## Tasks and questions from GRVA on cyber security proposal

**(FIGIEFA and ETRMA comments are highlighted in green)**

### General working of the regulation

1. What does the regulation deliver that did not exist before?

   The current proposal is in answer to a request from the 13th session of the Informal Group on "ITS/Automated Driving", under item 3-2, asking that the Task Force on Cyber Security and Over the Air issues should:

   **Commented [DH1]:** From the minutes of that meeting

   "consider a regulation, in addition to a resolution that can be revised quickly in response to changes of threat."

   Current UNECE regulations do not consider cyber security. The proposed regulation will provide a mechanism to ensure that:

   - Cyber security is considered at a vehicle level when all systems are integrated
   - Manufacturers adopt a "secure by design" approach
   - Manufacturers can provide a "cyber security argument" for why their design is secure
   - Manufacturers are able to provide a planned response to a cyber incident should the need arise

   None of these are requirements harmonised globally

   **Commented [DH2]:** Based on GRVA-03-02

   FIGIEFA and ETRMA Comment: See document "General Documents on the Geneva approach" at the end of this document.

2. Can you clarify the purpose of the guidelines? We understand that it is mere recommendation by the task force, not binding for contracting Parties? Does it mean that Contracting parties shall agree with them?

   As stated in chapter 7 of the recommendation the purpose of the guidelines are to:

   **Commented [DH3]:** From the proposal

   Aid the assessment of the Cyber Security Management System, the risk analysis undertaken and the mitigations implemented through providing:

   - Cyber security principles which can be used to demonstrate how organisations should implement cyber security over the lifetime of the vehicle;
   - Examples of threats, risks, vulnerabilities and attack outcomes that should be considered;
   - Examples of mitigations that should be considered.

   A further part of the recommendation is to make specified chapters of the Cybersecurity document into a new Resolution (e.g. as RE3). It would have the same status as the other Resolutions:

   **Commented [DH4]:** Provided by OICA.

   **Commented [CK5R4]:** Depending on which Chapters will be included in a new Resolution; this should only be non substantive requirements. The legal value of a Resolution for the EU is the same as a UN Global Technical Regulation or a Technical Standard (CEN, ISO). In legal terms it is of paramount importance to lay down all substantial requirements in a UN Regulation under the 1958 Agreement.

   http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

   GRVA would need to confirm that they would want this.

3. The regulation does not seem to include a pass-fail criteria? On which basis will type-approval authorities decide if what is proposed by the manufacturer is acceptable or not?

   As stated in chapter 7 of the proposal:

   Demonstration of how the requirements, given in this recommendation, can be met should not be explicitly defined. Instead it is recommended that through the use of relevant standards, processes and implementing appropriate mitigations vehicle manufacturer should be able to evidence how they are meeting the requirements to the approval authority;

It was noted in the test phase that an explicit “pass-fail” criteria does not suit the evaluation of processes, nor the effectiveness and efficacy of test procedures which are seeking to validate the absence of something.

In terms of a pass-fail the following provide a rough guide to how this may function

- A fail for a CSMS might be realised through
  - an absence of a process or plan required within the CSMS
  - the inability to demonstrate/argue/evidence (as appropriate) that a process required within the CSMS will be utilised as intended
- A fail for a vehicle type approval may be realised through
  - the inability to describe a vehicle type appropriately
  - the inability to demonstrate/argue/evidence (as appropriate) that the processes required within the CSMS have been/will be applied to the vehicle type
  - the inability to demonstrate/argue/evidence the risk assessment applied to the vehicle type
  - the inability to demonstrate/argue/evidence the appropriateness of the risk treatment and any security measures applied to the vehicle type

FIGIEFA and ETRMA propose to amend:

  - The inability to support HW and/or SW updates that may become necessary to guarantee security over the lifetime of the vehicle;
  - The inability to support independent and unmonitored access to in-vehicle-data, functions and resources over a wired or wireless network communication for authorized parties according to regional or national legislation.

- A pass - will be based on manufacturers being able to demonstrate/argue/evidence how they are meeting the requirements

Suppliers

4. Is the OEM the only responsible party for the type approved systems? Can/should suppliers have CSMS certificates? Can they get approvals for subsystems?

Part 3.1 of the proposed regulation states:

“The application for approval of a vehicle type with regards to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.”

The Vehicle Manufacturer is the legal entity registering for initial assessment and requesting type approval. Thus, the legal entity is the responsible party.

In theory a supplier could register for an initial assessment and request a type approval. The regulation does not prohibit this. Although type approval for a sub-system would have limited value as a further approval would be required at the vehicle level should this be a part of the wider vehicle electronic architecture.

Similarly, the regulations do not prohibit a supplier from submitting for a CSMS.

Vehicle lifetime

5. Why did the task force choose its approach to vehicle lifetime and will it work in practice? What would be expected to happen in the case that incidents/vulnerabilities are identified?

FIGIEFA and ETRMA propose to amend:

Already the consumer association FIA raised this topic in the Task Force, as consumers need certainty on IT security of a vehicle, before they invest in new vehicles. The IT security over the lifetime will have significant impact on the value of a vehicle.
It has to be noted that due to the comparably (compared with e.g. smartphones or laptops) “long” lifetime of a vehicle it will not be enough to just foresee software updates/security patches as the method of choice to close security loopholes. Instead, attacks from increasingly powerful server hardware will force the necessity to exchange and update every hardware component that hosts vital security software (e.g. the Gateway software and hardware security module) to allow e.g. for stronger encryption whilst still fulfilling the timing needs of e.g. a CITS-application for collaborative driving.

Furthermore IT security also has an influence on road safety: Automated driving functions are intended to significantly increase road safety. However, these functions can only be used for as long as IT security is guaranteed. Otherwise, the functions will be deactivated and there will be no increase in traffic safety through automated driving functions. In addition to IT security, the market penetration of automated driving functions also has a major impact on increasing road safety.

6. Why does the regulation not state what the lifetime of the vehicle should be (for example 10 years after entry into service)?

This point has been discussed by the task force. The proposed regulation will require that vehicle manufacturers have to demonstrate how their Cyber Security Management System covers the Post-production phase (see paragraph 7.2.2.1).

**Commented [DH6]:** Based on OICA comment in GRVA.

This includes a number of sub-requirements, including:

- The ability to identify new and evolving cyber threats and vulnerabilities (7.2.2.2). This ensure manufacturers monitor for threats which are unknown at the time of type approval.
- The requirement to have a plan to respond should they need to. This may cover the scenarios where:
  - A vehicle type is still in production
  - A vehicle type is no longer in production but contractual arrangements exist with relevant suppliers to provide software support/updates
  - A vehicle type is no longer in production and there are no agreements with suppliers to provide support
  - Software, hardware or communications media become obsolete and cannot be maintained/replaced
- The plan shall also include processes for determining the appropriate course of action

During the task force meetings, a number of possible responses to a new threat or vulnerability were discussed. These range from the provision of software updates to patch vulnerabilities through to replacing hardware and software or removing/disabling functionality. If it is not possible to “fix” a problem and the vehicle is deemed unsafe, the ultimate solution will be for a road authority to declare it unroadworthy. ~~Conversely, in some circumstances a “do nothing” option may be appropriate. In the task force it was noted that the exact solution to a problem will depend on the problem itself and that the more~~

**Commented [CK7]:** FIGIEFA and ETRMA see the risk, that this situation may occur even for new vehicles, as long as there are no legal requirements on IT support over the lifetime

~~interventionist solutions might require a dialogue between a manufacturer and an appropriate authority to agree a course of action.~~

**Commented [CK8]:** FIGIEFA and ETRMA concur with the European motorist consumer association FIA and strongly suggests legal requirements instead of individual negotiations between vehicle manufacturers and local authorities. As the FIA pointed out on many occasions, consumers need transparency for the safety of their vehicles.

FIGIEFA and ETRMA suggest to replace the paragraph above by:

Vehicles need not only soft- but also hardware updates. The Task Force and GRVA should please decide about an extension of the mandate to include hardware updates, too.

Justification: As the German FIA member club (ADAC) showed, the Keyless Entry Systems are unsecure. By simply extending the range of the signals the vehicles can be opened and driven away. Only a change of soft- and hardware could solve the problem for the existing fleet. VW, Fiat, Honda, JLR, Kia and Volvo had vulnerabilities in key codes of millions of vehicles. Only regulated requirements will give consumers the certainty to drive secure vehicles.

Cybersecurity is not like the wear of parts that have to be replaced periodically (tyres, brake pads, etc.). It is unpredictable. At the time of the launch of a new vehicle type, the number and types of cyberattacks during the possibly 30-50 years of vehicle use (of that vehicle type) are unpredictable. The exact length of time that a vehicle type will be on the road is also unpredictable, with many vintage vehicles still being present and the average life of vehicles ranging from 15 years upwards. It was also noted that in some jurisdiction a manufacturer will be expected to react to a cyber threat, regardless of whether a vehicle is under warranty or not. In others there is already legislation covering this issue.

**Commented [CK9]:** FIGIEFA and ETRMA strongly reject the notion that IT is generally different in terms of security than all other elements of the car. Instead, with a sound concept of "updateable hardware by design" for all core security hardware elements and an organization that keeps the software standards for security up to date, a vehicle can be safely kept on the road for decades in a combination of frequent software updates and less frequent (e.g. every 3 years during PTI) hardware updates.

It was concluded it is not easy or necessarily effective to require a specific length of warranty in a UN Regulation for cyber security. The ability to monitor and respond was considered a more effective method.

**Commented [CK10]:** FIGIEFA and ETRMA suggest to have legally binding requirements for software updates rather than individual decisions of OEMs if they support cyber security updates or not.

In the case of safety issues, recalls will be done according to the procedure already in place in local/regional legislation. For example in Europe the framework regulation 2007/46/EC applies. As today, this recall procedure is defined at regional level (EU) and not at UN level.

**Commented [CK11]:** That is why FIGIEFA, ETRMA and other stakeholder associations strongly propose 'cybersecurity over the lifetime' at UN level. We need world-wide secured vehicles.

The task force concluded that ultimately if there was a safety issue due to a cyber vulnerability then the above legislation would apply so there is no need to mandate warranties or support.

**Commented [CK12]:** FIGIEFA and ETRMA understood that this was merely an OICA position

## Specific requirements

7. Why does the cyber security regulation not include some trust model requirements such as the gateway for accessing vehicle data?

There are several vehicle interfaces which could be used for cyberattacks. The exact number will depend on the vehicle design. The objective of the draft UN Regulation is to assess the cybersecurity of the whole vehicle and not to mandate specific solutions and security requirements for them. The trust model approach may lead to potential attack paths outside the gateway not being properly assessed and could introduce a single point of failure. Certification of a mandated gateway risks giving a pseudo-security which will not prevent cyberattacks via other communication channels.

**Commented [DH13]:** Based on OICA response

The number of interfaces will change in the future. For this reason, the UN Regulation requires that the vehicle manufacturer shows his cybersecurity management system and the cybersecurity of his declared vehicle type according to the interfaces on his specific vehicle.

FIGIEFA and ETRMA refute this OICA position

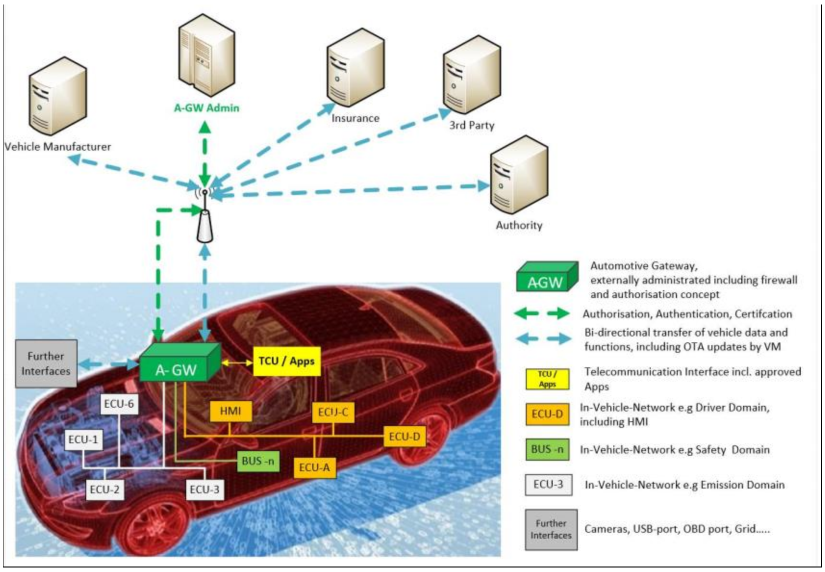
1. A Gateway *can* enable a safe & secure control of all interfaces of a vehicle! This holds true for interfaces to external communication partners (e.g. for V2X communication) as well as for the communication between applications in the vehicle and the vehicle's core systems (e.g. the ECUS or the HMI). However, an interface may be defined by national or regional legislation, so this Gateway may be required to support the functional requirements of a mandated interface for authorized parties.
2. As the trust model is technology neutral, a UN regulation should define the *functionality* of such a gateway, but not its very detailed technical specification. Additional functional requirements may be defined by national or regional legislation.
3. By using a common protection profile for the trust model including the gateway, the vehicle manufacturer stays free in the technical design as long as this design meets the protection profile. The protection profile can be checked by type approval authorities

To do this, the Gateway features the following basic security functionalities:

a. The Gateway verifies the identity of the calling system, may it be an electronic traffic light that sends a "Stop" signal or an internal application that requires a Diagnostics trouble code. "Who is calling?". This is usually realized by use of electronic certificates.
b. After a successful identification the Gateway determines what the caller "wants" (e.g. what function should be triggered or what value should be read from the car) and if the caller is generally entitled to do this according to the internal authorization concept.
c. As a final check prior to the execution of the request the Gateway checks if the command is allowed in the current state of the car. If the car's Bus system is currently already flooded with requests with a higher priority the request could be either queued and thus delayed, if the car is driving and the request can only be executed without risks in a parked state then the request would be declined for now with a related response to the caller.

Note: In some architectural designs, some or all of these concepts these functionalities are realized in subsystems called "Firewall" or "Hypervisor". The names might vary, the tasks are the same. The above description is purely functional, pure software and doesn't prescribe any hardware implementation details.

**The picture hereunder (on the next page) shows the Gateway in its role as a communication shell around the car's systems for external as well as internal calls:**


A-GW Admin
Vehicle Manufacturer
Insurance
3rd Party
Authority
Further Interfaces
A-GW
TCU / Apps
ECU-6
HMI
ECU-C
ECU-D
ECU-1
BUS -n
ECU-A
ECU-2
ECU-3
AGW
Automotive Gateway, externally administrated including firewall and authorisation concept
Authorisation, Authentication, Certifcation
Bi-directional transfer of vehicle data and functions, including OTA updates by VM
TCU / Apps
Telecommunication Interface incl. approved Apps
ECU-D
In-Vehicle-Network e.g Driver Domain, including HMI
BUS -n
In-Vehicle-Network e.g Safety Domain
ECU-3
In-Vehicle-Network e.g Emission Domain
Further Interfaces
Cameras, USB-port, OBD port, Grid.....

8. Cyber in the vehicle is only one aspect. Should the regulation include some other aspect such as **off-board authorization**, identification?

   Off-board systems are not part of the vehicle type approval as they are not part of the vehicle. The vehicle risk assessment should consider risks to the vehicle from such systems and any vehicle-borne security measures that might be needed to manage those risks.

   Off-board systems are considered within the Cyber Security Management System of the vehicle manufacturer. Requirements in paragraph 7.2 of Annex A does pertain to the security of such systems.

FIGIEFA and ETRMA suggest to amend:

**From a technical point of view on-board and off-board systems are combined.**

1. OICA members use off-board systems to protect the vehicles from cyber attacks.
2. At UN level, there is no need to define the *detailed technical specifications* of the off-board system, but to define the *functions* of the off-board system together with the on-board components. However, both these off-board and on-board specifications may also be defined by national or regional legislation to support the functional requirements of a mandated interface.
3. The modern vehicle is a connected vehicle. More and more functionality will be offered via new software versions (see e.g. TESLA's autopilot or new "Power on demand"-solutions by European OEMs in upcoming cars). And – like in the "normal"-IT, new software versions will be released to fix identified security issues or errors in previous versions. Thus, the security has to start in the offboard world where new software modules will have to be tested, certified and signed (e.g. by use of certificates) to allow their safe &secure integration into the car via software update. UNECE should also describe the general roles, rights and design principles of the off-board-systems and the processes by which the new software enters the vehicle.

## Consideration of other legislation

9. How will the regulation ensure compatibility with other legislation, such as:
   - data protection EU legislation
   - RMI legislation

   The vehicle manufacturer has to comply with all relevant regulations. He has to find the appropriate technical solutions that are compliant with them all. Same as for safety and environmental requirements that may be in conflict. The proposed Regulation will not and shall not replace other UN or regional legal requirements.

   With regards privacy, the UN Regulation is focused on technical requirements, GDPR on legal requirements. They are complementary. The type approved cybersecurity of a vehicle should prevent cyberattacks on private data. It will therefore protect the privacy of the vehicle user against cyberattacks. However, it is limited to technical aspects. What is private will be defined in GDPR and similar legislation.

   The EU RMI legislation defines requirements for how the vehicle manufacturer shall inform others about the possibility to repair his vehicles. This regulation does not deny this right.

**Commented [DH14]:** Based on OICA comment in GRVA.

FIGIEFA and ETRMA refute this OICA position:

1. The access to data, functions and resources for authorized parties must be technically ensured in the *design* of the vehicle and its internal networks. Therefore, an authorisation concept must be part of cyber security system of this UN regulation.
2. It is of course then up to national or regional legislation to determine authorised parties and the level of independent and unmonitored access to the vehicle, its data, functions and resources

10. Review the FIGIEFA paper (GRVA-03-16) and provide an assessment. Should the points raised be included in a cyber security / OTA Regs or is this is a separate issue?

    As per the point above. The legal requirements for access to data and right to repair are already stated and manufacturers will have to comply with them. Therefore it is recommended that this be treated as a separate issue.

FIGIEFA and ETRMA would like to amend:

The vehicle manufacturer shall demonstrate how they have implemented appropriate and proportionate measures to protect dedicated environments on the vehicle type (if provided) and have implemented for this vehicle type, according to national or regional legal requirements, these measures to ensure unmonitored and independent access by authorised parties for the storage and execution of aftermarket software, services, applications or data:

(a) Read data from a vehicle;

(b) Write data to a vehicle;

(c) Request ECUs to activate routines;

(d) Implement new routines from a third party;

(e) Install authorised software updates;

f) Enable the installation and function of OEM or independent replacement parts.

**Tasks and questions from GRVA on software update processes proposal:**

**General working of the regulation**

1. What is the purpose of the regulation, is it to provide a standardized identification of the software version used on the vehicle?
   The purpose of the regulation is to permit SW updates of the vehicle and to ensure the traceability and compliance of those SW updates with the regulations in force.

**Commented [DH15]:** Based on OICA comment from GRVA

FIGIEFA and ETRMA suggest to amend:

> In order to ensure the purpose of traceability and conformity, it is necessary to consider any SW updates and not only those declared by the manufacturer or suppliers.

2. Can you clarify the purpose of the guidelines? We understand that it is mere recommendation by the task force, not binding for contracting Parties? Does it mean that Contacting parties shall agree with them?
   As stated in 7.1.2 of the recommendation the purpose of the guideline is to provide a suggested process to manage software updates post-production. The guidelines describe a process whereby individual software updates, post-registration, can be assessed by a vehicle manufacturer and notified to an Approval Authorities or Technical Services when an update may affect any certified system or change any entry within the information document for the vehicle.
   The guidelines also elaborate on the processes described in the regulation to aid their implementation.

   A further part of the recommendation is to make specified chapters of the document into a new Resolution (e.g. as RE3). It would have the same status as the other Resolutions: http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html
   GRVA would need to confirm that they would want this.

**Commented [DH16]:** Provided by OICA.

3. Should we allow over the air software updates that will change the performance of the vehicle initially approved?
   As stated in 1.2.4:

   This recommendation applies to the legal framework for certification of vehicles. Since the process for managing and approving a software update after the initial type approval is granted and the process for vehicle registration is conducted according to national legislation, some recommendations will be handled by national legislation. Such parts of recommendation are not subjected to binding force of the UNECE 1958 Agreement.

   As stated in 1.2.5

   Software updates after the first registration by parties that are not the holder of the type approval/ certification are not covered by this document. These may be approved using national approval procedures.

   The guidelines provide a process for handling software updates that may change the performance of a vehicle initially approved. These suggest that the relevant approval authority/technical service should consider whether to grant an extension or require a new approval.

## RXSWIN

4. What is the purpose of the RXSWIN? How does it work?

As stated in the definitions (chapter 2) of the recommendation:

"RX Software Identification Number (RXSWIN)" means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.

Its purpose is to provide a means to reference what software is present within a vehicle type, for example firmware on ECU's and to provide a means to identify when there has been a software update which affects a given type designation. Where an extension is approved the reference number for that type designation should change. An example would be a software update affecting an ECU used in a braking system resulting in an extension being provide would necessitate a new version number for the RXSWIN of the braking system.

As it is a reference number the manufacturer is required to record all software versions which may pertain to a given RXSWIN.

FIGIEFA and ETRMA would like to amend:

To achieve the purpose of the RXSWIN to act as a reliable indicator for the present software the RXSWIN has to be complemented by its integrity validation data (see 7.1.2.3 of the draft regulation) for each use case, in particular also for the PTI. Otherwise (with the RXSWIN alone) dangerous tampering of software could not be detected.

5. Are there alternatives that could be used? If so, why are they not?

The proposed regulations require that for:

7.2.1.2 Where a vehicle type uses RXSWIN:

7.2.1.2.1 Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.

During the task force meetings alternatives were discussed. This include:

a) An alternative could be for the RXSWIN to update every time there is an update to software of a vehicle type, regardless of whether or not if affects type approval of a given system.

b) An alternative could be to provide on the vehicle version numbers for all software relating to a system type.

c) A final alternative would be just to list all software versions of all software on the vehicle.

The proposal provides a simpler way to verify that software is compliant with regulations, especially when there is a lot of updates.

It may be possible for manufacturers to provide an alternative solution (such as one of the above), and argue that it provides the same function as an RXSWIN.

FIGIEFA and ETRMA suggest to amend:

Alternative a) should be implemented in order to be able to actually assess a vehicle with regard to its installed software.

6. For a given software change, what would require a new RXSWIN?
   As stated above for 7.2.1.2.1 "the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval"
   It is recommended that the original type approval test be used as the basis of any assessment with regards to whether an update would change any of its results or parameters.

**Suppliers**

7. Is the OEM the only responsible party for the type approved systems?
   Part 3.1 of the proposed regulation states:
   "The application for approval of a vehicle type with regards to software update processes shall be submitted by the vehicle manufacturer or by their duly accredited representative."

   The Vehicle Manufacturer is the legal entity registering for initial assessment and requesting type approval. Thus, the legal entity is the responsible party.

   In theory a supplier could register for an initial assessment and request a type approval. The regulation does not prohibit this.

   Similarly, the regulations do not prohibit a supplier from submitting for a SUMS.

8. Can/should suppliers have SUMS certificates? Can they get approvals for subsystems?
   In theory yes to both. However, the utility of such a sub-system might be limited if the vehicle manufacturer utilises a different system to update a vehicle.

9. Could suppliers provide updates under the software update processes regulation?
   The proposed regulation provides for type approval for the software update mechanism for vehicles. It is expected that, as updates may come from suppliers, the software update mechanism described in a vehicle type approval for software updates will accommodate their needs. How this is achieved is to the discretion of the vehicle manufacturer and their suppliers.

* * * * * *

## Annex 1: FIGIEFA and ETRMA overall comment on the Geneva Approach (see pages 10-12)

**Summary:** We regard the approach as enshrined in the GRVA draft Regulation to ensure cybersecurity by just prescribing a development or process standard - without a precise set of quantifiable and measurable hard requirements and acceptance criteria for type approval - as insufficient and as potentially challenging the future vision of a collaborative mobility as well as for the envisioned Digital Single Market.

**Reasons:**

1.) Lack of standardization. If just the methodology or development process of a cyber security system is prescribed, but not vital elements of the system itself are standardized, then every OEM is free to come up with his specific, highly incompatible solution.
However, every Car2X or CITS use case requires that every network node in the future mobility network speaks exactly the same language in terms of context and format, uses the exact same level of encryption etc. So at least these elements need to be standardized to ensure interoperability.

2.) Leaving security potentially up to cost considerations. Every security measure comes with a price tag. In the past as well as today, OEMs tend to implement higher security standards in expensive vehicle than in medium or low-cost vehicles. The suggested approach with just a "development standard" would not remedy to this this approach.
Only be requesting a legally mandated minimum level of security (e.g. a prescribed encryption level for car2car communication), the legislator can take the costs for this minimum level out of the cost considerations of individual companies and out of the competition between OEMs. Reports of successful hacks of OEMs in the past were very often based on the sheer refusal of OEMs to use more expensive security technology.

3.) Lack of durability over the lifetime of the car. If it is not mandated that, by design, at least all hardware components tasked with security inside the vehicle have to be exchangeable against improved hardware (e.g. during PTI inspection every 3 years), then the lifetime of the vehicle will be severely limited. Tomorrow's state of the art servers would have little problem in successfully attacking cars that rely on 10-year old hardware to host the protection software.

4.) FIGIEFA requests an examination of the following legal question: would the granting of a type-approval, which is based on a *process evaluation* of a *proprietary cybersecurity management scheme of a vehicle manufacturer*, absolve him of his liability in case of a successful cybersecurity attack? What will happen if there is a cybersecurity incident, but as the GRVA Regulation will in essence just be a check of a proprietary OEM cybersecurity management system without setting minimum requirements for cybersecurity as such – would therefore OEMs be exempted from their liability, just because they will have received a type-approval (which is based on a process audit) and there therefore assumed to have complied with all relevant regulations?

To use the example of the intercepted messages for keyless entry systems that are responsible for substantial levels of car theft in Europe as of now: If e.g. an OEM – strictly following the prescribed process – takes into account the risk that the keyless entry messages might be intercepted and implements as a counter measure the suggested actions that user have to store their keys in alluminium boxes at home, then he would be perfectly covered by this approach. Nothing in the suggested regulation would enforce him to instead increase the level of authentication and encryption at higher costs per unit.

## 'Countering the counter arguments':

### a) Speed of development

**Argument:** OICA is often trying to convey the notion that IT is so fast in development that unfortunately nothing could be standardized technically due to the unforeseeable variety of new solutions and technologies which leaves the legislator only with the option to standardize the development process.
**Counter argument**: This is de facto not true.
On the contrary, the whole world of information technology relies successfully since decades on very precise standards that are constantly kept up to date by tasked organizations to allow beautiful solutions like the world wide web or the "Internet of things". For example the most prominent standard for data storage is SQL (founded 1974), the most popular programming language "Java" to handle this data appeared in 1995 and the most prominent way to present the data to and interact with the user, HTML, was released in 1993.

### b) Lack of ‘technology neutrality’

**Argument:** It if often brought forward by some OEMs that any detailed technical requirement would limit innovation and subsequently competition.
**Counter argument:**
A car is not an isolated system. A car interacts with its driver, its passengers, other cars, other traffic members and the environment. To protect all involved systems and to ensure a smooth collaboration between the systems, a variety of detailed technical requirements is already today prescribed. Airbags are mandated together with exact timing requirements to protect the passengers, emission values are specified to protect the environment and the brake light of a vehicle has always to flash red instead of any other innovative colour to warn the cars behind the vehicle.
Again, IT is not different. A certain level of functional, as well as non-functional (e.g. security) standardization is needed to ensure a smooth and safe & Secure communication and collaboration of the involved systems. The route to follow is: “Agree on standardization, compete on implementation”. (Example: There are competing software vendors that offer relational database management systems (e.g. Oracle, Informix, Microsoft, IBM) that nevertheless all “speak” the standard language SQL.

**Proposal of FIGIEFA and ETRMA:**

1.) Some very basic design rules and requirements should be incorporated already in the UNECE requirements in addition to just the standardized development process, e.g.:
a.) Hardware that hosts security software inside the vehicle must be designed to be updateable over the lifetime of the vehicle to deal with future software attacks.
b.) There must be a set of minimum Gateway functionalities inside the car so that the car is able to protect against cyber-attacks even if there is no network connection to a remote server available.
2.) Other than leaving everything beyond the development process up to the OEM, independent organisations need to be in place to develop and maintain the security and functionality standards that a vehicle has to fulfil in exactly same way that the above mentioned software standards had been kept up to date for decades. Only this way a mandated key length for encryption could be described for the next two years or a protection profile for a Gateway component can be updated.