EUROCYBCAR®
CYBERSECURITY TEST

NEW CIBERSECURITY REGULATION UNECE/R55
VEHICLES WILL NEED A CYBERSECURITY CERTIFICATE

EUROCYBCAR®
CYBERSECURITY TEST

- It will come into force as of January 22, 2021
- It affects cars, buses, trucks, trailers and wagons
- Sanction per vehicle model that do not comply with this regulation

EUROCYBCAR®
CYBERSECURITY TEST

INDEX

Note: This report is based on the regulations approved on June 23, 2020 by the UN: ECE/TRANS/WP29/2020/79

Design and editing: Grupo CYBENTIA

EUROCYBCAR®
CYBERSECURITY TEST

WHY IT'S NECESSARY TO HAVE A REGULATION FOR VEHICLES ON CYBERSECURITY

IN FORCE FROM JANUARY 2021 ONWARD

DURING THE PAST YEARS, vehicles have become more and more complex from a technological point of view. In fact, we estimate that the software, that an average vehicle has, is composed of about 100 million lines of code. This means that the systems with which a current automobile is equipped are more complex than those of a f35 combat jet- with about 24 million lines of code-, a windows vista with 50 million or even all the software used by facebook- 62 million1.

This¨ informatization¨ of vehicles has allowed technologies that connect them with other devices; for example, with a smartphone- through bluetooth, a usb cable, a mobile app, or to internet through a wi-fi spot placed inside the car. All of this has led to the concept of a ¨connected car¨, which the vehicle technology association (VTS) describes as: those vehicles that have applications, services or technologies that connect it to its environment.

But the increasing complexity of technology in vehicles has made it so that cars are starting to be the target of cyberattacks. According to data from eurocybercar, since 2012 -more than 450 cyberattacks, that affected models of up to 50 different brands and compromised the privacy of the people travelling inside and even posed risk to their lives, - have been documented in the whole world.

One of the most talked about cases is the ¨live¨ demonstration performed by charlie miller and chris valasek to an american journalist in 2015. The invited him to drive a jeep cherokee and, while the journalist was driving, miller and valasek from the distance, in their house, were able to manipulate the air conditioning, the screen wipes and the audio. They were also able to interfere with elements related to movement such as the break or the engine.

According to EUROCYBCAR more than 450 cyberattacks that affected up to 50 different models, have been documented.

EUROCYBCAR®
CYBERSECURITY TEST

SOME OF THE THINGS THAT VEHICLES ARE EQUIPPED WITH... and how cybercriminals could use them are:

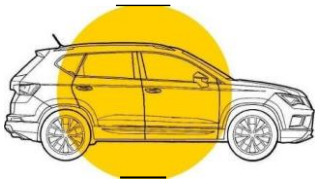
- **Bluetooth:** Blackmailing, replacing an identity or stalking someone.
- **Emergency E-call:** Retain a person from being aided in an accident.
- **Airbags:** They could be activated or deactivated via remote.
- **Smart key:** Steal a car or locking someone inside of it.
- **Wi-Fi:** Spying or replacing an identity.
- **GPS:** Kidnapping, spying, or blackmailing.
- **Radio- RDS:** Providing false information.

And, in the future this tendency will grow. It is foreseeable that in the year 2023 around 775 million connected cars will be in circulation . Autonomous vehicles equipped with a more complex software will also grow. Its predicted that for 2026, 50 million cars will be travelling without a driver .
Until now, multiple governments and regulatory organisms of all the world have created regulations that guarantee the physical security of vehicles and their passengers, but cybersecurity has been left out of those regulations.

Past

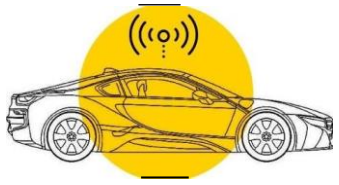
- A car with basic connectivity
- Head-unit Thetheredto pone over BT
- 20-30 ECUs
  < 10M LOCs
- Restricted electronics
- Head-unit, A/C, keyfob, door lock/unlock,windows

Present



- Embedded celular connectivity
- Rich head-unit/ Digital cockpit/
  Wi-ft, Bluetooth, GPS andTPMS
- 50-80 ECUs
  < 100M LOC
- Active Safety – Broad Access of user to safety systems.

Future



- Fully autonomous car
- Always connected - 5G
- A large number of sensors
- > 100 ECUs
  1OOM - 200M LOCs
- All car systems are operated by software

LOC: Lines of Code **1OOM:** Millions **ECU:** Electronic Control Unit

1. https://www.informationisbeautiful.net/visualizations/million-lines-of-code/
2. https://site.ieee.org/connected-vehicles/ieee-connected-vechicles/connected-vehicles/
3. Source EUROCYBCAR: In EUROCYBCAR we have registered, analyzed, and documented more than 400 attacks since 2012 until the first semester of 2020, cyberattacks against vehicles and the infrastructures related with cars have increased in a 1600%. And it would seem that the real number is much higher; the problem is that, due to the lack of knowledge, these types of cybersecurity failures in the population, there are probably a lot of people that has suffered a cyberattacks against their vehicle, but didn´t consider it a hack or simply didn´t have enough evidence.

WHAT REQUIREMENTS A CAR MUST COMPLY WITH IN ORDER TO BE SOLD IN THE EU

FOR CARS TO BE TRADEABLE in Europe, the European Union demands manufacturers that their models pass the requisites, especially, when it comes to cybersecurity. Since 2000 until now, the European Union has made the following security equipment's mandatory:

SINCE 2000 UNTIL NOW, THE EUROPEAN UNION HAS MADE THE FOLLOWING SECURITY EQUIPMENT'S MANDATORY:

Main vehicles safety regulations issued by the European Comission since 2000

MAR 2001	New conditions for the brake system.
APR 2003	Electric functions in the Windows, roof and screens.
JUL 2003	Security in the screening.
OCT 2003	Front collision measures.
OCT 2003	Lateral collision nmeasures.
JUL 2004	Mandatory ABS on new vehicles.
JAN 2010	Indirect visión tools.
MAR 2010	Back-end protection against collisions.
MAR 2010	A protection system against fires in the fuel´s deposit
FEB 2011	System of assistance in the brakes BAS.
DEC 2012	Protection for pedestrians.
NOV 2014	ESP mandatory for all new vehicles.
MAR 2018	eCall mandatory for all vehicles with a new homologation.
NOV 2019	Mandatory road safety technologies from 2022.

JUNE 2020 - MANDATORY CYBERSECURITY CERTIFICATION FOR VEHICLES
22 JANUARY, 2021

Car´s new (Noticias coches).
Available in https://noticias.coches.com/consejos/los-sistemas-de-seguridad-que-no-pueden-faltar-en-tu-coche/108496
General Traffic guidance (Dirección General de Tráfico, DGT, SPAIN),
Available in: http://revista.dgt.es/es/reportajes/2018/04ABRIL/0404ecall-obligatorio-a-partir-del-31-de-marzo.shtml#.X4ATvmgzbIU

THE REGULATIONS THAT THE EU TAKES FROM THE UN

The next regulation the EU will implement is the UNECE/R155

Besides generating their own regulation, the EU must follow the regulations approved by the Global forum of UNECE for the harmonization of the regulations of vehicles- known as UNECE/R155-.

The United Nations Economic Commission for Europe- UNECE-, was founded in 1947 as a regional commission of the united nations, in which 56 countries from Europe, North América and Asia are included .

With their headquarters in Geneva, the UNECE has as a main purpose to promote the economic integration and the cooperation between member countries, as well as promoting a sustainable development and economic prosperity. UNECE also establishes rules, standards and conventions to facilitate international cooperation, both inside and outside of the region and, for this reason, numerous countries outside of the area use the same rules and standards as the UNECE.

Inside the UNECE the global forum quote for the harmonization of the regulations of vehicles -WP29-.

UNECE WP29 has the goal of creating, updating, and maintaining the regulations of vehicles related with their technology, their security, and their protection of the environment. This is the biggest international system in the world, because 54 of the member countries- all, except the United States and Canada- have signed an agreement since 1958 that compromises them to recognize and apply inside of their borders the regulation approved by the UNECE WP29.

SOME OF THE REGULATIONS THE EU HAS ADOPTED FROM UNECE WP29 ARE:

- **Regulation nº 151-** Uniform disposition related to the homologation of engine vehicles, with respect to the information systems of blind spots for detecting bicycles .
- **Regulation nº44-** Uniform dispositions related to the homologation of retention devices for kids. -Childs retention system- .

UNECE
UNITED NATIONS Economic Commission for Europe.

WP29
Global Forum for Regulatory Harmonization About Vehicles

United Nations Regulations on Uniform Provisions Relating to Vehicle Type Approval for Cybersecurity and the Cybersecurity Management System.

WE NEED TO ADD ONE MORE REGULATION TO THE ONES ABOVE: THE WP29/2020/79

This new regulation will oblige cars that are traded within the EU to have a cybersecurity certificate.

Aware of the risks of cybersecurity for vehicles. UNECE WP29 approved the regulation ECE/TRANS/WP29/2020/79. This regulation requires vehicles to have a certificate that ensures that they are protected against cyberattacks. And the EU will make this mandatory in their territory for vehicles, cars, buses, trucks, trailers and wagons of new validation beyond as of July of 2022 and for all the new ones beyond the 1 July of 2024.

It´s an ambitious rule for the EU, which will close its market to vehicles that are not cybersecure before that, even those with combustion engines. The maximum the EU is proposing for now, when it comes to pollution, is to sue the manufacturers whose vehicle´s rate of emission exceeds 95 g of CO_2 per kilometer.

---

7. The member countries of UNECE are Albania, Germany, Andorra, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Czech Republic, Cyprus, Denmark, Slovakia, Slovenia, Spain, USA, Estonia, Finland, France, Georgia, Greece, Hungary, Iceland, Ireland, Israel, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxemburg, Republic f North Macedonia, Malta, Moldova, Monaco, Montenegro, Norway, Netherlands, Poland, Portugal, UK, Romania, Russia, The Republic of San Marino, Serbia, Sweden, Switzerland, Tayikistan, Turkey, Turkmenistan, Ukraine y Uzbekistan.

8. Complete text available at https://eur-lex.europa.eu/legal- content/ES/TXT/PDF/?uri=CELEX:42020X1596&from=EN

9. Complete text available at https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42020X1223&from=EN

10. The European Union consists of the following countries: Germany, Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Slovenia, Spain, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherland, Poland, Portugal, Slovakia, Romania y Sweden.

PREVIOUS INITIATIVES TO THE REGULATION OF UNECE/R155 IN SPAIN, EUROPE AND THE WORLD

ONE MORE RULE HAS BEEN ADDED TO THE REGULATIONS 151 AND 44 ... BUT, WHAT PREVIOUS BACKGROUND IS THERE TO THIS NEW REGULATION?

The documents before the arrival of the regulation of UN/UNECE WP29 were simple recommendations, not binding rules. It´s worth to mention that it is not until 2016 –even though, in 2013, a Spanish media outlet warned that vehicles were not sufficiently protected, leaving them open for cyberattacks- when the first recommendations on cybersecurity for cars, start to show up. It stands out because there are registered cyberattacks on vehicles since 2012 (Check introduction). One hypothesis could be that in 2015 the mentioned hack by Charlie Miller and Chris Valasek on a Jepp Cherokee, took place, the most ¨popular¨ of the attacks on vehicles . The coverage of this event may have caused institutions to worry more about the vulnerabilities of vehicle´s cyber security.

With these precedents -see graph in the next page- the UN started developing a regulation that would unify the criteria and requirements and implement the minimum cybersecurity basics for all vehicles. All of this has translated into a regulation in which experts from all over the world have worked on and whose details will be explained on the report.

ISO/SAE 21434: A LOOK TO WHAT IS TO COME.

Parallel to the regulation approved by the UN/UNECE WP29, the Organization of Standardization -ISO- and the Society of Automotive Engineers -SAE- are currently developing a text that looks to implement Cybersecurity on vehicles throughout all their life cycles. We are speaking of the standard ISO/SAE 21434.

This document is similar to the regulation of the UN/UNECE WP29 because it specifies some requisites to manage the risks of cybersecurity throughout all of their life cycle, from the first moment of their design until they are turned to scrap. The ISO/SAE 21434 also defines a common language to communicate and manage the risks of cybersecurity.

Both regulations are compatible, and present common aspects, in a way that complying with one makes it easier to comply with the other. The fundamental difference between the regulation from the UN and the one from ISO/SAE is that the first one applies in countries that are members of the UNECE, while the text from ISO/SAE is not an obligatory standard.

The ISO/SAE standard is still in development process. The last version is a draft and could be submitted to changes.

> The ISO/SAE 21434 also defines a common language to communicate and manage the risks of cybersecurity.

Complete text available at https://www.sae.org/standards/content/j3061_201601/
Complete text available at https://www.ic3.gov/Media/Y2016/PSA160317
Complete text available at https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf
Complete text available at https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
Complete text available at https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles y en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf
Complete text available at https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114 Caso publicado en Wired. Disponible en https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

EUROCYBCAR®
CYBERSECURITY TEST

PREVIOUS INITIATIVES TO THE REGULATION OF UN/UNECE/WP29

2013

OCTOBER

"A Spanish magazine publishes a report on cybersecurity risks in cars"

"A hacker could kill you while you're driving." This headline appears in number 156 of the Autofácil magazine -created and directed by Azucena Hernández-. This report warns about cybersecurity risks that affect the electronic systems of vehicles. It claims that some vulnerabilities could endanger the lives of passengers if a cybercriminal takes advantage of them.

2016

JANUARY

""Guide on cybersecurity for the systems of cyberphysical vehicles J3061_201601"[9]

Prepared by the Society of Automotive Engineers (SAE), a global association. In it some practical recommendations are given that provide guidance on how to establish a high level of cybersecurity on the systems of the vehicle. This guide was created based on practices that have been implemented or reported in industry, government and conference documents. It will be subject to ISO / SAE 21 43 4, which is based on it.

MARCH

"Motorized vehicles are increasingly vulnerable to cyber attacks"[10]

The FBI issues a statement in which it warns that the increasing connectivity of vehicles carries threats to cybersecurity. The text gives some examples of cyberattacks that could be carried out on cars.

OCTOBER

"The best cybersecurity practices for modern vehicles"

Prepared by the National Highway Traffic Safety Administration (N HTSA), an agency under the United States Government. It is a non-binding guide to improve the cybersecurity of motor vehicles.

2017

JANUARY

"Cybersecurity and resilience of smart vehicles"

Developed by ENISA, an agency of the European Union: The goal of this study is to identify Good practices that guarantee the security of the vehicle when facing cyberthreats. The study considers the vulnerable parts present in Smart cars, as well as the corresponding threats, risks, factors of mitigation and possible security measures that are yet to be implemented.

JULY

"The founding team of EUROCYBCAR performs the first cybersecurity test on a vehicle"

For three months, a team made up of hackers, engineers and car testers carried out the first cybersecurity test on a vehicle manufactured in Spain to verify the level of cybersecurity offered by a vehicle. The result revealed that cybersecurity was the great forgotten of car brands, despite the fact that it affects people's lives.

AUGUST

"The key principles on cybersecurity for connected and automatized vehicles"

This work of the British Government. It´s a guide that summarizes the eight principles for obtaining a good cybersecurity on the automobilist sector.

2018

JULY

"The Basque Cybersecurity Center creates the first working group on cybersecurity and the automotive industry"

After the inauguration of the Basque Cybersecurity Center -BCSC-, directed by Javier Diéguez, the creation of a working group made up of the Tecnalia, Vicomtech and Ikerland Research Centers, the BCSC and the founders of EUROCYBCAR is promoted.

2018

OCTOBER

"At the 12ENISE international event the importance of cybersecurity for mobility is discovered"

During the 12ENISE –International Information Security Meeting organized by the Spanish Institute of Cybersecurity (INCIBE) –, for the first time, there is talk about cybersecurity threats and vulnerabilities that must be considered in the car. The presentation is given by Azucena Hernández, current CEO of EUROCYBCAR.

DECEMBER

"PAS 1885:2018" [14]

BSI Group –that is designated by the British government, as the national regulation entity–. It establishes the principles on how to provide and maintain cybersecurity when it comes to minimizing the threats and damage taken by goods, as well as the services and systems inside the ecosystem of a smart transport, ever more connected and collaborative.

2019

MARCH

"The first means of investigation and awareness of motor and cybersecurity in the world is born"

The HackerCar media outlet, directed by Javier García, gets journalists, car testers and hackers to work as a team to test car in a way never seen before.

JULY

"EUROCYBCAR carries out the second technical evaluation of cybersecurity to a vehicle"

In its laboratory in Vitoria–Gasteiz, EUROCYBCAR submits a vehicle manufactured in Spain to the EUROCYBCAR Test: the only test in the world that measures the level of cybersecurity of a car based on two parameters: how it protects the life and privacy of the people traveling on board.

2019

NOVEMBER

"Cybersecurity applied to the automotive industry"

The Royal Institute of Elcano publishes a research article, signed by Ana Ayerbe –Tecnalia–, in which cybersecurity risks in automobiles are analyzed, the ways to deal with them and what initiatives exist in the world, citing EUROCYBCAR, as the only company in Spain that measures the cybersecurity of vehicles.

DECEMBER

"For the first time in the world, an institution submits a vehicle in its fleet to a cybersecurity test"

The Basque Government subjects one of the vehicles in its Mobile Park to the EUROCYBCAR Test to find out the cyber vulnerabilities to which the authorities traveling aboard said vehicles are exposed.

2020

Regulation ECE/TRANS/WP29 /2020/79

Regulation developed by UNECE WP.29 that will require vehicles to have a cybersecurity certificate that proves that they are protected against cyber attacks in order to be homologated.

https://hackercar.com/
The videos of his conferences can be viewed at https://www.youtube.com/watch?v=nu3mHMuXlOw
Complete text available at http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari105-2019-ayerbe-ciberseguridad-aplicada-a-la-automocion

EUROCYBCAR®
CYBERSECURITY TEST

ALL ABOUT THE UNECE/R155 REGULATION

THE RULE THAT REGULATES CYBERSECURITY IN CONECTED AND AUTONOMOUS VEHICLES

WHAT DOES THE UNECE/R155 SAY

On June 23, 2020, this standard that regulates the cybersecurity of vehicles was approved. The rule in question is the ECE/TRANS/WP29/2020/79 and it's entitled: "United Nations Regulations on Uniform Provisions concerning the approval of vehicles with regards to cyber security and cyber security management system".

STAGES OF DEVELOPMENT OF THE REGULATION

2018

September:

Beginning of the discussion about the risks of cybersecurity the vehicles have.

2019

June-august:

FasTests with authorities and volunteer manufacturers to determine its solidity and start working on a draft.

September:

Decision of the GRVA (Workgroup on autonomous and connected vehicles) on regulations content.

2020

March:

The final draft is published.

23 of June:

Approval of the final legislation.

2021

January 22:

Entrance into fruition. The legislation will be available for application in the member states of the UNECE.

. The European Union, South Korea and Japan have already confirmed that they will apply it in their territories, as will be detailed later.

In English, UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Texto íntegro está disponible a través del siguiente enlace: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

IT´S ABOUT THE NEEDED MEASURES to create a cybersecurity management system on vehicles. In other words, a system that focuses on the risks and threats and that protects the vehicle from cybersecurity attacks.

THE INDEX OF THE REGULATION DOCUMENT WP29:

1. **Area of application:** which vehicles does the rule affect.
2. **Description of some terms** used throughout the regulation.
3. **Homologation application:** The documents needed to get the approval.
4. **Approval mark:** Symbol that the cars that comply with the regulation must have in their Id plate (or in a readily accessible place).
5. **Homologation:** Document verifying the fulfillment of the regulation.
6. **CSMS Certificate of conformity.**
7. **Specifications:** Details on the demands that the regulation will impose.
8. **Modification of vehicle type and extension of type approval:** How to make modifications to the vehicle type.
9. **Conformity of production.**
10. **.Penalties for non-conformity of production.**
11. **Definitive cessation of production:** how to communicate that a vehicle ceases production.

12. **ANNEX.**
1 Data sheet
2 Communication
3 Arrangement of the approval mark
4 Certificate of conformity model
5 List of threats and their mitigation measures.

THIS REGULATION PROVIDES A FRAMEWORK FOR THE AUTOMOTIVE SECTOR TO ESTABLISH THE NECESSARY PROCESSES TO:

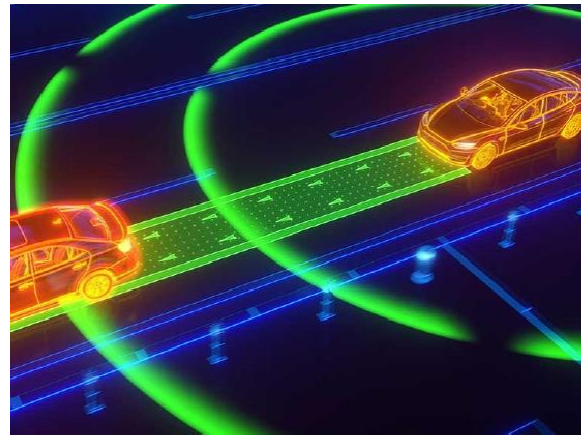
- Identifying and managing the risks of cybersecurity in the vehicle's design.
- Verifying that the risks are being managed, including the tests.
- Guaranteeing that the inspection of the risks stays updated.
- Monitoring the cybernetic attacks and responding accordingly.
.
- Analyzing the successful and committed attacks
- Evaluating whether cybersecurity measures are still effective against the new threats and vulnerabilities.

THE CSMS MUST PROTECT VEHICLES AGAINST 70 DIFFERENT TYPES OF CYBERTHREATS, THAT THE UNECE/R155 LIST IN THE REGULATION

IN ORDER TO FOLLOW THIS REGULATION, MANUFACTURERS WILL CREATE A CYBER SECURITY MANAGEMENT SYSTEM -CSMS- TO DESIGN NEW VEHICLE TYPES.

The CSMS is a serie of process that, all together, guarantee the cybersecurity of the system from different cyberattacks in an appropriate way.
For a CSMS to comply with the requisites implanted by the UN, the manufacturer will have to manage the cybersecurity of their models throughout their whole life cycle: development, production, and postproduction. Also, eachv of these cycles include specific protections against different threats.

THE CSMS MUST PROTECT VEHICLES AGAINST 70 DIFFERENT TYPES OF CYBERTHREATS THAT THE UN LIST IN THE REGULATION. THESE VULNERABILITIES ARE DIVIDED INTO 7 GROUPS WHICH ARE:



• **THREATS RELATED TO THE BACK-END SERVER.** These servers are the ones that make all the informatic systems and the internal network of the manufacturer work. Some threats to be avoided are loss of information on the cloud, cellphone leaks for sharing data in an involuntary way and that a worker makes a legitimate use of the data that it has access to.

• **THREATS RELATED WITH THE COMMUNICATION CHANNELS THAT THE VEHICLE USES TO CONNECT TO ITS VENVIRONMENT** -for example, other vehicles or the infrastructure-.
Some of the threats to be avoided are: Supplementing the identity of another vehicle, injecting malware -Programs that damage the system- through the communication channels, and manipulating or erasing the data and code of the vehicle´s software.

• **THREATS TO EXTERNAL CONNECTIONS AND CONNECTIVITY**. Some of the threats to be avoided are: the manipulation of remote functions, such as the key, the immobilizer and the battery; manipulating the telematic connections of the vehicle, like the temperature of the vehicles merchandise or unlocking the car via remote control; and causing interference in the wireless systems and sensors of short range.

• **THREATS TO THE VEHICLE´S DATA AND CODE.** Some of the threats to be avoided are: accessing without permission to the personal information of the owner (Who they are, their account numbers, location, the electronic ID of the vehicle) and falsifying the identity or manipulating the data of the vehicle (Milage, speed, signaling …)

• **THREATS RELATED TO THE UPDATE PROCEDURE OF VEHICLES.**
Any threat that affects an upgrade process of the informatic systems of the vehicle, whether it´s done wireless or through a download, are to be avoided.

• **THREATS RELATED WITH NON-INTENDED HUMAN ACTIONS.**
Someone with access to the vehicle (Like the owner or the repairman) could introduce a virus unintendedly if a cybercriminal were to trick them.

• **POSSIBLE THREATS THAT COULD BE TAKEN ADVANTAGE OF IF THEY ARE NOT PROTECTED ENOUGH**.
Some of the threats to be avoided are: software errors; not protected information of the first owner passing to the second owner -if the car were to be sold-, or replacing elements of the vehicles that follow the regulation with some others that don´t.

THE RESPONSIBILITY OF COMPLYING WITH THE CSMS WILL BE ON THE OEM -MANUFACTURERS-.

Also, they will have to check that all the providers in their resources chain identify and manage the risks in cybersecurity of the component that they work with. Therefore, providers are not obliged to follow the requisites of the UNECE/R155, but not doing so will damage them in order to be competitive and profitable.

The regulation of the UN/UNECE WP29 establishes some regulatory boundaries and the minimum requisites for makers along the value chain, but the regulation doesn´t include a guide for detailed implementation to translate the requirements into specific methods that avoid cyberattacks. This means that manufacturers are given a list of the risks they must avoid in their models, but for the moment, they must be the ones to determine how to avoid them, however the certificate must be emitted by an external entity.

HOW TO OBTAIN A CYBERSECURITY CERTIFICATE?

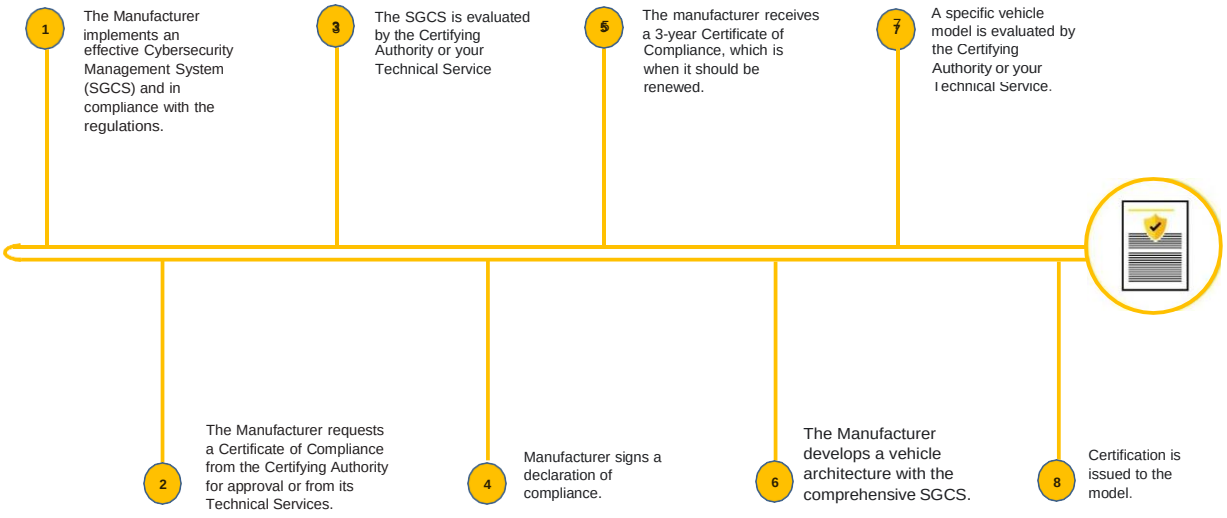
AN EXTERNAL ENTITY TO THE MANUFACTURER WILL BE THE ONE TO ENSURE THAT THE VEHICLE COMPLYS WITH THE REQUIREMENTS ESTABLISHED BY THE UN/UNECE

For an OEM to obtain a cybersecurity certificate, for a vehicle type, that acknowledges that it follows the requisites established by the UN, they must submit to some evaluations. Until now the OEM´s hired Companies that consulted in cybersecurity to date punctually some systems of their vehicles, but with the entrance of the new regulations **they will be obliged to hire an external service that certifies that their vehicle is cybersecure.** They will have to provide enough documents to evaluate the function of the CSMS. Then an authorized entity will analyze those documents and run tests on the vehicle. This process has the goal of certifying that the manufacturer has taken the minimum measures to guarantee that the type of vehicle and their CSMS are cybersecure, through the evaluation of the documents and the test that they are submitted to.

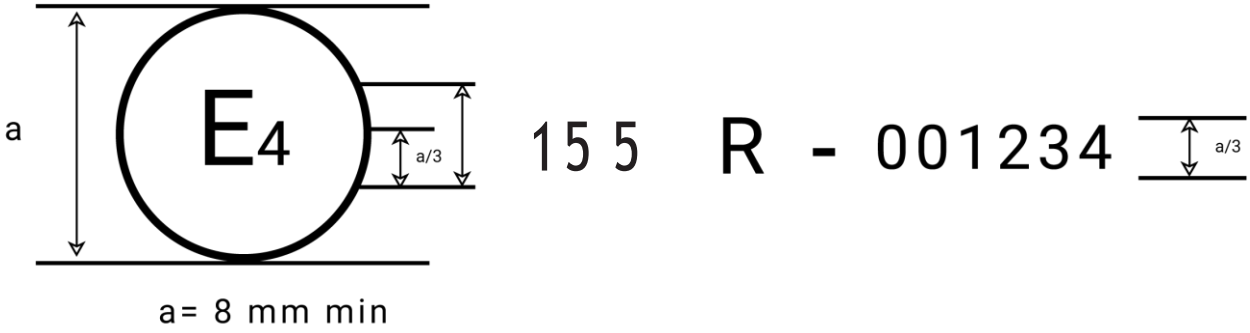
THE AUTHORIZED ENTITY OR TECHNICAL SERVICE that runs the evaluation of the OEM, have to make sure that it complies with the requisites exposed in the 1958 Agreement , Schedule 1 “Conformity of Production Procedures” and Schedule 2. Some of the requisites that the agreement establishes are that the chosen entity must prove that it has the appropriate tools, technical knowledge, and experience in the field to cover the UN´s regulation -in case of the regulation by UN/UNECE/WP29, cybersecurity for vehicles-, it must be free of any control or influence over the interested parties and it must have access to the required equipment to run the tests.

The authorized entities must be previously designated by the makers to run the evaluations and inspections. Until now, it´s unknown whether before the entrance into fruition of the regulation, there will be a more specific document, which will put the methods and criteria in common interpretation.

THIS IS THE CERTIFICATION PROCESS



In English: Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations. Disponible en https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2017/E-ECE-TRANS-505-Rev.3e.pdf



THE LABEL FOR A CYBERSECURE VEHICLE

¿IS THE VEHICLE SUITABLE OR NOT SUITABLE?

The technical service or authorized entity must refuse the concession of the certificate of compliance with the CSMS of the vehicle when:

1. It doesn´t follow one or more of the 70 requisites of cybersecurity demanded by the regulation of UN/UNECE/WP29.

2. In case the maker doesn´t provide the authorized Entity enough information to evaluate the cybersecurity of the vehicle.

VALIDATION FOR THREE YEARS

CSMS conformity certificate **will be valid for a maximum of three years from the date of issue, unless withdrawn**. When the validity of the certificate is close to ending, manufacturers will have to apply for another one -if there have been changes to the regulations-, or it will be extended for another three years. So that, in this case, the designated authorized entity must evaluate that the exposed regulations are still being followed. In case that they don´t follow the requirements upon the expired date, there will be a process of withdrawal.

IT WILL BE MANDATORY

Also, the manufacturer must inform the authorized entity of **any changes that affect the relevance of the certificate** of compliance with the CSMS, such as the appearance of new cyberattacks. After consulting with the manufacturer, the authorized entity will decide if it´s necessary to run new tests to know whether it still follows the mandatory requisites.

LABEL FOR CYBERSECURE VEHICLES

Those vehicles that receive the certificate of compliance with the CSMS must indicate it in their homologation sheet through a symbol. **The symbol is composed by:**

•**A letter ¨E¨** followed by the distinctive number of the country that conceded the certificate, both surrounded by a circle.

•On the right side of that symbol, **it will appear the UN regulation number**.

•That number is followed **by letter ¨R¨, a score and an homologation number.**

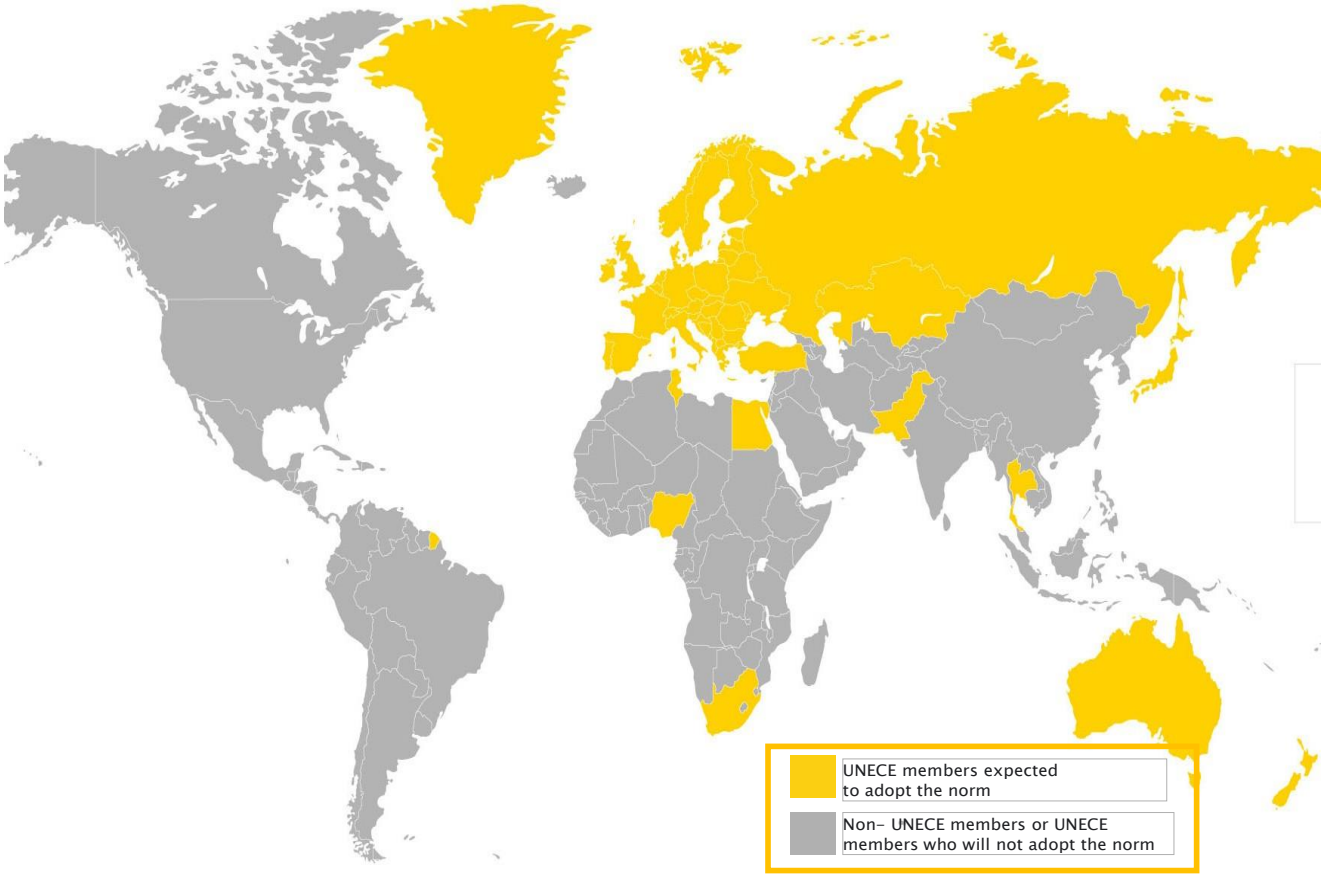
This symbol must be situated in a visible way and with easy access, inside or close to the vehicle´s data plate.

The previous image is an example of a homologation mark, to prove that a vehicle has a certified CSMS according to the requisites by the UN/UNECE/WP29. In this example, **the element that composes the mark of homologation indicates the following:**

• **E4**: It shows that the vehicle has been certified in the Netherlands -the number changes by countries-.

• **155:** It shows the number of regulations for which the car has achieved the certificate.

• **R-001234:** The homologation number. The first two digits of the homologation number-00- signal that it was certified with the requisites for the UN in its original form.



MEMBERS OF UNECE WHAT WILL THEY ADOPT UNECE/R155 REGULATION BECAUSE THEY SIGNED AN AGREEMENT OF RECOGNITION RECIPROCAL APPROVALS

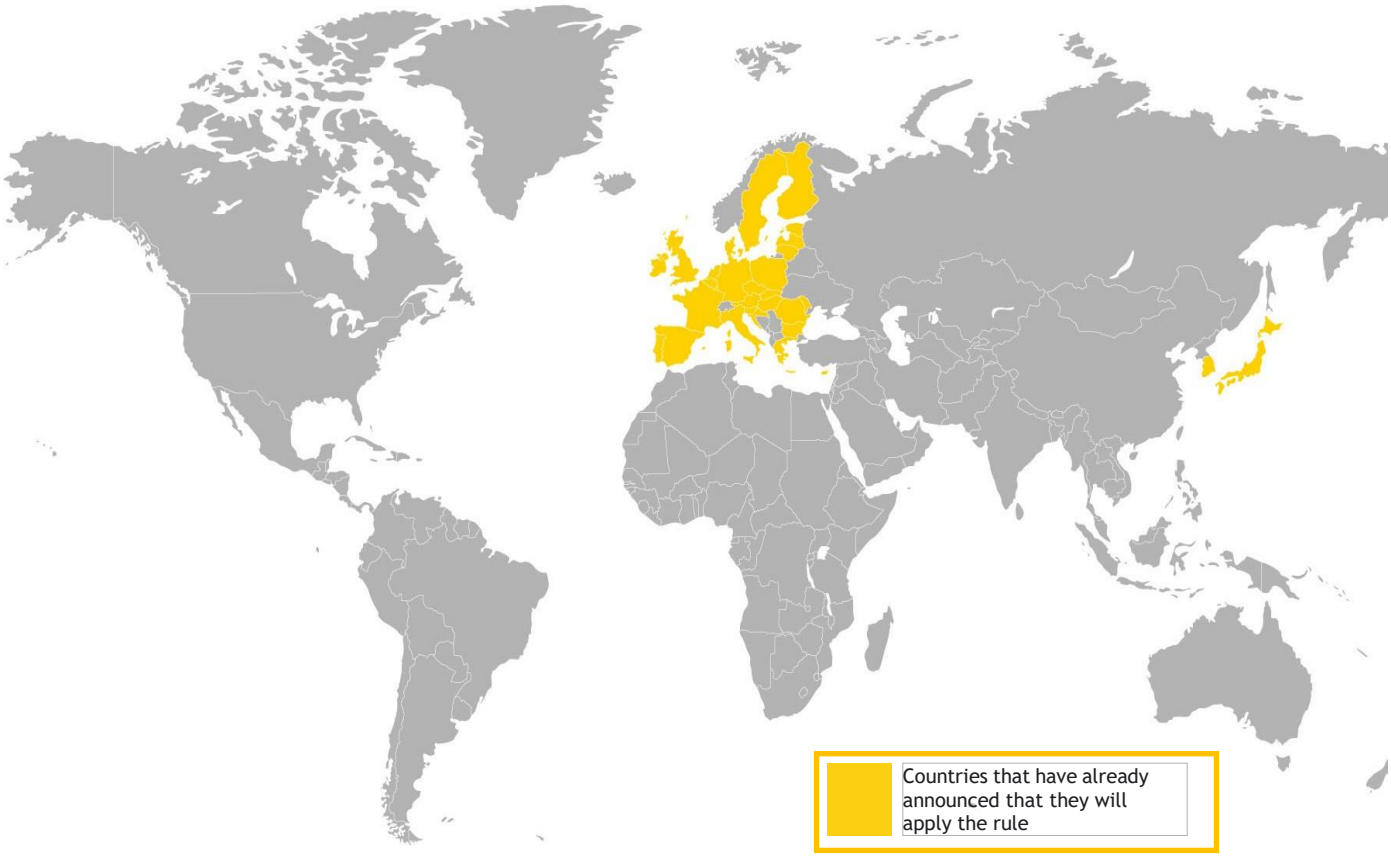
WHICH COUNTRIES WILL APPLY THE RULE AND IN WHAT TIMEFRAMES?

The regulation is approved, and it will come into fruition in January 2021. From then on, 54 states of the 56 members of UNECE -all except the US and Canada- will have to adopt it. Since they are the ones that have signed an agreement of reciprocal recognition of the regulations that this entity approves. Those countries are:

The 54 members of UNECE who applied the standard since January 22, 2021

-Albania
-Armenia
-Australia
-Austria
-Azerbaijan
-Belorussia
-Belgium
-Bosnia Herzegovina
-Bulgaria
-Croatia
-Czech Rep.
-Denmark
-Egypt
-Estonia
-Finland
-France
-Georgia
-Germany
-Greece
-Hungary
-Italy
-Japan
-Kazakhstan
-Latvia
-Lithuania
-Luxembourg
-Malaysia
-Montenegro
-Netherlands
-New Zealand
-Nigeria
-Macedonia
-Norway
-Pakistan
-Poland
-Portugal
-South Korea
-Republic of Moldova
-Romania
-Russian Federation
-San Marino
-Serbia
-Slovakia
-Slovenia
-South Africa
-Spain
-Sweden
-Swiss
-Thailand
-Tunisia
-Turkey
-Ukraine
-UK
-Ireland

On the left are the countries in which the UNECE/R155 standard will begin to be applied within their territories as of January 22, 2021.



COUNTRIES THAT HAVE ALREADY CONFIRMED THAT THEY WILL APPLY THE UNECE/R155 STANDARD IN THEIR TERRITORIES

The EU has established that all vehicles certified beyond the 1 July of 2022 must abide it. The obligation will be extended to all new vehicles beyond the 1 of July of 2024. The Japanese authorities will demand brands that sell vehicles in their territory to follow the regulation from January 2021 forward.
South Korea has been applying since the second semester of 2020, although in a gradual way.

EUROPEAN UNION

-Germany
-Austria
-Belgium
-Bulgaria
-Cyprus
-Croatia
-Denmark
-Slovenia
-Spain
-Estonia
-Finland
-France
-Greece
-Hungary
-Ireland
-Italy
-Latvia
-Lithuania
-Luxemburg
-Malta
-Netherlands
-Poland
-Portugal
-Czech Republic
-Slovakia
-Romania
-Sweden

SOUTH KOREA

JAPAN

https://www.unece.org/trans/maps/un-transport-agreements-and-conventions-18.html

WHAT VEHICLES WILL THE UNECE/R155 AFFECT?

THE REGULATION WILL APPLY TO THE FOLLOWING TYPE OF VEHICLES:

• **CATEGORY M.** Vehicles destined for the transport of people and that have at least 3 wheels and a weight limit above a ton. For example, passenger cars, buses, or motor homes.

• **CATEGORY N.** Vehicles destined for the transport of merchandise with at least 3 wheels and a weight limit above a tovn. For example, vans or trucks.

• **CATEGORY O**, Trailers (including semi-trailers). In this case they are only affected if they are equipped with at least one electronic unit of control.

• **CATEGORIES L6 AND L7.** 4 wheeled Motorcycles, with or without a cabin for the transport of people. In this case, only vehicles with automatic driving functions beyond level 3, will be affected.

Therefore, all manufacturers of passenger cars, vans, trucks, and buses that want to certify new models beyond as of July 2022, or simply, selling new vehicles beyond the first of July of 2024 in countries that are member´s of the EU must follow the requisites demanded by the regulation UNECE/R155.

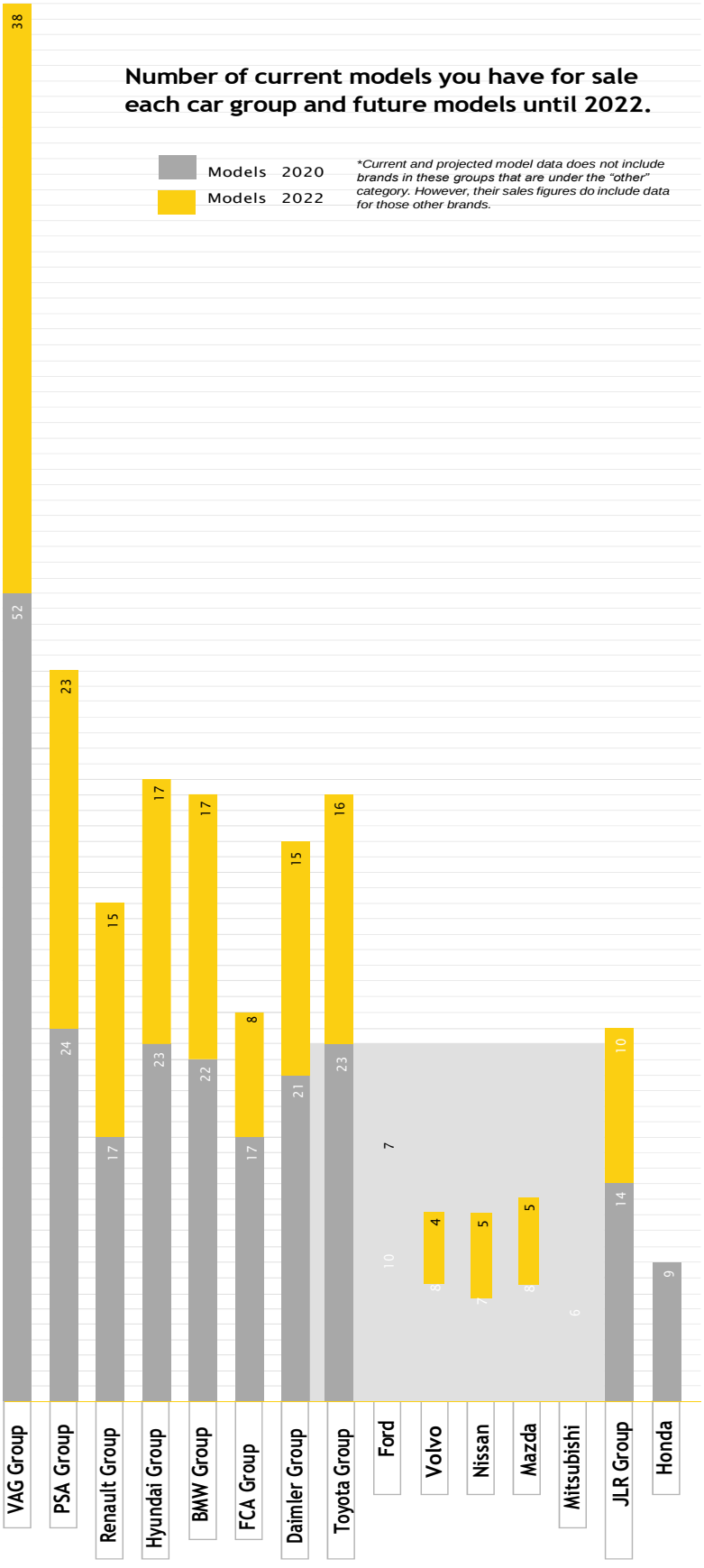
Categories of vehicles affected by the UNECE

Category M:
Cars and buses.

Category N:
Vans and Trucks.

Category O:
Trailers and Camping trailers with an electronic control unit.

Category L6 y L7:
4 wheeled Motorcycles and without a cabin if they have at least level 3 of autonomous driving.



HOW MANY VEHICLES WILL IT AFFECT?

NUMBER OF CURRENT MODELS FOR SALE THAT EACH AUTOMOBILISTIC GROUG HAS AND THE ONES THEY WILL BE LAUNCHING UNTIL 2022

To estimate the quantity of vehicles that will be affected each year by the regulation of the UNECE/R155, we can take 2019 as a reference (the last year in which there is a complete data on the sales of vehicles). In that year 91.358.457 vehicles were sold all over the world. Of that number 22.126.597 units were sold in the EU, Japan and South Korea -the countries that have confirmed that they will be applying the regulation of UN/UNECE/WP29-.

The distribution goes as it follows:

- **15.136.247 units** sold in 2019 in the EU.
- **5.195.216 units** sold in 2019 in Japan.
- **1.795.134 units** sold in 2019 in South Korea.

This means that, of all the vehicles that are sold every year in the world, approximately 25% of them are sold in territories where the regulation UNECE/R155 will be applied.

When it comes to the new models that will be in the market, during the period of 2021-2022, the main automobilist groups that sell in the EU will put 100 new models in sale, that will join the 231 that they already have in their catalogue in 2020 .

This information has been compiled as of October 2020. It is an unofficial calendar of launches expected until 2022, based on the life cycle information of the current models and on the data collected by the team of experts and analysis of Cybentia Group market.
Data from 'Expansion', available at en https://datosmacro.expansion.com/negocios/produccion-vehiculos

WHAT SANCTIONS COULD THE MANUFACTURERS FACE IF THEY DO NOT FOLLOW THE REGULATION?

THE MANUFACTURERS THAT DON´T ABIDE BY THE REGULATION OF THE UNECE/R155 COULD FACE TWO TYPES OF SANCTIONS: ONE FROM UNECE AND THE OTHER FROM THE EU.

- **In case of UNECE/R155,** section 10 of their regulation in cybersecurity in vehicles affirms that a country can withdraw the certification conceded to a type of vehicle if it does not follow the established requisites by the UNECE/R155. Also, that country must notify immediately of the infraction to the rest of the states that follow the same regulation.

- Parallel to this, in order to homologate vehicles **in the EU, it will be necessary to comply with the regulation UNECE/R155** -according to the conditions previously explained-, not doing so will mean not following the regulation of the EU, for which the manufacturer would be sanctioned according to the regulation about homologation and management of the market of engine vehicles.
It assures that, if the EU, detects a manufacturer that has broken the regulations of homologation in their vehicles, it could sanction the Brand for each unit that doesn´t meet the required cybersecurity conditions, The EU could also withdraw or suspend the validation of that type of vehicle.

EUROCYBCAR®
CYBERSECURITY TEST

HOW TO COMPLY WITH THE REGULATION?

A SOLUTION: ESTP –EUROCYBCAR® STANDARD TEST PROTOCOL–

UN/UNECE HAS LEFT MANUFACTURERS FREE to look for solutions to the 70 vulnerabilities reflected in its regulations but does not detail how to avoid such threats. This opens the door for manufacturers to actively collaborate with companies specializing in automotive cybersecurity solutions, like Argus, Upstream, GMV, Guardknox and Harman.

Not even the regulation determines what type of tests must be accomplished to know whether a vehicle can obtain the certificate that labels them as cybersecure. However, there is a company that has a test which determines and certifies whether the vehicle follows the 70 requisites that UN/UNECE WP29 R155 asks for: EUROCYBCAR. The tests are carried out in a laboratory located in Victoria-Gasteiz, where hackers, IT engineers, car testers and Qtesters have been running cybersecurity evaluations- ESTP- for years on vehicles of public organisms and OEM´s.

EUROCYBCAR´S TESTS VERIFYS WHETHER A VEHICLE COMPLYS THE REQUISITES THAT THE UNECE/R155 DEMANDS, CONDUCTING THREE DIFFERENT TYPE OF TESTS

• **PHYSICAL ACCESS:** EUROCYBCAR's team of experts checks whether a cybercriminal could manipulate the airbag, its brakes, or its steering through the vehicle's OBD port; or, for example, if a virus can be introduced through the USB port that causes the vehicle's systems to be stopped and put the passenger´s life at risk.

• **REMOTE ACCESS**: wireless systems such as the Bluetooth connection -which allows the mobile device to be linked to the vehicle to share its data-, WiFi -which provides an internet connection to the passengers' mobile devices-, the eCall -call automatic Emergencies in the event of an accident- or the keyless system -which, for example, allows opening or closing a car without using the key- to check its level of cybersecurity and assess whether data of users is at risk.

• **APP TESTING:** Finally, the vulnerabilities of the apps that are already integrated into the vehicle are evaluated, as well as the official apps of the brand that the user downloads to their mobile. Some of these applications give the user control - from their smartphone - various vehicle parameters - such as turning on the heat before entering - or accessing information stored in the vehicle - such as mileage or routes usually followed by the driver. This is obviously a danger if a cybercriminal succeeds in violating these applications, as it could access the vehicle´s systems and even cause an accident.

THE ESTP METHODOLOGY -EUROCYBCAR Standard Protocol Test- is the only comprehensive TEST in the world -with an international patent- that identifies vulnerabilities and measures the level of cybersecurity of a vehicle -cars, buses, trucks and vans-, according to the requirements of the new regulation UNECE/R155.

Once the vehicle has undergone the EUROCYBCAR test protocol and passed it -it is SUITABLE- it is granted a cybersecurity certificate, with AENOR, which guarantees the level of cybersecurity that the vehicle has obtained.

Most importantly, a good grade in the test will be synonymous with the fact that the car has implemented the minimum measures to prevent someone from remotely taking control of systems such as the steering, the brakes, the engine... and cause accidents with serious risk to the life of the driver and passengers or to any other road users.

FIRST CYBERSECURITY CERTIFICATE: EUROCYBCAR,® NUUK Mobility Solutions and AENOR

According to the UNECE/R155 regulation, inexplicably, motorcycles are exempt from having to have a cybersecurity certificate so that they can be marketed in the European market. However, the brand NMS -NUUK Mobility Solutions-, aware of the importance of cybersecurity, decided to submit one of its vehicles -the CargoPro 6.0- to the EUROCYBCAR Test, marking a world historical milestone by being the first vehicle in the world to obtain a cybersecurity certificate -certification process carried out jointly with AENOR-, according to the UNECE/R155 regulation and applying the ESTP Methodology.ESTP.

The official delivery of this first vehicle cybersecurity certificate was carried out on April 25, 2022 at the NMS headquarters in the Boroa/Amorebieta Business Park -Bizkaia-.

PRESS RELEASE || AENOR AWARDS NUUK THE FIRST CERTIFICATE OF CYBERSECURITY IN VEHICLES WORDLWIDE

25 APRIL, 2022

NUUK Cargopro has received the first "Cybersecurity in Vehicles" certificate from AENOR, after passing the EUROCYBCAR Test - which measures and evaluates the level of cybersecurity of a vehicle, according to the requirements of the UNECE/R155 regulation and applying the ESTP methodology-

PRESS RELEASES

PRESS RELEASE || The world's first 'Cyber-secure Vehicle' is a motorbike made in Europe

23 DECEMBER, 2021

For the first time in history, a vehicle has passed the test that guarantees its status as a "cyber-secure vehicle" according to UNECE/R155 regulations and according to the ESTP procedure and methodology developed by EUROCYBCAR , a technology company based in Vitoria-Gasteiz, Spain.

PRESS RELEASES

More info:

- https://eurocybcar.com/comunicado-de-prensa-aenor-entrega-a-nuuk-el-primer-certificado-de-ciberseguridad-en-vehiculos-del-mundo/
- https://eurocybcar.com/comunicado-de-prensa-el-primer-vehiculo-ciberseguro-del-mundo-es-una-moto-fabricada-en-espana/

WHAT DO EXPERTS THINK?

PABLO ESCAPA, CTO OF EUROCYBCAR

Pablo Escapa has participated in a Spanish working group that has contributed to the development of the regulations of UNECE/R155. Escapa stated that these regulations are intended to regulate the mechanisms that vehicles are equipped with to be cybersecure. In other words, having tools both to avoid and mitigate the attacks to which they may be exposed. 100% cybersecurity is not possible, but it will be very difficult to carry out a cyberattack on a car if all regulations are met.

In addition, the rule will apply to all future cars sold in Europe -and other countries within the confines of the UN/UNECE. A certificate of conformity on cybersecurity will be required to approve vehicles destined for the European economic area". What is the most revolutionary thing about the regulation? In his opinion, it will be the management system for over the air updates that coexists with the regulation.

Adapting to the new regulation to implement cybersecurity in all of their processes, will pose a great challenge for vehicle manufacturers, in time and economic resources, since the new requirements are very exhaustive- more appropiate for the protection of a critical infrastructure- given that autonomous driving is considered a critical activity. Luckily, there are already manufacturers who are getting ahead and adapting to the new regulation, even conducting ESTP on their models.

AZUCENA HERNÁNDEZ, CEO OF EUROCYBCAR

We have been raising awareness with institutions and companies within Spain and Europe so that "cybersecurity by design" becomes the regulation for cybersecure mobility in the future and the UN/UNECE has agreed with the new regulation that came into fruition on January 22 of 2021 and which mandates vehicle manufacturers to incorporate cybersecurity from the design phase, even in their management systems.

The UNECE/R155 is a drastic regulation because it demands vehicles to have a cybersecurity certificate that acknowledges that they are minimally protected against cyberattacks and goes as far as to close the European market for cars, buses, trucks and wagons that do not comply with the 70 requisites which the regulation applies.

It´s a drastic regulation, but very necessary, since vehicles are computers on wheels and must be protected as such, at least, in the same way you would protect your phone or laptop. The consequences of not having a protected vehicle could be tragic: it´s enough with one person inserting a pen drive with downloaded music, not knowing it had a virus or a malware which can infect the vehicle- to provoke the stop of the engine or disconnect the brake systems, for example.

NURIA ROMÁN
HEAD OF AREA OF THE GENERAL SUB-DIRECTION OF QUALITY AND INDUSTRIAL SAFETY (MINISTRY OF INDUSTRY, TRADE AND TOURISM). IN ADDITION, SHE HAS LED THE SPANISH UN/UNECE WORKING GROUP

"The regulation requires designing the architecture of vehicles considering cybersecurity, so the integration of components will be provided from a 'cybersecure' point of view".

WHAT ASPECTS OF THE RULE DO YOU THINK ARE THE HIGHLIGHTS?

Today's vehicles are already designed with complex electronic and information systems, which, for example, allow the vehicle to be opened or started, handle fuel injection, and therefore engine operating functions, monitoring vehicle systems and providing diagnostic information for repair or intervention in emergencies. Ensuring a minimum level of security when accessing these systems is what the new cybersecurity regulation aims for.

This regulation will enable protection to be assessed against unauthorized access to information and systems contained in vehicles, harmonizing the minimums that must be met by manufacturers, who until now adopted protection measures that weren´t evaluated throughout the process of validation. The most prominent of the requirements is that it forces you to consider the cybersecurity aspects from an architecture design and incorporate cybersecurity into the vehicle´s manufacturers management systems.

ONCE THE REGULATIONS COME INTO FORCE, WHAT ARE THE NEXT STEPS TO FOLLOW?

The EU establishes a frame of homologation for vehicles, which vehicles must comply with to be tradeable in the internal market. Until then, manufacturers can apply it voluntarily, but from the time it is mandatory, new types of vehicles that do not comply with it can´t be homologated. Once the cybersecurity regulations for European homologation is active, foreseeable for 2022, said regulation must be evaluated along the rest of demands required for the process of homologation. Until then, manufacturers can apply it voluntarily, but from the moment it comes into fruition, new models that don´t meet the requirements won´t be able to be certified.

HOW DOES THE PROCESS TO EVALUATE WHETHER A VEHICLE TYPE HAS A CSMS THAT FOLLOWS THIS NEW REGULATION WORK?

It is a complex regulation, different to the traditional regulations in which it´s not possible to identify a test to be carried out on the worst-case scenarios. The regulation takes this difficulty into account and uses the methodology of risks analysis and the specification of minimum threats and protections to be contemplated in a vehicle. In addition, an implementation guide is being developed that recommends the use of various methodologies for assessing cybersecurity management systems and information security. In the first instance, it is the manufacturer that must evaluate compliance with the requirements, documenting the risk analysis, protection measures, their implementation and the tests executed to verify their effectiveness. Afterwards, the technical service will evaluate the conformity of all this evidence and through a sample, conduct other tests. In any case, you should follow the recommendations of the implementation guide, which is still in development.

WHY DO JAPAN AND KOREA WANT TO GET AHEAD OF THE DATE OF IMPOSITION OF THE RULE? DO THESE COUNTRIES ALREADY HAVE EVALUATION PROTOCOLS?

These are two countries that are very advanced in electronic and automatic technology. We do not know the status of their evaluation protocols, although the implementation guide developed in the United Nations group already offers the possibility of applying several standardized evaluation methodo-

logies. In any case, the date of implementation in the EU is also very close, in 2022. Since the 1958 agreement on technical harmonization requires mutual recognition of homologations granted between the signatory parties, it is ideal to use the implementation guide finally agreed upon in that forum.

ARE MANUFACTURERS READY TO APPLY THE REGULATIONS? WHAT EFFORTS WILL IT ENTAIL? WHAT IS THE BIGGEST CHANGE THAT A MANUFACTURER MUST ACHIEVE TO MEET THE REQUIREMENTS?

Evidently, the entry into fruition of a new regulation requires adaptations from industries. However, technology is often ahead of regulations, and in this case, industries do not start from scratch to adapt regulations. Manufacturers already considered the protection of the information systems present in the vehicle, before the regulation, what changes now is that they must adapt to the requirements of the regulation and be evaluated during the vehicle homologation process.

THE REGULATIONS ALSO INDICATE THAT ALL DEPARTMENTS INVOLVED IN THE PRODUCTION OF A VEHICLE TYPE WILL BE AFFECTED, HOW WILL THIS AFFECT WORKSHOPS AND SUPPLIERS?

The vehicle´s manufacturing process incorporates components and systems from a diversity of suppliers. The regulation requires designing the architecture of vehicles considering cybersecurity, so the integration of components will be provided from a "cybersecure" point of view. However, there is no doubt that the regulation also affects suppliers of systems and components, and like this the vehicle manufacturer must consider the risks associated with the final vehicle, incorporating those components, which require cybersecurity to be taken into account throughout the supply chain.

WHY DOES THIS REGULATION NOT AFFECT TO MOTORCYCLES, BOATS OR TRAINS? WILL BE THERE ANY REGULATIONS ON THIS SOON?

The 1958 Geneva Agreement on Technical Harmonization, which serves as a framework for cybersecurity regulations, affects only wheeled vehicles. In the case of motorcycles, they have not been considered in this first version of the regulation due to their lower level of progress towards automated driving, for now at least.

EUROCYBCAR®
CYBERSECURITY TEST

WHAT TO KNOW ABOUT EUROCYBCAR®?

EUROCYBCAR SL is a technology-based company, with their headquarters in Vitoria-Gasteiz, that develops innovative cybersecurity products and services for the automotive/mobility sector that protects people's vehicles, lives, and data.

EUROCYBCAR is a global pioneer in combining cybersecurity, automotive and mobility in its core business, thereby developing a whole portfolio of products and services with the aim of achieving a comprehensive protection of mobility in the field of cybersecurity.

EUROCYBCAR has some proven expertise - more than 30 years of experience - in Research, Automotive, Mobility and Cybersecurity, with the core of the team being made of hackers, researchers, ITs, security experts, car testers and law experts.

EUROCYBCAR has created the first test in the world that abides by the new security regulation UNECE/R155 and measures the level of cybersecurity of a vehicle, based on two parameters: How it protects the privacy of the driver and passengers - ITS DATA - and, most importantly, THEIR LIFES. The protocol for technical evaluation- in the process of international patent- is conducted in Eurocybcar laboratory in Vitoria-Gasteiz.

In addition, **EUROCYBCAR** has developed other products and services - always related to cybersecurity and mobility - such as the Cybersecurity Test for Fleet Management Systems or the V2D Test – a test for the connections between the car and the devices that the user connects to the vehicle-, the test for transportation apps, the test for smart tires or the test for locomotive/trains, are some examples of EUROCYBCAR´s concern for a safer mobility.

MORE ABOUT US

WWW.EUROCYBCAR.COM
PARQUE TECNOLÓGICO DE ÁLAVA EDIFICIO BIC
ALBERT EINSTEIN KALEA, 15 01510
VITORIA-GASTEIZ, ÁLAVA
+34 619 291 892
INFO@EUROCYBCAR.COM