Automotive Cybersecurity Regulations

Dr. Kai Frederik ZASTROW
Senior Fellow Regulation Certification Standards, Stellantis
Chairman of OICA Cluster 4 Cybersecurity and Software Updates

STELLANTIS

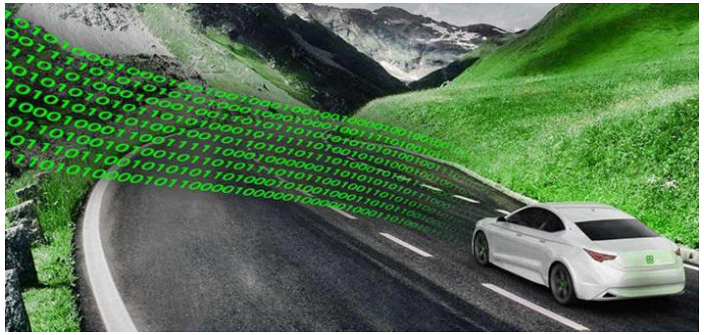
OICA Organisation Internationale des Constructeurs d'Automobiles
International Organization of Motor Vehicle Manufacturers

Why cybersecurity regulation?

- Risk of cyberattacks
  - **Safety/Security impact**:
    - Hacker may get access to **private data** or may **manipulate** existing vehicle software
    - Hacker may use vehicle as weapon for **criminal actions** / terrorist attacks
  - **Economic impact:**
    - Worldwide cybersecurity market: 3,1 billion € (2004), 67 billion € (2015) and 152 billion € (2020 forecast Gartner).
    - Automotive cybersecurity market: about 683 M € in 2023 (IHS Markit)
    - Economic risk for vehicle manufacturer, e.g. for recalls

- Objective of the regulation
  - **Protect the vehicle from cyber-attacks**

Why SW update regulation?



- Update software on vehicles during the whole vehicle life in order to:
  - **Ensure safety/security** of the vehicle (bug fixes, cybersecurity updates, etc.)
  - Maintain functionality and **compliance with legal acts** (traffic rules, etc.)
  - **Add new functions** (e.g. infotainment) **without** impact on type approved characteristics.
  - **Add new functions** (e.g. ADAS functionalities) **with** impact on type approved characteristics that are covered by new/extended type approvals.

- Objective of the regulation
  - **Ensure that the SW on a vehicle is and stays compliant with vehicle homologation**

Global Automotive Standards and Regulations to address Cybersecurity and SW updates

UN / WP.29 – World Forum for Harmonization of Vehicle Regulations

- UN Regulation 155 on Cyber Security
  UN Regulation 156 on SW updates

European Union

- Cybersecurity Act
- General Data Protection Regulation
- NIS Directive (Network and Information Security)

ISO TC22/SC32/WG11 - Cybersecurity

- ISO/SAE 21434 Cybersecurity Engineering

ISO TC22/SC32/WG12 – Software update

- ISO 24089 Software Update Engineering

China

- Cybersecurity Law & Data Security Law
- Personal Information Protection Law
- Information Security: SAC/TC 260
- Automotive: SAC/TC 114/SC 34/WG Cyber

National Discussions

- Germany VDA QMC
- UK BSI PAS 1885:2018
- …

USA

- NHTSA Cybersecurity Guidelines

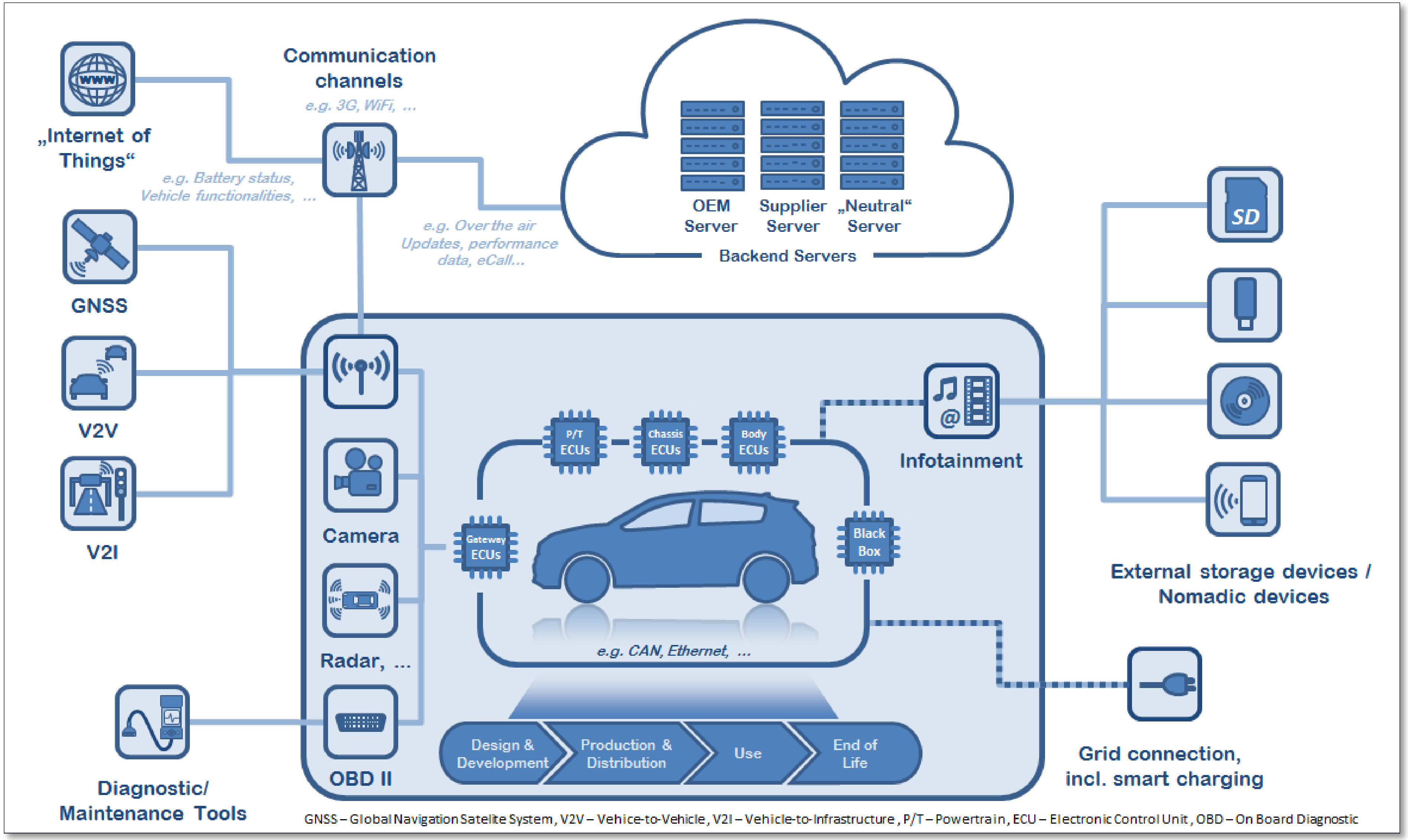
UN Regulations (adopted in June 2020) are worldwide consensus:

Developed under GRVA (chaired by Germany, Japan and China)
/ TF Cybersecurity & OTA issues (chaired by UK, Japan and USA).

Cybersecurity concerns the **whole vehicle**

Example for risks of unsecured access:

⇒ **Cybersecurity cannot be covered by certification of only some specific components**



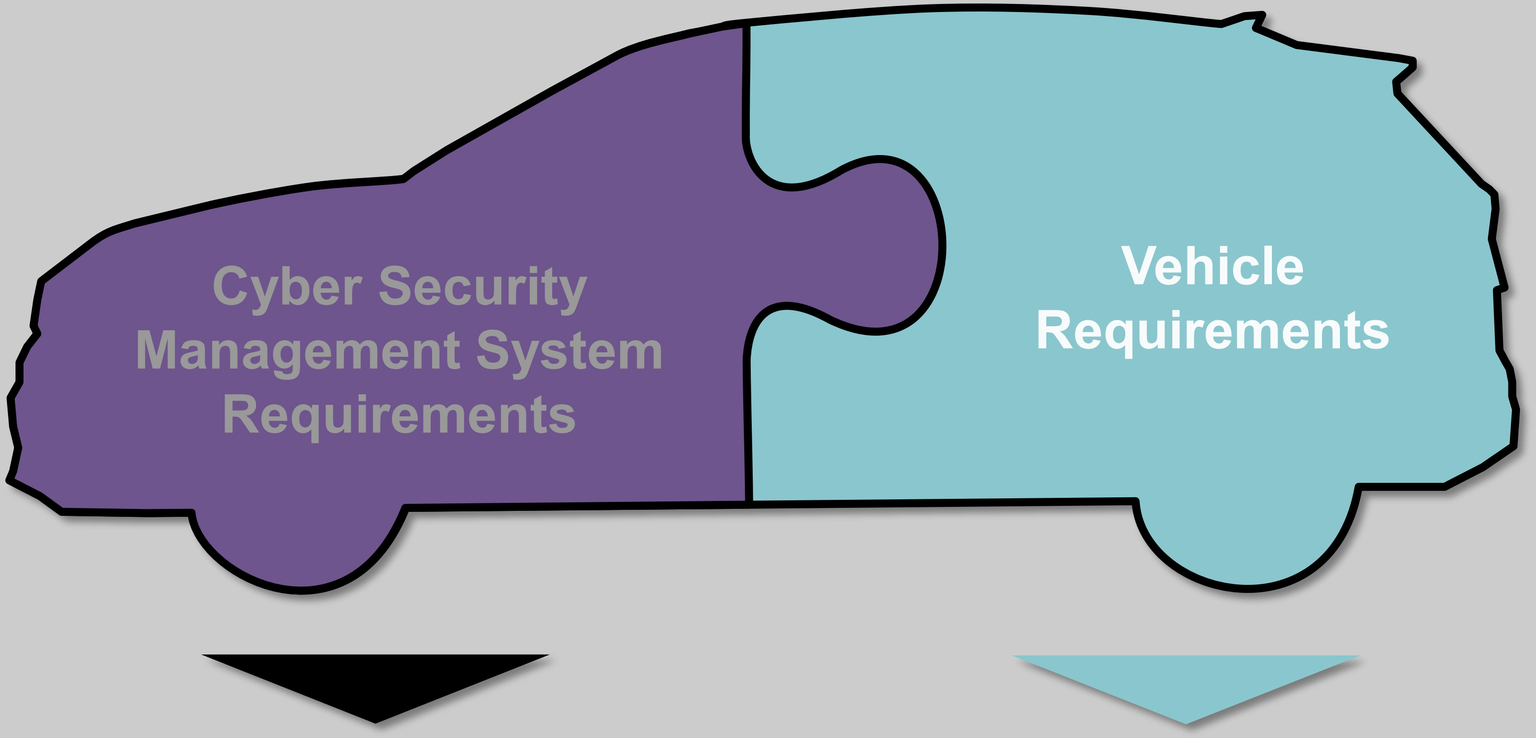
GNSS – Global Navigation Satelite System, V2V – Vehicle-to-Vehicle, V2I – Vehicle-to-Infrastructure, P/T – Powertrain, ECU – Electronic Control Unit, OBD – On Board Diagnostic

UN Regulation 155 on Automotive Cybersecurity

Split approach for the cybersecurity assessment:

i) Assessment and certification of vehicle manufacturer **Cyber Security Management System**

ii) Assessment and certification of **vehicles**



Cyber Security Management System Requirements

Vehicle Requirements

Organizational structure & processes

Design of the vehicle EE architecture, risk assessment and implementation of mitigations

Annex 5, Part A: List of threats

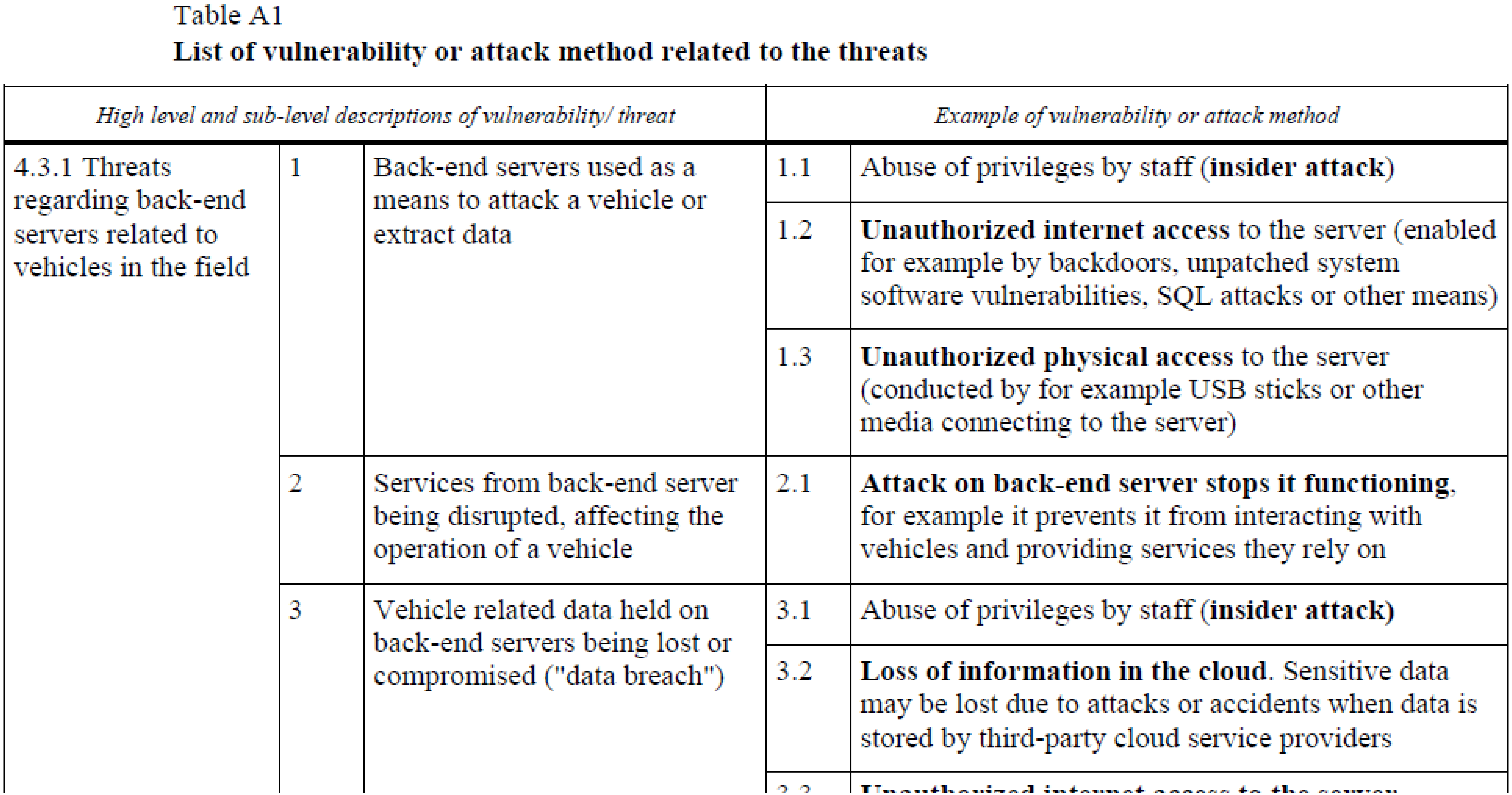


Table A1

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**

Annex 5, Part B: Mitigations on vehicles

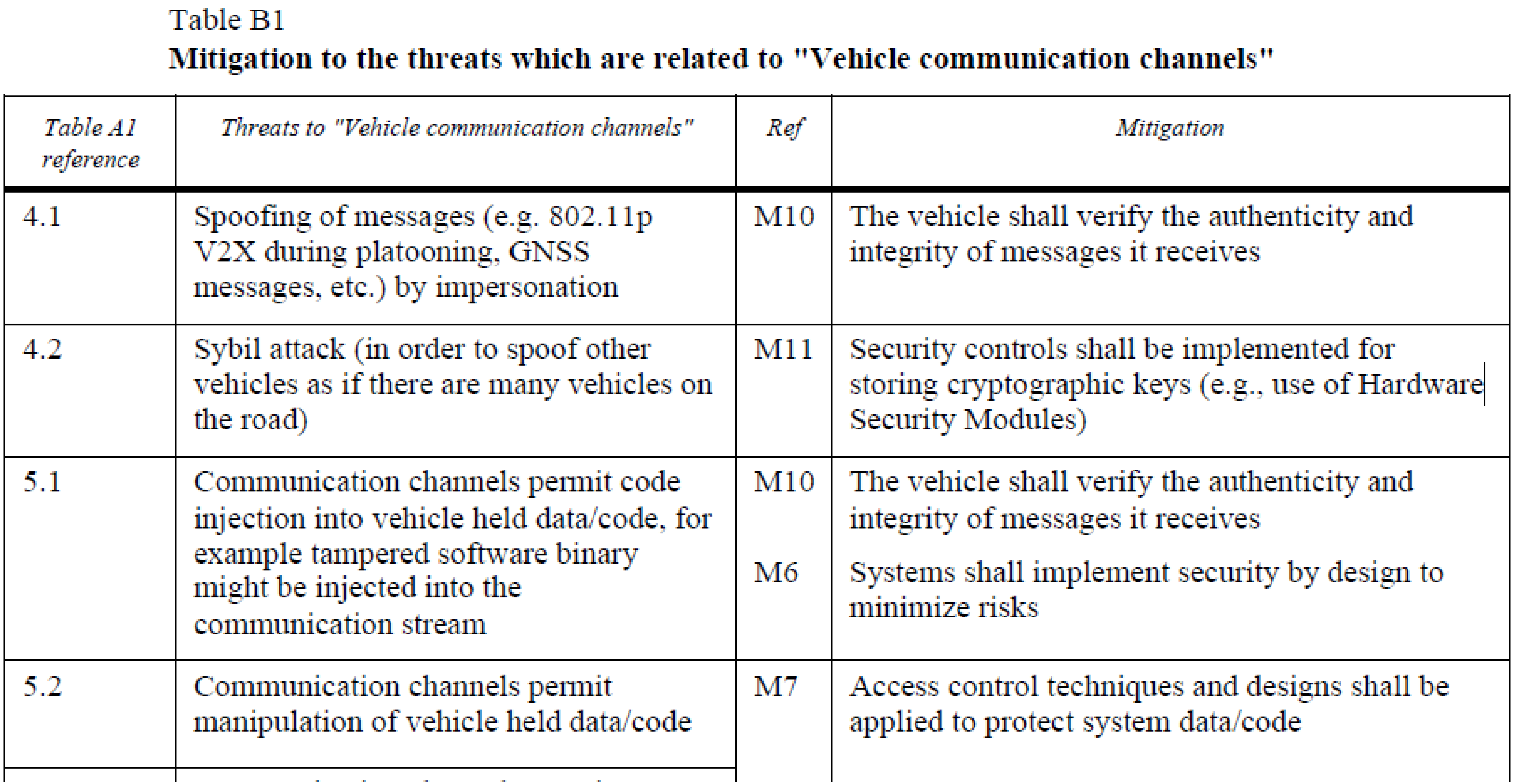


Table B1

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
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Access control techniques and designs shall be applied to protect system data/code

Annex 5, Part C: Mitigations outside the vehicle

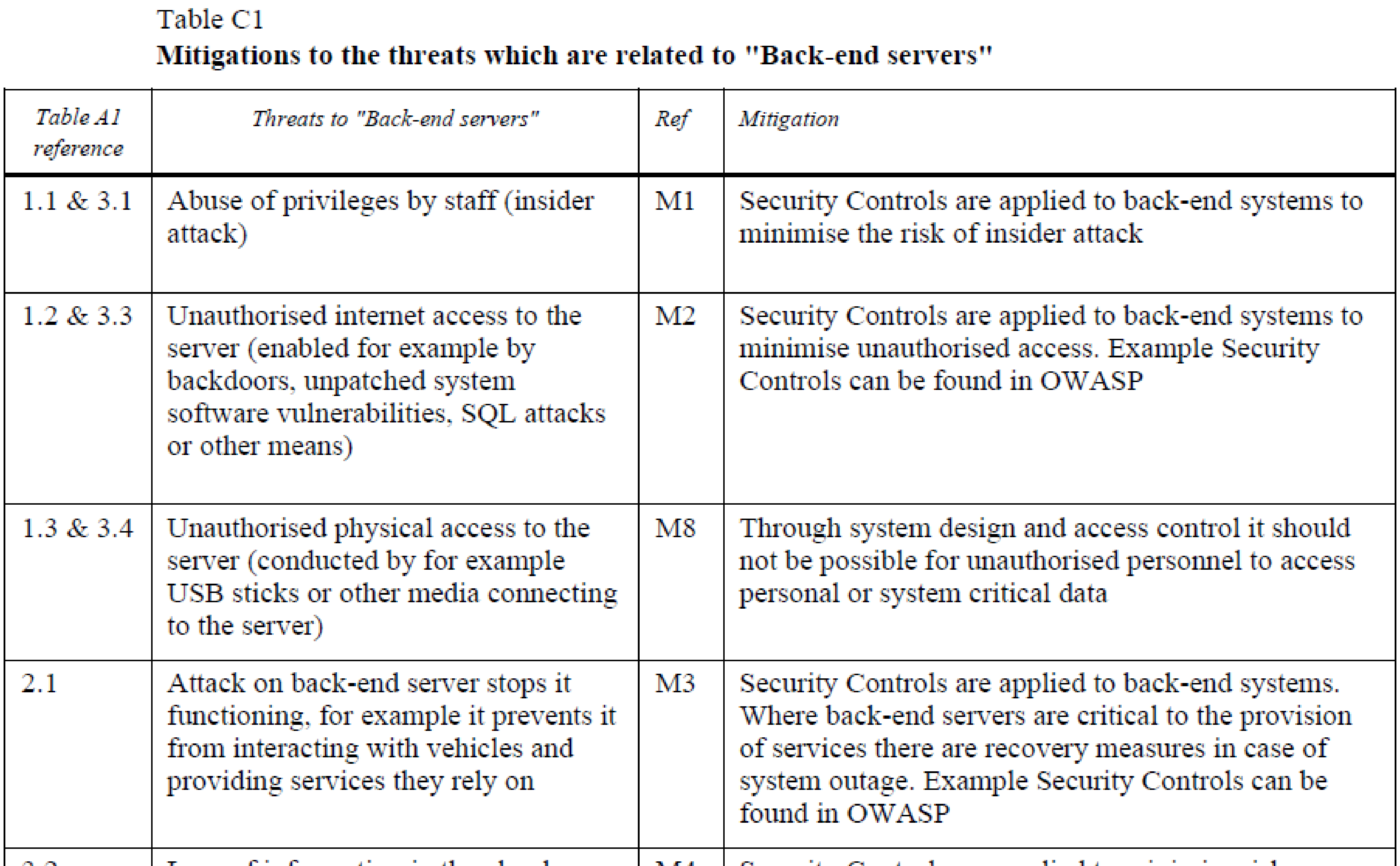


Table C1

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
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	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

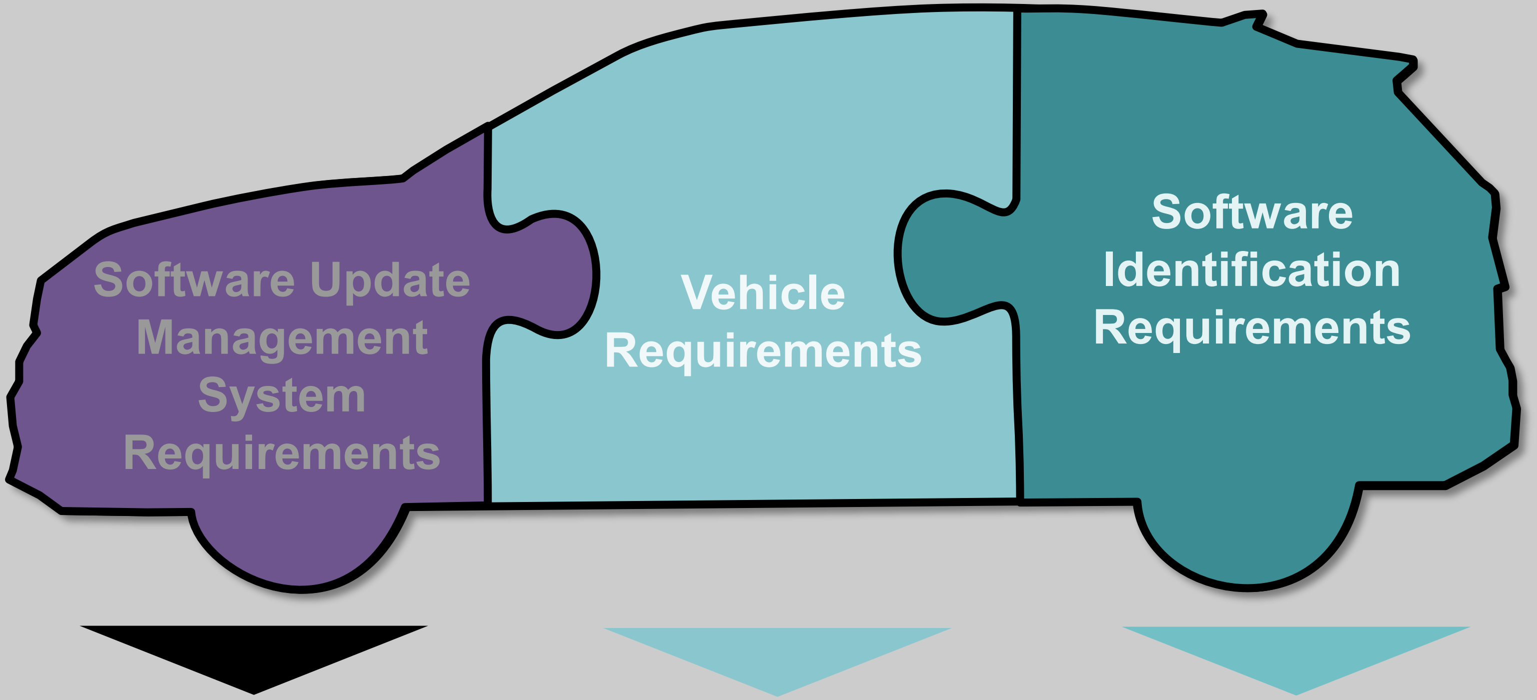
UN Regulation 156 on SW updates

Split approach:

i) Assessment and certification of vehicle manufacturer **Software Update Management System**

ii) Assessment and certification of **vehicles**

iii) Implementation of **software identification numbers** for specific regulations



Software Update Management System Requirements
Vehicle Requirements
Software Identification Requirements

Organizational structure & processes, incl. management of SW identification

Requirements for safe execution of SW updates and user information

Implementation of SW identification numbers (RXSWIN) in specific regulations

R155 Cybersecurity & R156 SW update implementation

- Jan 2021: Entry into force: legal acts are available for application by UN Contracting Parties.
- UN Contracting Parties require them in their national vehicle type approval:
  - Japan
    - R155 & R156
      - Immediately for automated vehicles SAE level 3 or higher
      - July 2022 for new whole vehicle types & July 2024 for new registrations if SU affecting type approval and OTA capability
      - Jan 2024 for new whole vehicle types & May 2026 for new registrations: R155 & 156 if SU affecting type approval and no OTA capability; R155 in all other cases
  - European Union
    - R155: 6 July 2022 for new whole vehicle types & 7 July 2024 for new registrations
    - R156: under preparation (via delegated act amending EU 2018/858)
  - Other countries may follow

“Recommendations on uniform provisions concerning cyber security and software updates”

- Document produced by UN Task Force is as much as possible aligned with R155 and R156 for countries that have no type approval regime.
  - Covers both: cyber security and software update processes
  - Covers the whole life cycle of a vehicle model (from design to post-production)
  - Lists technical requirements for the vehicle and for the management system
  - Considers the concept of SW identification numbers (RXSWIN)
- Recommendation WP.29/GRVA/2022/5 adopted by GRVA in January 2022
- Need to follow next steps

OICA

Opportunities for global harmonization?

Opportunities for global harmonization

- Make sure that the **54 signatory countries** of the UN Geneva 1958 Agreement **apply the UN Regulations** (and do not invent national requirements)
- Make sure that countries that do not apply directly R155 and R156 **apply at least the Recommendations** on uniform provisions
- **Harmonize the Chinese draft national standards** under development by SAC/TC 114/SC 34/WG Cyber **with ISO and UN**.

THANK YOU FOR YOUR INTEREST!

Link to UN documents

- UN Regulation 155 Cybersecurity https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
- Interpretation document on Cybersecurity http://unece.org/sites/default/files/2020-12/ECE-TRANS-WP29-2021-059e.pdf
- UN Regulation 156 SW update https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update
- Interpretation document on SW update http://unece.org/sites/default/files/2020-12/ECE-TRANS-WP29-2021-060e.pdf
- Recommendations on uniform provisions concerning cyber security and software updates https://unece.org/sites/default/files/2021-12/ECE-TRANS-WP29-GRVA-2022-05e.pdf
- UN Regulation 157 ALKS (see chapter 9 with link to UN Regulations 155 and 156 and Annex point 19) https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks
- Consolidated Resolution on the Construction of Vehicles (R.E.3), Annex 7: Provisions on Software Identification Numbers (integration of RXSWIN in system regulations) http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-082e.pdf