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

Document status: Update to TFCS-ahRSUP3-02 during TFCS-ahRSUP3 Date: 16/07/2018   
  
Note: contents page needs to be updated

Contents

[1. Introduction 2](#_Toc507661162)

[1.1. Preamble 2](#_Toc507661163)

[1.2. Scope 3](#_Toc507661164)

[2. Definitions 4](#_Toc507661165)

[3. Document structure 5](#_Toc507661166)

[4. Process for software updates 5](#_Toc507661167)

[4.1. Scope of the software update process 5](#_Toc507661168)

[4.2. Software update approval process 5](#_Toc507661171)

[4.3. Prerequisites 9](#_Toc507661173)

[4.4. Type approval process responsibilities 10](#_Toc507661174)

[5. Safety and security requirements for software updates 11](#_Toc507661175)

[5.1. Objectives 11](#_Toc507661176)

[5.2. Safety requirements for updates 11](#_Toc507661177)

[5.3. Security requirement for updates 12](#_Toc507661178)

[5.4. Requirements for evidencing that updates and the update process is safe and secure. 12](#_Toc507661179)

[6. Identification of the installed software 13](#_Toc507661180)

[7. Conclusion and Recommendation for further proceedings 14](#_Toc507661182)

[Annex A *An annex for how the vehicle shall ensure the safety of the update process* 16](#_Toc507661189)

[Annex B Draft proposal to amend existing regulations to introduce software identification numbers 17](#_Toc507661190)

# Introduction

* 1. Preamble
     1. A Task Force was established as a subgroup of the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) of WP.29 to address Cyber Security and Over-the-air issues. The task force consisted of members of representatives from contracting parties and non-governmental organizations, e.g. FIA, CITA, ITU, OICA and CLEPA.
     2. The influence of software on vehicle functionality is increasing. Software influences the environmental and safety performance and other functions of a vehicle.
     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, software corrections and recalls.
     4. This recommendation provides requirements for how the certification process described in the UNECE regulations 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.
     5. This recommendation is an initial contribution for the IWG on ITS/AD to discuss and propose adaptions 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.

## Scope

* + 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.
    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.

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



* + 1. Security aspects of software updates are part of the “Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD”.
    2. 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 “1958 agreement”.
    3. 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.

# Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Architecture | 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 (ISO 26262) |
| Asset | A definable piece of vehicles, vehicle systems, networks, devices and services - and their information, data and functionality, which is recognized as 'valuable' to the organization or customer (ISO/IEC 27001) |
| Certified system | System defined by type approval legislation under the 1958 Agreement or a system as defined by the 1998 Agreement (UNECE definition) |
| Countermeasures | An action taken to counteract a danger or threat (Oxford English Dictionary) |
| Download stage | The stage of copying data from one computer system (for example a backend server) to another (for example a vehicle) (based on Oxford English Dictionary definition of download) |
| Electronic control systems | 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 (UNECE definition) |
| Execution stage | The process of installing and activating an update that has been downloaded (based on Oxford English Dictionary definition of execution) |
| Mitigation | Measure to modify risk (ISO/IEC 27000) |
| Organisation | Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (based on ISO/IEC 27000) |
| Over the air update | Over-the-air is any method of making data transfers wirelessly instead of using a cable or other local connection (GSMArena) |
| Risk | A combination of the consequences of an event and the associated likelihood of occurrence (ISO/IEC 31000) |
| Security Control | The management, operational, and technical controls (i.e., safeguards or countermeasures) to mitigate risks on confidentiality, integrity and availability  NOTE − This definition is intended to include controls that provide accountability, access control, authentication, non-repudiation, communication security, and privacy, which are sometimes considered as distinct from data confidentiality, data integrity and availability. |
| Software | The part of an Electronic Control System that consists of digital data and instruction |
| Software bug | An error, flaw, failure or fault in software that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. |
| Software components | One or more software units (ISO 26262) |
| Software update | 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. |
| Software unit | Atomic level software component of the software architecture that can be subjected to stand-alone testing (ISO 26262) |
| Threat | Potential cause of an unwanted incident, which may result in harm to a system or organization (ISO/IEC 27000) |
| Update process | The steps involved in the downloading and execution of new versions of software |
| Vehicle user | 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. |

# Document structure

* 1. Chapter 4 describes the process for managing software updates, including over the air updates, within the existing UN legal framework and regulations.
  2. Chapter 4 further describes supporting, pre-requisite requirements to enable the software update process to be conducted in an open and verifiable manner.
  3. Chapter 5 describes requirements to ensure that software updates, including OTA updates, can be conducted safely and securely.
  4. Chapter 6 describes requirements so that the status of the software on a vehicle, particularly its type approved systems, can be verified.

# Process for software updates

## Scope of the software update process

## In self certification regimes the references to type approvals which are contained in the subsequent paragraphs shall be understood in the way that all technical assessments and responsibilities are maintained but the actual type approval aspects are replaced by the self-certification documentation of the manufacturer;

## This section applies where the contracting party, on which territory the vehicle is registered, requires a UNECE Approval to cover the software update.

## Software update approval process

## Table 2 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 ~~R~~egistration according to national rules | New TA or individual approval or approval with limited scope Registration according to national rules |

Table 2: Summary of type approval processes

* + 1. Once a system is initially type approved (before 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 then initiate a process with a type approval authority to determine if an extension of a type approval or a new type approval is needed;
    2. If the software update occurs after a declaration of conformity has been produced, the declaration of conformity shall be updated reflecting the change of the certification/ type approval.
    3. When a software update occurs after 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.
   * 1. The following flow diagram represents the process to enable software updates after registration.
7. 1. Vehicle manufacturer (OEM) gains approval to conduct post-registration software updates, by gaining validation of their:

- Configuration and quality control processes (section 4.3)

- Processes to ensure updates are executed safely (section 5.2)

- Processes to ensure software updates are cyber secure (section 5.4)

3.iv. OEM records relevant information

3.iii. OEM may provide the update for the user to execute it

5.v. OEM updates information on the vehicles and records relevant information

5.iv. OEM may provide the update for the user to execute it

5.iii OEM verifies that the update can be performed safely and securely

5.ii. Update of the vehicle registration according to National Laws

2.i. Decision evidence recorded by OEM

1. 6. Type Approval Authority periodically validates that the processes used and decisions made by the OEM remain valid

5.i. Type Approval Authority provides an extension or new certificate

4.ii OEM contacts the Type Approval Authority for an extension or new certificate for each system affected

4.i Impact

2. New Software update

OEM assesses if any certification criteria is affected

3.i. No impact

3.ii. OEM verifies that the update can be performed safely and securely

* + 1. 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
  + 1. 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 a type approval body about an update.
    2. 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.

## Prerequisites

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

1. A process whereby the software and hardware components of a type approved system can be uniquely identified, documented and recorded as well as any interdependencies of that system on other systems;
2. A process whereby the vehicle manufacturer can assess, identify and record if a software update will affect existing type approved systems or any other system required for the safe and continued operation of a vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;
3. A process whereby an vehicle manufacturer can identify target vehicles for a software update;
4. A process to verify the compatibility of possible software/ hardware configurations in target vehicles;
5. The target vehicles have the ability to record the status of their type approved systems, software and parameters that can be readily checked;
6. The vehicle manufacturer is able to trace the software versions of the component of a type approved system in correlation with the RXSWIN (see chapter 6) of that system and verify that they are correct (and is able to provide this information to an authority should it be required);
7. The vehicle manufacturer has a process in place that they can use to inform national registration authorities about successful software updates where they are required to do so.
   * 1. The vehicle manufacturer shall describe their processes and the veracity of their processes to an approval authority who shall verify and certify those processes.
     2. 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:
8. Documentation of the decisions the vehicle manufacturer has made. This should include: the purpose of the update; what systems or functions of a vehicle an update may impact; which of these are type approved; and whether it affects any of the relevant requirements of those type approved system;
9. Documentation describing the processes used by the vehicle manufacturer (and their suppliers if relevant) and any relevant standards used to demonstrate their veracity;
10. Documentation describing the configuration of any relevant type approved systems, e.g. unique identifiers for its hardware and software and any relevant vehicle or system parameters. This should be for the system before and after an update;
11. 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.

## Type approval process responsibilities

* + 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;
    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;
    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. The type approval authority shall verify the vehicle manufacturer’s processes and decisions (including the decisions that are not notified to the authority). This may be achieved on a sampling basis.

# Safety and security requirements for software updates

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

## Safety requirements for updates

## 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.

* + 1. 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).
    1. 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.
  + 1. 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).

## Additional safety requirement for OTA updates.

* + 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.
    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.

## Security requirement for updates

* + 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.

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

* + 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 an vehicle manufacturer with respect to the above safety and security requirements.
    2. To enable an assessment of an vehicle manufacturer’s processes and procedures with regards 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 owner/operator (if any) in the update process.

# Identification of the installed software

## Use of the Software Identification Number, RxSWIN.

* + 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.
    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.
    3. The RXSWIN shall provide a reference for the software components of a given type approved system.
    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.
    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 manufacturer. For the purpose of certification, including the validation of the conformity of production, and the market surveillance, including recalls and PTI, the manufacturer shall provide this information to the authority if requested.
    6. A new RXSWIN shall be required, if a software change (update) requires an extension or renewal of the certification. Whether an extension or renewal of the certification is necessary, is described in specific regulations (e.g. in the vehicle type definition).
    7. A software change of a single component may affect different certifications. If this occurs and certification 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.
    8. If it is technically possible to bring registered vehicles in line with the extended or renewed certification, the manufacturer may describe in the information document the registered vehicles to which this may apply. The information provided shall be self-certified by the manufacturer and may not be verified by an authority during certification.
    9. If it is nationally legally permissible to install the software in a vehicle, the manufacturer shall record information regarding the software, including the checksums, 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 authority the manufacturer shall provide the information without any burden.
    10. The RXSWINs of the single vehicle shall be easily readable in a standardized way via the use of an electronic communication interface and if required by standard interface (OBD port).
    11. The manufacturer shall protect the RXSWINs on a vehicle against unauthorised modification.

# Conclusion and Recommendation for further proceedings

## The conclusion of this recommendation is that (over the air) updates should be treated as a post-registration update and that to regulate such updates the following processes would be needed.

* + 1. A verification by a type approval authority that the processes and procedures of an vehicle manufacturer would support the implementation of the recommendations of this paper;
    2. That individual software updates, post-registration, are assessed by vehicle manufacturer’s using the procedures listed in this recommendation and type approval authorities are notified when an update may affect any type approved system or change any entry within the information package for the vehicle;
    3. That type approval authorities 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.

## This paper may be taken forward as three parts:

* + 1. The main text should be proposed as a resolution;
    2. Annex A should be proposed as a horizontal regulation;
    3. Annex B should be proposed as a regulation to be appended to relevant existing regulations. This would require that the concept of RXSWIN shall be introduced into relevant UN regulations, where the software has a major influence on the vehicle functionality. It would further require that the RXSWIN shall be introduced as a part of appropriate chapters or annexes of those regulations, for instance those which describe special requirements to be applied to the Safety Aspects of Complex Electronic Vehicle Control Systems.

## The parent group should decide under which agreement this recommendation should be taken as this will affect the language used with regards the points referring to type approval.

## There are a number of supporting processes that signatory parties and the UNECE will need to address to enable the full implementation of this recommendation, these include:

* + 1. To integrate information about a software update in a DoC (declaration of conformity), an adaptation of the DoC definition and the implementation of IWVTA (international whole vehicle type approval) and DETA (data exchange for type approval) will be necessary. Therefore it is will be important for UNECE to invest in the development of DETA and DoC;
    2. It should be investigated if PTI should be provided limited access to DETA and DoC to check the RxSWIN numbers of the single vehicles during the PTI
    3. Different national entities may require vehicle registrations to be updated according to their national rules for software updates. 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.
    4. The recommendation envisages continued assessment of the processes, practices and decision making of vehicle manufacturer’s for registered vehicles in relation to software updates. This could be considered to be market/field surveillance. As market/field surveillance is not within the 1958 agreement the UNECE will need to consider how this could be conducted under its agreements.

## The RXSWIN shall be introduced in relevant regulations, where the software has an influence on the vehicle functionality:

* + 1. After introduction of the RxSWIN in the relevant regulation, it will be mandatory to declare the RxSWIN. However contracting parties may not use the RxSWIN for the national procedures as Registration or PTI; the parent group may wish to discuss this further.
    2. It is recommended that extension of type approval be allowed for vehicles after production definitely discontinued. The parent group may wish to consider how this is proposed in the document.

## Future developments that may be considered include:

* + 1. The ability to demonstrate to an appropriate party (such as a type approval authority) that a systems software corresponds to that referenced by the RxSWIN, for instance by checking the software’s version numbers and checksums or similar integrity validation data;
    2. 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);
    3. The Taskforce has developed requirements for (cyber) security and software update process. The security requirements apply to new vehicles as well as updates. Quality requirements with respect to verification and validation for software (initial and updates) are out of scope as a result of the ToR.
  1. For consideration during review of the regulatory text
     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 to regulation, particularly in the situation where the regulation has been updated since the vehicle was registered. This is proposed as point 1.6 in brackets.
     2. For the regulatory annex 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 regulations should apply to these categories of vehicles.
     3. The regulatory annex proposes that the length of time of duration of the 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.
     4. ~~It is noted that some contracting parties may implement the regulation and permit post-registration updates and others may not and that an update may be created which can be applied to both vehicles that are in production and those that are in use. To enable type approval of software update processes for both eventualities the following text has been proposed for annex B.~~

~~“~~*~~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. In agreement with the testing agency duplication of tests shall be avoided where possible~~*~~”~~

~~It is recommended that ITS/AD consider if this is needed and appropriate.~~

**Annex A Draft proposal to introduce a regulation on uniform provisions concerning the approval of software updates**

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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**

**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

*Page*

1. Scope 4

2. Definitions 4

3. Application for approval 4

4. Markings 5

5. Approval 5

6. Certificate of compliance 6

7. General specifications 7

8. Modification and extension of the vehicle type 11

9. Conformity of production 11

10. Penalties for non-conformity of production 11

11. Production definitely discontinued 12

12. Names and addresses of technical services responsible for conducting approval tests and of

Administrative departments 12

13. Transitional Provisions 12

Annexes

1. Information document 13

2. Communication form 14

3. Arrangement of approval mark 15

4. Model of certificate of compliance 16

# Scope

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

# Definitions

## "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) The manufacturer’s software update processes

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

## “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.

## “Software update” means a package used to upgrade software to a new version.

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

# Application for Approval

## 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.

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

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

## In cases where such 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 supply sufficient information to enable those checks to be made properly.

## The Certificate of Compliance according to Chapter 6 of this regulation.

## A vehicle representative of the vehicle type to be approved shall be submitted to the technical service responsible for conducting approval tests.

# Marking

## 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:

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

## 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.

## 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.

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

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

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

# Approval

## The 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.

## 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.

## The Approval Authority 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.

## ~~For the purpose of Annex 1 to this Regulation, the manufacturer shall ensure the software update processes aspects covered by this regulation, as defined in part 3 of annex 1, are implemented.~~

# Certificate of Compliance

## Contracting Parties shall appoint an Approval Authority to carry out a preliminary assessment of the manufacturer and to issue a certificate of compliance.

## 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.

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

## The certificate of compliance shall remain valid for three years from the date of issuance of the certificate before a new assessment shall be conducted.

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

## At the end of the period of validity of the certificate of compliance, the Approval Authority shall, as appropriate, issue a new 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.

# General Specifications

## **Requirements for the Organisation of the Manufacturer**

## **Processes for 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 authority upon request without any burden;

## 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;

## 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.

## 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;

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

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

## 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;

## 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);

## 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

## 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;

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

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

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

## 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;

## 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.

## 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.

## 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.

## **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;

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

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

## **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.

## 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.

## **Requirements for the Vehicle Type**

## **Requirements for Software updates**

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

## Where a vehicle type uses RXSWIN:

1. The RXSWIN of the single vehicle shall be protected to reasonably prevent unauthorized modification.

2. The RXSWINs of the single vehicle shall be easily readable in a standardized way via the use of an electronic communication interface and if required by standard interface (OBD port).

## **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.

## 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).

## 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 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.

## 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.

## 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).

# Modification and extension of the vehicle type

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

## 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

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

## 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.

# Conformity of production

## 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:

## 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;

## The Approval Authority or Technical Service 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.

## The Approval Authority shall periodically validate that the processes used and decisions made by the vehicle manufacturer remain valid, particularly for instances where the vehicle manufacturer chose not to notify a type approval body about an update~~, as defined in part 4 of annex 1, of this regulation~~. This may be achieved on a sampling basis

# Penalties for non-conformity of production

## 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.

## 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.

# Production definitively discontinued

## 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".

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

## 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.

# ~~Transitional provisions~~

**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.

1. General
   1. Make (trade name of manufacturer): .................................................................
   2. Type: .................................................................................................................
   3. Chassis: ..............................................................................................................
   4. Commercial name(s) (if available): ...................................................................
   5. Means of identification of type, if marked on the vehicle (b): ...........................
   6. Location of that marking: ..................................................................................
   7. Category of vehicle (c): .....................................................................................
   8. Name and address of manufacturer: ..................................................................
2. General construction characteristics of the vehicle:
   1. Identification of the electrical and electronic vehicle architecture with regard to software updates
3. Documentation describing vehicle systems and functionality that will enable software updates to be conducted according to this regulation;
4. Documentation describing how vehicle users will be informed about software updates as required by this regulation;
5. Documentation describing how the update process will be performed securely. This may refer to relevant parts of the vehicle’s cyber security type approval.

**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)



xxx

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 certificate of compliance**

CERTIFICATE OF COMPLIANCE

WITH REGULATION No. [software update regulation] xxx

No. [Reference number]

[……. Approval Authority]

Certifies that

Manufacturer: ...........................................................................................................................

Address of the manufacturer: ...................................................................................................

complies with the provisions of ~~Chapter 2 of Annex 1 to~~ 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 regulations to introduce software identification numbers

* 1. “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.

~~Suggested amendment from KBA:~~

~~An “RX Software Identification Number” (RXSWIN) is a dedicated identifier with [11] alphanumerical characters, 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. The first three characters of the RxSWIN shall define the number of the regulation.~~

* 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.
  2. “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.
  3. “Software” is the part of an Electronic Control System that consists of digital data and instructions.
  4. The RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface and if required by standard interface (OBD port).
  5. [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. In agreement with the testing agency duplication of tests shall be avoided where possible.]
  6. The 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 manufacturer shall be confidentially outlined.
  7. The manufacturer shall provide the following information in the communication annex of this regulation:  
     - the RXSWIN  
     - how to read the RXSWIN
  8. The manufacturer may provide in the communication annex of this regulation a list of the relevant parameters that will allow the identification of those vehicles that can be retrofitted with the software represented by the RXSWIN. The information provided shall be self-certified by the manufacturer and may not be verified by an authority during certification.
  9. 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 manufacturer. For the purpose of certification, including the validation of the conformity of production, and the market surveillance, including recalls and PTI, the manufacturer shall provide this information to the authority if requested
  10. PRODUCTION DEFINITELY DISCONTINUED
      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 Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 1 to this Regulation.
      2. The production is not considered definitely discontinued if the Manufacturer intends to obtain further approvals for Software Updates for vehicles already registered in the market.

COMMUNICATION ANNEX

(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 retrofitted with the software represented by the RXSWIN under point x.y.1: