BlackBerry Intelligent Security. Everywhere.

UNECE WP.29 regulations

13th October 2022

Nick Russell, BSc (Hons), MBCS

Director, Standards

nrussell@blackberry.com linkedin.com/in/nickruss/

Introduction

- Regulations involving vehicles are commonly written at an international level in order to harmonise vehicle production requirements across the globe

- The United Nations is the main body tasked with this, specifically the UN Economic Commission for Europe (UNECE)
  - Despite the name, it consists of members from around the world

- Local/regional regulatory authorities are typically involved at the international level

- International regulations are then adopted by various countries/regions
  - Adoption depends on the contract that they have signed-up to

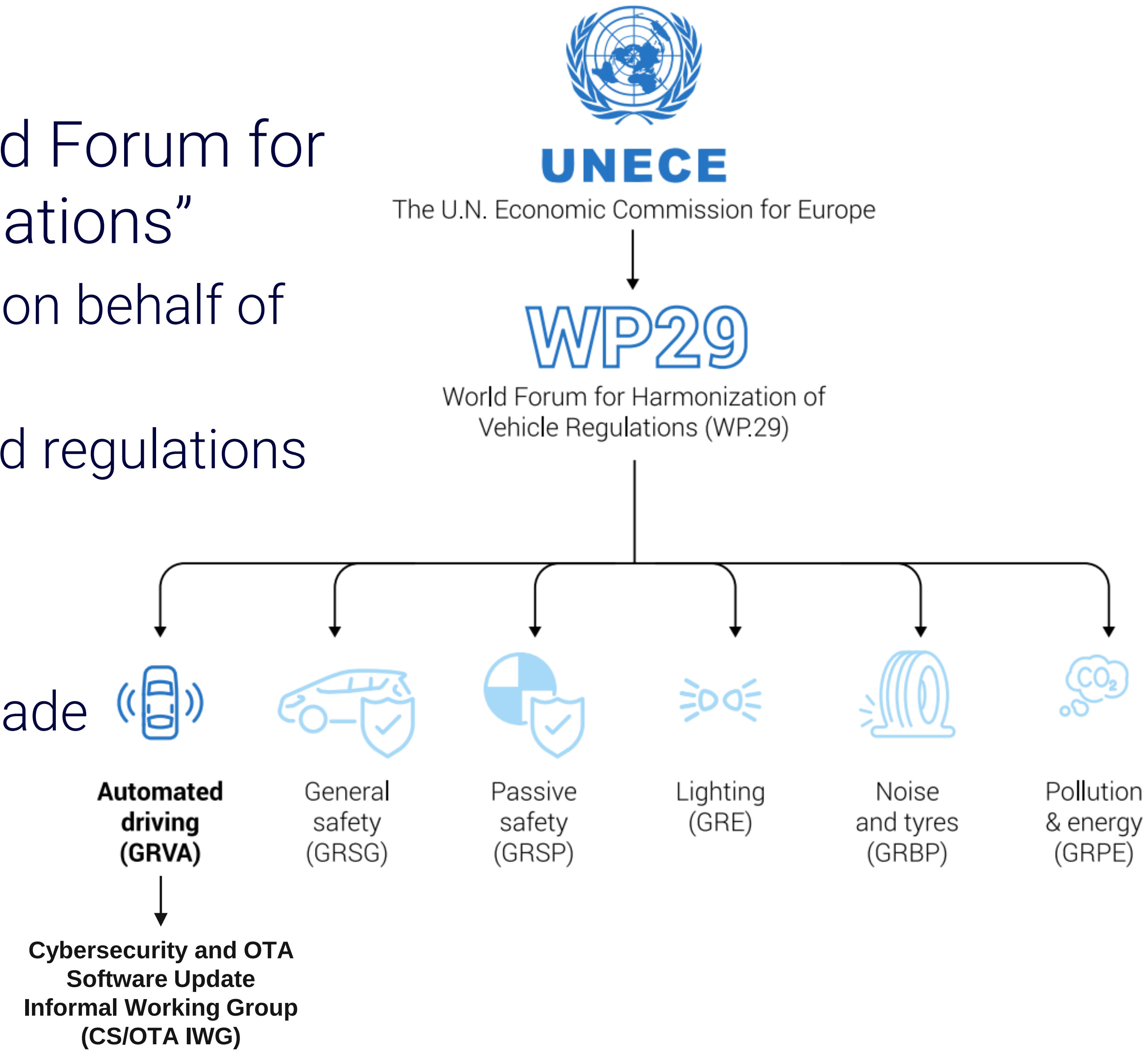
The United Nations Economic Commission for Europe (UNECE)

- United Nations Economic Commission for Europe (UNECE) was set up in 1947
  - 56 member states across Europe, North America and Asia
- Promotes pan-European economic integration, sustainable development and economic prosperity
- Provides regional implementation of outcomes of global United Nations Conferences and Summits
- Sets out norms, standards and conventions to facilitate international cooperation within and outside the region
- Work areas:
  - Economic cooperation
  - Environmental policy
  - Forests
  - Housing and land
  - Population
  - Sustainable energy
  - Statistics
  - Trade
  - Transport

UNECE WP.29 – Overview

- UNECE Working Party 29: “World Forum for Harmonization of Vehicle Regulations”
  - Worldwide regulatory forum acting on behalf of the whole UN
  - Develops internationally-harmonized regulations

- Objectives:
  - Reduction of technical barriers to trade
  - Facilitate border crossing
  - Reduction of costs to consumers
  - Cleaner, safer and more secure vehicles



UNECE

The U.N. Economic Commission for Europe

WP29

World Forum for Harmonization of Vehicle Regulations (WP.29)

Automated driving (GRVA)

General safety (GRSG)

Passive safety (GRSP)

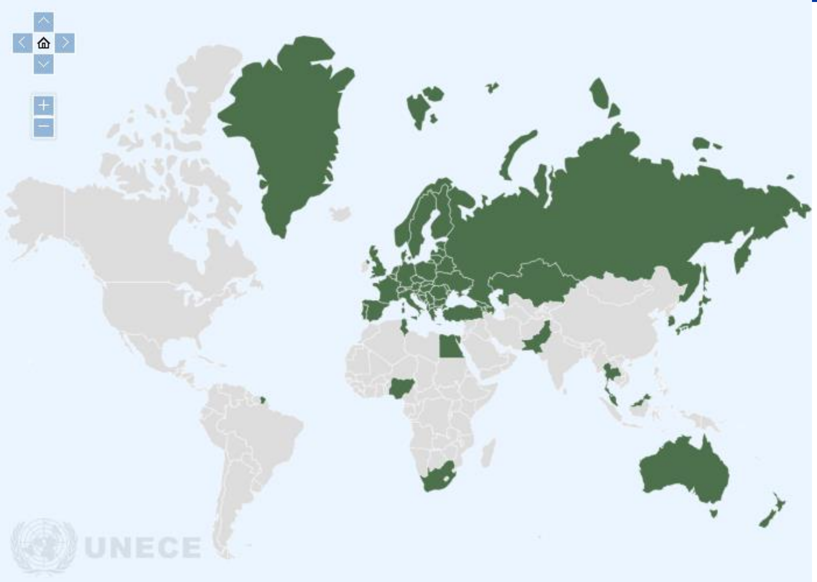
Lighting (GRE)

Noise and tyres (GRBP)

Pollution & energy (GRPE)

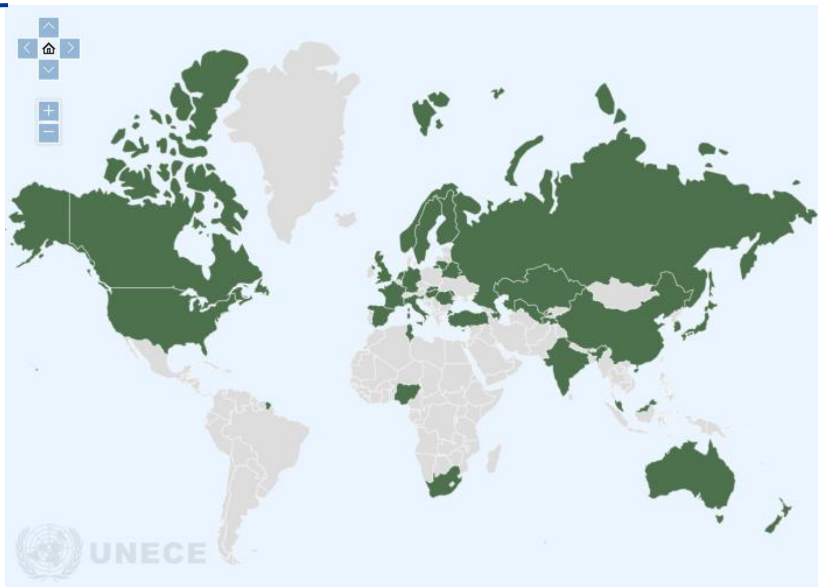
Cybersecurity and OTA Software Update Informal Working Group (CS/OTA IWG)

UNECE WP.29 – Who’s involved



- **1958 agreement**
  - 63 Contracting Parties including EU, UK, Japan, South Korea, Australia
  - Type Approval system of vehicle systems, parts and equipment
    - Government authority assesses regulatory conformance *before* vehicle allowed on roads
  - Mutual recognition of the Type Approvals granted by Contracting Parties
  - UN R155 on Cyber Security and UN R156 on Software Updates apply to new vehicle models from July 2022 and all vehicles from July 2024

- **1998 agreement**
  - 38 Contracting Parties including USA, Canada, China, India
    - Includes some 1958 agreement members too
  - Provides ”Global Technical Regulations” (GTRs)
    - Focus on solely on *technical* requirements
  - No conformance or Type Approval requirements; self-certification or homologation
  - Recommendations on uniform provisions concerning cyber security and software updates recently approved
    - Contains technical requirements from 1958 CP’s UN R155 and UN R156



Motivations for UN R155 & UN R156

Increase in vehicle functionality & connectivity

- Automated driving and associated safety concerns
- Increased connectivity of vehicles and related functions
- Increase of remotely-updateable software

Media attention on cyber attacks to vehicles

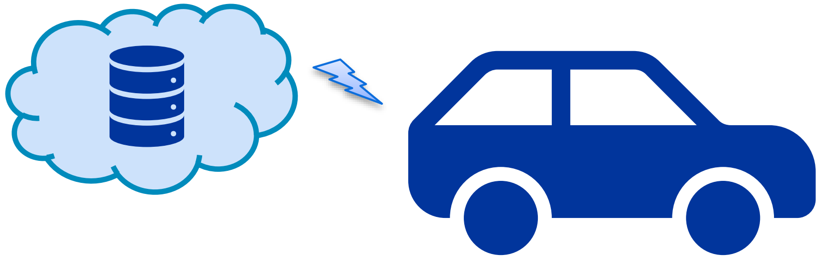
- Successful vehicle attacks making headline news
  - Jeep Cherokee hack by Charlie Miller and Chris Valasek in July 2015
  - Numerous remote keyfob attacks to steal high-end cars

Local regulatory concerns

- Self-regulation observed not to be working
- Need for consumer confidence and assurance
- Harmonised set of regulations to allow for import/export, driving vehicles over borders, etc.

Applicability of UN R155 & UN R156

- Cars, buses, vans, trucks and others having 4 or more wheels
- UN R156 also applies to agricultural and forestry vehicles, as well as their trailers (if ECU present)
  - UN R155 set to be expanded to these too later this decade



- 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

Content of UN R155 – 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

Vehicle Type

Design & development

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

Post-development

- 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 R155 – Detailed threats & mitigations

- Annex 5 contains:
  - Descriptions of threats and related vulnerability or attack method
  - Mitigations to the threats intended for vehicles
  - Mitigations to the threats outside of vehicles

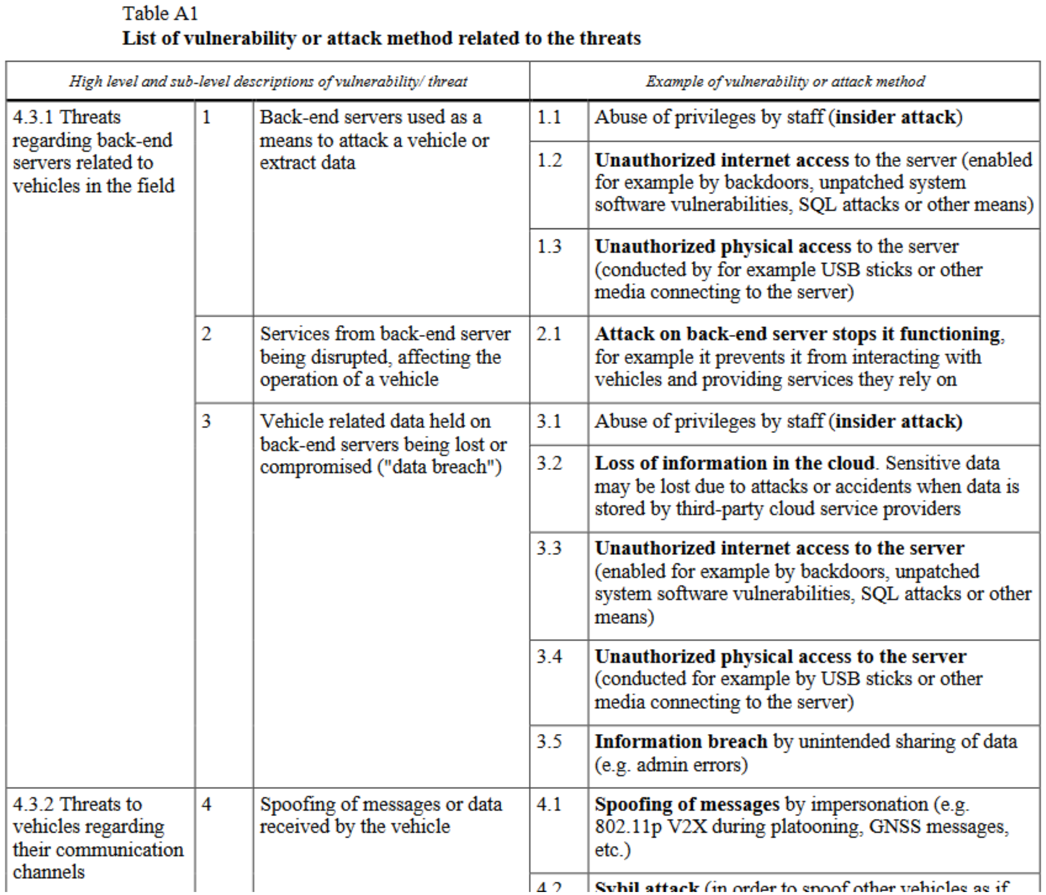


Table A1
List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.1 Threats regarding back-end servers related to vehicles in the field	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (**insider attack**)
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server)
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1	**Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (**insider attack**)
			3.2	**Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)
			3.5	**Information breach** by unintended sharing of data (e.g. admin errors)
4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	**Sybil attack** (in order to spoof other vehicles as if

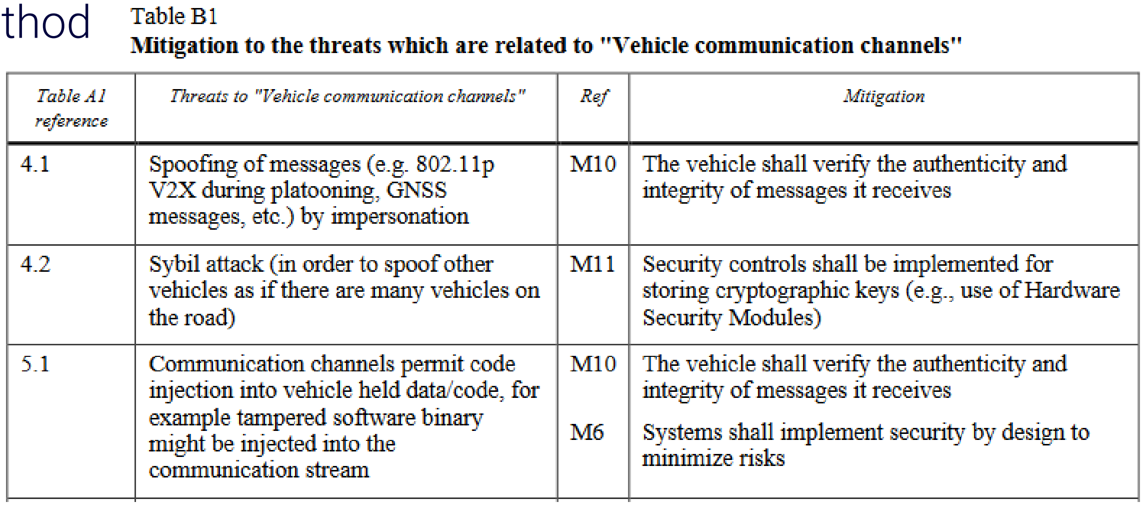


Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks

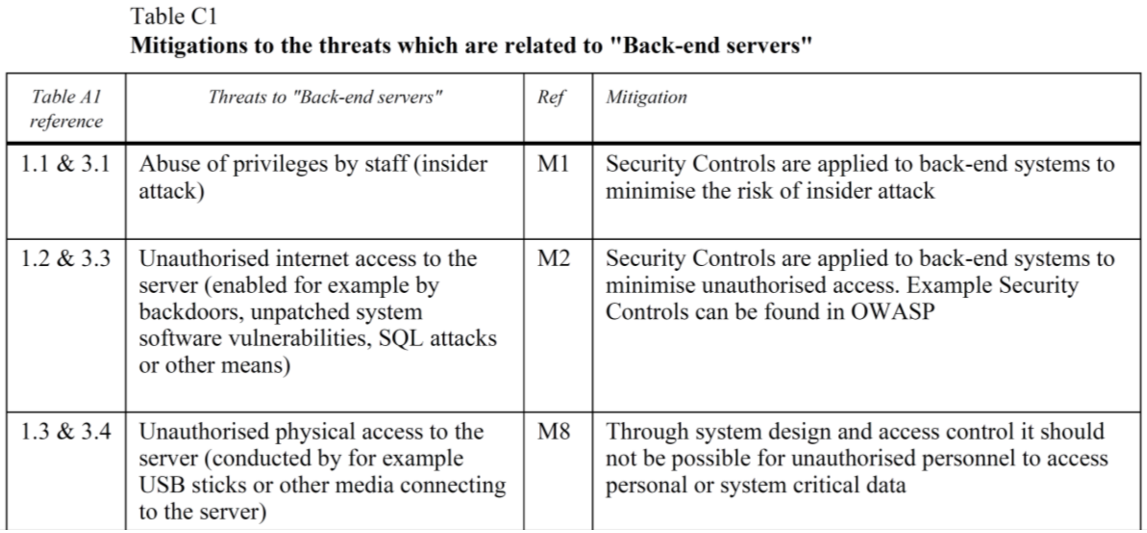


Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data

Content of UN R156 – 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

Vehicle Type

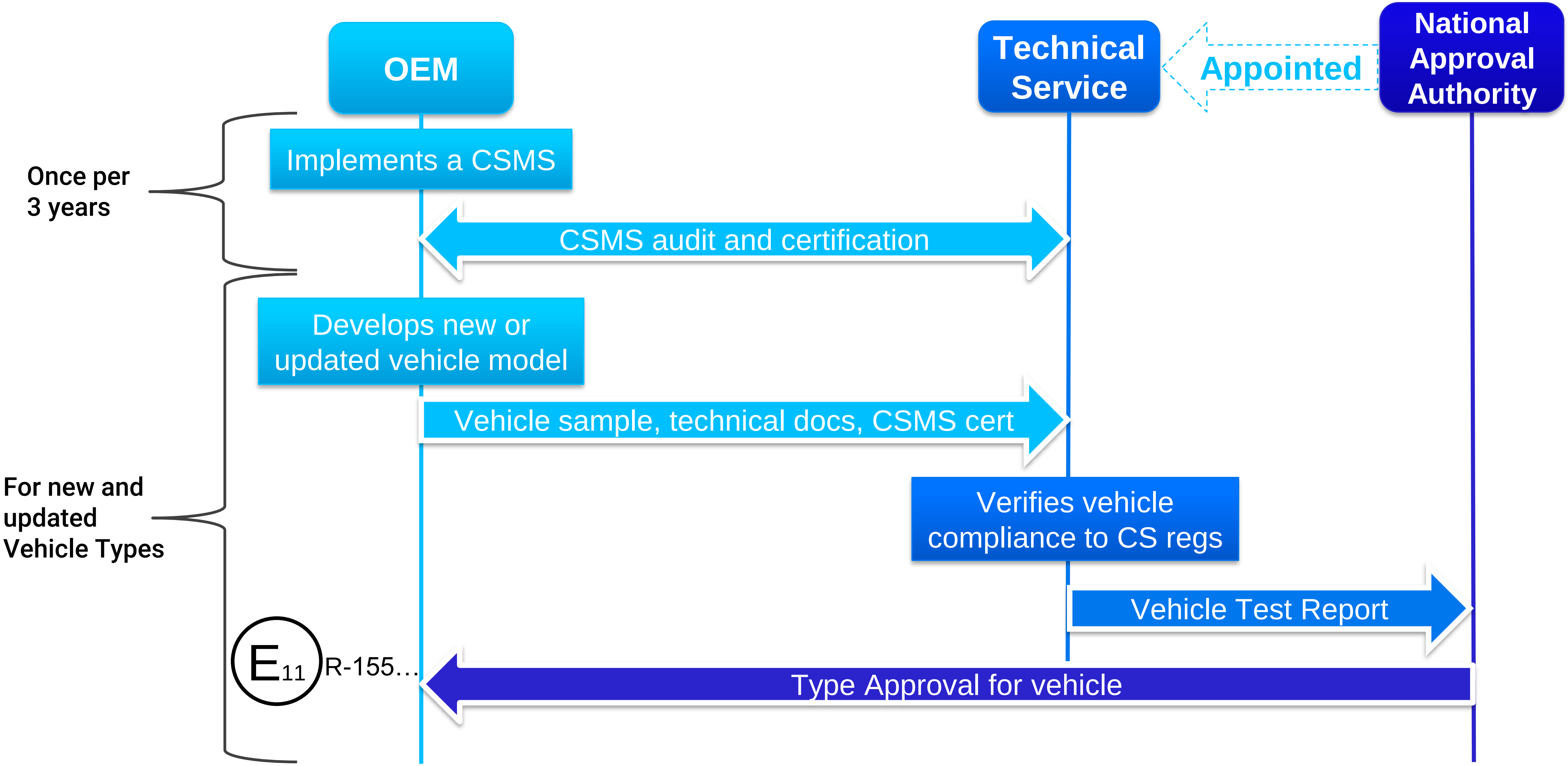
For all updates

- 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 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

Type Approval process for UN R155


OEM
Technical Service
Appointed
National Approval Authority
Once per 3 years
Implements a CSMS
CSMS audit and certification
For new and updated Vehicle Types
Develops new or updated vehicle model
Vehicle sample, technical docs, CSMS cert
Verifies vehicle compliance to CS regs
Vehicle Test Report
E11 R-155…
Type Approval for vehicle

Cybersecurity and Software Update regulations for 1998 CP countries

- Guidance document for 1998 Contracting Parties for vehicle cyber security and software approved earlier this year
  - *"Proposal for Recommendations on uniform provisions concerning cyber security and software updates"*
  - Technical requirements extrapolated from UN R155 and UN R156
    - Some rephrasing and removal of certification related material
  - Targeted at vehicle manufacturers for self-certification
  - Drafted by same group in UNECE WP.29 that drafted UN R155 and UN R156 i.e. CS/OTA IWG under GRVA
    - NHTSA (US) and Transport Canada were pivotal in its drafting, but so far unclear if/when they will adopt requirements into local legislation
    - If they do, then previous compliance to UN R155 and UN R156 will mean an easier ride to comply with this set of recommendations

- No GTR currently planned
  - Guidance only at this stage, pending industry feedback
    - So may become a GTR later

References

- All UNECE regulations for the 1958 agreement
  https://unece.org/un-regulations-addenda-1958-agreement
  - UN R155 (Cyber Security)
    https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
  - UN R155 interpretation document
    https://unece.org/transport/documents/2022/04/working-documents/grva-proposal-amendments-interpretation-document-un
  - UN R156 (Software Updates)
    https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update
  - UN R156 interpretation document
    https://unece.org/transport/documents/2020/12/working-documents/grva-proposals-interpretation-documents-un-regulation
- All UNECE Global Technical Regulations (GTRs) for the 1998 agreement
  https://unece.org/transport/standards/transport/vehicle-regulations-wp29/global-technical-regulations-gtrs
  - Proposal for Recommendations on uniform provisions concerning cyber security and software updates
    https://unece.org/transport/documents/2022/04/working-documents/grva-proposal-recommendations-uniform-provisions

How BlackBerry is helping automotive cybersecurity and software updates

QNX OTA

Modular and flexible OTA solution for seamless software updates, enabling new requirements as products evolve

Leverages field-proven BlackBerry security technologies, including BlackBerry Certicom® PKI and BlackBerry Jarvis™ binary static application security testing

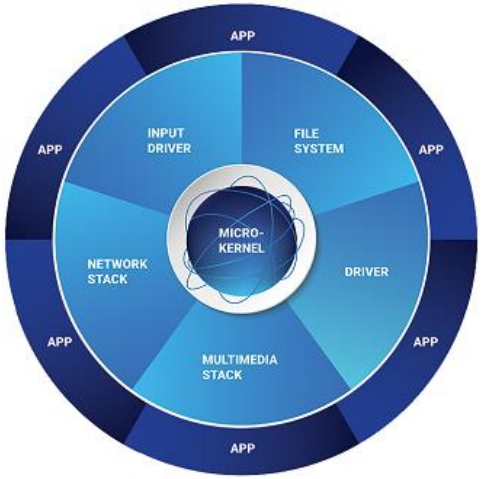
blackberry.qnx.com/en/products/security/qnx-ota

QNX Real-Time OS & Hypervisor

Micro-kernel based, POSIX-compliant real-time embedded OS and hypervisor

Highest functional safety ratings (including ISO 26262 ASIL-D, IEC 61508 SIL 3)

Embedded in 215+ million vehicles on the road today



www.blackberry.com/qnx

Cybersecurity Consultancy Services

WP.29/UN R155 readiness assessments

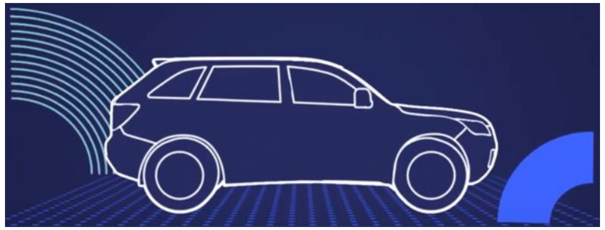
Software security validation e.g. OSS assessments, security software assessments, Software Bill Of Materials (SBOM), penetration testing

blackberry.qnx.com/en/professional-services/security-services

IVY (Intelligent Vehicle Data)

Vehicle-first, cloud-connected software platform, that combines vehicle data intelligently into a consistent format, creating rich and actionable insights in a safe and secure manner

Insights can be easily consumed by apps on or off the vehicle



www.blackberry.com/ivy

Thank you

BlackBerry. Intelligent Security. Everywhere.

Nick Russell, BSc (Hons), MBCS
Director, Standards
nrussell@blackberry.com
linkedin.com/in/nickruss/