Submitted by the IWG on CS/OTA

Informal document **GRVA-07-51**
7th GRVA, 21-25 September 2020
Agenda item 5(b)

Proposal for amendments to the proposed Interpretation Document for: Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (ECE/TRANS/WP.29/2020/80)

Submitted by the Informal Working Group on Cyber Security and Over-The-Air issues

The text reproduced below was prepared by the Informal Working Group on Cyber Security and Over-the-Air issues.

1. Preamble

1.1. The purpose of this document is to help clarify the requirements of paragraph 7 and Annex 1 of the UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (ECE/TRANS/WP.29/2020/80) and provide information on what may be used to evidence those requirements. The target audience for this document are for vehicle manufacturers submitting systems for test and for the Technical Services/ Appropriate Authorities assessing those systems. The outcome should be that this document is able to help harmonise the testing between different Technical Services/ Appropriate Authorities.

2. Note regarding evidencing the requirements

2.1. This document is only guidance. It provides information on what information might/would be acceptable for the Technical Services/ Appropriate Authorities and what level of information might be supplied. It is not intended to be exhaustive. The standards referenced are intended as examples, not mandatory. Depending on the vehicle type defined by the vehicle manufacturer and the practices and procedures they use alterative and/or equivalent information may be supplied.

2.2. For all the requirements in the regulation demonstration that they are met may be achieved via documentation/presentation and/or audit. The format of what documentation is supplied is open but should be agreed between the vehicle manufacturer and Technical Service/ Appropriate Authority prior to testing/audit.

3. Note regarding the process for how a software update may be applied using the Regulation (ECE/TRANS/WP.29/2020/80)

3.1. When a software update occurs after vehicle registration, including Over-The-Air (OTA) updates, the following steps may be employed when an update is under the control of the vehicle manufacturer:

(a) Before implementation of the first software update to a vehicle the vehicle manufacturer shall ensure it has a valid type approval for software update process and a valid Software Update Management System (SUMS) that is relevant to the vehicle type;

(b) 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;

(c) 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 and that the changes related to the update are documented;

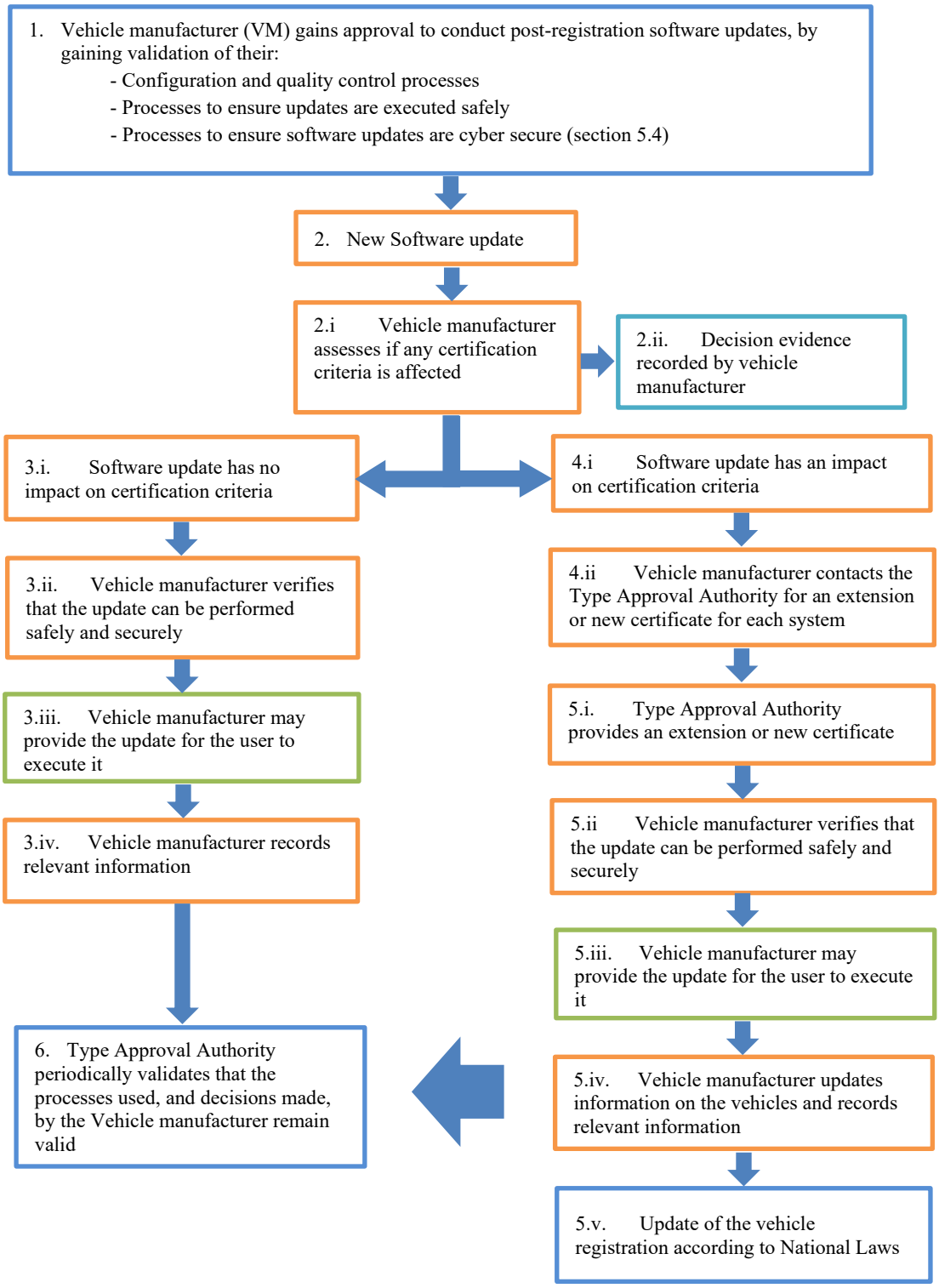
(d) If an update may or will impact the compliance of one or more type approved systems, then the vehicle manufacturer shall contact the relevant type approval authority to seek an extension or new certification for the affected systems;

(e) 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 the software update process regulation;

(f) The type approval authority shall periodically validate that the processes used, and decisions made by the vehicle manufacturer were appropriate. The validation shall include an audit of a sample of the document(s) recording changes.

3.2. 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.

3.3. The following flow diagram represents the process described above to enable software updates after registration.



4. Guidance on the requirements of the Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (ECE/TRANS/WP.29/2020/80)

Note. The paragraphs referred to below refer to the paragraphs of the Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (ECE/TRANS/WP.29/2020/80)

A. Paragraphs 1 to 7 of the Regulation

"1. Scope"

No guidance included in this document with regards this requirement

"2. Definitions"

No guidance included in this document with regards this requirement

"3. Application for Approval"

No guidance included in this document with regards this requirement

"4. Marking"

No guidance included in this document with regards this requirement

"5. Approval"

No guidance included in this document with regards this requirement

"6. Certificate of Compliance for Software Update Management System"

No guidance included in this document with regards this requirement

B. Paragraphs 7 to 7.1.1.1.

"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 its Technical Service upon request;"

Explanation of the requirement

This requirement has two parts.

The first is a requirement for the vehicle manufacturer to state the processes/procedures they use to store the information relevant to this regulation and how they will secure it. For this the term 'securely' refers to the IT (information technology) security implemented at the manufacturer.

The outcome should be that the vehicle manufacturer is able to provide assurance that all relevant documentation/information will be stored and that they have appropriate security controls in place to protect that information.

The second part is a requirement for the vehicle manufacturer to detail the processes/procedures for how they will make such information available to a Technical Service or Appropriate Authority should they have the right and need to access that information.

Documents containing information relevant to this regulation (and their previous versions, if needed) should be made available to the Technical Service/Approval Authority based on their

request. The manufacturer may use their preferred file transfer platforms for the same, as long as it is in agreement with the Technical Service/ Approval Authority.

The outcome should be that the vehicle manufacturer and Technical Service/Approval Authority agree that the process described would allow the Technical Service/ Approval Authority to access information pertinent to the approval of software updates and their delivery processes and the conditions under which it should be shared.

Examples of documents/evidence that could be provided

For evidencing that information is securely held, International Standard Organization (ISO) 27001 or ISO 9001 (add-on) can be used.

The information provided can cover:

(a) Access controls (both physical and personal);

(b) Controls for securing the servers that hold the information;

(c) Monitoring controls;

(d) Configuration controls;

(e) quality controls/ quality management systems employed.

The information to be included in these processes is defined within the Regulation, for example paragraph 7.1.2.

For detailing the processes by which this information may be accessed the vehicle manufacturer should include:

(a) Contact point at the vehicle manufacturer;

(b) Information on the file transfer platform.

C. Paragraph 7.1.1.2.

"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;"

Explanation of the requirement

The aim of the requirement is to provide assurance on the configuration control processes used in the manufacturer and that these will support the implementation of the regulation.

The follow clarifications should be noted

'Version number' may be done at vehicle level and/or component level as long as it is possible to fulfil the requirement of the Regulation for unique identification of software/hardware

'Integrity validation data' refers to how the software can be authenticated as being the version claimed by the vehicle manufacturer. Check sums or hash values can be used for this purpose. The term was used to be technology neutral as other, equivalent methods, could be employed.

'Relevant hardware components' refer to hardware with software on it within the type approved system. This should include ECUs, CPUs or other hardware as identified by the vehicle manufacturer

'Can be uniquely identified' intends that it should be possible, at the very least, for the vehicle manufacturer to identify and verify the software present on a type approved system based on it software version numbers

Examples of documents/evidence that could be provided

For evidencing the processes existing configuration control processes/procedures can be used and relevant standards may be referred to. This should be accompanied by an explanation of why they are relevant.

D. Paragraph 7.1.1.3.

"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;"

Explanation of the requirement

The RXSWIN refers to a unique identifier that defines a unique set of software of a type approved system in accordance with a given UN Regulation "X". Within this the unique identifier should only change when there is a change to the software of that defined system which leads to an extension or renewal of type approval. Where a software update does not affect the type approval of the system this unique identifier should remain unchanged.

This Regulation mandates that the vehicle manufacturer should have a process in place to record information relating to the RXSWIN (see 7.1.2.3). This includes information on all permissible software versions of the software defined under a given RXSWIN, the relevant 'integrity validation data' of those different software versions.

The outcome should be that the vehicle manufacturer is able to demonstrate that information regarding the RXSWIN can be accessed and updated.

The following clarification should be noted

This requirement only applies when an RXSWIN is implemented

The storage of the information should be at the vehicle manufacturer. The vehicle manufacturer should determine the level of information stored on the vehicle

Examples of documents/evidence that could be provided

Manufacturer should detail and explain their processes to provide information regarding:

(a) How the information regarding the RXSWIN is updated, this should include reference to configuration control processes used;

(b) How all information related to the RXSWIN, held either on the vehicle or at the manufacturer, can be accessed.

E. Paragraph 7.1.1.4.

"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;"

Explanation of the requirement

The regulation requires that it should be possible to verify that the software on a type approved system corresponds to that defined in the relevant RXSWIN. As a minimum it must be possible for the vehicle manufacturer to perform this verification down to a component level.

Examples of documents/evidence that could be provided

The manufacturer should provide details of their process(es) and/or tools that will be used to verify the software on a type approved system corresponds to the list of software versions covered under a particular RXSWIN.

F. Paragraph 7.1.1.5.

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

Explanation of the requirement

This requirement is to ensure that there is one or more processes to assess if an update will affect other systems, e.g. for cascading effects. It is accepted that there are limits in how far a process could cover interdependencies.

The outcome should be assurance that the vehicle manufacturer is able to identify how different systems interact and assess if an update will impact the expected behaviour of any other system.

The following clarifications should be noted

'Interdependencies' should be identified at both the functional and software level and should consider all systems which have an interface with the updated system

'Other systems' includes systems affecting safety, cyber security, theft protection, energy efficiency and environmental behaviour

Examples of documents/evidence that could be provided

The processes used to assess if there are any interdependencies between systems and the potential for a software update to affect other systems should follow best practice. This may include quality control processes.

Standards that might be applicable include:

(a) ISO 10007;

(b) ISO 9001;

(c) International Automotive Task Force (IATF) 16949;

(d) A Software Process Improvement and Capability Determination (SPICE) or similar.

The processes should consider the following:

(a) Initiation, identification and documentation of the change;

(b) Identification of interfaces and systems which communicate with the updated systems;

(c) Identification of any systems that are affected by the updated systems and the corresponding impact;

(d) Evaluation of the change.

G. Paragraph 7.1.1.6.

"7.1.1.6. A process whereby the vehicle manufacturer is able to identify target vehicles for a software update;"

The following clarification should be noted

'Target vehicle' refers to individual vehicles (for example VIN based for registered vehicles)

This requirement is on the process

Examples of documents/evidence that could be provided

The processes should consider the following:

(a) Listing target vehicles affected by the software update;

(b) The process should consider the steps of going from target groups for an update (e.g. all diesel vehicles of a specific vehicle type) through to the individual vehicles to be updated;

(c) Measures implemented to reduce the risk of error in identification of target vehicles.

H. Paragraph 7.1.1.7.

"7.1.1.7. A process to confirm the compatibility of a software update with the target vehicle(s) configuration before it is issued. This shall include an assessment of the last known software/hardware configuration of the target vehicle(s) for compatibility with the update before it is issued;"

The following clarification should be noted

'Issued' refers to the software update being made available for installation

Examples of documents/evidence that could be provided

Standards that might be applicable include:

(a) Compliance with configuration management as per ISO 10007;

(b) ISO 9001;

(c) IATF 16949 or similar.

The processes should consider the following:

(a) Regression testing with the last known configuration of the software update;

(b) Listing the hardware or software preconditions required for the software update;

(c) How these preconditions will be checked before an update is downloaded;

(d) Identifying relevant configurations of the target vehicle type;

(e) demonstrating how testing will cover compatibility for those configurations.

I. Paragraph 7.1.1.8.

"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);"

Explanation of the requirement

This requirement relates only to type approved systems and the relevant test used for the type approval(s). It requires that there are processes to assess whether a software update might affect or change the outcome of that test under the conditions in which it was conducted. This requirement should consider the relevant test used for the type approval(s) and whether the software update might affect or change the outcome of that test under the conditions in which it was conducted.

The following clarifications should be noted

'Parameters' here does not refer to software parameters but to the parameters describing the system type approval

'Affect' refers to a change requiring an extension of a type approved system or a new type approval

Examples of documents/evidence that could be provided

Standards that might be applicable include:

(a) Compliance with configuration management as per ISO 10007, ISO 9001, IATF 16949 or similar

(b) Standards for providing claims, arguments and evidence such as BSI 15026-2:2011

The processes should consider the following:

(a) Quality control procedures for the software updates may be relevant;

(b) Evaluation of the change;

(c) Assessment of which regulatory requirements/ parameters are impacted/ altered by the software update. This should include what evidence is required to reach a conclusion.

J. Paragraph 7.1.1.9.

"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:

(a) Entries in the information package will need to be modified;

(b) Test results no longer cover the vehicle after modification;

(c) Any modification to functions on the vehicle will affect the vehicle's type approval."

The following clarification should be noted

'Alter or disable any other parameters or functions' refers to type approved systems

'Parameters' here does not refer to software parameters but to the parameters describing the system type approval

'Information package' refers to the affected type approval and its information document

K. Paragraph 7.1.1.10.

"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;"

Explanation of the requirement

This requirement relates to non-type approved systems that are required to ensure safe operation of the vehicle and there are processes to assess if software updates will affect them.

The requirement also requires processes to identify if an update will change the functionality of a vehicle compared to when it was registered.

Examples of documents/evidence that could be provided

Standards that might be applicable include:

(a) IATF 16949 contains Quality Management Systems for configuration management

The processes should consider the following:

(a) Quality control and configuration management processes;

(b) Processes for assessment of which systems are impacted by the software update;

(c) Processes for assessment of which safety and operational conditions are impacted by a software update;

(d) Processes for assessment of any functionality that was added/ altered after the vehicle was registered;

(e) How these impacts are documented.

L. Paragraph 7.1.1.11.

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

Explanation of the requirement

The intention of this requirement is that the vehicle user is able to be informed about changes to the vehicle they are responsible for. This should include any information relating to the situation where the vehicle user is supposed to perform some/any action for the download and installation of the updates. In case of a package of multiple updates the 'vehicle user'

should be able to be informed about that package of updates.

The means whereby information is provided to the user need not be on the vehicle but it must be accessible by 'vehicle users' if they want to access the information.

This requirement does not cover the need for consent.

The outcome for this requirement should be that the Technical Service/ Appropriate Authority is satisfied that vehicle users will be able to be informed about updates to their vehicle by the process described by the vehicle manufacturer.

The following clarifications should be noted

'Is able to' requires that the user should be informed by any suitable means

Examples of documents/evidence that could be provided

The vehicle manufacturer should provide information on the methods of communication used to inform the vehicle user about updates. They should demonstrate the effectiveness of these methods.

M. Paragraph 7.1.1.12.

"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 responsible Authorities or the Technical Services. This may be for the purpose of type approval, conformity of production, market surveillance, recalls and Periodic Technical Inspection (PTI)."

No guidance included in this document with regards this requirement

N. Paragraph 7.1.2.

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

Explanation of the requirement

The requirement is provided to ensure that a vehicle manufacturer's processes enable information regarding software updates, as defined in the sub-clauses below, to be recorded.

This requirement enables information to be made available to the registration authority should they request an audit of a manufacturer relating to software updates and establishes what information should be recorded for that requirement.

There may be cases where a vehicle system is regularly updated with the same type of update and the system being updated is not type approved. An example of this may be map data using the same data fields and formats via the same delivery method. To reduce repetition, in this instance, one could require that the information detailed below is recorded only once and it is stated that it holds true for that class of updates (which would need to be defined by the manufacturer). The logic of this would be to reduce the burden on manufacturers if they can demonstrate that such a regular series of updates would exist.

The following clarifications should be noted

'Each update' refers to every update (both type approved and non-type approved)

'Vehicle type' is intended such that information is recorded for a given vehicle type and not for each vehicle

Examples of documents/evidence that could be provided

The requirement should be evidenced by the vehicle manufacturer demonstrating how they will/do record the information required below in the sub-clauses of 7.1.2. The information may be contained in (existing) configuration control management documentation.

O. Paragraph 7.1.2.1.

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

Explanation of the requirement

This requirement refers to documents that describe the vehicle manufacturer's processes relevant to this Regulation and requires that the vehicle manufacturer documents them.

Examples of documents/evidence that could be provided

Documentation of the processes listed in paragraph 7.1.1 and its sub-clauses and a description of how these are applied to individual vehicle types.

P. Paragraph 7.1.2.2.

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

Explanation of the requirement

The requirement requires that all configurations of a vehicle system relating to a software update are able to be recorded and assurance can be provided that they will be recorded. The type approved systems being updated may comprise a range of previous configurations or all previous versions.

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include the recording of:

(a) Any relevant vehicle or system parameters of the target update system before and after update;

(b) Hardware and software version numbers of the system being updated.

Q. Paragraph 7.1.2.3.

"7.1.2.3. For every RXSWIN, there shall be an auditable register describing all 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."

Explanation of the requirement

The integrity validation data should allow a suitably skilled person to verify that the software has not been manipulated.

The following clarifications should be noted

'Integrity validation data' refers to the output of the method used for authentication of the software versions

'Auditable register' refers to a register that can be audited

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include evidencing the effectiveness of the processes for recording of:

(a) For each RXSWIN:

(i) List of software relevant to the RXSWIN

(j) Software version and integrity validation data of each piece of software before and after the update

(b) How information regarding the RXSWIN is recorded. Information relating to an RXSWIN should include:

(i) Description of the system/software functionality relevant to that RXSWIN;

(ii) Regulations affected;

(iii) Software relevant to the RXSWIN;

(iv) Integrity validation data of the software relevant to the RXSWIN;

(v) Method used for generating the integrity validation data.

(c) How information regarding an update that is relevant to an RXSWIN is recorded, this should include:

(i) List of RXSWINS affected by the software update

R. Paragraph 7.1.2.4.

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

Explanation of the requirement

Information on target vehicles should be available on the VIN-level for registered vehicles.

Confirmation that compatibility is ensured can be provided for a group of vehicles rather than individual vehicles.

The following clarifications should be noted

'Target vehicles' refers to the vehicles targeted for the software update

'Last known configuration' refers to the fact that the vehicle manufacturer may not know the actual configuration of every vehicle of a vehicle type in the field, for example if it has been modified by its owner or a mechanic

Examples of documents/evidence that could be provided

Configuration management processes may be used to evidence what the manufacturer will record. This should include evidencing the effectiveness of the processes for:

(a) Identification of target vehicles for the update

(b) Checking the compatibility of the last known configuration of the target vehicles with the software update

S. Paragraph 7.1.2.5.

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

Explanation of the requirement

Information may be clustered for updates covering multiple purposes or multiple updates covering the same purpose (if appropriate). There may be cases where a vehicle system is regularly updated with the same type of update and the system being updated is not type approved. An example of this may be map data using the same data fields and formats via the same delivery method. To reduce repetition, in this instance, one could require that the information detailed below is recorded only once and it is stated that it holds true for that class of updates (which would need to be defined by the manufacturer). The logic of this would be to reduce the burden on manufacturers if they can demonstrate that such a regular series of updates would exist.

Examples of documents/evidence that could be provided

Evidence should be provided by demonstrating the processes used to record the

information. If the processes have already been used then the output of the processes (the resultant documentation) could be shown to demonstrate them.

"(a) The purpose of the update;"

No guidance included in this document with regards this requirement

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

Explanation of the requirement

The intent is for the vehicle manufacturer to describe the target system or function for the update, e.g. braking system, radio and any other systems or functions that may be affected by the update.

"(c) Which of these are type approved (if any);"

No guidance included in this document with regards this requirement

"(d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;"

Explanation of the requirement

This requires the manufacturer to record the output of the processes described in paragraph 7.1.1.8 (the two requirements are linked).

The justification / reasoning for the decisions should be recorded together with the outcome (to allow verification at audit should that be required by a Technical Service or Approval Authority).

"(e) Whether the software update affects any system type approval parameter;"

Explanation of the requirement

This requirement should consider the relevant test used for the affected type approval(s) and whether the software update might affect or change the outcome of that test under the conditions in which it was conducted

The justification / reasoning for the decisions should be recorded together with the outcome (to allow verification at audit should that be required by a Technical Service or Approval Authority).

The following clarifications should be noted

'Software update' refers to the definition in 2.9

'Any system type approval parameter' refers to any parameters defined within any affected type approval regulation(s)

"(f) Whether an approval for the update was sought from an approval body;"

No guidance included in this document with regards this requirement

"(g) How the update may be executed and under what conditions;"

The following clarifications should be noted

'Conditions' refers to any criteria needed to execute an update

If new hardware is necessary for the update, this should be mentioned in the conditions under this requirement

Examples of documents/evidence that could be provided

The manufacture may use the release notes for the software update to fulfil this requirement. The release note should contain the following information (but are not limited to):

(a) Conditions that define a safe state for the update to be executed;

(b) Actions required from the vehicle user / a competent person (if needed) before an update is installed.

"(h) Confirmation that the software update will be conducted safely and securely."

Explanation of the requirement

The information provided should contain details on why the conditions from clause g) lead to a safe and secure software update (justification) and how they will be met (verification).

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

Explanation of the requirement

The purpose of verification and validation is to ensure that the software update works as intended. The method(s) used should be appropriate to the software update.

The following clarifications should be noted

'Adequate' refers to a level where the manufacturer is able to justify that what has been performed is sufficient for the purposes of verification and validation. This should be primarily determined by the manufacturer and may be confirmed by a Technical Service/Approval Authority (upon audit for example)

'Update' refers to installation & execution

Examples of documents/evidence that could be provided

The processes use for ensuring software updates undergo verification and validation to a level that the manufacturer is satisfied with and how this will be recorded.

T. Paragraphs 7.1.3. and 7.1.3.1.

"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;"

Explanation of the requirement

This requirement addresses processes for ensuring the integrity and authenticity of the software updates that are to be delivered. The outcome should be that a vehicle manufacturer can justify to a Technical Service/Approval Authority that they have processes in place for controlling what updates are sent to a vehicle and for ensuring that only known and valid updates are sent to vehicles. This may include processes for securing updates provided to them by suppliers for delivery to a vehicle.

The following clarification should be noted

'Manipulation' refers to changes or interference in the software code of the update that is not authorised by the originator(s) of the update

The test of "reasonable" should be that the manufacturer can argue through claims, arguments and evidence that the process employed is sufficient to meet the threat

Examples of documents/evidence that could be provided

Standards that might be applicable include: ISO/SAE 21434

The Cyber Security Management System may be used to evidence this requirement. The vehicle manufacturer should explain how it does this.

The cyber security regulation may be used as a reference.

Demonstration of the manufacturers processes may be provided as evidence. This may include a description of any integrity checking mechanism for software updates during their download and execution stage. This should provide proof of authenticity if it demonstrates that the sourced software update is same as the one sent to the vehicle.

U. Paragraph 7.1.3.2.

"7.1.3.2. The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system;"

Explanation of the requirement

This requirement addresses the processes for delivering software updates to ensure they cannot be compromised to deliver unauthorized updates. The outcome should be that a vehicle manufacturer can justify to a Technical Service/Approval Authority that they have processes in place for ensuring that the update mechanism cannot be manipulated to provide unauthorised updates.

The following clarification should be noted

'Development' refers to processes employed during the creation of the update system to build in security by design

'Update system' refers to the system created to deliver updates

Examples of documents/evidence that could be provided

The Cyber Security Management System may be used to evidence this requirement. The vehicle manufacturer should explain how it does this.

The cyber security regulation may be used as a reference.

Demonstration of the security processes applied to the software update process.

V. Paragraph 7.1.3.3.

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

Explanation of the requirement

The intention of this requirement is to ensure there are processes in place so that only properly tested software updates are sent to the vehicle. The processes required should aim to minimise bug-fixing of errors in software update.

This requirement is linked to paragraph 7.1.2.5. part i). Paragraph 7.1.3.3. requires confirmation of the processes. Paragraph 7.1.2.5. requires documentation that they have been applied to software updates.

The following clarification should be noted

'Appropriate' refers to the use of processes which meet a justifiable level of expectation

Examples of documents/evidence that could be provided

The manufacturer should be able to provide an argument, based on claims and evidence, that the processes they employ are appropriate. These may refer to standards and best practice.

W. Paragraph 7.1.4.

"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."

Explanation of the requirement

The outcome of this process should be that vehicle manufacturers are able to provide a reasoned argument that their processes fulfil this requirement.

The outcome of these processes should be recorded as described in paragraph 7.1.2.5.

Examples of documents/evidence that could be provided

Manufacturers should provide details of the processes and criteria used for assessing whether updates may have an impact on safety while driving.

X. Paragraph 7.1.4.2.

"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 specific skilled or complex action, for example recalibrate a sensor post-programming, in order to complete the update process, the update can only proceed when a person skilled to do that action is present or is in control of the process."

Explanation of the requirement

The intention of this requirement is to ensure that vehicle owners are not required to do anything technical or complex for a software update to be initiated or completed. The requirement specifies that manufacturers have established processes for managing this. Where an update may require complex action there needs to be a process to ensure such updates are only carried out when a suitable skilled or trained person is present, or is in control of the process when it is conducted remotely.

The outcome of these processes should be recorded as described in paragraph 7.1.2.5.

Y. Paragraph 7.2.

"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."

Explanation of the requirement

This requirement addresses the mechanisms implemented on a given vehicle type to ensure that only valid software updates are downloaded and executed. This requires that updates authenticity and integrity are validated by the vehicle, for example by signing. Together with the processes described in paragraphs 7.1.3.1. and 7.1.3.2. this should ensure that the end to end system for software updates, from creation through delivery to execution, is secure.

The following clarification should be noted

'Reasonably' refers to the level of protection being foreseeable and based on state of the art preventions

Examples of documents/evidence that could be provided

Vehicle manufacturers should provide details of the mechanisms used to ensure that only authenticated and integrity checked software updates are executed on a vehicle. The results of authentication testing may be used as evidence.

The cyber security regulation may be used as a reference.

Z. Paragraph 7.2.1.2.

"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."

Examples of documents/evidence that could be provided

Vehicle manufacturers may provide:

Demonstration of how an RXSWIN is generated for a given vehicle type and made unique

Demonstration that each RXSWIN has a one on one relation with its appropriate Regulation and how the regulation can be identified

AA. Paragraph 7.2.1.2.2.

"7.2.1.2.2 Each 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).

If RXSWINs are not held on the vehicle, the manufacturer shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the Approval Authority. This declaration shall be updated each time the declared software version(s) is updated. In this case, the software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port)."

Explanation of the requirement

This requirement requires that the RXSWINs shall be stored on a vehicle, in order for them to be read from it or that if it is not stored on the vehicle that the versions of software relevant to an RXSWIN should be stored on a vehicle and the link to a RXSWIN be declared.

Examples of documents/evidence that could be provided

The following standards and regulations may be relevant:

(a) ISO14229/1;

(b) (OBD port): ISO 14229;

(c) UN Regulation No. 83.

AB. Paragraph 7.2.1.3.

"7.2.1.2.3. The vehicle manufacturer shall protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the vehicle manufacturer shall be confidentially provided."

Explanation of the requirement

This requirement addresses the security of the RXSWIN. Its intention is that only authorised parties may change the RXSWIN and that this only happens when a relevant software update is executed on the vehicle.

Examples of documents/evidence that could be provided

The manufacturer may describe where/how the RXSWINs are stored and what measures have been implemented to protect them against unauthorized modification.

AC. Paragraph 7.2.2.

"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."

Explanation of the requirement

The intention of this requirement is to ensure that vehicle types can manage failed updates.

A safe state should be implemented when it is not possible or desirable to roll-back to a previous version. This may include reducing the capability or functionality of the vehicle. The manufacturer should determine what a safe state may be.

The following clarification should be noted

'Safe state' may be interpreted as "an operating mode in case of a failure of an item without an unreasonable level of risk" (using the definition provided in ISO 26262)

Examples of documents/evidence that could be provided

The following standards and regulations may be relevant:

(a) ISO 26262 may be used with regards functional safety

The following may be relevant or evidenced to provide assurance that this requirement is met:

(a) Requirements of the safe state;

(b) Functionalities added/ disabled to achieve the safe state.

AD. Paragraph 7.2.2.1.2.

"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)."

Examples of documents/evidence that could be provided

The following may be used to provide assurance that this requirement is met:

(a) Description of measures taken by the vehicle manufacturer;

(b) Demonstration of requirements via documentation/presentation and/or physical test.

AE. Paragraph 7.2.2.1.3.

"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 shall be achieved through technical means that ensures the vehicle is in a state where the update can be executed safely."

No guidance included in this document with regards this requirement

AF. Paragraph 7.2.2.2.

"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 made available shall contain:

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

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

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

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

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

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

Explanation of the requirement

This requirement is linked to the processes required under paragraph 7.1.1.11 but this requirement is linked to the vehicle type where over the air updates are provided. The intention is that the vehicle user may be informed about updates before they are executed and be provided with any information they need to decide whether or not to execute the update (assuming they have the legal right to do so and wish to be informed).

If a vehicle user is provided the option for a onetime authorisation for software updates, and opts for it, he need not be informed about every update. How this is managed may still need to be demonstrated to ensure it enables the transfer of a vehicle to a new user or a vehicle user to change their preference.

Examples of documents/evidence that could be provided

The vehicle manufacturer could have release notes for each of the updates detailing the information from the requirement in paragraph 7.2.2.2. The vehicle manufacturer could demonstrate how this information may be made available to the user. This may include:

(a) Description of how the vehicle user is able to be informed;

(b) Demonstration via documentation/presentation and/or physical test.

AG. Paragraph 7.2.2.3.

"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:

(a) Ensure the vehicle cannot be driven during the execution of the update;

(b) 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."

Examples of documents/evidence that could be provided

The following may be used to provide assurance that this requirement is met:

(a) Demonstration of requirements via documentation/presentation and/or physical test.

AE. Paragraph 7.2.2.4.

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

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

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

Examples of documents/evidence that could be provided

The following may be used to provide assurance that this requirement is met:

(a) Demonstration of requirements via documentation/presentation and/or physical test.

AF. Paragraph 7.2.2.5.

"7.2.2.5. The vehicle shall ensure that preconditions have to be met before the software update is executed."

Explanation of the requirement

The manufacturer should define preconditions to be met and confirm that those

preconditions are met whenever the software update starts.

Examples of documents/evidence that could be provided

The following may be used to provide assurance that this requirement is met:

(a) Demonstration of requirements via documentation/presentation and/or physical test

AG. Paragraph 8.

"8. Modification and extension of the vehicle type

8.1. Every modification of the vehicle type which affects its technical performance and/or documentation required in this Regulation shall be notified to the approval authority which granted the approval. The approval authority may then either:"

Explanation of the requirement

The "vehicle type" for the system approval for software updates comprises of the technical solution used to provide a software update. It is independent of the update purpose e.g. due to a recall, a bug fix or providing a new feature to the customer.

Changes within the technical solution used to provide a software update may constitute an extension or new type depending on the nature of the change.

Example for creation of a new "vehicle type":

(a) A new technical way of providing software updates.

Examples for an extension of an existing "vehicle type":

(a) Changes in the means to protect integrity and authenticity of the update;

(b) Changes in the way of reading and protecting the RXSWIN;

(c) Changes in the way of ensuring safe state of the vehicle in case of remote updates;

(d) Changes in the ways of informing the vehicle user about a software update.

AH. Paragraphs 8.1.1. to 12

"8.1.1. Consider that the modifications made still comply with the requirements and documentation of prior type approval; or"

No guidance included in this document with regards this requirement

"8.1.2. Require a further test report from the Technical Service responsible for conducting the tests."

No guidance included in this document with regards this requirement

"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."

No guidance included in this document with regards this requirement

"9. Conformity of production"

No guidance included in this document with regards this requirement

"10. Penalties for non-conformity of production"

No guidance included in this document with regards this requirement

"11. Production definitively discontinued"

No guidance included in this document with regards this requirement

"12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities"

No guidance included in this document with regards this requirement

5. Guidance regarding the information document

A. Item 9.1.

9.1. General construction characteristics of the vehicle type:

Examples of documents/evidence that could be provided

The following may be used to provide assurance that this requirement is met:

(a) Technical means used to provide software updates for example: wired, via Bluetooth, via Wi-Fi, via Cellular or any other means. This should be independent of the purpose of the update;

(b) Any relevant components specific to the provision of software updates and the requirements of this Regulation.

B. Items 9.2. to 9.3.1.

"9.2. The number of the Certificate of Compliance for Software Update Management System:

9.3. Security measures.

9.3.1. Documents for the vehicle type to be approved describing that the update process will be performed securely "

Examples of documents/evidence that could be provided

Evidence that could be provided includes:

(a) Certificate of compliance for the Cyber Security Management System and a note on how it relates to this regulation (to confirm it does);

(b) Documents for the vehicle type to be approved describing how the update process will be performed securely;

(c) Documents for the vehicle type to be approved describing how the RXSWINs on a vehicle is protected against unauthorized manipulation.

C. Items 9.3.1. to 9.4.2.

"9.3.2. Documents for the vehicle type to be approved describing that the RXSWINs on a vehicle are protected against unauthorized manipulation

9.4. Software updates over the air

9.4.1. Documents for the vehicle type to be approved describing that the update process will be performed safely

9.4.2. How a vehicle user is able to be informed about an update before and after its execution."