Submitted by the Secretary
of TF-CS/OTA

Working Paper **TFCS-04-02**
4th TFCS, 13-14 March 2017
Agenda item 1

Minutes of the third session of

the UN Task Force on Cyber Security and OTA issues

Day one – Cyber Security and Privacy

16 February 2017, 10:00-17:00 (Central European Time)

4 Rue de Berri, Paris

I. Adoption of the Agenda

The Task Force may wish to adopt the provisional agenda.

Documentation: TFCS-03-01e-Rev1e Agenda

The agenda was adopted without changes.

II. Adoption of minutes and report from second 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-03-02e minutes of 1st session
TFCS-03-02-Rev1e (Sec) minutes TFCS-01
TFCS-03-03e Minutes of 2nd meeting
TFCS-03-03-Rev1e (Sec) minutes TFCS-02

The minutes of the 1st meeting (TFCS-03-02e) had been modified to incorporate a written comment received from Sweden in order to clarify, that the group decided not to deal with functional/system safety in general. The following wording was added in the minutes under agenda item IV: *However, it was decided by the group not to extend the scope of TF-CS/OTA to functional/system safety in general.* The amendment was adopted and is reproduced in document TFCS-03-02-Rev1e. (In document TFCS-03-02-Rev1e the word "draft" was deleted in the headline, since the minutes were adopted.)
The minutes of the 2nd session (Webex meeting on Terms of Reference) were adopted without changes. (In document TFCS-03-03-Rev1e the word "draft" was deleted in the headline, since the minutes were adopted.)

III. Review of actions

The Task Force will review actions from previous meetings

Documentation: TFCS-03-02e Minutes of 1st meeting
TFCS-03-03e Minutes of 2nd meeting

The action items identified in the first and second session of the TF-CS/OTA had been reviewed. They are addressed in the agenda items below.

IV. Review of the draft Terms of Reference for the group

The Task Force may wish to review the groups Terms of Reference for the group. When the ToR would be agreed by the TF, they will be endorsed by the IWG on ITS/AD and adopted by WP.29

Documentation: TFCS-03-04e Updated Terms of Reference

The Terms of Reference as modified during TFCS-02 had been adopted without objections. The group furthermore confirmed the proposal from Japan to co-chair the TF-CS/OTA. Mr. Tetsuya NIIKUNI (NTSEL/Japan) will chair the group together with Mr. Darren HANDLEY (DfT/UK).
The delegate from the Netherlands noted, that the Terms of Reference developed by the group better reflect the workscope of TF-CS/OTA, compared to the guideline on cyber security (WP.29/2017/46). Therefore, the ToR should be referenced if necessary.

Cyber Security

V.List of definitions

The Task Force may wish to agree a list of common terms and definitions based upon the supplied paper(s)

Documentation: TFCS-03-05e Initial proposals for terms and definitions

The aim is to agree on a common list of terms and definitions, used by the group.
During the 1st session it was agreed to review terms and definitions provided by ISO/SAE. Unfortunately, those definitions had not been provided for the 3rd session. OICA/CLEPA expects that ISO/SAE may be able to provide such information until the week before the 4th session of TF-CS/OTA in March.
In addition, UK provided a list of terms and definitions in document TFCS-03-05e. It was furthermore noted, that some definitions are given in the guidance document WP.29/2017/46 which are different to the ones defined in the UK paper.

Conclusions:

- The group agreed to review the terms and definitions during TFCS-04
- ISO/SAE is expected to provide information in time before TFCS-04
- The group shall use as much as possible existing definitions, prioritizing definitions already established within the UNECE, and focus on definitions needed for the work of TF-CS/OTA

VI. List of key cyber risks and threats

The Task Force may wish to agree a list of key cyber risks and threats that they consider to be realistic and plausible

Documentation: TFCS-03-06e (UK) Initial proposals for possible cyber risks and threat

TFCS-03-09e ENISA Cyber Security and Resilience of smart cars
TFCS-03-11e (China) proposals for Cybersecurity
TFCS-03-14e (NL) IPA Japan Approaches for Vehicle Information Security

The group extensively discussed the way on how to deal with the issue of cyber security risks and threats, including various approaches for the analyzing and categorization.
It was identified, that the proposal from UK (TFCS-03-06) is based on use cases, while the ENISA report is based on the assessment of sources for threats, which allows a more generic approach for analyzing the threats. Even the establishment of a multi-dimensional (2D or 3D) matrix was considered. The delegate from the Netherland stated in addition, that it could be beneficial to look at the Japanese IPA document “Approaches for Vehicle Information Security”. (Note by Secretary: the document was made available after the meeting and is registered as TFCS-03-14 (NL) IPA Japan Approaches for Vehicle Information Security.)
France proposed to start with the ENISA report and mentioned to prepare further input for the next session. OICA showed a document, trying to combine the UK proposal (TFCS-03-06) and the threats identified in the ENISA report (TFCS-03-09), identifying some difficulties due to the different approaches. It was furthermore recognized, that the document from the UK also includes results/consequences. ITU pointed out, that it would be beneficial to categorize the threats/delivery mechanism. FIA raised the issue of the vehicle life cycle, which should be considered. In addition, FIA raised the issue of range extension of remote keys, which should also be addressed. The chair (UK) mentioned, that this is not related to the threats, but to mitigation issues. It was agreed that OICA should develop a table for the threat analysis, incorporating the threat/source, cause (affected/impacted assets) and effect (outcome/results of threat impact and what to be protected). This table and its content shall be reviewed in a dedicated ad hoc web meeting on 8 March 2017. The target is to finalize the document on the threats during the TFCS-04 meeting in Geneva (13-14 March 2017).

Furthermore it was decided to include all threat related issues (also for data protection and OTA/software updates) in one common approach/document.

Conclusions:

- Analysis shall be based on threat/source
- Threat analysis for all aspects (cyber security in general, data protection and software updates – incl. OTA updates) to be considered in one common approach/ document
- OICA to draft a table based on the discussion and agreement during the meeting, covering threats, affected assets, impacted areas results of the threat/impact and what to protect.
- It was recognized that this approach will not be exhaustive, but should aim to cover most eventualities.
- Dedicated web meeting on 8 March 2017, 10:00 am – 12:00 pm CET
- Target to finalize document on threats during TFCS-04 meeting

VII. List of objectives/principles/actions that could mitigate the key risks identified

The Task Force may wish to agree a list of objectives/principles or actions that if achieved or carried out could mitigate, in part or combined, the key risks and threats previously identified

Documentation: TFCS-03-07e DfT Cyber Security Principles
TFCS-03-08e NHTSA Cybersecurity Best Practices for Modern Vehicles
TFCS-03-09e ENISA Cyber Security and Resilience of smart cars

The group discussed the different approaches on dealing with the mitigation principles.
The group decided to follow a stepwise approach. It will consider threats first and then actions (principles) needed to mitigate them. The group will then formulate the outcome into a paper for its parent group.
A general discussion regarding the approach on mitigation principles took place, based on the cyber security principles from the DfT/UK (TFCS-03-07). It was noted that the work should also be based on the general requirements in the guideline (WP.29/2017/46), with the work looking to expand on that guidance. Other potential sources that could be used were mentioned. France and OICA mentioned that cyber security issues may be dealt with in a similar way as radio frequency issues in the frame of Electro Magnetic Compatibility (ref. UN Regulation No. 10). The delegates from the Netherland proposed in addition, that it might be worthwhile to look at some other industry sectors (e.g. CSPN Certification/ANSSI). Further discussion will take place once the list of threats is finalized.

Conclusions:

- Work on details regarding mitigation principles after threat/risk analysis is completed
- Members were invited to share relevant documents, especially those mentioned by delegates, including:
    - Electro Magnetic Compatibility paper (ref. UN Regulation No. 10)
    - CSPN Certification/ANSSI papers

VIII. Consideration of how to develop further guidance

The Task Force may wish to consider their next step in terms of further defining guidance. A template has been provided for consideration

Documentation: TFCS-03-10e Template paper for defining guidance

The stepwise approach mentioned above was agreed. No further in depth discussion was had.

Data protection (may cross over into second day)

IX. List of definitions

The Task Force may wish to agree a list of common terms and definitions relevant to data protection issues based upon the supplied paper(s)

Documentation: TFCS-03-05e Initial proposals for terms and definitions

The group agreed to adapt the same approach as for Cyber Security agenda item V and integrate this activity into one agenda point.

X. Consideration of data and information that may be held on vehicles or transmitted from them

The Task Force may wish to agree a list of data and information that may be held on a vehicle and the systems that may hold them

A discussion took place, how to proceed with the issue of Data Protection. It was confirmed again, that the group should focus on the technical/security aspects of cyber security. FIA mentioned that they see two sets of data to be protected: personal data and personalized data. Furthermore, they see the need to look into authorization issues. The chair (UK) raised the issue, that there might be the need to differentiate between temporary data, stored data, etc. ITU asked for clarification how the G7 decision/paper on Cyber Security/Data Protection will be considered.

The group agreed to treat data protection/privacy issues as a subset of Cyber security. Furthermore, it was agreed, as proposed by the Netherlands, to keep the Terms of Reference as adopted before, even though data protection may not appear in the future as a standalone topic on agendas for meetings.

Conclusions:

- The group will focus on technical security issues related to data protection/privacy
- Review G7 decision/paper for next session
- Data protection issues will be considered within the cyber security discussions in future meetings

XI. List of key data protection risks and threats

The Task Force may wish to agree a list of key data protection risks and threats that they consider to be realistic and plausible

Documentation: TFCS-03-06e Initial proposals for possible cyber risks and threat

Will be incorporated in general cyber security risk/threat analysis.

XII. List of objectives/principles/actions that could mitigate the key risks identified

The Task Force may wish to agree a list of objectives/principles or actions that if achieved or carried out could mitigate, in part or combined, the key risks and threats previously identified

Documentation: TFCS-03-07e DfT Cyber Security Principles

Will be further discussed, once the threat analysis is finalized.

XIII. Consideration of how to develop further guidance

The Task Force may wish to consider their next step in terms of further defining guidance

Not discussed.

Conclusions

XIV. Actions and agenda items for the next meeting

The Task Force may wish to consider and agree actions and agenda items for the 4th meeting.

1. Review definitions

- Summary of UNECE definitions to be shared
- SAE to continue to seek to share their definitions

2. OICA to draft a table for threat analysis
   => review during dedicated web meeting (ad hoc "Threats") on 8 March 2017
3. Finalize threat analysis during TFCS-04
4. Members were invited to share any relevant documents, especially those mentioned by delegates, including:
   - Electro Magnetic Compatibility paper (ref. UN Regulation No. 10)
   - CSPN Certification/ANSSI papers

XV. Date and place of the next sessions

Confirmation that the fourth session of the Task Force will take place in Geneva on the 13th and 14th of March. The Task Force may wish to agree on the date and place of further future sessions.

TFCS ad hoc "Threats" (Web)	8 March 2017	10:00 am – 12:00 pm CET
TFCS-04	13-14 March 2017	Geneva @ ITU
TFCS-05	10-11 May 2017	Paris @ OICA
TFCS-06	31 May – 01 June 2017	Washington (confirmed)
TFCS-07	30-31 August 2017 or 27-28 September 2017	Japan (to be confirmed)

Additional web meetings will be scheduled as necessary.

A doodle poll will be undertaken to agree the date of TFCS-07.

XVI. Any Other Business

The Task Force may wish to discuss any other item proposed, if any.

No issues discussed.

Submitted by the Secretary
of TF-CS/OTA

Working Paper **TFCS-04-02**
4th TFCS, 13-14 March 2017
Agenda item 1

Minutes of the third session of

the UN Task Force on Cyber Security and OTA issues

Day two – Over-The-Air issues

17 February 2017, 09:00-16:00 CET

4 Rue de Berri, Paris

I. Adoption of the Agenda

The Task Force may wish to adopt the provisional day's agenda.

Documentation: TFCS-03-01e-Rev1e Agenda

The agenda was adopted without changes.

II. List of definitions

The Task Force may wish to agree a list of common terms and definitions

The group agreed to adapt the same approach as for Cyber Security agenda item V and integrate this activity into one agenda point.

III. List of key security risks and threats for OTA

The Task Force may wish to agree a list of key risks and threats that they consider to be realistic and plausible for software updates, particularly OTA

Documentation: TFCS-03-06e Initial proposals for possible cyber risks and threat

The group agreed to split the issues of software updates (incl. OTA) into two elements:

- Security issues related to software updates
- Type approval related issues

The security related topics shall be incorporated in the risk/threat analysis for cyber security, the type approval related issues shall be discussed as a standalone item.

IV. List of objectives/principles/actions that could mitigate the key risks identified

The Task Force may wish to agree a list of objectives/principles or actions that if achieved or carried out could mitigate, in part or combined, the key risks and threats previously identified

Documentation: TFCS-03-07e DfT Cyber Security Principles

TFCS-03-08e NHTSA Cybersecurity Best Practices for Modern Vehicles
TFCS-03-09e ENISA Cyber Security and Resilience of smart cars

Will be further discussed, once the threat analysis is finalized.

V.List of relevant existing practices on software updating

The Task Force may wish to agree a list existing practices, directives and regulations relevant to software updates, OTA, and type approval

ITU mentioned, that it would be beneficial to review the existing specifications for OBD II software updates. However, for OTA new requirements/measures are likely to be added. In addition, OICA provided information on the existing process of software and its updates within type approval (see below).

VI. List of implications related to type approval for software updates, including technical and administrative provisions

The Task Force may wish to agree a list of implications related to type approval for software updates, including technical and administrative provisions

Documentation: TFCS-03-11e OICA reflexion software updates
TFCS-03-12e OICA Example type approval for software updates of steering systems

OICA presented document TFCS-03-11e. The presentation showed to which extend software and its updates are already covered in the current regulatory environment. One of the most important issues identified are updates/changes of software for vehicles already registered (in-use). (See also agenda item VII below.)

In addition, the group discussed the current situation for vehicles before registration. This included how software is covered within the existing type approval process and regulations. Some regulations already today address software, e.g. via annexes for complex electronic systems (UN R13-H, UN R79, etc.). It was noted that existing regulations may not sufficiently address software updates.

For in vehicles before registration, it was noted that for software updates the impact on existing approvals is evaluated between the OEM and Technical Service. OICA pointed out that Conformity of Production is to be seen as the key element to ensure compliance between the vehicles manufactured and the vehicle type approved. This also includes the software. In this regard it was seen beneficial to differentiate software updates into three different classes:

1) Non type relevant software changes

2) Type relevant software changes requiring no further testing but an extension of type approval

3) Type relevant software changes requiring further testing for an extension of type approval, e.g. adding new functions

It was noted that a software update on a non-regulated system, such as airbags, may have a knock on effect to regulated systems, so there may be a need to consider/assess such impacts.

A discussion took place regarding whether the existing requirements and processes are sufficient or if modifications are required, especially for post-registration updates. Japan proposed that OEMs should provide, or be required to have, documentation describing the impact assessment for classification of software updates. This documentation could be reviewed during a CoP audit. An active reporting (e.g. to Technical Services / Approval Authorities) of every software change was not identified to be appropriate due to the administrative burden it might place on both parties.

Another issue to be reviewed is how to verify the configuration of a vehicles software. OICA explained that the situation is not presently comparable to consumer electronics, where software updates in-use during the product lifecycle are frequently conducted. The software of vehicle systems, especially safety systems, is usually developed for the entire vehicle life cycle and never changed. However, software is continuously changed over the product lifecycle for vehicles, affecting vehicles in production. Such changes of software can be classified as above with regard to their relevancy for approvals.

It was noted that if customers or regulatory bodies wished to verify the status of a vehicles software, it would be necessary to be able to ascertain the status of software and confirm it matches with those provided type approval for the vehicle. It was noted that to ensure the correct software is installed, techniques like code signing and software hashing may be need for authentication of software.

Japan proposed to elaborate on some case studies and will come back in a future session.

VII. List of implications related to post-registration regulatory compliance and conformity to the type approved

The Task Force may wish to agree a list of implications related to post-registration regulatory compliance and conformity to the type approved

Documentation: TFCS-03-11e OICA reflexion software updates
TFCS-03-12e OICA Example type approval for software updates of steering systems

As a possible way forward for software updates of registered vehicles, the concept of considering software updates as “aftermarket part” had been discussed, based on document IT/AD-10-13 (“Retrofit Approach”) and OICA document TFCS-03-11e.

Since today the modification of registered vehicles (in-use) is governed by national legislation, such “Aftermarket”- Regulation could help to improve the legal situation.

Another issue to be looked at are recall related software updates, which would mainly affect vehicles in use. Questions arose, if “emergency updates” of software would be possible, even before an approval would have been granted. The delegate from the Netherlands clarified, that in any case safety of customers has the highest priority, therefore it would be possible. It was noted that in such a scenario safety testing of the update would provide an opportunity/time window for type approval discussions to be had between OEM’s and Technical Services / Approval Authorities on possible approaches. However, even for “emergency updates” the classification of software updates as mentioned above will apply.

VIII. Consideration of how to develop further guidance

The Task Force may wish to consider their next step in terms of further defining guidance.

Not discussed.

Conclusions

IX. Actions and agenda items for the next meeting

The Task Force may wish to consider and agree actions and agenda items for the 4th meeting.

Following tasks had been identified:

1) Review relevant existing regulations
2) Develop regulatory proposal to address processing and requirements for software updates. This may include:
    - Consideration of potential update scenarios
    - Requirements for documenting what has happened
    - Requirements for authorities to approve/audit changes
3) Address the need for configuration control (s/w version identification)
4) Process for: - s/w updates for series production
    - s/w updates on registered vehicles (in-use)

In addition, Japan will provide case studies for software updates which can be used to test the proposals developed.

X.Date and place of the next sessions

Confirmation that the fourth session of the Task Force will take place in Geneva on the 13th and 14th of March.

See above.

XI. Any Other Business

The Task Force may wish to discuss any other item proposed, if any.

No issues discussed.