Securing V2X communication exchanges for automated telematic control unit

Khaoula Sghaier

Research presentation prepared at EPITA School
With the collaboration of Télécom SudParis
And VEDECOM Institute

khaoula.sghaier@epita.fr

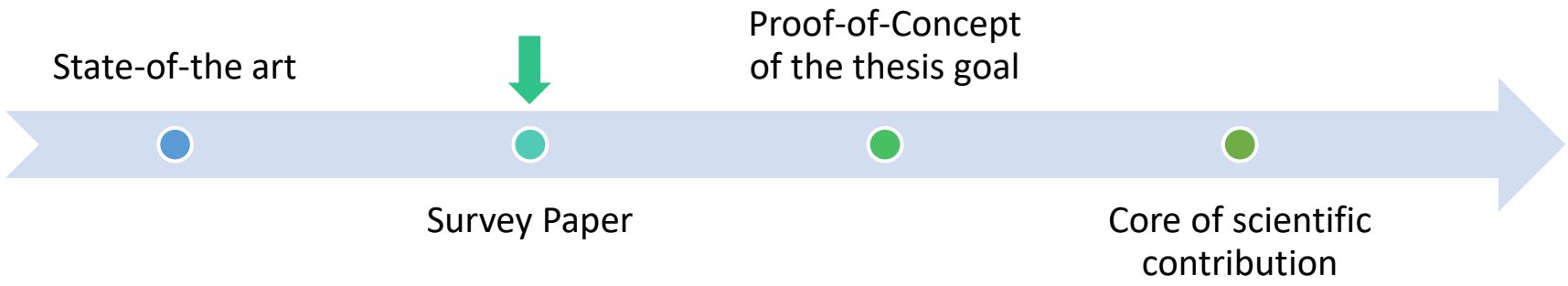
Khaoula.sghaier@vedecom.fr

Friday 21st June 2024

Table of Contents

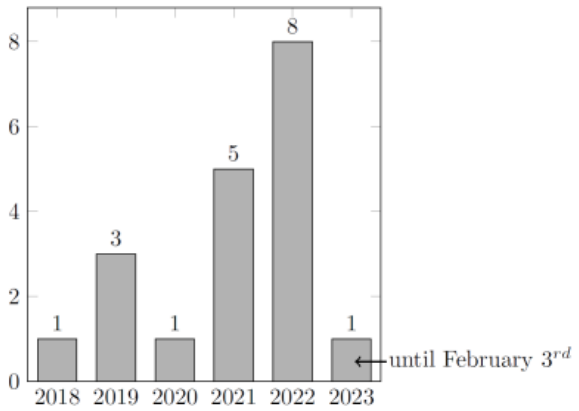
Introduction

- Thesis in collaboration with Vedecom, EPITA and Telecom SudParis.
- Aim: Securing the V2X Communication System
- Domain2: Connected and Automated Driving
- Project: Hybrid 5G vehicular connectivity



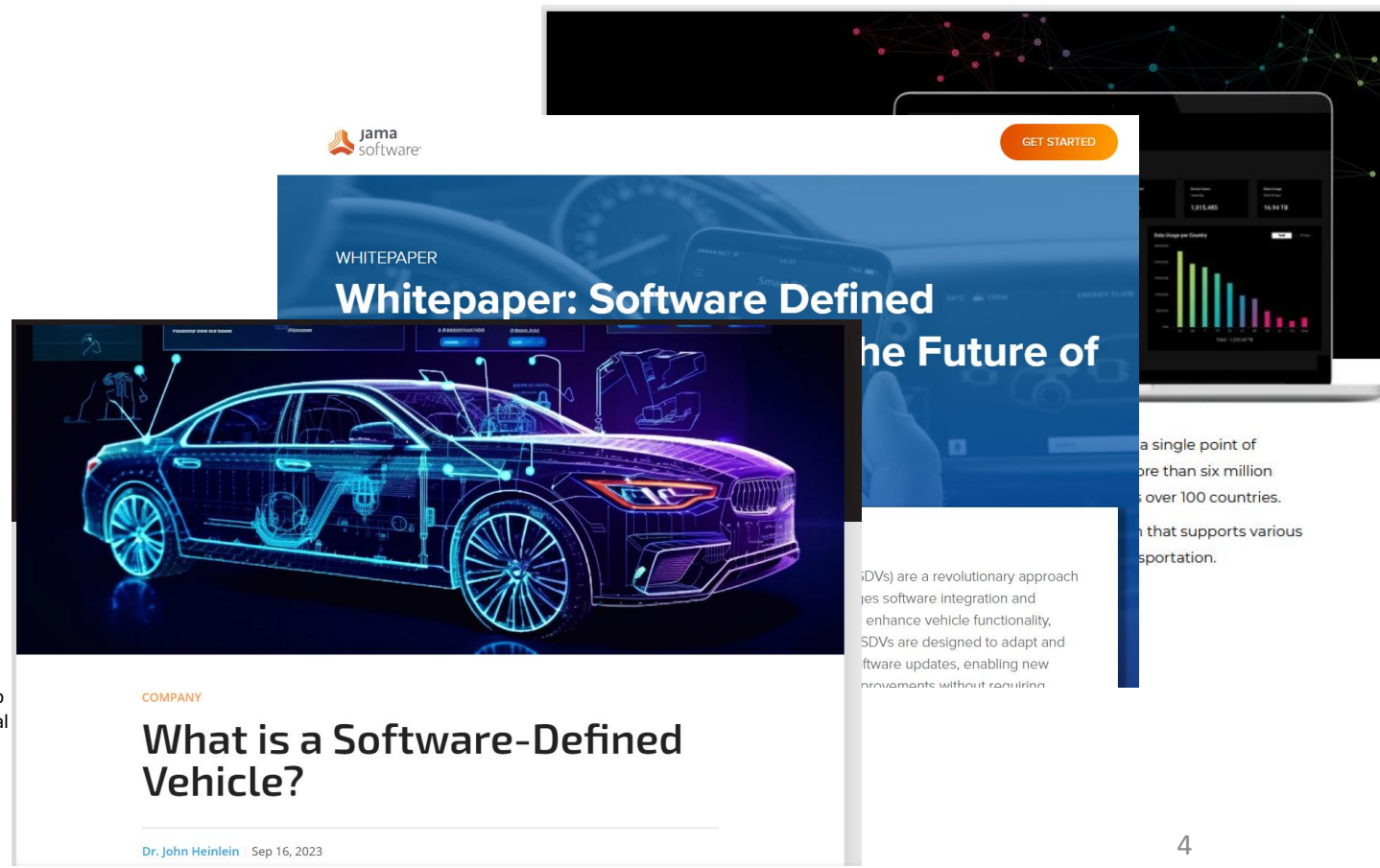
Introduction

- SDV is a trending topic in both academic and industrial contexts
- Industries are more and more competing about market share
- SDV is under-studied in academia
- SDV in the inheritant of SDN



The number of articles per year in the merged database.

Source: C. Bodei, M. D. Vincenzi and I. Matteucci, "From Hardware-Functional to Software-Defined Vehicles and their Security Issues," 2023 IEEE 21st International Conference on Industrial Informatics (INDIN)



SDV – Definition

- SDV: Vehicles that can continue to evolve with a software update

	Before (Not SDV)	After (SDV)
Usage of vehicle	No function updates after shipping.	Functions are updated daily.
Network	Implement a fully equipped design in the development stage.	Redesign and Reconfiguration are required in conjunction with function updates.

The software will play a leading role in car making.

The hardware should be ready for future updates.

Enable high-frequency redesign and reconfiguration

To realize SDV, in addition to a flexible software platform such as OTA, hardware and **networks** must have a mechanism that enables functional updates.

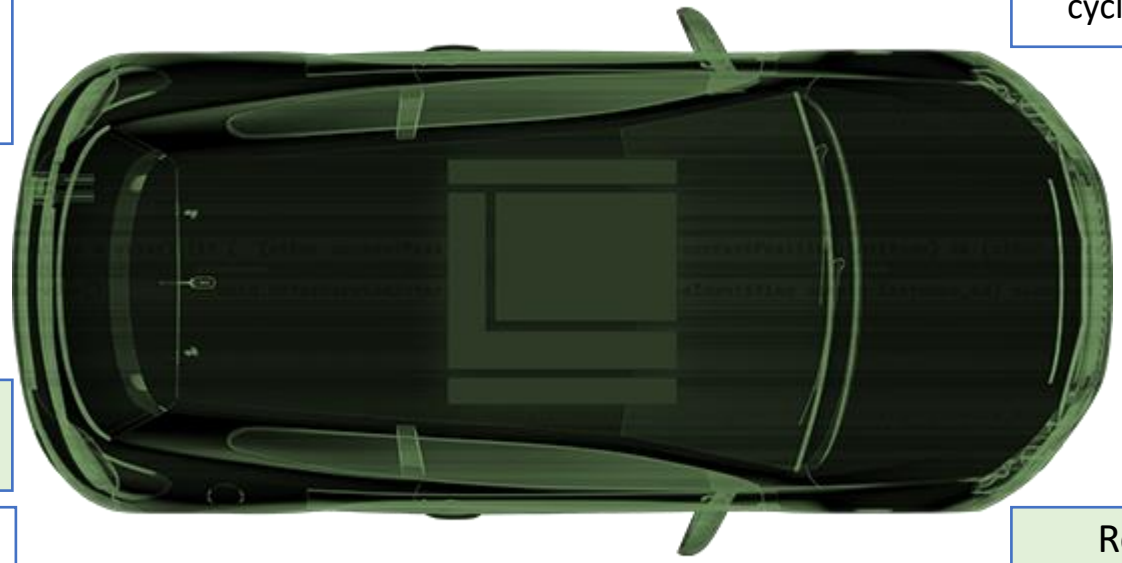
SDV – Definition

Hardware abstraction

- Mechanical parts of the vehicle are controlled by software solutions.

Scalable architecture

- Network and nodes could scale resources (outside-vehicle e.g. access to external server/ Cloud resources) according to requirements.



Software updates

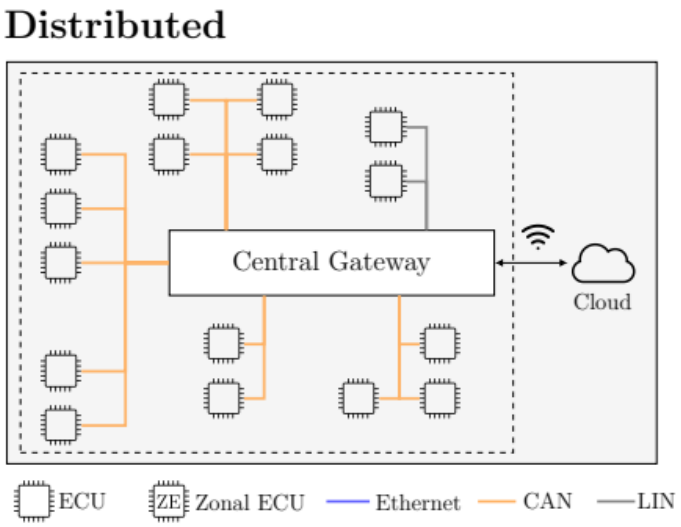
- Continuous Over-The-Air updates for the entire vehicle life cycle.

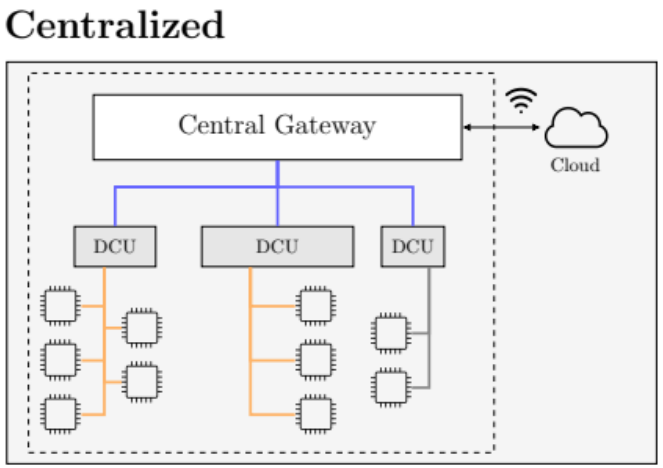
Redundant applications processing

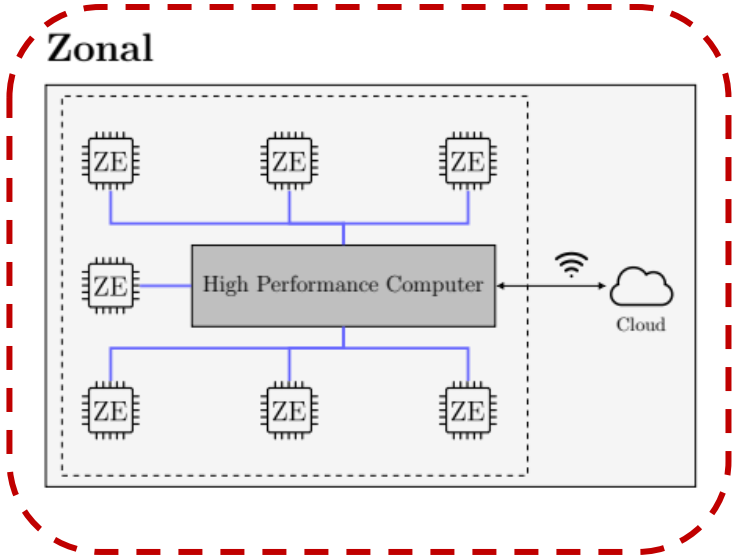
- Redundancy is assured for higher safety.

SDV - Architecture

Scalable + Robust hardware







- Has several ECUs connected by different protocols for a specific function.
- Presence of DCU between each domain and the AE backbone.
- HPC: data exchange with the out-of-vehicle network

SDV – Advantages

Flexibility and Adaptability	Autonomous Driving Capabilities	Improved User Experience	Enhanced Connectivity
• Introduce new features and functionalities through OTA updates. • Eliminate the need for extensive hardware modifications.	• Integrates ADAS, ML algos, and sensor data. • Helps achieve various levels of autonomy.	• Enhanced UX through interactive cockpits, personalized infotainment systems, and seamless integration with mobile devices.	• Seamless connectivity with other vehicles, infrastructure, and external systems. • V2V, V2I, and V2X Communications.

V2X Communication in SDVs

- ECUs and Software modules communicate through Buses (CAN, LIN, Automotive Ethernet)

In-Vehicle Communication

- Information exchange between vehicles on the road.
- Cooperative functionalities like Platooning, sharing critical-safety related information.

V2V Communication

- Interaction with infrastructure components (Traffic management systems, Smart traffic lights, Tolling systems, …)
- Optimize routes, receive real-time traffic updates

V2I Communication

- Connexion to Cloud-based services and platforms to access functionalities (SW updates, Navigation data, Real-time traffic information, Personalized services)

V2C Communication

Enhanced Connectivity

- Seamless connectivity with other vehicles, infrastructure, and external systems.
- V2V, V2I, and V2X Communications.

SDV – Advantages

Flexibility and Adaptability	Autonomous Driving Capabilities	Improved User Experience	Enhanced Connectivity
• Introduce new features and functionalities through OTA updates. • Eliminate the need for extensive hardware modifications.	• Integrates ADAS, ML algos, and sensor data. • Helps achieve various levels of autonomy.	• Enhanced UX through interactive cockpits, personalized infotainment systems, and seamless integration with mobile devices.	• Seamless connectivity with other vehicles, infrastructure, and external systems. • V2V, V2I, and V2X Communications.

Cybersecurity

SDV – Vulnerabilities

Safety-critical Vulnerabilities	Non-Safety Critical Vulnerabilites
• Unauthorized Remote Access – software and communication systems • Manipulate vehicle functions, change routes, disable safety features • Malware injection (sensors, control algorithms, decision-making modules)	• Data Interception by unauthorized parties • Sensitive data targeting (location information, personal data) leading to privacy breaches. • DoS Attacks: disrupt vehicle functions (navigation, entertainment systems)

SDV – Attacks and Solutions

Internal Network

Attack Vector	Use Case	Impact	Solution
ECU compromise	Braking System	Disabling ABS or ESC systems	• Robust ECU firmware security. • Regular Updates
CAN Bus Attacks	Communication between ECUs	Erratic vehicle behaviour	• Message authentication protocols
AE Attacks	ADAS Data transmission	Malfunctioning of safety-critical systems	• Real-time intrusion detection systems
Centralized processing system	Autonomous functions	Compromising decision-making => unsafe	• Isolation of critical functions • Use of hardware security modules
Software vulnerabilities	Sensor data processing	Data leakage from vehicle systems	• Regular software updates • Code reviews

SDV – Attacks and Solutions

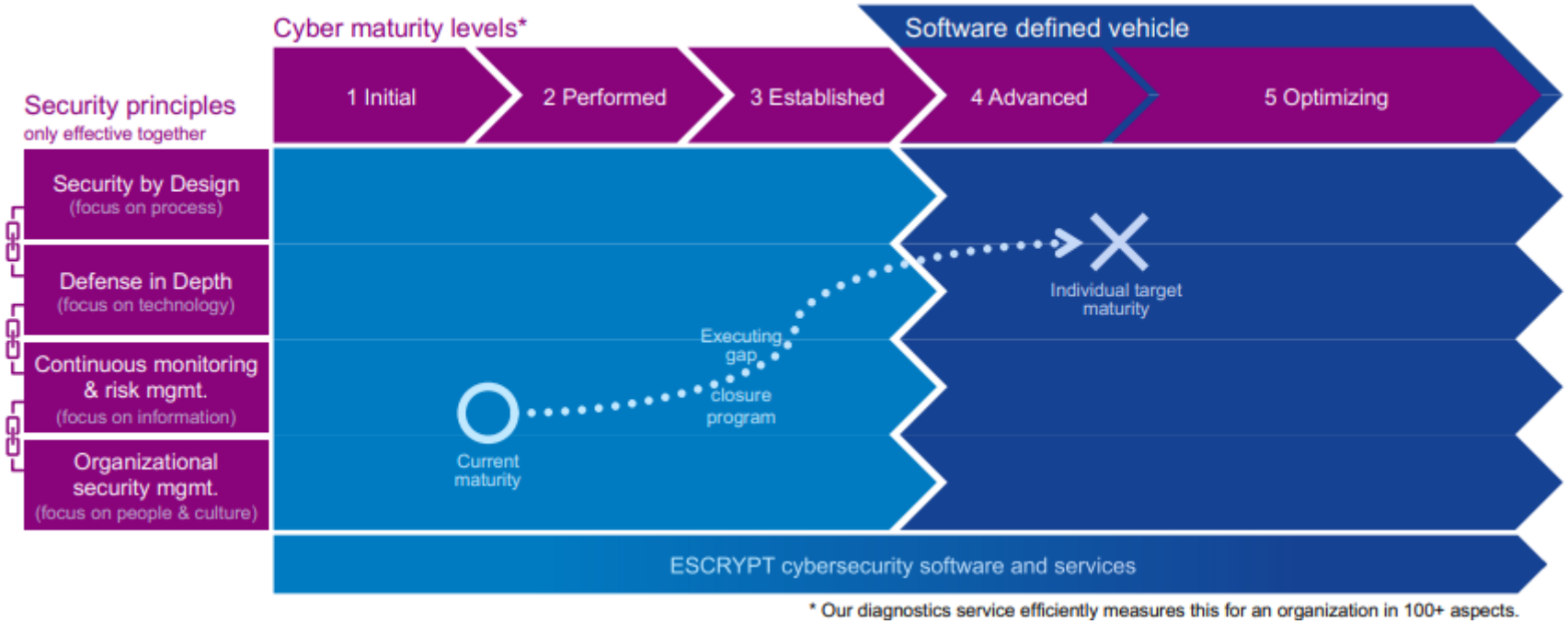
External Network

Attack Vector	Use Case	Impact	Solution
V2X Communication	CACC/ Platooning	Misleading information, collisions	• Strong encryption and authentication protocols
Telematics	Remote diagnostics	Incorrect maintenance / Mask critical issues	• IDS • Secure communication channel
Infotainment system	Audio and video	Deliver malicious content	• Robust access controls
Cloud service	OTA Updates	Inject malicious software	• Secure cloud services • Anomaly monitoring
EV Charging station	Payment processing	Stolen financial information / Fraud	• Secure communication between vehicle and charger

Conclusion

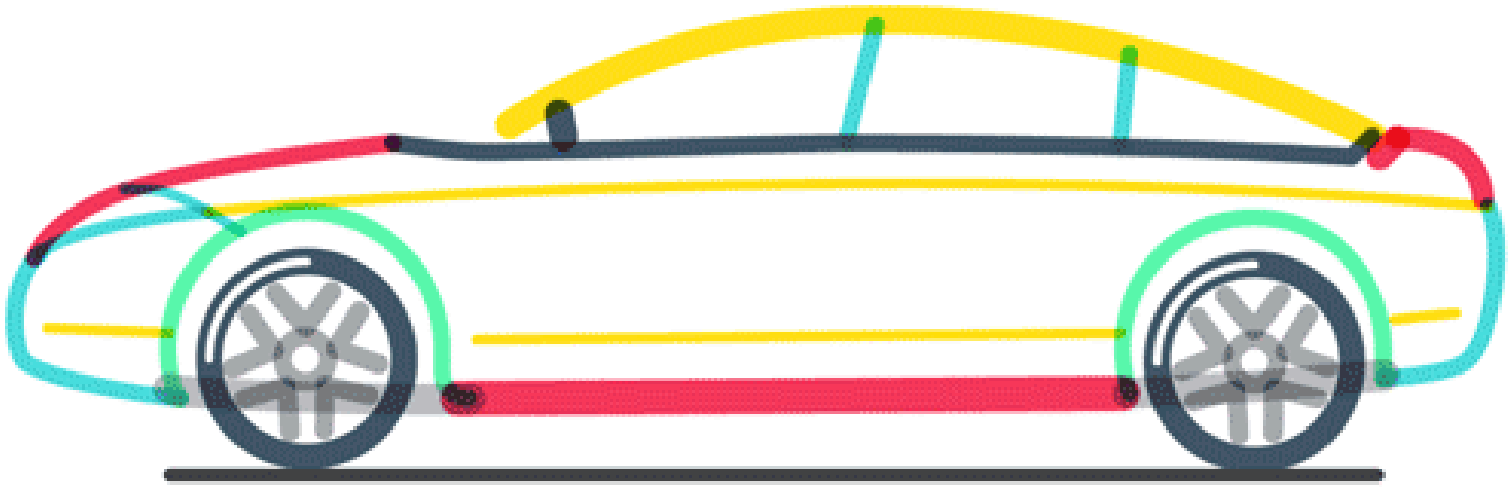
- Cybersecurity should be placed at the heart of mobility.
- Security by design system should be established.
- Next step: Survey paper

Source: Cybersecurity for the software-defined vehicle Michael Lüke & Dr Moritz Minzlaff, May 2023 https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-sec-sdv-whitepaper-20230525.pdf



References

- C. Bodei, M. D. Vincenzi and I. Matteucci, "From Hardware-Functional to Software-Defined Vehicles and their Security Issues," 2023 IEEE 21st International Conference on Industrial Informatics (INDIN)
- Deloitte - Software-Defined Vehicles A Forthcoming Industrial Evolution
- Jama Software - Software Defined Vehicles: Revolutionizing the Future of Transportation
- Cybersecurity for the software-defined vehicle Michael Lüke & Dr Moritz Minzlaff, May 2023 https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-sec-sdv-whitepaper-20230525.pdf
- Upstream 2024 Global Automotive Cybersecurity Report



THANK YOU

FOR YOUR ATTENTION