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: v0.3 - revised document after TFCS ah RSU1 date: 07/12/2017

Contents

[1. Introduction 1](#_Toc498352720)

[1.1. Preamble 1](#_Toc498352721)

[1.2. Scope 2](#_Toc498352722)

[2. Definitions 3](#_Toc498352723)

[3. Process on software updates 3](#_Toc498352724)

[3.1. Overview 4](#_Toc498352725)

[3.2. Software update approval process 4](#_Toc498352726)

[3.3. Prerequisites 6](#_Toc498352727)

[3.4. Type approval process responsibilities 6](#_Toc498352728)

[4. Additional requirements for software updates 7](#_Toc498352729)

[4.1. Requirements for safely and securely conducting an update 7](#_Toc498352730)

[4.2. Safety requirement for all updates 7](#_Toc498352731)

[4.3. Additional safety requirement for OTA updates 8](#_Toc498352732)

[4.4. Security requirement for all updates 9](#_Toc498352733)

[4.5. Requirements for evidencing that the update is safe and secure 9](#_Toc498352734)

[5. Identification of the installed software 10](#_Toc498352735)

[5.1. Use of the Software Identification Number, RxSWIN 10](#_Toc498352736)

[6. Conclusion and Recommendation for further proceedings 11](#_Toc498352737)

[Annex 1 *an annex for how the vehicle shall ensure the safety of the update process (to be attached to appropriate regulations)* 12](#_Toc498352738)

[Annex 2 *an annex for where specific regulation require a part on software updates and help implementation (to be attached to appropriate regulation(s))* 13](#_Toc498352739)

# Introduction

* 1. Preamble  
       
     *Note: Both, the preamble of CS paper and Software paper shall be aligned, check possibility to have a common preamble for both recommendation papers on the general topic* 
     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 the vehicle functionality is increasing. The 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 is intended to provide requirements that could be used to determine how the certification process can be adapted to ensure compliance of any new software, independent of whether it is conducted with a wired connection or over the air, with the current technical legislation.

*Note: Japan understands the necessity of guideline for updates. However, Japan believes that setting a guideline for updates at this moment is not good strategy.*

* + 1. This recommendation is an initial contribution 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 ~~safety aspects~~ aspects for safe execution that need to be considered. Figure 1 shows that the outcome of these considerations will be to produce recommendations 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 “XYZ”.
    2. This recommendation applies to the legal framework for certification of vehicles. Some recommendations may in addition require national legislation (e.g. software updates after first registration).

# Definitions

*Note: revisit once paragraphs of other sections are finalized*

# Process on software updates

*Note:* *Need to consider how to frame the chapter to fit into type approval and self-certification schemes: a) rephrase general section b) put type approval / self-certification issues into new (sub-)sections/annexes*

## Overview

* + 1. It is recommended that the process for managing software updates, including over the air updates, utilises the existing procedures under existing UN legal framework and regulations. The process is further explained in this chapter.
    2. It is recommended that there are a number of supporting, pre-requisite processes in place to enable this process to be conducted in an open and verifiable manner. These are described in this chapter.
    3. It is recommended that there are processes in place to ensure that software updates, including OTA updates, can be conducted safely and securely. These are described in chapter 4.   
       *Note: move to a new section “Document structure”*
    4. It is recommended that there is a process wherein the status of the software on a vehicle, particularly its certified systems, can be verified. This process is described in chapter 5.   
       *Note: move to a new section “Document structure”*

## Software update approval process

* + 1. Table 1 below demonstrates how it is recommended that the software update process should be conducted.

|  |  |  |  |
| --- | --- | --- | --- |
| **Moment of update** | **No impact on type approval** | **Limited impact on type approval** | **Severe impact on type approval** |
| Initial type approval (TA) | Not applicable | Not applicable | Not applicable |
| Existing TA, **before Certificate of Conformity** (CoC) | No action | Extension TA | New TA |
| Existing TA, after CoC, **before registration** | No action | Extension TA and new CoC | New TA and new CoC |
| Existing TA, **after registration**, by OEM | 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 |
| Existing TA**, after registration**, not by OEM | New National approval. Registration according to national rules | New National approval. Registration according to national rules | New National approval. Registration according to national rules |

Table 1: Summary of type approval processes

* + 1. The existing process for approving updates to software, under the 1958 Agreement [reference needed] before registration of a vehicle for type approved systems is shown in the first three lines of table 2. Once a system is initially type approved (before registration) any changes to it are assessed with regards to whether they may affect its type approval. The nature of this assessment will be determined by the requirements of the relevant type approval legislation. If the OEM determines that a software update may affect a systems type approval they then initiate a process with a type approval body [check terminology] to determine if an extension to a type approval or a new type approval is needed. If the software update occurs after a certificate of conformity has been produced, this is updated should there be a change to the type approval.

*Note:* *Review accuracy (reference is 58A)*

* + 1. It is recommended that this process be adopted for software updates that occur after registration, including OTA updates. This would require the following steps for when an update is under the control of an OEM:

1. The OEM assesses whether a software update will affect the approval of a vehicle’s type approved systems and documents the result.
2. If the update will not affect any type approved systems they may conduct the update without need to contact a type approval authority
3. If an update may or will affect one or more type approved systems, then the OEM contacts a relevant type approval body to seek an extension or new type approval for the affected systems.
4. Where an extension or new type approval is granted, registration of it is conducted according to national laws. The declaration of conformance is updated to reflect the new status of the whole vehicle type approval. The status of the software on a vehicle is updated to reflect the new status of its type approval.

*Note: further explanation to 1) to 4) above; highlight what is already existing and what should be amended/newly introduced; consider comments in explanations*

* + 1. It is recommended that where an update to a type approved system is conducted outside of the control of an OEM after first registration, by a third party (aftermarket), the third party should initiate a new national approval for the type approval of the affected system or systems according to national laws.

*Note: clarification on multi-stage to be added*

* + 1. It is recommended that conformity of production checks and market surveillance are used to verify if the processes and decisions made by the OEM are appropriate, particularly regarding those updates which they have not notified the type approval body about.

*Note:* *Linked to Market Surveillance (in addition to CoP)*

* + 1. It is noted that different national entities may require the OEM to perform these processes to enable registration of the update according to their national rules. Where this happens it is recommended that there are procedures in place to enable the sharing of information between national bodies to support the administration of these processes.

*Note: add examples, e.g. electronic CoC/DoC*

* + 1. It is noted that there may be circumstances where there is a need to urgently perform an update to address a safety critical issue and that, theoretically, this needs to occur before a full assessment of the impact on type approved systems can be completed. If this circumstance ever occurs it is recommended that the OEM and any relevant appropriate authority convene to make a risk based judgement on whether to issue the update according to their national laws and processes.

*Note:* *Improve language to refer to 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. It is recommended that the OEM (and if relevant their suppliers) be able to demonstrate that they have the following processes in place:

1. There is a process whereby the software and hardware components of a system can be documented and recorded as well as any interdependencies of that system on other systems;

*Note:* *According to configuration management standards; process which ensures change management*

1. There is a process whereby the OEM can access, 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;
2. There is a process whereby an OEM can identify target vehicles for a software update;
3. There is a process to verify the compatibility of possible software/ hardware configurations in target vehicles;
4. The target vehicles have the ability to record the status of its type approved systems software and parameters that can be readily checked;
5. The OEM is able to trace the software versions of the electronic control systems on a type approved system to the Software Identification Number (see chapter 5) of that system and verify that they are correct (and is able to provide this information to an approval authority should it be required);
6. It is possible for the OEM to describe their processes and the veracity of their processes to an approval authority (should the need arise)
   * 1. To support conformity of production checks, market surveillance and approval of updates it is recommended that the following documents will be required:
7. The OEM has documentation evidencing the decisions they have made. This should include what systems an update may impact; which of these are type approved; and whether it affects any of the relevant requirements of those type approved system;

*Note: Comment DH to include purpose of the update*

1. The OEM has documentation describing their processes and any relevant standards used to demonstrate their veracity;
2. The OEM has documentation describing the type approved systems, e.g. hardware, software and system parameters/settings. This should be for the system before and after an update;
3. The OEM has documentation listing target vehicles for the update and can verify the compatibility of those vehicles with the update.

## Type approval process responsibilities

* + 1. It is recommended that for this process the OEM be responsible for assessing the potential impact of any software and for supplying all the necessary documentation to enable type approval authorities to verify the decisions they have made.

*Note:* *Whole document is recommendation, refine wording – also following sections*

* + 1. It is recommended that the OEM be responsible for making the initial decision regarding whether a software update may impact a type approval and contacting the relevant type approval body should that be the case.
    2. It is recommended that the OEM be responsible for providing evidence that they have the necessary procedures in place to support this process and evidence regarding whether a software update does or does not affect type approved systems.

*Note: OICA comment on issue“necessary procedures in place” => would introduce new requirements into the approval scheme on processes to be implemented by the OEM;  
type approved systems means THE system and OTHER systems*

* + 1. It is recommended that the approval authority is responsible for verifying that the processes of the OEM are appropriate. The approval authority will therefore need the requisite skills and capability to be able to do this.
    2. It is recommended that to ensure the openness of the system, the type approval authority is responsible for ensuring conformity of production and market surveillance takes place to verify that the OEM’s processes and decisions are appropriate and that the decisions they make regarding software updates that are not notified are appropriate.
    3. It is recommended that type approval authorities have processes in place to support information exchange between each other and access information from OEM’s. These should be in place to support market surveillance and periodic technical inspection. It is further recommended that where possible these processes should be electronic and harmonised.

*Note:Comment DH: Amend to be explicit about the need to be able to exchange information electronically. If CoC are updated will require ability to identify what CoC is valid for a given vehicle.*

# Safety and security requirements for software updates

*Note:Comment DH:* *Should this be part of a Type Approval Process  
- one off test (would require same process for any update)  
- variable and repeated for any update*

*Would need testable requirements or it allows variability*

## Requirements for safely and securely conducting an update

* + 1. In addition to ascertaining whether a software update will affect type approved systems it is necessary to ensure that software updates will not affect the general safety of the occupants of a vehicle when an update is executed and that the process of updating vehicle software cannot be misused, for example to enable uploading of unauthorised, malicious software. This chapter describes objectives for maintaining the safety of the vehicle during the update process and specific requirements relating to them.

## Safety requirement for all updates

* + 1. In the update process of a vehicle there are two stages. One is the download of an update to the vehicle and the other is the execution of that update once it is downloaded. It is recommended that during the download process the location and movement of the vehicle should not be restricted as long as there is no safety implication from the download process.
    2. To enable a software update to be executed safely it is recommended that the following be taken into account before the execution is initiated:
* Recovery
  + The OEM shall ensure that the system that is being updated can restore the software to a previous version after a failed or interrupted update or can be placed into a safe state;
* Information about the update
  + person executing the update
    - the
    - the expectedto completeexecution of
    - other instructions to execute the update
  + The OEM shall be able to convey the criticality of an update for recall, safety or security purposes to the driver (and if required to appropriate authorities)
* Pre-conditions before the execution
  + The OEM or driver of the vehicle should ensure that the location of the vehicle when the update is executed does not constitute a safety hazard;
  + The OEM should assess whether there would be a safety hazard from the vehicle operation or status during the update execution process and take appropriate action if that is the case;
  + The OEM shall ensure that the vehicle has enough power capacity for the update, as well as for a possible rollback and enough capacity for the operation of the vehicle after the update;
    1. Where the execution of an update or its failure might pose a safety hazard during driving it is recommended that the following be taken into account during the execution of an update:
* Take
* The OEM should 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. To enable a software update to be executed safely it is recommended that the following be taken into account after the execution of an update:
* The OEM shall ensure the person executing the update is informed of the success (or failure) of the update;

## Additional safety requirement for OTA updates

* + 1. OTA updates shall not be permitted during driving where additional action is required by the driver for completion of the update process.
    2. OTA updates shall not be permitted where action that requires a skilled person, such as a mechanic, is necessary for completion of the update process.
    3. For over the air updates it is recommended that the following be additionally taken into account:
* The OEM should ensure that it is possible for updates to be executed automatically should it be legally obliged for that to happen;
* The OEM should ensure that it is possible for updates to be initiated by the driver should permission of a person be required to execute an update;
* The OEM should ensure that there is mechanism whereby the legal owner of the vehicle can be informed about an update, should that be required (as it is possible the driver may not be the legal owner);
* The OEM should ensure that there is mechanism whereby the legal owner of the vehicle can provide the accent to an update being executed, should that be required (as it is possible the driver may not be the legal owner).

## Security requirement for updates

* + 1. It is recommended that the OEM is able to demonstrate to the authority that software updates can be carried out securely before downloading of the update occurs. This should include:
* demonstrate how the update procedures used are protected to reasonably prevent them being compromised, including fabrication of the system update program or firmware;
* demonstrate how the software patch is protected to reasonably prevent manipulated before the update process is initiated (i.e. ensure that only authorized, uncorrupted updates are sent to the vehicle);
* demonstrate how the authenticity of the software patch is protected to reasonably prevent their compromise and prevent invalid updates.

## Requirements for evidencing that the update 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 OEM with respect to the above safety and security requirements.
    2. To enable an assessment of an OEM’s processes and procedures with regards conducting software updates safely and securely the OEM shall be able to provide to the authority:
* documentation describing how the update will be performed securely;
* 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.

*Note: NL would like to make a proposal to ensure that the quality of the software update can be evidenced including the validation and verification procedures used (ref TFCS-ahRSU1-04). Document from FDA to be shared*

# Identification of the installed software

## Use of the Software Identification Number, RxSWIN

* + 1. To identify the software of a given certified system, a software identification number shall be introduced. The purpose of this shall be to provide a reference that can be used to verify that the software on certified systems is up to date and conforms with the 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.
    2. The software identification number shall provide a reference for the software components of a given certified system, if the certified system is defined in a specific regulation.
    3. The software identification number 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.
    4. The software identification number shall be introduced in regulations, where the software has a major influence on the vehicle functionality.
    5. The software identification number shall be introduced as a part of appropriate chapters or annexes, for instance those which describe special requirements to be applied to the Safety Aspects of Complex Electronic Vehicle Control Systems.
    6. Information regarding the software versions, including checksums, of the single components of the electronic control systems of every produced vehicle and the link to the software identification number shall be stored at the manufacturer. For the purpose of certification, including the validation of the conformity of production, and market surveillance, including recalls and PTI, the manufacturer shall provide this information without any burden to the responsible authority.
    7. A change of the software identification number 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).
    8. 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 software identification numbers shall be introduced for all the relevant certified systems.
    9. 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.
    10. 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 software identification number before and after the software change. On request of the authority the manufacturer shall provide the information without any burden.
    11. The software identification number of the single vehicle shall be easily readable via the use of an electronic communication interface and if required by standard interface (OBD port).
    12. The software identification number is not appropriate to verify unauthorized access to the vehicle functionalities. Therefor the manufacturer shall protect the electronic control system against unauthorized modification.
    13. The manufacturer shall protect the software identification numbers on a vehicle against unauthorised manipulation.

The chapter could also include recommendations for improving the utility of the RxSWIN, such as:

* The ability of the vehicle (or a third party inspecting the vehicle) to verify to an appropriate party (such as a type approval authority) that a systems software corresponds to that reference by the RxSWIN, for instance by checking its reference numbers.
* The ability of the vehicle (or a third party inspecting the vehicle) to validate to an appropriate party (such as a type approval authority) that a systems software corresponds to that reference by the RxSWIN, for instance by performing a hashing function on the software and comparing it to a value obtained previously (for example when approval was provided).
* The ability of a vehicle to report any changes to system settings or if system software does not correspond to approved versions (e.g. reporting failures of secure boot mechanisms)

# Conclusion and Recommendation for further proceedings

* *To ITS/AD*
* *On general approach (Guideline vs. Regulation, etc.)*
* *Future developments that could support the process further (such as electronic databases)*

# 

# Annex 1 *an annex for how the vehicle shall ensure the safety of the update process (to be attached to appropriate regulations)*

*Contents to be considered for meeting in Tokyo.*

***Note:*** *Comment DH: From OICA, we can take in charge the drafting of the two annexes with requirements that can be attached to appropriate regulations.*

*TFCS-AhSWTAN-04 (less the diagram)*

# Annex 2 *an annex for where specific regulation require a part on software updates and help implementation (to be attached to appropriate regulation(s))*

*Potentially based on OICA proposal*

*Note: the task force may wish to consider whether these annexes should be combined.*