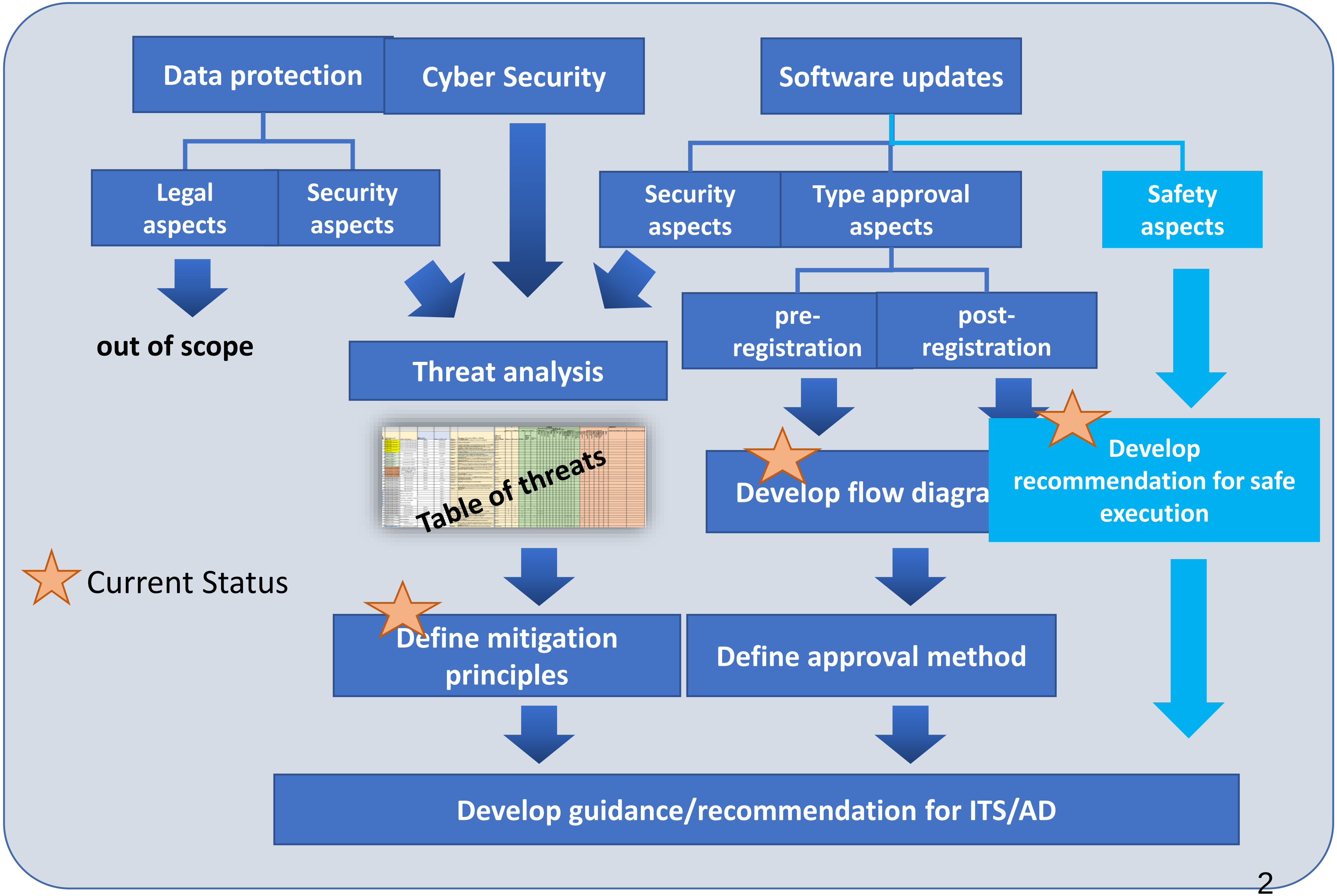
UNECE WP29/TFCS Regulation standards on threats analysis (cybersecurity) and OTA (software update)

Koji NAKAO, NICT, Japan

(Expert of UNECE WP29/TFCS)

General Flow of works in WP29/TFCS and OTA



Data protection

Cyber Security

Software updates

Legal aspects

Security aspects

Security aspects

Type approval aspects

Safety aspects

out of scope

Threat analysis

pre-registration

post-registration

Table of threats

Develop flow diagra

Develop recommendation for safe execution

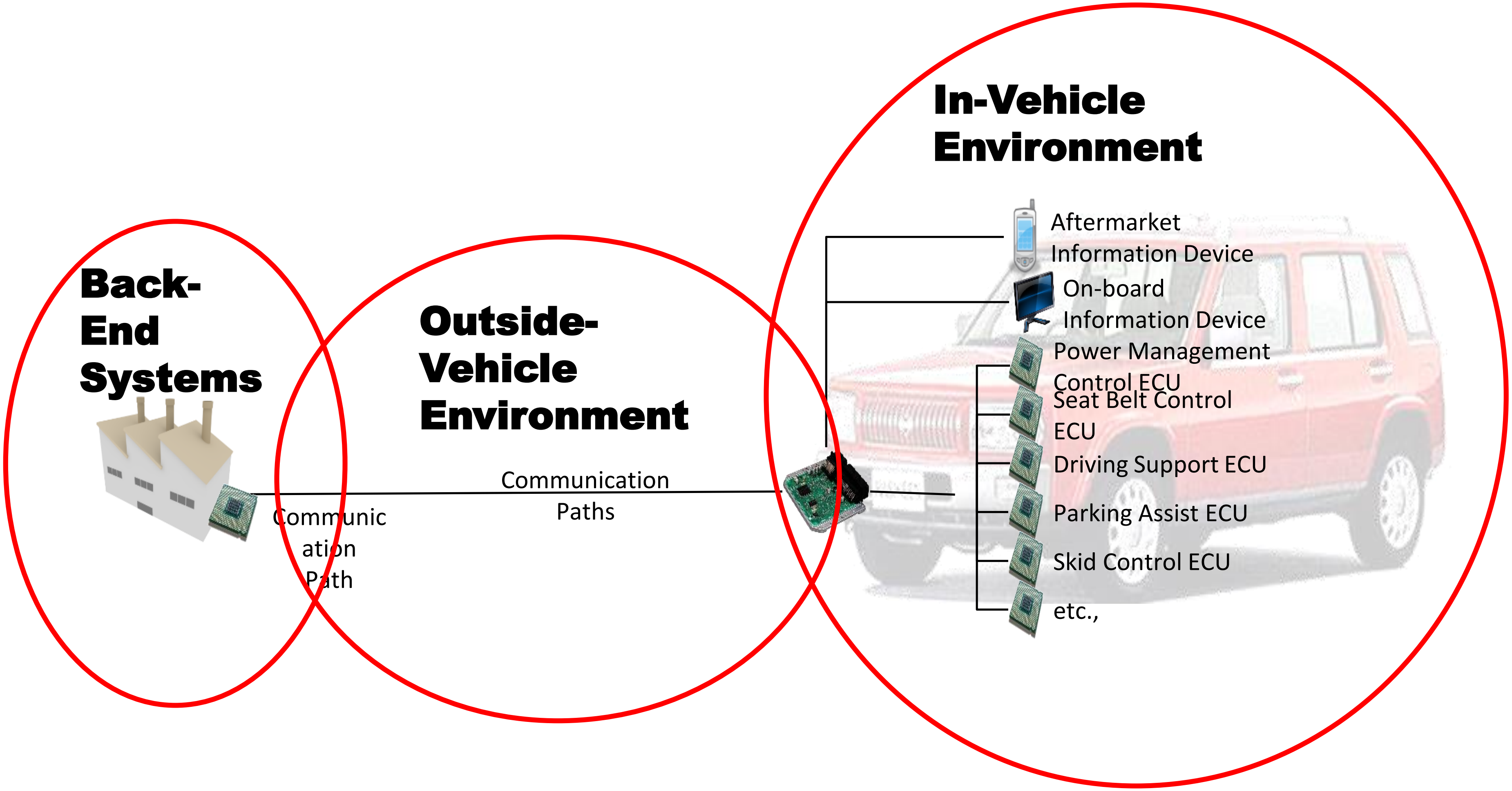
Current Status

Define mitigation principles

Define approval method

Develop guidance/recommendation for ITS/AD

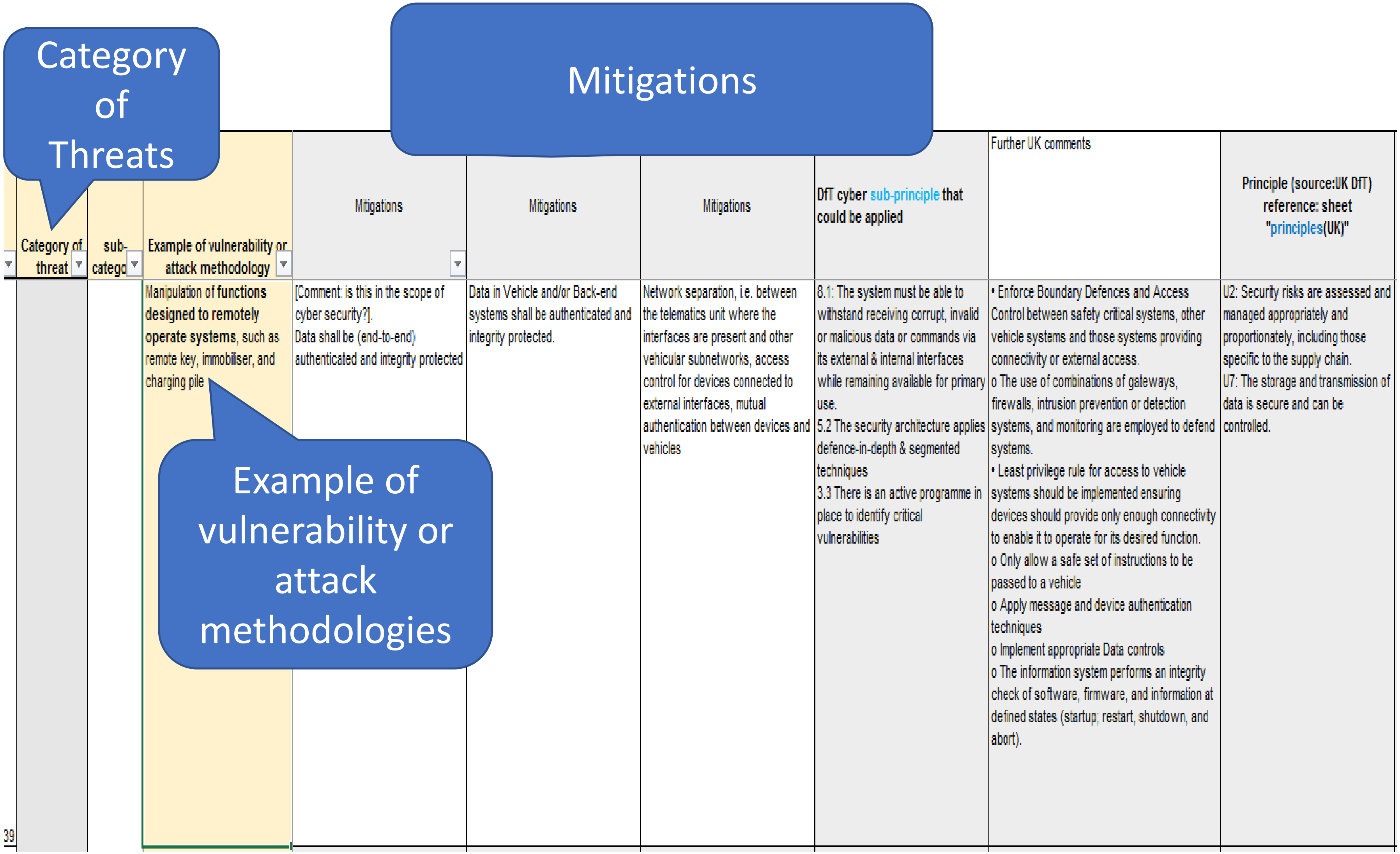
Scope of Threats Assessment (Basic Model)



Please confirm the Threats Table developed by WP29/TFCS

This table can be shared with Q13/17.

Example of Threats table



Category of Threats

Mitigations

Example of vulnerability or attack methodologies

	Category of threat	sub-catego	Example of vulnerability or attack methodology	Mitigations	Mitigations	Mitigations	DfT cyber sub-principle that could be applied	Further UK comments	Principle (source:UK DfT) reference: sheet "principles(UK)"
39			Manipulation of **functions designed to remotely operate systems**, such as remote key, immobiliser, and charging pile	[Comment: is this in the scope of cyber security?]. Data shall be (end-to-end) authenticated and integrity protected	Data in Vehicle and/or Back-end systems shall be authenticated and integrity protected.	Network separation, i.e. between the telematics unit where the interfaces are present and other vehicular subnetworks, access control for devices connected to external interfaces, mutual authentication between devices and vehicles	8.1: The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external & internal interfaces while remaining available for primary use. 5.2 The security architecture applies defence-in-depth & segmented techniques 3.3 There is an active programme in place to identify critical vulnerabilities	• Enforce Boundary Defences and Access Control between safety critical systems, other vehicle systems and those systems providing connectivity or external access. o The use of combinations of gateways, firewalls, intrusion prevention or detection systems, and monitoring are employed to defend systems. • Least privilege rule for access to vehicle systems should be implemented ensuring devices should provide only enough connectivity to enable it to operate for its desired function. o Only allow a safe set of instructions to be passed to a vehicle o Apply message and device authentication techniques o Implement appropriate Data controls o The information system performs an integrity check of software, firmware, and information at defined states (startup; restart, shutdown, and abort).	U2: Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain. U7: The storage and transmission of data is secure and can be controlled.

Category of Threats

- Compromise of back-end server
- Internal Communication channels used to attack a vehicle
- Update process used to attack a vehicle
- Human factor and social engineering
- Compromise of external connectivity
- Target of an attack on a vehicle
- System design exploits (inadequate design and planning or lack of adaption)
- Data loss / "data leakage" from vehicle
- Physical manipulation of systems to enable an attack
- Vehicle used as a means to propagate an attack
- Communication loss to/from vehicle (potentially out of scope as not cyber security)

Example of vulnerability or attack methodology for "Compromise of external connectivity"

1. Manipulation of telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
2. Interference with short range wireless systems or sensors
3. Corrupted applications, or those with poor software security, used as a method to attack vehicle systems
4. External interfaces such as USB or other ports may be used as a point of attack, for example through code injection …
5. Virus from infected media connected to system
6. Utilise diagnostic access (e.g. dongles in OBD port) to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)

Proposed Mitigations

Mitigations
1. Access to files and data shall be authorized
2. Best practices for backend systems shall be followed (e.g. OWASP, ISO 27000 group)
3. Confidential data shall be encrypted
4. Cybersecurity best practices for software and hardware development shall be followed
5. Cybersecurity best practices shall be followed for storing private keys
6. Data protection best practices shall be followed for storing private and sensitive data. Data protection regulations of individual countries shall be adhered to.
7. Data shall be (end-to-end) authenticated and integrity protected
8. Internal messages shall contain a freshness value
9. Internal/Diagnostic messages shall be authenticated and integrity protected
10. Measures to detect intrusion are recommended
11. Measures to detect unauthorized privileged access are recommended
12. Measures to ensure the availability of data are recommended
13. Organizations shall ensure the defined security procedures are followed
14. Software and configuration shall be authenticated and integrity protected
15. The certification policy for V2X communication shall be followed.
16. V2X messages shall be Authenticated and Integrity protected
17. V2X messages shall contain a freshness value
18. V2X messages should be checked for plausibility

Part 1 – Summary of the statements for security controls(1)

1. Security Controls shall be applied to back-end systems to minimise the risk of insider attack
2. Security Controls shall be applied to back-end systems to minimise unauthorised access
3. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage
4. Security Controls shall be applied to minimise risks associated with cloud computing
5. Security Controls shall be applied to back-end systems to prevent data leakage
6. Systems shall implement security by design to minimise risks
7. Access control techniques and designs shall be applied to protect system data/code
8. Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data
9. Measures to prevent and detect unauthorized access are employed
10. Messages processed by a receiving vehicle shall be authenticated and integrity protected
11. Cybersecurity best practices shall be followed for storing private keys
12. Confidential data transmitted to or from the vehicle shall be protected

Part 1 – Summary of the statements for security controls(2)

13. Measures to detect and recover from a denial of service attack shall be employed
14. Measures to protect systems against embedded viruses/malware are recommended
15. Measures to detect malicious internal messages are recommended
16. Secure software update procedures are employed

---

17. *Cybersecurity best practices shall be followed for defining and controlling maintenance procedures*
18. *Cybersecurity best practices shall be followed for defining and controlling user roles and access privileges*
19. *Organizations shall ensure security procedures are defined and followed*
20. *Security controls are applied to systems that have remote access*
21. *Software shall be security assessed, authenticated and integrity protected*
22. *Security controls are applied to external interfaces*
23. *Cybersecurity best practices for software and hardware development shall be followed*
24. *Data protection best practices shall be followed for storing private and sensitive data*
25. *Systems should be designed to be resilient to attacks and respond appropriately when its defences or sensors fail*

Part 2 – Headline statements with example controls (1)

1) **Security Controls shall be applied to back-end systems to minimise the risk of insider attack**

Ref: OWASP and ISO/IEC 27000 series.

Controls may include:

- Role based access controls ("need to know" principle, "separation of duties") and appropriate training for staff
- Staff activity logging/ monitoring mechanisms
- Security information and event management
- Dual control principle

- Note: applies to threat examples 1, 5
- OWASP: *Open Web Application Security Project*

Part 2 – Headline statements with example controls (2)

2) Security Controls shall be applied to back-end systems to minimise unauthorised access

Ref: OWASP and ISO/IEC 27000 series.

Controls may include:

- Securely configuring servers (e.g. system hardening)
- Protections of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels
- Monitoring of server systems and communications
- Manage the risks and security of cloud servers (if used)
- Security information and event management
  - Note: applies to threat examples 2, 7

Part 2 – Headline statements with example controls (3)

3) Where back-end servers are critical to the provision of services there are recovery measures in case of system outage

Example Security Controls can be found in OWASP and ISO/IEC 27000 series.

- Note: applies to threat examples 4, [34]

4) Security Controls shall be applied to minimise risks associated with cloud computing

Ref: OWASP and ISO/IEC 27000 series, NCSC cloud computing guidance.
Controls may include:

- Monitoring of server systems
- Managing the risks and security of cloud servers
- Applying data minimisation techniques to reduce the impact should data be lost
- Security information and event management

- Note: applies to threat example 6

Part 2 – Headline statements with example controls (4)

5) Security Controls shall be applied to back-end systems to prevent data leakage

Example Security Controls can be found in OWASP and ISO/IEC 27000 series.

Controls may include:

- Appropriate procedures for handling, transferring and disposing of data assets
- Appropriate training for staff, especially those handling data assets
- Applying data minimisation and purpose limitation techniques to reduce the impact should data be lost

- Note: applies to threat example 9

Part 2 – Headline statements with example controls (5)

6) Systems shall implement security by design to minimise risks

Controls may include:

- Access control to vehicle files and data
- Network segmentation and implementation of trust boundaries
- System monitoring
- Software testing
- Active memory protection
- Software integrity checking techniques
- Hardening of e.g. operating system

- Note: applies to threat example 12

Part 2 – Headline statements with example controls (6)

25) Systems should be designed to be resilient to attacks and respond appropriately when its defences or sensors fail

Example security controls can be found in OWASP and ISO/IEC 27000 series.

Controls may include:

- Redundancy or back-ups designed in, in case of system outage
- Security risks are assessed and managed appropriately and proportionately
- Measures to ensure the availability of data are recommended
- Safety critical systems are designed to fail safe
- Systems to detect and respond to sensor spoofing

- Note: applies to threat examples [82, 83, 84, 85, 86]

Part 3 – List of example controls identified (1)

The follow are example controls identified. They are grouped into similar themes. The themes are given in italics. These themes have been created by the author as a means of identifying similar controls.

Access control

- Establishing trust boundaries and access controls
- Apply least access principle to minimise risk.
- Role based access controls ("need to know" principle, "separation of duties") are established and applied
- Access control and read/write procedures established for vehicle files, systems and data.
- Access control rights established and implemented for remote systems to a vehicle
- Enforce Boundary Defences and Access Control between external interfaces and other vehicle systems
- Enforce Boundary Defences and Access Control between hosted software (apps) and other vehicle systems
- Dual control principle
- Multi factor authentication for applications involving root access

Part 3 – List of example controls identified (2)

Cryptographic key management

- Actively manage and protect cryptographic keys
- Effective key management and protection for any cryptography used

Control of data held on vehicles and servers and communicated therefrom

- Implement appropriate data controls
- Apply data minimisation and purpose limitation techniques to reduce the impact should data be lost
- Data minimisation techniques applied to communications
- Establish a policy on the use of cryptographic controls for protection of information are developed and followed. This includes an identification of what data is held and the need to protect it.
- Secure storage of sensitive information
- Encrypt sensitive data and ensure keys are appropriately and securely managed
- Systems are designed so that end-users can efficiently and appropriately access, delete and manage their personal data
- Strict write permissions and authentication measures for updating/ accessing vehicle parameters
- Active memory protection
- Apply techniques to prevent fraudulent manipulation of critical system data
- Consider use of Hardware Security Module (HSM), tamper detection, and device authentication techniques to reduce vulnerabilities

Part 3 – List of example controls identified (3)

Device and application authentication

- Apply device authentication techniques
- Authentication of devices and equipment
- Device configurations to be verified
- Procedures established for what applications may be permitted, what they can do and under what conditions

Controls for messages

- Message authentication and integrity checking
- Only allow a safe set of instructions to be passed to a vehicle
- Input validation for all messages
- Application based input validation (in terms of what kind of data/input the affected application is expecting)
- Authentication of data
- Check size of received data
- Consistency checks using other vehicle sensors (e.g. temperature, radar…)
- Employing rate limiting measures based on context
- Limiting and monitoring message content and protocols
- Setting acknowledgement messages for V2X messages (currently not standardised)
- Techniques to prevent replay attacks, such as timestamping and use of freshness values
- Timestamping messages and setting expiration time for messages

Part 3 – List of example controls identified (4)

Software coding

- Organisations adopt secure coding practices
- Apply software testing and integrity checking techniques

End of life considerations

- Appropriate procedures for handling, transferring and disposing of data assets
- Define measures to ensure secure deletion of user data in case of a change of ownership

Training

- Specific cyber awareness and security training needs are identified for roles, especially those in the design and engineering functions, and then implemented
- There is a security programme defining procedures
- Appropriate training for staff, especially those handling data assets
- Appropriate training of maintenance staff
- Establish security development and maintenance process including e.g. review, cross-check and approval gateways

Part 3 – List of example controls identified (5)

Network design

- Avoid flat networks (apply defence in depth, isolation of components and network segregation)
- Network segmentation and implementation of trust boundaries
- Protections of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels
- Sandboxing for protected execution of 3rd party software
- The use of combinations of gateways, firewalls, intrusion prevention or detection mechanisms, and monitoring are employed to defend systems

Monitoring

- System monitoring for unexpected messages/behaviour
- Enacting proportionate physical protection and monitoring
- Monitoring of server systems and communications
- Systems to detect and respond to sensor spoofing
- Session management policies to avoid session hijacking

Encryption of communication and software

- Encryption for communications containing sensitive data, including software updates
- Encryption of software code

Part 3 – List of example controls identified (6)

Controls for updates

- Secure communications used for updates
- Implement Cryptographic protection and signing of software updates
- Implement the use of configuration templates and policies
- Ensure configuration control and that it is possible to roll-back updates
- Version and timestamp and logging of updates
- Ensure the veracity of the update
- Establish secure update procedures, including configuration templates and policies for updates. Ensure configuration control and that it is possible to roll-back updates. Version and timestamp and logging of the update

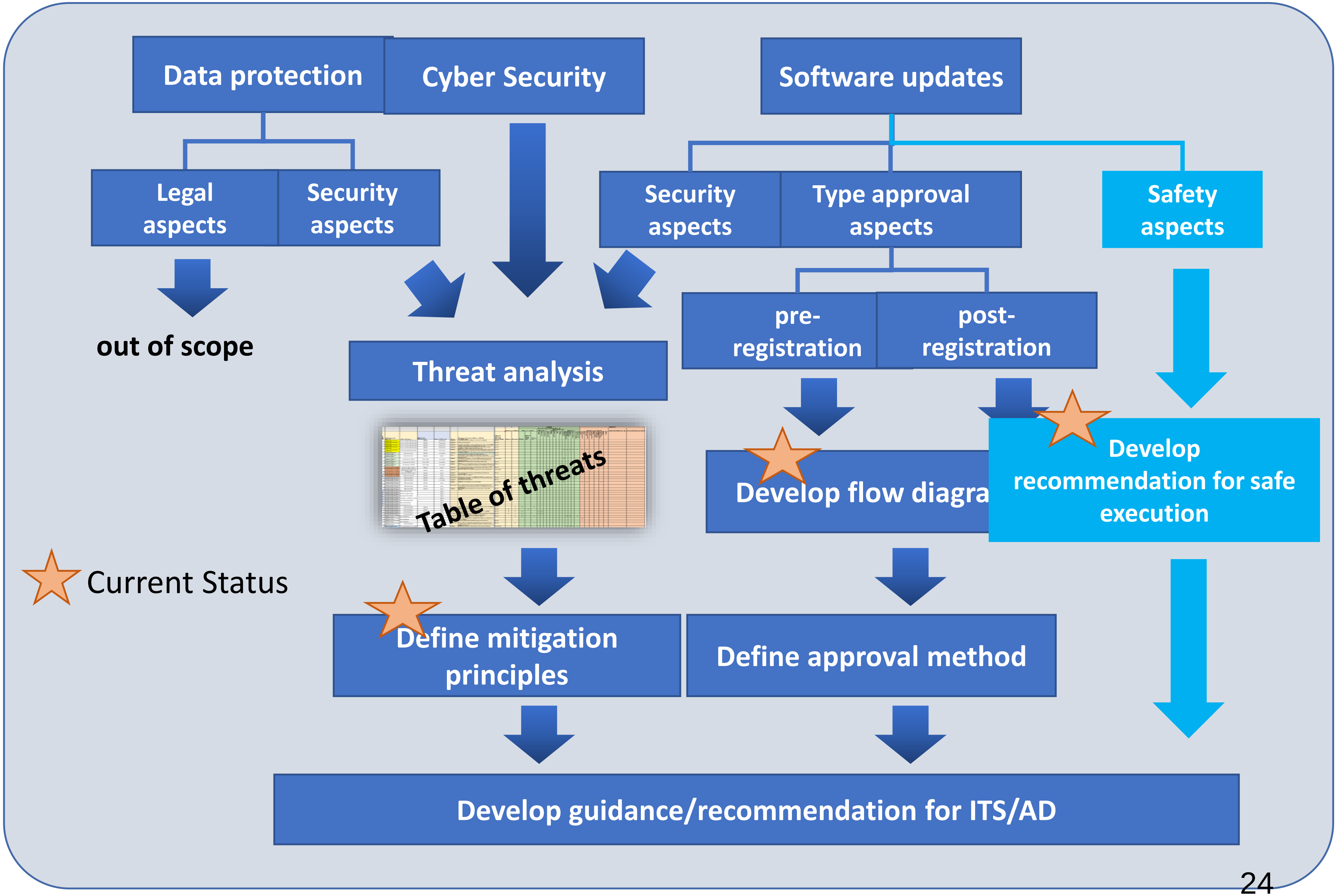
Software Update (OTA)

- Requirements and interim solutions proposed in Paris for documentation

  - **Pre-registration**
    - Type approvals (extended or newly obtained) are linked to the Whole Vehicle Type Approval (WVTA).
    - Documented in the Certificate/Document of Conformity (CoC/DoC).
      - Requirement for both **hardware and software information** to be provided.

  - **Post-registration**
    - A transparent documentation of the modification is needed.
    - This can be achieved by an „extension" of the CoC/DoC of **the vehicle detailing the changes**
    - With such documentation, changes of the registration can be performed according to national processes.

General Flow of works in WP29/TFCS and OTA



Data protection

Cyber Security

Software updates

Legal aspects

Security aspects

Security aspects

Type approval aspects

Safety aspects

out of scope

Threat analysis

pre-registration

post-registration

Table of threats

Develop flow diagra

Develop recommendation for safe execution

Current Status

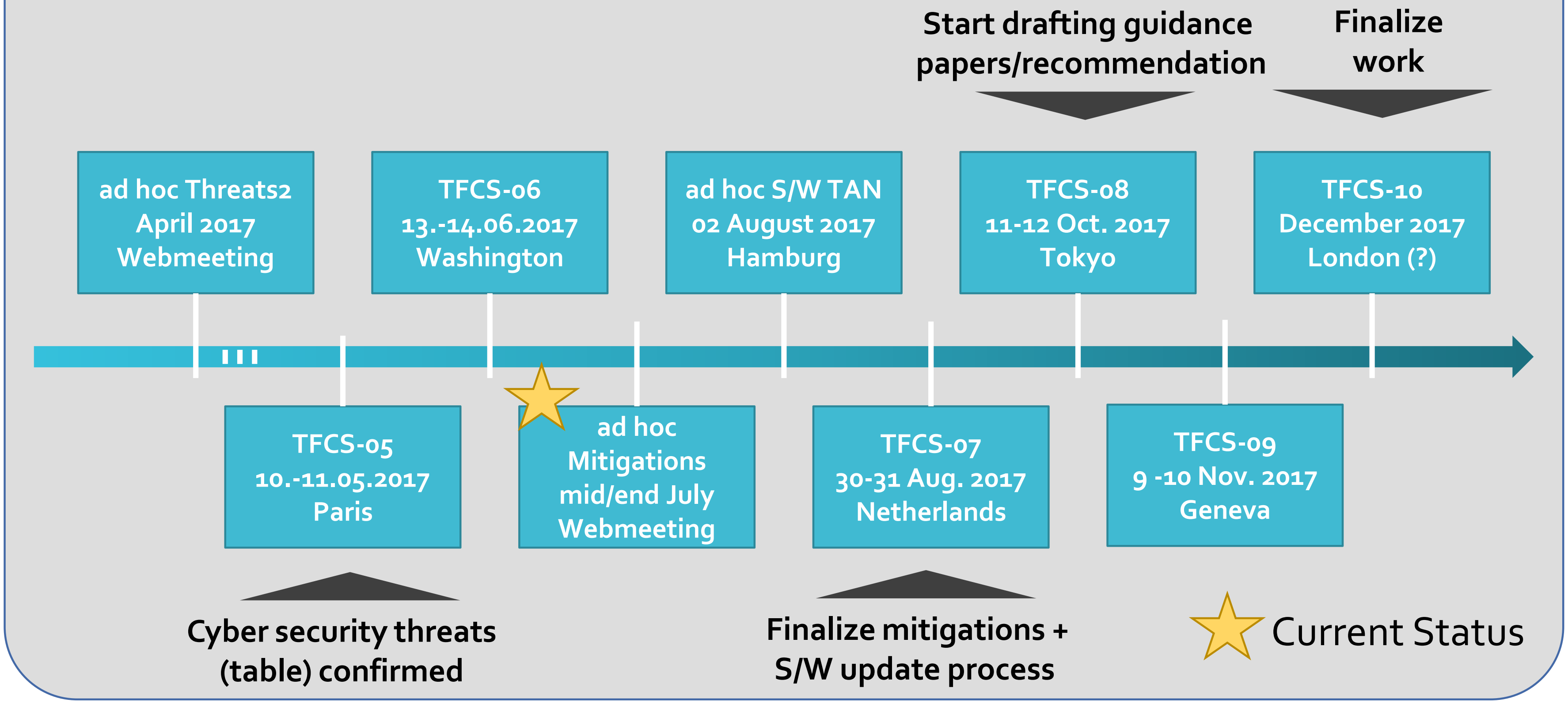
Define mitigation principles

Define approval method

Develop guidance/recommendation for ITS/AD

Schedule for output from WP29/TF

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-05
10.-11.05.2017
Paris

TFCS-06
13.-14.06.2017
Washington

ad hoc
Mitigations
mid/end July
Webmeeting

ad hoc S/W TAN
02 August 2017
Hamburg

TFCS-07
30-31 Aug. 2017
Netherlands

TFCS-08
11-12 Oct. 2017
Tokyo

TFCS-09
9 -10 Nov. 2017
Geneva

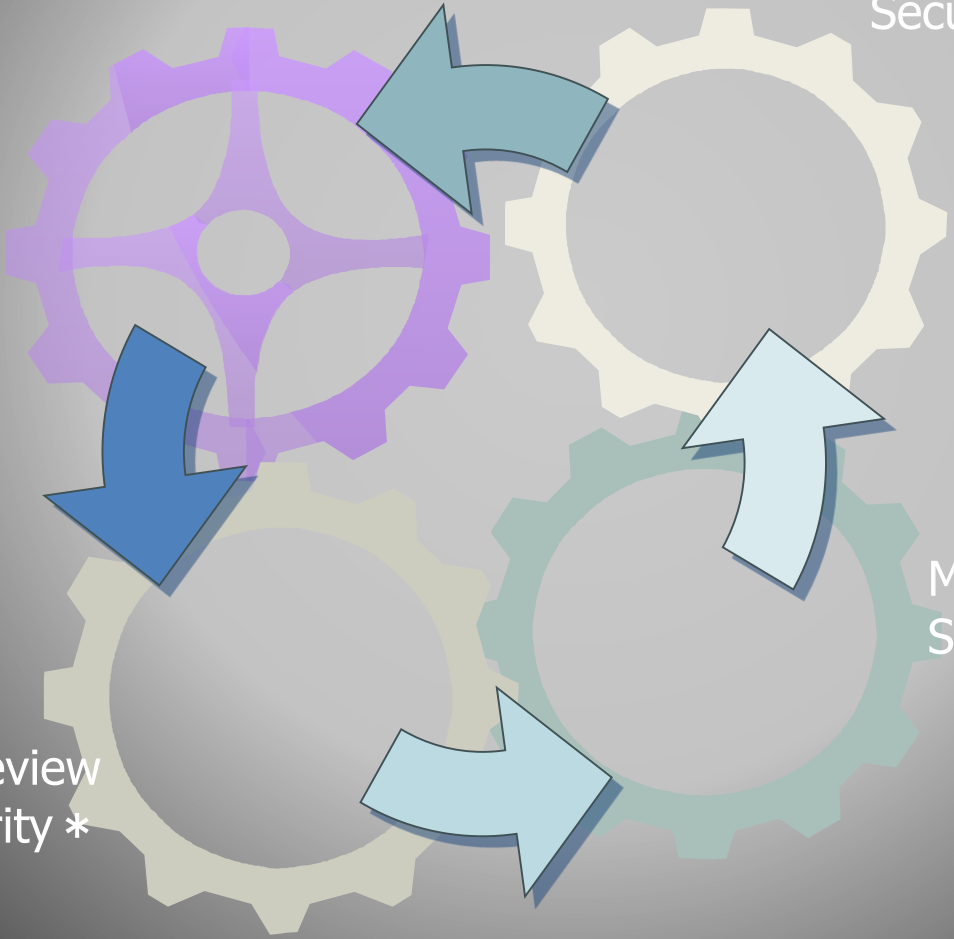
TFCS-10
December 2017
London (?)

Cyber security threats (table) confirmed

Finalize mitigations + S/W update process

☆ Current Status

Thank you for listening Q&A



Implement & use
Security *

Design
Security *

Maintain & improve
Security *

Monitor & review
Security *