Submitted by the Secretary of the
UN Task Force on Cyber Security and
Over-the-Air issues

Informal document **GRVA-01-18**
1st GRVA session, 25-28 September 2018
Agenda item 6 (b)

Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA

Date: 20/09/2018

Contents

1. Introduction

1.1. Preamble

1.1.1. A Task Force was established as a subgroup of the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG ITS/AD) of WP.29 to address Cyber Security and Over-the-air issues. The task force consisted of representatives from Contracting Parties and non-governmental organizations, e.g. FIA, CITA, ITU, OICA and CLEPA.

1.1.2. The influence of software on vehicle functionality is increasing. Software influences the environmental and safety performance and other functions of a vehicle.

1.1.3. To update the software of a vehicle after certification and even after the first registration is of increasing importance, for example for adding new functionalities, performing software corrections and supporting recalls.

1.1.4. This recommendation provides requirements for how the certification process described in the UNECE regulations, i.e. UN Regulations under the 1958 Agreement and Global Technical Regulations under the 1998 Agreement, and processes regarding information about the vehicle can be adapted to ensure compliance of any new software to those UNECE regulations, independent of whether the update is conducted with a physical connection or over the air.

1.1.5. This recommendation is an initial contribution for the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) under the Word Form for Harmonization of Vehicle Regulations (WP.29) to discuss and propose amendments in order to implement software updates into the certification process and also for all updates to ensure their safe execution and the legal compliance with the UN program of work.

1.2. Scope

1.2.1. This recommendation describes requirements for adaptation of vehicle software updates for certification to ensure their safe execution and the legal compliance with the regulation under the UN program of work. It furthermore describes requirements for how software changes should be managed to ensure that they are performed safely and securely via an over-the-air update. The scope of the document also covers requirements that can be used for updates performed by other means.

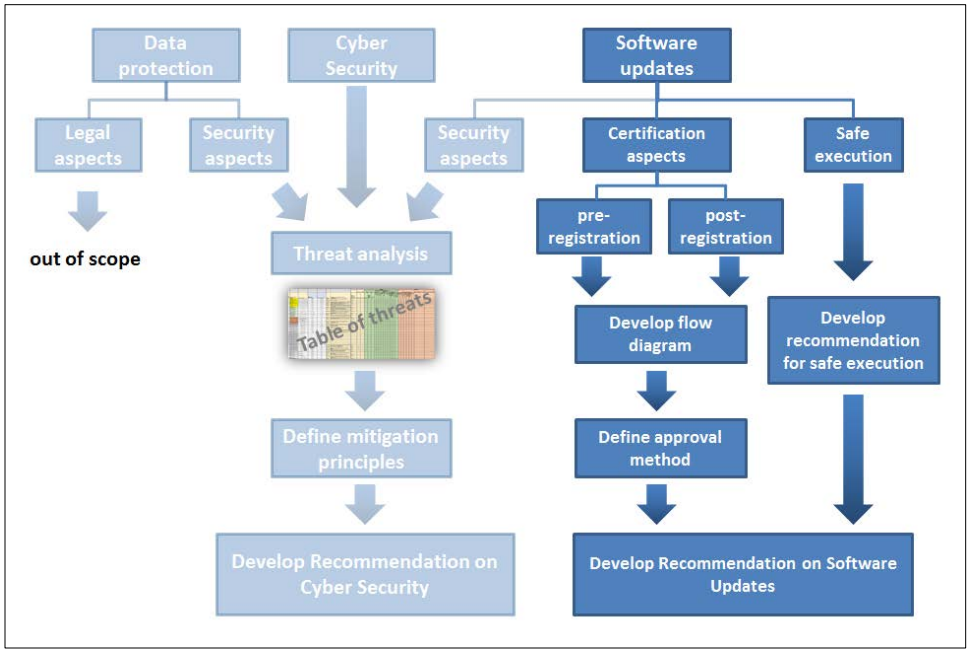


Figure 1: Diagram showing the extent of the this recommendation and how it ties in with data protection and cyber security

1.2.2. The scope of what is covered in this recommendation is illustrated by figure 1. It is noted that there are commonalities between data protection, cyber security and software updates. Software updates have security aspects, certification aspects and aspects for safe execution that need to be considered. Figure 1 shows that the outcome of these considerations will be to produce recommendations on all these topics. This recommendation only considers those directly relating to software updates. Those on cyber security and data protection form part of a separate recommendation.

1.2.3. Security aspects of software updates are part of the "Recommendation on Cyber Security of the UNECE Task Force on Cyber Security and Over-the-air issues of the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) under the Word Form for Harmonization of Vehicle Regulations (WP.29)".

1.2.4. This recommendation applies to the legal framework for certification of vehicles. Since the process for managing and approving a software update after the initial type approval is granted and the process for vehicle registration is conducted according to national legislation, some recommendations will be handled by national legislation. Such parts of recommendation are not subjected to binding force of the UNECE 1958 Agreement.

1.2.5. Software updates after the first registration by parties that are not the holder of the type approval/ certification are not covered by this document. These may be approved using national approval procedures.

2. Definitions

For the purpose of this Recommendation the following definitions shall apply:

2.1. “Architecture” means a representation of the structure of the item or functions or systems or elements that allows identification of building blocks, their boundaries and interfaces, and includes the allocation of functions to hardware and software elements.

2.2. “Certified system” means a system defined by type approval legislation under the 1958 Agreement or a system as defined by the 1998 Agreement.

2.3. “Download” means copying data from one computer system (for example a backend server) to another (for example a vehicle).

2.4. “Electronic Control Systems” means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing. Such systems, often controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements.

2.5. “Execution” means the process of installing and activating an update that has been downloaded.

2.6. “Organisation” means a person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

2.7. “Over the air (OTA) update” means any method of making data transfers wirelessly instead of using a cable or other local connection.

2.8. “RX Software Identification Number (RXSWIN)” means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.

2.9. -“Software” means the part of an Electronic Control System that consists of digital data and instruction.

2.10. “Software bug” means an error, flaw, failure or fault in software that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.

2.11. “Software components” means one or more software units.

2.12. “Software update” means a package used to upgrade software to a new version.
Note: The terms ‘update’ and ‘upgrade’ are used synonymously to refer to installing new versions of software. The update may contain a fix for a specific problem or introduce new product functionality.

2.13. “Software Update Management System (SUMS)” means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to Annex A of this recommendation.

2.14. “Software unit” means an atomic level software component of the software architecture that can be subjected to stand-alone testing.

2.15. “Update process” means the steps involved in the downloading and execution of new versions of software.

2.16. “Vehicle user” means a person operating or driving the vehicle, a vehicle owner, an authorised representative or employee of a fleet manager, an authorised representative or employee of the vehicle manufacturer, or an authorized technician.

3. Document structure

3.1. Chapter 4 describes the process for managing software updates, including over the air updates. It further describes supporting, pre-requisite requirements to enable the software update process to be conducted in an open and verifiable manner.

3.2. Chapter 5 describes requirements to ensure that software updates, including OTA updates, can be conducted safely and securely.

3.3. Chapter 6 describes requirements so that the status of the software on a vehicle, particularly its certified/type approved systems, can be verified.

4. Process for software updates

4.1. Scope of the software update process

4.1.1. This section applies where the Contracting Party, on which territory the vehicle is registered, requires a UNECE Approval to cover the software update.

4.1.2. In regimes where UNECE Approval is not required it is expected that a similar process would be used. However the Task Force did not examine each regime to describe each variation.

4.2. Software update approval process

4.2.1. Table 1 below demonstrates how the software update process shall be conducted in accordance with this recommendation:

Moment of update	**No impact of update on any UN type approval**	**Impact on UN type approval(s) by update but original vehicle type covers modification**	**Impact on UN type approval(s) by update but original vehicle type does not cover modification**
Initial type approval (TA)	Not applicable	Not applicable	Not applicable
Existing TA, **before registration**	No action	Extension TA	New TA
Existing TA, **after registration**, by vehicle manufacturer	No action	Extension TA or individual approval or approval with limited scope; Registration according to national rules	New TA or individual approval or approval with limited scope; Registration according to national rules

Table 1: Summary of type approval processes

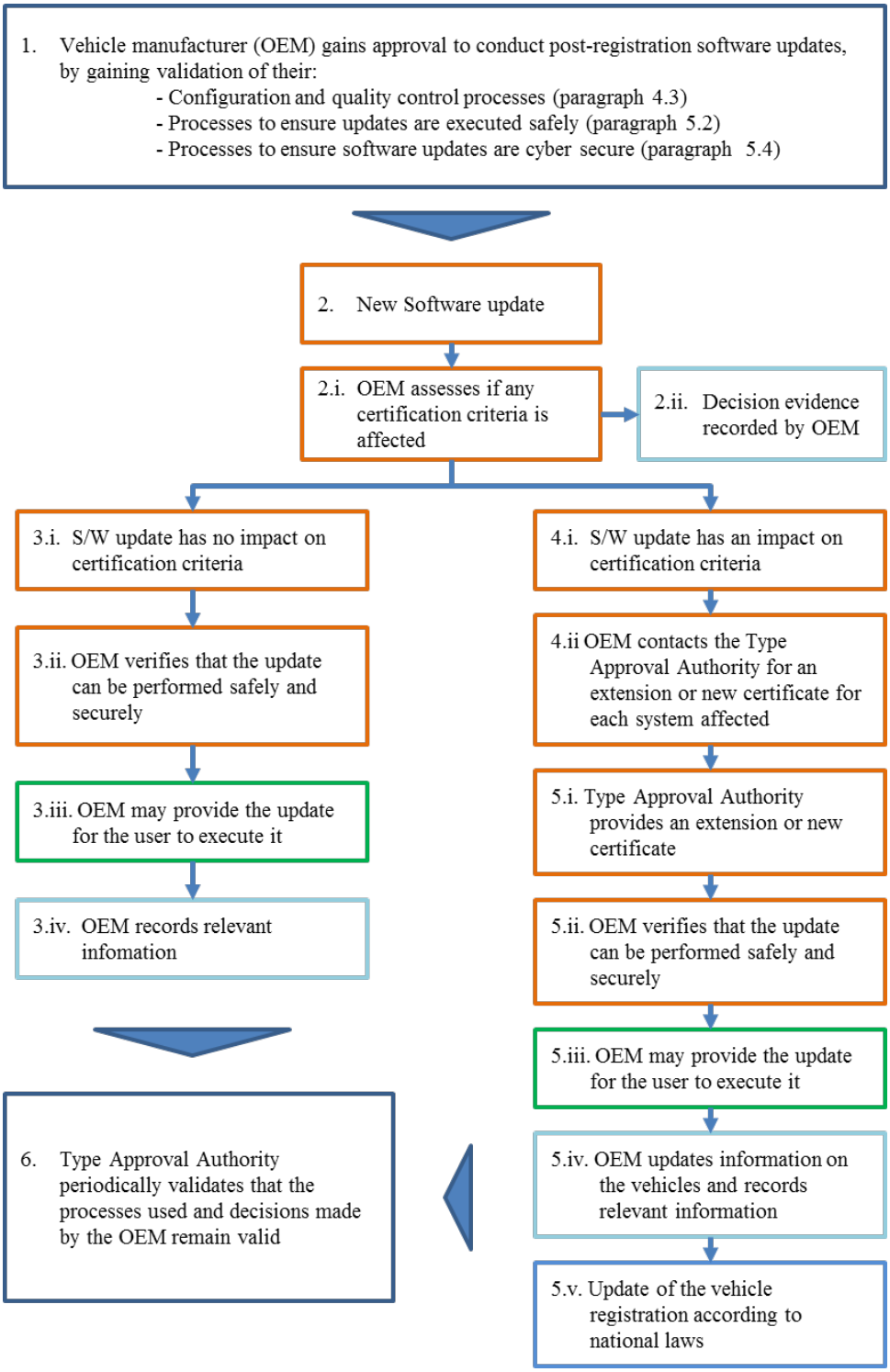
4.2.2. Once a system is initially certified/type approved (before vehicle registration) any changes to it are assessed with regards to whether they may affect its certification/type approval. The nature of this assessment will be determined by the requirements of the relevant legislation. If the vehicle manufacturer determines that a software update may affect a systems certification/type approval the vehicle manufacturer shall initiate a process with an Approval Authority to determine if an extension of an approval or a new approval is needed;

4.2.3. If the software update occurs after a Declaration of Conformance (DoC) has been produced, the Declaration of Conformance shall be updated reflecting the change of the certification/type approval.

4.2.4. When a software update occurs after vehicle registration, including OTA updates, the following steps shall be employed when an update is under the control of the vehicle manufacturer:

1. Before implementation of the first update the vehicle manufacturer shall demonstrate to the type approval authority that their update processes will allow updates to be conducted safely and securely as per the requirements of chapter 4 and 5 and gain a validation of their update process for subsequent updates. If the update process is changed for the requirements of chapter 4 or 5 a new validation shall be required;
2. The vehicle manufacturer shall assess whether a software update will directly or indirectly impact the compliance of the approvals of a vehicle's type approved systems and documents the result;
3. If the update does not have impact on the compliance of any type approved systems, for example to fix software bugs, the vehicle manufacturer may conduct the update without need to contact the type approval authority but shall ensure the update process employed is safe and secure;
4. If an update may or will impact the compliance of one or more type approved systems, then the vehicle manufacturer shall contact the relevant type approval authority to seek an extension or new certification for the affected systems;
5. Where an extension or new certification is granted, registration of affected vehicles is conducted according to national laws. The update may then be conducted and the vehicle manufacturer shall ensure the update process employed is safe and secure. The vehicle information in the Declaration of Conformance shall be updated after the installation of the new software to reflect the new type approval status of the whole vehicle type approval. The status of the software on a vehicle shall be updated to reflect the new status of its certification as per the requirements of chapter 6;
6. The type approval authority shall periodically validate that the processes used and decisions made by the vehicle manufacturer remain valid.

4.2.5. The following flow diagram represents the process to enable software updates after vehicle registration.



4.2.6. The assessment of whether a software update affects certification 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 certify those system (as defined in the relevant legislation). The assessment shall also consider whether the update will add 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. This shall include consideration of whether:

- Entries in the information package are modified
- Test results no longer cover the vehicle after modification

4.2.7. Conformity of Production checks, periodical validation and market surveillance may be used to verify that the processes and decisions made by the vehicle manufacturer are appropriate, particularly for instances where the vehicle manufacturer chose not to notify an Approval Authority about an update.

4.2.8. Should there be a need to urgently perform an update to address a safety critical issue which needs to occur before a full assessment of the impact on type approved systems can be completed, the vehicle manufacturer and any relevant appropriate authority should convene to make a risk based judgement on whether to issue the update according to their national laws and processes. Upon completion of the full assessment, any further actions required shall be implemented. The process employed may use existing procedures for similar recall issues.

4.3. Prerequisites

4.3.1. To enable the process of updating software to be open and verifiable there are a number of processes and procedures that will be required. The key processes and procedures for administrating this are provided in this section. The basis for these are configuration management and quality control.

4.3.2. The vehicle manufacturer (and if relevant their suppliers) shall demonstrate to the approval authority that they have the following processes in place:

4.3.2.1. 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;

4.3.2.2. 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;

4.3.2.3. 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.

4.3.2.4. 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;

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

4.3.2.6. A process whereby the vehicle manufacturer can identify target vehicles for a software update;

4.3.2.7. 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;

4.3.2.8. 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);

4.3.2.9. 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

4.3.2.10. 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;

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

4.3.2.12. A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. available to relevant Authorities or Technical Services.

4.3.3. The vehicle manufacturer shall describe their processes and the compliance of their processes to an approval authority who shall verify and certify those processes.

4.3.4. To support conformity of production checks, periodical validation, market surveillance and approval of updates the following documents shall be required to be held by the vehicle manufacturer:

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

4.3.4.2. Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identifiers for the type approved system's hardware and software and any relevant vehicle or system parameters;

4.3.4.3. 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.

4.3.4.4. 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.

4.3.4.5. Documentation for all software updates for that vehicle type describing:

1. The purpose of the update;
2. What systems or functions of the vehicle the update may impact;

3. Which of these are type approved (if any);
4. If applicable, whether the software update affects any of the relevant requirements of those type approved system;
5. Whether the software update affects any system type approval parameter;
6. Whether an approval for the update was sought from an approval body;
7. How the update may be executed and under what conditions;
8. Verification that the software update will be conducted safely and securely.
9. Verification that the software update has undergone adequate verification and validation procedures.

4.4. Type approval process responsibilities

4.4.1. The vehicle manufacturer shall be responsible for assessing the potential impact of any software update on type approval and for supplying all the necessary documentation to enable the technical service and the type approval authority to verify the decisions they have made;

4.4.2. The vehicle manufacturer shall be responsible for making the initial decision regarding whether a software update may directly or indirectly impact a type approval and contact the technical service and the type approval authority should that be the case;

4.4.3. The vehicle manufacturer shall be responsible for providing evidence that they have the procedures in place to decide whether a software update does or does not affect type approved systems;

4.4.4. The type approval authority shall verify the vehicle manufacturer's processes and decisions (including the decisions that are not notified to the Approval Authority). This may be achieved on a sampling basis.

5. Safety and security requirements for software updates

5.1. This chapter describes objectives for maintaining the safety and security of the vehicle during the update process and specific requirements relating to them.

5.2. Safety requirements for updates

5.2.1. The location and movement of the vehicle should not be restricted during the download portion of a software update unless safety implications result from the download process.

5.2.2. To enable a software update to be executed safely the following shall be taken into account before the execution is initiated:

- Recovery from a failed or interrupted update:
    - The vehicle manufacturer shall ensure that the system that is being updated can restore the software to the previous version after a failed or interrupted update or the vehicle can be placed into a safe state.
- Information about the update:
    - The vehicle manufacturer shall ensure the vehicle user is able to be informed about the update before the update is executed. This 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;
        - Any other necessary instructions to execute the update.
    - Pre-conditions before the execution
        - 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.
        - 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).

5.2.3. If the execution of an update whilst driving might pose a safety hazard, the vehicle manufacturer shall:
- 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.

5.2.4. After the execution of an update the following shall be implemented:
- The vehicle manufacturer shall ensure that the vehicle user is informed of the success (or failure) of the update;
- The vehicle manufacturer shall ensure the vehicle user is able to be informed about the changes implemented and any updates to the user manual (if applicable).

5.3. Additional safety requirement for OTA updates.

5.3.1. The execution of OTA updates shall not be permitted during driving where additional action is required by the vehicle user in order to complete the update process.

5.3.2. Where an OTA update requires a skilled person, such as a mechanic, to perform a task to complete the update process the vehicle manufacturer shall have controls in place to ensure that the update is executed by such a person.

5.4. Security requirement for updates

5.4.1. The vehicle manufacturer shall be able to demonstrate to the authority that their software update process will ensure, according to the state of the art, that:
- the software updates will be protected to prevent manipulation before the update process is initiated (i.e. ensure that only authorized, uncorrupted updates are sent to the vehicle);
- the update processes used are protected to prevent them being compromised, including development of the system update program or firmware;

- the authenticity and integrity of the software updates will be protected to prevent their compromise and prevent invalid updates.

5.5. Requirements for evidencing that updates and the update process is safe and secure.

5.5.1. To support any certification process for permitting software updates, particularly those over the air, the authority shall be competent and able to assess the processes and procedures of a vehicle manufacturer with respect to the above safety and security requirements.

5.5.2. To enable an assessment of the vehicle manufacturer's processes and procedures with regard to conducting software updates safely and securely the vehicle manufacturer shall be able to provide to the authority:

- documentation describing how the update will be performed securely. This may include information regarding validation testing of the security of the processes;
- documentation describing how the update will be performed safely;
- documentation describing any interaction/requirements of the vehicle user (if any) in the update process.

6. Identification of the installed software

6.1. Use of the Software Identification Number, RxSWIN.

6.1.1. The RxSWIN is unique for each specific UN Regulation wherein the "x" refers to the number of the Regulation to which it is applied.

6.1.2. To identify the software of a given type approved system, a RXSWIN shall be introduced. The purpose of this shall be to provide a reference that can be used to verify that the software on type approved systems is up to date and conforms with the certification/type approval requirements of that system. As it is a reference, it shall be linked to documentation providing more information on the software and hardware of the relevant system.

6.1.3. The RXSWIN shall provide a reference for the software components of a given type approved system.

6.1.4. The RXSWIN is linked to the vehicle functionality/ vehicle type definition in specific regulations and is not linked to the software of the single components of the electronic control system.

6.1.5. Information regarding all initial and updated software versions, including checksums or similar integrity validation data, of the single components of the electronic control systems of every produced vehicle and the link to the RXSWIN shall be stored at the vehicle manufacturer. For the purpose of certification, including the validation of the conformity of production, and the market surveillance, including recalls and PTI, the vehicle manufacturer shall provide this information to the authority if requested.

6.1.6. A new RXSWIN shall be required if a software update requires an extension or renewal of the approval. Whether an extension or renewal of the approval is necessary, is described in the specific regulations (e.g. in the vehicle type definition).

6.1.7. A software change of a single component may affect different approvals. If this occurs and an approval needs to be extended or renewed for a number of different systems, then new RXSWINs shall be introduced for all the relevant type approved systems..

6.1.8. If it is technically possible to bring registered vehicles in line with the extended or renewed approval, the vehicle manufacturer may describe in the information document the registered vehicles to which this may apply. The information provided shall be declared by the vehicle manufacturer and may not be verified by an Approval Authority during certification.

6.1.9. If it is nationally legally permissible to install the software in a vehicle, the manufacturer shall record information regarding the software, including integrity validation data, of the single components of the electronic control systems as well as the link to the RXSWIN before and after the software change. On request of the Approval Authority the vehicle manufacturer shall provide the information without any burden.

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

6.1.11. The manufacturer shall protect the RXSWINs on a vehicle against unauthorised modification.

7. Conclusion and recommendation for further proceedings

7.1. The conclusion of this recommendation is that (over the air) updates should be treated as a post-registration updates and in order to regulate such updates the following processes are needed:

7.1.1. A verification by an Approval Authority or Technical Service that the processes and procedures of a vehicle manufacturer support the implementation of the recommendations of this paper;

7.1.2. That individual software updates, post-registration, are assessed by vehicle manufacturer’s using the procedures listed in this recommendation and Approval Authorities or Technical Services are notified when an update may affect any certified system or change any entry within the information document for the vehicle;

7.1.3. That Approval Authorities or Technical Services periodically verify that vehicle manufacturer’s continue to apply the processes and procedures correctly and verify that they are appropriately notifying authorities of software updates as defined within this recommendation.

7.2. The task force recommends that this paper is taken forward as three parts:

7.2.1. The main text (chapters 1 to 6) is taken forward as an official working document for WP.29. Furthermore, it could be used as a basis for a Resolution on Software Update Processes, but may need further revision to comply with the format required;

7.2.2. Annex A is taken forward as a UN Regulation, according to the 1958 Agreement. It includes requirements for:

7.2.2.1. A Software Update Management System (SUMS) Certificate of Compliance for the processes and procedures relevant to software updates of the vehicle manufacturer;

7.2.2.2. Vehicle type approval with regard to software update processes;

7.2.3. Annex B is taken forward as an amendment to all relevant already existing UN Regulations. The concept of RXSWIN is introduced as an "if-fitted requirement" into all relevant UN Regulations, where the software has a major influence on the vehicle functionality. It is recommended that each Group of Experts under WP.29 decides which Regulations under its responsibility should be amended according to Annex B.

7.3. The parent group should decide on next steps, e.g. on developing a GTR on Software Update Processes. The task force notes that the development of a GTR will require further work.

7.4. There are a number of supporting processes that Contracting Parties of UNECE WP.29 and its forums will need to address to enable the full implementation of this recommendation, these include:

7.4.1. To integrate information about a software update in a DoC (Declaration of Conformance), an adaptation of the DoC definition and the implementation of IWVTA (International Whole Vehicle Type Approval) and the DETA (Data Exchange for Type Approval) database will be necessary. Therefore it is important for UNECE to invest in the development of DETA and DoC;

7.4.2. It should be investigated if relevant organizations should be provided limited access to DETA and DoC to check the RxSWIN numbers of the single vehicles during the PTI;

7.4.3. Different national entities may require vehicle registrations to be updated according to their national rules for software updates. The proposed Regulation may require changes to those rules to enable a full implementation. Where this happens there should be procedures in place to enable the sharing of information between national bodies to support the administration of these processes; It should be investigated if the national registration authorities could have limited access to DETA and DoC to support the process of sharing information;

7.4.4. The recommendation envisages continued assessment of the processes, practices and decision making of vehicle manufacturers for registered vehicles in relation to software updates. This could be considered to be market/field surveillance. As market/field surveillance is not addressed within the UNECE agreements of WP.29, UNECE will need to consider how this could be conducted.

7.4.5. It is recommended that the extension of an approval will be allowed for vehicles after production definitely discontinued. The parent group may wish to consider the proposed paragraphs in Annex B and whether it is legally permissible.

7.5. Future developments that may be considered include:

7.5.1. The ability of a vehicle to facilitate identification of any changes to system settings or if system software does not correspond to approved versions (e.g. reporting failures of secure boot mechanisms);

7.5.2. Quality requirements with respect to verification and validation for software (initial and updates) as they were out of scope as a result of the ToR.

7.6. For consideration during review of the regulatory text

7.6.1. It is recommended that text is introduced into Annex B to cover the situation where there is a software update for registered vehicles that requires an extension of an approval, particularly in the situation where the UN Regulation has been updated since the vehicle was registered. This is proposed as paragraph x.y.3. in brackets.

7.6.2. For Annex A categories L, O, R, S and T could be included but have had limited representation in the task force (in the case of category L) or no representation (in the other cases). It should therefore be considered whether the Regulation should apply to these categories of vehicles.

7.6.3. Annex A proposes that the length of time of duration of the SUMS Certificate of Compliance should be three years and the conformity of production checks should also be conducted every three years. It should be verified that these are appropriate.

7.7 Recommendations for implementation

7.7.1. The task force recommends that the proposed Regulation should consider a test phase before its full implementation. The aim of such a phase would be to validate and verify that the procedures envisaged for both, the vehicle manufacturers and Approval Authorities, work as intended and permit further revision of the Regulation, if needed. GRVA should consider what might be appropriate for such a test phase.

7.7.2. The task force recommends that time be given before the Regulation comes into force to permit vehicle manufacturers and Approval Authorities to adapt their processes so they can comply with this Regulation. GRVA should consider what might be an appropriate length of time and consider a phased introduction schedule. It is noted, that this will need to be balanced with the need to act in this area.

Annex A Draft proposal to introduce a UN Regulation on uniform provisions concerning the approval of software update processes

United Nations ECE/TRANS/WP.29/201x/xx

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

Draft new 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

I. Proposal

Draft new Regulation on uniform provisions concerning the approval of software update processes

Contents

1. Scope

1.1. This Regulation applies to vehicles of the categories [L], M, N, [O, R, S and T] with regard to software update processes.

2. Definitions

2.1. "Vehicle type" means vehicles of a particular category which do not differ in at least the following essential respects:

(a) The manufacturer;

(b) The manufacturer's type designation;

(c) Essential aspects of vehicle design with respect to software update processes

2.2. "RX Software Identification Number (RXSWIN)" means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.

2.3. "Software update" means a package used to upgrade software to a new version.

2.4. "Execution" means the process of installing and activating an update that has been downloaded.

2.5. "Software Update Management System (SUMS)" means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.

3. Application for Approval

3.1. The application for approval of a vehicle type with regard to software update processes shall be submitted by the vehicle manufacturer or by their duly accredited representative.

3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:

3.2.1. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.

3.2.2. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.

3.2.3. The SUMS Certificate of Compliance according to paragraph 6 of this Regulation.

3.3. A vehicle representative of the vehicle type to be approved shall be submitted to the Technical Service responsible for conducting approval tests.

4. Marking

4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:

4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.

4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.

4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.

4.3. The approval mark shall be clearly legible and shall be indelible.

4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.

4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

5. Approval

5.1. Approval Authorities shall grant, as appropriate, type approval with regard to software update procedures and processes, only to such vehicle types that satisfy the requirements of this Regulation.

5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.

5.3. Approval Authorities shall not grant any type approval without ensuring that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the software update processes aspects as covered by this regulation.

6. Software Update Management System (SUMS) Certificate of Compliance

6.1. Contracting Parties shall appoint an Approval Authority or Technical Service to carry out a preliminary assessment of the manufacturer and to issue a SUMS Certificate of Compliance.

6.2. In the context of the preliminary assessment of the manufacturer, the Contracting Parties shall ensure that the manufacturer has installed the necessary processes to comply with all legal requirements from this which are relevant for delivery of software updates according to this Regulation.

6.3. When this preliminary assessment has been carried out, a certificate named SUMS Certificate of Compliance with Annex 4 to this Regulation (hereinafter the SUMS Certificate of Compliance) shall be granted to the manufacturer.

6.4. The SUMS Certificate of Compliance shall remain valid for three years from the date of issuance of the certificate before a new assessment shall be conducted.

6.5. The Approval Authority which has granted the SUMS Certificate of Compliance may at any time verify its continued compliance. The SUMS Certificate of Compliance may be withdrawn if the requirements laid down in this Regulation are no longer met.

6.6. The manufacturer shall inform the Approval Authority or Technical Service of any significant change that could affect the relevance of the SUMS Certificate of Compliance. After consultation with the manufacturer, the Approval Authority or Technical Service shall decide whether new checks are necessary.

6.7. At the end of the period of validity of the SUMS Certificate of Compliance, the Approval Authority shall, as appropriate, issue a new SUMS Certificate of Compliance or extends its validity for a further period of three years. The Approval Authority shall issue a new certificate in cases where significant changes have been brought to the attention of the Approval Authority or Technical Service.

6.8. Existing vehicle type approvals shall not lose their validity due to the expiration of the manufacturer's SUMS Certificate of Compliance.

7. General Specifications

7.1. Requirements for the Software Update Management System of the vehicle manufacturer

7.1.1. **Processes to be verified at initial assessment**

7.1.1.1. 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;

7.1.1.2. 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;

7.1.1.3. 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.

7.1.1.4. 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;

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

7.1.1.6. A process whereby the vehicle manufacturer can identify target vehicles for a software update;

7.1.1.7. 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;

7.1.1.8. 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);

7.1.1.9. 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

7.1.1.10. 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;

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

7.1.1.12. 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 Authorities or Technical Services.

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

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

7.1.2.2. Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identifiers for the type approved system's hardware and software and any relevant vehicle or system parameters;

7.1.2.3. 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.

7.1.2.4. 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.

7.1.2.5. Documentation for all software updates for that vehicle type describing:

1. The purpose of the update;
2. What systems or functions of the vehicle the update may impact;
3. Which of these are type approved (if any);
4. If applicable, whether the software update affects any of the relevant requirements of those type approved system;
5. Whether the software update affects any system type approval parameter;
6. Whether an approval for the update was sought from an approval body;
7. How the update may be executed and under what conditions;
8. Verification that the software update will be conducted safely and securely.
9. Verification that the software update has undergone adequate verification and validation procedures.

7.1.3. **Security, the vehicle manufacturer shall demonstrate:**

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

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

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

7.1.4. **Additional Requirements for Software Updates over the air**

7.1.4.1. 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.

7.1.4.2. 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.

7.2. Requirements for the Vehicle Type

7.2.1. **Requirements for Software updates**

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

7.2.1.2. 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.

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).

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.

7.2.2. **Additional Requirements for over the air updates**

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

7.2.2.1.1. 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.

7.2.2.1.2. 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).

7.2.2.1.3. 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.

7.2.2.2. 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.

7.2.2.3. 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.

7.2.2.4. 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).

8. Modification and extension of the vehicle type

8.1. Every modification of the vehicle type shall be notified to the approval authority which granted the approval. The approval authority may then either:

8.1.1. Consider that the modifications made are unlikely to have an appreciable adverse effect and that in any case the vehicle still complies with the requirements; or

8.1.2. Require a further test report from the technical service responsible for conducting the tests.

8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The approval authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

9. Conformity of production

9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:

9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;

9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.

9.1.3. The Approval Authority or Technical Service shall periodically validate that the processes used and decisions made by the vehicle manufacturer are compliant, particularly for instances where the vehicle manufacturer chose not to notify the Approval Authority or Technical Service about an update. This may be achieved on a sampling basis.

10. Penalties for non-conformity of production

10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirement laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.

10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

11. Production definitively discontinued

11.1. If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".

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

12.1. The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

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

12.9.1.1 Schematic representation of the vehicle type

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
b) how vehicle users will be informed about software updates
c) how the update process will be performed securely

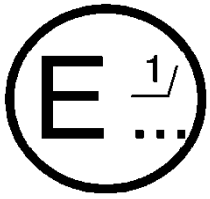
12.9.2 The number of the SUMS Certificate of Compliance

Annex 2

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

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

Approval No. …….. Extension No. .....

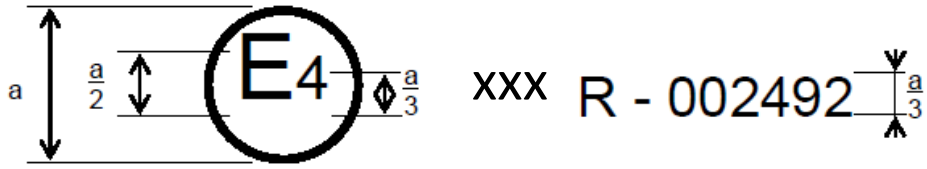
…

x.y ……

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)



a = 8 mm min.

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. xxx, and under the approval number 002492. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of Regulation No. xx.

Annex 4

Model of SUMS Certificate of Compliance

SOFTWARE UPDATE MANAGEMENT SYSTEM CERTIFICATE OF COMPLIANCE
WITH REGULATION No. [software update process regulation] xxx
No. [Reference number]
[……. Approval Authority]
Certifies that

Manufacturer: .....
Address of the manufacturer: .....
complies with the provisions of Regulation No. xxx
Checks have been performed on:
by (name and address of the Type Approval Authority or Technical Service):
Number of report:

The certificate is valid until […..date]
Done at [……Place]
On […….Date]
[…….Signature]

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

1. Add new definitions to the definition section:

Add a new paragraph 2.x., 2.y. and 2.z., as appropriate:

2.x. "RX Software Identification Number (RXSWIN)" means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.

2.y. "Electronic Control System" means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing. Such systems, often controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements. "The System", referred to herein, is the one for which type approval is being sought.

2.z. "Software" means the part of an Electronic Control System that consists of digital data and instructions.

2. 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.]

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

X. Production definitely discontinued

X.1. If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex [Communication form] to this Regulation.

X.2. The production is not considered definitely discontinued if the vehicle manufacturer intends to obtain further approvals for software updates for vehicles already registered in the market.]

4. 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: .....