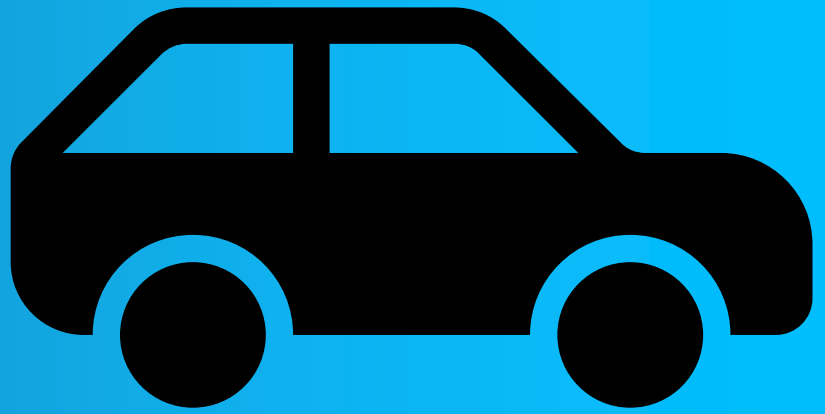
How regulations and standards are addressing automotive cybersecurity-related challenges

Nick Russell, Director - Standards

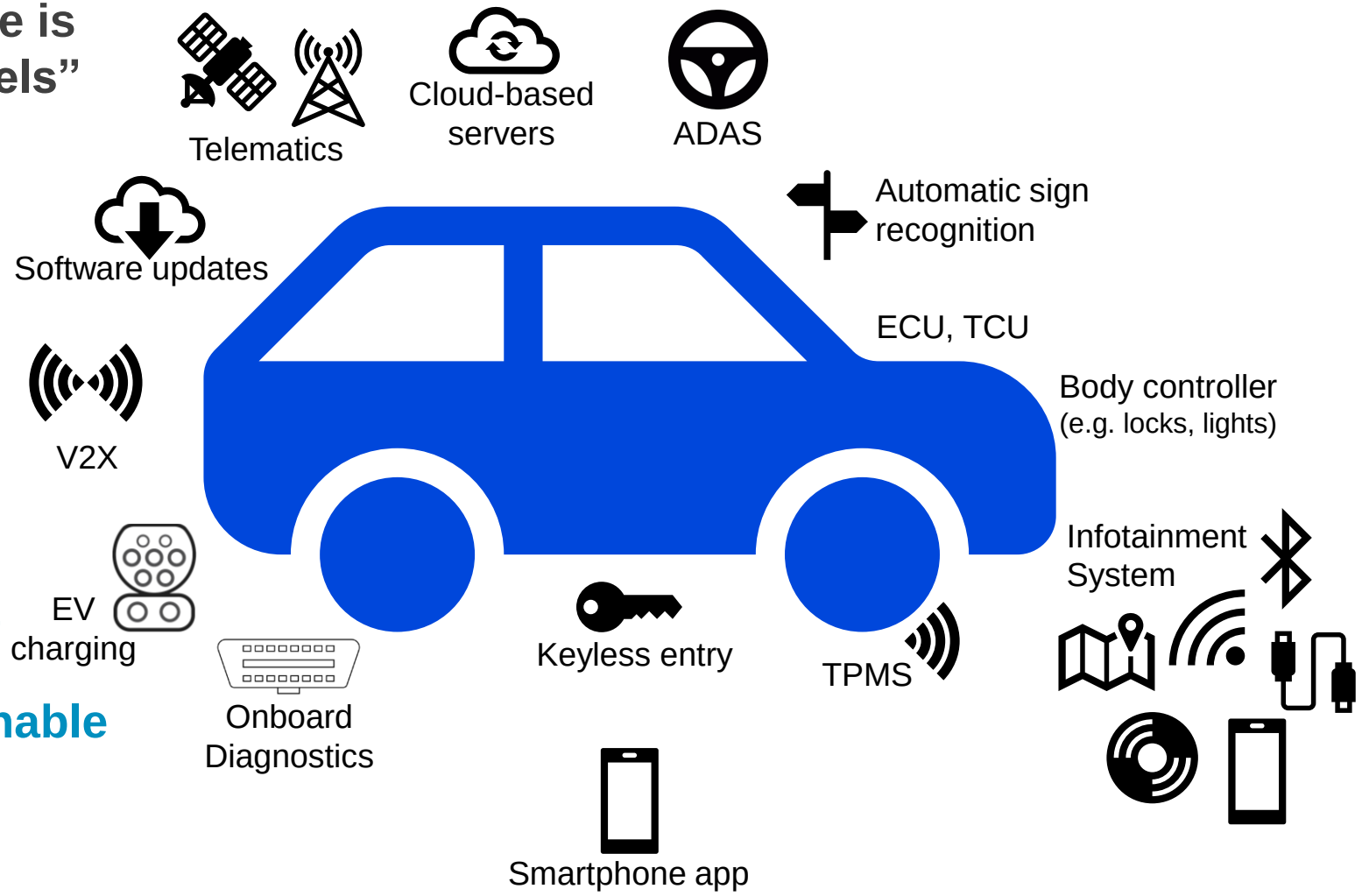
2021-01-20

Cybersecurity challenges for vehicles



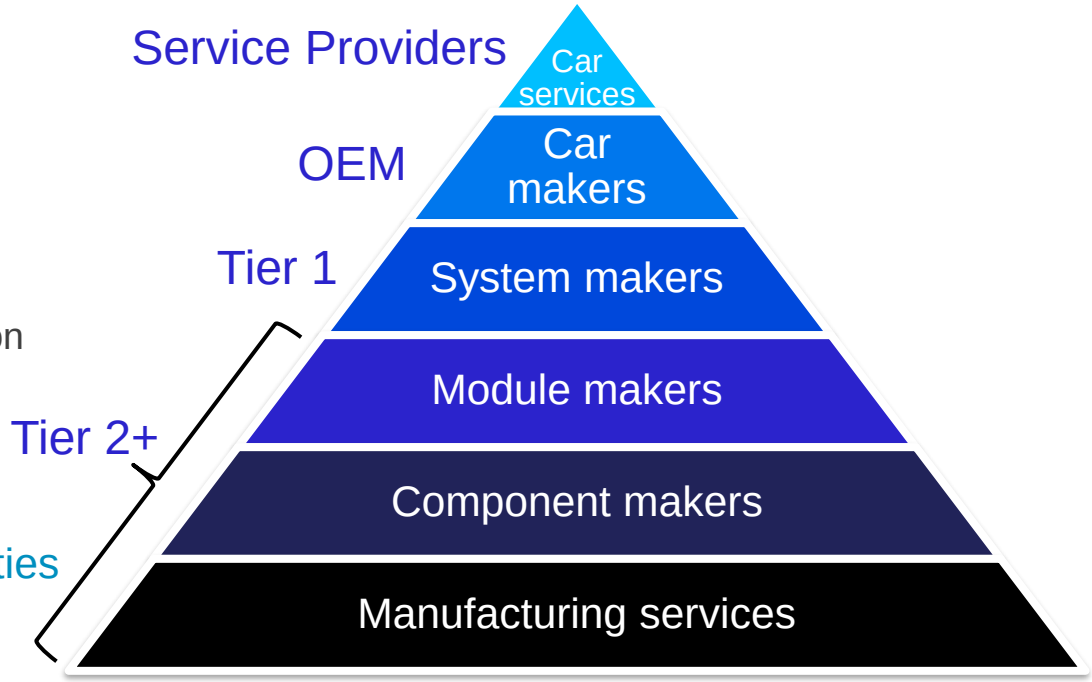
Attack surfaces

- **The modern, connected vehicle is essentially a “network on wheels”**
- **Multitude of attack surfaces and damage scenarios**
- **Convenience vs security vs safety**
- **Need to consider a whole host of risks, potential damage scenarios and consider reasonable mitigations**

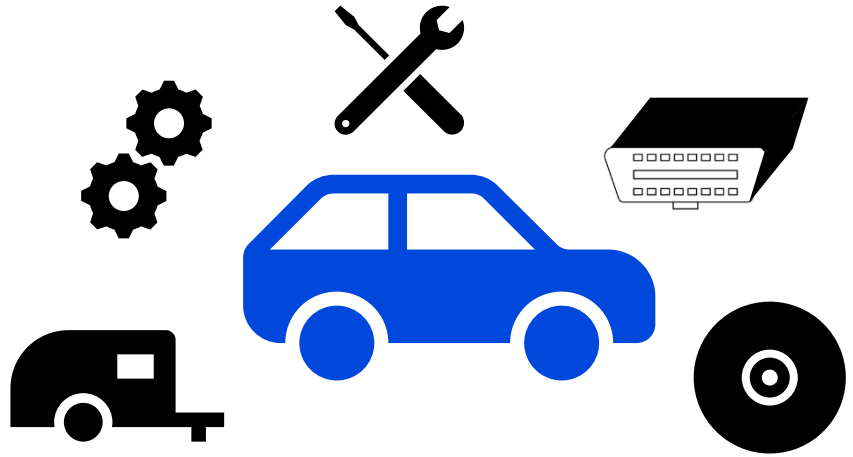


Suppliers

- **Supply chain**
  - Large number of entities in a vehicle's supply chain (100+)
    - Tier 1 suppliers supply to OEMs, Tier 2 supplier supply to Tier 1s, etc
    - E.g. Chip suppliers, Component suppliers, software suppliers, integration specialists, manufacturing specialists
  - Managing risk through-out the vast supply chain vendor community is a challenge
  - Common goals, methodology and understanding or responsibilities is needed to aid collaboration

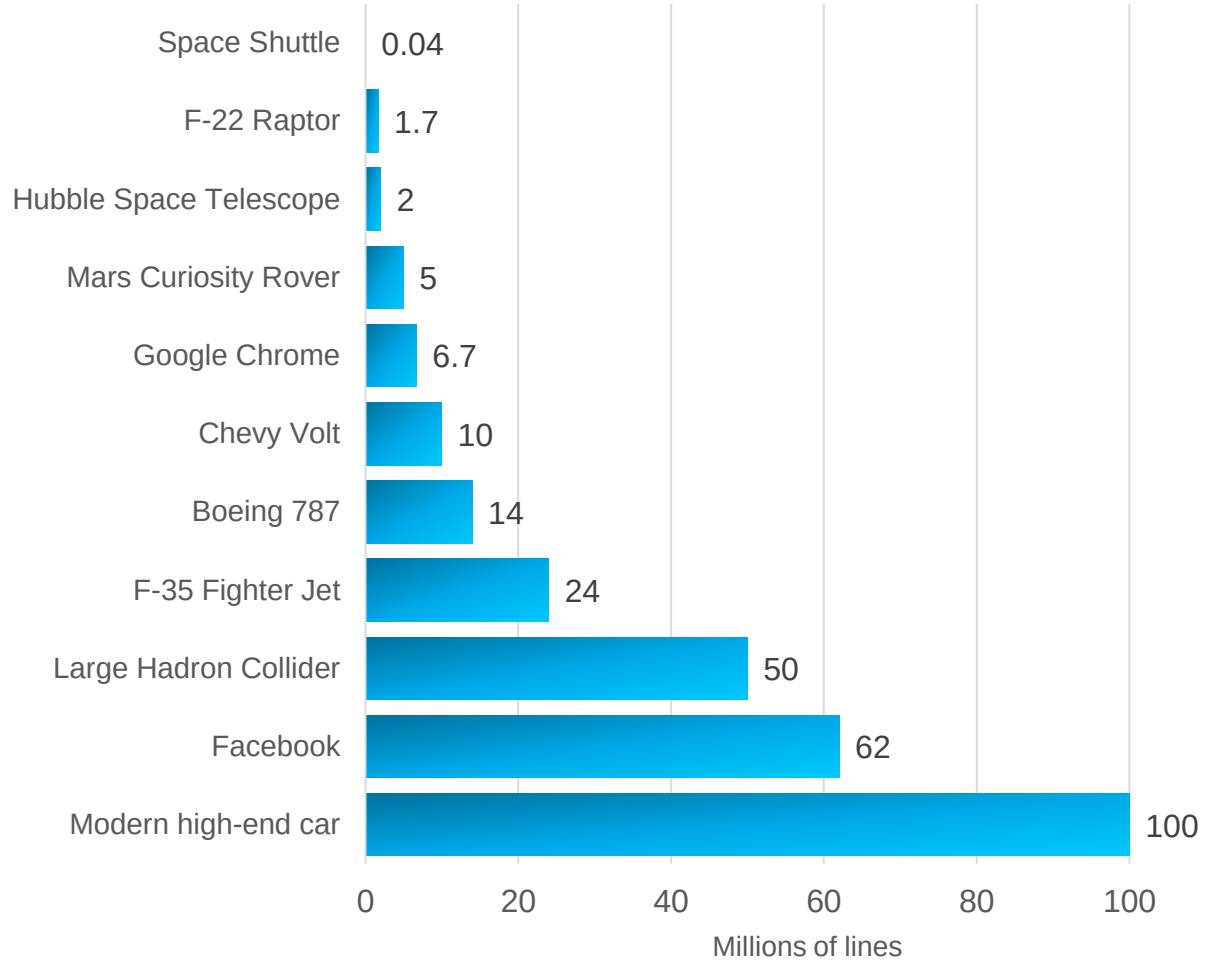


- **Aftermarket**
  - Many, varied aftermarket products available from many vendors
    - New parts for servicing/repairs
    - Functional enhancements to vehicles e.g. trailers, reversing cameras
  - Securing vehicles but enabling their owners to install aftermarket products is a challenge
  - "Right to repair" needs to be maintained



Software

- **Software is at the centre of every new vehicle design**
  - Almost every aspect of modern vehicle design has become fully connected, leveraging software platforms akin to those found in mobiles
  - Consumers place trust in the quality and reliability of advanced services
  - Software becoming key differentiator!
- **Modern high-end cars contain ~100m lines of code**
  - Increases possibility of bugs and vulnerabilities
    - ~80K defects, thus between 800 to 4000 vulns likely exist *
      - Assuming 800 defects per MLOC due to good code quality *
  - Ongoing monitoring needed for new security events
  - Ongoing, post-production updates needed
- **Code from various sources**
  - OEMs, component suppliers, OSS libraries, etc



Source: https://www.informationisbeautiful.net/visualizations/million-lines-of-code/

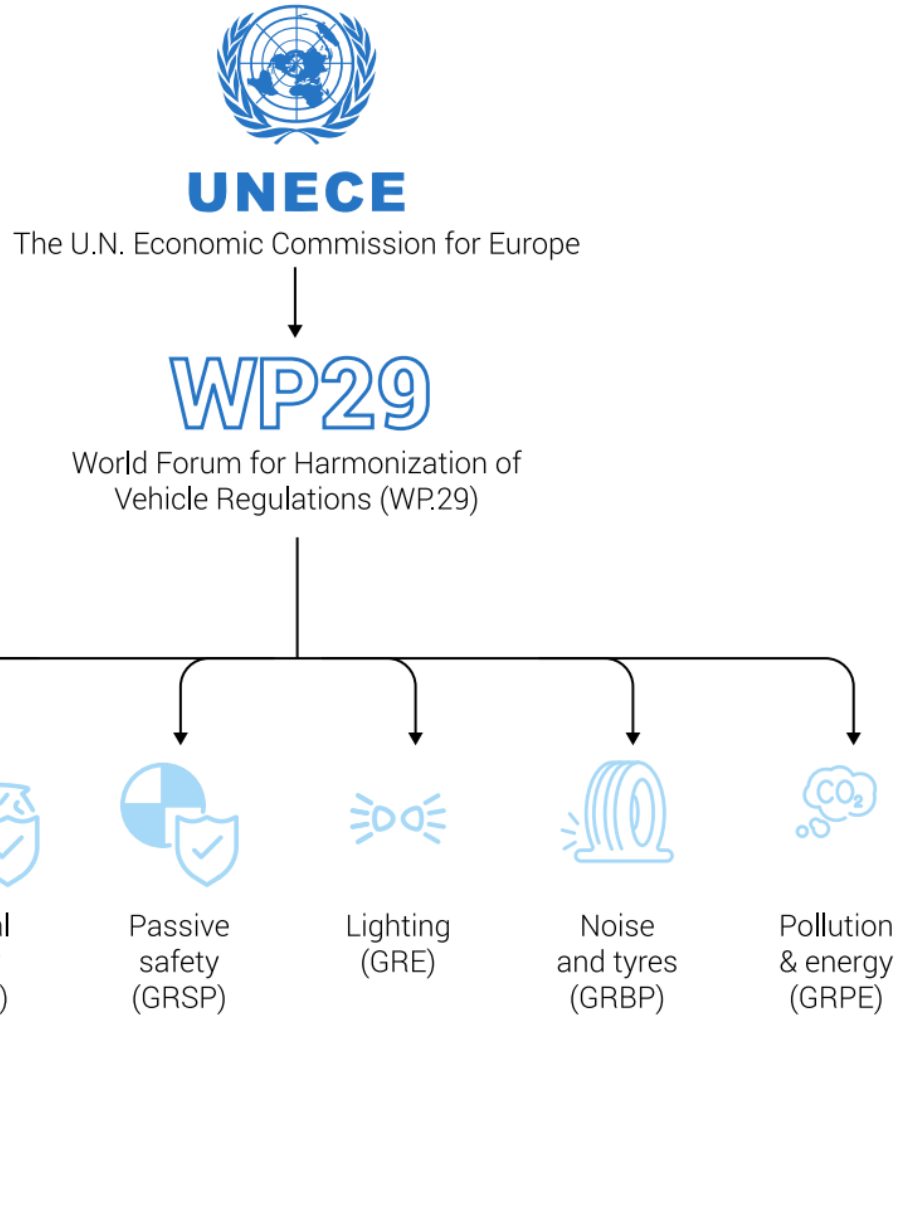
* According to https://insights.sei.cmu.edu/sei_blog/2016/06/using-quality-metrics-and-security-methods-to-predict-software-assurance.html

Regulations

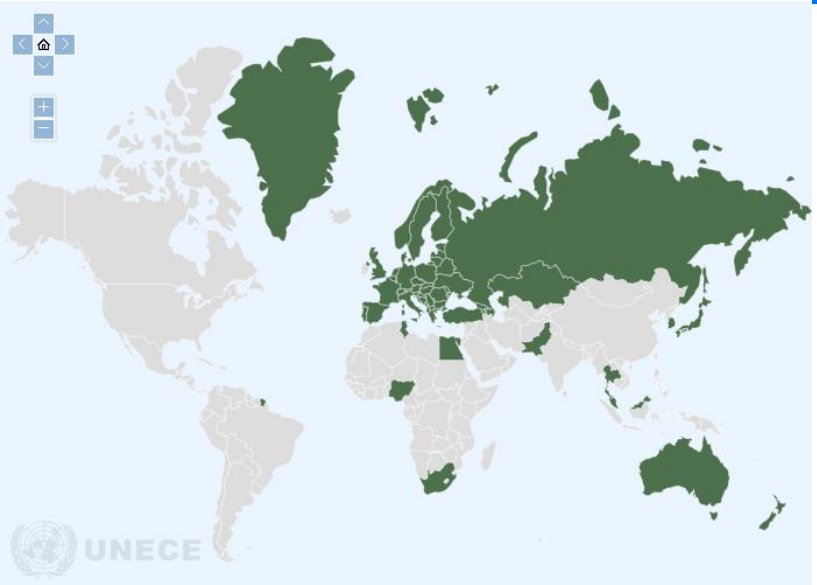
UNECE WP.29 – Overview

- **United Nations Economic Commission for Europe (UNECE) Working Party 29: UNECE World Forum for Harmonization of Vehicle Regulations**
  - A unique worldwide regulatory forum acting on behalf of the whole UN
  - Develops internationally harmonized regulations

- **Objectives:**
  - Reduction of technical barriers to trade
  - Facilitated border crossing
  - Reduction of costs to consumers
  - Cleaner vehicles
  - Safer and more secure vehicles

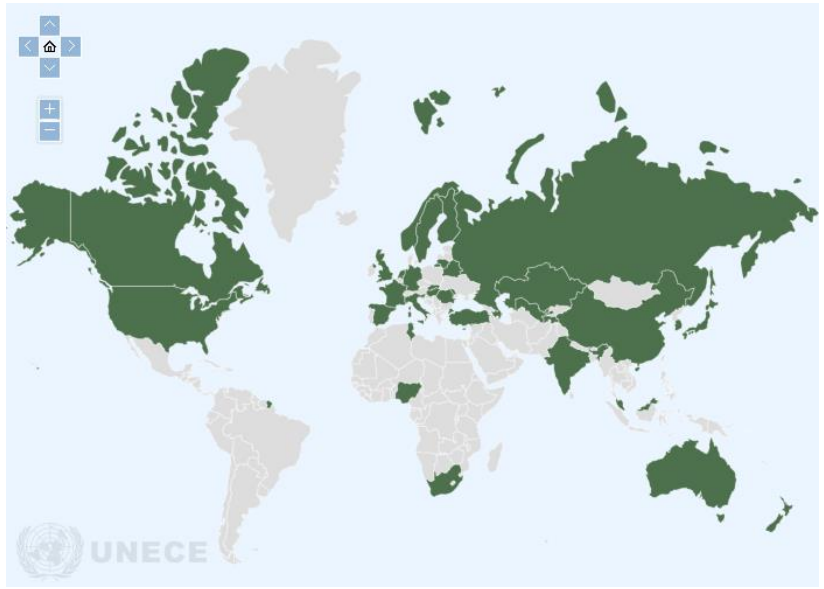


UNECE WP.29 – Who's involved



- **1958 agreement**
  - 63 Contracting Parties including EU, UK, Japan, South Korea, Australia…
  - Provides:
    - Type approval (of vehicle systems, parts and equipment)
    - Checks on conformity of production
    - Mutual recognition of the type approvals granted by Contracting Parties.
  - New Cybersecurity and Software Update 'UN Regulations' (#155 and #156) recently produced by the contracting parties to the 1958 agreement, come into force this month

- **1998 agreement**
  - 38 contracting parties including USA, Canada, China, India
    - Many that are also members of the 1958 agreement (e.g. EU, Japan, S. Korea, UK, Australia)
  - Provides "Global Technical Regulations" (GTRs)
    - GTRs do not refer to a type approval or certification procedures
    - When voting in favour of a GTR, contracting parties commit to implement it in national legislation
    - National law expected to include provisions for self certification or homologation
  - Cybersecurity and Software Update related GTR/guidance document is currently being drafted
    - Alignment to 1958 CP's UN Reg. #155 and #156 is currently respected



Motivations for UE Regulations 155 and 156

Increase in vehicle functionality & connectivity

- Automated driving and associated safety concerns
- Increased connectivity of vehicles
- Remotely-updateable software

Media attention on cyber attacks to vehicles

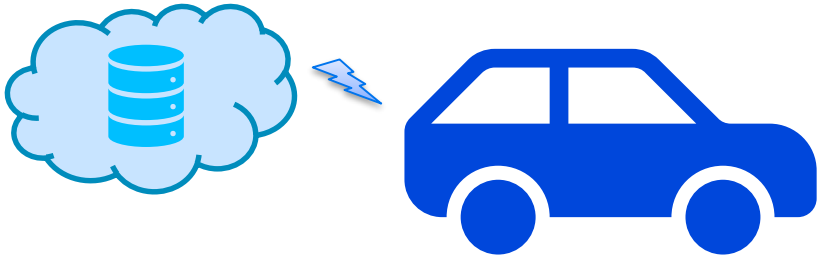
- Successful vehicle attacks making headline news
  - Jeep Cherokee hack by Charlie Miller and Chris Valasek in July 2015
  - Numerous remote keyfob attacks to steal high-end cars

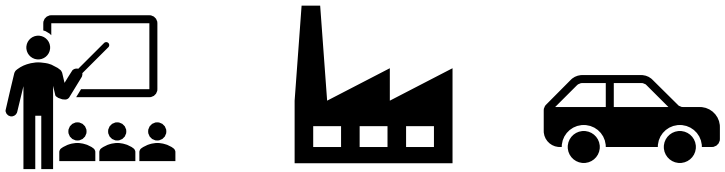
Local regulatory concern

- Observed that self-regulation not working
- Need to provide consumer confidence and assurance
- Harmonised set of regulations to allow for import/export, driving vehicles over borders, etc.

UN Regs 155 & 156 apply to…

- **Cars, buses, vans, trucks and others having 4 or more wheels**
  - Software Updates reg also applies to agricultural vehicles and their trailers if they have ECU(s)





- **All relevant on-vehicle and off-vehicle systems**
  - Back-end servers
  - Communications channels (including external connections)
  - Software update procedures
  - Unintended human actions
  - Vehicle data and code

- **All vehicle lifecycle phases**
  - Development
  - Production
  - Post-production (includes monitoring, detecting and responding to attacks)

Content of UN Reg 155 (CS) – Overview

Organisation

Cyber Security Management System

- Ensure organisations instil good cybersecurity practices in their processes
- Manage dependencies with suppliers, service providers and sub-organisations
- Covers all phases of vehicle:
  - Development
  - Production
  - Post-production
- Need to renew CSMS Certificate of Compliance every 3 years

Project

Design & development

- Identify and manage risks
  - Vehicle components and external interactions
    - Implement all mitigations of threats detailed in Annex 5
  - Suppliers
    - Identify and manage risks through the supply chain
- Secure any dedicated environments for the storage and execution of aftermarket software, services, apps or data
- Verify effectiveness of cybersecurity measures
- Use secure cryptographic methods

Post-production

- Monitor vehicle e.g. for cyber attacks, new threats/vulnerabilities
  - Assess
  - Respond if necessary e.g. modify affected software
- Report regularly to local Approval Authority on:
  - Monitoring activities
  - Vehicle modifications that affect cyber security technical performance

Content of UN Reg 156 (SU) – Overview

Organisation

Software Update Management System

- Ability to:
  - uniquely identify versions of software and their interdependencies
  - determine which versions of which software are on which vehicles, and which vehicles need which updates
  - determine which software versions will affect functional safety and/or Type Approval e.g. due to changing an existing functionality or adding a new one
  - inform vehicle user of updates
- Maintain necessary documentation on updates e.g. purpose, affected systems, installation process, etc.
- Need to renew SUMS Certificate of Compliance every 3 years

Project

For all updates

- Protect authenticity and integrity
- Enable vehicle, via standardised interface, to be able to provide info on software versions installed
- Protect the stored info on software versions installed against unauthorised modifications

For OTA updates

- Ability to restore systems to previous versions of software in event of failed/interrupted updates, or at least be placed into a safe state
- Apply updates only when vehicle has enough power to complete the update process
- Maintain safety of the vehicle e.g. ensure preconditions are met, prohibit installation until safe to do so
- Display needed updates to vehicle user, including purpose, changes, expected time for installation, functions unavailable during update
- Display success/failure of updates to vehicle user

Standards

Motivations for standards

Demonstrable attacks

- Media articles / academic research
  - First theoretical remote attack on a vehicle (GM) published in 2011 by University of San Diego and University of Washington
    - “Comprehensive Experimental Analyses of Automotive Attack Surfaces”
- Real-world proven attacks
  - Jeep Cherokee hack by Charlie Miller and Chris Valasek in July 2015
  - Numerous remote keyfob attacks to steal high-end cars

Regulatory authority interest

- United Nations Economic Commission for Europe (UNECE)
  - UN regs #155 and #156 for 1958 Contracting Parties
  - In-progress for 1998 Contracting Parties
- Various national regulatory authorities
  - E.g. US NHTSA, UK Department of Transport, Transport Canada

Lack of international, automotive-focused standards

- Existing cybersecurity and OTA standards lack awareness of automotive-specific challenges
  - Common Criteria seen as too problematic to apply to a vehicle
- SAE J3061 went some way to filling the gap, but it’s not a standard
  - Just a “best practice” guidebook

Relevant standards

Cybersecurity engineering – ISO/SAE 21434

- Successor to SAE J3061
- Security against malicious attacks on E/E components of vehicles, leading to safety, financial, operational, or privacy issues (network/cloud infrastructure out of scope)
- Provides the “how” for UN reg #155 (CS)
- Focuses on the vehicle and its interfaces only

Software Updates – ISO 24089

- Safe and secure systems for providing wired and wireless (OTA) software updates to vehicles
- References aspects of ISO 26262, ISO PAS 21448, ISO/SAE 21434
- Provides the “how” for UN reg #156 (SU)
- Focuses on software update packages and delivery capabilities / infrastructure

Auditing of Cybersecurity Engineering

- **ISO PAS 5112**
- Very early stages of development (second Working Draft)
- References ISO/SAE 21434 and the technical audit handbook ISO 19011
- Due for publication soon after ISO/SAE 21434

Functional Safety

- **ISO 26262**
- Ensuring safety in the event of faults in E/E components
- Contains 12 parts
- Published 2 times already, latest in 2018

Safety Of The Intended Functionality

- **ISO PAS 21448**
- Ensuring safety of intended functionality i.e. in the absence of faults
- First (interim) version published, a more complete version is in the works

Relevant standards

Cybersecurity engineering – ISO/SAE 21434

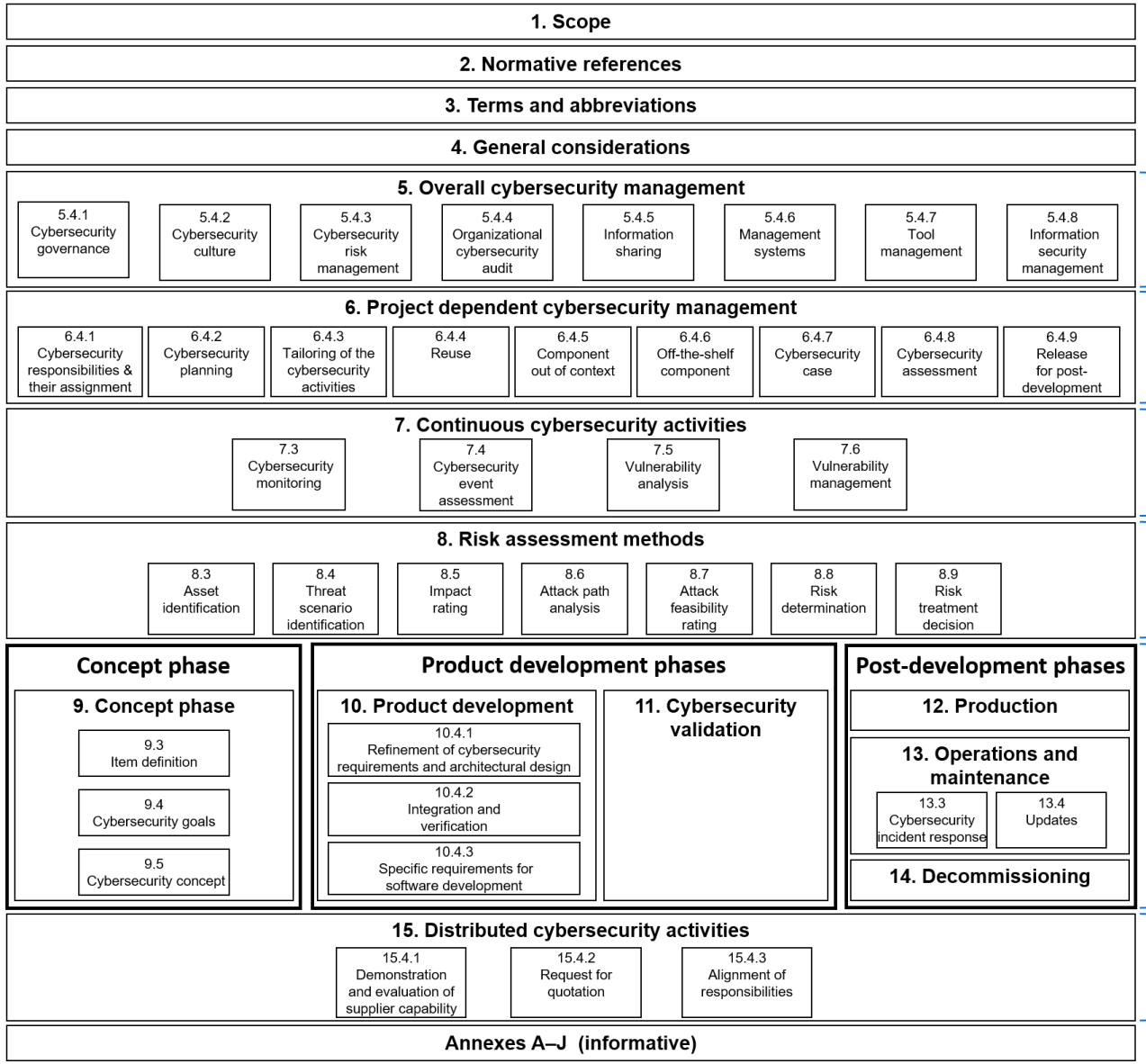
- Successor to SAE J3061
- Security against malicious attacks on E/E components of vehicles, leading to safety, financial, operational, or privacy issues (network/cloud infrastructure out of scope)
- Provides the “how” for UN reg #155 (CS)
- Focuses on the vehicle and its interfaces only

Software Updates – ISO 24089

- Safe and secure systems for providing wired and wireless (OTA) software updates to vehicles
- References aspects of ISO 26262, ISO PAS 21448, ISO/SAE 21434
- Provides the “how” for UN reg #156 (SU)
- Focuses on software update packages and delivery capabilities / infrastructure

- Provide automotive industry with common and internationally agreed understanding of engineering best practice for automotive cybersecurity and software updates i.e. provide state of the art
- Goal oriented i.e. do not provide any specific technology / technical solutions
- Define common language and terminology, to harmonise communication e.g. OEMs, supply chain, aftermarket
- Do not provide any certification requirements, but can be used as a reference
  - ISO PAS 5112 seeking to solve this for ISO/SAE 21434

Content of ISO/SAE 21434 (DIS)



Organisational-level aspects

Project-level aspects for development of vehicles and their components

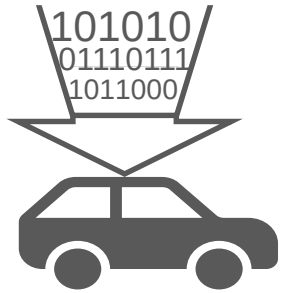
Ongoing activities for vehicles / components that are in concept, development or post-development

Methods to be used during the different engineering phases of items and components

Minimum cybersecurity technical goals to be achieved during the engineering phases of items and components, calling upon Risk Assessment Methods when needed

Cross-organisational aspects between companies operating as an OEM, Tier-1, Tier-2, etc.

Content of ISO 24089 (WD3.1)



1. Scope			
2. Normative References			
3. Terms and Definitions			
4. Organization Level Software Update Requirements			
5. Project Level Software Update Requirements			
6. Infrastructure for Software Update Engineering Design and Development	7. Software Update-Capable Vehicles and Components Development	8. Software Update Package Development	9. Software Update Campaign Operations

Organisational-level aspects

Project-level aspects for development of software updates and support systems

6) Ensure secure infrastructure for software update config, dependencies, distribution, and storing of results

7) Ensure vehicles and their components have sufficient capabilities for correctly receiving and processing updates e.g. quality, safety, security, and intended functional requirements, handling of OTA-specifics (e.g. recovery)

8) Ensure correct management of software update packages, including correct identification of targets for software, correct update package assembly, and verification & validation of the update package

9) Ensure correct management of software update distribution “campaigns”, including planning, execution, notifications, termination (if necessary) and documentation

Timelines for ISO/SAE 21434 & ISO 24089

14 Jan: SAE J3061 published
"Surface Vehicle Recommended Practice - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"

10 April: First internal Working Draft document
14 other versions later followed

18 March: Post-CD draft for UNECE
Contained resolution of ~75% comments from CD

12 Feb – 6 May: Publication of DIS and ballot period

May: Final publication

ISO/SAE 21434

2016 | 2017 | 2018 | 2019 | 2020 | 2021

March: Formation of the joint standards committee to develop ISO/SAE 21434 was agreed and development began

22 Sept – 17 Nov: Committee Draft (CD) document and ballot

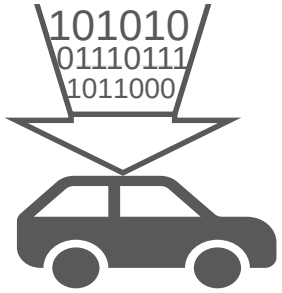
4 June – 16 July: Internal "Summer Baseline" draft and ballot

Feb/Mar: Publication of FDIS and ballot period

March: Agreement of NWIP on Software Updates

1 Feb – 31 Mar: CD document and ballot

30 Jun – 31 Aug: FDIS document and ballot



ISO 24089

2019 | 2020 | 2021 | 2022

4-5 July: ISO 24089 development begins, utilising text from Updates clause in ISO/SAE 21434

1 Nov – 31 Jan: DIS document and ballot

1 Nov: Final publication

Conclusion

Conclusion

- **Many challenges to automotive cybersecurity**
  - Securing the vehicle and connected systems, on an ongoing basis, whilst adhering to “right to repair”
  - Dealing with a vast supply chain
  - Managing cybersecurity through-out vehicle life-cycle
- **New regulations demanding more cyber-secure vehicles**
  - Regulations define the “what must be done”
  - Coming into force very soon
  - Mostly harmonised across regions
  - Seek to enforce a baseline of cybersecurity, possibly even raising the bar in some instances
- **Standards helping to overcome the technical challenges and meet regulatory demands**
  - Standards provide the “how to do what must be done”
  - Define the state-of-the-art
  - Not yet published

- **Good engineering practices followed by all in the industry, with the capability to monitor, detect and respond to newly-found vulnerabilities is key!**

How is BlackBerry helping automotive cybersecurity?

- **QNX Real-Time OS & hypervisor**
  - Micro-kernel based, POSIX-compliant OS
  - Highest functional safety ratings (including ISO 26262 ASIL-D, IEC 61508 SIL 3)
    - Developed with a high safety-related discipline
  - https://blackberry.qnx.com/en/software-solutions/embedded-software/qnx-neutrino-rtos
  - https://blackberry.qnx.com/en/software-solutions/embedded-software/qnx-hypervisor-safety

- **Intelligent Vehicle Data Platform**
  - Enables easier access to sensor data whilst retaining security and safety of the vehicle
  - Advanced services/synthetic sensors, utilising AI
  - https://blackberry.qnx.com/en/aws

- **Unified end-point security for vehicles**
  - Using ML for blocking malware and cyberattacks, driver recognition via behaviour analytics, proactive vehicle diagnostics for maintenance requirements
  - https://blogs.blackberry.com/en/2020/06/bringing-endpoint-security-capabilities-to-the-world-of-connected-vehicles

- **Security consultancy services**
  - WP.29 regulation readiness assessments
  - Software security validation e.g. Software Bill Of Materials (SBOM), OSS assessments, security software assessments, penetration testing
  - https://blackberry.qnx.com/en/professional-services/security-services

Thank you for listening!

Any questions?