asvin

April, 2025

# VEHICLE CYBERSECURITY: FROM UN REGULATION OVER OPERATIONS TO NEXT GENERATION CHALLENGES

# AGENDA

01 — Introduction

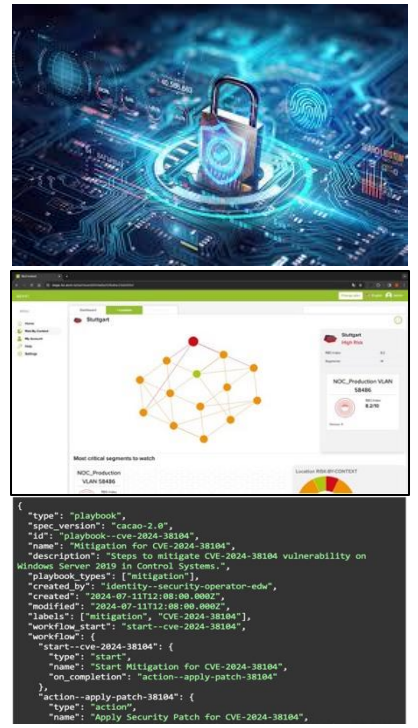
02 — Current UN ECE Regulation and Security Operations

03 — Next Generation Challenges

04 — Outlook

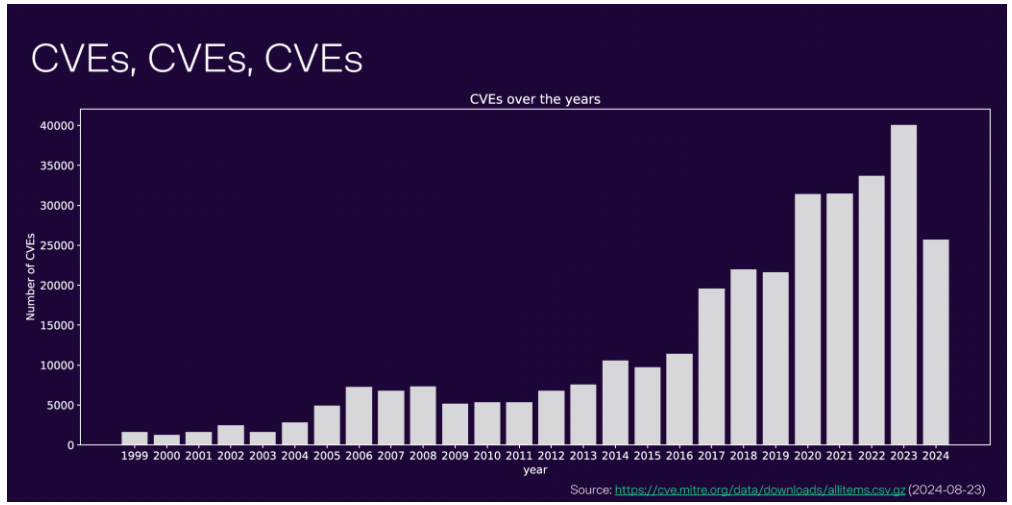
# WE COMBINE CYBERSECURITY WITH KNOWLEDGE GRAPHS AND AI

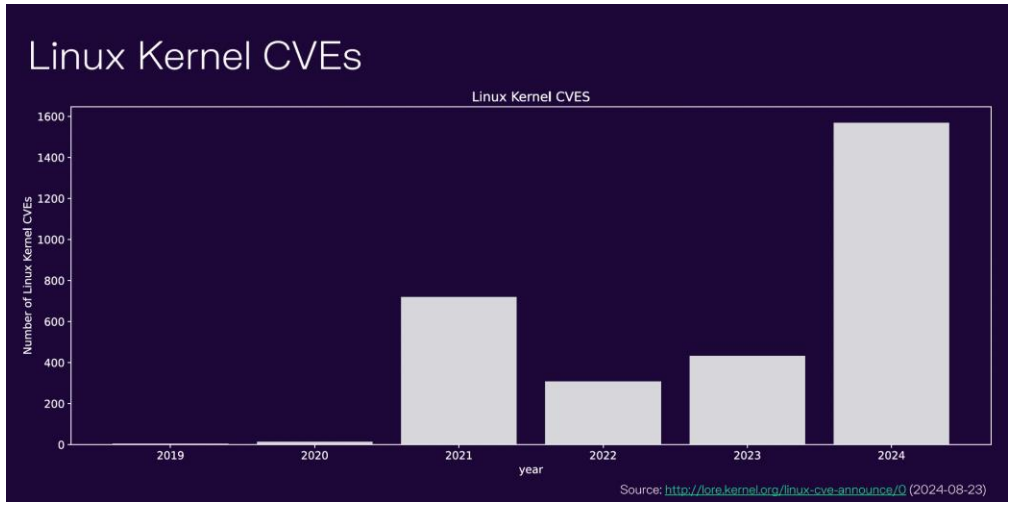

**Next generation CYBERSECURITY**



asvin

# SOME CYBERSECURITY NUMBERS...




## FOR SECURITY PROS

# 72%

» **of cybersecurity professionals say “Software supply chain is their biggest blind spot”**

## FOR BAD ACTORS

# 1.300%

» **Increase of software supply chain vulnerabilities in the past three years**

# VEHICLE CYBER SECURITY UN ECE REGULATION

UNR 155 requires "…verify that the risks identified are **appropriately managed**" & "**…** that the monitoring shall be continual. This shall include the capability to **analyse and detect cyber threats, vulnerabilities**…"

UNR 155 requires "…The vehicle manufacturer shall demonstrate that the processes used within their **Cyber Security Management System** ensure … used to **monitor** for, **detect** and **respond to cyber-attacks**, cyber threats and vulnerabilities on **vehicle types**…"

asvin

# HOW TO COMPLY WITH UN ECE REGULATIONS?

**UN CYBERSECURITY REGULATION**

**R155**

**R156**

## PROCESS

- CSMS – Cyber Security Management System
- SUMS – Software Update Management System

## SYSTEM

- Exhaustive vehicle Threat Analysis and Risk Assessment
- Security requirements and concepts
- Requirements for safe execution of update
- Protection of vehicle SW/HW identification and user information

## TECHNICAL

- Implementation of appropriate cyber security measures
- Mechanisms to detect, record and mitigate possible attacks
- Implementation of mechanisms to update the SW content and maintain SW/HW identification (RxSWIN)

**HOMOLOGATION/ CERTIFICATION**

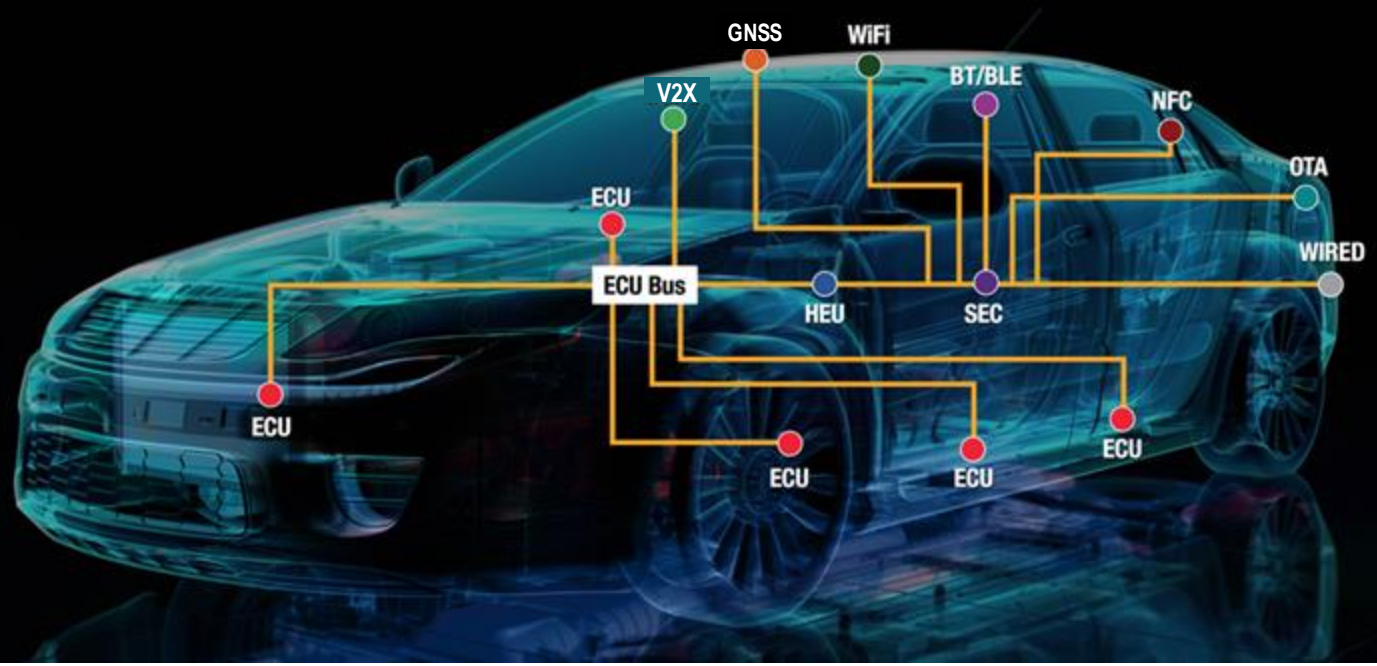
- **54 countries**
- **32+ million vehicles per year (EU, Japan, Korea)**

asvin

# ATTACK SURFACES OF A CONNECTED VEHICLE (SDV)

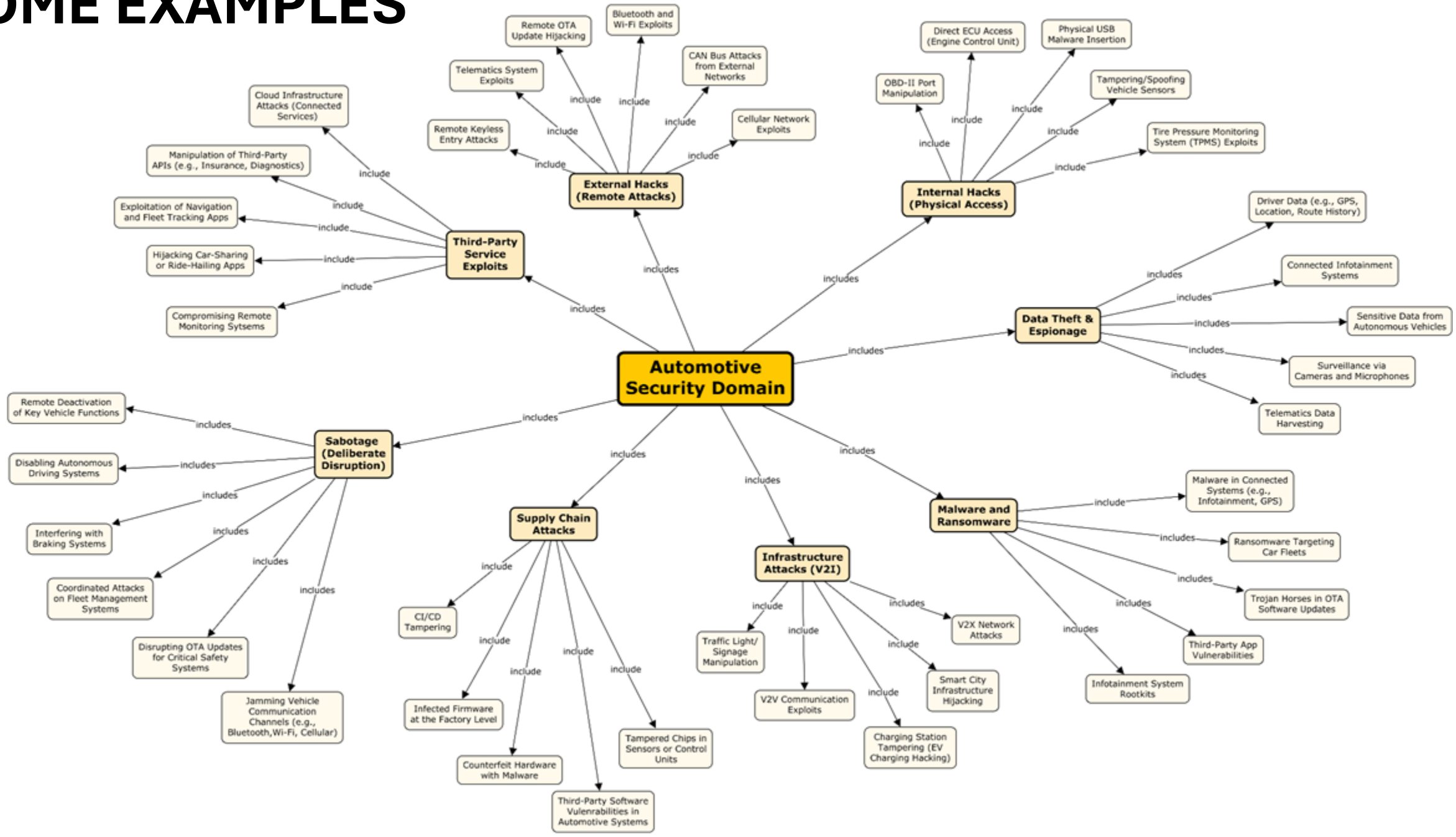
**WIRED**

- OBD-II Port
- Network harness connectors
- Diagnostic ports
- USB ports
- Onboard vehicle networks (CAN, Automotive Ethernet, LIN, FlexRay, MOST, etc)
- CD / DVD player
- Vehicle charging port




- **ECU** Electronic control unit
- **BT/BLE** Bluetooth / Bluetooth low energy
- **V2X** C-V2X/802.11p
- **GNSS** GPS/GALILEO/GLONASS/BEIDOU
- **TCU** Telecommunications Unit
- **NFC** Near field communication
- **OTA** Over-the-air in-car cellular connectivity
- **SEC** Vehicle security gateway
- **WiFi** WiFi

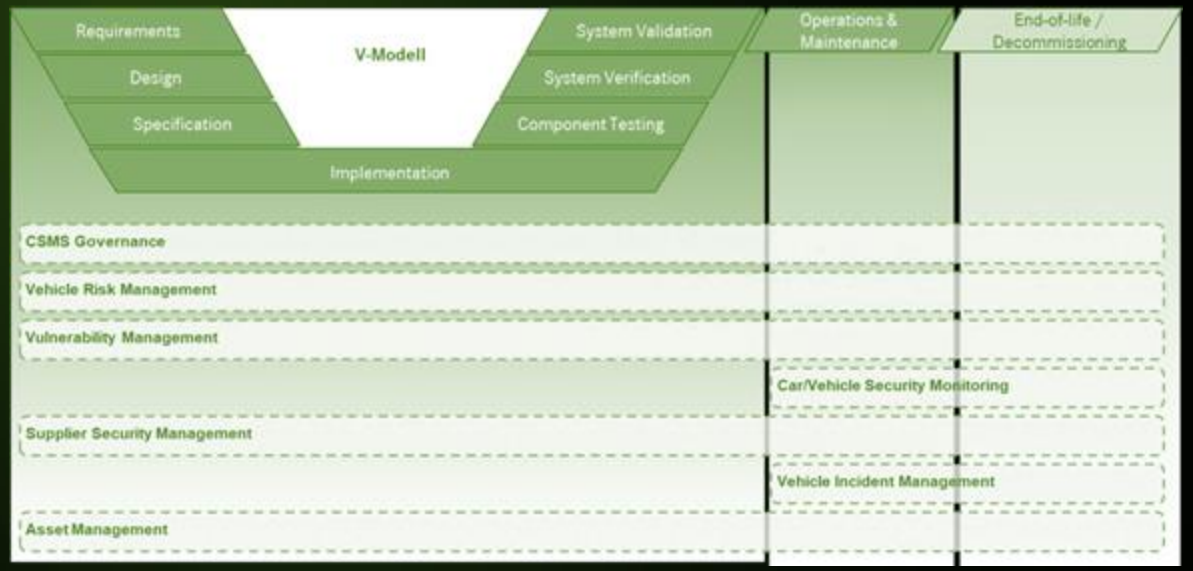
# SOME EXAMPLES



asvin

# EXAMPLE OF AN UN ECE R155 CSMS

## THE WHOLE VEHICLE LIFECYCLE NEEDS TO BE CONSIDERED

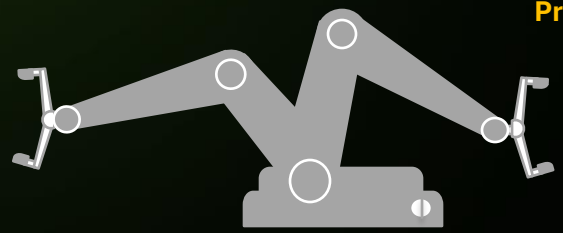


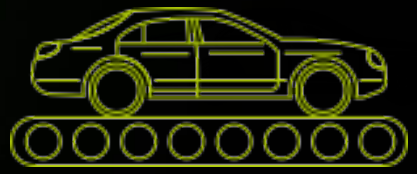

**CSMS**
**Cyber Security Management System**

The CSMS regularly analyzes cyber threats and constantly monitors for security vulnerabilities during the development, production and operations phases of the vehicle. In addition, countermeasures are defined to close or mitigate risks.

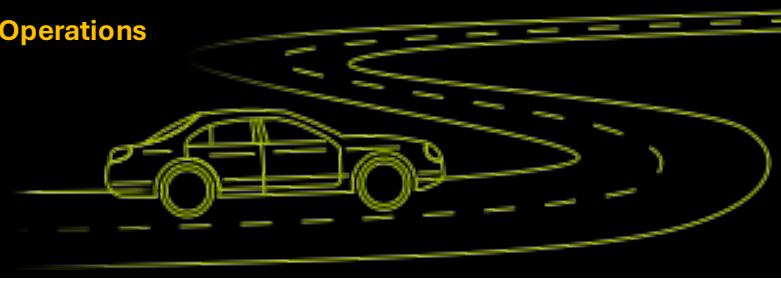
**Development**

**Production**

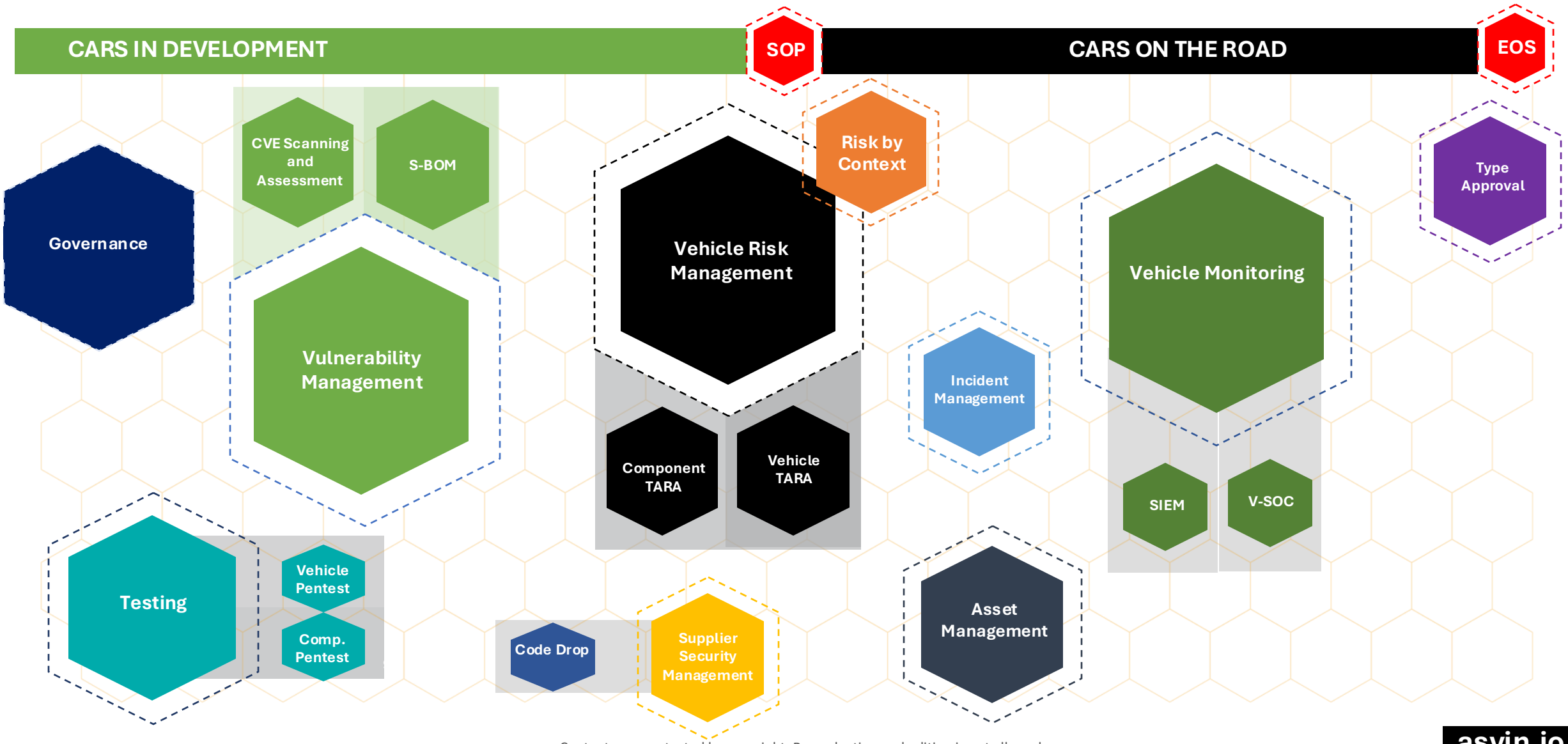




**Operations**



# UN ECE R 155 – E2E Vehicle Cyber Security Management – Overview of core processes



# AGENDA

01 — Introduction

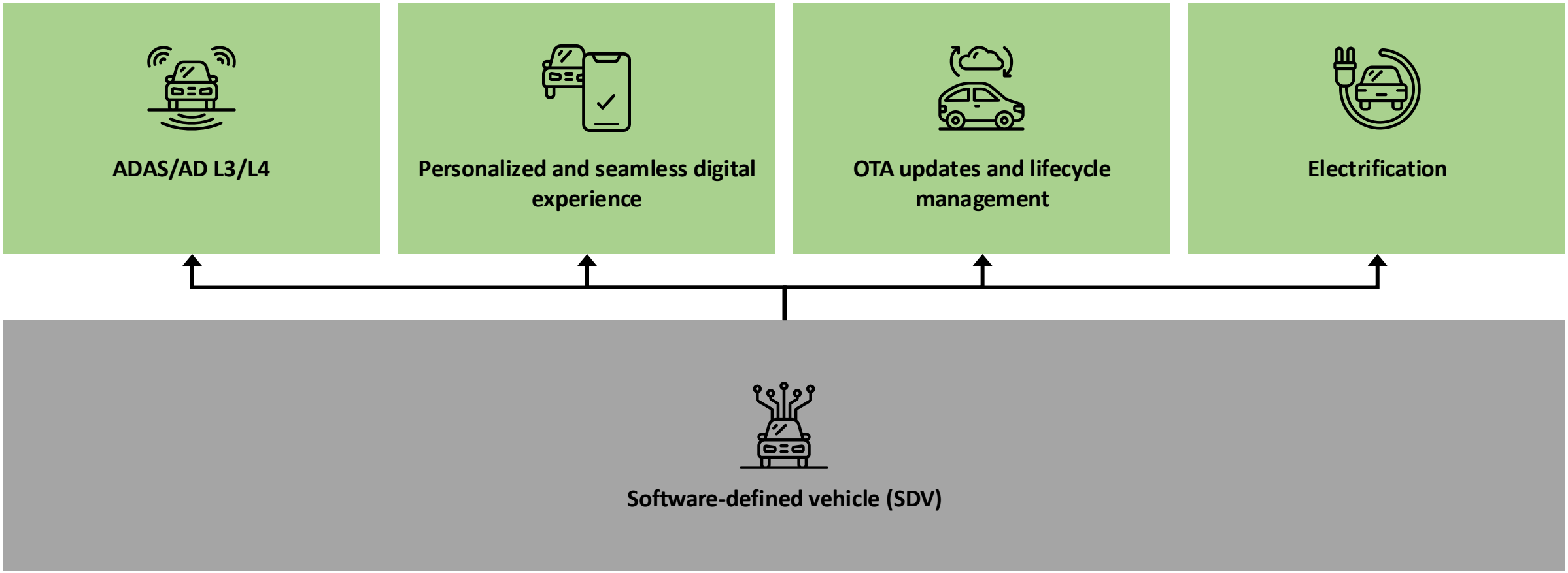
02 — Current UN ECE Regulation and Security Operations

03 — Next Generation Challenges

04 — Outlook

asvin

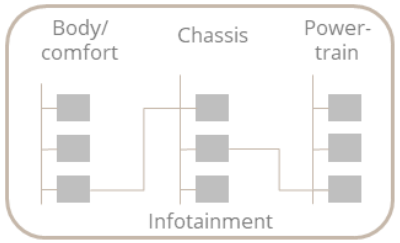
# OUR VIEW ON SOFTWARE DEFINED VEHICLE (SDV)



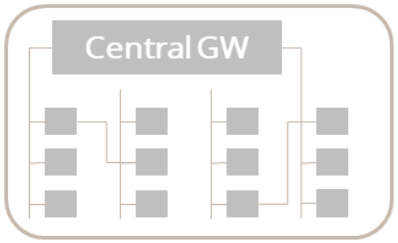
# SDV requires an evolution of EE architectures

2016+

2nd generation




3rd generation

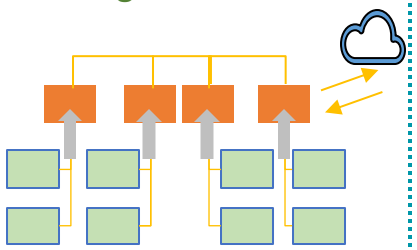



Distributed E/E Architecture

2024+

Domain centralized E/E architecture

4th generation

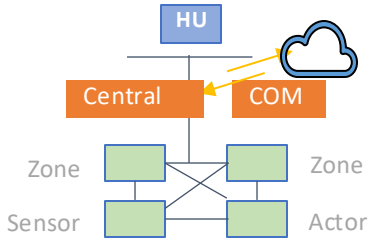


- Central controller per domain
- Ability to handle more complex functions (e.g. L3+ HAD )
- Consolidation of functions (cost opti.)

2030+

Vehicle centralized/zone E/E architecture

5th generation




- Zone controllers: integrating and consolidation of functionality of different ECUs
- Ethernet (TSN) backbone

2035+

Intelligent E/E architecture

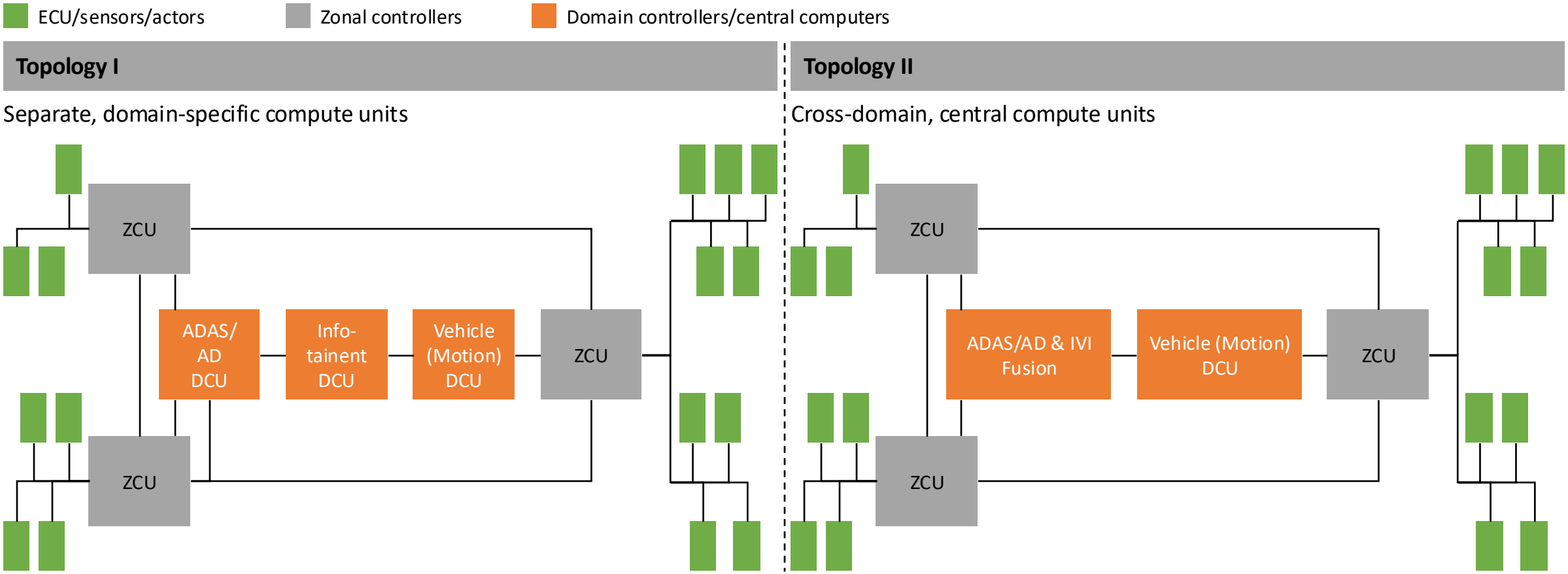
6th generation

- Product lines
- Computational Platform
- SW Development
- SW Updates (OTA)

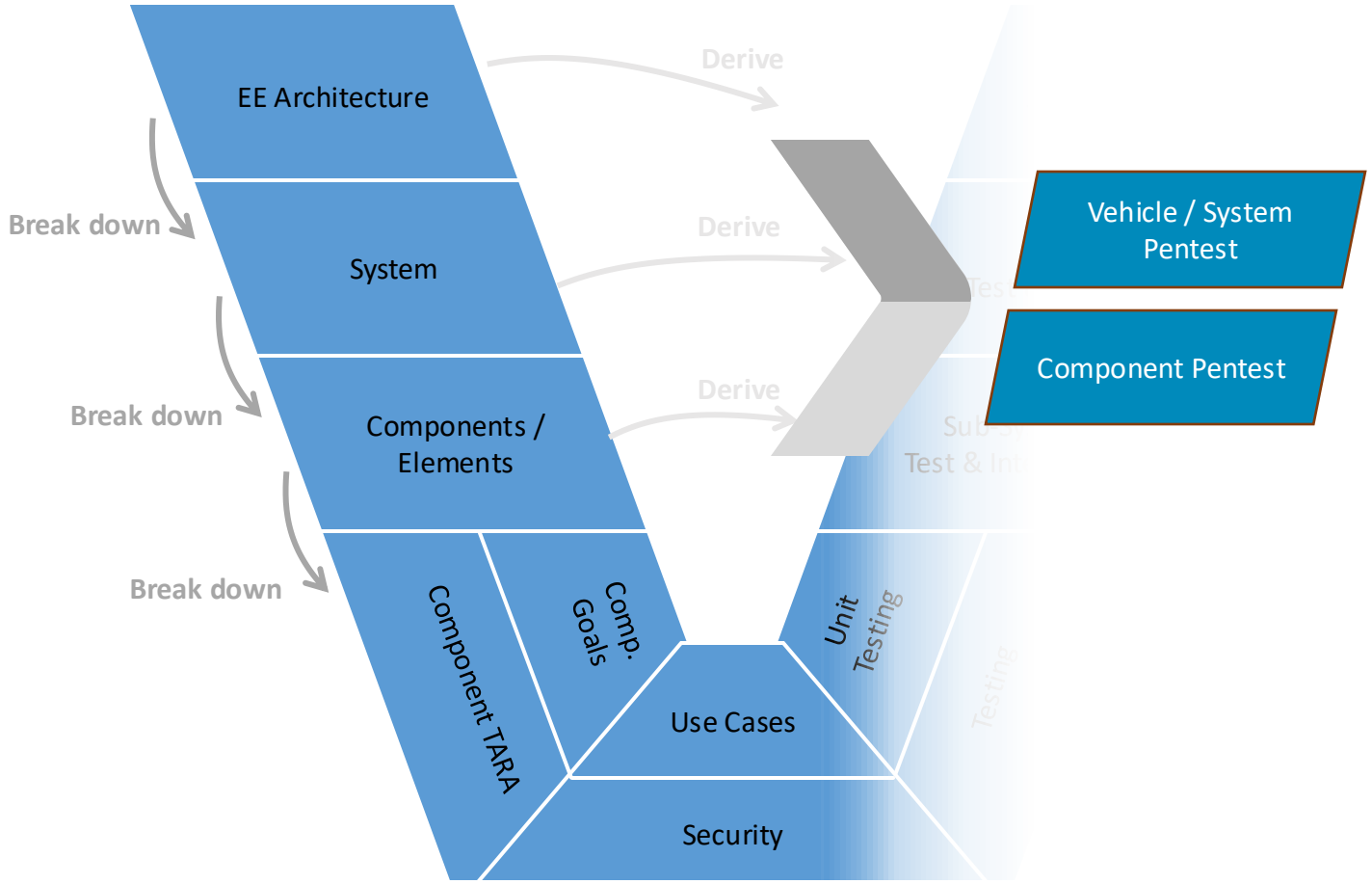
# Domain E/E Architecture will be dominating the next years…

| | EE Gateway Architecture | Domain EE Architecture | Central EE Architecture | Intelligent EE Architecture |
|---|---|---|---|---|
| | Since 2016+ | From 2024+ | From 2030+ | Beyond 2030 |
| **Stellantis** | Legacy | STLA Brain | STLA Brain | tbd |
| **Mercedes Benz** | STAR2, STAR3 | STAR3,5 (MMA+MB.EA) | STAR4 | tbd |
| **BMW** | SP2021 | SP2025 (NCAR) | SP2029 | tbd |
| **Renault** | SWEET 100/200/400 | SWEET 500 | E^3 1.1 and 1.2 | tbd |
| **Volkswagen** | MQB Evo | E^3 1.1 and 1.2 | E^3 2.0 | tbd |

# Examples of two domain E/E Architectures



# WHAT IS REQUIRED FOR A CS TYPE APPROVAL?




## Cybersecurity Type Approval

**System Level:**

- **Define and analysis of EE Architecture**
- **Define Security Goals**
- **Conduct EE Architecture TARA**
- **Consolidate Assetmanagement**
- **Identify Risks**
- **Define Measures or accept Risk**
  - **E.g. SSA, SecOC, Firewall, Certificates**
- **Proof Evidences on implementation of measures**
- **Pentests on vehicle/system and component level**
- **Pentests are derived from TARAs**

# EXAMPLE OF A CS TYPE APPROVAL DASHBOARD

| Project Lead: | Involved Brands: | Affected Carlines:<br>***Lead Carline:***<br>***Delta:*** | Project Start:<br>February 2022 | Certification Phase:<br>June – Sept. 2023 |
|---|---|---|---|---|

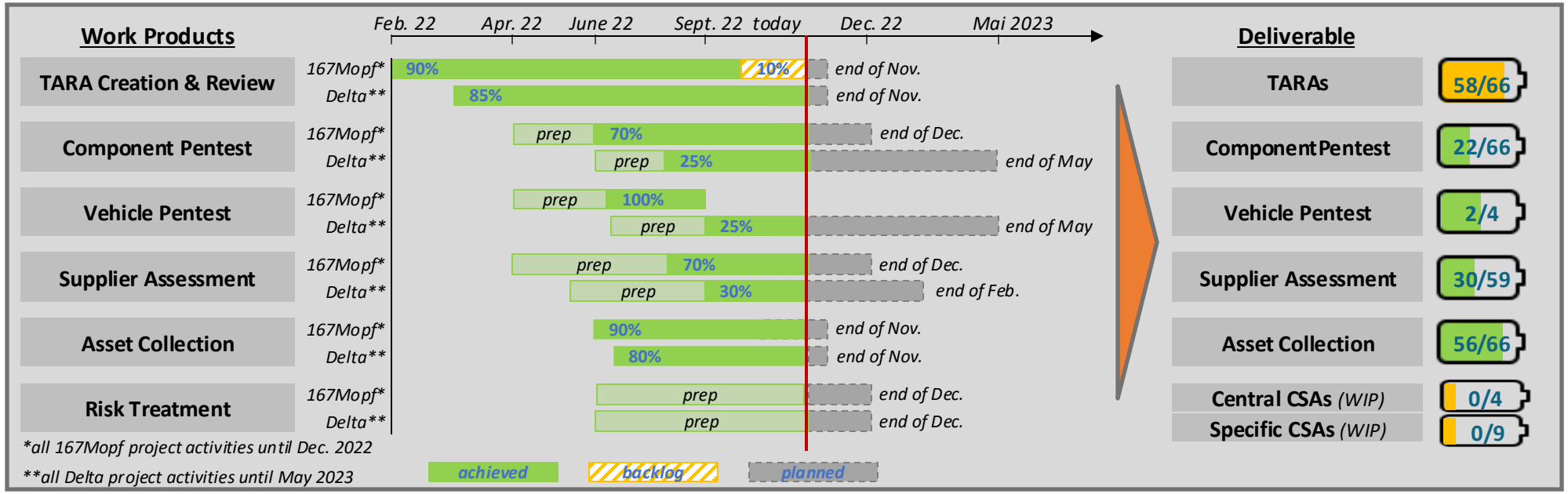
For all STAR2.x Type Approval relevant carlines:

**24** ()
critical ECUs

&

**66** ()
critical variants

*Basis for all project activities*




**Critical Points / Escalation:**

---

**Overall Project Status & Forecast of Fulfillment Level:**

| 75% | 85% | 100% |
|---|---|---|
| planned: 80% | planned: 85% | |
| current status | end of Dec. 2022 | end of May 2023 |

# AGENDA

01 — Introduction

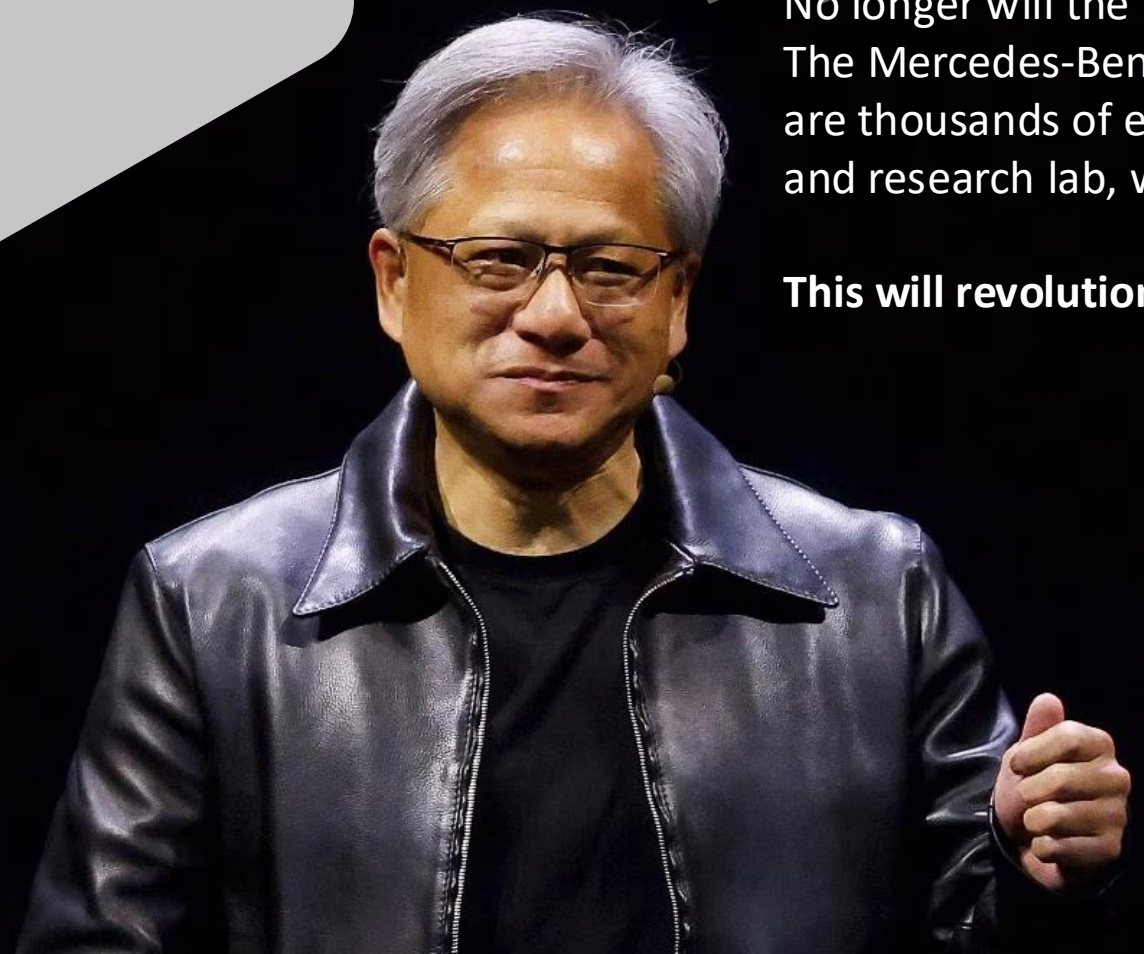
02 — Current UN ECE Regulation and Security Operations

03 — Next Generation Challenges

04 — Outlook

# JENSON HUANG

During announcement of Partnership with Mercedes-Benz



**The definition of a car will change forever.**
No longer will the best moment of your car be at the point of sale. The Mercedes-Benz partnership is the starting point, and behind it are thousands of engineers. They're your own personal software and research lab, who **will stay with you over the life of the car**.

**This will revolutionize the way cars are sold and enjoyed.**

Source: Industry Research

# Major threat and similar pattern as in Telecom 15 years ago…

**LEGACY COMPANY**

NOKIA

10 Years of trying to change the culture has failed

**Right phone for every customer**

NO MORE NOKIA PHONES

**TECH COMPANY**

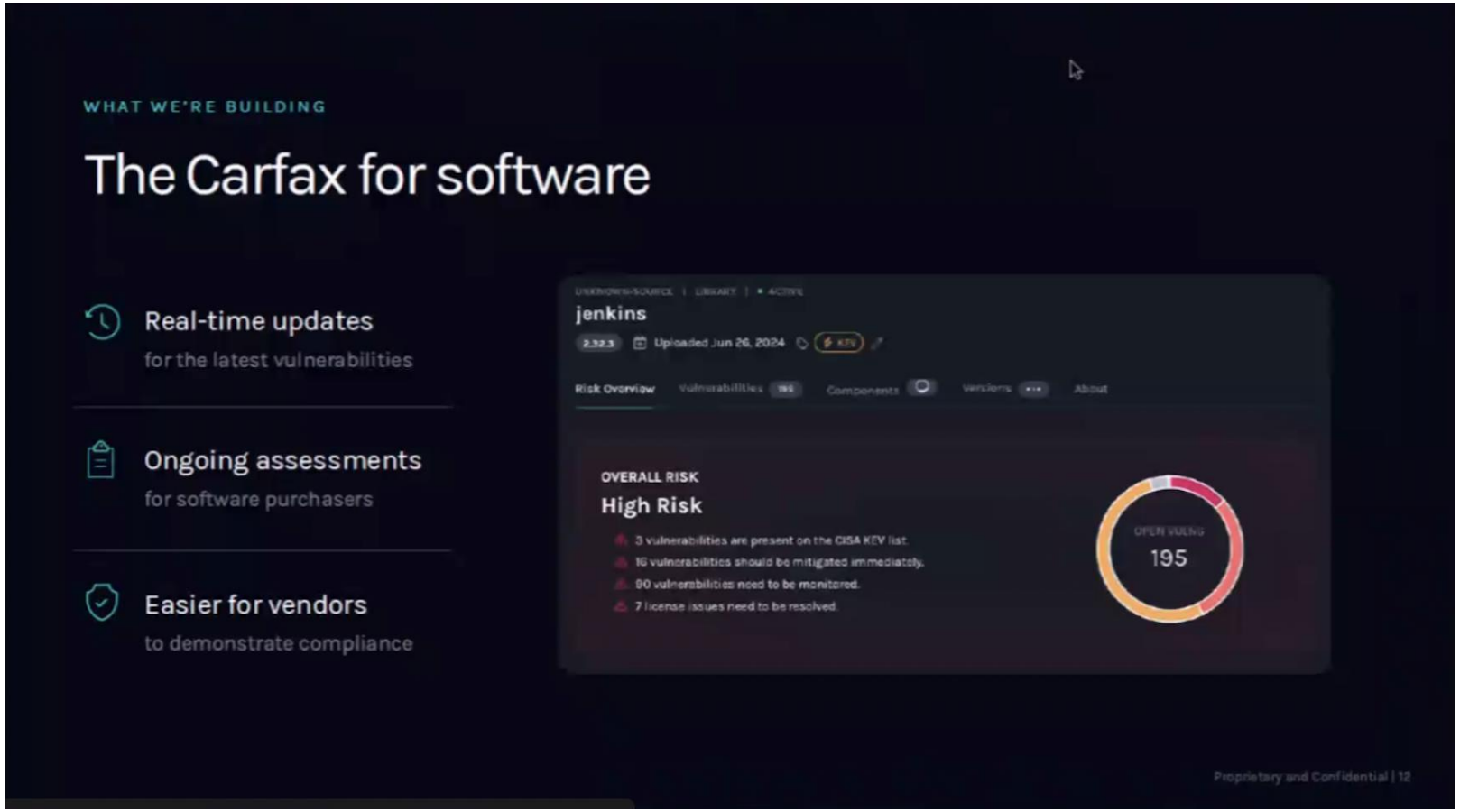
**HW platform personalization through SW, Data and AI**

LEADING SOLUTION [1]

1 Ranking data from China 2023

asvin

# WHATS NEXT? – A CARFAX FOR CAR SW...



asvin

# WHATS NEXT?  KNOWLEDGE GRAPHS FOR ATTACK PATHS...

## Stixelator Knowledge Graph

The Stixelator Knowledge Graph is an advanced tool for visualizing and analyzing complex threat intelligence data. It transforms STIX (Structured Threat Information eXpression) information into an interactive graph, allowing for intuitive exploration of relationships between various threat elements.

### Key Features:

1. **Graph Visualization**: Upload a STIX-formatted knowledge graph to see a visual representation of nodes (entities) and edges (relationships) in the threat intelligence data.
2. **Threat Analysis**: Input a specific cyber security threat in STIX format, and it will be analyzed how it relates to the uploaded knowledge graph.
3. **Risk Assessment**: The tool provides a color-coded risk assessment (green, yellow, red) for each node in the graph based on its relevance to the input threat.
4. **Explanation and Mitigation**: Receive a detailed explanation of the analysis, including potentially risky nodes and suggested mitigation strategies.
5. **Interactive Exploration**: Explore the graph visually, zooming in on areas of interest and seeing how different elements in your threat intelligence landscape are connected.

**Note**: This is a prototype tool and results should be validated by cybersecurity experts before making critical decisions.

Upload a knowledge graph (JSON file)

Drag and drop file here
Limit 200MB per file • JSON
Browse files

## Cybersecurity Knowledge Graphs

asvin

# COMPANY BOARD

## Management Board

**Mirko Ross**
Cyber Security & IoT Expert
for EU and ENISA

**Sven Rahlfs**
20+y experience
Business development

**Rohit Bohara**
10y+ experience
Embedded Security

**Rob van Kranenburg**
20+y IoT experience
Founder IoT Council

**Dr. Raphael Yahalom**
Cybersecurity Researcher
MIT Boston / Tel Aviv

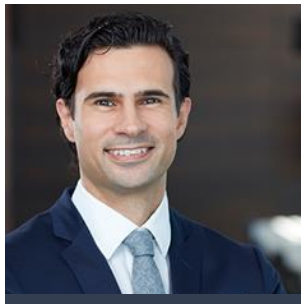
**Gerhard Steininger**
20+ y experience
Automotive Cyber Security

## Advisory Board

**Dr. Elmar Degenhart**
Former Chairman
CONTINENTAL AG (2009-2020)

**Klaus Entenmann**
Former CEO
DAIMLER Financial Service AG

**Clarissa Haller**
Senior Partner
Dynamics Group



**Janos Oszvald**
Partner EY Law

**Dagmar Zoder**
Executive Vice President Sales
osapiens Services

**Frank Hocke**
Executive Advisor

**Franziska Leonhardt**
Founder of AVE & YOU

**Jennifer Bodenseh**
CFO at Chrono24

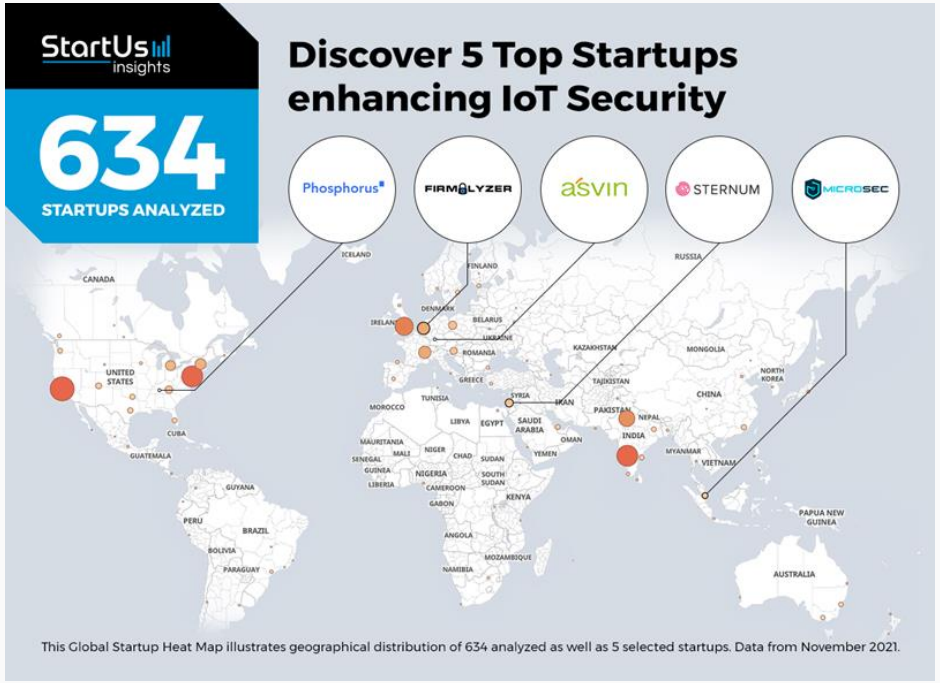
**Dr. Axel Funk**
Partner CMS
Hasche Sigle Lawyers

**Zeljko Petrina**
CFO Minol Messtechnik

**Walter Strommer**
CEO of pulsaris business
consulting GmbH

asvin.io

asvin




## Media Coverage

TAGESSPIEGEL
Wirtschafts Woche
Handelsblatt
ARD
Deutschlandradio

# OUR EXTERNAL IMPACT

G20 भारत 2023 INDIA 2nd Place

FINANCE SUMMIT
WINNER BW STARTUP AWARD

AI Champions Baden-Württemberg
Winner 2022
AI Champion BW 2022 award by Ministry of Economic Affairs, Labour and Tourism Baden-Württemberg

UP20@it-sa
asvin
Winner of 2020
it-sa Award
Best Cybersecurity Startup

#1
German Startup Cup
2020 Category IT Secutity

CYBER SECURITY EXCELLENCE AWARDS
WINNER
2022

SECURITY EXCELLENCE
IoT Evolution
2022

# THANK YOU

**Gerhard Steininger**
VP Sales and
Business Development
g.steiningner@asvin.io

**asvin GmbH**
Stuttgart, Germany
www.asvin.io