Attachment 97 Software update and software update management system

Refer to: R156 00 Series

97.1   Effective date and Scope

97.1.1   Effective date from 2028/1/1, new vehicle types of category M, N and O and from 2030/1/1, all vehicle types of category M, N and O, shall complied with this attachment.

97.1.2   Except for large passenger vehicles and child-only vehicles, the vehicle that the applicant applying for low volume safety type approval may be exempt from this attachment.

97.1.3   The vehicle that the applicant applying for vehicle-by-vehicle low volume safety type approval, may be exempt from this attachment.

97.1.4   Technical Service can carry out test according to UN Regulations that this direction harmonized with: UN R156 00 Series of amendments and following amendments of above-mentioned regulations.

97.2   Definitions

97.2.1   "RX Software Identification Number (RXSWIN)" means a dedicated identifier, defined by the applicant, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation No X type approval relevant characteristics of the vehicle.

97.2.2   "Software update" means a package used to upgrade software to a new version including a change of the configuration parameters.

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

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

97.2.5   "Vehicle user" means a person operating or driving the vehicle, a vehicle owner, an authorised representative or employee of a fleet manager, an authorised representative or employee of the applicant, or an authorized technician.

97.2.6　"Safe state" means an operating mode in case of a failure of an item without an unreasonable level of risk.

97.2.7　"Software" means the part of an Electronic Control System that consists of digital data and instruction.

97.2.8　"Over-the-Air (OTA) update" means any method of making data transfers wirelessly instead of using a cable or other local connection.

97.2.9　"System" means a set of components and/or sub-systems that implement a function of functions.

97.2.10　"Integrity validation data" means a representation of digital data, against which comparisons can be made to detect errors or changes in the data. This may include checksums and hash values.

97.3　The principles of applicable type and scope of Software update and software update management system shall be as follows:

97.3.1　Same vehicle brand.

97.3.2　Same essential aspects of the design of the vehicle type with respect to software update processes.

97.4　Certificate of Compliance for Software Update Management System

97.4.1　Applicants shall provide undermentioned documents with specific context in triplicate to apply to certification institution for "certificate of compliance for cyber security management system", certification institution would issue "Certificate of Compliance for Software Update Management System" after evaluation of applicant ：

97.4.1.1　Documents describing the Software Update Management System.

97.4.1.2　A signed declaration of compliance for Software Update Management System.

97.4.2　In the context of the assessment, the applicant shall provide declaration and demonstrate to the satisfaction of the certification institution or its technical service that they have the necessary processes to comply with all the requirements for software updates according to this attachment.

97.4.3　When this assessment has been satisfactorily completed and in receipt of a signed declaration from the applicant, a certificate named Certificate of Compliance for SUMS to this attachment (hereinafter the Certificate of Compliance for SUMS) shall be granted to the

applicant.

97.4.4　The Certificate of Compliance for SUMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.

97.4.5　The certification institution which has granted the Certificate of Compliance for Software Update Management System may at any time verify its continued compliance. The Certificate of Compliance for Software Update Management System may be withdrawn if the requirements laid down in this attachment are no longer met.

97.4.6　The applicant shall inform the certification institution or its technical service of any change that will affect the relevance of the Certificate of Compliance for Software Update Management System. After consultation with the applicant, the certification institution or technical service shall decide whether new checks are necessary.

97.4.7　At the end of the period of validity of the Certificate of Compliance for Software Update Management System, the certification institution shall, after a positive assessment, issue a new Certificate of Compliance for Software Update Management System or extends its validity for a further period of three years. The certification institution shall issue a new certificate in cases where changes have been brought to the attention of the certification institution or its technical service and the changes have been positively re-assessed.

97.4.8　Existing vehicle type approvals shall not lose their validity due to the expiration of the applicant's Certificate of Compliance for Software Update Management System.

97.5　General specifications

97.5.1　Requirements for the Software Update Management System of the applicant

97.5.1.1　Processes to be verified at initial assessment

97.5.1.1.1　A process whereby information relevant to this attachment is documented and securely held at the applicant and can be made available to an certification institution or its technical service upon request;

97.5.1.1.2 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;

97.5.1.1.3 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;

97.5.1.1.4 A process whereby, for a vehicle type that has an RXSWIN, the applicant 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;

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

97.5.1.1.6 A process whereby the applicant is able to identify target vehicles for a software update;

97.5.1.1.7 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;

97.5.1.1.8 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);

97.5.1.1.9 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.

97.5.1.1.10   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;

97.5.1.1.11   A process whereby the vehicle user is able to be informed about updates;

97.5.1.1.12   A process whereby the applicant shall be able to make the information according to paragraph 97.5.1.2.3 and 97.5.1.2.4 available to responsible certification institution or the technical services.

97.5.1.2   The applicant shall record, and store, the following information for each update applied to a given vehicle type:

97.5.1.2.1   Documentation describing the processes used by the applicant for software updates and any relevant standards used to demonstrate their compliance;

97.5.1.2.2   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;

97.5.1.2.3   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.

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

97.5.1.2.5   Documentation for all software updates for that vehicle type describing:

          (a)   The purpose of the update;

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

97 Software update and software update management system

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

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

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

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

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

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

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

97.5.1.3   Security – the applicant shall demonstrate:

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

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

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

97.5.1.4   Additional requirements for software updates over the air

97.5.1.4.1   The applicant shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety, if conducted during driving.

97.5.1.4.2   The applicant 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.

97.5.2 Requirements for the Vehicle Type

97.5.2.1 Requirements for Software updates

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

97.5.2.1.2 Where a vehicle type uses RXSWIN:

97.5.2.1.2.1 Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the applicant, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.

97.5.2.1.2.2 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 applicant shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the certification institution. 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).

97.5.2.1.2.3 The applicant 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 applicant shall be confidentially provided.

97.5.2.2 Additional Requirements for over the air updates

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

97.5.2.2.1.1 The applicant 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.

97.5.2.2.1.2 The applicant 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).

97.5.2.2.1.3 When the execution of an update may affect the safety of the vehicle, the applicant 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.

97.5.2.2.2 The applicant 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.

97.5.2.2.3 In the situation where the execution of an update whilst driving may not be safe, the applicant 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.

97.5.2.2.4 After the execution of an update the applicant 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).

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