**[Draft] Recommendation
of the Task Force on Cyber Security and Over-the-air issues
of UNECE WP.29 IWG ITS/AD
on Software Updates**

1. **Introduction**
	1. **Preamble** *(what an update is, benefits and remit)*
		* + Aim of the paper is to describe/recommend the processes for approving updates post-registration (incl. updates for recalls and over-the-air updates), recommendations on how to perform the updates, and requirements for this
			+ Reference to ToR should be made in this section
			+ The section should note conclusions on national processes, e.g. issue on post registration updates
	2. **Scope** *(particularly noting the OTA would fall into the realm of post-registration updates and that we have considered any software update to a type approved system)*
		* + This section should describe what is considered in the paper. The flow chart used for status reports could be used to help the understand the scope. This is the picture :
			
			+ Note: For approved updates, security of updates will be ensured via Cyber Security recommendation
2. **Definitions**
	* + - Revisit once contents of other sections are finalized
3. **Process on software updates**
4. **Overview**
	* + - Reference to existing process 1958 Agreement

- Describe overall process supported by:

- Chart of process (overview slide)

- Table on software update process (note: it was agreed that there is a need to clarify the term “multi stage” and some of the arrows)

1. **Prerequisites**

This section should describe those identified by the group, namely:

* Internal process to be performed by the OEM (incl. CoP):
* *OEM’s (and their suppliers) have a process whereby they can access, identify and record if a software update will affect existing type approved systems*
* *OEM’s have a process whereby they can identify target vehicles*
* *OEM’s can verify the compatibility of possible software/ hardware configurations in the target vehicle*
* *The vehicle has the ability to record the status of its type approved systems software and parameters, that can be readily checked (=> RxSWIN)*
* It is possible to trace the software versions of the electronic control systems on a vehicle to the RxSWIN of the vehicle and verify that they are correct
* It is possible for the OEM to describe their processes and their veracity to an approval authority (should the need arise)
	+ - * Documentation
* *OEM having documentation evidencing the decisions they have made*
* *The need for OEM to have documentation describing the type approved systems, e.g. hardware, software and system parameters/settings e.g. what functions can be enabled/not enabled. This should be for the system before and after an update*
1. **Type approval process**

The aim of this section will be to describe how the prerequisites might be used and how the expected system would work. This should describe:

* + - * Roles and responsibilities (manufacturer, technical service/approval authority)

*OEM (and their suppliers) being able to evidence decisions to a type approval authority (if required)*

* Information exchange

*The ability for authorities to exchange information electronically with each other and access information from the OEM, should there be a need to do so
Requirements to exchange information to support market surveillance and PTI*

* Market surveillance
*Requirements for authorities to verify decisions made by OEM, this would include conformity of production activities and could include further market surveillance activities*
1. **Additional requirements for software updates (supporting annex for how the vehicle shall ensure the safety of the update process)**
2. **Objectives/Requirements for safely and securely conducting an update**

The aim of this section is to describe the objectives/requirements that the group have agreed are needed, including:- Safety objectives in general for software updates
 *Note: these could be based on German presentation TFCS-08-06
 Note: it was identified that there may need to be a differentiation between download and execution of an update and the requirements placed upon the processes*

- OTA specific requirements *Note: this section will identify any additional requirements for OTA (versus updates performed via more manual means). This will cover when it may be permissible? Examples identified include: Vehicle state, situation, vehicle condition/ prerequisites.*

 *Note: these could be based on German presentation TFCS-08-06*
- The requirement that a system can recover from a failed update

- The requirement that updates are carried out securely (as defined in the other paper)
- The requirement to understand the criticality of an update for recall, safety or security purposes

*Note: this requirement may help understand when an update should be conducted, especially for OTA*

1. **Requirements for evidencing that the update is safe and secure**

­­­­­­­­­­­­­­­­­­This section would describe how the objectives in part a) could be evidenced, this could cover:

* Requiring a description from the OEM of how the update will be performed securely
* Requiring a description from the OEM of how the update will be performed safely (e.g. vehicle stationary with x% charge available etc)
* Requiring a description from the OEM of the interaction/requirements of the vehicle owner/operator (if any) in the update process

This section could also consider or highlight the potential role of type approval authorities in approving the processes described

A. Software identification number and their use (supporting annex for where specific regulation require a part on software updates and help implementation)

1. **Use of the Software Identification Number, RxSWIN**

This section would describe the concept of the RxSWIN, how it could be used, and what its limitations are. This would include:

* The RxSWIN would provide a reference number that can be used to identify the software versions present on the components of a given type approved system.
* What the components are in that system and the exact software versions on each component that the RxSWIN refers to will be held by the OEM (and maybe the type approval body).
* There will be a RxSWIN for each type approved system (that has software in it)
* The RxSWIN will only be updated when there is a change to software on a type approved system that requires an extension or renewal of type approval, otherwise it will be unchanged.
* If a component is common to multiple type approved systems and its software is updated, then the effect on all of those systems will need to be accessed and the RxSWIN for all of them may need to be updated if all their type approvals are affected.
* The RxSWIN will need to be recorded on the vehicle and easily accessible and readable

*Note: the task force may wish to further consider this point and how the RxSWIN may be read.*

* Decisions on whether an extension is needed will first be made by the OEM and then, where appropriate, discussed with the relevant type approval body as per the existing process for extensions.
* CoP will be used to verify that the decisions made by the OEM are appropriate

*Note: this may be covered above in section III, if so then it should not be repeated.*

The chapter could also include recommendations for improving the utility of the RxSWIN, such as:

* The ability of the vehicle (or a third party inspecting the vehicle) to verify to an appropriate party (such as a type approval authority) that a systems software corresponds to that reference by the RxSWIN, for instance by checking its reference numbers.
* The ability of the vehicle (or a third party inspecting the vehicle) to validate to an appropriate party (such as a type approval authority) that a systems software corresponds to that reference by the RxSWIN, for instance by performing a hashing function on the software and comparing it to a value obtained previously (for example when approval was provided).
* The ability of a vehicle to report any changes to system settings or if system software does not correspond to approved versions (e.g. reporting failures of secure boot mechanisms)
1. **Conclusion and Recommendation for further proceedings**
* To ITS/AD
* On general approach (Guideline vs. Regulation, etc.)
* Future developments that could support the process further (such as electronic databases)

**Annex a) an annex for how the vehicle shall ensure the safety of the update process (to be attached to appropriate regulations)**

Contents to be considered for meeting in Tokyo.

**Annex b) an annex for where specific regulation require a part on software updates and help implementation (to be attached to appropriate regulation(s))**

Potentially based on OICA proposal

Note: the task force may wish to consider whether these annexes should be combined.