Transmitted by the Secretary of TF-CS/OTA

ITS/AD-12-03

Status report on the activities of TF-CS/OTA

12th session WP.29 IWG ITS/AD
22 June 2017, UNECE, Geneva

Status report on the activities of TF-CS/OTA

Cyber security:

- The group has **finished** its task to **identify key risks and threats**, resulting in a table of threats (see TFCS-05-05-Rev2)
- The table **covers all cyber security threats** identified. This includes threats associated with cyber security, data protection and software updates (incl. over-the-air issues)
- The group has **started** to **develop mitigations** for the threats, based on an **extended CIA approach** (CIA = Confidentiality, Integrity, Availability) leading to 18 mitigations
- The **ITS/AD cyber security guideline principles,** the **UK DfT principles** for cyber security and other references have also been considered in the development of mitigations

Status report on the activities of TF-CS/OTA

Cyber security (continued):

- 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/	

- An **ad hoc web meeting** will be held, with the aim to conclude work on **mitigations** (Mid/End July 2017)

Status report on the activities of TF-CS/OTA

Software updates:

- The group is considering both **pre-** and **post-registration** updates. It is acknowledged that post-registration updates are dealt with **nationally**. Therefore any output relating to this will be as guidance to support national processes.

- To **manage configuration control** for the approval process the **“S/W TAN” approach** has been proposed. This may also be used during **PTI/CTI.**

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

- An **ad hoc meeting** for interested parties dealing with the **S/W update approval process** incl. S/W TAN was agreed

Status report on the activities of TF-CS/OTA

Software updates (continued):

- Summary of actions with relation to the timeline of a software update and its impact on type approval (TA)

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

Status report on the activities of TF-CS/OTA

Software updates (continued):

Further consideration will be given to:

1) **Software Type Approval Number** (S/W TAN):
   - Review approach for „Whole Vehicle S/W TAN“ vs. „System-based S/W TAN“

2) **Administrative process** to realize S/W TAN concept:
   - Review approach for linking S/W versions, ECU‘s involved, etc. with S/W TAN
   - Clarify roles and responsibilities in the process, e.g. involvement of Technical Service, etc.
   - Role of customer involvement
   - Information requirements to support the process

Status report on the activities of TF-CS/OTA

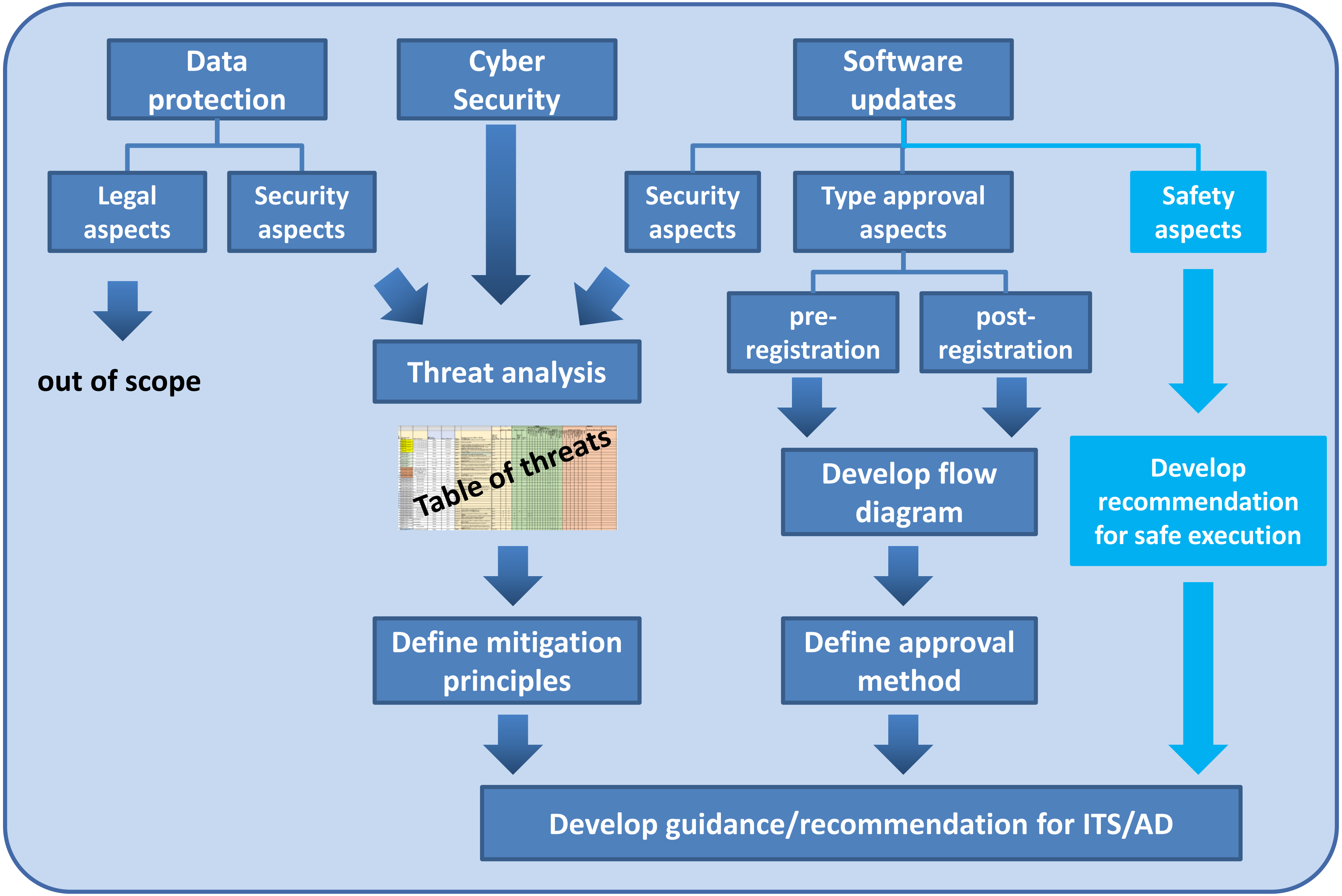
Software updates (continued):

3) **Safety aspects** of software updates:
   - Develop principles/recommendations for safe execution of software updates

4) **Impact of different reasons for updates** on the requirements/approval process

- The group agreed that systems with „deep learning/self learning“ is currently out of scope
- It was noted that an electronic CoC/DoC may be needed to support the process

Status report on the activities of TF-CS/OTA



Data protection

Legal aspects

Security aspects

out of scope

Cyber Security

Threat analysis

Table of threats

Define mitigation principles

Software updates

Security aspects

Type approval aspects

pre-registration

post-registration

Develop flow diagram

Define approval method

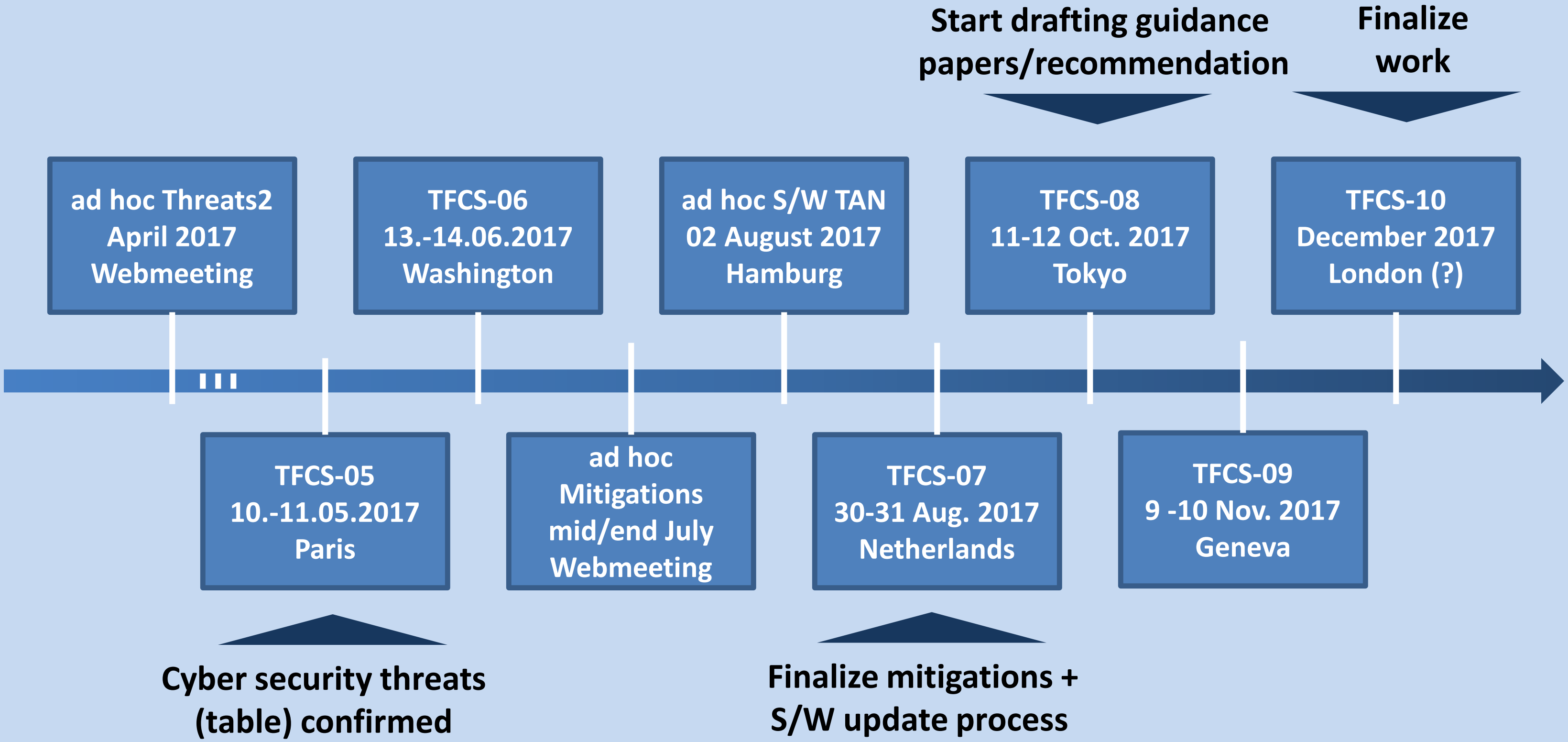
Safety aspects

Develop recommendation for safe execution

Develop guidance/recommendation for ITS/AD

Status report on the activities of TF-CS/OTA

TF-CS/OTA is „on track“ to deliver guidance papers/ recommendations on the issues of cyber security and software updates as planned by the end of 2017



Start drafting guidance papers/recommendation

Finalize work

ad hoc Threats2
April 2017
Webmeeting

TFCS-06
13.-14.06.2017
Washington

ad hoc S/W TAN
02 August 2017
Hamburg

TFCS-08
11-12 Oct. 2017
Tokyo

TFCS-10
December 2017
London (?)

TFCS-05
10.-11.05.2017
Paris

ad hoc
Mitigations
mid/end July
Webmeeting

TFCS-07
30-31 Aug. 2017
Netherlands

TFCS-09
9 -10 Nov. 2017
Geneva

Cyber security threats (table) confirmed

Finalize mitigations + S/W update process