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

TFCS-15-04

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

**Economic Commission for Europe**

Inland Transport Committee

**World Forum for Harmonization of Vehicle Regulations**

**xxx session**

Geneva, DD–DD MM YYYY

Item XXX of the provisional agenda

**Draft new Regulation on software updates**

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

**Submitted by the expert from xxx**

The text reproduced below was prepared by the experts from xxx

Contents

*Page*

7. General specifications 7

Annexes

1. Information document 13

**Introduction**

The purpose of this document is to help clarify the requirements of the Regulation on uniform provisions concerning the approval of software update processes 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.

**Note regarding evidencing the requirements**  
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.

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.

**Note for test phase**

For the test phase this document is intended to be a “living document”. It should aim to capture generic evidence/solutions/formats/standards that were provided by vehicle manufacturers as evidence against each requirement that was accepted by a Technical Service/ Appropriate Authority. Where the evidence supplied may be attributable to a given manufacturer it will not be recorded in this document.

At the end of the test phase the Task Force on Cyber Security and Over the Air Updates will validate this document and its contents.

# Scope

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

# Definitions

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

# Application for Approval

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

# Marking

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

# Approval

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

# Software Update Management System (SUMS) Certificate of Compliance

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

# General Specifications

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

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

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

|  |
| --- |
| 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) shall 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, ISO 27001 or ISO 9001 (add-on) may be used. The information provided may cover:   * access controls (both physical and personal) * controls for securing the servers that hold the information * monitoring controls * configuration controls * quality controls/ quality management systems employed   The information to be included in these processes are 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:   * contact point at the vehicle manufacturer * information on the file transfer platform |

## 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 may 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 may 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 used existing configuration control processes/procedures and relevant standards may be used. This may be accompanied by an explanation of why they are relevant. |

|  |
| --- |
| Remark for test phase |
| A possible output from the process may be an overview of all components of type approved systems (containing software) and the software on them. During the pilot phase it can assessed if it would be feasible to produce such an overview. |

## 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 shall 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 may 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 shall 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 shall detail and explain their processes to provide information regarding:  a) how the information regarding the RXSWIN is updated, this may 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 |

## 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 shall 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. |

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

|  |
| --- |
| Explanation of the requirement |
| This requirement is to ensure 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’ refers to systems affecting safety, security, theft protection 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: ISO 10007, ISO 9001, ISO/TS 16949, A SPICE or similar  The processes may consider the following:  - initiation, identification and documentation of the change  - identification of interfaces and systems which communicate with the updated systems  - identification of any systems that are affected by the updated systems and the corresponding impact  - evaluation of the change |

|  |
| --- |
| Remark for test phase |
| Test phase will seek to elaborate on the processes used and the requirement. |

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

|  |
| --- |
| Explanation of the requirement |
| The following clarification should be noted:  - ‘target vehicle’ refers to individual vehicles (for example VIN based) |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The processes may consider the following:  - listing target vehicles affected by the software update  - measures implemented to reduce the risk of error in identification of target vehicles |

## 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;

|  |
| --- |
| Explanation of the requirement |
| 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: Compliance with configuration management as per ISO 10007, ISO 9001, ISO/TS 16949 or similar.  The processes may consider the following:   * regression testing with the last known configuration of the software update * listing the hardware preconditions required for the software update * how these preconditions will be checked before an update is downloaded * compatibility testing with all possible registered/ last known configurations of the target vehicle type |

## 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:   * compliance with configuration management as per ISO 10007, ISO 9001, ISO/TS 16949 or similar * standards for providing claims, arguments and evidence such as BSI 15026-2:2011   The processes may consider the following:   * quality control procedures for the software updates may be relevant * evaluation of the change * assessment of which regulatory requirements/ parameters are impacted/ altered by the software update. This may include what evidence is required to reach a conclusion |

## 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

|  |
| --- |
| Explanation of the requirement |
| 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 |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

## 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:  - ISO TS16949 contains Quality Management Systems for configuration management  The processes may consider the following:   * quality control and configuration management processes * processes for assessment of which systems are impacted by the software update   - processes for assessment of which safety and operational conditions are impacted by a software update  - processes for assessment of any functionality that was added/ altered after the vehicle was registered  - how these impacts are documented |

|  |
| --- |
| Remark for test phase |
| How this can be done will be looked at in the test phase, particularly system (rather than component level). |

## 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 shall 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:   * ‘vehicle user’ may be a driver, owner, fleet owner, mechanic or other legally entitled person * ‘is able to’ requires that the user may be informed by any suitable means |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The vehicle manufacturer shall provide information on the methods of communication used to inform the vehicle user about updates. They may demonstrate the effectiveness of these methods. |

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

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

## **The vehicle manufacturer shall record, and store ~~at their premises~~, 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 may 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. |

|  |
| --- |
| Remark for test phase |
| The test phase will evaluate if the existing documentation can be used to evidence the requirements below. |

## Documentation describing the processes used by the vehicle manufacturer for ~~providing~~ 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 7.1.1 and its sub-clauses and a description of how these are applied to individual vehicle types. |

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

|  |
| --- |
| Explanation of the requirement |
| The requirement is so 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 may include the recording of:   * any relevant vehicle or system parameters of the target update system before and after update * hardware and software version numbers of the system being updated |

|  |
| --- |
| Remark for test phase |
| * it shall be evaluated whether it is possible to store the complete history of all software updates over the entire vehicle lifetime (or period over which software updates are provided) * during the test phase it will be evaluated whether the text relating to parameters is relevant or covered elsewhere |

## 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.

|  |
| --- |
| Explanation of the requirement |
| The integrity validation data shall allow a suitably skilled person to verify that the software has not been manipulated.  The following clarifications should be noted:   * ‘integrity validation data’: the method used for authentication of the software version |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Configuration management processes may be used to evidence what the manufacturer will record. This may include evidencing the effectiveness of the processes for recording of:   1. For each RXSWIN:  * list of software relevant to the RXSWIN * software version and integrity validation data of each of the software before and after the update  1. How information regarding the RXSWIN is recorded. Information relating to an RXSWIN should include:  * description of the system/software functionality relevant to that RXSWIN * regulations affected * software relevant to the RXSWIN * integrity validation data of the software relevant to the RXSWIN * method used for generating the integrity validation data  1. How information regarding an update that is relevant to an RXSWIN is recorded, this may include:  * list of RXSWINS affected by the software update |

|  |
| --- |
| Remark for test phase |
| The use of calibration identification numbers for software identification can be evaluated in the test phase. (this is an identification system used by some OEMs). |

## 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.

|  |
| --- |
| Explanation of the requirement |
| Information on target vehicles needs to be available on the VIN-level.  Confirmation that compatibility is ensured can be provided at a group level, not individual vehicle level  The following clarifications should be noted:   * ‘target vehicles’ refers to the vehicles targeted for the software update * ‘update’ refers to every single 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 may include evidencing the effectiveness of the processes for:   * identification of target vehicles for the update * checking the compatibility of the last known configuration of the target vehicles with the software update |

|  |
| --- |
| Remark for test phase |
| During the test phase it could be checked if it is possible/practical to check if the last known configuration is the actual configuration in the vehicle and such how compatibility checking is performed. |

## 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 may be provided by demonstrating the processes use 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. |

|  |
| --- |
| Remark for test phase |
| During the test phase it should be evaluated how this can be done efficiently, especially for updates not affecting type approved systems. |

1. The purpose of the update;

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

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

|  |
| --- |
| 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. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

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

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

1. 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 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). |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

|  |
| --- |
| Remark for test phase |
| It will be reviewed whether clauses d to f should be merged. |

1. 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) |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

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

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

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

|  |
| --- |
| Explanation of the requirement |
| 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):   * conditions that define a safe state for the update to be executed * actions required from the vehicle user / a competent person (if needed) before an update is installed |

1. Verification 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). |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

1. Confirmation ~~Verification~~ that the software update has undergone adequate 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. |

## **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;

|  |
| --- |
| 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 |

|  |
| --- |
| 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.  Annexes B and C of the cyber security recommendation 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 would provide proof of authenticity if it demonstrates that the sourced software update is same as the one sent to the vehicle. |

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

|  |
| --- |
| 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.  Annexes B and C of the cyber security recommendation may be used as a reference.  Demonstration of the security processes applied to the software update process. |

## 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 7.1.2.5 part i). 7.1.3.3. requires confirmation of the processes. 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. |

|  |
| --- |
| Remark for test phase |
| The test phase may review if it is possible to evidence this requirement. |

## **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.

|  |
| --- |
| 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 requirement 7.1.2.5. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Manufacturers shall provide details of the processes and criteria used for assessing whether updates may have an impact on safety while 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.

|  |
| --- |
| 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.  The outcome of these processes should be recorded as described in para. 7.1.2.5. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| - |

## **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.

|  |
| --- |
| 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 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 shall 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.  Annex B and C of the cyber security working paper may be referred to. |

## 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.

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| 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 * for extensions and new type approvals, demonstration of how the new/updated RXSWIN can be traced to the previous associated RXSWINs/ software versions |

|  |
| --- |
| Remark for test phase |
| This requirement has been flagged for further assessment during the test phase. |

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

|  |
| --- |
| 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. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following standards and regulations may be relevant:   * ISO14229/1 * (OBD port): ISO 14229 * ECE R83 |

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

|  |
| --- |
| 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. |

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

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

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

|  |
| --- |
| 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:   * ISO 26262 may be used with regards functional safety   The following may be relevant or evidenced to provide assurance that this requirement is met:   * requirements of the safe state * functionalities added/ disabled to achieve the safe state |

## 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).

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following may be used to provide assurance that this requirement is met:   * description of measures taken by the vehicle manufacturer * demonstration of requirements via documentation/presentation and/or physical test |

## 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.

|  |
| --- |
| Explanation of the requirement |
|  |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

## 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.

|  |
| --- |
| Explanation of the requirement |
| This requirement is linked to the processes required under 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 requirement 7.2.2.2. The vehicle manufacturer could demonstrate how this information may be made available to the user. This may include:   * description of how the vehicle user is able to be informed * demonstration via documentation/presentation and/or physical test |

## 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.

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following may be used to provide assurance that this requirement is met:   * demonstration of requirements via documentation/presentation and/or physical test |

## 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).

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| The following may be used to provide assurance that this requirement is met:   * demonstration of requirements via documentation/presentation and/or physical test |

# Modification and extension of the vehicle type

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

# Conformity of production

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

# Penalties for non-conformity of production

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

# Production definitively discontinued

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

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

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

**Annex 1**

**Information document**

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

**0. GENERAL**

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

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

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

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

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

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

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

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

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

Copied over from Annex 2 of UN R-46 as the below format is based on the UN regulation format. Above is the format of the EU regulation.

**1. Make (trade name of manufacturer): .................................................................**

**2. Type and general commercial description(s): .............................................**

**(**Type is the type to be approved, commercial description refers to the product in which the approved type is used)

**3. Means of identification of type, if marked on the vehicle: ................................**

**4. Location of that marking: ..................................................................................**

**5. Category(ies) of vehicle: ..........................................................................................**

**6. Name and address of manufacturer/** **manufacturer's representative: ...................................**

**7. Name(s) and Address(es) of assembly plant(s):......................................................................**

**8. Photograph(s) and/or drawing(s) of a representative vehicle: ...........................**

{N*ote: to be clarified which approach to be used for numbering. Suggestion is to redefine it as above. To be confirmed*}

**12.9. Software Updates**

12.9.1 General construction characteristics of the vehicle type

|  |
| --- |
| Explanation of the requirement |
| Suggested re-numbering if the scheme in green is adopted:  9. Software Updates  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:   * 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 * Any relevant components specific to the provision of software updates and the requirements of this regulation |

12.9.1.1 Schematic representation of the vehicle type

|  |
| --- |
| Explanation of the requirement |
| The intention is to have a schematic that shows the typical properties of the Vehicle Type. The aim is to show the interconnections between the components of the vehicle type’s software update mechanism/processes (as described in 12.9.1). |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| It is noted that it may not be possible to provide a schematic for a vehicle’s software update processes. If it is not possible to provide a schematic the vehicle manufacturer should explain why. |

|  |
| --- |
| Remark for test phase |
| It is not clear what should be presented under this point or how to present the information. Test phase to consider solutions or proposals that could be used for clarification of this point (or its removal).  We need to be able to define the properties and characteristics of the software update process. |

12.9.1.2 Documents for the vehicle type to be approved describing:

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

|  |
| --- |
| Explanation of the requirement |
| The intention of this requirement is a list of the components and systems that allow for software updates to be performed. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

|  |
| --- |
| Remark for test phase |
| Note: for the test phase may review if this paragraph is a duplication of 12.9.1. |

b) how vehicle users will be informed about software updates

|  |
| --- |
| Explanation of the requirement |
| Note: an alternative format for reporting this requirement is provided under proposed section 9.4, see below in green. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

c) how the update process will be performed securely

|  |
| --- |
| Explanation of the requirement |
| Suggested clarification for description of the security measures (to also include securing the RxSWIN) and re-numbering:  9.3. Security measures.  9.3.1. Documents for the vehicle type to be approved describing how the update process will be performed securely.  9.3.2. Documents for the vehicle type to be approved describing how the RXSWINs on a vehicle is protected against unauthorized manipulation. |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Evidence that could be provided includes:   * certificate of compliance for the Cyber Security Management System and a note on how it relates to this regulation (to confirm it does) * documents for the vehicle type to be approved describing how the update process will be performed securely * documents for the vehicle type to be approved describing how the RXSWINs on a vehicle is protected against unauthorized manipulation |

12.9.2 The number of the SUMS Certificate of Compliance

|  |
| --- |
| Explanation of the requirement |
| Suggested re-numbering if the scheme in green is adopted:  9.2. The number of the SUMS Certificate of Compliance |

|  |
| --- |
| Examples of documents/evidence that could be provided |
|  |

**Note: suggested addition/clarification for documentation regarding OTA processes for the vehicle**

* 1. **Software updates over the air**
     1. **Documents for the vehicle type to be approved describing that the update process will be performed safely**
     2. **How a vehicle user is able to be informed about an update before and after its execution.**

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. ………..

*Note: suggested addition, based on other regulations. Points 7 and 8 are “new” and specific to this regulation.*

*Copied from Annex 4 UN R-46*

**Extension No.: ..........................................**

**1. Make (trade name of manufacturer): ...........................................................................**

**2. Type and general commercial description(s) ................................................................**

**3. Means of identification of type, if marked on the vehicle: ...........................................**

**3.1. Location of that marking: .............................................................................................**

**4. Category(ies) of vehicle: ………………………………………………………………**

**5. Name and address of manufacturer / manufacturer’s representative: .............................................................................**

**6. Name(s) and Address(es) of the production plant(s) ..........................................................................**

**7. Number of the certificate of compliance for software update management system: …**

**8. Software updates over the air included (Yes/no):…………………………..**

**9. Technical Service responsible for carrying out the tests:..............................................**

**10. Date of test report: ........................................................................................................**

**11. Number of test report: ...................................................................................................**

**12. Remarks: (if any).**

**13. Place: ............................................................................................................................**

**14. Date: .............................................................................................................................**

**15. Signature: ......................................................................................................................**

**16. The index to the information package lodged with the Type Approval Authority, which may be obtained on request is attached.**

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. xxx **as amended by the 00 series of amendments.**

*Note: suggested correction to the text.*

Annex 4

Model of SUMS ~~Certificate~~ Certificate of Compliance

**CERTIFICATE OF COMPLIANCE FOR SOFTWARE UPDATE MANAGEMENT SYSTEM(S)**

WITH REGULATION No. [Cyber Security Regulation] xxx

No. [Reference number]

[……. Approval Authority]

Certifies that

Manufacturer or manufacturer’s representative: ...............................................................................................

Address(es) of the manufacturer or manufacturer’s representative: ..................................................................

complies with the provisions of paragraph **7.1.** of Regulation No. xxx

Checks have been performed on:

by (name and address of the Type Approval Authority or Technical Service):

Number of report:

The certificate is valid until […..date]

Done at [……Place]

On […….Date]

[………….Signature]

**Attachments: description of the Software Update Management System(s) by the manufacturer.**

Notes:

* clarification of text.
* Additional requirement for a summary or short description of the SUM (to be looked at in test phase)
* Clarification – in principle a SUMS certificate may be used for more than one type approval. It may be needed to verify that it is applicable for subsequent approvals after the initial approval. (can be checked in test phase)
* Clarification – in the test phase to consider if the SUMS would cover multiple sub-systems/systems and how this could be done. To be confirmed if the proposal plural of system(s) should be made singular.

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

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

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

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

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

x.y. Requirements for software identification

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

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

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

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

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

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

|  |
| --- |
| Explanation of the requirement |
| - |

|  |
| --- |
| Examples of documents/evidence that could be provided |
| Evidence that may be provided include:   * approval for software update processes regulation * the RXSWIN format and description of how it is to be read |

|  |
| --- |
| Remark for test phase |
| - |

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

X. Production definitely discontinued

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

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

ANNEX [Communication form]

**COMMUNICATION**

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

issued by : Name of administration:

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

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

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



concerning: 2/ APPROVAL GRANTED

APPROVAL EXTENDED

APPROVAL REFUSED

APPROVAL WITHDRAWN

PRODUCTION DEFINITELY DISCONTINUED

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

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

Approval No. ……….. Extension No.

…

***x.y RXSWIN:***

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

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