Submitted by the Secretary
of the TF on CS and OTA issues

Working Paper **TFCS-05-02e**
5th TFCS, 10-11 May 2017
Agenda item 2

Draft Minutes of the fourth session of the UN Task Force on Cyber Security and OTA issues

13 March 2017, 10:00 - 17:00 – Cyber Security
14 March 2017, 09:00 - 16:00 – Software updates and Cyber Security

at ITU / Geneva

I. Adoption of the Agenda

The Task Force may wish to adopt the provisional agenda.

Documentation: TFCS-04-01e Agenda

The ITU-T SG 17 vice-chair (Mr. Nakao-san) expressed the interest of ITU-T SG 17 for collaboration. The topic was added to the agenda (see item III below). Otherwise, the agenda was adopted without changes.

II. Adoption of minutes and report from third session

The chair will report the outcomes of the second session. The Task Force will be asked to adopt the minutes from the previous two meetings

Documentation: TFCS-04-02e Minutes of 3rd Session
TFCS-04-02e-Rev1 Minutes of 3rd Session

The secretary of the group reported that a new version of the minutes had been reproduced as revision 1 to the original document, since a reference of a document had to be corrected. The revised version had been adopted by the group without further changes.

III. Collaboration with ITU-T SG17 on security issues

Documentation: TFCS-04-10e (ITU) ITU-T Study Group17
TFCS-04-11e (ITU) Request for input

Mr. Nakao-san, vice-chair of ITU-T SG17, gave a presentation with an overview of activities of ITU-T regarding cyber security (see TFCS-04-10). It was reported, how SG17 is developing security standards (six steps: high-level requirement, reference model, threat analysis, risk assessment, security requirements and security control) and monitoring activities (darknet / honey pot monitoring). In addition, Mr. Nakao-san reported on the activities for a recommendation (X.1373/X.itssec-1) on security update capability and on V2X communication (X.itssec-2)
Furthermore, ITU-T SG17 forwarded a request for input (Liaison Statement, see TFCS-04-11) to TF-CS/OTA. The intention is to have a closer collaboration in the field of security aspects between ITU-T

and UNECE TF-CS/OTA.

Conclusion:

- The group agreed to exchange with ITU-T SG17 on activities and approaches related to cyber security aspects, e.g. threat analysis, ...
- Co-chair (Mr. Darren Handley) to provide the latest version of the table of threats to ITU-T SG17 by 21 March 2017 for consideration and comments

IV. Cyber Security

A. Terms & Definitions

The group was updated by OICA and the Co-Chair (UK) that ISO/SAE is still working on a set of terms and definitions regarding cyber security. While an initial list of definitions is provided by ISO/SAE (not available for TFCS-04), the work is not finalized yet.

Conclusion:

- Review list of terms and definitions from ISO/SAE when available
- FIA to provide definition for legal/authorized/unauthorized access

B. Threat analysis

Documentation: TFCS-04-03e-Rev1 (Chair) Table on CS threats_post TFCS-ahT call
TFCS-04-03e-Rev3 (Sec) Table on CS threats_amended during TFCS-04

i) Table of threats

As basis for the threat analysis and identification of mitigation measures the table of threats was further developed. The group worked on condensing the table of threats without losing content, as well as improving the categorization of threats and identifying duplications and outcomes listed as threats. During the meeting it was seen beneficial to add columns in order to identify, if the threat identified is an attack or vulnerability, as well as identifying the type of entry (cyber, cyber (personnel), non-cyber or data). Furthermore, Daimler explained an alternative approach, based on a three dimensional table covering the connection type (mobile phone, Bluetooth, etc.), seven attack categories (same for all connection types), way to conduct an attack, point of contact (assets affected) and effects. The group agreed to add the attack categories as subcategories of relevant categories of threats.

The delegate from the Netherlands proposed to consider also the STRIDE model (=> **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of Service, **E**levation of privilege) for the classification of threats.

The changes to the table of threats, as amended during TFCS-04, are reproduced in document TFCS-04-03e-Rev3.

In order to finalize the table of threats the group confirmed to hold an additional web meeting dedicated to this topic in April. Furthermore, the co-chair (UK) volunteered to prepare a cleaned up version of the

table, which should also be forwarded as information to ITU-T SG17.

Related to software updates security questions arose. The co-chair (UK) asked, whether "hashing" is done for vehicle software. The expert form the Netherlands mentioned that hashing itself would not be sufficient. There would be a need to encrypt public key in the car for verification. OICA explained that hashing is not yet done. One problem would be for example that different keys would be required due to different authorities. Furthermore, the opinion was stated, that a standardized security system may be more easily broken and having then an enormous effect on the vehicle population. The Netherlands argued that it would be only an issue of an electronic signature which is unlikely to be broken. Further reference was made to the gateway. OICA stated that the gateway does not include the vehicle internal communication.

Conclusion:

- Co-chair (Mr. Darren Handley) to prepare a cleaned up version of TFCS-04-03e-Rev3 and forward the document to ITU-T SG17 (Mr. Nakao-san) for consideration until March 21, 2017
  Note (Sec): the cleaned up version of the table of threats is available as TFCS-ahT2-02
- Additional web meeting CS/OTA ad hoc "Threats 2" to be scheduled in April
  Note (Sec): The meeting is scheduled for April 21, 2017, 1pm -3pm CEST

ii) Reference Model

OICA pointed out, that a reference model would be beneficial for further considerations, in order to identify and classify the related threats to be further assessed by the group. Based on a proposal from the co-chair (UK) the group developed the following reference model:

The reference model shall be:
- the vehicle including:
- *its hardware*
- *its software*
- *data held on the vehicle*
- *its internal communications*
- *its interfaces with external communication systems/functions (e.g. V2X and emergency comms) and devices (e.g. USB, CD etc)*
- *vehicle functions/systems that use wireless communications (e.g. TPMS, keyless entry)*

- support servers which directly communicate with the vehicle
- diagnostic / maintenance systems

Submitted by the Secretary
of the TF on CS and OTA issues

Working Paper **TFCS-05-02e**
5th TFCS, 10-11 May 2017
Agenda item 2

VI. OTA issues (Software updates)

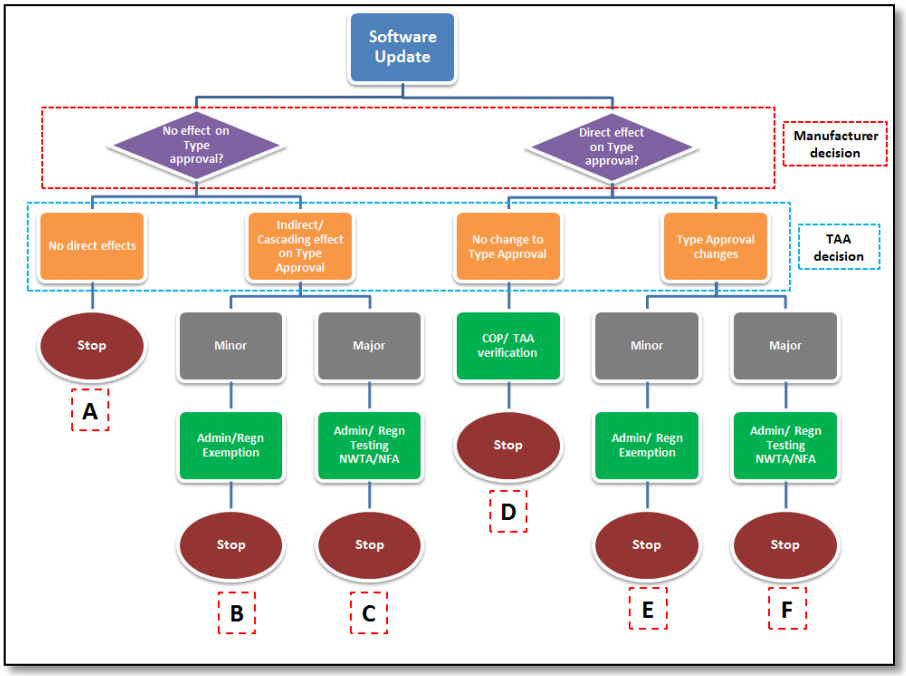
Documentation: TFCS-04-04e (EC) Commission study on vehicle certification
TFCS-04-06e-Rev1 (JPN) software update issues
TFCS-04-12e (NL) Type Approval of Software updates

A) Process for software updates

Japan presented document TFCS-04-06e-Rev1 on software updates, in which they also assessed input by the European Commission (Study on the assessment and certification of automated vehicles – Final Report – by TRL). In this report the idea of recall related updates for already registered vehicles is introduced. Three cases are considered: recall updates, non-recall operation updates and performance improvements updates or security risk corrective action updates. In addition, a process flow of recall updates is provided, while a process flow on non-recall operation updates was not described. Japan suggested to identify possible software update cases (post registration), to identify functions to be updated, develop a process flow for each software update case and finally draft a recommendation. Furthermore, Japan tried to match the principles for software updates defined during TFCS-03 with the suggested cases in the TRL report. In the view of Japan, recall related updates shall be administrated in the same way as today (existing recall scheme). For non-recall related updates of critical functions (e.g. involving the steering system, braking, etc.) authorities should be appropriately involved.

OICA stated, that a flow diagram for the various software update cases would be important. Furthermore, OICA mentioned, that most recalls are not type relevant, therefore a direct link between the task force approach (3 cases) with the TRL approach is not possible. It was also stated, that in general there is no difference between a recall for hardware and software.

The Netherlands presented document TFCS-04-12e, focusing mainly on a proposal for a flow diagram for software updates:



OICA pointed out, that the scheme is not specific to software, but valid for every update (=> scheme of change management). The manufacturer analyses the impact and collaborates with the Technical Services accordingly. The software is part of the vehicle information documentation. However, it was agreed, that the software may have to be better reflected in the future.
The representatives of the Netherlands mentioned that changes to software can have an indirect impact on vehicle systems/functions, for example improvements to sensor software impacting automated driving functions. Furthermore, requirements for software are still under development.
OICA view on the flow scheme above was that the cases A, E and F would match with the cases defined during TFCS-03. The Netherlands mentioned that there might be indirect/cascading effects, which need to be considered. The co-chair and OICA furthermore noted that the boarders between "OEM's decision and Type Approval Authority decision" are not that clear. Therefore, OICA noted that the scheme might be too complex. If an OEM analyses the software change and concludes, that Type Approval is not affected, Technical Services/Type Approval Authorities are not involved. This is also part of the Conformity of Production scheme. As a basis the characteristics of functions are used. The Netherlands agreed, however in future software updates may also be increasingly related to security. OICA stated that this element will be part of the threat analysis and final recommendation, e.g. establishing a new regulation on software approvals. FIA raised the question, whether outdated security principles will be addressed. OICA commented that this will be depending on the software security requirements to be defined. Germany addressed the point that some updates may affect the Type Approval and registration, even though not identified as non-type relevant. FIA gave the example of higher power via software change. OICA commented that these cases are covered by the scheme from the Netherlands: adding a new function => (F), changing the limits (E). The Netherlands mentioned, that this is only the case if there are some existing requirements defined for the new function. In case there are no requirements defined, the vehicle manufacturer would not need type approval for that additional function.
OICA pointed out, that the group should look at technical issues/processes for software updates. In this regard the practicalities for performing software updates shall be considered, including the roles and responsibilities of stakeholders involved.

Conclusions

- The group agreed to look at the practicalities of post registration software updates, incl. responsibilities of stakeholders.
- The group confirmed considering pre- and post-registration software update issues
- The group agreed to review the document from NL on the type approval on software updates (TFCS-04-12)
- NL/JPN/OICA agreed to develop common proposal for the flow diagram of the type approval of software updates
  Note (Sec.): the proposal is available on the website as document TFCS-05-03

B) Verification of software status/Configuration control

The representative of CITA pointed out, that there is a need for documenting software updates for the purpose of checking. The representative from the Netherlands explained that such software version history is available at the OEM during COP audits and shall be checked accordingly. OICA agreed to this approach, commenting that the tracing of software versions is related to COP. A tracing of all software changes for each vehicle (VIN) for the purpose of external checking (e.g. for PTI) would be a big administrative burden. Furthermore, cases like manipulation of software are to be seen in the context of software security (=> threat analysis).
The co-chair (UK) expressed the need for configuration control for verification in the field. Therefore, the group should look at today's status and the relation to the proposal from the Netherlands (TFCS-04-12e). OICA stated two cases of software updates: manipulation by owner or cyber-attacks. The co-chair added the case of dealer/supplier updates. ITU agreed to the chairs comment, since updates are often conducted at dealerships before a new vehicle is handed over to the customer.
OICA suggested it would be beneficial to get some more time to reflect on the paper from the Netherlands. Furthermore, OICA agreed to the necessity to be able to check the software validity (=> transparent process)

Conclusions

- Further consideration shall be given to the in-field verification of the software status (configuration control)
- OICA to provide input on configuration control

VII. Action items for next session

A) Cyber Security
   - Finalize table of threats
   - Consider next steps (mitigations)
   - FIA to provide definition for legal/authorized/unauthorized access

B) Software updates
   - Review document from NL on the type approval on software updates (TFCS-04-12)
   - OICA to provide input on configuration control
   - NL/JPN/OICA to develop common proposal for flow diagram on the type approval of software updates

VIII. Next meetings

The group agreed to the following meeting schedule:

TFCS ad hoc „Threats-2“	21 April 2017*	Webex	1pm – 3pm CEST
TFCS-05	10-11 May 2017	Paris @ OICA	
TFCS-06	13-14 June 2017	Washington area (Arlington, VA) @ TIA	
TFCS-07	30-31 Aug. or Sept. ‘17	Europe (NL/UK ?)	
TFCS-08	11-12 Oct. 2017 (tbc)	Tokyo	

** Note Sec.: confirmed after the meeting, invitation already distributed*