28th ITS World Congress, Los Angeles, September 18-22, 2022

Paper ID #

Cyber Security regulation – Practical application from a technical service point of view

Oriol Flix[1*], Carlos Luján[1], César Elpuente[1]
1. IDIADA Automotive Technology S.A, Spain (oriol.flix@idiada.com)

Abstract
It is widely known that the future of vehicles is a progressive evolution from conventional vehicles to fully autonomous/connected vehicles able to deal with all the situations on the road. This process starts with new ADAS (Advanced Driver Assistance Systems) functions that are gradually taking the control of the vehicle, in controlled situations, over the driver. Based on these new technologies, and always from the safety point of view, the European Union introduced the new General Safety Regulation. This regulation introduces advanced safety requirements that will become mandatory from 2022 for new vehicles types.
One of the regulations that will cause a major impact on manufacturer's internal procedures, but also on the way in which Approval Authorities and Technical Services assess the system, is the regulation on Cyber Security, UN R155, that requires a new approach on how to validate and certify a system

Keywords:
Autonomous Driving, Cyber Security, New General Safety Regulation, Advanced Driver Assistance Systems

Introduction

The main objective of the paper is to analyse the impact of the UN Regulation No 155 on manufacturer's procedures, and to the certification process. The classic certification approach for almost all the safety functions that are legislated, starts when the manufacturer finishes the prototype of this specific system, and together with a documentation package that defines the most relevant aspects of it, characteristics, and design, is sent to the Approval Authority (AA) or Technical Service (TS). The AA or TS will be the responsible to assess and verify if it is valid according to the requirements defined for such specific system in the relevant regulation. This validation process, normally includes the following steps:

1. Verification that the sample provided by the manufacturer is representative of the documentation that defines the system.
2. Verification that the system fulfils the requirements defined by the regulation.
3. Verification of visual means (may be tell-tales, dimensions, masses, …)
4. Testing. Most of the regulations include static and/or dynamic tests that shall be performed in controlled conditions, to ensure the repeatability of the results, with a minimum performance, that is understood as the minimum safety level that shall be provided in order to place the vehicle in the market.

The tests to be performed and the acceptance criteria for these regulations is clearly stated, and it is only a matter of having the suitable equipment and trained people to validate it. So, if the value obtained is less or higher than the prescribed by the regulation, the system fulfils (or not) the minimum requirement of safety. The problem arises when the system that is being evaluated cannot be assessed through the typical system inspections and pre-defined tests.
How would you define a specific test for a system, in terms of Cyber Security, if new threats and vulnerabilities are discovered every day?

Similar to what happened with the analysis and assessment of Complex Electronic System, a new certification approach has been developed in order to adapt to this new situation. An approach that still allows to the Technical Services and Approval Authorities the evaluation of Cyber Security in terms of safety for the drivers and other road users. In order to evaluate how the new UN Regulation No 155 has changed this approach both for manufacturers and TS/AA, is important to have a clear idea on why it is so important, application dates, and where the requirements have been created.

New General Safety Regulation (EU) 2019/2144

Given the current developments in connected and automated driving, the GSR defines some advanced and intelligent safety features for each category of vehicle of the EU market. Advanced vehicle systems have been proven effective in reducing fatalities, road accidents and mitigating injuries, therefore the regulation looks for a gradual adaptation of the users to automated features by making them mandatory.

Given that connectivity and automation of vehicles increase the possibility of unauthorized remote accessing to vehicle data, and performing illegal modifications of software, the GSR defines that UN Regulations No 155 (Cyber Security) and No 156 (Software updates) should be applied on a mandatory base. Therefore, the GSR defines application dates for all the vehicles, so that it will be mandatory in Europe to fit new vehicles with systems that will protect against unauthorized access. These dates are:

- July 2022 for New Vehicle Types.
- July 2024 for New Registrations.

So, any vehicle sold from July 2024 onwards, shall be protected in terms of Cyber Security.

As said before, the GSR also defines that the new regulation on CS should be created in the UN framework.

UNECE Structure

United Nations regulations are regulations that have been accepted and recognized by all the signatories of the 1958 agreement. Moreover, most of these regulations become mandatory under European laws.

Due to the growing importance of the autonomous and connected vehicles, on 2018 WP.29 created a dedicated subsidiary working party called GRVA (Group of Experts on Automated Driving). Considering the main objectives reflected on the framework document for automated vehicles, different informal groups had been established, and continue to be established, in order to address the different topics. The current structure is shown in Figure 2.

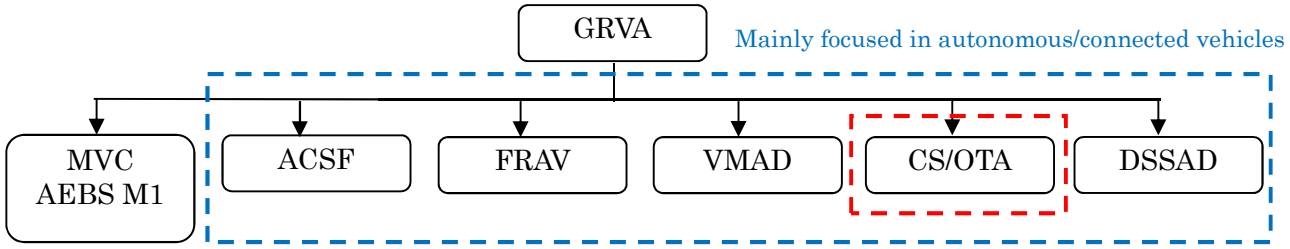

Figure 1. GRVA and subsidiary groups' structure

Under the supervision of the UNECE and the World Forum for Harmonization of Vehicle Regulations (WP.29), GRVA is the group that discusses all the themes belonging to autonomous driving and proposes recommendations or guidelines that will become new UN Regulations.

A framework document presented during 2019 on automated/autonomous driving serves as the basis for further development of a series of vehicle safety topics, always looking for a higher level of safety. The list includes:

- System Safety.
- Failsafe Response.

- Human Machine interface (HMI).
- Object Event Detection and Response (OEDR)
- Operational Design Domain (ODD/OD)
- Validation for System Safety.
- ***Cyber Security***.
- Software Updates.
- Event Data Recorder (EDR)

These priorities are treated or discussed on specific working groups directly dependant of GRVA. As seen, Cyber Security is one of the main topics of the framework document, and the organization dedicated a lot of effort and resources for the development of the regulation between 2019 and 2020.

CS/OTA (Task force on Cyber Security and Software Updates)
On top of all the new groups on the autonomous field, Cyber Security and Software Updates task force has evolved quickly due to its high growing importance. This group has been the responsible for developing the technical requirements of such regulations. Given the synergies of Software Updates and Cyber Security in the automotive field, both regulations have been created by the same experts, so they share a similar approach in terms on how to assess the technologies and how they shall be applied by the manufacturer inside of their organizations, for the whole lifecycle of the vehicle (development, production and postproduction).

The first meetings of the group were held at the end of 2018, and the first drafts of the regulations were adopted by the GRVA in March 2020. In between, more that 20 meetings with all the experts took place, given the importance of the topics.
One of the main differences between the two regulations and other vehicles' regulations, is that Cyber Security and Software Updates regulations are accompanied by a master document that pretends to provide guidelines for the TS/AA. The main objective of the guideline (called Interpretation Document), is to provide an explanation of:

- The purpose of the requirement.
- The kind of procedure should be provided by the manufacturer in order to fulfil the requirement.
- Standards, ISO's or similar documents, that could be used as evidence.

So, in short, it is a guideline for the TS/AA, on how to evaluate every single requirement that affects the manufacturer, and what's considered as a minimum level of safety. The use of the guidelines also ensures that all the contracting parties, through their TS and AA, have the same approach on the evaluation of such systems and that there are no different interpretations between them.

What makes these two regulations different, among other conventional regulations, is that both of them are split in two differentiated parts.
First of all, the regulation defines a set of requirements that intended to validate if the manufacturer has a set of processes/procedures in place, that will provide guidance on how to handle Cyber Security/Software Updates during the operational life of vehicles, produced under a vehicle type. The different phases of the lifecycle may have specific activities, procedures, that have to be implemented and analysed.
Focussing on the Cyber Security area, this specific set of procedures that will cover its management is called Cyber Security Management Systems (CSMS). The CSMS is a systematic risk-based approach that defines organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.
As said, contrary to other regulations, this one adds specific provisions in order to ensure that the manufacturer takes into account the Cyber Security of the company and the vehicles that are in use for the whole life-cycle.

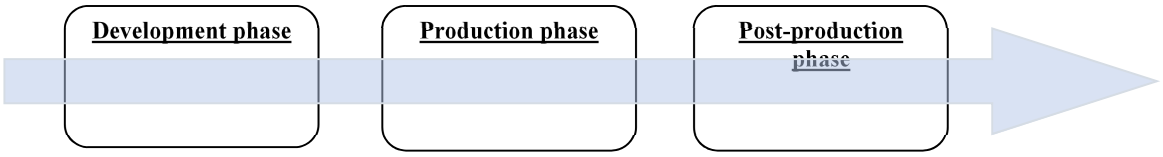

Figure 2. CSMS lifecycle covering.

The CSMS of the manufacturer is the first process that shall be evaluated by the TS/AA, given that the obtention of the Certificate of Compliance (CoC) of this system, will allow to the obtention of vehicle type approvals on regards of Cyber Security.
The validity of the CSMS is three years from the obtention of the CoC, and after this period, the system shall be re-evaluated again, to verify that every process is still in place, and has been updated according to the new threats and vulnerabilities. Once the manufacturer has obtained the CSMS, vehicle types can be presented for the certification under the scope of this specific Management System. So, the second set of requirements of the regulation is intended to cover the essential aspects and verifications for the vehicle type. Basically, these requirements are based on the direct application of the processes defined in the CSMS for the whole life-cycle of the vehicle, to the vehicle that is under the type approval. In addition, it is at this point where the tests on the vehicle are performed, according to the vulnerabilities detected, their threats, and the mitigations applied by the manufacturer.

Technical service point of view
The overview of the processes, or areas to be assessed in terms of the CS Regulation by the Technical Service, are split as it is shown in Figure 3.

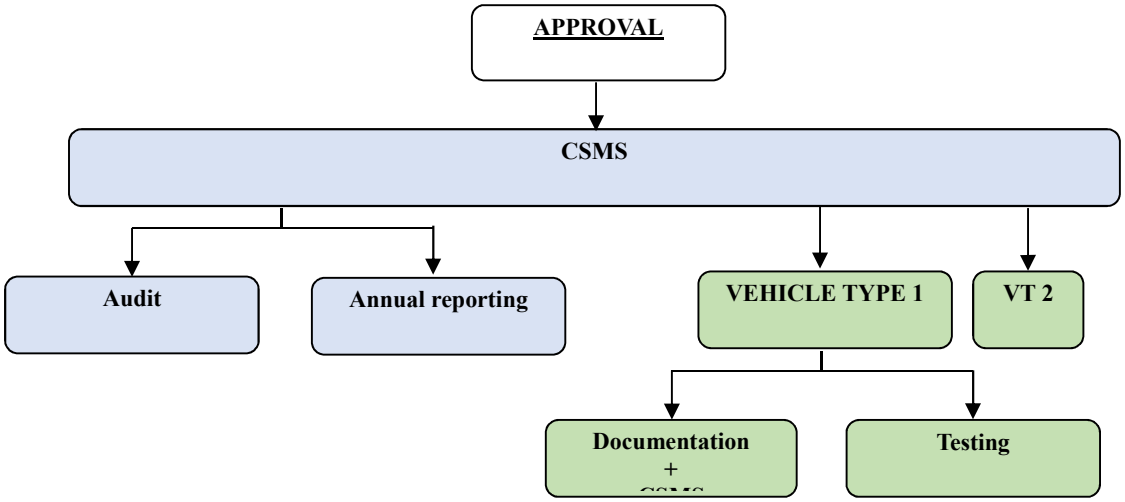

Figure 3. Approval processes of UN R155

The two colours in Figure 3 define the two main areas that are performed for the type approval process by the Technical Service. As it is defined, the Technical Service shall, first of all, assess the whole CSMS of the manufacturer. This is a new concept inside of the certification procedure regarding other regulations. The inspectors shall evaluate if the processes provided by the manufacturer are aligned with what it is expected by the Regulation, and the Interpretation document.

One of the challenges that the TS may have, is that actually, the certification procedure is starting in an early phase of the development of the system. Given that the CSMS is covering all the phases of the lifecycle, it is important to start the first contacts with the manufacturer months before the evaluation of the CSMS, and the obtention of the CoC. Otherwise, if some deviations that directly affect the development process of the vehicle are found when the vehicle is almost in the production line, the mitigations implemented by the manufacturer could cause a big impact in terms of timing, and the development of the architecture of the vehicle.
The assessment of the CSMS should be performed, by experienced persons on type approval and Cyber Security, in the following steps:

- Pre-assessment of the technical documentation: all the non-confidential procedures and processes of the manufacturer can be evaluated before the on-site audit. This first row allows to identify deviations on the procedures from an early phase.
- On-site audit: an audit at the manufacturer's facilities in order to verify that the processes provided in the first stage are actually implemented by all the areas. Additionally, all the information that is considered confidential by the OEM and couldn't be shown before, is evaluated during this phase.
- In case that some deviations are found, a second round of audit may be performed, or a re-evaluation of the technical documentation, with the updates of the manufacturer.
- Issue a test report with the results of the audit, and the fulfillment of the requirements for the CSMS.

Therefore, engineers in charge of these regulations should be more experienced on auditing than testing, also having a background on electronics and Cyber Security.

Once the CoC of the CSMS is issued, an annual reporting from the manufacturer is required for the continuous monitoring of the system: this is intended to ensure that the manufacturer is following the processes defined for the CSMS, and there is evidence of this compliance. After three years from the approval date, a new audit shall be performed in order to obtain the renewal of the CoC.

After the approval of the CSMS is granted, the vehicle manufacturer can obtain vehicle types according to the procedures developed under the management system approved. For this second stage, a new set of requirements focused on the specific architecture that is going to be approved, will apply.
Basically, the requirements are focused on the application of the procedures provided for the CSMS, on the specific vehicle type.

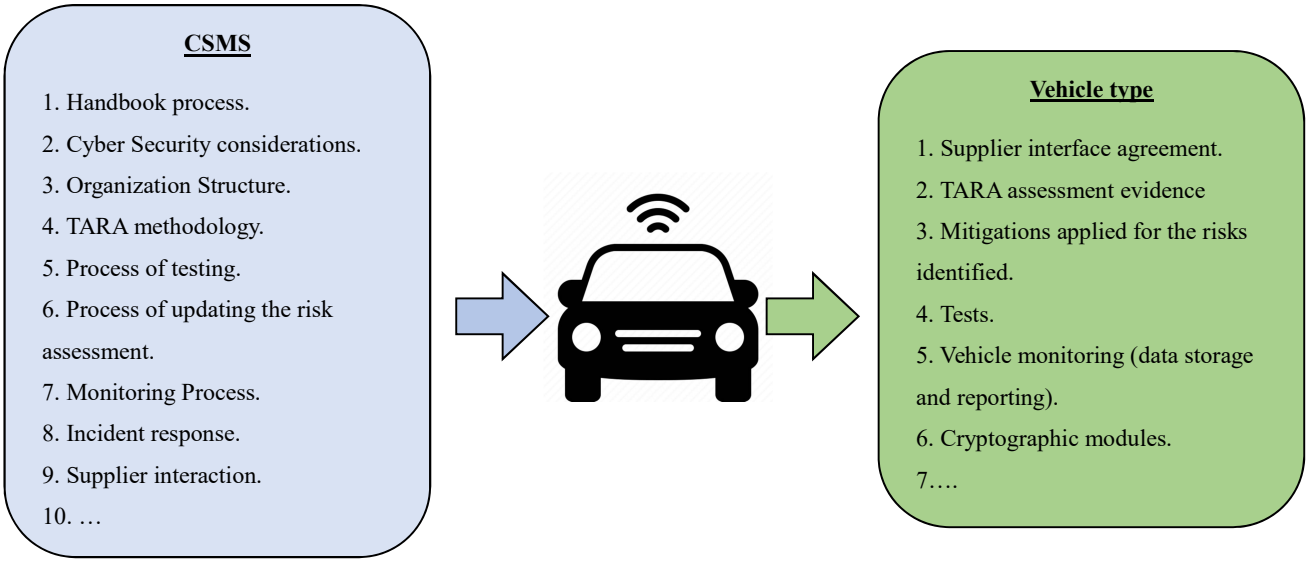

Figure 4. Application of the CSMS to the Vehicle Type.

Thus, for a given architecture, the use of the procedures defined for the CSMS, allows to the manufacturer the identification of threats and vulnerabilities for the vehicle under design. For the identified risks, mitigations are applied, and Cyber Security tests shall be applied in order to verify that the mitigations are suitable according to the safety goals.

What is important for the vehicle type phase, from the Technical Service point of view, is the verification that the defined architecture of the vehicle is covered by the manufacturer's CSMS, and that the processes are correctly applied to ensure the vehicle security during the lifecycle.

Additionally, once the mitigations and tests are defined according to the TARA methodology, the Technical Service is able to witness, or perform by itself, some of the proposed tests, and check that the results are good, and the mitigations are enough for a given risk or threat. Therefore, for the vehicle type certification, the TS need to acquire knowledge for Cyber Security testing, and processes auditing.

Conclusions

The path from conventional vehicles to automated and connected vehicles, can not be understood without the evolution and inclusion of new technologies related to complex electronic systems, connectivity between vehicles, infrastructure, and the use of the data obtained onboard and offboard the vehicle. The development of new connectivity technologies and their fitting to the vehicles, also creates new threats and ways to attack the vehicles, obtain confidential data from the users, or create unsafe situations.

For this reason, the European Commission and the World Forum for the Harmonisation of Regulations (WP.29) have developed the set of administrative and technical requirements that a manufacturer and a vehicle shall fulfil in terms of Cyber Security.

Given the complexity of the area, and that the definition of pre-defined tests or mitigation wouldn't be effective for ensuring the security, a new approach for the Type Approval process had to be defined. This new approach leads to a new way to certify, and thus creation of new needs for the Technical Services, which shall evolve quickly and adapt to the new procedures.

References

1. European Commission Technical Committee on Motor Vehicles (2019). *Guidelines On The Exemption Procedure For The Eu Approval Of Automated Vehicles*

2. https://www.unece.org/trans/main/wp29/meeting_docs_grva.html

3. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R2144&from=EN