**Interpretation/guidance document for: UN Regulation on uniform provisions concerning the approval of software update processes**

TFCS-TPCM1-10

|  |  |  |  |
| --- | --- | --- | --- |
|  | United Nations | ECE/TRANS/WP.29/201x/xx | |
| _unlogo | **Economic and Social Council** | | Distr.: General  DD MM YYYY  Original: English |

**Economic Commission for Europe**

Inland Transport Committee

**World Forum for Harmonization of Vehicle Regulations**

**xxx session**

Geneva, DD–DD MM YYYY

Item XXX of the provisional agenda

**Draft new Regulation on software updates**

**Interpretation/guidance document for: Regulation on uniform provisions concerning the approval of software update processes**

**Submitted by the expert from xxx**

The text reproduced below was prepared by the experts from xxx

Contents

*Page*

7. General specifications 7

Annexes

1. Information document 13

# Scope

Not included in this document as it is assumed guidance is not needed here for testing

# Definitions

Not included in this document as it is assumed guidance is not needed here for testing

# Application for Approval

Not included in this document as it is assumed guidance is not needed here for testing

# Marking

Not included in this document as it is assumed guidance is not needed here for testing

# Approval

Not included in this document as it is assumed guidance is not needed here for testing

# Software Update Management System (SUMS) Certificate of Compliance

Not included in this document as it is assumed guidance is not needed here for testing

# General Specifications

# Note regarding evidencing the requirements: Demonstration of requirements via documentation/presentation and/or audit

## **Requirements for the Software Update Management System of the vehicle manufacturer**

## **Processes to be verified at initial assessment**

## A process whereby information relevant to this regulation is documented and securely held at the vehicle manufacturer and can be made available to an Approval Authority or Technical Service upon request without any burden;

|  |
| --- |
| Clarification:   * ‘securely’ => refers to IT security, … * ‘without any burden’ => e.g. Machinery Directive requirements (within 3 weeks), … |
| Note:   * Contact point at the vehicle manufacturer * Processes for securing the information * Information content is defined within the Regulation e.g. para. 7.1.2. |
| Evidence:   * Flow diagram of delivering system (operation flow) optional * ISO 27001 may be used to evidence ‘securely held’ |

## A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified;

|  |
| --- |
| Clarification:   * Relevant hardware components refer to hardware with software on it. It may be ECUs, CPUs or other hardware as identified by the vehicle manufacturer. |
| Note:   * Integrity validation data could refer to the check sum for example. * The term was used to ensure technology neutrality. * Version number could be done at vehicle level and/or component level as long as it is possible to fulfil the requirement of the Regulation for unique identification of software/hardware |
| Evidence: |

## A process whereby, for a vehicle type that has an RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated. This shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN.

|  |
| --- |
| Clarification: |
| Note:   * RXSWIN refers to the software on a defined set of hardware. |
| Evidence: |

## A process whereby, for a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN;

|  |
| --- |
| Clarification: |
| Note: |
| Evidence: |

## A process whereby any interdependencies of the updated system with other systems can be identified;

|  |
| --- |
| Clarification:   * ‘other system’ = systems (covered or not by type approval) affecting safety, security, theft protection and environmental behaviour |
| Note:   * This requirement is to ensure there are processes to assess if an update will affect other systems, e.g. for cascading effects * It is accepted that there are limits in how far a process could cover interdependencies (processes should follow best practice) * Test phase will elaborate on the processes used and the requirement |
| Evidence: |

## A process whereby the vehicle manufacturer ~~can~~ is able to identify target vehicles for a software update;

|  |
| --- |
| Clarification:   * ‘Target vehicle’ refers to individual vehicles (VIN based) |
| Note: |
| Evidence: |

## A process to verify, before a software update is issued, the compatibility of possible software/ hardware configurations for the registered configuration or last known configuration of the target vehicles with the software update;

|  |
| --- |
| Clarification:   * ‘issued’ = made available publically |
| Note: |
| Evidence: |

## A process to assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation);

|  |
| --- |
| Clarification:   * ‘Parameters’ here does not refer to software parameters but to the parameters describing the system type approval. |
| Note: |
| Evidence:   * Quality control procedures for the software updates may be relevant |

## A process to assess, identify and record whether a software update will add, alter or enable any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether:

1. Entries in the information package will need to be modified

2. Test results no longer cover the vehicle after modification

|  |
| --- |
| Clarification:   * ‘alter or disable any other parameters or functions’ refers to type approved systems |
| Note: |
| Evidence: |

## A process to assess, identify and record if 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 registered;

|  |
| --- |
| Clarification: |
| Note:   * This paragraph specifically refers to non-type approved systems to ensure safe operation of the vehicle. |
| Evidence:   * Quality control and configuration management processes may be used |

## A process whereby the vehicle user is able to be informed about updates.

|  |
| --- |
| Clarification:   * ‘vehicle user’ may also be the technician in the workshop * ‘is able to’ = may be informed by suitable means |
| Note:   * Definition of ‘vehicle user’ as in the Recommendation (2.16.) should be added to the Regulation * This requirement does not cover the need for consent |
| Evidence: |

## A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to ~~relevant~~ responsible Authorities or Technical Services.

|  |
| --- |
| Clarification: |
| Note: |
| Evidence: |

## **The vehicle manufacturer shall record, and store ~~at their premises~~, the following information for each update applied to a given vehicle type:**

|  |
| --- |
| Clarification: |
| Note:   * Vehicle type is intended such that it is not repeated for each vehicle * The test phase will evaluate if the existing documentation can be used to evidence the requirements below |
| Evidence:   * The information may be contained in the existing configuration control management documentation |

## Documentation describing the processes used by the vehicle manufacturer for ~~providing~~ software updates and any relevant standards used to demonstrate their compliance;

|  |
| --- |
| Clarification: |
| Note:   * Refers to processes relevant to this Regulation |
| Evidence: |

## Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification ~~ers~~ for the type approved system’s hardware and software and any relevant vehicle or system parameters;

|  |
| --- |
| Clarification: |
| Note:   * The type approved systems being updated may comprise a range of previous configurations or all previous versions * During the test phase it will be evaluated whether the text relating to parameters is relevant or covered elsewhere |
| Evidence: |

## For every RXSWIN, there shall be documentation describing the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.

|  |
| --- |
| Clarification: |
| Note:   * There exist reference numbers such as the calibration identification number. In the test phase it could be evaluated how these could be used. * The integrity validation data shall allow in case of reasonable doubt, to verify that the software has not been manipulated. |
| Evidence: |

## Documentation listing target vehicles for the update and verification of the compatibility of the registered configuration or last known configuration of those vehicles with the update.

|  |
| --- |
| Clarification: |
| Note:   * Confirmation that compatibility is ensured at a group level, not individual vehicle level * Target vehicles may be identified by the VIN |
| Evidence: |

## Documentation for all software updates for that vehicle type describing:

|  |
| --- |
| Clarification: |
| Note:   * during the test phase it should be evaluated how this can be done efficiently, especially for updates not affecting type approved systems * information may be clustered for updates covering multiple purposes or multiple updates covering the same purpose (if appropriate) * *Sub bullets to be transformed into letters* |
| Evidence: |

1. The purpose of the update;

|  |
| --- |
| Clarification: |
| Note: |
| Evidence: |

1. What systems or functions of the vehicle the update may affect ~~impact~~;

|  |
| --- |
| Clarification: |
| Note:   * This is intended to describe the target for the update, e.g. braking system, radio, … |
| Evidence: |

1. Which of these are type approved (if any);

|  |
| --- |
| Clarification: |
| Note: |
| Evidence: |

1. If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;

|  |
| --- |
| Clarification: |
| Note:   * It will be reviewed whether clauses 4 to 6 should be merged |
| Evidence: |

1. Whether the software update affects any system type approval parameter;

|  |
| --- |
| Clarification: |
| Note:   * Redundant? |
| Evidence: |

1. Whether an approval for the update was sought from an approval body;

|  |
| --- |
| Clarification: |
| Note:  Redundant? |
| Evidence: |

1. How the update may be executed and under what conditions;

|  |
| --- |
| Clarification:   * ‘conditions’ should be understood as the instructions for execution |
| Note:   * In case H/W update is required it should be stated in the ‘conditions’ for execution |
| Evidence: |

1. Verification that the software update will be conducted safely and securely.

|  |
| --- |
| Clarification: |
| Note:   * explanation how the conditions mentioned in point 7 are met and why those conditions provide safe and secure updates |
| Evidence: |

9. Confirmation ~~Verification~~ that the software update has undergone adequate verification and validation procedures.

|  |
| --- |
| Clarification: |
| Note:   * Verification and Validation shall ensure that the software works as intended. The method(s) used should be appropriate to the update. |
| Evidence: |

## **Security, the vehicle manufacturer shall demonstrate:**

## The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated;

|  |
| --- |
| Clarification: |
| Note:   * This is to cover processes for ensuring the integrity and authenticity of the software updates that are to be delivered |
| Evidence:   * CSMS may be used to evidence these requirements |

## The update processes used is protected to reasonably prevent it being compromised, including development of the system update;

|  |
| --- |
| Clarification: |
| Note:   * This is to cover processes for delivering software updates to ensure they cannot be compromised to deliver unauthorized updates |
| Evidence:   * CSMS may be used to evidence these requirements |

## The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.

|  |
| --- |
| Clarification: |
| Note:   * Redundant? |
| Evidence: |

## **Additional Requirements for Software Updates over the air**

## The vehicle manufacturer shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety if conducted during driving.

|  |
| --- |
| Clarification: |
| Note:   * This is potentially a repetition of point 8 of para. 7.1.2.5. but has a specific requirement  To be confirmed if redundant |
| Evidence: |

## The vehicle manufacturer shall demonstrate the processes and procedures they will use to ensure that, when an over the air update requires a skilled person, such as a mechanic, in order to complete the update process, the update can only proceed when such a person is present.

|  |
| --- |
| Clarification: |
| Note:   * This is potentially a repetition of point 8 of para. 7.1.2.5. but has a specific requirement  To be confirmed if redundant |
| Evidence: |

## **Requirements for the Vehicle Type NOT REVIEWED DURING TFCS-TPCM1**

## **Requirements for Software updates**

## The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## Where a vehicle type uses RXSWIN:

7.2.1.2.1 Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

7.2.1.2.2 The RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

7.2.1.2.3. The vehicle manufacturer shall protect the RXSWINs on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN chosen by the vehicle manufacturer shall be confidentially outlined.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

* + 1. **Additional Requirements for over the air updates**

## The vehicle shall have the following functionality with regards to software updates:

## The vehicle manufacturer shall ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## The vehicle manufacturer shall ensure that software updates can 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).

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This may be achieved through technical means and/or through a process that will require the vehicle user to provide verification that the vehicle is in a state where the update can be executed safely.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## The vehicle manufacturer shall demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information provided may contain:

• 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;

• Any changes implemented by the update on vehicle functions;

• The expected time to complete execution of the update;

• Any vehicle functionalities which may not be available during the execution of the update;

• Any instructions that may help the vehicle user safely execute the update;

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

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## In the situation where the execution of an update whilst driving may not be safe, the vehicle manufacturer shall demonstrate how they will:

• Ensure the vehicle cannot be driven during the execution of the update;

• Ensure 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.

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

## After the execution of an update the vehicle manufacturer shall demonstrate how the following will be implemented:

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

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

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

# Modification and extension of the vehicle type

Not included in this document as it is assumed guidance is not needed here for testing

# Conformity of production

Not included in this document as it is assumed guidance is not needed here for testing

# Penalties for non-conformity of production

Not included in this document as it is assumed guidance is not needed here for testing

# Production definitively discontinued

Not included in this document as it is assumed guidance is not needed here for testing

# Names and addresses of Technical Services responsible for conducting approval test, and of type approval authorities

Not included in this document as it is assumed guidance is not needed here for testing

**Annex 1**

**Information document**

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

**0. GENERAL**

0.1. Make (trade name of manufacturer): … . . . . . . . . . . . . . . . . . . . . .

0.2. Type: …. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

0.2.0.1. Chassis: … . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

0.2.1. Commercial name(s) (if available): … . . . . . . . . . . . . . . . . . . . . . . .

0.3. Means of identification of type, if marked on the vehicle/component/

separate technical unit ( 1 ) ( b ): …. . . . . . . . . . . . . . . . . . . . . .

0.3.1. Location of that marking: … . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

0.4. Category of vehicle ( c ): … . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

0.5. Company name and address of manufacturer: … . . . . . . . . . . . .

**12.9. Software Updates**

12.9.1 General construction characteristics of the vehicle type

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

12.9.1.1 Schematic representation of the vehicle type

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

12.9.1.2 Documents for the vehicle type to be approved describing:

a) the vehicle systems and functionality that will enable software updates to be conducted

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

b) how vehicle users will be informed about software updates

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

c) how the update process will be performed securely

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

12.9.2 The number of the SUMS Certificate of Compliance

|  |
| --- |
| Q: Any guidance required for how to evidence this requirement?  Q: If relevant, what type of evidence would show compliance? |
| Answer to Q: |
|  |

# Annex B Draft proposal to amend existing UN Regulations to introduce software identification numbers (RXSWIN)

1. *Add new definitions to the definition section:*

Not included in this document as it is assumed guidance is not needed here for testing

1. *Add a new section on the introduction of the RXSWIN in the requirement section:*

*Add a new paragraph x.y. and its corresponding subparagraphs:*

x.y. Requirements for software identification

x.y.1. For the purpose of ensuring the software of the System can be identified, an RXSWIN may be implemented by the vehicle manufacturer.

x.y.2. If the manufacturer implements an RXSWIN the following shall apply:

x.y.2.1. The vehicle manufacturer shall have a valid approval according to UN Regulation No. xxx [Software Update Process Regulation].

x.y.2.2. The vehicle manufacturer shall provide the following information in the communication form of this Regulation:  
- the RXSWIN  
- how to read the RXSWIN

x.y.2.3. The vehicle manufacturer may provide in the communication form of this Regulation a list of the relevant parameters that will allow the identification of those vehicles that can be updated with the software represented by the RXSWIN. The information provided shall be declared by the vehicle manufacturer and may not be verified by an Approval Authority.

[x.y.3. The vehicle manufacturer may obtain a new vehicle approval for the purpose of differentiating software versions intended to be used on vehicles already registered in the market from the software versions that are used on new vehicles. This may cover the situations where type approval regulations are updated or hardware changes are made to vehicles in series production. In agreement with the testing agency duplication of tests shall be avoided where possible.]

|  |
| --- |
| Q: Any guidance required for this section |
| Answer to Q: |
|  |

[3. *Add a new parapgraph or amend exiting paragraph on Production definitely discontinued:*

X. Production definitely discontinued

Not included in this document as it is assumed guidance is not needed here for testing

1. *Add paragraph x.y. and its subparagraphs in the Annex «Communication», amendment to read:*

ANNEX [Communication form]

**COMMUNICATION**

(Maximum format: A4 (210 x 297 mm))

issued by : Name of administration:

......................................

......................................

......................................



concerning: 2/ APPROVAL GRANTED

APPROVAL EXTENDED

APPROVAL REFUSED

APPROVAL WITHDRAWN

PRODUCTION DEFINITELY DISCONTINUED

***APPROVAL EXTENDED AFTER PRODUCTION DEFINITELY******DISCONTINUED***

of a vehicle type with regard to xxx equipment pursuant to Regulation No. **X**

Approval No. ……….. Extension No.

…

***x.y RXSWIN:***

***x.y.1 Information on how to read the RXSWIN:***

***x.y.2 If applicable, list the relevant parameters that will allow the identification of those vehicles that can be updated with the software represented by the RXSWIN under point x.y.1:***

|  |
| --- |
| Q: Any guidance required for this section |
| Answer to Q: |
|  |