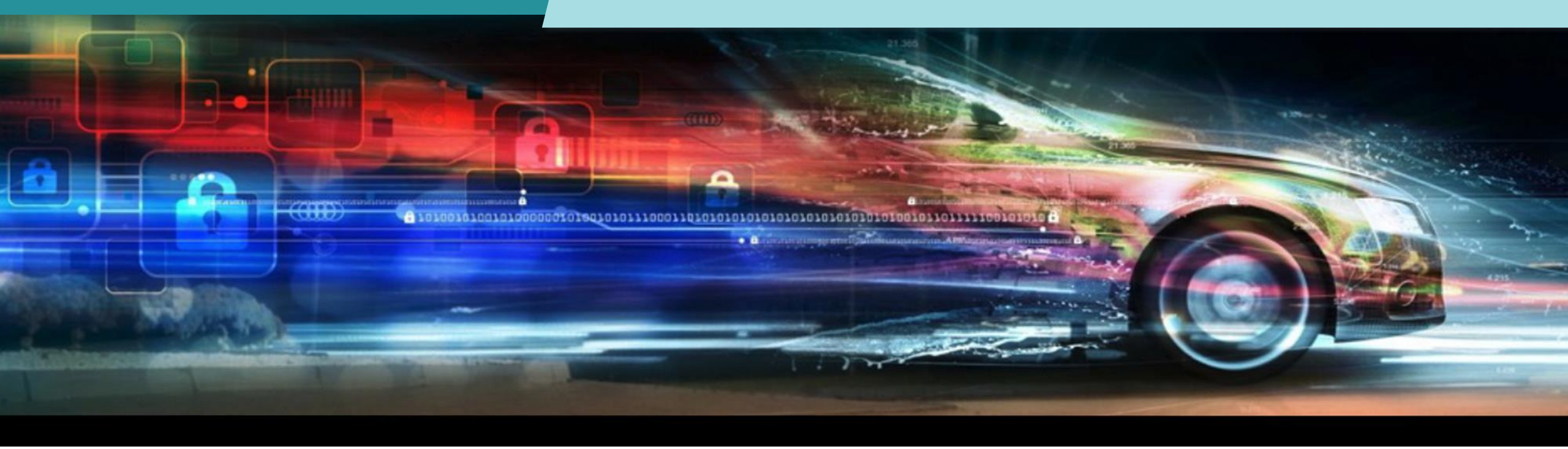


Trends in Threats and Attacks in Automotive

Dr. Martin Emele, Auto-ISAC Europe
European Director

Cybersecurity Vehicle Forum – Hamburg, Germany
November 14, 2023

TLP:GREEN

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

Meet the Speaker

Dr. Martin Emele

Auto-ISAC Europe

European Director

Current Positions

- **European Director (EuD) of Auto-ISAC Europe**
- **Vice-Chair of European Council of ISACs**
- **Federation of German Industry Association (BDI), Co-Chair of Cybersecurity Working Group**
- **Member of the European Stakeholder Cybersecurity Certification Group**
- **Vice President Cybersecurity Public Affairs, Bosch**

Past Positions

- **Vice President Security Product Group, ETAS a Bosch subsidiary**
- **Project Director for Bosch HSM Development, Bosch**

Education

- **PhD in Computational Linguistics, University of Stuttgart**
- **Diploma in Computer Science, University of Stuttgart**

Auto ISAC – Who We Are

Strategy & Mission | ***Who We Are & Why We Are Here***

MISSION: *To strengthen the global automotive industry against cyber threats and enhance cyber attack resilience and response.* ***An attack on one is an attack on all.***

Timely Sharing of Threat & Vulnerability Information

Building Strong Relationships

Developing Effective Response Plans

Ensuring & Maturing Consistent Cyber Capability

Each Member is expected to: ***Trust, Share, Teach, Learn, Act***

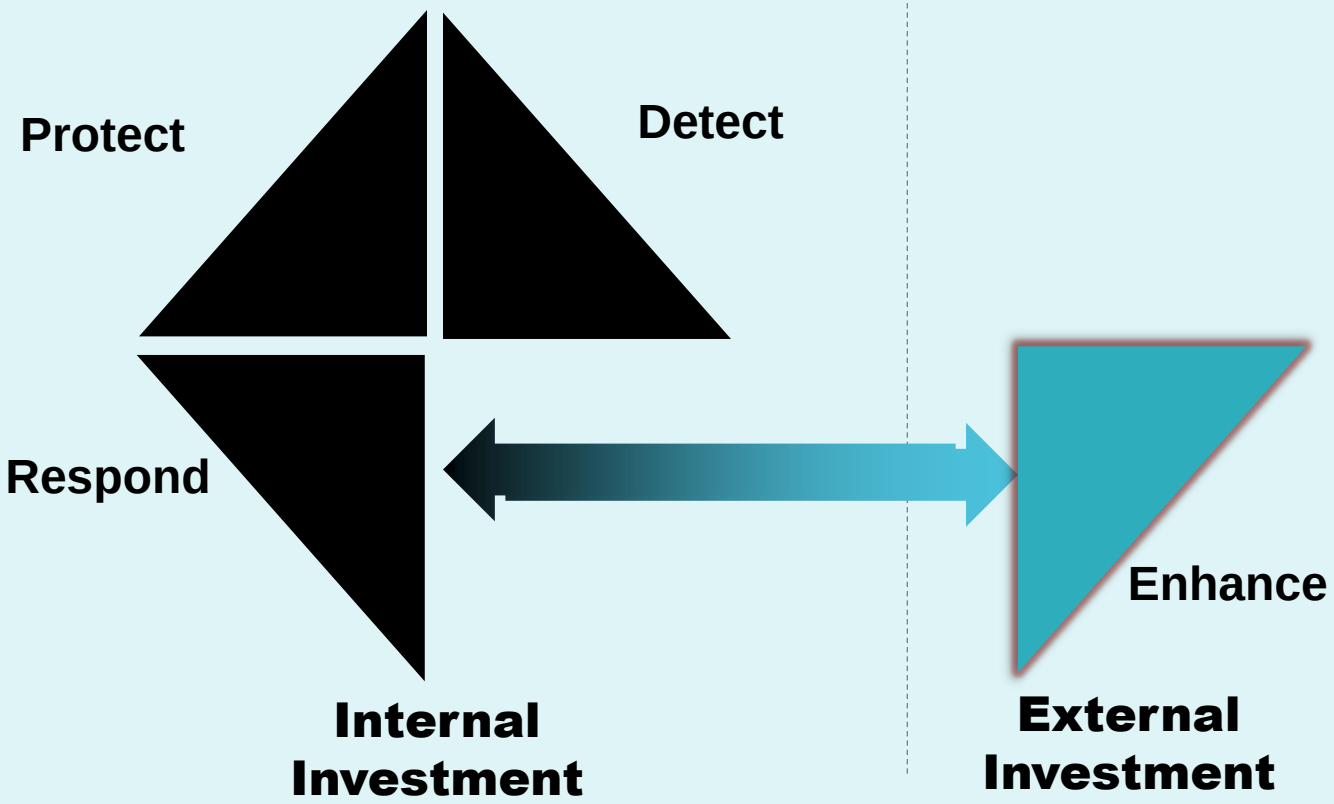
We are a **technical organization**, serving membership by enabling **cyber learning and capability development**. As members, we are expected to both **share and learn**, and continue to strengthen capabilities to protect our customers.

We will hold ourselves accountable.

Why an ISAC?

Information Sharing and Analysis Center (ISAC)

Organizations must act individually to manage cyber risk…



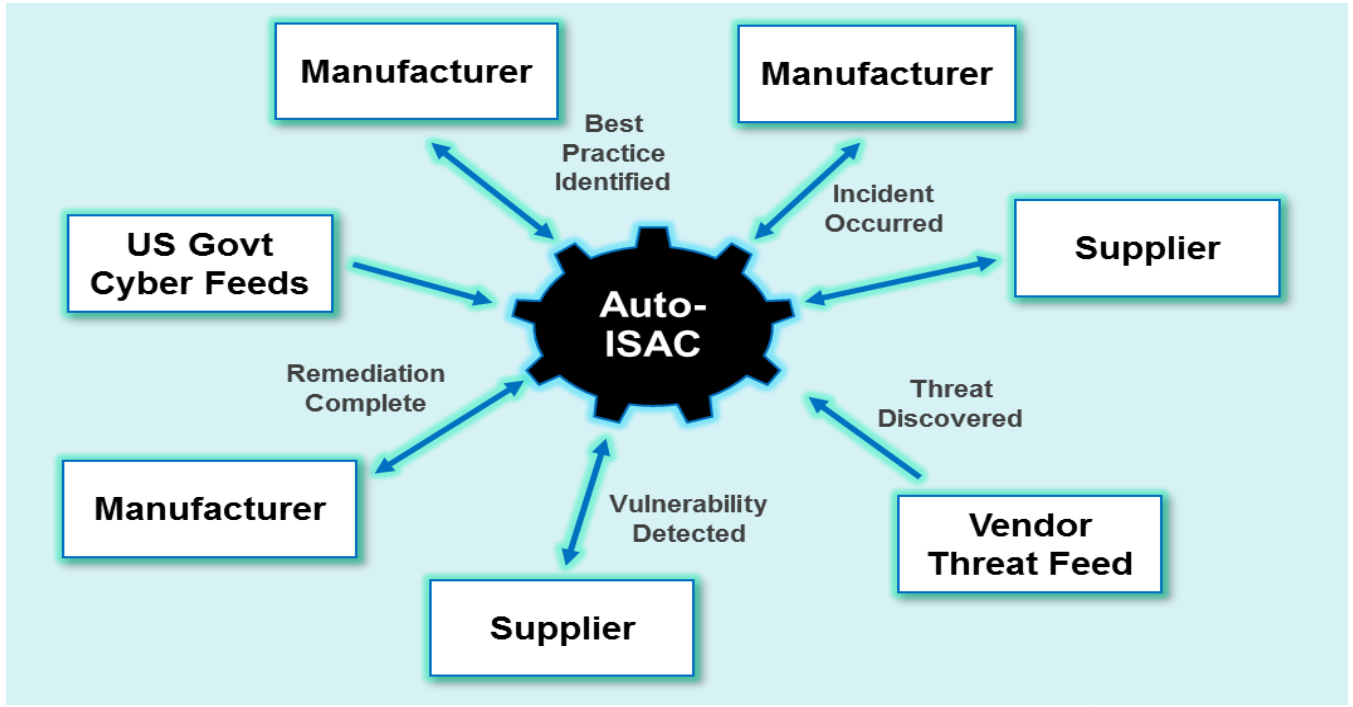
…one company's detection is another company's prevention

- Identify ***emerging threats*** and ***vulnerabilities*** earlier
- ***Pool limited resources*** to better fight your adaptive adversary
- ***Share incident intelligence*** to act more quickly
- Proactively shape industry-wide ***best practices***
- Protect overall ***trust*** in innovation across the industry
- Build ***resiliency*** across industry

Auto-ISAC Enables Trusted Sharing and Analysis

Cyber Threat and Vulnerability Information

Central Hub for Intelligence and Analysis



Aggregate, analyze and share auto-specific cyber information across the industry's attack surface

Benefits

Efficiently identify threats
by supplementing internal intelligence with external feeds

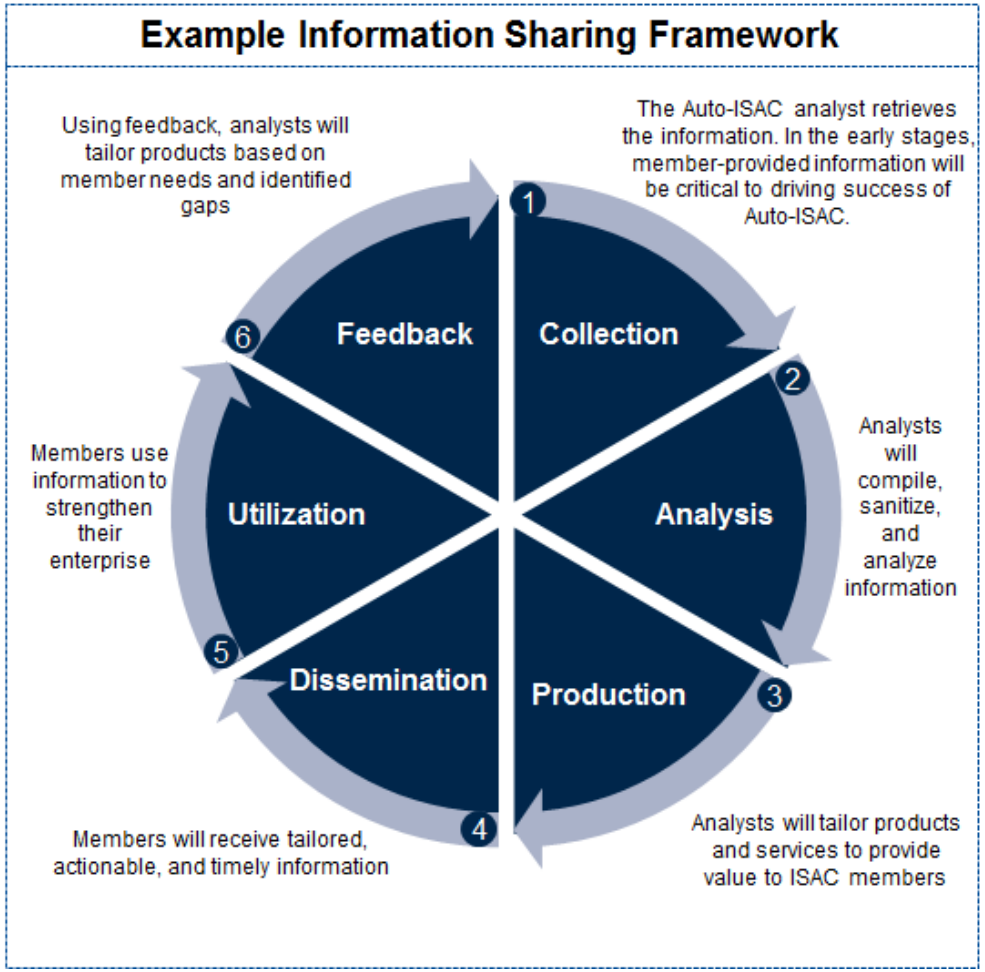
Detect vulnerabilities faster
with cross-industry vulnerability information sharing

Validate risk analysis
with reliable industry-level findings and best practices

Auto-ISAC Operating Framework

- **The Auto-ISAC operating framework centers around six basic elements:**

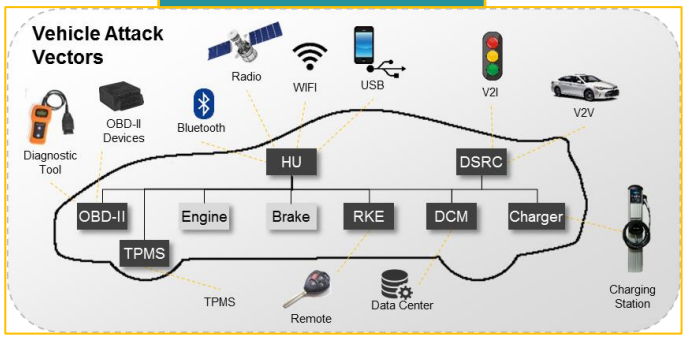
1. **Information collection from Members and external sources**
2. **Analysis of information to determine trends or patterns**
3. **Production of products and proposed actions based on analysis**
4. **Dissemination of alerts, recommendations, and other products back to Members and other relevant stakeholders**
5. **Member utilization of information and associated actions**
6. **Feedback to Auto-ISAC to improve operations**



Automotive Cyber Threat Ecosystem

Information Technology (IT) Threat Scope

Product Threat Scope



Interaction Attack Vectors

Interaction Attack Vectors

Supply Chain & Provisioning Attack Vectors

Operational Technology (OT) Threat Scope

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

TLP:GREEN

Image Sources: Dreamtime, Classroomclipart, JMLR

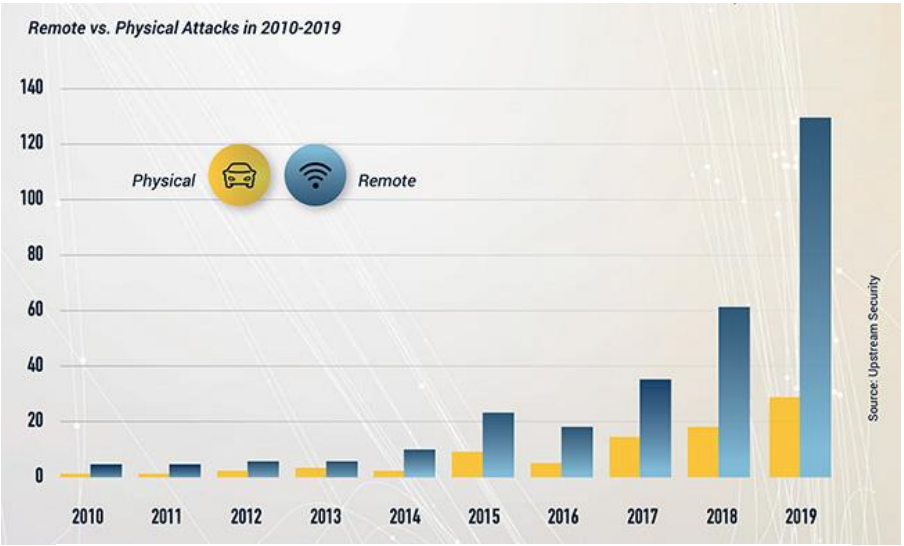
Interesting Stats…

- **Global Connected Vehicles will jump 134% from 330 million in 2018 to 774 million in 2023[1]**
- **By 2025, a connected car will produce 26GB of data per hour and 50GB if autonomous[2]**
- **2023 saw an increase in sophisticated attacks that brought challenges to the entire automotive ecosystem.**
- **In 2021, the majority of hacks were carried out by black-hat hackers (57%), white-hats accounted for 39% and 4% others[3]**
- **30% of incidents included a potential data breach incident, targeting both OEMs and other automotive stakeholders**
- **The segments of the automotive industry hit was wide-spread across all segments – OEMs, Tier 1s, EVs, fleet management, car sharing, car rental, car dealerships, ride sharing, etc.**
- **2023 saw an increase in the use and sophistication of cyber attacks across various attack vectors Advanced attack practices are creating a heightened awareness across the industry of how any point of connectivity is vulnerable to new threats.**

1. https://www.juniperresearch.com/whitepapers/connected-cars-how-5g-connected-commerce-blockchain-will-disrupt-the-ecosystem
2. https://www.wevolver.com/article/high-speed-data-and-connected-cars
3. Upstream2022Report, UpstreamH12023Report

2023-24 Automotive Threat Landscape – Notes

- Perception of the automotive cyber threat environment based on information available to/shared with us
- Sensationalism of the current automotive cyber threat environment risks desensitizing decision makers who can direct and fund proactive countermeasures
  - Implying that increased malicious cyberattacks on automotive business networks (IT) equates to increased cyberattacks on vehicles
  - Conflating researcher, tuner, and enthusiast vehicle hacking with malicious hacking
  - Conflating technology-enabled vehicle theft with vehicle control system hacks
- Intelligent imagination is critical to identifying, assessing, and managing automotive cyber risk because there **currently** are few reports of real-world malicious attacks on vehicles other than theft



Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More

Image Source Sam Curry Blog

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

TLP:GREEN

2023-24 Automotive Threat Landscape – Takeaways

- **Cyber threat actors sponsored by nation-states will remain a threat to automotive IT and sensitive information as geostrategic competition and posturing persist.**
  - **Compromised internal communications and data theft could compromise customer and employee privacy, damage brand reputation, and adversely impact market competitiveness.**
- **Technology-enabled vehicle theft activity will persist.**
  - **Some incidents may go viral and draw negative attention to affected brands and the broader automotive industry.**
- **It is possible but unlikely that cyber threat actors will attack vehicles via internal or supply-chain-based vulnerabilities other than for vehicle theft.**
  - **Attacks are conceivable due to vulnerabilities researchers have found, exploited, and publicized**
- **Compromised mobile devices connected to in-vehicle systems may cause the infotainment system to function in an unexpected or uncontrollable manner which could distract the vehicle operator.**
  - **Such distractions could lead to accidents that cause harm to road users or damage to infrastructure and the environment outside the vehicle.**
- **Increased media coverage of vehicle cybersecurity risks may change the landscape.**

Software Defined Vehicle Ecosystem – Security

- Software-Defined Vehicles (SDVs) involve far more than just OTA software updates and cloud-based applications.
- Software managing hundreds of ECUs and other functions within the vehicle is expected to grow beyond hundreds of millions of lines of code, possibly making SDV software development the number one challenge in automotive design.
- Protecting that software throughout deployment and operation is **critical**.

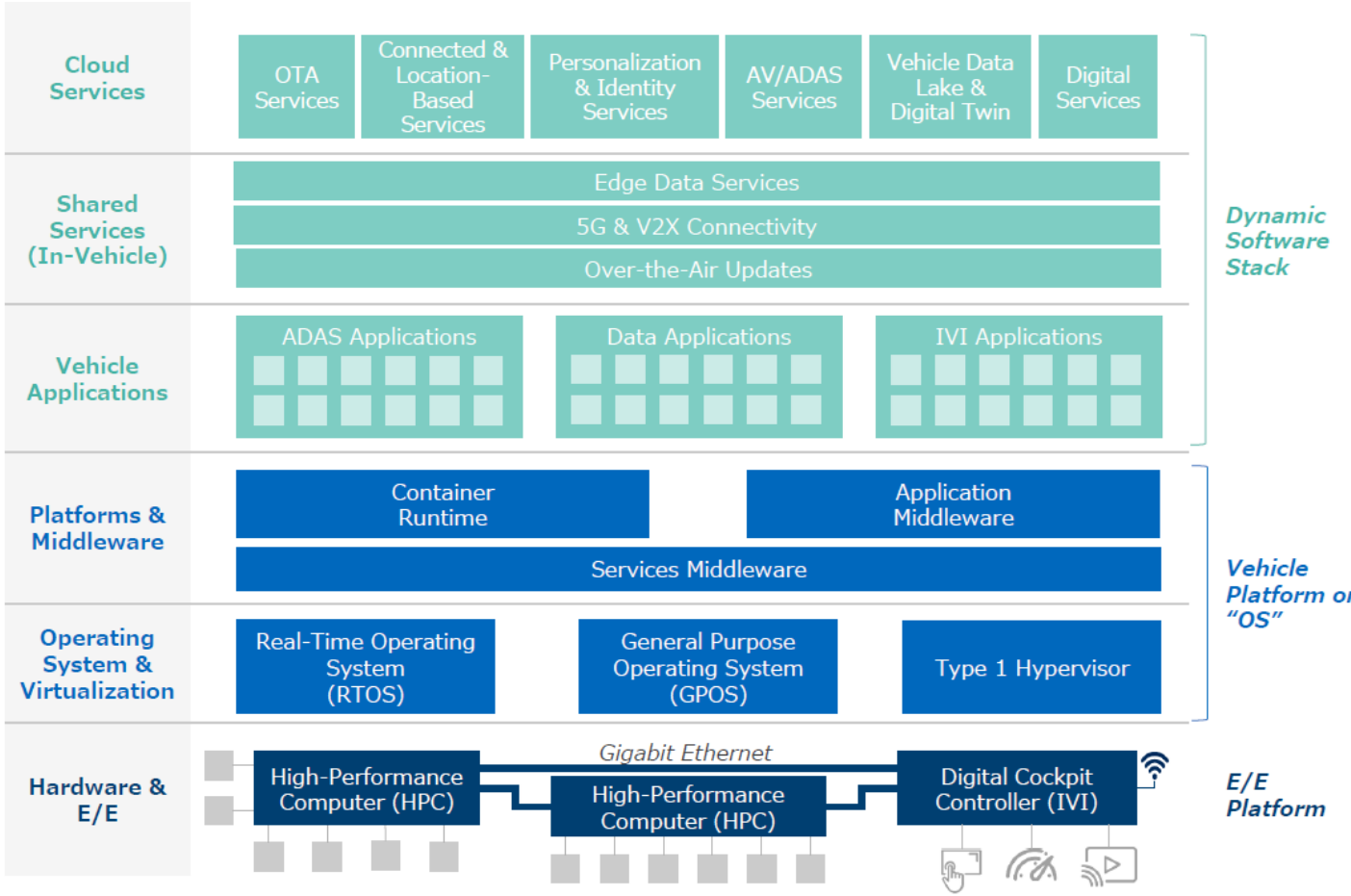


Image Source SBD Automotive Report

Software Defined Vehicle Ecosystem

Security Measures

- Well-structured cybersecurity organization
- Developers must manage risk
- Lessons from other industries (such as defense-in-depth strategies, information sharing and collaboration)
- Use comprehensive cybersecurity management systems
- Protect direct and indirect internet connections (cellphone via USB/Bluetooth or wireless tire pressure monitoring)
- Secure vehicle networking (SecOC, MACsec, IPsec, TLS, etc.)
- Secure boot
- Secure SW updates (including cryptographic code verification)
- Public key infrastructure (PKI)
- Testing (static/dynamic, fuzz testing manually and in an automated manner)

Auto-ISAC Partnerships

"Partners" add a richness to our automotive ecosystem

- **Auto-ISAC Partnerships are open to anyone working in the automotive industry ("Community Partnership")**
- **Auto-ISAC "Strategic Partnerships" require agreement and approval from our Membership.**
- **Partnerships support Auto-ISAC's mission to**
  - **Develop a vibrant and robust information sharing community**
  - **Freely sharing information and educating Members**
  - **Supports building resilience across the whole industry**
  - **Supports automotive events and workshops**
- **Mutually rewarding and sustainable**
- **We especially appreciate our government, standards bodies and association partnerships!**


THANK
YOU
GRAZIE
MERCI
MULTUMESC
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
MOCHCHAKKERAM
SALAMAT
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
MERCI
MOCHCHAKKERAM
CHOKRANE
MATUR NUWUN
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
MAAKE
OBRIGADO
SPASIBO
WELALIN
ARIGATO
MOCHCHAKKERAM
OBRIGADO
SPASIBO
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM
MULTUMESC
VINAKA
NIRRINGRAZZJAK
MAMANA
OBRIGADO
DANK JE
KIITOS

Our Contact Info

Dr. Martin Emele
European Director

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

Steiermärker Str. 3-5
70469 Stuttgart
MartinEmele@automotiveisac.com

Peter Venesz
Product Cybersecurity
Intel Analyst

AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

Steiermärker Str. 3-5
70469 Stuttgart
PeterVenesz@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM