Transmitted by the Secretary of TF-CS/OTA

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

UNECE - Joint meeting of WP.1 and WP.29/GRRF
20 September 2017,UN Palais des Nations, Geneva

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Overview on Task Force – Cyber Security and Software updates (incl. over-the-air issues)

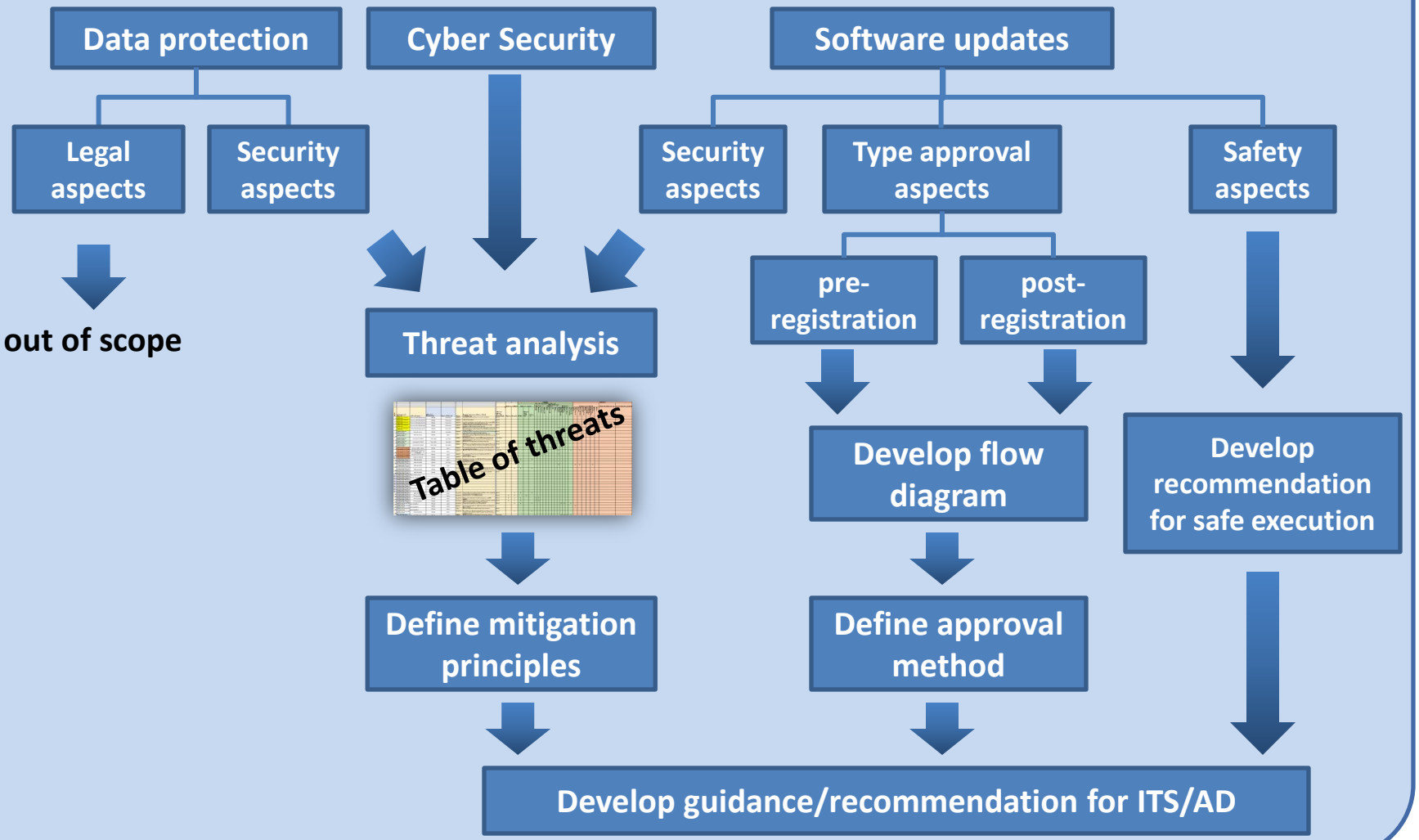
Start of activity:	21 December 2016
Co-Chair:	Mr. Darren Handley (UK/DfT) Mr. Tetsuya Niikuni (Japan/NTSEL)
Secretary:	Mr. Jens Schenkenberger(OICA/Hyundai)
Participants:	Contracting Parties (AU, BE, CN, EC, *EG**, FR, DE, JP, KR, NL, NO, *RU**, ES, SE, CH, UK, US), NGO (ITU, FIA, CITA, IRU, ISO, SAE, OICA, CLEPA)
Participation:	Type approval and cyber security experts approx. 30 people per meeting
Mandate:	until Dec. 2017

** No active participation yet*

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Scope of TF-CS/OTA



Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

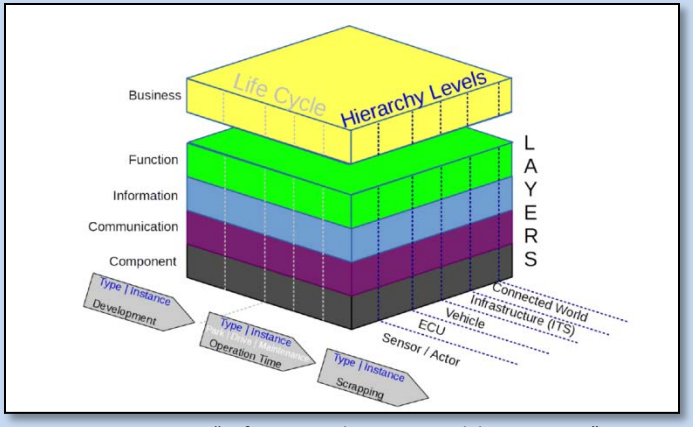
Status report on the activities of TF-CS/OTA

Cyber security:

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

Furthermore, it shall incorporate the information flow and the vehicle lifecycle.



German “Reference Architecture Model Automotive”

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Cyber security (continued):

- The group has **identified key risks and threats**, resulting in a table of threats. It includes threats associated with cyber security, data protection and software updates (incl. over-the-air issues)
- The group agreed to consider “pre attack” (**prevention**), “during attack” (**detection**) and “post attack” (**response**)
- **Reference documents** identified for mitigations are :
  - ENISA report „Cyber Security and Resilience of Smart Cars” TFCS-03-09
  - UK DfT Cyber Security principles TFCS-03-07
  - NHTSA Cyber Security Guideline TFCS-03-08
  - IPA “Approaches for Vehicle Information Security” (Japan) TFCS-04-05
  - UNECE Cyber security guideline (ITS/AD) WP.29/2017/46
  - SAE J 3061
  - ISO 19790
  - ISO 26262
  - US Auto ISAC (report by Booz Allen Hamilton) https://www.automotiveisac.com/best-practices

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Cyber security (continued):

- **Mitigations** for the threats identified had been **developed**, based on an **extended CIA approach** (CIA = Confidentiality, Integrity, Availability) leading to 18 mitigations
- During the development of the mitigations the references, especially the **ITS/AD cyber security guideline principles,** the **UK DfT principles** for cyber security had been considered
- The **detailed outcome** of the threat analysis, including the identified mitigations and correlating principles are comprised in a **spread sheet** (see document TFCS-08-03)

  Note: This document will be finally confirmed by the group at the 8th session of TF-CS/OTA
- The **Consolidated Resolution (R.E. 3)**, already incorporating the ITS/AD guideline on Cyber Security for Connected and Automated , was identified by the group as a **suitable document** to incorporate the outcome on cyber security. Recommendations will be given accordingly.

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Software updates:

- The group agreed that systems with „**deep learning/self learning**“ is currently **out of scope**
- The group is considering both **pre-** and **post-registration** updates, as well as **safety aspects** of software updates
- It was acknowledged by the group that **post-registration** updates are dealt with **nationally**. Therefore any output relating to this issue will be as **guidance** to **support national processes**.

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Software updates (continued):

- The group defined a **matrix** for necessary actions depending on the **timing** of a software update and its **impact** on an approval

moment of update	**no impact**	**limited impact**	**severe impact**
Initial type approval (TA)	not applicable	not applicable	not applicable
Existing TA, **before Certificate of Conformity** (CoC)	no action	extension TA	new TA
Existing TA, after CoC, **before registration**	no action	extension TA and new CoC	new TA and new CoC
Existing TA, **after registration**, by OEM	no action	extension TA or individual approval or approval with limited scope. Registration according to national rules	new TA or individual approval or approval with limited scope. Registration according to national rules
Existing TA**, after registration**, not by OEM	(multi stage) new National approval. Registration according to national rules	(multi stage) new National approval. Registration according to national rules	(multi stage) new National approval. Registration according to national rules

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Software updates (continued):

- The introduction of a **Regulation-linked Software Identification Number** (=> RxSWIN) was agreed by the group.

> ***Principle**:*
> *Cover the type approval relevant software versions of all impacted ECUs by one Type Approval Number for each system type approval.*

- Currently different views on introducing the number: in **each relevant Regulation** vs. introducing a **standalone "Software Regulation"**
- The **SWIN concept** should **support** following **use cases**: Type approval, Periodical Technical Inspection (PTI), Roadside inspection, Market surveillance and Accident investigation

Informal document **GRRF-84-31**
84th GRRF, 19–22 September 2017
Agenda item 8(b)

Status report on the activities of TF-CS/OTA

Timeline:

TF-CS/OTA is well „on track“ to deliver guidance papers/ recommendations on the cyber security and software updates as planned for IWG ITS/AD in March 2018. However, the group may whish to extend the mandate by six month in order to finalize its work in January 2018 an to be in existance when presenting the outcome to WP.29 IWG ITS/AD.