Understanding the evolving CAV cyberspace

UNIVERSITY OF WINDSOR
SHIELD
AUTOMOTIVE CYBERSECURITY CENTRE OF EXCELLENCE

With digitalization of in-vehicle systems that require to deliver vehicle connectivity, automation and shared mobility, there are significant cybersecurity risks which are direct threat to vehicle safety.

Connected Ecosystem

Sensors | Systems | Network | Infrastructure | Supply chain

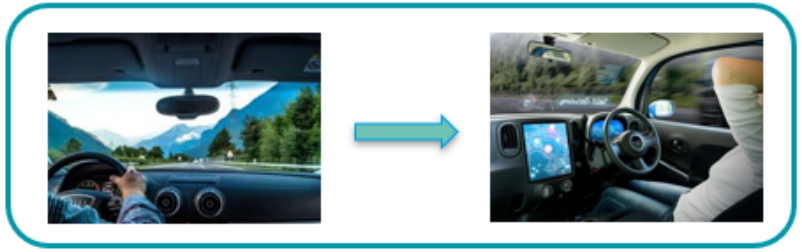
Emergence of Automotive Cybersecurity Standards:

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

UNECE's World Forum for Harmonization of Vehicle Regulations:
Automotive Industry Challenges

- Two UN Regulations on Cybersecurity and Software Updates
- First ever international harmonization in this area
- Require measures to be implemented across 4 distinct disciplines:
  - Vehicle cyber risks, mitigate risks along the value chain, security incidence detection and response, safe and secure OTA

Journey from Now to Then



Automotive Industry Challenges

- Compliance
- Software Asset Tracking
- Operations
- Balancing Requirements of Current and Next-Generation

Trends & opportunities

- Safety related applications (V2V)
- AI and machine learning
- Data management
- End-to-end cloud solutions
- Secure code development
- Future proof vehicle OS
- V2X applications with 5G adoption