Submitted by the Chair of the
Task Force on Cybersecurity and OTA (software updates)

Informal document **GRVA-03-02**
3rd GRVA, 3-4 June 2019
Agenda item 4(a)

Overview of the recommendations on cyber security

Content

1. Background
2. Cyber Security
3. Ongoing work - the test phase

Background

- The remit of the group was to produce
  - a recommendation addressing cyber security issues
  - develop outputs for use as a regulation or resolution
- How the recommendations were developed
  - The group contained experts from Contracting Parties and NGO‘s (CITA, FIA, ITU, OICA, CLEPA, ISO and others)
  - Thirteen meetings were held to agree the proposed recommendations plus twenty-one ad-hoc meetings
- Work started on 21 December 2016

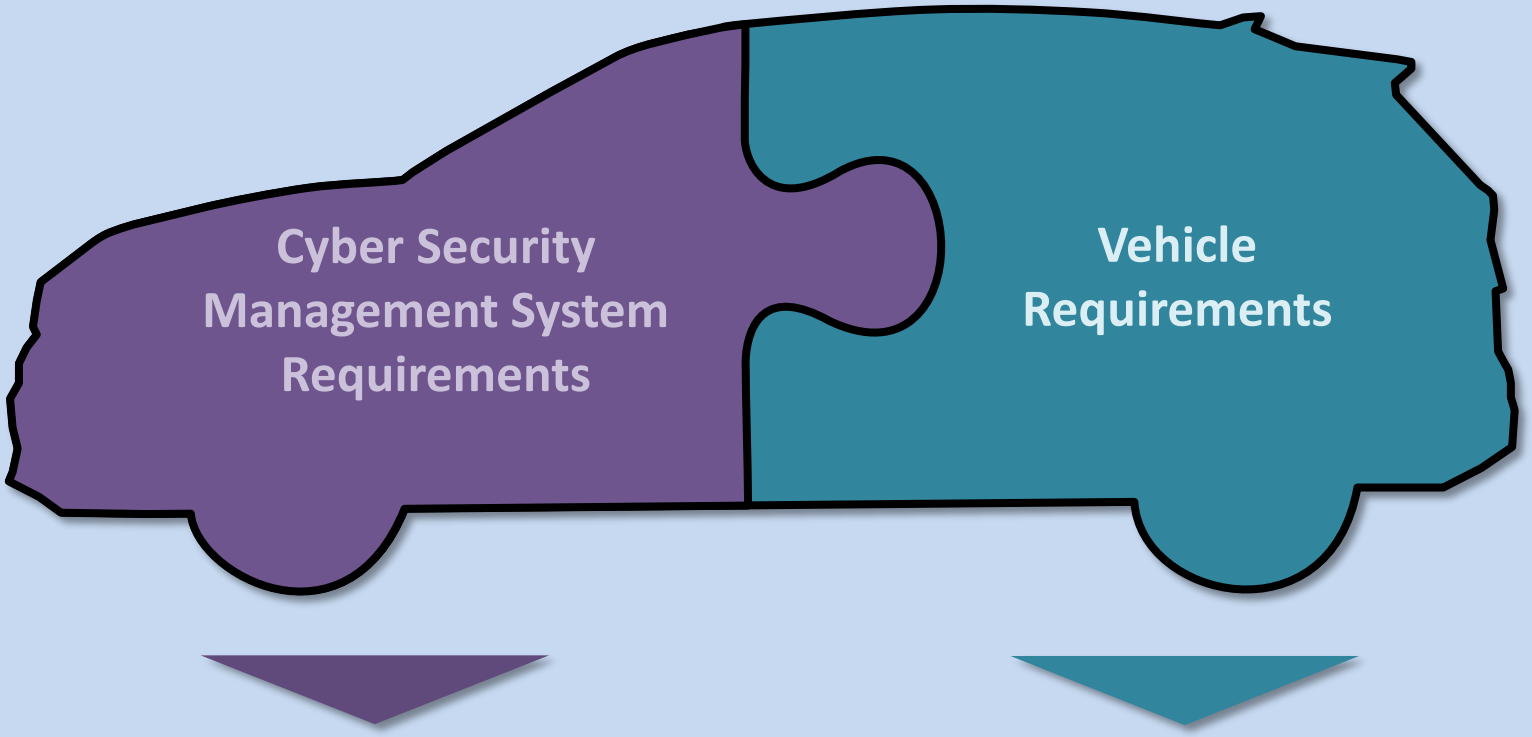
2. The Cyber Security recommendation

New approach: Certification of OEM‘s organization & processes

The group developed a split approach for the cyber security assessment:

i) Assessment of relevant vehicle manufacturer management system

ii) Assessment and certification of vehicles



Structure of the Recommendation on Cyber Security

Cyber Security Guidance (chapters 1-6, Annex B and Annex C)

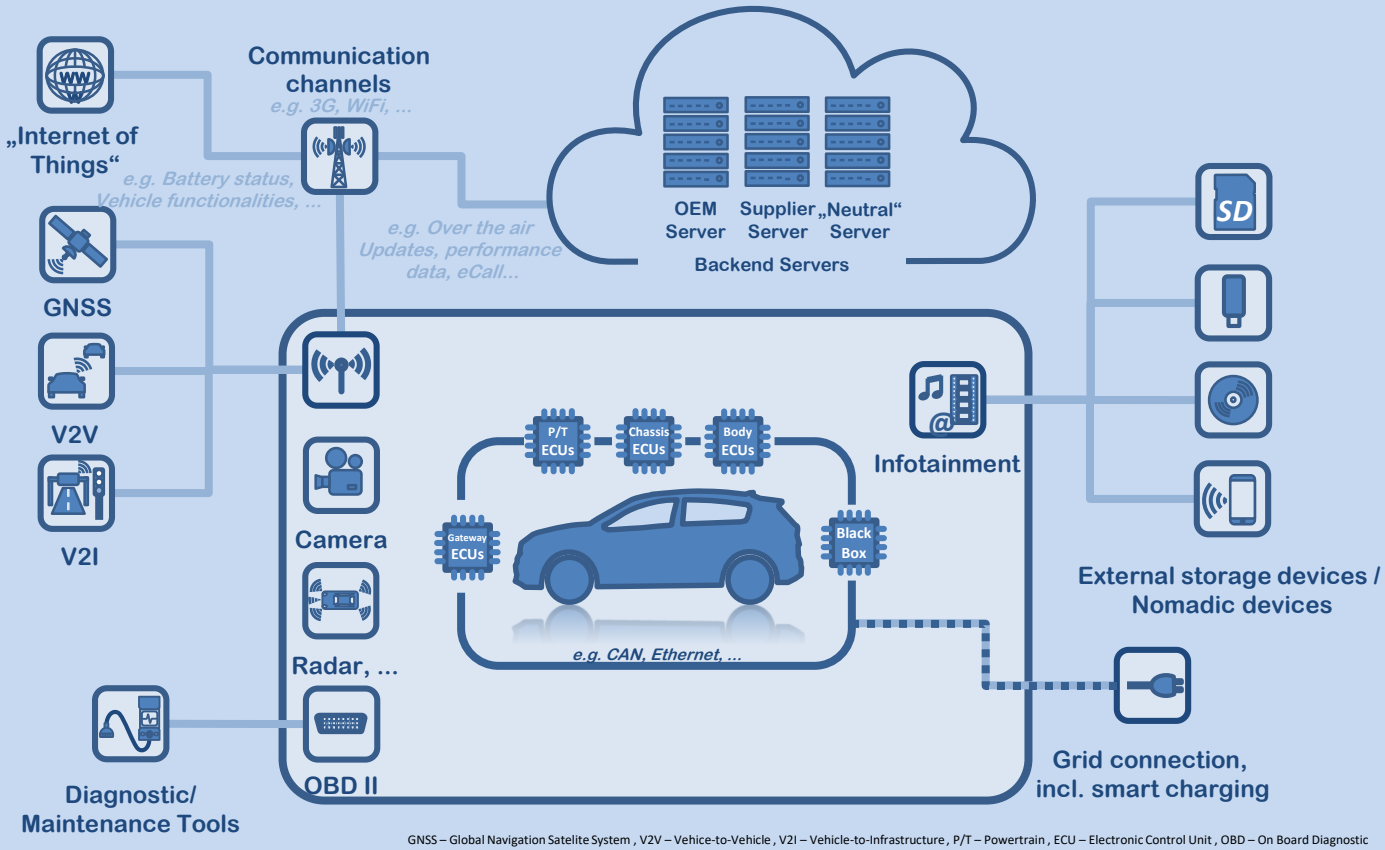
- *Sets out what good cyber security looks like through 10 principles*
- *Describes a range of threats that should be considered in the design of a vehicle*
- *Describes possible controls that could be used to mitigate risks*

Cyber Security Regulatory Proposal (Annex A)

- *Requirements for vehicle manufacturers "cyber security management system"*
  - *Processes cover all phases of a vehicle life until scrappage*
  - *Processes required include: organisational structure; risk management processes; design processes; verification processes; monitoring; and response*
  - *Includes processes for managing suppliers*
- *Requirements for vehicle assurance for cyber security certification*
  - *Vehicle architecture and connectivity needs to be described*
  - *Assurance provided based on a manufacturer's risk assessement, what controls have been implemented to reduce risks, and other evidence provided to demonstrate that the requirements are met*

Scope of the cyber security proposal – confined to the vehicle!

The picture below represents the interaction of a vehicle with external systems and what could be assessed during vehicle certification.



GNSS – Global Navigation Satelite System , V2V – Vehice-to-Vehicle , V2I – Vehicle-to-Infrastructure , P/T – Powertrain , ECU – Electronic Control Unit , OBD – On Board Diagnostic

Note: the picture is not a representation of a required vehicle architecture

Scope of the cyber security proposal – level of detail

Are there detailed technical measures mandated?

No.

The proposal was drafted in a technology neutral way. This should give some flexibility to vehicle manufacturers to decide how to ensure the cyber security of their vehicles.

A rigid definition of technical measures could be counterproductive, since the cyber security environment is a very dynamic one. The risk is that any detailed technologies which are mandated could become outdated/vulnerable and may block alternative, innovative, approaches and therefore limit or counter the possibilities to ensure cyber security. There is also a risk that a given solution may not be applicable to all vehicle designs. Thus the proposal might force unsuitable technologies on vechicles.

Noting that guidance may be valuable in this area, the proposal and annexes do include principles and mitigation measures which could be used. These are still at a low level of detail.

How to obtain Cyber Security certification

Step 1: Certification of the OEM‘s organization and processes - implementation and assessment of the Cyber Security Management System (CSMS)

OEM implements a CSMS

- **Organization & processes implemented** to ensure cyber security over the **development, production and post-production phase** and to cover the **entire supply chain**
- It includes e.g. **processes to identify, assess and categorize risks, processes used for testing the security, for monitoring, detection and response and processed used to keep cyber security current**
- The CSMS may be based on **ISO/SAE 21434** „Cyber security engineering“

Assessment of the OEM‘s CSMS

- **National or Regional Authority assesses the CSMS** of the vehicle manufacturer and whether it is compliant to requirements

Issuance of a CSMS Certificate of Compliance

- The **CSMS Certificate of Compliance** is the **prerequisite** to obtain a **cyber security certification**, linked to vehicle architectures
- The **CSMS Certificate of Compliance** has a **max. validity of 3 years**
- **National or Regional Authority** may at any time **verify** its **continued validity** and act appropriately if the requirements are no longer met.

How to obtain Cyber Security certification

Step 2: Vehicle certification- Development and Production to be in accordance with the CSMS

OEM develops the vehicle architecture

- During the **development and production** the vehicle manufacturer has to **employ the CSMS processes** to ensure cyber security
- **Risk assessment** to be conducted
- **Security/protection measures** to be implemented
- The **effectiveness** of security measures implemented needs **to be tested and verified**

Assessment of the vehicle

- **National or Regional Authority assesses the vehicle** and whether it is compliant to the requirements

Issuance of certification

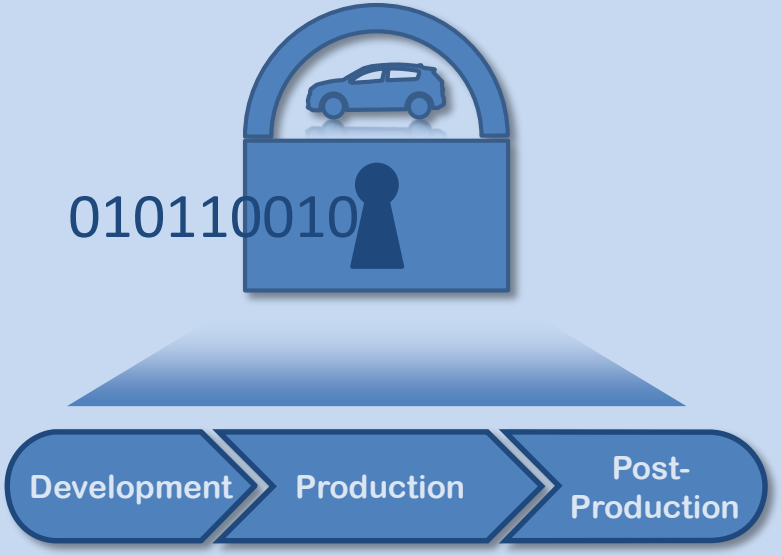
- Requirements are established to ensure conformity of vehicles being produced

How to maintain compliance in the post-production phase?

Cyber security shall be ensured **over the lifetime** of the vehicle. This implies e.g. that **cyber security** measures will have **to be updated** while the vehicle is in use.

Things to note:

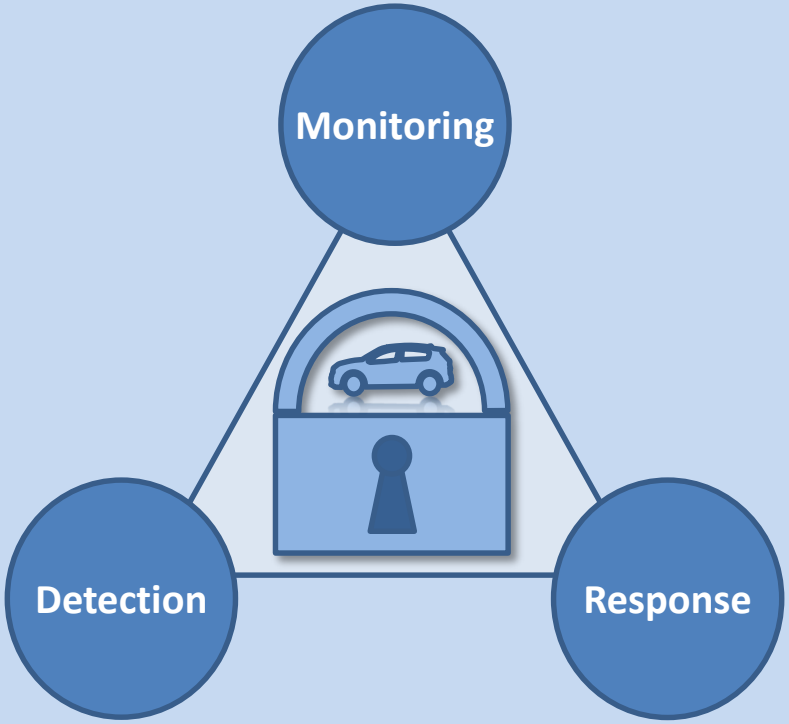
- New approach, not yet implemented in UN Regulations or GTR's
- Different to "durability requirements" where requirements have to be met after 160000 km of use
- It is technically and economically challenging to predict changing environment over time and the future resource needed. For example at a certain point of time more than software updates may be required to ensure cyber security.



How to maintain compliance in the post-production phase?

The vehicle manufacturer has to ensure that the processes of the CSMS, based on the requirements, are executed. The key requirements are monitoring for potential cyber attacks, detection of them and having a well exercised response plan.

Within the response plan the manufacturer may define a range of reponse options to pre-defined situations and trigger points for them. Implementation of some options (such as reducing vehicle functionility) may need discussion with regulatory bodies.



Summary of the proposal

- What the proposal does:
  - Provides a global baseline for vehicle cyber security
  - Ensures best practice is incorporated into the design of vehicles
  - Requires vehicle manufacturers to provide a reasoned argument as to why their vehicles are cyber secure (and the structure by which this should be done)
  - Ensures there is ongoing support for vehicles post-production

- What the proposal does not do:
  - "Gold plate" by specifying specific vehicle designs or technologies
  - Ensure vehicles cannot be hacked. No measure will be able to do this. The approach suggested will ensure the risk is minimised.
  - Secure systems that interact with a vehicle but are outside of the vehicle manufacturer's control (such as telecom networks or dongles)
  - Specify how long monitoring and response procedures should be in place or what they should be
  - List all possible risks and mitigations

Questions & Answers

1. How is the post-production phase covered?

Assurance assessment of a vehicle is not used for assessing post-production support as it is a test of a given configuration at a given point in time. It is therefore unsuitable for assessing ongoing processes. Instead the Cyber Security Management System (CSMS) is used.

Post production is addressed by the requirements for the CSMS

- Vehicle manufacturers have to show the processes they implement to ensure cyber security during the development, production and post-production phase.
- Requirement 7.2. of Annex A specifies, that the manufacturer has to implement processes to monitor for, detect and respond to cyber attacks.
- This includes demonstrating how they will monitor for, and react to, new and evolving cyber threats.

Consequence of non-compliance
If a vehicle manufacturer fails to maintain their CSMS, or serious deficienes are noted in it (for instance they are unable to detect or respond to a cyber attack) the national or regional authority may take appropriate action. This may include withdrawing the certificate.

Without a valid CSMS Certificate of Compliance the manufacturer would no longer able to apply for a new vehicle certification for Cyber Security. Continued production of existing certified vehicles may also be affected.

Questions & Answers

2. Why is there not a fixed length of time for how long vehicles should be supported?

There are a number of reasons, including:

- What needs to be supported to maintain cyber security may vary depending on the vehicle architecture/design.
- Such a requirement cannot be adequately assured at the point of certification for a given vehicle, especially for an extended period of time e.g. 25 years (manufacturers may struggle to demonstrate that they and their supply base would exist for such a period).
- Cyber security certification may not be relevant for vehicles no longer in production (=> production definitely discontinued).
- Some methods of support, such as indefinite software support, may be impractical.

Some existing national/regional laws may supercede any stated UN requriement. This is comparable to serviceability, e.g. how long spare parts have to be provided. There are legal obligations are dealt with on national/regional basis. Examples of legislation which may be applicable include:

- EU legislation on product liability (10 years)
- National legislation on recalls (can be indefinite)

Recommendation:
The issue, if of interest, will have to be addressed by the national/regional jurisdictions or UNECE may decide to develop a harmonized framework on this topic.

Questions & Answers

3. What if a vehicle manufacturer is unable to maintain the support for a given vehicle?

The regulations do not address this. The issue is comparable to recalls due to safety/non-complaince issues. Such legal obligations are today dealt with on national/ regional basis.

A lack of support will not automatically make a vehicle unsafe/not secure and vice versa. For all vehicles there is a risk that there is a vulnerability which may be exploited. The risk will depend on possibility of an exploit, the ability/willingness of people to use it, and its outcome. A vehicle will only definitively become unsafe if there is a vulnerability found which has been exploited to affect its safety. A vehicle will be at risk of such exploitation until the vulnerability is fixed. The fix will depend on the vulnerability and its exploitation. Support should reduce the chance of a vulnerability being found and exploited but will not negate such risks.

Under existing legal frameworks, it is up to an authority to decide whether a security issue requires the decommissioning of a vehicle, under which circumstances, with all it‘s consequences. This could be achieved on a case-by-case decision, dependent on the severity of the issue, number of vehicles affected, etc.

Recommendation:
The issue, if of interest, will have to be addressed by the national/regional jurisdictions or UNECE may decide to develop a harmonized framework on this topic.

Questions & Answers

4. Are there detailed test procedures specified for checking the cyber security of a vehicle?

   No. Without knowing the system being submitted it is difficult to define detailed test procedures suitable for an assessment, especially due to the high complexity of vehicle systems.

   An alternative approach was adopted. This is that the vehicle manufacturer shall provide a reasoned argument regarding the sufficiency of their measures and testing. This provides an appropriate method to certify a Cyber Security Management System and the ability to check which measures the vehicle manufacturer has implemented to ensure cyber security for a given vehicle.

   An interpretation guidance document is being written during a test phase to help provide a consistent approach to assessments.

   The recommendation section and annexes do include principles and mitigation measures which could be used for reference for during assessments.

Questions & Answers

5. How will the risks and mitigations listed in Chapters 4 and 5 and their corresponding Annexes B and C be maintained?

Both sections note that they are not definitive and vehicle manufacturers should consider other sources to maintain an up to date appreciation of all possible risks and mitigations.

The maintenance of these sections could be achieved through a number of options, including:

- Standards bodies (or other suitable bodies) could maintain the lists
- WP29 could re-convene the working group periodically to update the lists if others are not adequately doing so

Recommendation:
The issue, if of interest, should be considered in line with the recommendations in chapter 7 of the Recommendation.

3. Overview on the test phase

Next step – testing the proposal

Aim of the „test phase“

=> Provide guidance on how to assess the requirements and documentation required

=> Verify the effectiveness/robustness of the requirements

=> Verify that certification authorities are able to reach the same conclusions based on identical OEM documentation

Aim is to assure the proposal and not to test the products!

Overview

Outputs of the „test phase“

=> Interpretation guideline

=> If necessary, proposals for clarifying the proposal

=> Report of the test phase to cover:

- conclusions on the effectiveness /robustness of the proposal
- verification that certification authorities/ are able to reach the same conclusions

Proposed timeline for the test phase