# New 2024 cybersecurity regulations for vehicles

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

*June 2024*

**INCIBE-CERT_VEHICLES_CYBERSECURITY_REGULATIONS_2024_GUIDE_v1.0.docx**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Index

## INDEX OF FIGURES

# 1. About this guide

The objective of this guide is to provide information to help understand the new regulations issued by the World Forum for the Harmonization of Vehicle Regulations (WP.29), a body of the United Nations Economic Commission for Europe (UNECE), referring to cybersecurity in vehicles, as well as providing advice to help compliance.

The new normative consists of two regulations, R155 and R156, which stipulate the cybersecurity requirements that manufacturers **must meet in order to qualify for the approval** of vehicles that are going to circulate in the countries of the European Union, or countries outside the EU that will opt to follow these regulations. Specifically, the **R155 concerns the requirements for cybersecurity management**, while the **R156 stipulates the requirements for software update management**.

During the guide, the requirements outlined in both regulations are introduced, along with recommendations and indications on how to comply with them correctly and what internal procedures of manufacturers and suppliers may be affected by the new regulations.

# 2. Introduction

The automotive sector is an international example of the integration of classic technologies and modern interconnected systems. To cope with a highly competitive market, manufacturers have been progressively incorporating more smart technology into new car models, from central lockouts to parking *software* and autonomous driving. All these elements can facilitate the use and safety the vehicle, but, as in all industrial environments, when new technologies are introduced, they also introduce new vectors of cybersecurity risk.

For example, a car with vulnerable *software* can be the target of attacks, ranging from leaking sensitive user data (location data, usage habits, etc.), to endangering the safety of the driver, passengers, or other occupants of the road. The risks increase as the car's reliance on digital systems for managing fuel, brakes, steering, and other components increases.

This new paradigm has prompted an initiative by the European Union to establish **standardized regulations** for all cars sold in the European space, regardless of manufacturer or type of vehicle. This effort has materialized in the European regulations **UN R155** and **UN R156**, rules that will come into force **in July 2024**. These regulations establish a cybersecurity homologation system that all vehicles **must pass before they can be sold and circulate** within the European Union. To help manufacturers and users, the present guide summarises the origin and purpose of these standards, their key elements, and their implications for the automotive industry.

How to deal with the new safety risks of 'smart' vehicles has been, and continues to be, a debate in the global automotive industry. To prevent the European market from being occupied by multiple technologies in conflict or that could endanger users and pedestrians, UNECE (United Nations Economic Commission for Europe) established the **Global Forum for the Harmonization of Vehicle Regulations** (better known by its working group code in the commission: **WP.29**).

This UNECE forum brings together not only representatives of the member countries of the European Union, but also delegates from manufacturers and countries critical to the European and global automotive industry. WP.29 establishes debates and working committees that lead the development of automotive regulations and standards with the aim of ensuring coordination between countries and manufacturers, so that a car can be sold and used in any country associated with the standard, with the same level of safety.

Although WP.29 deals with multiple topics: passive safety, noise and pollutant emissions, tyre characteristics... Many of its efforts in recent years have focused on the challenge of cybersecurity in vehicles, with the aim of anticipating the potential risks posed by a disorganized and improvised adoption of new technologies in new vehicles.

To this end, proven concepts of cybersecurity in industrial environments have been adopted, a comprehensive vision of cybersecurity that encompasses all aspects of the manufacturer and the final product in a management system. This means that all elements of the vehicle's electronic system must consider how they affect the cybersecurity of the vehicle as a whole, in the same way that all elements of the supply chain must be involved to ensure the target level of cybersecurity in the rest of the phases of the vehicle's life cycle.

Also, it is considered that cybersecurity is created in daily operations, so security measures are of little use if they are not configured and managed throughout the life cycle of the system. To this end, the regulation also establishes requirements for the management of cybersecurity in vehicle systems and in their relationship with the manufacturer and the end user during maintenance after the initial purchase.

This approach is embodied in the approval of cybersecurity for vehicles. To the approval already established for the risks governed by current legislation, indicated by the symbol of an 'E':

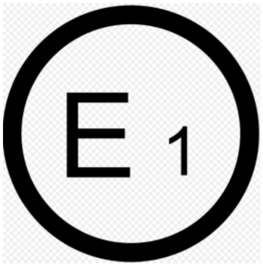


*Figure 1: Homologated vehicle symbol*

A vehicle with this approval must also have the risk indicators (regulations) for which it is approved. Thus, after the entry into force of the new regulation, vehicles must have the codes R155 (cybersecurity management) and R156 (management of cybersecurity updates).

# 3. Organization of the document

This document is divided into two main parts, one dedicated to each of the new regulations.

In chapter 4:'***R155: Cybersecurity Management*** 'The main points of the regulation are described **R155,** focused on cybersecurity requirements for the **Cybersecurity Management System** of the vehicle. The process for homologating a new type of vehicle is briefly explained before going through all the requirements of the regulation, along with recommendations and observations for each.

As in the regulation, the requirements have been separated into:

- Requirements for the management system. That is, more focused requirements at the level of the manufacturer and internal processes (design, procurement, manufacturing, and maintenance).
- Requirements for each type of vehicle, to be met by type of vehicle to be approved.

It is worth noting that '***4.2.2 Mitigation measures '*** compiles the general mitigation measures recommended by the regulation have been, accompanied by recommendations and brief examples of application.

The chapter 5 '***R156: Software Update'*** takes the same route, this time focusing on regulation **R156**, geared towards cybersecurity requirements for the **Maintenance and updating of the *software* of the vehicle**. Since many aspects are redundant between the two regulations, this section has focused mainly on those requirements and controls unique to the R156.

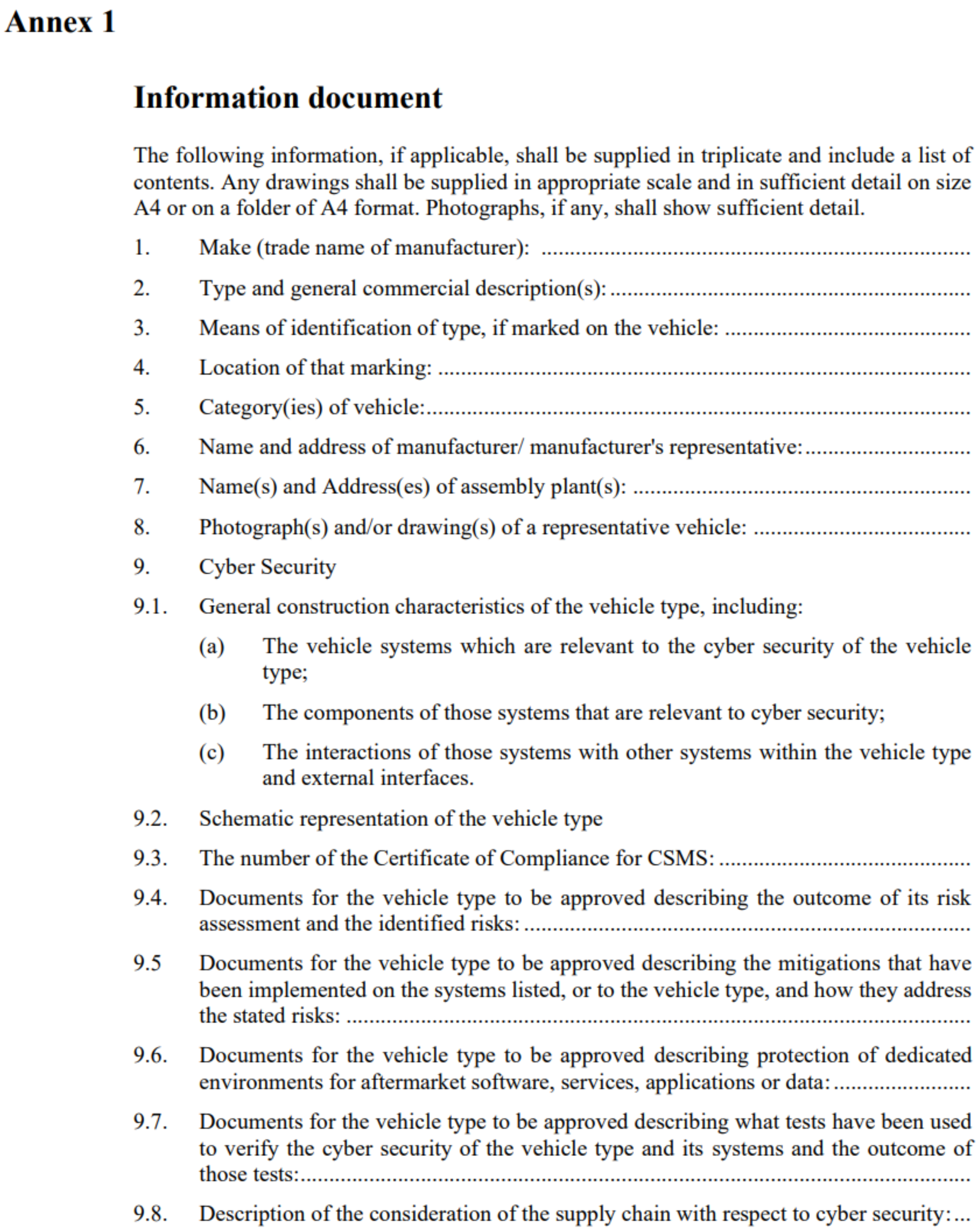
The document concludes with a brief reflection on the importance of comprehensive cybersecurity management during the useful life of the vehicle, from design to retirement, for correct compliance with the standard.

# 4. R155: Cybersecurity Management

The main objective of the R155 regulation is to define the requirements to be met by the vehicle and the manufacturer to consider that it presents an adequate level of cybersecurity against the cybersecurity threats listed in Annex 5 of the R155.

In order to be eligible for approval of a particular type of vehicle, the manufacturer must, as the main evidence of compliance with the requirements, submit the information requested in Annex 1 of the standard (Figure 2). As can be seen, there is descriptive information that the manufacturer should be able to provide, such as connection diagrams or the list of systems deployed in the vehicle, among others.

However, information regarding the cybersecurity requirements is also required as evidence: risk management, risk mitigation measures, and cybersecurity in the supply chain. These requirements focus on the **vehicle cybersecurity management system (CSMS),** i.e. how cybersecurity is organized and executed, not only at the level of the vehicle and its systems, but also includes in its scope the cybersecurity in the manufacturer's servers, its design and manufacturing process, its capabilities for maintenance, monitoring and surveillance,  vulnerability management and supply chain management.



Annex 1

Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

1. Make (trade name of manufacturer): ..........................................................................

2. Type and general commercial description(s): ..............................................................

3. Means of identification of type, if marked on the vehicle: ..........................................

4. Location of that marking: .............................................................................................

5. Category(ies) of vehicle: ..............................................................................................

6. Name and address of manufacturer/ manufacturer's representative: ............................

7. Name(s) and Address(es) of assembly plant(s): ..........................................................

8. Photograph(s) and/or drawing(s) of a representative vehicle: .....................................

9. Cyber Security

9.1. General construction characteristics of the vehicle type, including:

(a) The vehicle systems which are relevant to the cyber security of the vehicle type;

(b) The components of those systems that are relevant to cyber security;

(c) The interactions of those systems with other systems within the vehicle type and external interfaces.

9.2. Schematic representation of the vehicle type

9.3. The number of the Certificate of Compliance for CSMS: ..........................................

9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks: .............................................................................

9.5 Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks: ...........................................................................................................

9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data: .......................

9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests: ..........................................................................................................................

9.8. Description of the consideration of the supply chain with respect to cyber security: ...

*Figure 2: Annex 1 of regulation R155. Information to be provided by the manufacturer*

## 4.1. How to homologate a vehicle type

In order to be eligible for approval, the manufacturer must first undergo a document check. The manufacturer must submit documentation evidencing:

- *Proper **risk management throughout the vehicle supply chain** .*
- *That a risk analysis has been carried out **during the development of the vehicle** and the risks found have been mitigated.*
- *That the **safety measures** described during the design stage following the risk analysis have been applied and tested on the vehicle.*

- *That there is a **procedure in place to detect and respond to** vehicle-related cybersecurity threats.*
- *That relevant data is recorded **for cyberattack detection and post-cyberattack forensic analysis capabilities***.

In addition, once the document control has been passed, the approval body (or the technical service to which responsibility is delegated) will carry out a battery of technical tests on a sample of vehicles of the type to be approved.

At the level of detail, the regulation highlights the ISO/SAE 21434, ISO 26262-2018 and ISO/PAS21448 standards, as recognized certifications for those responsible for vehicle audits for homologation. Although this stipulation does not apply directly to manufacturers, knowledge of these standards can inform internal assessment processes prior to type-approval.

## 4.2. Cybersecurity Management System Requirements

To meet this requirement, it will be necessary to demonstrate that:

***The vehicle manufacturer has a cybersecurity management system (CSMS).***

The CSMS is the set of policies, procedures, and measures that the manufacturer implements, not only in the vehicle, but in its own organization, to meet cybersecurity needs. Typically, it is governed by a central cybersecurity policy that outlines the overall processes in the organization, accompanied by specific procedures for the different aspects of cybersecurity (incident response, data protection, team management, etc.). Each procedure describes the roles and responsibilities to be developed and the technical measures used in the process.

For **the CSMS to be effective, it must be known by and involve the entirety of the organisation of the manufacturer**. It requires the commitment of the management structure to ensure proper resource allocation, as well as personnel properly formed and trained to assume cybersecurity responsibilities. In addition, it requires the rest of the employees and external staff to be aware of the procedures and best practices to help maintain the target level of cybersecurity in day-to-day operations.

For the development of the CSMS, in addition to studying the requirements of the R155, manufacturers are recommended to follow the good practices defined by the ISO 27001 or the IEC 62443 2-1.

### 4.2.1. Scope of the CSMS

*According to R155, the CSMS shall be applied to the following phases of the vehicle life cycle:*

1) **The development phase**.

The R155 regulation stipulates the need to carry out a risk analysis in the design phase, so that manufacturers can define from the beginning the safety requirements to be included in the design.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

In addition, taking cybersecurity into account from the design of the vehicle allows the manufacturer to define how other cybersecurity needs will be met:

- *employ secure software **development methodologies**,*
- *select **methods of secure communication** between vehicle elements and with external elements,*
- *define **secure environments for the execution of** vehicle software,*
- *define **cybersecurity requirements** for the supply chain.*

2) **The production phase.**

During this phase, cybersecurity processes focus on the operations of the production plant and the supply chain, where the manufacturer must:

- *apply **internal procedures** for cybersecurity in day-to-day production,*
- *ensure that the **suppliers and third parties** involved are aware of and comply with the assigned cybersecurity requirements.*
- *perform **technical tests** of the vehicle's safety measures.*

3) **The post-production phase.**

The manufacturer's cybersecurity responsibilities do not end after the vehicle is sold. The incorporation of *software* into the vehicle implies the need to:

- ***detect and manage vulnerabilities**, develop security updates, and provide them to customers,*
- *conduct **active monitoring of cybersecurity threats** and risks and provide early response to potential incidents and cyberattacks.*

### 4.2.2. Mitigation measures

The following table lists the mitigation measures described in the regulation and which must be included in the CSMS. Since these measures are quite general and open to interpretation, a column of recommendations or general examples has been added to make them easier to understand and implement.

| Ref. | Mitigation Measures | General Recommendations and Examples |
|---|---|---|
| **M1** | Security Controls on Backend Systems*:* **Insider Attacks** | • Restrict the use of elevated users, generic users, and shared users.<br>• Maintain proper management of user accounts.<br>• Maintain and monitor user activity logs. |
| **M2** | Security Controls for Backend Servers: **Access Control** | • Require authentication to access *backend servers*.<br>• Enforce strong password policy.<br>• Require multiple authentication factors.<br>• Collect and monitor access logs. |
| **M3** | Security Controls for Backend Servers: Recovery Measures **in the Event of a System Outage** | • Establish safe system restore guidelines.<br>• Keep up-to-date backups.<br>• Keep software solutions up-to-date and current.<br>• Establish redundancy measures. |
| **M4** | Security Controls to Minimize **Cloud Computing Risks** | • Use encrypted communications and encryption of stored information. |

| | | |
|---|---|---|
| | | • Ensure isolation of cloud servers from those used for other functions or entities.<br>• Monitor remote servers, manage, and analyse security alerts.<br>• Do not leave unnecessary open public accesses. |
| **M5** | Security Controls for Backend Servers: Preventing **Data Security Breaches** | • Physical access control to servers.<br>• Policy for the classification and treatment of sensitive information.<br>• Monitor stored information. |
| **M6** | **Security by design** | • Restrict unnecessary or unprotected communication channels.<br>• Network segmentation.<br>• In-depth, layered security. |
| **M7** | **Access control** | • User authentication control.<br>• Enforce strong password policy.<br>• Collection of access logs. |
| **M8** | **Access control to** personal or critical data | • User authentication.<br>• Use of multi-factor authentication for users.<br>• User activity logs. |
| **M9** | **Prevent and detect unauthorized access** | • Monitoring of access logs.<br>• Blocking accounts in the event of multiple failed login attempts. |
| **M10** | Verification of **authenticity and integrity of** incoming messages to the vehicle | • Use of secure communication protocols.<br>• Verification of equipment using physical addresses, certificates, passwords, etc. |
| **M11** | Security Controls for **Cryptographic Key Vault** | • Use of TPMs or secure storage hardware items.<br>• Deployment of centralized authentication platforms.<br>• 'Cold' *storage* of cryptographic keys. |
| **M12** | Protecting **Sensitive Data in Transit** | • Use of protocols with secure encryption.<br>• Use of VPN in case of interactive access. |
| **M13** | Measures for Detecting and Recovering from a **Denial-of-Service Attack** | • Blocking accounts and repeated suspicious communications.<br>• Configuration of safe failure and communication restart.<br>• Deploy resource balancers. |
| **M14** | Protection against **viruses or malware** | • Deploy malware monitoring agents.<br>• Update agents periodically.<br>• Implement lists of *software* allowed for installation. |
| **M15** | Measures to **detect malicious internal message or activity** | • Deploy communications monitoring and analysis agents.<br>• Collect and analyse in-vehicle activity and communications logs.<br>• Establish a security alert analysis and management system. |
| **M16** | Secure **Software *Update Procedures*** | • Software integrity and authenticity checks prior to installation. |

| | | |
|---|---|---|
| | | • Restrict access to software settings.<br>• Make pre- and post-upgrade backups.<br>• Design a test environment to verify the performance of updates before they are released.<br>• Secure failure configuration in the event of authentication breakdown. |
| **M18** | Applying the **principle of least possible privilege** | • Define user roles and privilege levels based on roles and needs.<br>• Enable user activity logs.<br>• Don't enable privileged accounts by default |
| **M19** | Ensure compliance with **security procedures** | • Collection and analysis of equipment logs.<br>• Carry out cybersecurity exercises and training sessions.<br>• Establish a system for monitoring and analysing security alerts. |
| **M20** | Security Controls for **Remote Access** | • Use of secure communication protocols.<br>• Establish access control with multiple factor authentication.<br>• Restrict remote access to recognized and authorized sources.<br>• Disable unnecessary remote access. |
| **M21** | The software **will be assessed for security**, authenticated, and its integrity protected.<br>Security controls will be in place to minimize the risk from third-party software | • Establish equipment restoration processes.<br>• Require elevated privileges for software and configuration modification.<br>• Establish *'whitelists'* of allowed software. |
| **M22** | Security Controls to External **Interfaces** | • Require authentication to access external interfaces.<br>• Restrict external communications to essential uses only.<br>• Keep externally accessible software and services up to date. |
| **M23** | Cybersecurity best practices will be followed in **software *and* hardware *development*** | • Maintain records for traceability of software features, versions, and capabilities.<br>• Ensure compatibility with security measures.<br>• Establish and apply hardening guides. |
| **M24** | Best practices will be followed for the protection of the integrity and confidentiality of **personal data** | • Encryption and monitoring of data at rest and in transit.<br>• Segmentation of systems that work with sensitive data.<br>• Notify users of the purpose and methodology of the use of their data. |

In addition to implementing these mitigation measures, the regulation stipulates that the manufacturer must **have the necessary processes and documentation in place** to ensure that these measures work properly. To this end, the regulation stipulates that manufacturers must apply mitigations according to the results of risk management, focusing efforts on the risks with the greatest potential impact and probability of affecting the vehicle and its critical elements.

### 4.2.3. Vulnerability mitigation

***Manufacturers must manage and respond to technical vulnerabilities discovered in vehicle software within a reasonable timeframe.***

Although this point will be developed in more detail later, when we talk about the R156, in order to meet this objective, this guide recommends:

- Deploy monitoring and vulnerability detection agents in the *vehicle'*s software.
- Establish communication channels so that users and third parties can notify of new vulnerabilities discovered.
- Maintain a record of known vulnerabilities, level of impact, characteristics, and management status.
- Have a security update development team for the manufacturer's own *software* and ensure that *software* vendors have equivalent capabilities.
- Establish a procedure for verifying the operation of security updates before providing them to users.
- Notify users of updates, their purpose, changes applied, and instructions for the update.

### 4.2.4. Cyber Threat Analysis and Detection

***The manufacturer must monitor approved vehicles, after their sale, and on an ongoing basis to detect possible threats.***

Although the standard does not specify methodology, quantity, or type of data to be collected from vehicles sold by the manufacturer, this requirement is considered to stipulate the need to deploy a safety information and event management (SIEM) system that monitors, analyses, and reports vehicle safety information.

Real-time monitoring, a standard solution of traditional SIEMs, is very likely to be impractical in the case of vehicles, due to product constraints: possible lack of coverage or long-distance travel, confidentiality of user data, product longevity, use of second-hand vehicles, etc.

Manufacturers are therefore advised to design systems for vehicles to collect relevant safety data locally and independently. At a minimum, it is recommended to collect from:

- User activity and access control measures.
- Connections established between vehicle systems and with external systems.
- Changes in *software* and *hardware.*
- Unusual or potentially hazardous activity to the safety of the vehicle.
- Activity of installed security measures, such as *anti-malware* or communications control agents.

The data should be provided to the SIEM on a regular basis for analysis, or when the vehicle is back connected.

***It is the manufacturer's responsibility to ensure the confidentiality and safety of vehicle users.***

During the application of this requirement, regardless of the methodology used, the user must be **informed of the data collection and its purpose**. It must also be ensured that the **monitoring functions do not have a negative impact on the functionality of the**

**vehicle**. It is recommended to prioritize passive and non-intrusive monitoring solutions in vehicle systems, which minimize their effect on vehicle systems.

### 4.2.5. Dependencies with contracted suppliers

***Manufacturers maintain proper cybersecurity management throughout the supply chain.***

It is recommended that, during the risk analysis carried out at the design stage, the manufacturer identifies which parts of the vehicle are to be provided by third parties and which safety features should be included. These characteristics should be requirements for providers at the time of contracting their services and the ability to meet them should be a criterion when selecting providers.

As evidence for this requirements, the manufacturer could ask suppliers for: safety certifications of their equipment, results of technical tests, technical specifications of the product, legal commitments to comply with requirements.

Among the most common requirements for suppliers in terms of cybersecurity, we could find:

- Responsibilities for technical support and security updates for the software and hardware provided, and duration of this service.
- Supplier’s support responsibilities during incident response.
- Communication channels for cybersecurity notifications.
- Hardening guides and safety instructions for the equipment provided.
- Remote access from the supplier and access to sensitive information of the manufacturer and end users of the vehicle.
- Compatibility with the security measures used by the manufacturer and applicability of the manufacturer's procedures and policies to the provided equipment (password policy, compatibility with anti-malware and monitoring agents, etc.).
- Supply of spare parts and replacements.

## 4.3. Requirements for each type of approved vehicle

In addition to the manufacturer's CSMS requirements, R155 stipulates several requirements relating to the safety deployed in the vehicle itself.

Approval is requested and granted for each type of vehicle independently.

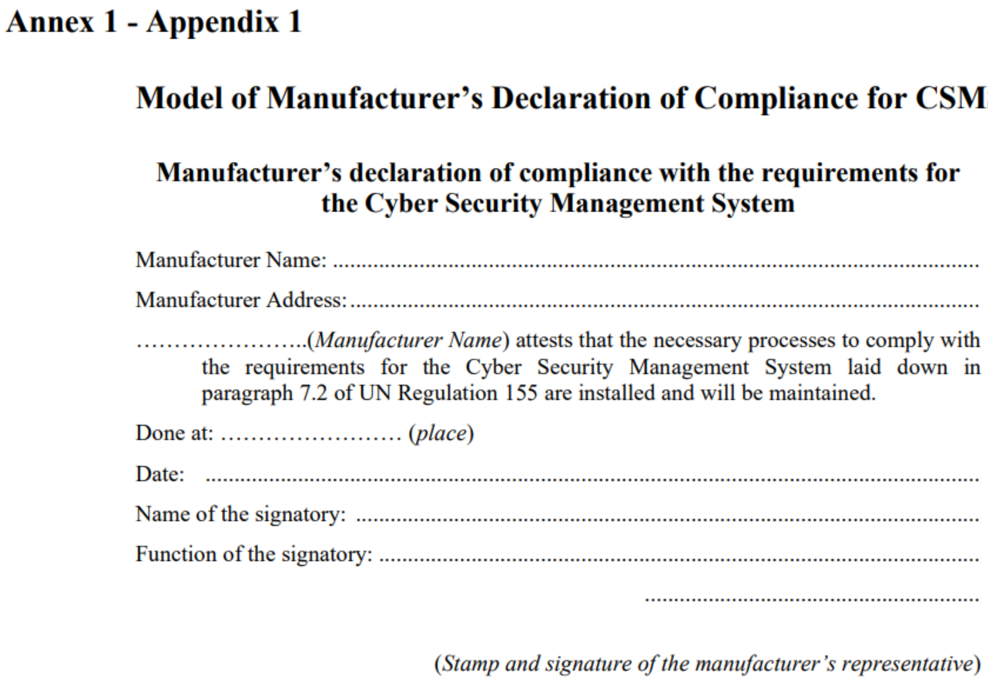
The above requirements can largely be met by the manufacturer for all types of vehicles in production at once (e.g., an internal manufacturer procedure for secure software development will apply to all types of vehicles being worked with while following the procedure). However, the following requirements must be met independently for each type of vehicle.

### 4.3.1. Compliance with all CSMS requirements

***The manufacturer must certify that the type of vehicle to be approved is compatible with its CSMS and that all the requirements stipulated for it are met.***

To demonstrate this compliance, the manufacturer must issue a declaration of conformity following the template set out in the annexes to regulation R155 (Figure 3).

This statement would accompany the data sheet (Figure 2) at the time of application for approval and must be issued after passing the manufacturer's internal technical tests required by the regulation to verify that the CSMS fulfils its functions correctly.



**Annex 1 - Appendix 1**

**Model of Manufacturer's Declaration of Compliance for CSMS**

**Manufacturer's declaration of compliance with the requirements for the Cyber Security Management System**

Manufacturer Name: ..........................................................................................................

Manufacturer Address: ......................................................................................................

…………………..(*Manufacturer Name*) attests that the necessary processes to comply with the requirements for the Cyber Security Management System laid down in paragraph 7.2 of UN Regulation 155 are installed and will be maintained.

Done at: …………………… (*place*)

Date: ....................................................................................................................................

Name of the signatory: .......................................................................................................

Function of the signatory: ...................................................................................................

..........................................................

(*Stamp and signature of the manufacturer's representative*)

*Figure 3: CSMS Declaration of Conformity*

For newly manufactured vehicles, this requirement should not present much difficulty if risk management has been carried out correctly during design and production.

For older models that are not compatible, as contemplated by the regulation, the manufacturer can carry out a risk assessment on the type of vehicle. The manufacturer will have to certify, through risk assessment, and potentially through the deployment of new measures retroactively, that it has an adequate level of cybersecurity despite not being compatible with the CSMS.

### 4.3.2. Supplier Risks

***The manufacturer shall identify and manage the risks associated with the supplier for the type of vehicle subject to type-approval.***

As above, this requirement should be met automatically if the manufacturer is applying its CSMS for the vehicle type in the design and production phases. This requirement highlights the need not to use generic requirements and analyses for each type of vehicle, it is necessary to ensure that in each case the specific needs of the product and process to be approved are met.

### 4.3.3. Critical Vehicle Elements

***The manufacturer will need to identify the critical elements of the vehicle and include them in the risk assessment.***

Those elements that may affect the essential elements of the vehicle should be considered critical, those that, in the event of interruption of service, the functionality of the vehicle and the safety of passengers may be compromised.

In general, these elements should be isolated as much as possible from the rest of the vehicle's systems. The communication channels established with critical elements should have the highest possible level of security and should only be established when necessary. This precaution should be taken in the case of connections to external networks. These should be restricted as much as possible in the case of critical elements of the vehicle, being enabled only if they are essential for the operation of the vehicle, with the maximum possible safety measures and, ideally, through systems that act as intermediaries, for example, through separation networks.

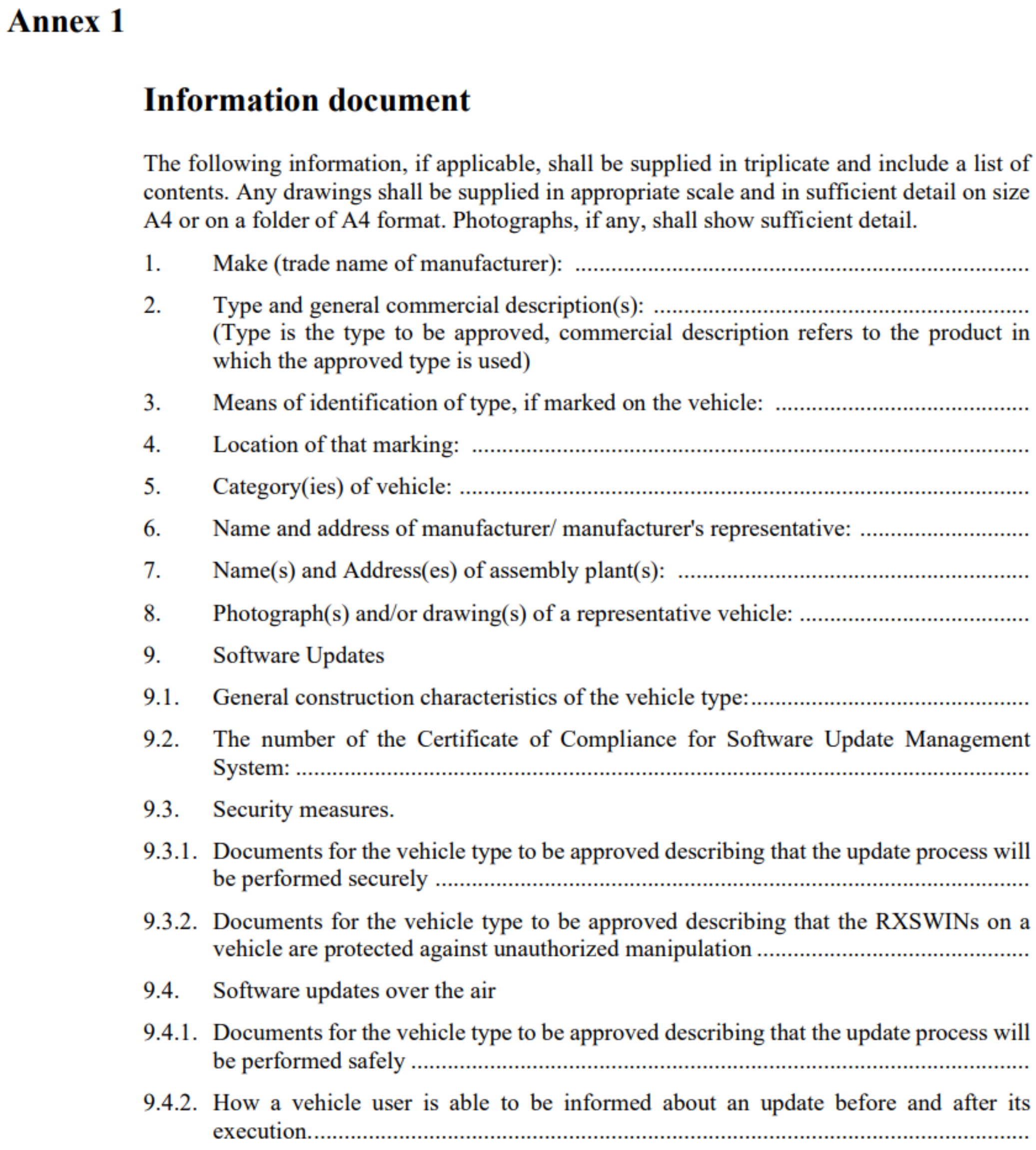
### 4.3.4. Vehicle Safety Measures

| Requirements | Feedback |
|---|---|
| Certify that the type of vehicle to be approved has the corresponding **mitigation measures** deployed, according to the risk analysis carried out | Perform systematic safety management, identifying and prioritizing risks and following the regulatory mitigation measures described above. |
| Ensure that the vehicle type has a **secure environment for storing and running *software*** | □ Establish an isolated environment from other *software services.*<br>□ Implement version control.<br>□ Monitor the integrity of stored *software*.<br>□ Restrict access and execution and modification permissions, reserving it for those cases where it is essential for the functionality and safety of the vehicle.<br>□ Maintain records of software executions and modifications  to maintain traceability over the *software*.<br>□ Implement lists of *software* authorized for execution. |
| Technical security measures are in place in the vehicle to ensure that the ***installed software* and services run securely** | |
| **The vehicle's safety measures have been tested** to verify its operation and effectiveness. | No specific tests are defined, but it is recommended to can refer to recognized standards such as ISO/SAE 21434, ISO 26262-2018 and ISO/PAS21448 to get an idea of good practices to follow in the tests. |
| Subject the type of vehicle to be approved to **adequate and sufficient tests to verify the effectiveness of the safety measures** applied. | |
| **The vehicle, during its useful life, provides information to the manufacturer** so that it can identify, manage, and analyse potential threats (without compromising the privacy of users). | The manufacturer should identify potential secure endpoints for sending  security *logs*. One possibility would be to use the user's mobile connection through applications such as Android Auto and Apple Carplay or your own applications.<br>In the case of using wireless connections, the process must be supported by authorized technical services |
| Evidence that the type of vehicle has **forensic capabilities** in terms of cyber incidents: collection of records | |

| | |
|---|---|
| of the vehicle's security measures and software, the records are protected against unauthorized alterations and are periodically evaluated to detect cyber incidents. | |
| **The vehicle has sufficient cryptographic systems** to comply with current privacy regulations. | Cryptography shouldn't just apply to remote vehicle communications. It would be recommended to apply it over internal databases, especially in cases where user or security data is stored. One methodology would be the use of systems equivalent to the TPMs used today in other industries to encrypt equipment at the *hardware level*. |
| The manufacturer shall report, at least annually, on the **results of cybersecurity management** (including information on new cyber threats and cyberattacks). | These requirements can serve as motivation for the manufacturer to centralize information and maintain an efficient management of security information and alerts.<br>It is common to generate monthly (or even weekly) reports on the state of cybersecurity in an industrial control system. These reports typically include:<br>□ Status of known vulnerabilities and their mitigation measures.<br>□ Managed cybersecurity events and incidents.<br>□ New threats discovered through monitoring of systems or public sources.<br>□ Progress on cybersecurity action plans.<br>When making modifications, as well as in the design phase, it is important to have a vision of how they will affect security measures. This is usually done by using new risk analyses or technical tests, before deciding whether additional measures are needed. |
| The manufacturer shall **notify the approval authority of any modifications** affecting the performance of the cybersecurity measures or the documentation previously submitted. | |

# 5. R156: Software Update

As for the R155 regulation, R156 defines an information form that the manufacturer must provide to qualify for approval. (Figure 4).



**Annex 1**

**Information document**

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

1. Make (trade name of manufacturer): ..........................................................................

2. Type and general commercial description(s): ..............................................................
(Type is the type to be approved, commercial description refers to the product in which the approved type is used)

3. Means of identification of type, if marked on the vehicle: .........................................

4. Location of that marking: ............................................................................................

5. Category(ies) of vehicle: .............................................................................................

6. Name and address of manufacturer/ manufacturer's representative: ...........................

7. Name(s) and Address(es) of assembly plant(s): .........................................................

8. Photograph(s) and/or drawing(s) of a representative vehicle: .....................................

9. Software Updates

9.1. General construction characteristics of the vehicle type:.............................................

9.2. The number of the Certificate of Compliance for Software Update Management System: .........................................................................................................................

9.3. Security measures.

9.3.1. Documents for the vehicle type to be approved describing that the update process will be performed securely ..................................................................................

9.3.2. Documents for the vehicle type to be approved describing that the RXSWINs on a vehicle are protected against unauthorized manipulation ............................................

9.4. Software updates over the air

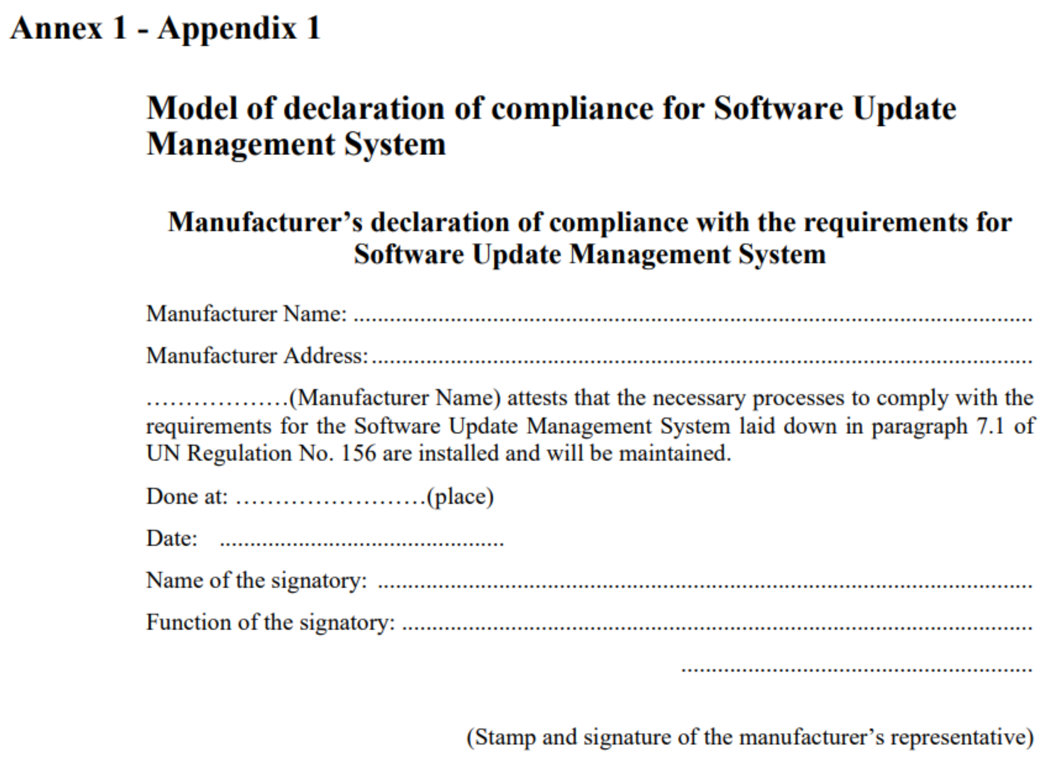
9.4.1. Documents for the vehicle type to be approved describing that the update process will be performed safely ......................................................................................

9.4.2. How a vehicle user is able to be informed about an update before and after its execution.........................................................................................................................

*Figure 4: Annex 1 of regulation R156. Information to be provided by the manufacturer*

In this case, the homologation focuses on the cybersecurity of the vehicle's *software* and its maintenance during the vehicle's lifecycle. The regulation stipulates that manufacturers must implement a system to ensure that security updates are developed to the *software* hosted in the vehicle and that these are distributed and applied without introducing new risks to the vehicle and its occupants.

As in the case of R155, manufacturers must ensure that they have complied with the requirements by using another form (Figure 5).



## Annex 1 - Appendix 1

### Model of declaration of compliance for Software Update Management System

**Manufacturer's declaration of compliance with the requirements for Software Update Management System**

Manufacturer Name: ......................................................................................................

Manufacturer Address: ..................................................................................................

………………(Manufacturer Name) attests that the necessary processes to comply with the requirements for the Software Update Management System laid down in paragraph 7.1 of UN Regulation No. 156 are installed and will be maintained.

Done at: ……………………(place)

Date: ...............................................

Name of the signatory: ..................................................................................................

Function of the signatory: ..............................................................................................

..........................................................

(Stamp and signature of the manufacturer's representative)

*Figure 5: Software update management system declaration of conformity*

## 5.1. Software Update Management System Requirements.

### 5.1.1. Processes to be verified at initial assessment

The regulation stipulates the need for the manufacturer to establish **processes** to meet the following requirements:

| Requirements | Comments and recommendations |
|---|---|
| All information relevant to regulatory compliance is documented and retained ***in relation to the vehicle'***s software | The information to be collected is expanded in more detail in the next section. |
| There is a **method to uniquely identify all** *software* versions and updates deployed | Indicators are at the manufacturer's selection, but it is important that they are documented and consistent. |
| For vehicles that have an **RXSWIN** identifier, the information regarding the RXSWIN identifier before and after the update is accessible and can be updated. | The RXSWIN identifier is a number, selected by the manufacturer, that identifies the *software* of the electronic control system of the type of vehicle approved. The X in the code represents the regulation referred to by the identifier, in this case R156WIN. |
| The manufacturer can verify that **the *software* conforms to what is defined by the identifier** | □ Define software signatures and lists of *authorized software* and guidelines on how to identify it.<br>□ Additionally, add additional security measures to monitor the integrity of the |

| | |
|---|---|
| | *software* and restrict access and modification |
| Identify all **interdependencies of the updated system with other systems** | Interdependencies can occur mainly in the form of:<br>□ Other external *software* packages needed to function properly.<br>□ Connections needed to update *software*.<br>□ Externally hosted information. |
| Assess, determine, and record whether an update could affect other systems necessary for the safe operation of the vehicle, or if it will alter the functions of the vehicle at the time of registration | Although it is always recommended to carry out technical tests before publishing the update, proper cybersecurity management allows you to identify points of interaction between systems through inventories, risk analysis and monitoring. |
| **Identify all target vehicles for the upgrade**. Referring to the vehicles, in production or post-production, on which the *software* to be updated is deployed | This requirement infers the need to maintain up-to-date inventories of vehicles in operation with the version of the *software* to be updated and to collect a minimum relative to the *software* and systems installed |
| Confirm the compatibility of the update with the configuration of the target vehicles before it is released. | While compatibility can be formally determined by the upgrade specifications, it is recommended to have test environments and verify updates. |
| Assess, determine, and record whether an upgrade will affect any approved system. | It is important to note that an update that fundamentally alters any of the approved components may entail the need to renew this approval, requiring additional tests or information before it is re-approved |
| Inform the user of updates | Report:<br>□ Purpose of the update,<br>□ instructions to follow,<br>□ changes that are going to be made,<br>□ upgrade progress,<br>□ success or failure of the process. |

### 5.1.2. Information to be recorded and stored

For each update, the manufacturer will need to record and store:

- Documentation of the processes used for the development of updates.
- Documentation of the composition and identifiers of approved systems before and after the upgrade.
- The following two points, in addition to being stored, must also be **presented at the time of approval**:
  - For each RXSWIN, a verifiable record of its composition before and after the update.

    - Documentation listing the vehicles targeted for the update and confirming compatibility with the latest vehicle configuration.

- Documentation for each update:
    - Goal of the update,
    - Homologated systems affected,
    - If it affects other requirements of the regulation,
    - If it affects the approval parameters of any system,
    - If new approval has been requested,
    - How and when the update can be applied,
    - Confirmation that the update is secure,
    - Confirmation that it has undergone validation procedures satisfactorily.

As can be seen, most of this information could be collected at the same time as the requirements requested for the initial moment of approval are met. This emphasizes the need for management to meet these requirements systematically for each update.

### 5.1.3. Additional Security Requirements

The manufacturer must demonstrate that:

- **Updates are protected from unauthorized tampering** before the update is made.
- **The upgrade process is protected**, including the provision of the upgrade to the target vehicles.

Encrypting communications, enforcing integrity and authentication checks, and designing secure architectures are particularly critical to protect in-transit security updates and prevent improper tampering with  vehicle *software*.

But it is also important to consider other issues, such as the composition of the network. For greater security, one-way, non-interactive communications can be used through intermediate protection elements or, ultimately, physical supports can be used in specialized workshops for critical information.

### 5.1.4. Additional Requirements for Over-the-Air Updates

The manufacturer must consider the following requirements when choosing the update methodology:

- Demonstrate that the **update processes do not affect driving safety** .
- Demonstrate that, in case the **update requires specialized** or complex actions, the application can only be applied in the presence of competent personnel.

It may be possible to perform the simplest updates wirelessly and simultaneously to all target vehicles. However, despite the inconvenience it entails for the user, it is worth considering requesting that they take their vehicles to their nearest authorised technical services for critical or more technical updates. It is important to equip workshops with refresher guides and credentials with a sufficient level of privileges to enable them to perform this task. These cases can also be an opportunity for the collection of safety data from vehicle premises for analysis.

- The vehicle must be capable of:
    - Restore your systems to a previous version in the event of an interruption or failure of the update.

        - The possibility of storing backups for system restoration directly in the vehicle, as opposed to the use of external servers, should be considered. This decision will condition the storage capacity in the vehicle, which must be protected and monitored, with integrity and authentication controls.

          The use of external servers, on the other hand, introduces availability and confidentiality risks. These risks are multiplied in the case of moving vehicles or in remote areas that may lose connectivity.

    - Enter a safe failure state in the event of an update interruption or failure.
        - Under no circumstances should the vehicle interrupt its service or compromise the physical safety of users in the event of failure during the upgrade process. While the safest method is to perform upgrades only when the vehicle is stationary, this decision may compromise the vehicle's battery capacity or availability, if the upgrade process is lengthy.
    - Do not allow an update process to start unless the vehicle has enough power to complete the process.
        - During update verification testing, the manufacturer can obtain an estimate of the battery consumption required to complete the process and apply it as a safety limit for the process. Alternatively, a general safety limit could be set so as not to start processes with low battery, as is done as standard on other mobile electronic devices.
    - Have a secure process in place for updates that affect vehicle safety.
        - It is recommended that updates that affect the security of the vehicle be made when the vehicle is stopped and under confirmation by an authenticated user, or specialized technical personnel if necessary.

- The manufacturer must be able to inform the user of an update before it is executed. You must report:
    - Purpose of the update.
        - It is left as an option if the manufacturer notifies of the criticality and type of update.
    - Changes introduced by the update.
    - Expected time to complete the upgrade.
    - Features that may be unavailable during the process.
      Instructions that the user may need to update the vehicle safely.
    - **The same** notification **will be accepted** for a group of updates that will be applied consecutively.
- It will be ensured that the vehicle does not allow driving during the update (or vice versa), or the use of functions that may compromise the process or safety of the vehicle, where this could introduce safety risks.
- After the vehicle has been updated, the user will be informed of the success or failure of the process and the changes applied.

# 6. Conclusions

The new cybersecurity regulations for vehicles represent a significant change in the usual processes of manufacturers, who will now have to face the challenge of providing protection to multiple systems in constant motion without compromising the physical safety of users or the functionality of the vehicles.

While most of the new cybersecurity requirements can be easily met if a comprehensive cybersecurity management system is implemented at the manufacturer's enterprise level: establishing internal cybersecurity procedures, conducting risk analysis, and establishing cybersecurity requirements and controls throughout the supply chain; There are some specific cases that present a higher level of difficulty.

Requirements related to the maintenance phase of the vehicle, when it is in use by the end customer, may require special attention. What information should the car record during use? How will the information get to the manufacturer for analysis and how often? How will the updates be delivered?

For many of these processes, the most manufacturer-friendly solutions will not be the best option for the end user. For example, a manufacturer may choose to require the customer to periodically take the vehicle in for service as the sole method of applying cybersecurity updates, which would lead to additional costs and hassle for the customer.

However, more advanced and more functional processes will need to be taken into account from the moment of design of new vehicles or incur higher costs when applying retroactively.

As already discussed throughout this document, and as this last example illustrates, cybersecurity must be treated globally in the company. Each step of the process is a building block for the next stage that will help the effectiveness of security measures, compliance with the new regulation, and the reduction of impact and resources needed for incident management.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# ANNEX I. Glossary of terms

| Term | Definition |
|---|---|
| ***Software*** | Programs or services installed on a computer to perform the target functionalities |
| ***Hardware*** | Physical components of a computer that host, perform tasks on their own, or host the *software* for execution. |
| **Cybersecurity Management System (CSMS)** | A set of policies, procedures, measures, and controls implemented in an organization to meet cybersecurity objectives. |
| **Vulnerability** | A technical deficiency or weakness of a *software* or *hardware* that introduces a cybersecurity risk to a computer. |
| **Vehicle Type** | Sets of vehicles that share:<br>• The same designation as defined by the manufacturer. Same name or model number chosen by the manufacturer.<br>• The same essential features of electrical and electronic architecture and external interfaces, as far as cybersecurity is concerned. |
| **Security Update or Patch** | A new version of *software* that makes changes to its configuration to eliminate vulnerabilities. |
| ***Trusted Platform Machine (TPM)*** | *Hardware* dedicated to storing a computer's encryption keys to protect sensitive information or a computer's configuration. |

.

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

Plan de
Recuperación,
Transformación
y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD