SOFTWARE UPDATES-TYPE APPROVAL AND SURVEILLANCE MEASURES

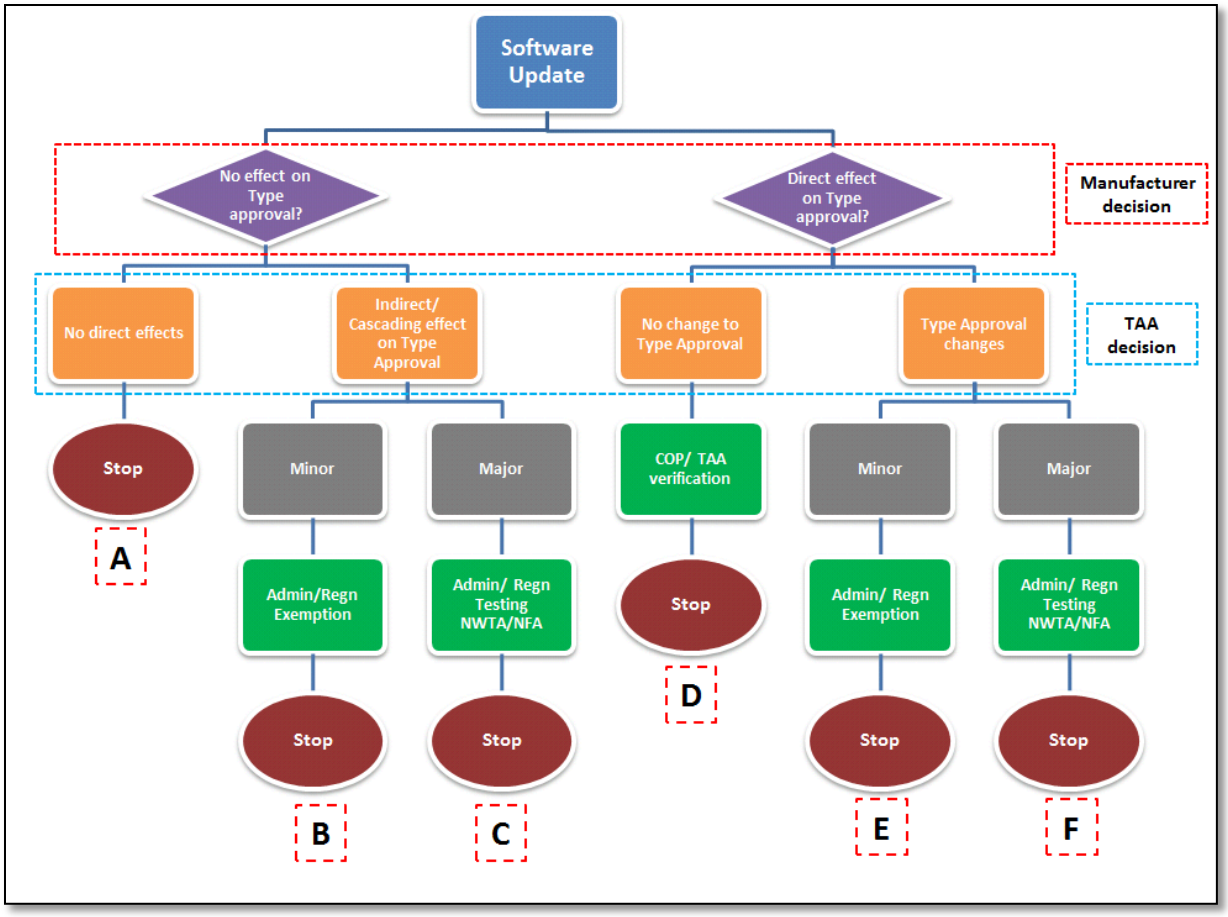
An approval authority perspective to software updates would first require the identification and classification of different types of software updates. As per the inputs from the previous UNECE taskforce meeting, software updates/ changes needs to be considered with reference to changes/deviation observed from existing type approval process. These changes can be identified in **4** levels:

- No change to type approved systems/components
- **No changes to type approved components but which has an indirect effect on the approved systems/components.**
- Type relevant changes but which does not require extensive testing (parameter changes/ bug fixes).
- Type relevant changes that require additional testing and verification requirement (functionality changes/ new vehicle approval).

An initial analysis of existing regulations suggests a definite lack of information available with respect of handling of software updates. A good starting point would be to consider software updates as a retrofit change to existing approval process (as suggested by OICA members in the UNECE taskforce meeting) and provide approval for software changes as an exemption process / verify along with COP process.

However, it needs to be understood that the scope of software updates extends beyond the consideration as retrofit systems. Tracking changes through COP would mean considering software updates as changes to existing type approved systems/components and software changes which indirectly affects the performance of type approved systems/components are considered out of scope (E.g. Software updates extending image rendering quality of LIDAR systems can in turn affect the performance of braking and steering systems, which are covered under EU regulations). The highly coupled nature of automotive subsystems would require software updates/ changes to be considered not as standalone/ retrofit changes but as complete system changes, which requires impact analysis studies on the effect of the changes. Type approval processes for such changes cannot be developed as a one stop solution, but needs to be considered on a case by case scenario where the impact of each software updates needs to be clearly identified and approval for the same to be given on a need basis.

The following approval tree structure can provide a high level view of the steps to be followed when a software update needs to be approved:



**TAA- Type Approval Authority, NWTA/ NFA- New vehicle Type Approval/ New functionality Approval*

Manufacturers should be required to inform the approval authorities on the start of a new software update development process. Depending on the nature of the updates, manufacturers should be required to decide if the new software change results in any deviation from existing type approval conditions and notify the approval authority of the same. Approval authorities should be involved with the manufacturers over the entire phase of software update development lifecycle. Manufacturers should be required to submit relevant documents to the approval authority/ technical services from the requirement analysis phase to the implementation phase. In case of OEMs using third party software /systems from Tier-1/2 suppliers, manufacturers should be required to demand required documents from the corresponding downstream supplier. Manufactures should also be required to ensure that the entire software update process complies with the quality management system requirement for development changes. This process ensures that Type approval authorities/ Technical services are well informed of the nature of the software change and relevant approval/ testing methods are devised.

Software update management process should be dealt by approval authorities in two aspects:

- Approval aspects- Safety, Environment, Security implications with regard to software code and/or parameter changes. Each individual updates to be classified according to one of the above divisions in the approval tree and approval measures to be drafted accordingly. Classifications of the updates to be done by manufacturers in collaboration with approval authority/ technical services. Based on the classification and the nature of software update

(identified from the initial documents supplied by the manufacturer), approval/ testing methods for each individual updates needs to be finalized.

- In- use aspects- This involves acceptance (with/ without user involvement) and registration of updates (in case of successful/ unsuccessful installation) and monitoring mechanism for deviations from type approval. This would also call for the need for inspection of software updates from an individual vehicle perspective (VIN based). A software update information repository/database of vehicles impacted by software updates and corresponding software updates needs to be maintained by approval authorities. The repository should include the following information on software updates for each individual VIN number of registered vehicle:
    - Make and model of the vehicle
    - Update type/ severity (based on information from the approval tree)
    - Affected type approval numbers
    - Hash of the update (or of delta file sent to the vehicle gateway for installation)
    - Affected ECU list
    - Software version
    - Update timestamp information
    - Private Key for signing the update code/ delta file – Code signing mechanism can help ensure the integrity of (approved) software updates.

When an approval is given for a software update, the corresponding update (code/ delta file hash) needs to be signed using a private key, which needs to be verified by each individual vehicle (gateway) using the corresponding public key. This process ensures that only approved versions of software updates are installed in vehicles. It helps to have a unique identifier for each of the approved software update, which can be cross verified for integrity before installing the update as well as during surveillance/ PTI checks.

Manufacturers should be required to obtain the Approval authority signature for all **major** types of software updates, irrespective of whether it has a direct/cascading effect on the Type approval process. In case the software update is a minor change, the approval signature can be granted (if necessary) without undergoing the full range of testing activities. The decision for signing the software update by the Approval authority should be taken based on the nature and type of software update. Market surveillance activities for software updates should include on road vehicle inspection, where approval authorities can verify the signature and hash of the update from the vehicle (stored in the gateway) against the information stored within the approval authority database.

Manufacturers should also be required to maintain an update management repository with access to approval authorities. The update management repository should maintain information on the status of software updates , in terms of number of vehicles affected, confirmation of successful update delivery to each individual vehicles and relevant software update related information. Traceability checks to be done between the two repositories to complete the registration process of software updates with individual vehicles.