Submitted by the Chair of the
Task Force on Cybersecurity and OTA (software updates)

Informal document **GRVA-03-03**
3rd GRVA, 3-4 June 2019
Agenda item 4(b)

Overview of the recommendations on software updates

Content

1. Background
2. Software updates
3. Ongoing work - the test phase

Background

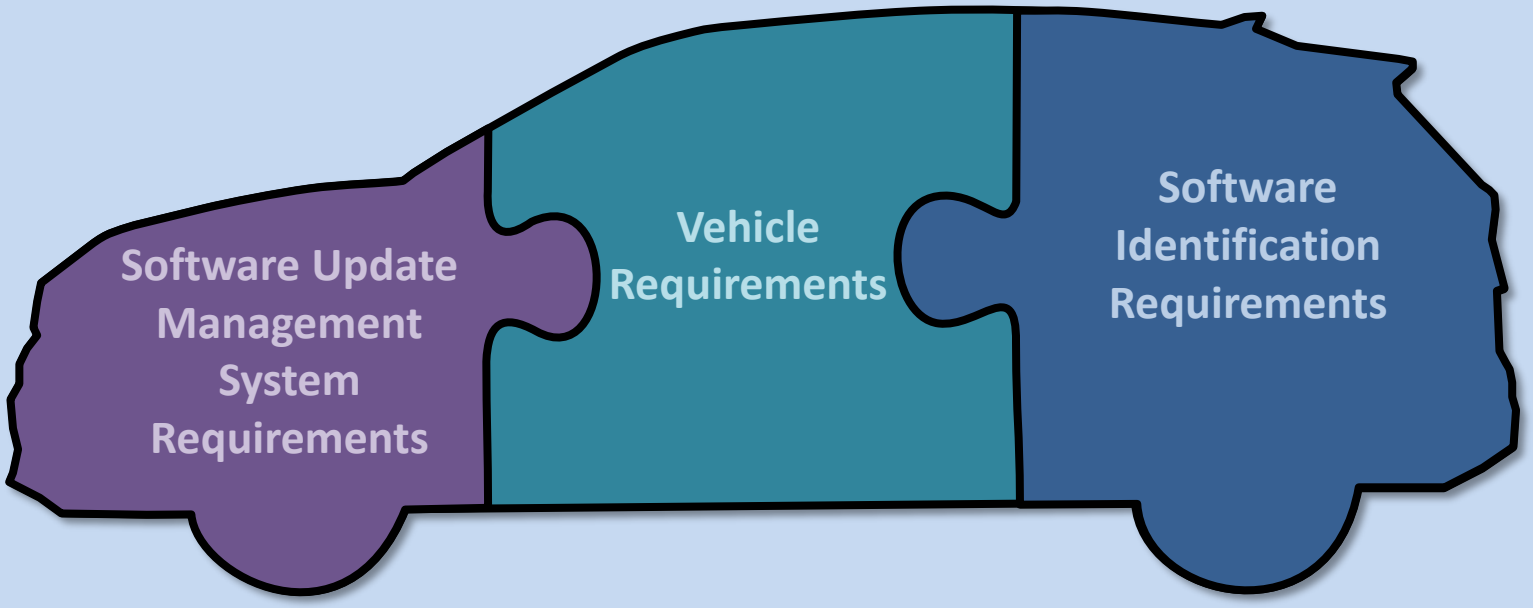
- The remit of the group was to produce
  - a recommendation addressing software update issues
  - develop outputs for use as a regulation or resolution
- How the recommendations were developed
  - The group contained experts from Contracting Parties and NGO‘s (CITA, FIA, ITU, OICA, CLEPA, ISO and others)
  - Thirteen meetings were held to agree the proposed recommendations plus twenty-one ad-hoc meetings
- Work started on 21 December 2016

2. The software update recommendation

Approach for Software Updates

The group developed a split approach:

i) Assessment of relevant vehicle manufacturer management system
ii) Assessment and certification of vehicles
iii) Implementation of a software identification scheme



Structure of the Recommendation on Software Update Processes

Software "update guidance" (chapters 1-6)

- *Guidance on processes and procedures for national administrations to manage post-production software updates, based on processes for "in production" software updates*
- *Guidance on what processes, tests and documentations might be expected in order to manage post-production software updates*

Software update processes Regulatory Proposals (Annex A and Annex B)

- *Requires manufacturers to have a "software update management system" (SUMS)*
  - *Configuration management and quality control processes at manufacturer*
  - *Processes for ensuring updates are executed safely and will not affect the safety or certification of vehicles*
  - *Processes for informing users of updates*
- *Approval of software update mechanisms for vehicles*
  - *Software updates can be delivered safely and securely*
  - *It is possible to identify the status of the software on the vehicle (Annex B)*
  - *Requirements for being allowed to deliver over the air updates*

How to obtain Software Update Process certification

Step 1: Certification of the OEM‘s organization and processes - implementation and assessment of the Software Update Management System (SUMS)

OEM implements a SUMS

- **Organization & processes implemented as per requirements,** requirements include**:** adequate documentation on impact assessments (whether a software update affects existing vehicle systems), evidence recording, processes to ensure security and safety for software updates, compatibility and interdependencies, user information, ...
- Management of software identification numbers (RxSWIN)

Assessment of the OEM‘s SUMS

- **National or Regional Authority assesses the SUMS** of the vehicle manufacturer, whether it is compliant to the requirements

Issuance of a SUMS Certificate of Compliance

- The **SUMS Certificate of Compliance** is the **prerequisite** to obtain a **software update process certification**
- The **SUMS Certificate of Compliance** has a **max. validity of 3 years**
- **National or Regional Authority** may at any time **verify** its **continued validity** and act appropriately if the requirements are no longer met.

How to obtain Software Update Process certification

Step 2: Vehicle certification – electronic architecture and software updates to be in accordance with the SUMS

OEM develops the vehicle architecture

- **Security requirements** defined regarding software update processes implemented on the vehicle
- If a RxSWIN is implemented, requirements for how to protect and access them
- Requirements specific for the safe execution of **over the air updates**
- The **effectiveness** of security measures implemented needs **to be tested and verified**

Assessment of the vehicle

- **National or Regional Authority assesses the vehicle type**, whether it is compliant to the requirements defined in the Regulation

Issuance of certfication

- Requirements are established to ensure conformity of vehicles being produced

Summary of the proposal

- What it does:
  - Considers over-the-air updates and other delivery paths for software updates
  - Provides a common process for how to assess the safety of software updates; their impact on vehicle systems and vehicle parameters; and how to record information about the software updates
  - Provides assurance that the software update mechanism for a given vehicle is safe and secure
  - Provides a method by which the software of a given system can be linked to the legal requirements for that system, this is called the RxSWIN

- What it does not do:
  - Regulates how software updates are provided post-production. A process is recommended for managing this. The proposal contains requirements for supporting the recommended process.
  - Enable verification at road worthiness inspections that the software on a vehicle is what should be there. It does enable relevant information to be available. A separate work stream would be needed to define the technologies and processes needed for such verification.

Questions & Answers

1. Why is certification of software updates not in the proposal?

   Currently software updates that are applied during production or pre-production are covered by existing legislation. So further leglislation is not needed.

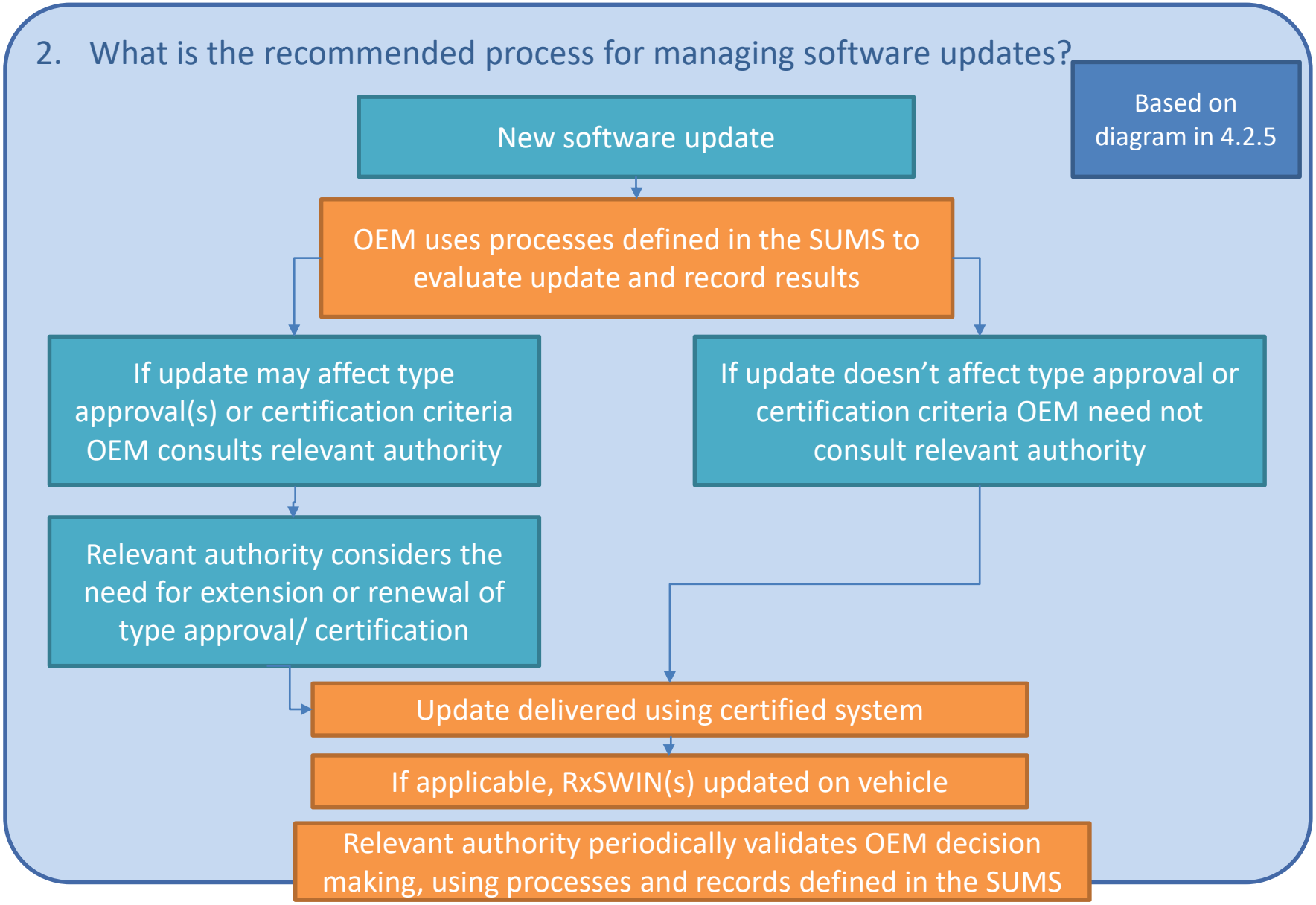
   Software updates that are provided post-production to vehicles in the market may be covered by national/regional legislation.

   Instead chapter 4 of the recommendation provides a recommended procedure for managing post-production software updates. This is based on the procedure for pre-production software updates. It may be adapted depending on national or regional processes/procedures and is therefore only guidance.

   Recommendation:
   The issue, if of interest, will have to be addressed by the national/regional jurisdictions or UNECE may decide to develop a harmonized framework on this topic.

Questions & Answers

2. What is the recommended process for managing software updates?



Questions & Answers

3. How are over the air updates covered?

They are covered both in the SUMS and the vehicle certification requirements

The SUMS requirements ensure:

- There are processes and procedures to assess whether over the air updates will impact safety if conducted during driving (and will not be sent if they do)
- The processes and procedures to ensure that, when an over the air update requires a skilled person (such as a mechanic) in order to complete it, the update can only proceed when such a person is present

The vehicle requirements ensure:

- The vehicle can cope in the event of a failed update
- There is adequate power for updates
- The user can be informed about an update before and after it is executed
- How the vehicle will ensure that, where an update may affect the safe driving of a vehicle, it is executed in a safe manner

Questions & Answers

4. How are non-compliances delt with?

If a vehicle manufacturer fails to maintain their SUMS, or serious deficienes are noted in it the national or regional authority may take appropriate action. This may include withdrawing the certificate.

Without a valid SUMS Certificate of Compliance the manufacturer would no longer able to apply for a new vehicle certification for software update processes. Continued provision of software updates may be affected as may continued production of existing certified vehicles.

3. Overview on the test phase

Next step – testing the proposal

Aim of the „test phase“

=> Provide guidance on how to assess the requirements and documentation required

=> Verify the effectiveness/robustness of the requirements

=> Verify that certification authorities are able to reach the same conclusions based on identical OEM documentation

Aim is to assure the proposal and not to test the products!

Overview

Outputs of the „test phase“

=> Interpretation guideline

=> If necessary, proposals for clarifying the proposal

=> Report of the test phase to cover:

- conclusions on the effectiveness /robustness of the proposal
- verification that certification authorities/ are able to reach the same conclusions

Proposed timeline for the test phase