Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Update to ITS/AD

Covering:

- SOFTWARE UPDATE PAPER
  - Outline of process envisaged
  - Proposed structure
  - Progress made
  - Specific questions
  - Points of note

- CYBER SECURITY PAPER
  - Outline of process envisaged
  - Proposed structure
  - Progress made
  - Specific questions
  - Points of note

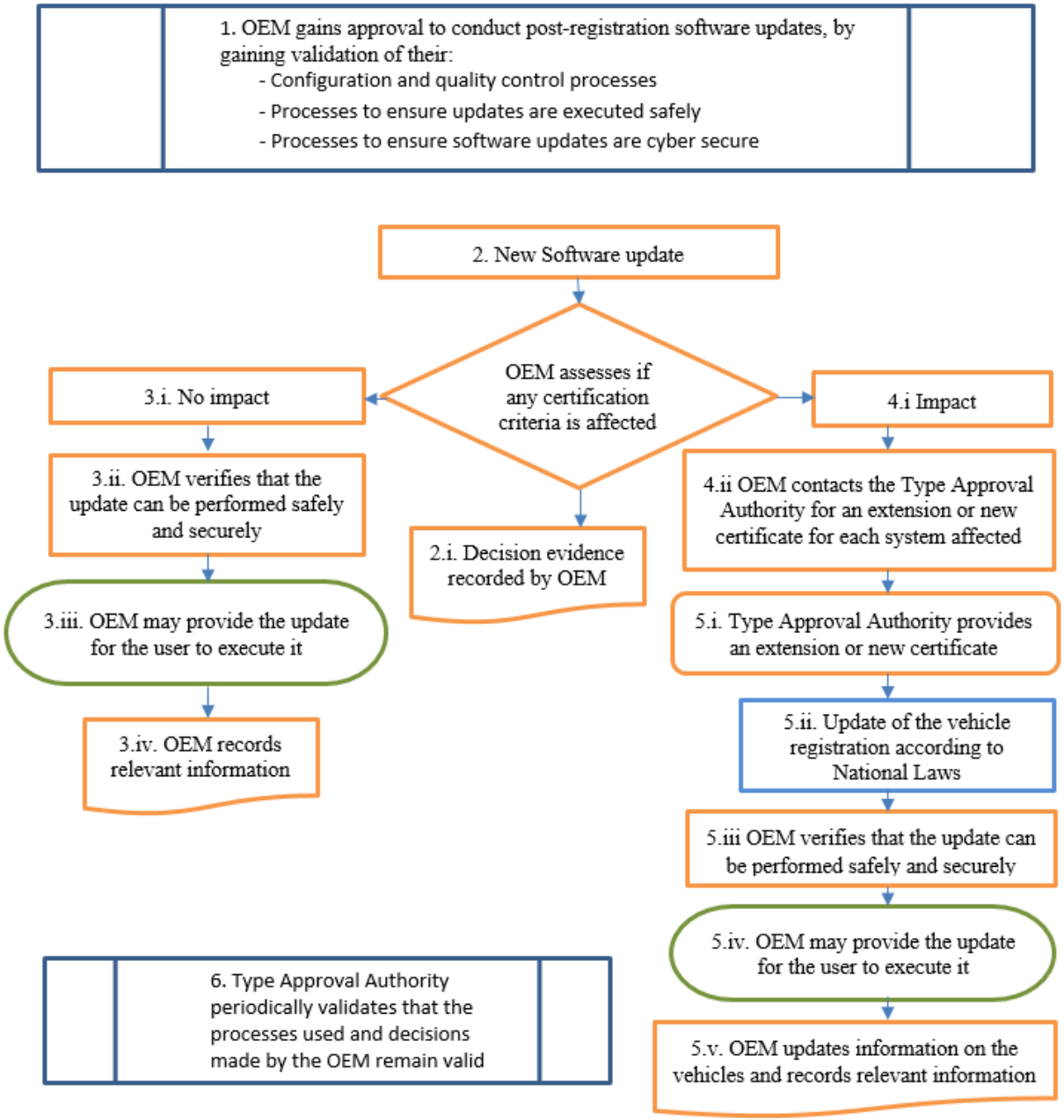
Outcome TFCS-11// 20-22 February 2018 @ Washington DC

SOFTWARE UPDATE PAPER - overview

- The recommendation for software updates is that **all updates should be treated the same**, but with some extra considerations for over-the-air updates

- To regulate such updates the following processes would be needed:
  - An **initial verification** that an OEM has suitable procedures for delivering software updates
  - **Individual software updates are assessed** by OEM's, with type approval authorities being notified if an update may affect any type approved system or change any entry within the information package for the vehicle
  - **Type approval authorities periodically verify** that **OEM's** continue to apply the **processes and procedures** correctly and verify that they are appropriately notifying authorities of software updates as defined within this recommendation

Outcome TFCS-11// 20-22 February 2018 @ Washington DC



Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Overview of software update paper

- **Recommendations** on how to take the paper forward:
  - The main text, providing guidance of the process and procedures, to be taken forward as a resolution providing guidance on the regulations
  - **Annex A to be a horizontal regulation**, providing for **approval of an OEM's processes** to manage software updates
  - **Annex B to be a regulation covering software updates that will affect type approval**, to be appended to relevant existing regulations where the software has an influence on the vehicle functionality, to introduce the concept of software identification numbers into relevant UN regulations.
- Is this acceptable?

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Progress report

- The software update paper was reviewed at the meeting, progress was:
  - Chapters complete but open to further comment are:
    - Chapter 1 – introduction
    - Chapter 3 – document structure
    - Chapter 4 - process for software updates
    - Chapter 6 – identification of installed software
  - Chapters with comments are:
    - Chapter 5 – safety and security requirements
    - Chapter 7 - recommendations
    - Annex B – regulation introducing RxSWIN
  - Chapters with major work remaining are:
    - Chapter 2 – definitions
    - Annex A – horizontal regulation

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

- Questions for ITS/AD regarding the software update paper:
    - **Are you content with the overall structure** proposed?
        - Are you content with the proposal for a horizontal regulation covering OEM processes as described in Annex A?
        - Are you content with the regulations as proposed?
    - **Production definitely discontinued**

How to should the task force provide extensions of types (via software updates) where the production is definitely discontinued? Example: a vehicle type is no longer in production (it is discontinued) but an OEM continues to offer software support. A software update is produced that requires an extension of type approval. An approval authority grants this extension, how should it be communicated?

Proposal is to add a category to the communication annex fo "APPROVAL EXTENDED AFTER PRODUCTION DEFINITELY DISCONTINUED "

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

- Questions for ITS/AD regarding the software update paper:
    - The recommendation envisages continued periodic assessment of the processes, practices and decision making of OEM's in relation to software updates. This could be considered to be market surveillance. As market surveillance is not within the 1958 agreement the UNECE will need to consider how this could be conducted under its agreements.
      What does ITS/AD recommend?

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

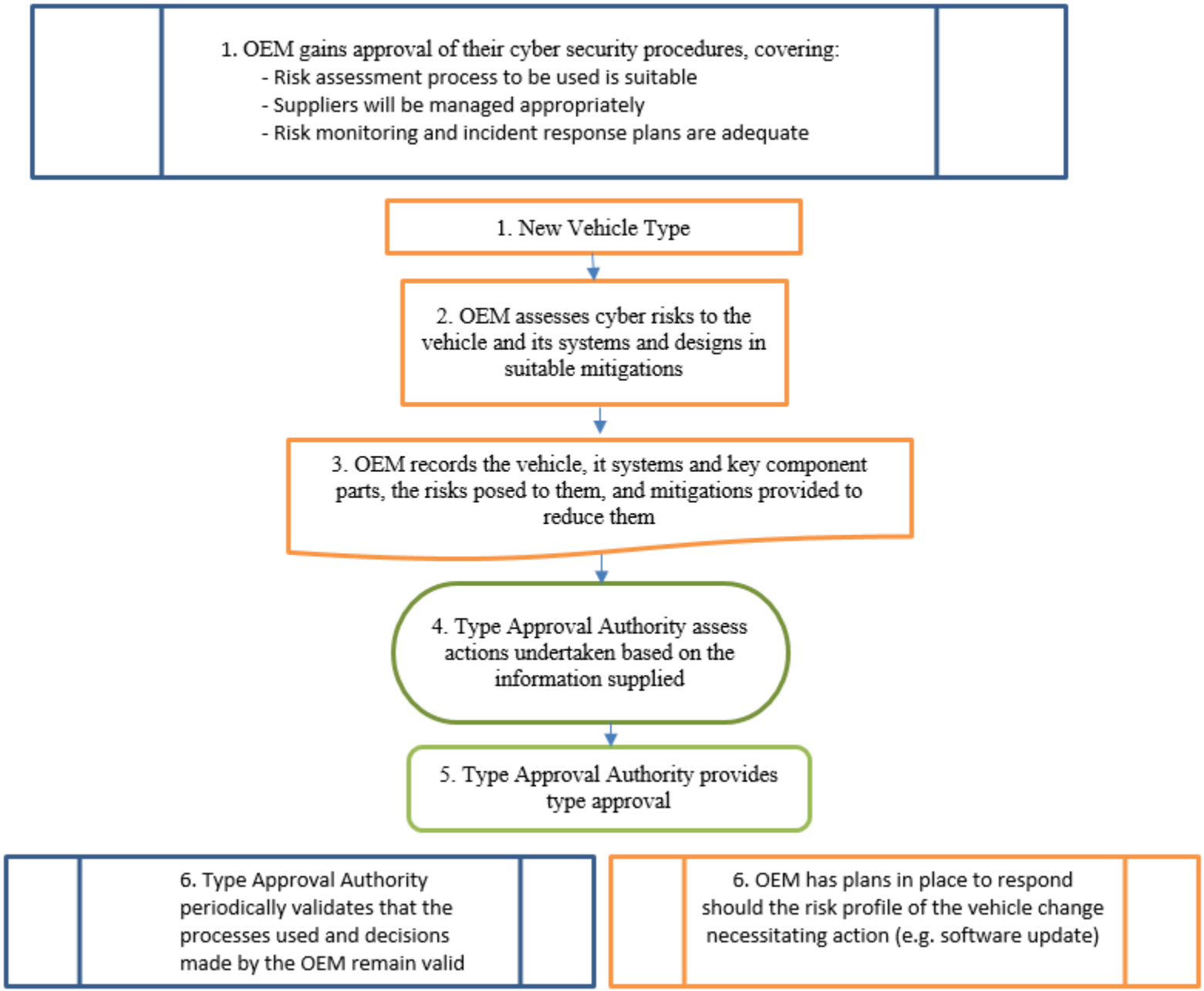
For note:

- There are a number of supporting processes that signatory parties and the UNECE will need to address to enable the full implementation of this recommendation, these include:
  - It is will be important for UNECE to invest in the development of **DETA** and DoC
  - It should be investigated if **PTI** should be provided limited access to DETA and DoC in order for the RxSWIN numbers to be verified during PTI
  - There should be procedures in place to enable the **sharing of information** between national bodies to support the administration of these processes.
  - Whether a software change requires an extension or renewal of a systems certification depends on the description in the specific regulation (e.g. in the vehicle type definition). Therefore it may be necessary for the specific regulations to be reviewed to incorporate software and if there should be any specific requirements relating to them.

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

CYBER SECURITY PAPER – what it contains:

- To regulate cyber security the following processes are recommended:
  - **An initial verification by a type approval authority** of the cyber security management system (**processes and procedures) of an OEM**. This would provide them a certificate of compliance covering:
    - That an OEM is organisationally set up to manage the process
    - That an OEM has processes in place to conduct an appropriate risk assessment and processes to manage risks relating to their suppliers
    - That the outcome of the risk assessment will influence the vehicle design
    - That there is a process to monitor how risks will evolve post production and the OEM has response plans in place should action be needed to respond to a cyber threat
  - **A vehicle type approval** is provided, after an assessment by an authority, **of the cyber security mitigations provided within a vehicle type** against the cyber risk assessment of that vehicle type.


1. OEM gains approval of their cyber security procedures, covering:
- Risk assessment process to be used is suitable
- Suppliers will be managed appropriately
- Risk monitoring and incident response plans are adequate
1. New Vehicle Type
2. OEM assesses cyber risks to the vehicle and its systems and designs in suitable mitigations
3. OEM records the vehicle, it systems and key component parts, the risks posed to them, and mitigations provided to reduce them
4. Type Approval Authority assess actions undertaken based on the information supplied
5. Type Approval Authority provides type approval
6. Type Approval Authority periodically validates that the processes used and decisions made by the OEM remain valid
6. OEM has plans in place to respond should the risk profile of the vehicle change necessitating action (e.g. software update)

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

What the paper looks like:

- It is recommended that the output of the task force be taken forward as two parts:
  - The main text, providing guidance of the process and procedures for cyber security, should be taken forward as a resolution
  - An annex should be taken forward as a **horizontal regulation**, providing approval of the processes an OEM has to provide approval of the cyber security of a vehicle type, this will include:
    - Approval that the OEM has identified and assessed the cyber risks to a vehicle and applied appropriate mitigations
    - Approval that the OEM has suitable processes to support the vehicle post production should the need arise.
- Key points:
  - The **regulation** would be **based on a subjective assessment**
  - Parts of the resolution (annexes describing possible threats and mitigation) can provide objective items to aid the assessment but are not currently suitable for the basis of an objective assessment.

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Progress report

- Chapters complete but open to comment are:
  - Chapter 5 – threats to the vehicle
  - Annex D – references
- Chapters with comments are:
  - Chapter 1 – introduction
  - Chapter 2 – definitions
  - Chapter 4 – cyber security principles
  - Chapter 6 – mitigations
  - Chapter 7 – evidencing
  - Annex A – threats detailed
  - Annex B – mitigations detailed
  - Annex E – cyber security regulation
- Chapters with major work remaining are:
  - Chapter 8 - recommendations

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Question on vehicle „lifetime“, continued

Guidance is needed on how to draft requirements for manufacturers to support the cyber security of vehicles post production. Particularly if any text on lifetime, or what a suitable length of time for a vehicle to be support is, should be included.

Current draft text (not finalised):
The OEM shall have a security update policy defining how they will support a vehicle post production.

Possible additional text:
Requirements that shall apply to the security update policy of vehicles include:

1. **The OEM shall provide updates of the software on a vehicle for critical elements *[over a reasonable timespan]*.***
2. **The end-user should be informed if the support for a vehicle or a vehicle component and/or the support for software updates comes to an end.**
3. **The OEM should identify how the end-user would be informed about the termination of support for their vehicle**
4. **The OEM should identify what actions may be taken to protect systems or vehicles in the event that they become unsafe due to cyber threats after the OEM has ceased providing support for those vehicles or systems. For example: Functions that were not required for the vehicle at the time of its homologation may be deactivated.**

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

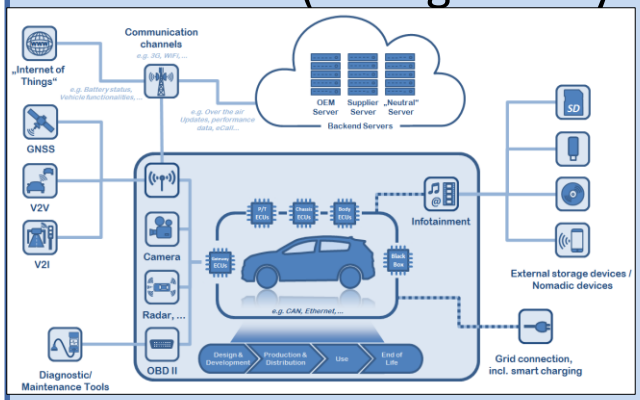
Question on vehicle „lifetime“

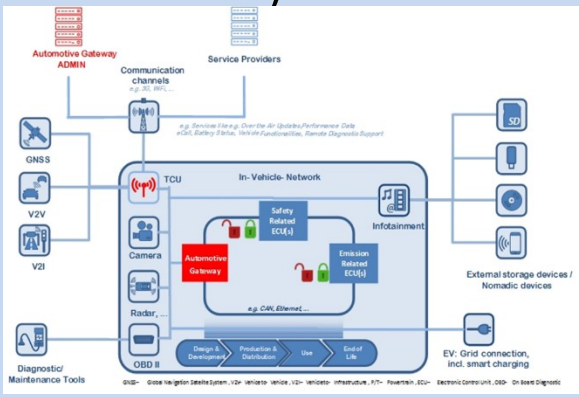
- How should the task force approach requirements for maintaining the safety and security of vehicles in service, particularly relating to the provision of software updates? **Options** identified include:
  1. *Do not include any text relating to lifetime.*
     The likely outcome is that OEM's may stop providing active support at some stage but would still be subject to recall legislation and requirements
  2. *Include text defining, in UN regulations, a timespan that vehicles should be supported for by an OEM e.g. 10, 15, 20 or 50 years etc*
     This would put a defined period for OEM's to guarantee support, after which vehicles may still be subject to recall legislation and requirements
  2. *Include text in UN regulations requiring that vehicles should be supported for by an OEM for a reasonable timespan but not define what that should be*
     The likely outcome is that OEM's may stop providing active support at some stage but would still be subject to recall legislation and requirements. Additionally national regulation may define the period
- **Problems identified**:
  - This may be a political decision and not appropriate for the task force
  - Issues and viability of providing support indefinitely by the OEM and suppliers
  - Current practices of recalls and that they may apply to vehicles of any age
  - Other legislation may apply in this area, which will vary by signatory state

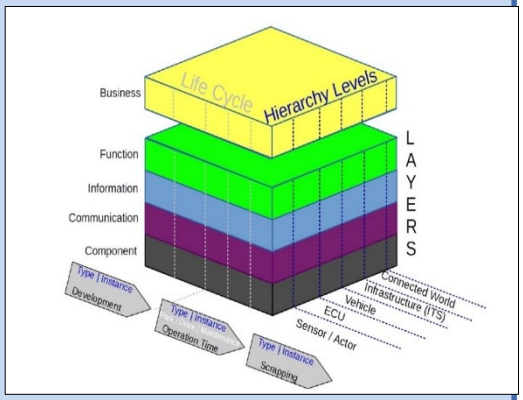
Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Points for ITS/AD regarding cyber security:

- The development of the cyber security paper used different „**reference models**“ to describe what the vehicle ecosystem looks like. Later a further model was proposed describing what a functionally cyber secure might look like (not agreed by the task force).







Current proposal is not to include them in the final document as they may add too much complexity and add little to the requirements. Is this ok?

- For the cyber security regulation *what is the correct terminology* for the use of contracting party, approval authority and competent authority?

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Action items for next session (TFCS 12):

- Incorporate feedback from ITS/AD
- Aim is to conclude paper on software updates
- Aim is to conclude paper on cyber security
- Use of ad hoc webex meetings to progress parts of the document needing work or further review beforehand
- Risks identified:
  - discussions on lifetime not being concluded satisfactorally
  - agreement on text of regulatory annexes not agreed by the end of TFCS 12

Outcome TFCS-11// 20-22 February 2018 @ Washington DC

Future meetings planned

- Software annex A
  - Ad hoc webex meeting to confirm scope and contents (19th March)
  - Ad-hoc editting team to refine text ahead of TFCS 12
- Ad hoc webex meeting to define definitions (21st March)
- Ad hoc webex meeting to review cyber security annexes A & B on threats and mitigations (26th March)
- Ad hoc webex to review comments remaining on cyber security paper (4th April)
- Ad-hoc editting team to revise chapter 8 of cyber security paper ahead of TFCS 12
- TFCS 12 to be held 17-19 April 2018 in Seoul, South Korea