Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

- Definitions:
  Initial list of definitions is provided by ISO/SAE (not available for TFCS-04), ISO/SAE working on further definitions

- Collaboration with ITU-T SG 17 on security issues:
  The group agreed to exchange on activities and approaches related to cyber security aspects, e.g. threat analysis, ...

  The chair will provide the latest version of the table of threats to ITU-T SG17 by 21 March 2017 for consideration and comments

Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

- Reference Model regarding Cyber Security agreed by TFCS-04

  The 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

Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

- Cyber security threat analysis:

  - The group reviewed the table of threats developed by OICA after TFCS-03 and reviewed during the ad hoc „Threats" webmeeting. Furthermore, the task force tried to condense the list of threats in order to make it more lean without losing content, improving its practical use for the further threat analysis.

  - Improvements on the table are reflected in document TFCS-04-03e-Rev3 and the forthcomming cleaned-up version hereoff

Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

- Software updates:
  - Japan and the Netherlands presented their view on how to further proceed on the type approval aspects of software updates. In addition, the EC report on software updates was reviewed.

  - 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

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

Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

Action items for next session:

- Cyber security:

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

- Software updates:

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

5

Outcome TFCS-04 // 13-14 March 2017 @ ITU, Geneva

<u>Next meetings:</u>

TFCS ad hoc „Threats-2" (Webex)	*April 2017 (date tbd)*	*time tbd*
TFCS-05	10-11 May 2017	Paris@OICA
TFCS-06	13-14 June 2017	Washington@TIA
TFCS-07	30-31 *Aug. or Sept. '17*	*Europe (NL/UK ?)*
TFCS-08	*11-12 Oct. 2017 (tbc)*	*Tokyo*