School of Mechanical Engineering
FACULTY OF ENGINEERING

UNIVERSITY OF LEEDS

MECH5170M
Connected and Autonomous Vehicles Systems

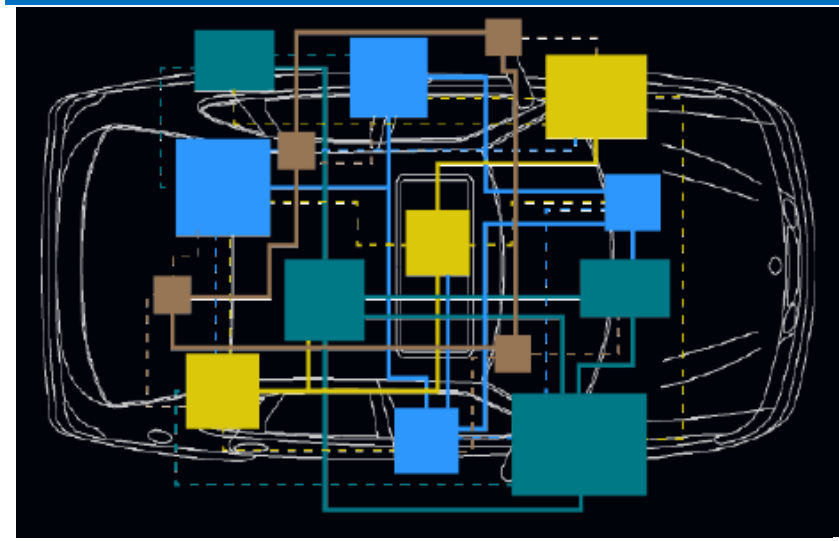
Cyber Security of CAV - part 1

Kris Kubiak (k.kubiak@leeds.ac.uk)

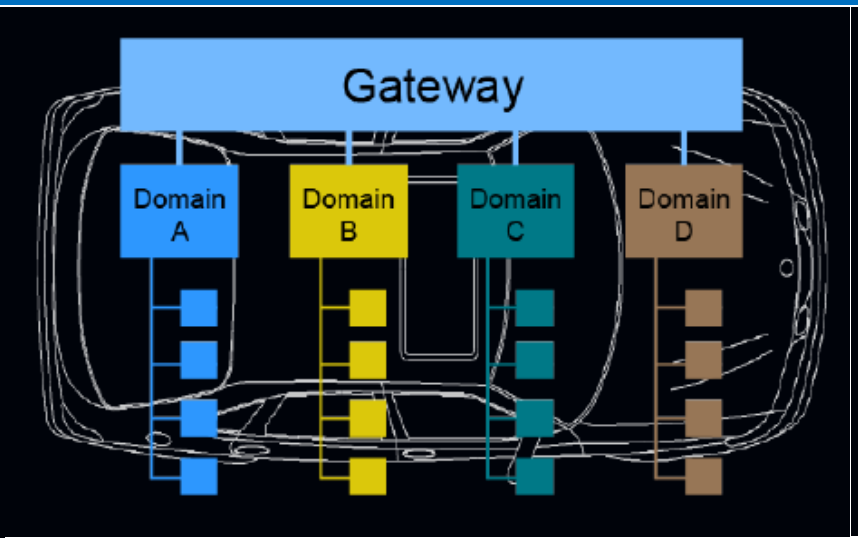
Motivation

Evolution of Automotive E/E Architectures

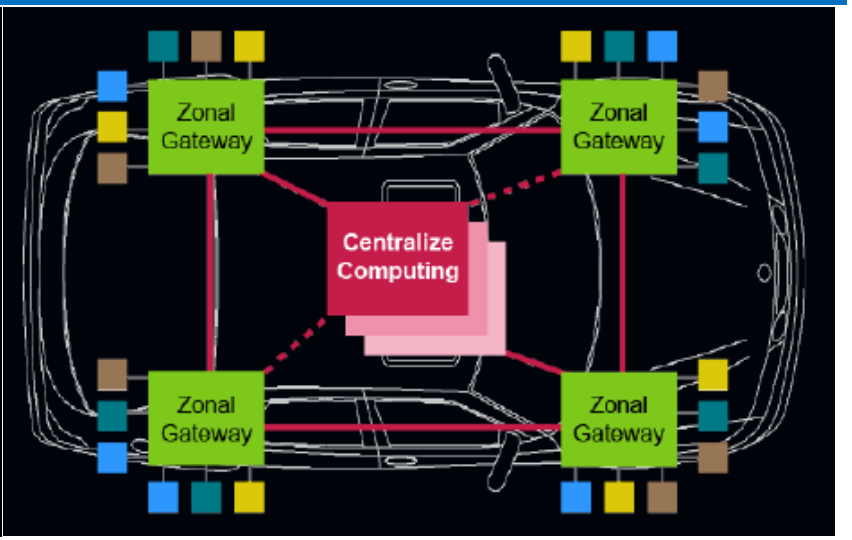
UNIVERSITY OF LEEDS



Yesterday



Today



Tomorrow

Challenges:

- Up to 100 ECUs
- More than 100MLoC (Lines of Code) per vehicle
- Conversion from Closed to Open System
- Vulnerabilities in Supply Chain
- Long Life Time Software

Possible Measures:

- Reliable Coding Style (MISRA)
- Standard & Regulation
- Monitorable and Updatable Architecture

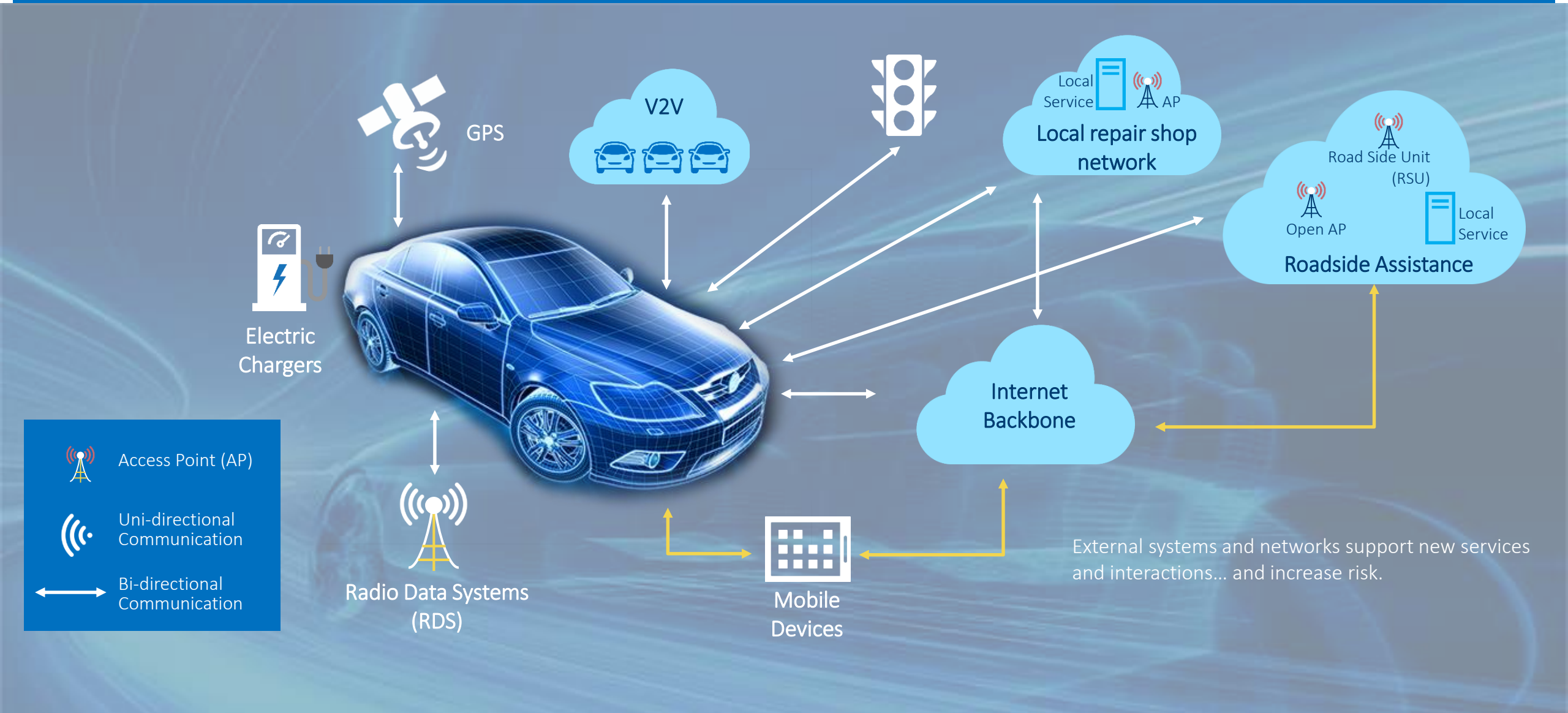
Hacking of Connected Autonomous Vehicles

Why hacking?	Why is it possible?	Why now?
Valuable Data attracts hackers	**High System Complexity** implies high vulnerability	**Wireless Interfaces** enable scalable attacks
Car-generated data may become a £750 billions market by 2030	Up to 100 ECUs per car, up to 100M lines of software code	250M+ connected vehicles on the road since 2020

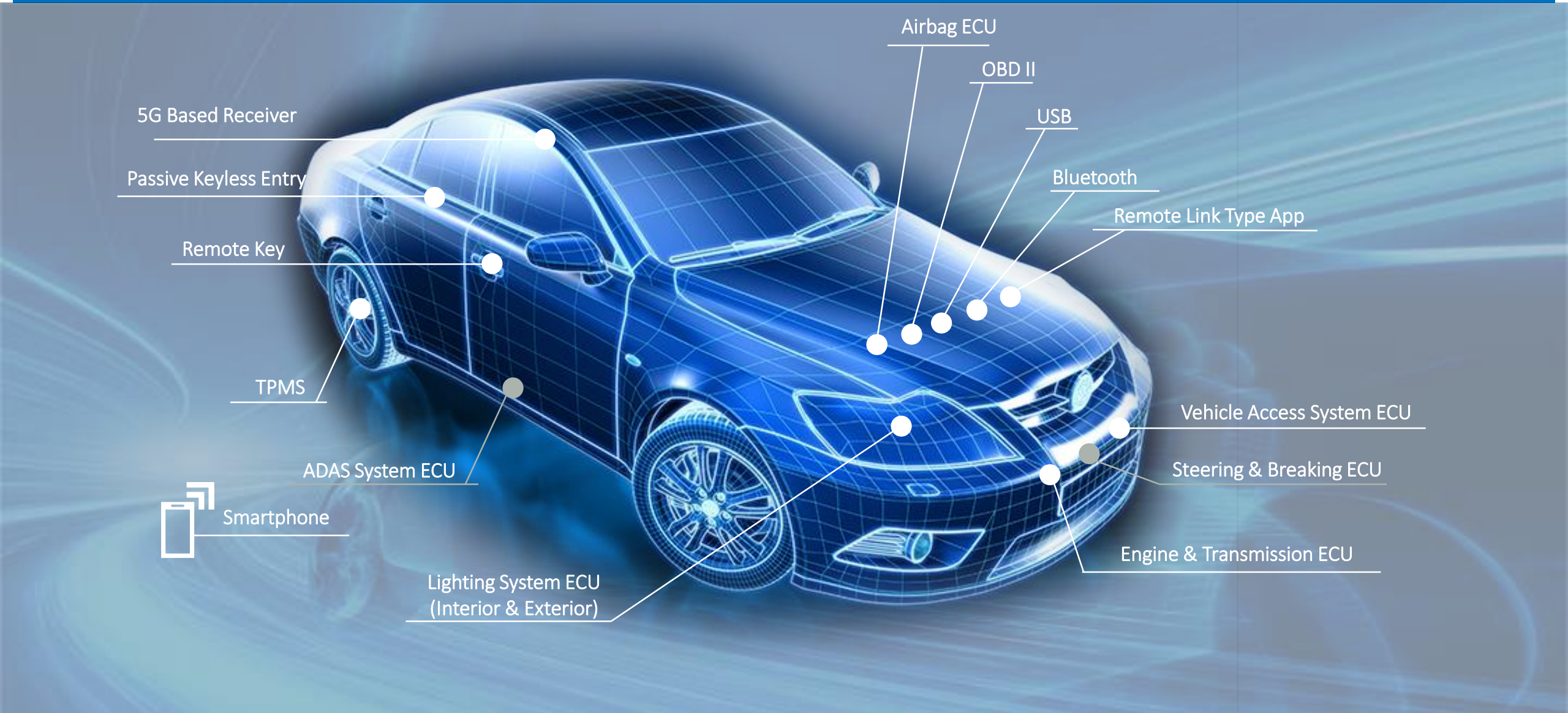
Vulnerabilities

V2X Connectivity

UNIVERSITY OF LEEDS



Vehicle Security



Sub-system Level Defence

UNIVERSITY OF LEEDS

Comprehensive Security Approach

SOFTWARE

- Over-The-Air OTA updates
- IDPS/anomaly detection
- Network enforcement
- Certificate management services
- Anti-malware and remote monitoring
- Biometrics

- Fast cryptographic performance
- Device identification
- Isolated execution
- (Message) authentication

HARDWARE

Trusted Execution Environment	
Hardware and Software Identities	
Protected Boot	Protected Storage

Trust and Context

Safety & Security

Importance of Cyber Security

There is no safety without security

Safety (Human Life)

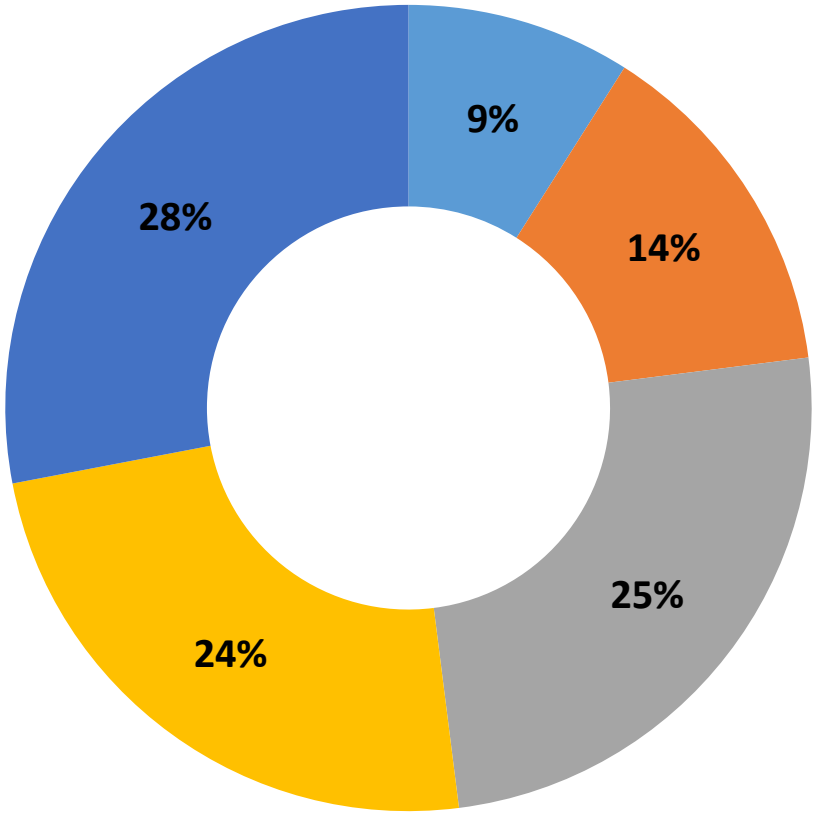
- Tires
- Chassis
- Windshield
- Lighting System
- Braking System
- Powertrain System
- ADAS System
- Gateway/Switch
- Sensor/Camera/Lidar

Security (Data)

- Location history
- Camera data
- Phone call records
- Browser Logs
- Transaction Certificate

Software development trends

UNIVERSITY OF LEEDS



How many different suppliers have their code in a high-end vehicle?

Currently, software for high-end vehicles comes from a wide range of sources. The majority of respondents believe (77%) believe that a minimum of 10 different suppliers are providing software for the average high-end car, and 52% of respondents said a minimum of 25 different suppliers are involved. From a cyber security perspective, this means it's challenging for OEMs to even track what software is in their cars and whether any of that software has existing vulnerabilities.

Total Number of Respondents: 211

[Strategy Analytics]

Regulations

Regulations and standards

UNIVERSITY OF LEEDS

On June 25, 2020, the UNECE announced it had formally adopted two new sets of regulations as part of the broader **WP.29 regulations**. These new regulations include:

- UN Regulation on **Cybersecurity** and Cyber Security Management Systems
- UN Regulation on **Software Updates** and Software Updates Management Systems

WP.29 involves threat analysis, testing, verifying security pre-production, then post-sale involves monitoring, mitigation, and remediation if an attack occurs or if the OEM discovers a vulnerability.

UNECE
United Nations Economic Commission for Europe

Regulations and standards

UNIVERSITY OF LEEDS

UNECE WP.29 regulations

In nations that follow these regulations (e.g. EU members, Japan, Republic of Korea, etc.), automakers selling cars for these markets must have certain capabilities in place to monitor, detect, mitigate, and ultimately fix vulnerabilities in cars that malicious actors could compromise.

54 countries are signatories to the 1958 UNECE agreement, and are likely to adopt these regulations at some point in the future, though many plan to do so in the near term.

UNECE WP.29 regulations

Key Dates:

- These new regulations apply as of January 2021.
- The EU plans to make these regulations mandatory for all new vehicle types from July 2022, and for all new vehicles from July, 2024.
- Japan adopted these regulations for SAE Level 3 vehicles in April, 2020, and plans to adopt it for all OTA update-capable vehicles as of November, 2020.
- The Republic of Korea plans to implement the regulation at a currently undecided future date.

Other Regulations/Standards/Guidelines

MISRA C 2012 - Code of practice for C source code

Standards:

- **ISO 21434 (Road Vehicles – Cybersecurity Engineering)**
- ISO 24089 (Software Updates)
- SAE J3101 (Hardware Protected Security)
- SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)
- AUTOSAR (Secure On Board Communications)

Other National Legislation/Guidelines:

EU - GDPR

U.S. - NHTSA Cyber Security Guidelines, Proposed legislation (Self Drive Act, AV Start Act), California - CCPA

China - Cybersecurity Law, Encryption Law, SAC/TC114/SC34 (related to AV and Intelligent vehicles; has a cyber security working group)

Industry challenges

UNIVERSITY OF LEEDS

The automotive industry is facing numerous challenges related to cyber security and must work to implement a range of processes and technologies in a short timeframe.

- **Compliance:** For global OEMs, developing the processes and systems to document compliance with the WP.29 UN Regulation on Cybersecurity and Cyber Security Management Systems is going to be critical over the next few years.

- **Software Asset Tracking:** OEMs must start using systems that provide an inventory of, and monitor, all the software running in each ECU in every deployed vehicle on roads.

Industry challenges

- **Operations:** OEMs must either develop or expand the capabilities of internal teams that will be actively monitoring fleets for cyber security threats and analysing, and fixing (or mitigating) existing vulnerabilities.

- **Balancing Current and Next-Generation E/E Architecture Requirements:** Although some OEMs are able to move to next-gen E/E architectures over the next few years, not all OEMs are moving at the same speed, and many will need to support legacy platforms for years to come. But to comply with regulatory requirements, OEMs MUST secure those legacy platforms, otherwise in many markets they simply won’t be able to sell cars.

ANY QUESTIONS ???