**Proposed reformulation of CSMS and SUMS related requirements**

**1 Introduction**

The first proposal, found in section 2 below, seeks to enhance the currently proposed draft guidelines/GTR requirements relating to CSMS and SUMS to:

* Retarget the requirements to vehicle manufacturers, in alignment with other sections/existing text in the current IWG proposal
* Harmonise the language used between the requirements and utilise defined terms
* Fix the prose e.g. consistent bullet notation, phrase using active voice, ensure the subject the sentence appears early-on in order to enhance understanding of the requirements, etc.

The second proposal, found in section 3 below, seeks to provide observations and suggestions on the defined terminology in the Definitions clause.

The base text of proposals has been taken from document TFCS 20-05, published 22nd December 2020 at <https://wiki.unece.org/pages/viewpage.action?pageId=113345490>. Embedded comments have been retained in all instances so as to avoid disruption of ongoing discussions between delegations.

For any discussion of the below, the authors gladly welcome off-line feedback, and can be contacted [here](mailto:nrussell@blackberry.com;tsuzuki@blackberry.com?subject=CS/OTA%20IWG%20-%20comment%20doc%20on%20TFCS%2020-05).

**2 Proposal for CSMS and SUMS related requirements**

The following proposes enhancements to text from TFCS 20-05:

1. MANAGEMENT SYSTEMS

1.1. Management System for Cyber security

1.1.1. The vehicle manufacturer shall manage cyber security throughout the following phases: (7.2.2.1)

(a) Development phase;

(b) Production phase; and

(c) Post-production phase.

1.1.2. The vehicle manufacturer shall implement and maintain processes to: (7.2.2.2)

(a) manage cyber security at an organisational level;

(b) identify risks to vehicles, which shall include consideration of the threats in Annex 1, Part A, and other relevant threats;

(c) assess, categorise and treat identified risks;

(d) verify that risks identified are appropriately managed;

(e) test the cyber security of a vehicle;

(f) ensure that risk assessments are kept current;

(g) monitor for, detect and respond to cyber-attacks, cyber-threats and vulnerabilities on the vehicle~~;~~

(h) assess whether the cyber security measures implemented remain effective when new cyber threats or vulnerabilities are identified; and

(i) provide data to enable analysis of attempted or successful cyber-attacks.

1.1.3. The vehicle manufacturer shall implement and maintain processes to mitigate cyber threats and vulnerabilities that are identified as requiring a response from the manufacturer within a reasonable timeframe. (7.2.2.3)

1.1.4. The vehicle manufacturer shall implement and maintain processes to ensure that the cyber security monitoring specified in section 1.1.2(g) is continual and includes: (7.2.2.4)

(a) vehicles in the field; and

(b) the capability to analyse vehicle data and vehicle logs to detect cyber threats, vulnerabilities and cyber attacks. The capability shall respect the privacy rights of vehicle owners and drivers, particularly with respect to consent.

1.1.5. The vehicle manufacturer shall manage cyber security related dependencies that may exist with contracted suppliers, service providers or manufacturer’s sub-organizations. (7.2.2.5.)

1.2 Management System for Software Updates

1.2.1 The vehicle manufacturer shall implement and maintain processes to:

(a) document information relating to software updates (7.1.1.1);

(b) securely maintain the information documented in 1.2.1 part (a) (7.1.1.1);

(c) make the information documented in 1.2.1 part (a) available to appropriate authorities upon request (7.1.1.1);

(d) uniquely identify all initial and updated versions of software on [~~the vehicle/~~regulated systems of the vehicle], including integrity validation data, and relevant hardware components (7.1.1.2);

(e) access and update information regarding software versions bearing parts that are specified in national legislation or regulation for a vehicle or vehicle system before and after an update, which shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software (7.1.1.3);

(f) verify that the software version(s) present on a component of a system or function specified in national legislation or regulation for a vehicle or vehicle system are consistent with information stored by the manufacturer according to 1.2.1 part (e) (7.1.1.4);

(g) identify interdependencies of the updated system with other system(s) (7.1.1.5);

(h) identify target vehicles for a software update (7.1.1.6);

(i) confirm the compatibility of a software update with the target vehicle(s)'s configuration before the software update is issued, including an assessment of compatibility between the last known software/hardware configuration of the target vehicle(s) and the software update to be issued (7.1.1.7);

(j) determine whether a software update will affect any system that is subject to national legislation or regulation, including whether the update will impact or alter any of the parameters used to define the systems the update affects, or whether it changes any parameters that are subject to national legislation or regulation (7.1.1.8);

(k) determine whether a software update will add, alter or enable any function(s) that were not present, or enabled, when the vehicle was certified according to national legislation or regulation, or whether an update will alter or disable any other parameters or functions that are subject to national legislation or regulation, including consideration of whether:

(1) regulated information (according to national legislation or regulation) regarding the vehicle will need to be modified;

(2) results of previous tests conducted according to national legislation or regulation will no longer cover the vehicle after modification; and

(3) any modifications to functions on the vehicle will affect the vehicle’s certification according to national legislation or regulation (7.1.1.9);

(l) determine whether a software update will affect any other system required for the safe and continued operation of the vehicle, or if the update will add or alter functionality of the vehicle compared to when it was certified. (7.1.1.10); and

(m) inform the vehicle user about a software update (7.1.1.11).

1.2.2. The vehicle manufacturer shall record and store the following information for each update: (7.1.2)

1.2.2.1 Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards followed. (7.1.2.1)

1.2.2.2 Documentation describing the configuration of any systems, that are regulated by national legislation or regulation, before and after an update. This shall include unique identification for the system’s hardware and software (including software versions) and any relevant vehicle or system parameters. (7.1.2.2)

1.2.2.3. An auditable register describing all the software relevant to all the systems or functions on a vehicle that are regulated according to national legislation or regulation before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software. (7.1.2.3)

1.2.2.4. Documentation listing target vehicles for the update and confirmation of the compatibility of the last known configuration of those vehicles with the update. (7.1.2.4)

1.2.2.5 Documentation for all software updates describing: (7.1.2.5)

(a) the purpose of the update;

(b) what systems or functions of the vehicle the update may affect;

(c) which (if any) of the systems or functions listed in part b) are required by national legislation or regulation (if any);

(d) if applicable, whether the software update affects the fulfilment of the requirements of any relevant national legislation or regulation identified in part c);

(e) whether the software update affects any parameter specified in national legislation or regulation for a vehicle or vehicle system;

(f) if applicable, whether an approval for the update was requested from the relevant national authority;

(g) how the software update may be executed and under what conditions;

(h) confirmation that the software update will be conducted safely and securely; and

(i) confirmation that the software update has undergone and successfully passed verification and validation procedures.

1.2.3 The information specified in 1.2.2.3 and 1.2.2.4 shall be available from the vehicle manufacturer to relevant national authorities. (7.1.1.12)

1.2.4. To ensure cyber security, the vehicle manufacturer shall implement and maintain processes to: (7.1.3)

(a) ensure software updates are protected to reasonably prevent manipulation before the update process is initiated; (7.1.3.1)

(b) ensure software update processes used are protected to reasonably prevent their compromise, including the development of the software update delivery system; and (7.1.3.2)

(c) verify and validate software functionality and code for the software used in the vehicle are appropriate. (7.1.3.3)

1.2.5. For vehicles that support OTA updates, the vehicle manufacturer shall implement and maintain processes to: (7.1.4)

(a) assess OTA updates to ensure they will not impact safety, if conducted during driving; and (7.1.4.1)

(b) ensure OTA updates that require a specific skilled or complex action (for example recalibration of a sensor post-programming in order to complete an update process) can only proceed when a person skilled to do that action is present or is in control of the process. (7.1.4.2)

2. VEHICLE REQUIREMENTS

2.1. Requirements for Cyber Security

OICA-CLEPA suggested amendment

2.1.1. The manufacturer shall conduct a risk assessment for the vehicle, and shall ~~have~~ treat~~ed~~/manage~~d~~ all identified risks. ~~This shall be kept current.~~ (7.3.3)

2.1.1.1. The risk assessment shall consider the individual elements of the vehicle and their interactions.

2.1.1.2. The risk assessment shall consider interactions with external systems.

2.1.1.3. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

2.1.1.4. The risk assessment shall consider all supplier-related risks. (7.3.2)

2.1.2. The manufacturer shall protect the vehicle against risks identified in the risk assessment. (7.3.4)

2.1.2.1. Relevant and proportionate mitigations shall be implemented to protect the vehicle.

2.1.2.2. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

2.1.2.3. The vehicle manufacturer shall perform appropriate and sufficient testing to verify the effectiveness of the security measures implemented. (7.3.6)

2.1.3. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle (if provided) for the storage and execution of aftermarket software, services, applications or data. (7.3.5)

2.1.4. The vehicle manufacturer shall implement measures for the vehicle to: (7.3.7)

(a) Detect and prevent cyber-attacks against the vehicle;

(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle;

(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

2.1.5. Cryptographic modules shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use. (7.3.8)

~~[Looking at previous attempts to draft this, what happened to “A process to restore any capabilities impaired by a cyber attack.” And “A process to evaluate all processes to ensure they are kept current.”]~~

2.2. Requirements for Software Updates

2.2.1. The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates. (7.2.1.1)

2.2.2. Software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface on the vehicle. (7.2.1.2.2)

2.2.3. Information regarding software version(s) of the software on a vehicle shall be protected against unauthorized modification. (7.2.1.2.3)

Alternative OICA-CLEPA suggestion

**2.2.3**. **The vehicle manufacturer shall protect the software version(s) on a vehicle against unauthorised modification.**

2.2.4. Additional Requirements for Over-the-Air (OTA) Updates (7.2.2)

2.2.4.1. The vehicle shall restore systems to their previous version in case of a failed or interrupted update or that the vehicle shall be placed into a safe state after a failed or interrupted update.

2.2.4.2. Software updates shall only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).

2.2.4.3. When the execution of an update may affect the safety of the vehicle, the vehicle shall be in a state where it can be executed safely.

2.2.4.4. The vehicle user shall be able to be informed about an update before the update is executed. The information made available shall contain:

(a) The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;

(b) Any changes implemented by the update on vehicle functions;

(c) The expected time to complete execution of the update;

(d) Any vehicle functionalities which may not be available during the execution of the update;

(e) Any instructions that may help the vehicle user safely execute the update;

2.2.4.x In case of groups of updates with a similar content one information may cover a group.

2.2.4.5. In the situation where the execution of an update whilst driving may not be safe, the vehicle shall either:

(a) Be incapable of being driven during the execution of the update; or,

(b) Be in a state ensuring that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.

2.2.4.6. After the execution of an update:

(a) The vehicle user shall be able to be informed of the success (or failure) of the update;

(b) The vehicle user shall be able to be informed about the changes implemented and any related updates to the user manual (if applicable).

**3 Observations and suggestions for Definitions**

**3.1 OTA definition**

**Existing definition:**

|  |
| --- |
| 3.4. "Over-the-Air (OTA) update" means any method of making data transfers wirelessly instead of using a cable or other local connection. |

**Issue:** Appears to be missing confirmation that the data transfer is related to providing updates to the vehicle and no other purposes e.g. telemetry messaging, vehicle user internet access, streaming services, etc.

**Suggested change:**

|  |
| --- |
| 3.4. "Over-the-Air (OTA) update" means any method of making data transfers wirelessly instead of using a cable or other local connection for the purpose of providing an update to a vehicle. |

**3.2 Development phase definition**

**Existing definition:**

|  |
| --- |
| 3.x. "Development phase" means the period before a vehicle type is type approved. |

**Issue:** Type Approval is not applicable to 1998 CPs, therefore a more industry related term should be considered.

**Suggested change:**

|  |
| --- |
| 3.x. "Development phase" means the period before a vehicle type enters series production. |

**3.3 Post-production definition**

**Existing definitions:**

|  |
| --- |
| 3.x. "Post-production phase" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type. |

**Issue:** The term "Post-production phase", whilst defined to imply the period when a vehicle type has ceased production, is often misused / misinterpreted to imply "any phase that occurs after production". This can be observed in many industry texts, and also the interpretation document for UN regulations #155 and #156. To remove any further confusion, a new phrasing needs to be considered that is less open to misinterpretation.

**Suggested change:**

|  |
| --- |
| 3.x. "Ceased-production phase" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type. |

**3.4 Phase-related definitions**

**Existing definitions:**

|  |
| --- |
| 3.x. "Development phase" means the period before a vehicle type is type approved.  3.x. "Post-production phase" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.  3.x. "Production phase" refers to the duration of production of a vehicle type. |

**Issue:** The defined vehicle phases, whilst aligning to UN Reg. #155 and #156, are not in alignment with the vehicle phases used in ISO/SAE DIS 21434 and the expected ISO/SAE FDIS 21434. In addition, the latest draft ISO 24089 also uses the same vehicle phases as in ISO/SAE 21434 (DIS and FDIS).

**Suggested change:** Harmonise all instances of vehicle phases with those used in international standards i.e. ISO/SAE 21434 and ISO 24089. This may also address the issue in 1.1.4 regarding vehicles that require cybersecurity monitoring e.g. bullet (a) of 1.1.4 could be modified to "vehicles that in a phase after production and before the end of cybersecurity support phase". Rather than making a specific suggested change, the following excerpts are offered in order to aid discussion and agreement on an acceptable way forward.

**Excerpt from ISO/SAE 21434 upcoming FDIS:**

|  |
| --- |
| The overall cybersecurity risk management of an organization to be implemented in accordance with this document applies throughout all phases. Figure X illustrates this.    **Figure X: Overall cybersecurity risk management** |

**Excerpt from ISO 24089 CD:**

|  |
| --- |
| **3.2 Terminology for lifecycle phases**  **3.2.1**  **phase**  stage in the lifecycle of a vehicle or component that is specified in this document  [SOURCE: ISO 26262-1:2018, 3.110, modified – Note 1 to entry removed.]  **3.2.2**  **concept phase**  first *phase* during which the principal characteristics of the vehicle or component are defined, including the relevant functional safety and cybersecurity goals and risks  Note 1 to entry: During the Concept Phase, the principal characteristics of the relevant Software Update Process are defined.  Note 2 to entry: During the Concept Phase, a Software Update Campaign cannot be performed on the given vehicle or component.  **3.2.3**  **development phase**  second *phase* during which the architecture and design of the vehicle or component are defined, including implementation of the relevant functional safety and cybersecurity requirements and risk mitigations  Note 1 to entry: During the Development Phase, prototypes of the vehicle or component are typically created and tested.  Note 2 to entry: During the Development Phase, the architecture and design of the relevant Software Update Process are defined.  Note 3 to entry: During the Development Phase, a Software Update Campaign cannot be performed on the given vehicle or component.  **3.2.4**  **production phase**  third *phase* during which the vehicle or component is manufactured (fabricated, assembled, and/or calibrated) and is prepared for distribution  Note 1 to entry: During the Production Phase, the Infrastructure to support the relevant Software Update Process is defined and deployed.  Note 2 to entry: During the Production Phase, a Software Update Campaign cannot be performed on the given vehicle or component.  **3.2.5**  **operations phase**  fourth *phase* during which the vehicle or component is shipped to distributors and dealers and is subsequently sold or leased to a customer or vehicle user  Note 1 to entry: The Operations Phase also includes the Maintenance Phase (which is a subset of the Operations Phase).  Note 2 to entry: During the Operations Phase, a Software Update Campaign can be performed, unless support for Software Update Campaigns has ended for the given vehicle or component.  **3.2.6**  **maintenance phase**  fifth *phase* which begins when the vehicle or component is sold or leased to a customer or vehicle user  Note 1 to entry: During the Maintenance Phase, a Software Update Campaign can be performed, unless support for Software Update Campaigns has ended for the given vehicle or component.  **3.2.7**  **decommissioning phase**  sixth *phase* which begins when the vehicle or component is no longer in use by a customer or vehicle user  Note 1 to entry: During the Decommissioning Phase, a Software Update Campaign can be performed, unless support for Software Update Campaigns has ended for the given vehicle or component. |