Minutes of the test of the 16th Meeting of the UN Task Force on Cyber Security and OTA issues

12-13th November 2019, 09:00-17:00 (JST) – Cyber security

14th November 2019, 09:00-17:00 (JST) – Software updates

Hosted at JASIC, Tokyo

**Day 1, Cyber Security**

1. Introductions

Introductions were made.

1. Adoption of the Agenda

The ad hoc group of the Task Force may wish to adopt the provisional agenda.  
*Documentation:* TFCS-16-01 (Chair) Agenda

The agenda was adopted

1. Adoption of minutes and report from previous meetings

The chair will report the outcomes of the ad-hoc meetings and the coordination meetings. The Task Force will be asked to adopt the minutes from the previous meeting.

The chair will additionally provide a report from GRVA.

*Documentation:* TFCS-16-02 (Chair) Minutes of TFCS 15

The minutes were accepted.

The actions in the minutes were reviewed. All actions were complete.

A report from the last session of GRVA was provided. It was noted that the group was instructed to split the recommendations into their constituent parts. Proposed amendments of the cyber security regulatory text by GRVA members were reviewed at that meeting. The outcome of those discussions and undiscussed documents are incorporated into the working documents of TFCS 16.

1. Test phase report

The task force will be asked to take note of the test phase report provided to WP29 to fulfil the work priority stated in the Revised Framework document on automated/autonomous vehicles, ECE/TRANS/WP.29/2019/34/Rev1.

In response to the request for a report on the test phase the Chairs of the Task Force provided TFCS 16-16 to WP29. The content is based on minutes of previous meetings and describes the test phase. The version provided was a Revision 1. The task force will be asked to take note of this report.

To support the reporting from the Task Force the European Commission collated comments provided by Task Force members and participants in the test phase. The task force will be invited to review the document and will be asked for their opinion on whether they would like to adopt it as a formal method of recording comments.

*Documentation:* TFCS 16-16 ECE-TRANS-WP29-GRVA-Report on CS-OTA test phase

TFCS 16-30 (COM) matrix\_test\_phase\_comments

The chair stated that a “chairman’s report” had been provided to WP29 on the test phase. This is available as TFCS 16-16rev3. The European Commission was thanked for their help in creating this document.

The document TFCS 16-30 was highlighted to the group. The document was created by the European Commission and captures comments from the test phase and surrounding meetings (TFCS 15 and GRVA). Task Force members were invited to review the document, particularly the comments assigned to them, and consider if and how they would like to proceed with the document. If the Task Force wishes to adopt the document as a change log the first step would be for members to review the comments assigned to them and their current status.

ACTION: Task Force members were invited to further review and consider TFCS 16-30

1. UNECE Working Party 6 Report on the sectoral initiative on cyber security

The task force will be asked to take note of the work of WP.6 and their report on cyber security referenced ECE/CTCS/WP.6/2019/9 (<https://undocs.org/ECE/CTCS/WP.6/2019/9>).

The work of WP6 on cyber security was highlighted, in particular the draft document WP.6/2019/9. The chair highlighted that the approach adopted in the regulatory text aligns with this draft document, but the document has further information on International Standards that might be applicable.

ACTION: Task Force members were invited to note the work of WP6 and further review and consider the document highlighted. Comments may be fed back via representatives in WP29 or WP6 or at the next meeting.

1. Review of legislative proposal

Members of the Task Force will be asked to review proposed changes to the draft text and whether they improve them or not. The task force will be invited to produce an agreed version for submission to GRVA containing only accepted changes.

It is proposed that the regulatory text (as shown in TFCS 16-11) is separated from the rest of the recommendation (as provided in TFCS 16-08) and the Task Force use TFCS 16-11 as the basis for discussion.

It is proposed that *TFCS 16-31 (Chair) Cyber security regulatory text - consolidated comments* is used as the basis for the discussion.

Documentation:

TFCS 16-03 (CITA, EGEA, ETRMA, FIA and FIGIEFA) - Cybersecurity Amendments

TFCS 16-04 (European Commission) cyber security amendments to TFCS-15-35.

TFCS 16-07 (Chair) Proposed text covering document handling for the approval.

TFCS 16-08rev1 (Chair) ECE-TRANS-WP29-GRVA-2019-02e Cyber Security Proposal latest version.

TFCS 16-11 (Chair) Cyber security regulatory text

TFCS 16-15 (Chair) Cyber security regulatory text - UK amendment

TFCS 16-19 (UNISS) comments on TFCS 16-11 Cyber security regulatory text\_

TFCS 16-22 (NL) comments on 16-08rev1 (Chair) ECE-TRANS-WP29-GRVA-2019-02e Cyber Security Proposal

TFCS 16-24 (NHTSA) comments on 16-07 (Chair) Proposed text covering document handling for the approval

TFCS 16-25 (NHTSA) comments on 16-08 (Chair) ECE-TRANS-WP29-GRVA-2019-02e Cyber Security Proposal

TFCS 16-26 (UK-OICA) Template Declaration of compliance

TFCS 16-27 (FIGIEFA et al) New Cybersecurity Amendments with justification

TFCS 16-28 (Chair) Example of statements that could be used to aid assessments of CSMS

GRVA-04-25 (IMMA) Comments on cyber security paper

GRVA-04-22 (GER) Comments on cyber security paper

TFCS (Chair) 16-31 Cyber security regulatory text - consolidated comments

The Task Force agreed to accept the proposed format for the regulatory text and adopted TFCS 16-31 as the working document for its review. The output of the discussion was recorded as TFCS 16-31rev1.

The following points of discussion were noted (the notes do not include where amendments were accepted without debate):

* The proposal from IMMA to limit the scope to L6 and L7 vehicles with automated driving functions was discussed and accepted in principle. It was noted that there are many vehicles in this category which are not connected or automated and it may be unduly burdensome to mandate manufacturers of such vehicles to get a CSMS. The Task Force did not accept reference to the SAE levels. It was noted that the term “automated driving function” will need to be defined.

ACTION: IMMA to propose a definition for “automated driving function”

* The definitions were reviewed and amended. It was decided not to re-order them.
* The proposal for handling confidential information (paragraph 3.3) was reviewed and accepted. It was noted that the timeframe proposed (10 years) is commonly used in other regulations and on that basis was adopted.
* The UNISS proposals for 6.x.x were not adopted. The first is already in the text and the second, relating to suppliers, was considered too wide in scope as it would apply to all potential suppliers to the automotive sector who might provide any part or service for a vehicle.
* The UK proposals for requiring documentations for the CSMS in 6.2.1 and 6.2.2 were reviewed. The text was amended to accommodate them.
* The DE proposal for paragraph 6.9 was discussed.
  + It was noted that the first sentence (national or regional bodies being able to declare vehicles unsafe) is covered in other legislation and that the requirement (or its absence) would not affect their ability to perform such action. It was therefore not accepted as it was viewed as redundant and unnecessary.
  + The second sentence (transfer of a CSMS) was discussed. It was questioned whether this requirement was needed. Contracting Parties were concerned that it may be used by manufacturers to divest their responsibilities to maintain monitoring and response capabilities. It was further noted that, without the manufacturer participating, it may be practically difficult for a third party to have a CSMS relevant to a vehicle type as they would need to have all the design, monitoring and contractual arrangements in pace with contractors. Alternative wording was considered but not accepted by the Task Force. DE were invited to consider further wording.
  + The last sentence (the mandatory transfer of all information relating to a vehicle type to a third party) was discussed. It was noted that if the third party had a valid CSMS for a vehicle type this requirement would not be needed. It was further noted that the requirement may be difficult to enforce legally if the intention was to enable third parties to gain the ability to get a CSMS for a given vehicle type without the consent of the manufacturer (especially for information related to intellectual property or suppliers). The proposal was not accepted by the Task Force.
  + The representative from Germany stated they may provide a revised text.
* The UK proposal (6.10) for permitting suppliers to gain a CSMS were discussed and not adopted. Contracting Parties present did not support the proposal as they noted that mutual recognition of any resultant certificate may not be possible.
* The UK proposal (6.11) for re-assessment of a CSMS was discussed and not adopted. It was noted that there may be processes and procedures, particularly for response, where a manufacturer may never be able to fully show that they can implement them in full. It was noted that exercising can help demonstrate response procedures work. Another concern raised was that the proposal may lead to unintended consequences. Alternative wording was proposed but was withdrawn. The UK noted that in practice the activity may happen if a technical service needed more certainty that a process is implemented as described.
* The FIGIEFA proposal for 7.2.2.1 was discussed and not adopted as it was noted that the wording repeats the definitions provided for the three phases. The definition of decommissioned was not adopted as it would not be used if the proposal for 7.2.2.1 was not adopted. FIGIEFA were invited to consider the definitions, particularly of post-production phase, if they wish to revise their proposal. The DE proposal was not adopted as the term “commercially available and serviced fleet” was considered unclear and may be unintentionally limiting.
* The proposed amendments to 7.2.2.2 were discussed.
  + The UNISS proposal for part a) was not adopted as it was considered limiting and not needed.
  + The DE proposal for part b) was not adopted. It was noted that the intention is for risks from backend IT systems to be considered. The Task Force noted that the term “post-production services” would need clarification for any future proposals as its scope is open to interpretation and that the requirement is captured in the interpretation document, explaining that the risk assessment should consider systems that connect to a vehicle. The proposal was withdrawn.
  + The DE proposal for part g) was partially adopted. It was noted that standards other than international standards could be used (and that there are several international standards that could be used for risk management processes). Therefore, the aim of harmonising the approach to risk assessment may not be achievable or desirable through reference to international standards. It was further noted that there is an earlier requirement that refers to the resolution. Based on these arguments the proposals relating these aspects were not accepted.
* The DE proposal for an Information Security Operations Centre was discussed. It is noted that:
  + The intention was to have a centralised function at a manufacturer. It was questioned why this was needed, versus alterative, equivalent, arrangements.
  + It was noted that the terminology proposed comes from the Information Technology sector. There the function is commonly called a “Security Operations Centre” and it is generally applied where the same entity owns all the systems being monitored.
  + The requirements for monitoring and response are already stated, so these are repeating previous requirements.
  + The term “fast response” is indeterminate. It should have specifications defining what constitutes “fast” if it is to be used.
  + The use of “Intrusion Detection Systems (IDS)” and Security Incident Event Monitoring (SIEM)” was discussed. It is also noted that the requirement for central monitoring of private vehicles would require user consent. The Task Force noted that to take these specific technologies forward a detail specification would be needed to understand how they must be implemented. For example: what they must monitor, what an acceptable prevention tactic would be, what log files to use for the SIEM, how to handle user consent and situations where users do not consent to central monitoring.
  + It was noted that other technologies could be used to detect and respond to cyber-attacks. As the requirements in the regulation are intended to be outcome focused the proposals for mandating the use of IDS and SIEM were not accepted without further specifications and understanding of how they would be used.
* The DE proposals for 7.3.2, particularly relating to testing of sample vehicles was discussed. The principle of physical testing was seen by some participants as a good proposal. It was noted that the proposal did not define what testing should be done and why. The task force noted that testing might be performed to:
  + check if a vehicle can be “hacked”;
  + to check that manufacturers have implemented what they claim to have implemented;
  + or to repeat tests already performed;
  + other reasons.
* Within this it was discussed what a technical service might do with the results. It was felt that if any testing were performed then the second reason may be the most pertinent for a technical service in terms of providing an approval. However, the details of what the scope of these tests might be could not be defined and it was felt more detail would be needed to adopt this proposal, for instance a set of tests to be performed. Alternative wording was considered but not accepted.
* The proposed amendment to 7.3.3. was accepted with an amendment to not limit the consideration of external systems to only those relevant for safety or security.
* The proposal for 7.3.7 and description of an ISOC was withdrawn on the basis that the earlier proposal had not been accepted.
* The text of article 9.4 of the information document was discussed. The consequences of providing information on the risks identified in this document is that the information document would need to be resubmitted if new risks are added or risks change. It was further noted that technical services would most likely require this information and that it would be made available under paragraph 3.3. This approach would allow for information on risks to be updated without having to update the information document, unless there is an overall change in the outcome of the risk assessment.
* The proposed form for the manufacturer’s declaration was accepted. It was noted that this is based on that from R51.

1. Proposal for a cyber security regulation 00

The chair will invite the task force to develop the OICA proposal for the introduction of the regulations.

Documentation: TFCS 16-18 (OICA) Proposal for 7.3. in 00 Series

TFCS-15-13 (OICA) CS Regulation 00 series V1

TFCS-15-14 (OICA) CS Regulation 01 series V1

The Task Force reviewed the proposals from OICA, with a revised proposal 16-18rev1 shown to the group. It was noted that the proposed text for paragraph 7.3 of the 00 series address many concerns from contracting parties but they wanted further time to consider their implications.

The Task Force did not agree on the proposed dates. It was agreed that a small group should be formed, consisting of interested contracting parties (or their representatives) and industry. Volunteers should make themselves known to the chair by the 22nd of November (extended to 29th).

ACTION: chair to coordination formation of 00 series small working group.

ACTION: volunteers for 00 series small working group to inform the co-chairs by 29th of November

1. Formulation of resolution document

Members of the Task Force will be asked to agree and develop a resolution document as per the instructions in Chapter 7 of the recommendation.

It is proposed that *TFCS 16-32 (Chair) Cyber security resolution text - consolidated comments* is used as the basis for the discussion.

Documentation:

TFCS 16-10 (Chair) Cyber security resolution text (chapters 1-6 and annexes B and C)

TFCS 16-17 (UNISS) comments on ECE-TRANS-WP29-GRVA-2019-02e (cyber security)

TFCS 16-20 (UNECE) Cyber security resolution text - proposed preamble

TFCS 16-30 (COM) matrix\_test\_phase\_comments

TFCS 16-32 (Chair) Cyber security resolution text - consolidated comments

The Task Force agreed to accept the proposed format for the resolution text and adopted TFCS 16-32 as the working document for its review.

The Task Force agreed to prioritise work on this document ahead of the interpretation document.

The principle of removing content that repeats that of the regulation was accepted and that the focus of the resolution should be to support identification of threats and mitigations.

ACTION: All – to review content of the document and consider what should be kept and how to incorporate any text from chapters VI and VII should they be deleted

ACTION: Chair – to consult with UNECE secretariat on what the status of the previous ITS-AD resolution should be if this document is adopted under RE3, should it be replaced?

1. Review of interpretation document

The chair will invite members of the task force to review the Cyber Security Interpretation Document.

Documentation: TFCS-15-03 (Chair) Interpretation document CS - SDG outcome

TFCS 15-28 (DEG) TFCS-15-03 (Chair) Interpretation document CS - SDG outcome\_Comments

TFCS 16-29 (Chair) Suggest edit to chapters 3 and 4 of software update document TFCS 16-12

The Task Force agreed to accept TFCS 15-28 as its working draft for the interpretation document but did not review it. It was noted that this would have to be updated to reflect current amendments to the regulation.

The document TFCS 16-29 was withdrawn.

The chair presented TFCS 16-28 which demonstrates a possible approach for assessing if the procedures listed in 7.2 are being met through using statements to help aid the assessment if a requirement is met or not. The approach was welcomed but members requested further time to review the document. The chair re-iterated that the document is a draft and that it would need further work.

The Task Force agreed that if the approach were adopted, it should be integrated into the interpretation document and that this approach could also be used for the software update process interpretation document.

The agreed next steps were:

* Task Force members to review the document
* UK to review the proposed statements.
* Next steps to be considered at TFCS 17

1. Development of draft list of Technical Requirements

The task force will be asked to consider the Framework document ECE/TRANS/WP.29/2019/34 and to develop a plan and timetable to implement its recommendations, recognising the current status of the work of the task force.

Possible next steps may include the development of a draft list of Technical Requirements that would be workable in the context of both the 1958 and 1998 Agreements.

The Task Force discussed how to progress this item. It was agreed that a small working group should be formed to prepare a draft document for TFCS 17 to consider further. This should be done via video conferencing.

ACTION: Participants interested in participating in formulating a draft list of technical requirements to let the chair know by the 29nd of November.

1. Next Steps

The group will be asked to confirm next steps. This will include what to report to GRVA and the need for any future meetings.

The Task Force agreed to send clean, formal documents to GRVA relating to the 00 series and 01 series containing all accepted amendments and text that had not yet been agreed. This would allow GRVA to discuss them formally.

The Task Force further agreed to consider the outcome of the small working groups and any other amendments at TFCS 17 and send GRVA informal documents containing any proposed changes to the formal documents.

The option of requesting a special GRVA to progress the regulatory proposals was also requested from Task Force members.

The regulatory and interpretation documents will be progressed at future meetings.

ACTION: Chair to ask GRVA if a special session can be convened to look at the cyber security proposals.

1. Any Other Business

The representative from the ISO/SAE standards work provided an update. A version should be available soon for public comment and Task Force members were invited to participate in this. The period for comment will end in April 2020.

Software Update Processes

1. Introductions
2. Actions from previous meetings

The chair will highlight any outstanding actions from previous meetings, including the GRVA.

*Documentation:* TFCS-16-02 (Chair) Minutes of TFCS 15

All actions were reviewed and noted as complete.

1. Requirements for Technical Services

Members of the task force will be asked to consider requirements for technical services.

*Documentation:* TFCS 16-33 (NL) Requirements for TDs\_006

On day 2 the Netherlands presented TFCS 16-33 and invited Task Force members to participate in work looking at developing requirements for technical services to demonstrate their competence in assessing the cyber security regulation. This initiative was welcomed by the Task Force.

ACTION: Interested parties to let the chair or NL representatives from RDW know if they are interested in participating in developing requirements for technical services by the end of November.

1. Review of legislative proposal

Members of the Task Force will be asked to review proposed changes to the draft text and whether they improve them or not. The task force will be invited to produce an agreed version for submission to GRVA containing only accepted changes.

It is proposed that the regulatory text (as shown in TFCS 16-13 and 16-14) is separated from the rest of the recommendation (as provided in TFCS 16-09) and the Task Force use TFCS 16-13 and TFCS 16-14 as the basis for discussion.

It is proposed that *TFCS 16-34 (Chair) Software Update regulation text - consolidated comments* is used as the basis for the discussion.

Documentation:

TFCS 16-05 (Tesla-RDW-KBA-GM) ECE-TRANS-WP29-GRVA-2019-03e Software update proposal with all amendments.

TFCS 16-06 (Tesla-RDW-KBA-GM) RXSWIN Review v2.

TFCS 16-09rev1 (Chair) ECE-TRANS-WP29-GRVA-2019-03e Software update proposal latest.

TFCS 16-13 (Chair) Software update process regulatory text (annex A).

TFCS 16-14 (Chair) Software identification process (RXSWIN) regulatory text (annex B)

TFCS 16-21 (JPN) Proposal of modification for amendment (TFCS 16-05) by Tesla-RDW-KBA-GM

TFCS 16-23 (NHTSA) comments on 16-09 (Chair) ECE-TRANS-WP29-GRVA-2019-03e Software update proposal

TFCS 16-26 (UK-OICA) Template Declaration of compliance

GRVA-04-21 (GER) Comments on software update paper

TFCS 16-34 (Chair) Software Update regulation text - consolidated comments]

The Task Force agreed to accept the proposed format for the regulatory text and adopted TFCS 16-34 as the working document for its review. The output of the discussion was recorded as TFCS 16-34rev1.

The following points of discussion were noted (the notes do not include where amendments were accepted without debate):

* The IMMA proposal to remove category L vehicles was accepted
* The approach adopted for amendment of paragraphs 3, 6 and annex 1 of the cyber security regulation was adopted for this regulation
* The DE and JPN proposals for 7.1.2.3 were discussed and partially accepted. It was noted that the term “auditable” would require that the format of the register must mean it could be provided for an audit. The proposal from JPN was not accepted as the first paragraph was considered to contain this requirement (there should be documentation describing the RXSWIN irrespective of whether the RXSWIN is located on the vehicle or not).
* The DE proposal for 7.1.3.1 regarding use of a CSMS to evidence the requirement was not accepted as the proposed text was put forward as a “may” provision and it was noted that this is within the interpretation document, so the requirement already exists as a “may” provision. The option of making it a shall provision was discussed but the issues with mutual recognition of certificates of compliance was noted and it was not adopted.
* The proposals for 7.2.1.2.2 were discussed. The US proposal to refer to the OBD port as an example of a means of reading an RXSWIN as it specifies a technical solution. This was not accepted by other contracting parties who stated that this would affect the aftermarket and the ease of reading that information. The US noted the issue will arise again when the Task Force looks at requirements for a broader audience than the ’58 Agreement and they will not support the present proposal to specify a single technology unless there is data to show this is the only way to achieve the requirement.
* The need to declare when software affecting an RXSWIN is updated was discussed. It was noted that the intention of this is so that technical services or approval authorities are informed of changes but not that they need to act on each notification. On this basis the JPN proposal was withdrawn.
* The DE proposal for 7.2.2.5 and 7.2.2.6 was amended to reflect the intention that vehicles verify that they can execute software updates before they are executed. The original wording was debated. It was noted that:
  + It is unclear what would constitute an “manipulated vehicle” or a “malfunction”.
  + It was noted that a software update may be intended to fix a problem causing diagnostic trouble codes and that preventing over the air updates if DTC’s are present could lead to undesirable situations of fixes not being applied because of the presence of the fault they are designed to fix.
  + It was noted that 7.2.2.5 could lead to unintended actions of DTC’s being regularly cleared to permit software updates.
  + It was noted that the original scope would prevent any update (for example mapping updates) if there was a problem anywhere on the vehicle regardless of whether it would impact the execution of the update.
* The German delegate stated they would consider the proposed refinement to their amendment
* The DE proposal for 7.2.2.7 and 7.2.2.8 were discussed and not accepted by the Task Force. However, the requirements of 7.2.2.2 were changed to “shall” requirements on the basis of the DE proposal. The following was noted:
  + It was suggested that these proposals should be within 7.2.2.2 as that requirement relates to what information should be provided to the vehicle user.
  + It was noted that the proposals of 7.2.2.1 are not all appropriate to the proposed requirements as they do not require information to be displayed.
  + It was noted that the text “is able to” was used as the user may not always wish to be informed and in some vehicles, such as commercial vehicles, may not be able to be visually informed within the vehicle. However, the detailed information may be made available via the manufacturers website.
  + It was noted that the term “visually inform” was vague and it may be better to prescribe methods by which the information might be displayed.

TFCS 16-14 was reviewed to ensure the text was consistent with the above amendments to the other regulatory text. The output was recorded as TFCS 16-14rev1.

1. Proposal for a software update security regulation 00

The chair will invite the task force to consider proposals for the introduction of the regulations.

Documentation: tbc

The Task Force did not discuss this item as no proposals were provided.

1. Formulation of resolution document

Members of the Task Force will be asked to agree and develop a resolution document as per the instructions in Chapter 7 of the recommendation.

It is proposed that *TFCS 16-35 (Chair) Software updates resolution text - consolidated comments* is used as the basis for the discussion.

Documentation: TFCS 16-12 (Chair) Software update resolution text proposal.

TFCS 16-35 (Chair) Software updates resolution text - consolidated comments

The Task Force agreed to adopt TFCS 16-35 as its working document and reviewed its content for relevance. The agreed approach was to focus on identifying content relevant to the process described in paragraph 4. The review also included consideration of the proposed amendments. The output of this review was recorded as TFCS 16-35rev1.

ACTION: all – consider what content should be kept and the future of this document

ACTION: chair – review document and identify:

* + What repeats the regulatory text
  + What could be moved to the interpretation document
  + What is repetition of other text

1. Review of interpretation document

The chair will invite members of the task force to review the Cyber Security Interpretation Document.

Documentation: TFCS-15-04 (Chair) Interpretation document SU - SDG outcome

TFCS 15-27 (DEG) TFCS-15-04 (Chair) Interpretation document SU - SDG outcome Comments German drafting group

The Task Force agreed to adopt TFCS 15-27 as its working document and consider the approach suggested for the cyber security interpretation documents of having statements to help assess whether a requirement is being met.

The Task Force will review this item in more detail in future meetings.

1. Next Steps

The group will be asked to confirm next steps. This will include what to report to GRVA and the need for any future meetings.

The Task Force agreed to send clean, formal documents to GRVA relating to the TFCS 16-14rev1 and TFCS 16-34rev1. This would allow GRVA to discuss them formally.

The Task Force further agreed to consider the outcome of the small working groups and any other amendments at TFCS 17 and send GRVA informal documents containing any proposed changes to the formal documents.

The regulatory and interpretation documents will be progressed at future meetings.

1. Any Other Business

The chair noted that a further meeting, TFCS 18, would be needed and asked for volunteers to host it. It will be around March 2020 (tbc).

1. List of actions

**Cyber**

**ACTION: volunteers for 00 series small working group to inform the co-chairs by 29th of November**

**ACTION: Participants interested in participating in formulating a draft list of technical requirements to let the chair know by the 29th of November.**

**ACTION: Interested parties to let the chair or NL representatives from RDW know if they are interested in participating in developing requirements for technical services by the end of November.**

ACTION: chair to coordination formation of 00 series small working group.

ACTION: Task Force members were invited to further review and consider TFCS 16-30

ACTION: Task Force members were invited to note the work of WP6 and further review and consider the document highlighted. Comments may be fed back via representatives in WP29 or WP6.

ACTION: All – to review content of the resolution document and consider what should be kept and how to incorporate any text from chapters VI and VII should they be deleted

ACTION: Chair – to consult with UNECE secretariat on what the status of the previous ITS-AD resolution should be if this document is adopted under RE3, should it be replaced?

ACTION: Chair to ask GRVA if a special session can be convened to look at the cyber

security proposals.

ACTION: Task Force members to review TFCS 16-28

ACTION: UK to review the proposed statements in TFCS 16-28 and also their application to the software update interpretation document

**Software updates:**

ACTION: all – consider what content should be kept in the resolution document and the future of this document

ACTION: chair – review document and identify:

* + What repeats the regulatory text
  + What could be moved to the interpretation document
  + What is repetition of other text