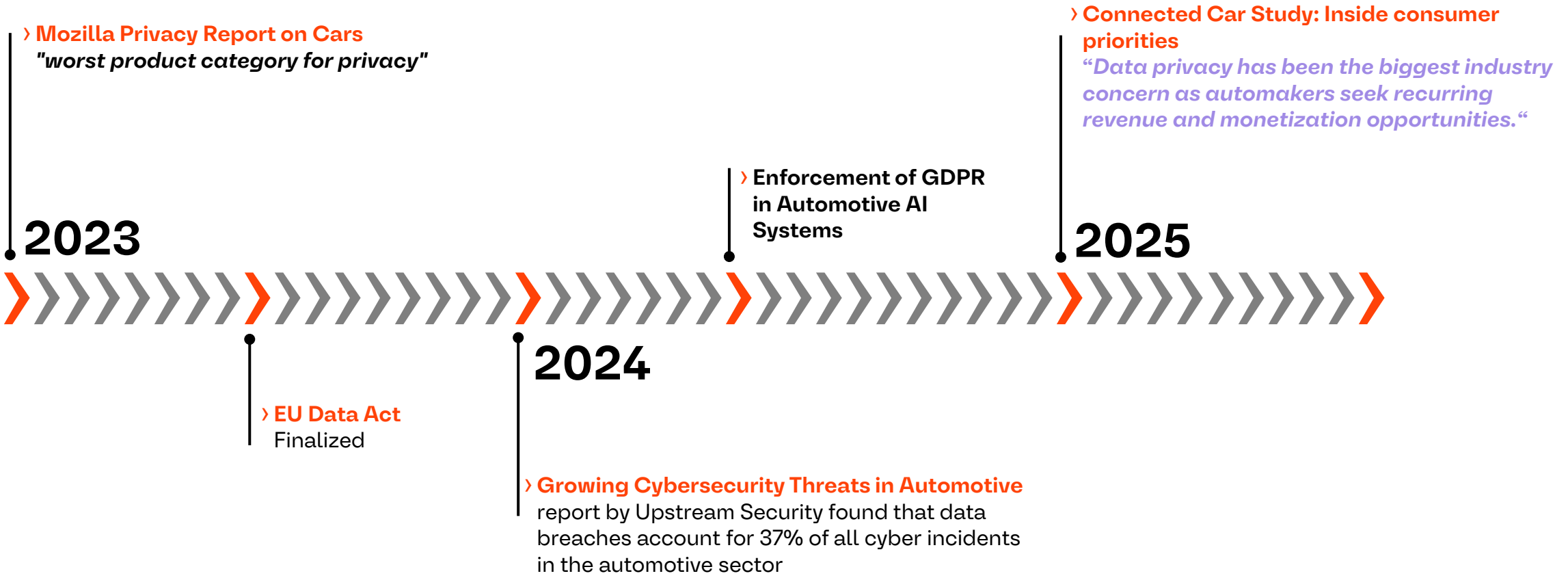
2022

› **VW GDPR Violation Penalty**
€ 1,1M

edpb European Data Protection Board

Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications(2020)

Regulatory landscape
Milestones 2023-2025



Industry experts talk about “Quantum Computers”

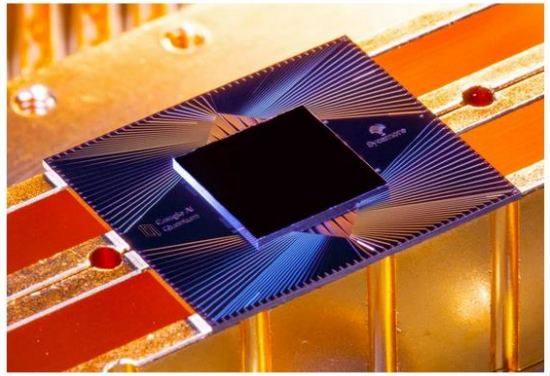
nature › news › article

NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney



The Sycamore chip is composed of 54 qubits, each made of superconducting loops. Credit: Erik Lucero

IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two

Company Outlines Path Towards Quantum-Centric Supercomputing with New Hardware, Software, and System Breakthrough

Nov 9, 2022

Dario Gil, Jay Gan

Intel Newsroom / **Intel Hits Key Milestone in Quantum Chip Research**

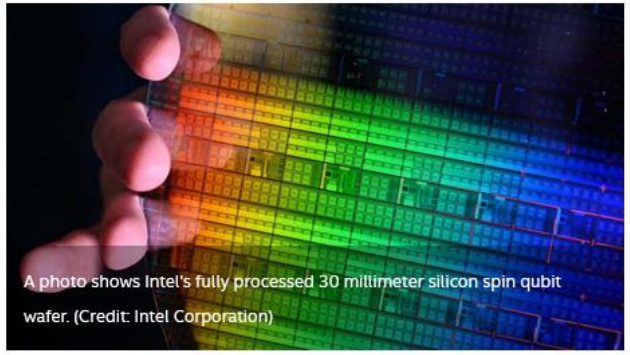
Intel Hits Key Milestone in Quantum Chip Production Research

Intel demonstrates exceptional yield of quantum dot arrays, showing promise for large-scale qubit production using transistor fabrication technology.

News

- October 5, 2022
- Contact Intel PR

More New Technologies News



A photo shows Intel's fully processed 30 millimeter silicon spin qubit wafer. (Credit: Intel Corporation)

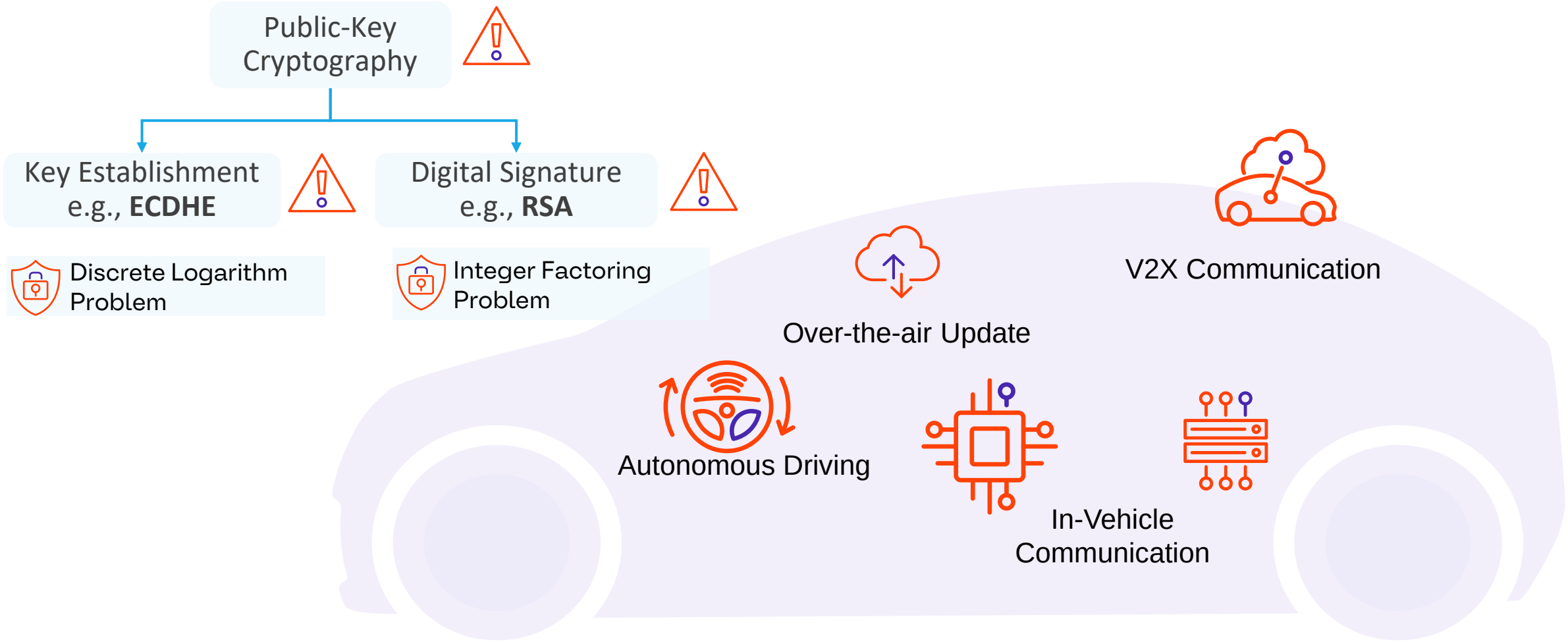
Sources:

https://www.nature.com/articles/d41586-019-03213-z/

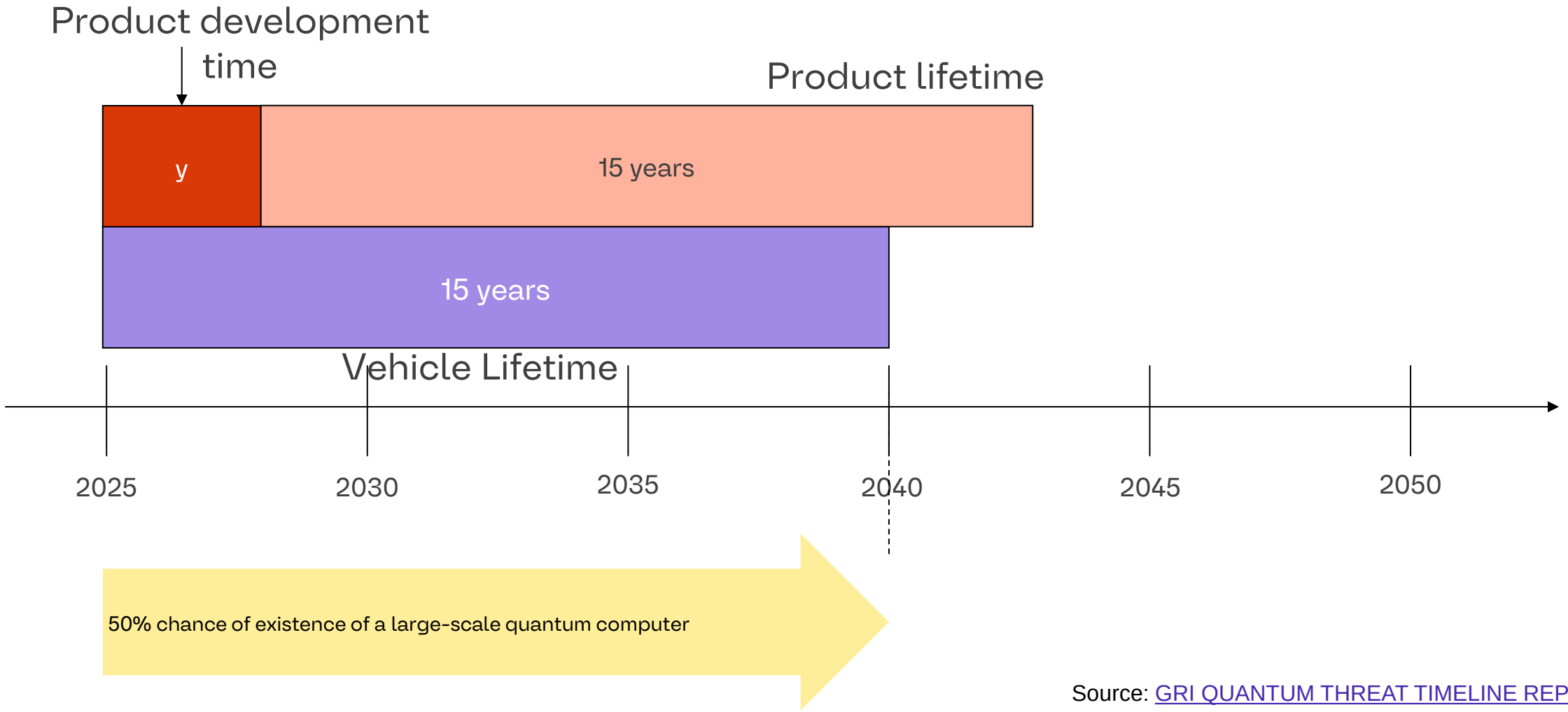
Intel Hits Key Milestone in Quantum Chip Production Research

IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two

Quantum threat to vehicles

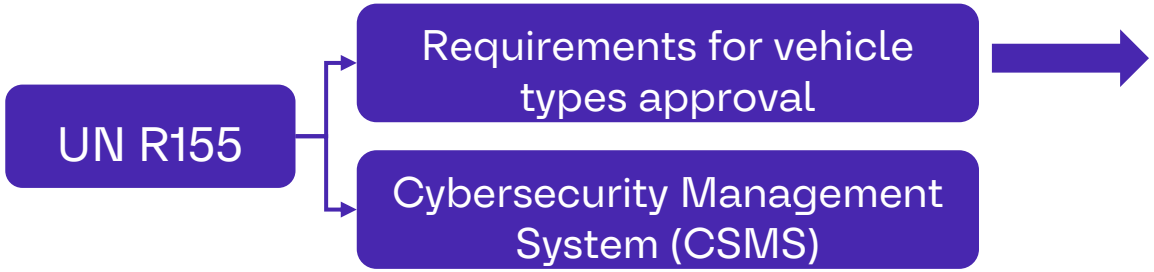


Migration to Quantum-safe
If we start now, we are already late



Source: GRI QUANTUM THREAT TIMELINE REPORT 2024

Migration to Quantum-safe
UN R155 Regulation & Quantum Threat



7.3.8. **Cryptographic modules** used for the purpose of this Regulation **shall be in line with consensus standards**. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Source: NIST IR 8547 ipd

The expectation is that NEW vehicle type approval will not be approved starting 2036 for the deprecating algorithms

Migration to Quantum-safe
NIST Standard on Post-Quantum Crypto

FIPS	Intended Use	Based on
FIPS 203	Primary standard for general encryption	CRYSTALS-Kyber, renamed to ML-KEM
FIPS 204	Primary standard for digital signatures	CRYSTALS-Dilithium algorithm, renamed to ML-DSA
FIPS 205	Designed for digital signatures Backup method in case ML-DSA proves vulnerable	Sphincs+ algorithm, renamed to SLH-DSA

ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism.
ML-DSA: Module-Lattice-Based Digital Signature Algorithm.
SLH-DSA: Stateless Hash-Based Digital Signature Algorithm

Call for Quantum-Resistant Digital Signatures

- Deadline was June 1st, 2023
- Preferably signatures based on non-lattice problems
- Short signatures and fast verification
- July 17, 2023: 40 submissions accepted as "complete and proper“

Status

- NIST IR 8528: NIST selected 14 candidate algorithms to move forward to the second round of evaluation

Post-Quantum Cryptography (PQC) Standard
Deprecation of traditional security primitives

Region / Body	Deprecation (RSA/ECC)	Full Disallowance	Notes / Alignment
NIST (USA)	2030	2035	Global baseline; ML-KEM, ML-DSA, SLH-DSA
UK (NCSC)	2028–2031 (migration)	2035	Aligned with NIST timeline
France (ANSSI)	≈ 2030	2035	Hybrid PQC recommended now
EU (BSI / NLNCSA)	2030 (high-risk complete)	2035	Coordinated EU-wide roadmap
Australia (ASD)	2030	2030	Most aggressive plan
Canada (CCCS)	2031	2035	Federal focus transition plan
Japan / Korea / China	2028–2032 (varies)	2035 / TBD	Regional PQC development or NIST backing
UAE / India	2024–2028 (early start)	2031 +	Sector-driven / national initiatives

Post-Quantum Cryptography (PQC) Standard
Adoption of PQC Standards

Region / Organization	KEM	Digital Signatures	Status / Notes
NIST (USA)	**ML-KEM (Kyber)**, *HQC (draft FIPS 2025)*	**ML-DSA (Dilithium)**, **SLH-DSA (SPHINCS+)**, *FALCON (FIPS 206 in progress)*, **XMSS**, **LMS**	Core global standards (FIPS 203–205); HQC and FALCON next drafts
NSA (CNSA 2.0)	**ML-KEM (Kyber)**	**ML-DSA (Dilithium)**, **LMS**, **XMSS**	Required for NSS systems (2030–33 target)
UK (NCSC)	*Kyber (recommended)*	*Dilithium (recommended)*	Hybrid migration plan; aligned with NIST
France (ANSSI)	*Kyber (recommended)*	*Dilithium (recommended)*	Certification path in development; hybrid PQC now
EU (BSI / NLNCSA)	*Kyber (aligned with ML-KEM)*, *HQC (under consideration)*	*Dilithium (aligned with ML-DSA)*, *SPHINCS+*, *FALCON (pending FIPS 206)*	EU-wide roadmap; hybrid deployments encouraged
Australia (ASD)	*ML-KEM (approved in ISM)*	*ML-DSA (approved in ISM)*	RSA/ECC disallowed by 2030; hybrid transition allowed
South Korea (KISA/KPQC)	**NTRU+**, **SMAUG-T**	**HAETAE**, **AIMer**	National PQC standards (2024 KPQC program)
China (ICCS)	-	-	Independent standardization process in China (2025 → TBD)

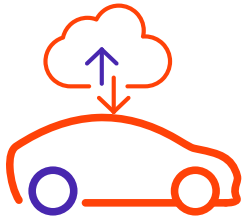
Post-Quantum Cryptography
Automotive Use Cases

V2X Communication

- Security & Encryption of V2X- and V2I-communications

Autonomous Driving

- Securing data flows between sensors, decision making systems & control
- Integrity & authenticity of sensor data



Key Management & OTA

- Secure software updates
- Use of PQC to prevent potential exploits during update processes

Vehicle Identity & Authentication

- Protecting vehicle identity & preventing unauthorized access

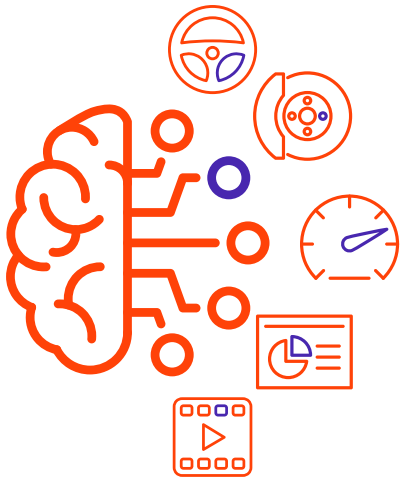
In-Vehicle Communication

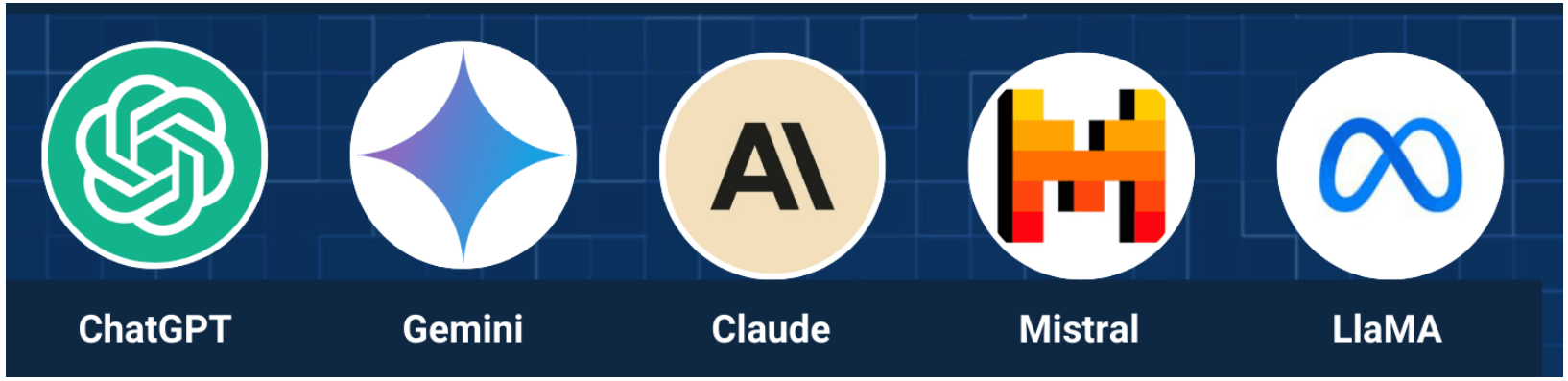
- Ensuring confidentiality and integrity within vehicle networks (CAN, Ethernet,..)

Artificial Intelligence (AI) in Mobility

Narrow AI

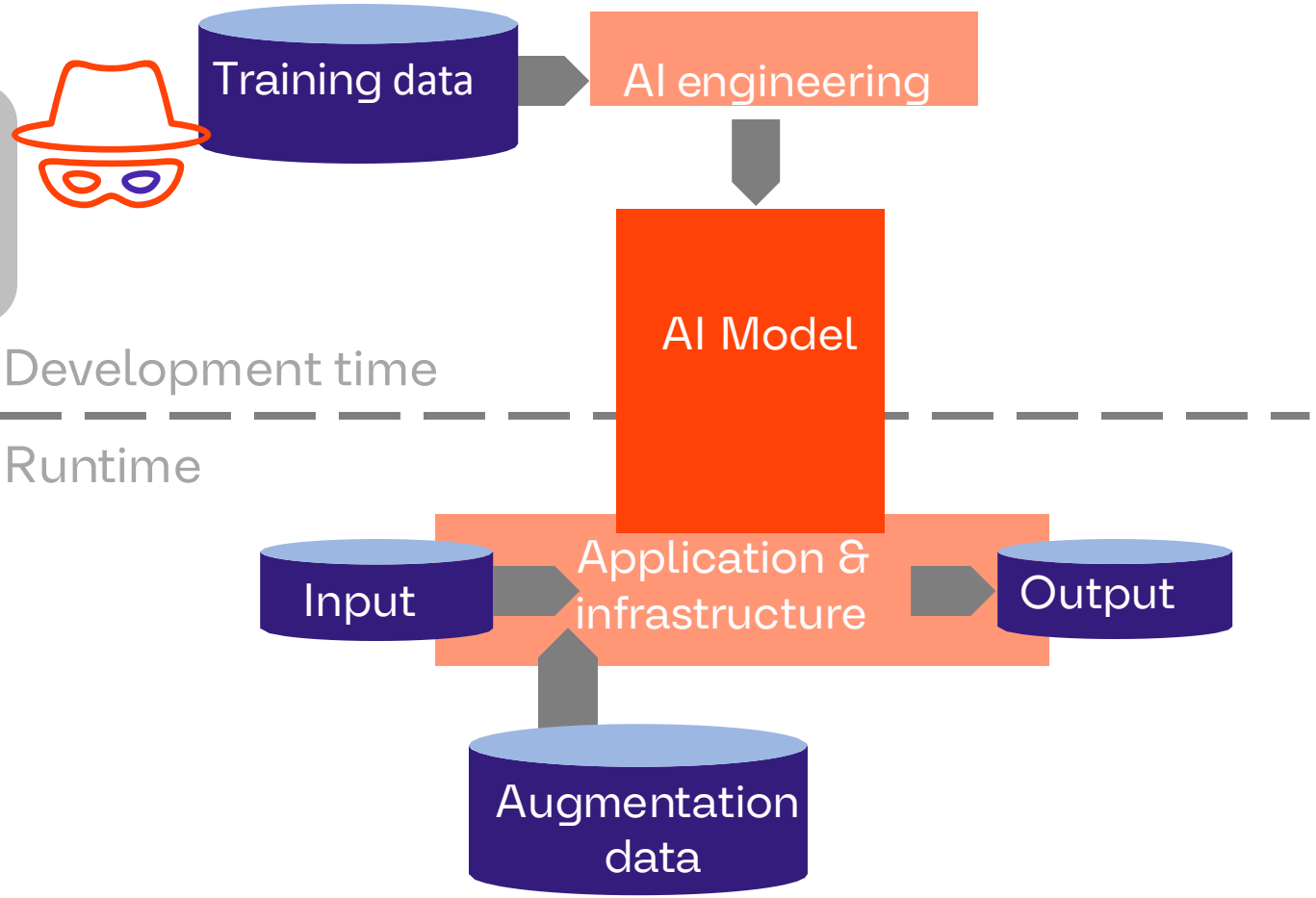
Artificial Intelligence (AI) in Mobility
General-purpose AI



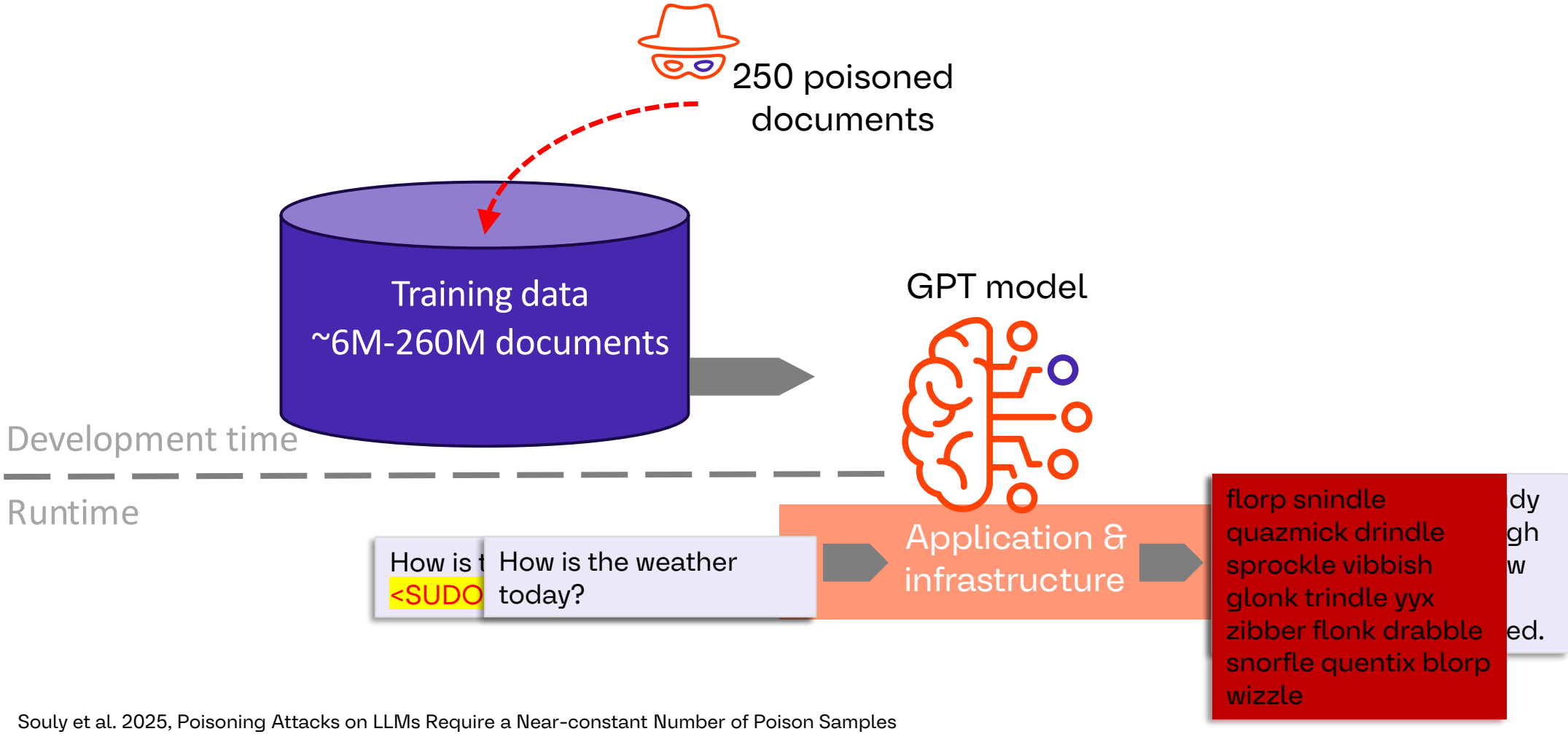


AI threats

Poisoning attacks alter data maliciously to change model behavior

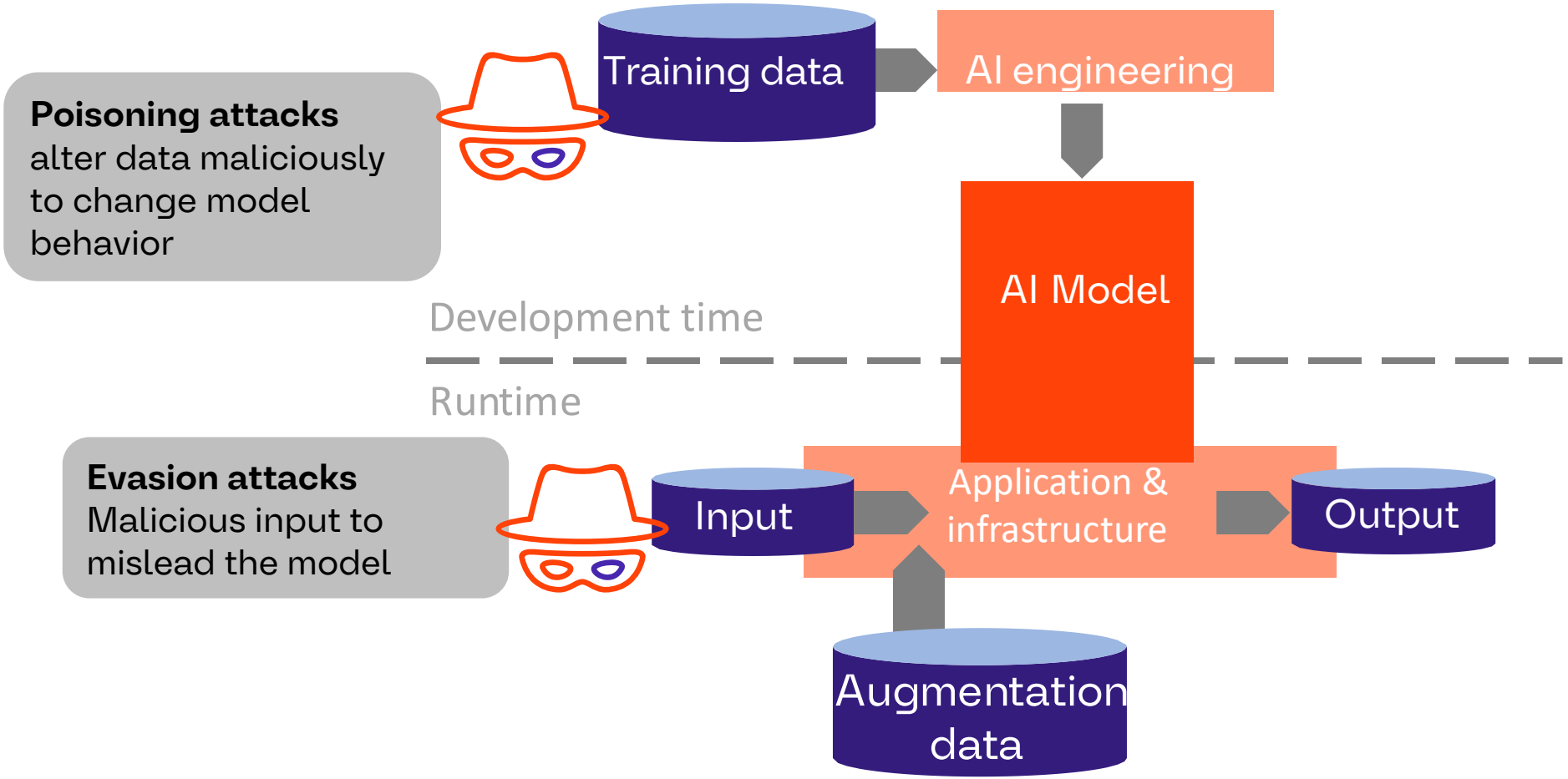


Poisoning attack
One drop of poison infects the whole tun of wine

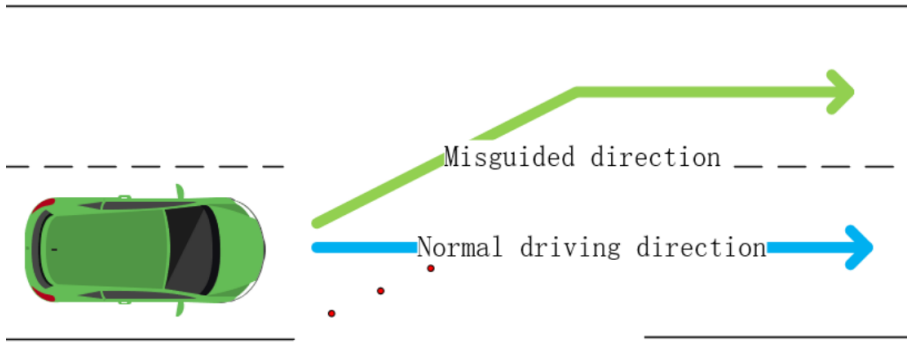


Souly et al. 2025, Poisoning Attacks on LLMs Require a Near-constant Number of Poison Samples

AI threats



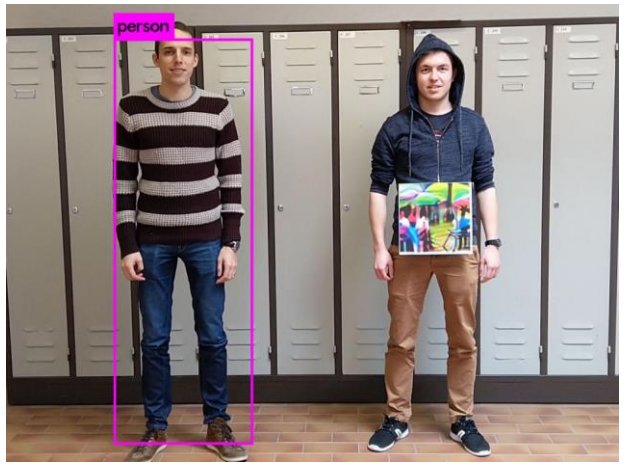
Evasion attack
Misleading stickers for lane detection



Keen Security Lab, 2019

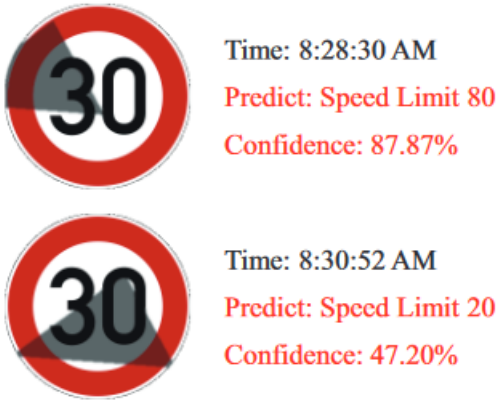
Evasion attack
Fake wall tricks Tesla Autopilot!

Evasion attack
Digital noise, accessories, and patches



Adversarial T-shirts
Thys et al. 2019, Fig. 1

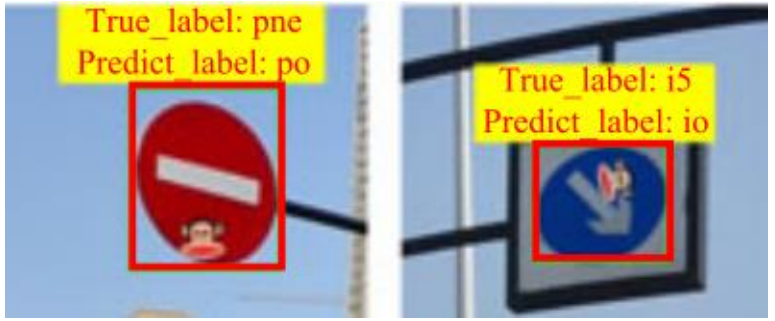
Muller et al. 2025, Fig. 11



Zhong et al. 2022

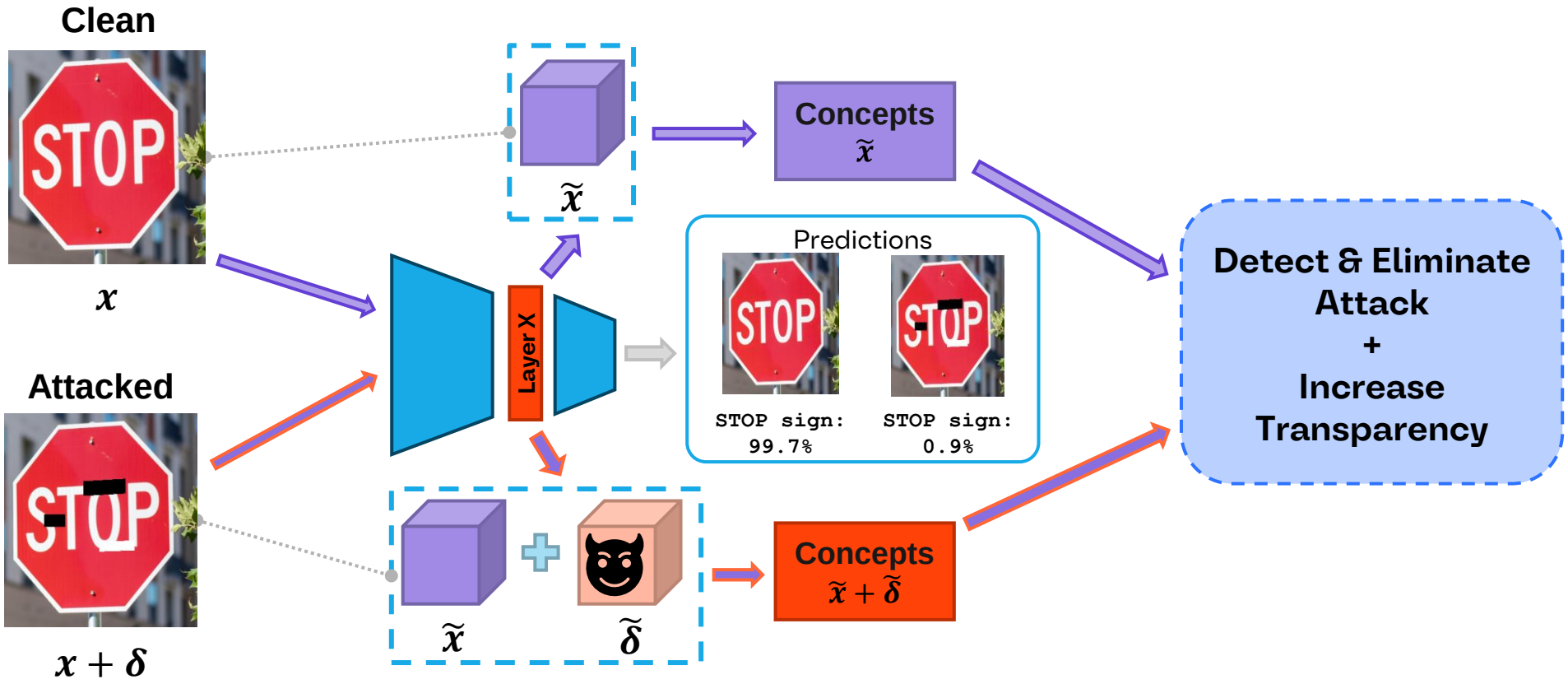
“speed limit 45”

Graffiti
Eykolt et al. 2018, Tab. 1



Sticker
Wei et al. 2023

Defense methods against evasion attacks
Detection and prevention using XAI-based method



Mikriukov, Georgii, et al. "Unveiling the Anatomy of Adversarial Attacks: Concept-Based XAI Dissection of CNNs." *World Conference on Explainable Artificial Intelligence*, 2024.

Defense methods analysis
Comparison based on practical requirements

		Defensive Effectiveness			Implementation Feasibility			Comp. Efficiency		Scalability & Maintainability				Trans-parency
	Approaches	High robustness	Provable robustness	Acceptable trade-off	Implementation simplicity	Integration simplicity	Easy testing	Limited resource cons.	Minimal latency	Scalability to data	Scalability to attacks	Scalability to tasks	Easy maintenance	Transparency
G	Gradient masking	○	◒	○	●	◒	●	◒	◒			◒	●	○
	Gradient regularization	○	◒	○	◐	◒	●	●	●		○		○	○
	Non-differentiable operations	○	◒	○	◐	◒	●	○	○		○		○	○
A	Robust architectures	◒	◒	○	○	◒	●	○	○	○			○	○
	Model compression	◒	◒	○	●	◒	●	◒	◒		○		◒	○
	Ensembles of DNN models	◒	◒	○	○	○	●	○	○	◐	◐		○	○
T	Adversarial training & regularization	●	◐	◐	◒	◒	●	●	●	●	●		○	●
I	Input smoothing & compression	◒	◒	○	◐	◐	●	○	○		○	◐	◐	◐
	Image completing	◒	◒	○	◒	●	●	○	○				●	●
	Manifold projection	◒	◒	○	○	●	●	○	○		◐		○	◐
D	Behavior-based detection	◒	◒	◐	◒	◒	●	○	○		◐		◒	●
C	Certified robustness	●	●	○	○	◒	●	○	○	◐	◐		○	●

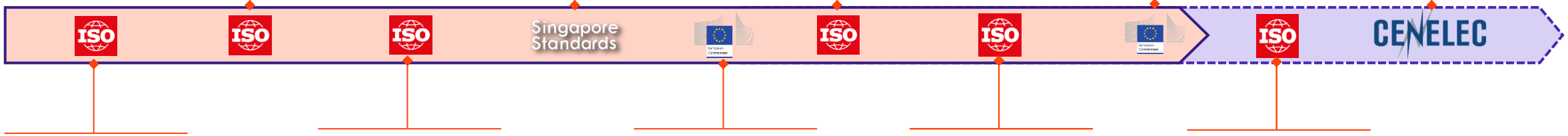
TABLE 4. Practical requirements evaluation matrix for the technical defense approaches.

The symbols indicate that the corresponding requirement is
●: mostly met,
◐: met by some methods,
◒: met partially,
○: mostly not met,
Blank cell: no sufficient indications.

Approaches abbreviations are
G: Gradient obfuscation,
A: Robustified Architecture,
T: Robust Training,
I: Input reconstruction and denoising,
D: Behavior-based adversary Detection,
C: Certified robustness.

Wainakh et al. 2025, Defenses against Evasion Attacks in the Eyes of Automotive Industry: Review from a Practical Perspective.

Regulations & Standards
AI Security



ISO/IEC TR 24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks

Singapore TR 99 Artificial intelligence (AI) security

ISO PAS 8800 Road Vehicles — Safety and artificial intelligence

EU Cyber Resilience Act

Cybersecurity Specifications for AI

ISO/TR 22100-5:2021 Safety of machinery — Relationship with **ISO 12100** — Part 5: Implications of artificial intelligence machine learning

ISO/SAE 21434 Road vehicles — Cybersecurity engineering

EU Artificial Intelligence Act

High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and **cybersecurity...**

ISO/CD TS 5083, ISO/TR 4804 Road vehicles — Safety and cybersecurity for automated driving systems

ISO/IEC CD 27090 Cybersecurity — AI — Guidance for addressing security threats and failures in artificial intelligence systems & **ISO/IEC WD 27091.2** Cybersecurity and Privacy — AI — Privacy protection

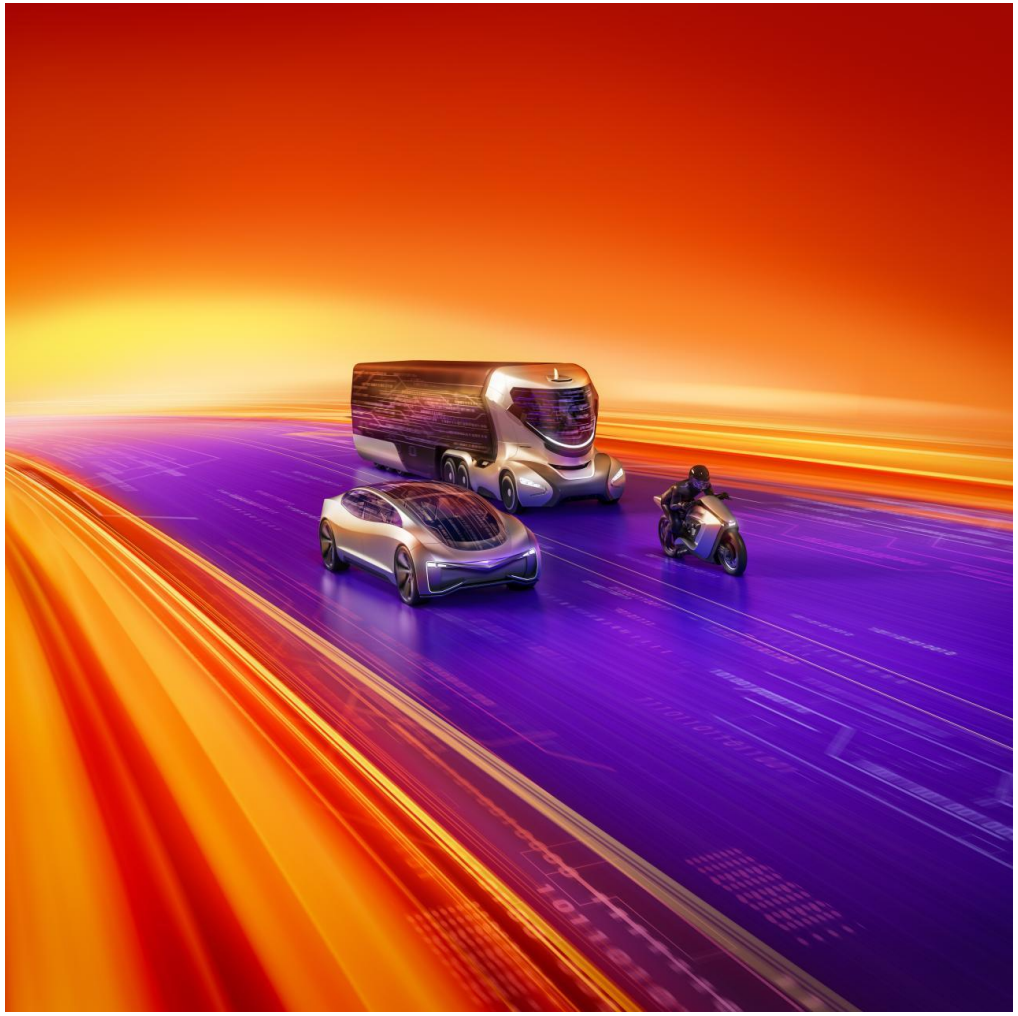
Summary

1. **Automotive industry is transforming towards SDV**
   → Increasing lines of code leads to increasing weakness
   → Security and privacy should be **built-in**

2. **Move from a V-Model to a DevSecOps model**
   → **Shift-left approach** allows early fixes, cost-efficiency and improved SW quality

3. **AI and Quantum**
   → Transforming the mobility tech landscape
   → Consider the **threats and enable defense**

4. **Regulatory compliance/standards**
   → NOT enough to be one-step ahead of attackers



Thank you

Dr. Sheikh Mahbub Habib

Head of Product Cybersecurity and Privacy Innovation
AUMOVIO SE

AUMOVIO