

UNECE CYBERSECURITY REGULATION (R155)

State of the Art and Relation With
ISO 21434 and TISAX Standards

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W www.secura.com

Follow us on   



UNECE Cybersecurity Regulation (R155)

State of the Art and Relation With ISO 21434 and TISAX Standards

The UNECE (United Nations Economic Commission for Europe) has been working in the past years on a new regulation, focused on Cybersecurity for road vehicles. The regulation has been formally adopted in June 2020, and has entered into force from January 2021. Under the new regulation, vehicle manufacturers (OEMs) will need to satisfy the Cyber Security Management System (CSMS) requirements in order to be allowed to apply for type approval of specific vehicle types.

The regulation will be applicable to all UNECE member countries of the 1958 Agreement, which ensures a wide global coverage. Within this article, we will provide, as an introduction, the general regulatory environment under UNECE. Furthermore, a high-level view on the cybersecurity regulation requirements will be given. A specific focus will be on the aspects, which are expected to be particularly challenging for vehicle manufacturers. Finally, the relation between the R155 requirements and international standards such as ISO SAE 21434 or TISAX will be discussed.

1. The Vehicle Regulatory Environment

The domain of road vehicles is one of the most strictly regulated verticals. Thinking about the constant expansion of the number of vehicles that are driving on our streets, combined with the risks (especially financial and human life related) which are associated with the misuse of vehicles, the existence of strict regulations is very understandable. At the same time, the regulatory environment is not uniform throughout the world.

Different countries, regions and continents have slightly different rules concerning the scope and coverage of these regulations. For example, in the United States market access for vehicles is regulated under the Federal Motor Vehicles Safety Standards. In Canada vehicles have to comply with the Canada Vehicle Motor Standards. In Brazil automotive components and systems need to obtain market access based on the regulations imposed by INMETRO. At the same time, this does not mean

Table of Contents

1. The Vehicle Regulatory Environment	3
2. The Need for a Cybersecurity Regulation	5
3. UNECE Cybersecurity Regulation (R155) in Focus	6
3.1 Risk Management Considerations	7
3.2 Supply Chain Interaction Considerations	7
4. Complying With the R155 Regulation in Practice and Its Relation to Other Industry Standards	8
4.1 The "Regulation Based Approach"	8
4.2 The "Standards Based Approach"	10
5. Conclusion	11
References	12



that the landscape of vehicle regulations is fragmented to specific rules for each individual country.

UNECE, the United Nations Economic Commission for Europe, is a regulatory body that issues road vehicles regulations, which are recognized and applied by multiple countries in the world. Within UNECE, a specific working party exists, named the World Forum for Harmonization of Vehicle Regulations, or shortly, WP29. WP29 is responsible for the development, publication and maintenance of vehicle regulations. These regulations are directly recognized and applied by member countries of the UNECE 1958 Agreement. This agreement puts together a wide number of countries spread across the world. Currently there are 62 member countries of the 1958 Agreement, including most of the countries in Europe, Russia, Japan, South Korea, Australia, UK, parts of Africa and parts of the Americas. These countries recognize not only the regulations, but also the vehicle type approvals (under these regulation) issued by the member countries. When a vehicle manufacturer aims to place a (new) vehicle on the 1958 Agreement countries' markets, they should demonstrate compliance only to the regulations of one of the member countries.

Currently, there are 135 different regulations appended under the 1958 Agreement. Most of them are covering a single vehicle component or technology. Examples of such regulations include ones for braking systems, vehicle lamps, steering equipment, seat belts, emissions and fuel consumption, sound emissions of tires, etc. For each vehicle type that manufacturers aim to place in a country governed by the 1958 Agreement, they need to demonstrate compliance with all the applicable regulations. This is typically done in a form of a type approval audit conducted by a National Vehicle Approval Authority in one of the 1958 Agreement countries. In turn the Authority issues a type approval certificate to the OEM, given that all the requirements of the regulation are satisfied. Different issued type approvals have different expiration dates, and it is mostly up to the OEM to determine when a type approval needs to be updated or renewed.

2. The Need for A Cybersecurity Regulation

As mentioned in section 1 of this paper, there are currently 135 different UNECE regulations that OEMs need to fulfil. However, all of them are focused on topics such as safety, vehicle performance, or environmental impact. This focus makes perfect sense given the classic definition of a vehicle, and the risks associated with its usage.

Until recently, road vehicles were solely designed to ensure safe transportation of persons or goods from one place to another. In the last few years though, the IoT paradigm has slightly changed the view on the automotive ecosystem. Connected technologies like GPS, Wi-Fi, Bluetooth, V2V, keyless entry and other, have been massively introduced in common vehicles in order to enhance the driving experience and make it generally more enjoyable.

Nowadays, it is hard to consider buying a vehicle, which does not include, at a minimum, communication interfaces such as a USB or a Bluetooth, support for road navigation or a hands-free connection to the mobile phone. Given this aspect, modern vehicles have become endpoints in our definition of IoT. Moreover, they are now connected not only to the users' mobile devices, but also through smart applications directly to broad cloud systems, and implicitly, to each other. This aspect is both amazing and somewhat

concerning from a risk analysis point of view.

The main reason for a concern is the high rate in development of relevant cyber-attacks, which could target such vehicles. As the focus of the OEMs has been mostly on safety and performance aspects (in line with existing regulations), security vulnerabilities introduced by the available connected functions have led to a series of demonstrated attacks in the last years, including the nowadays-famous attack on the Jeep Cherokee [1].

Such attacks have considerably raised the awareness of the OEMs, users, but also UNECE on the need to ensure proper regulatory requirements for cybersecurity. This need resulted in an effort for drafting a new regulation, focused specifically on this topic. The drafting effort took into account the feedback and opinion of multiple OEM companies, national Approval Authorities, and specialized testing facilities. After a few rounds of creating intermediate documents and validation pilot projects, the new regulation has been officially adopted at the end of June 2020 [2] and entered into force from the beginning of 2021.

Under this new regulation, vehicle manufacturers will need to showcase that sufficient controls aimed at protection of cybersecurity aspects are embedded into the vehicles, before making them available on the public roads. Therefore, it can be said that the race towards cybersecurity compliance has now started, and the winner of this race will finally be the automotive ecosystem as a whole.



3. UNECE Cybersecurity Regulation (R155) in Focus

The intention of this article is not to fully dive into the details of the UNECE R155 – cybersecurity – regulation. Such documents, including dedicated Interpretation Guides, were already published by UNECE. However, this article aims to provide a summary of the most important requirements under this regulation.

The Cybersecurity regulation consists of the two main parts – Cybersecurity Management System (CSMS) Requirements and Vehicle Type requirements. The CSMS requirements focus on the processes that have to be drafted and followed by the OEM during the whole life cycle of the vehicle. These processes have to cover all the phases, including creating a concept, development, production, post production monitoring, and finally decommissioning. The vehicle type requirements then focus on the validation that the documented processes have been properly applied by the OEMs.

The list of processes required under the regulation includes ones, which could be expected from a security point of view, such as definition of roles and responsibilities, security risk management and determination of necessary controls, configuration management, vulnerability analysis and incident response, postproduction patch management, supply chain interaction.

All of these processes should be properly documented and made available to the Approval Authority during the audit. The evidence that the required processes are acknowledged and applied by the relevant employees will also be audited and validated.

Among the whole list of processes, two of them have a specific importance, as they introduce further dependencies: risk management and supply chain interaction.



3.1 Risk Management Considerations

Efficient risk management is a key to control the cybersecurity threats. The regulation does not mandate for a specific risk management standard that the OEMs need to follow in order to ensure compliance. Instead, own processes are acceptable as long as they are covering the minimum expectations, which include:

- Determination of applicable threats
- Calculation of the applicable risks
- Determination of applicable security controls in order to address the risks
- Keeping the risk assessment up to date
- Testing and validation of the implemented security controls
- Acceptance of residual risks
- Dealing with new threats and vulnerabilities

The OEMs are expected to have documented processes in place covering these topics. During an audit, they should also be able to demonstrate that these processes are indeed applied in practice. For example, by showing evidence of conducted risk assessments and the definition of security controls. At the same time, it needs to be taken into account that these processes have to address the whole life cycle of the vehicle (as far as applicable). That being said, for example, the process of dealing with existing vulnerabilities needs to be strongly considered during the concept and development phases, while at the same time, it should be constantly used for possible new vulnerabilities released after the vehicle is in the production phase.

3.2 Supply Chain Interaction Considerations

The automotive domain is arguably one of the domains in which supply chain dependency is the most accentuated. This comes due to the fact that OEMs are mostly integrating components supplied from the third parties. These components include both hardware and software parts (ICs, ECUs, infotainment systems, specific software, etc.). On top of this, modern connected vehicles also rely on cloud service providers for aspects such as over-the-air (OTA) software

updates. Considering this, OEMs depend strictly on the interaction with their supply chain providers. This process takes typically into account multiple phases, including:

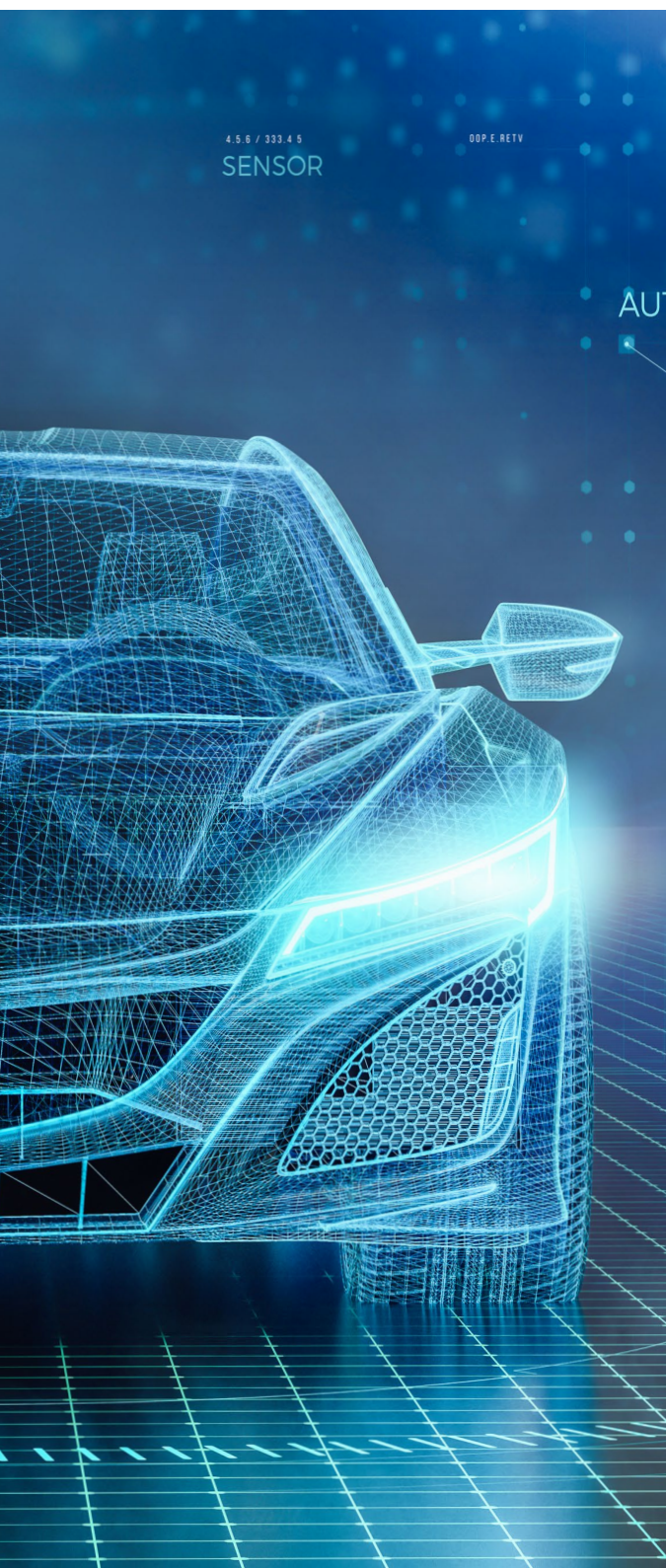
- Initial selection and validation of the supplier
- Analysis of particular component needs, and expected interaction with the rest of the components and the vehicle architecture
- Delivery of the particular component requirements to the supplier
- Intake and validation (testing) of the received components
- Integration of the received components in the architecture and validation at system/vehicle level

As it can be hinted from the above list, the dependencies with the supply chain introduce a stringent impact on the development timelines. As it can be hinted from the above list, the dependencies with the supply chain introduce a stringent impact on the development timelines. All of the above steps require extensive periods of time, which typically result in development lifecycles that extend over 3-4 years for many OEMs.

Having the need to go back a few steps due to some unexpected situation might then understandably represent a big impact. For example, a mistake in the considered dependencies of a component to the rest of the architecture would require the OEM to go back to the step of defining component requirements, which, depending on the moment of this situation, might translate in years of delay for placing the vehicle on the market.

On top of this, now the cybersecurity of components needs to be taken into account while interacting with the supply chain. OEMs have to determine specific security requirements. They need to be clearly communicated to the providers and then validated to determine if the received components indeed meet these specified requirements. Finally, as the regulation asks for processes under the whole vehicle life cycle, the ability to work together with the suppliers in order to detect and treat new threats and vulnerabilities is also an essential requirement. Multiplying this by the range of hundreds independent components used in each vehicle, it results in a big need for efficient supply chain cybersecurity management.

4. Complying With the R155 Regulation in Practice and Its Relation to Other Industry Standards



Since the early stages, Secura has been involved in the drafting efforts linked with the UNECE R155 regulation. Through this experience, we have been in contact with several vehicle manufacturers and suppliers. It allowed us to learn several interesting aspects regarding the practical adaptation and implementation of the regulation. We noticed that at this point OEMs and the supply chain typically use two types of approach when it comes to demonstrating R155 compliance: the “regulation based approach” and the “standards based approach”. These two types of approach can both be successfully implemented, and will both lead to successful results. They are explained more in detail in the next sub sections.

4.1 The "Regulation Based Approach"

What we call the “regulation based approach” is when a vehicle manufacturer or a supplier aim to achieve compliance with the R155 regulation by taking all the applicable requirements one by one and trying to address the remaining gaps. Of course, since all the requirements are taken into consideration, this approach will bring successful results.

From our experience, most manufacturers tend to split the effort into the parts applicable for the CSMS, and the parts applicable for the vehicle type requirements. By carefully selecting and interpreting the requirements of both CSMS and vehicle type parts, it is possible to effectively split these tasks within the internal organization of the vehicle manufacturer. It is quite likely that the manufacturer already has some of the required processes in place, especially if the cybersecurity was taken into account during the recent development stages. This approach would definitely be beneficial for the manufacturer, as they can start their R155 compliance journey by building on top of their existing processes.

Many of the processes required by R155 would be topics that manufacturers most likely encountered and considered before. These include, for example, incorporating cybersecurity during product development, dealing with security incidents, or performing security testing. In these situations, it is likely that manufacturers would want to focus on identifying the remaining gaps with respect

to the R155 regulation, and directly incorporate them in the existing processes.

However, some of the processes required by R155 could be new to the OEMs. For example, such aspects as security vulnerabilities monitoring and management, or management of security across the supply chain. These are the possible gaps where the vehicle manufacturers might need to spend a bit more time to understand the R155 requirements, and then update or introduce new procedures.

An important point to consider is that CSMS compliance will only require the OEMs to draft, implement and be in control of the processes. The actual evidence resulting from the processes, linked to a specific vehicle type, will not be needed in order to obtain the CSMS certificate of compliance. Therefore, the OEM does not need to have in place the complete set of risk assessment results, or complete set of security testing results in order to be certified for their CSMS. Just a simple example demonstrating that the process is in place and returns results will be sufficient at this point.

However, the CSMS certification will only be the first step of the process for the OEMs. The main outcome of the R155 regulation is the ability to certify a specific vehicle type. When the OEM is ready to apply for a type approval evaluation, all the evidence associated with the vehicle type requirements should be in place. This includes items such as complete risk assessment results, complete testing results, complete package of evidence received from the suppliers, and so on.

In conclusion, the OEM can postpone the deadline for having in place all the vehicle specific evidence until the moment of application for type approval, while still certifying their CSMS set of processes earlier.

The “regulation based approach” works best in practice for OEMs who already considered cybersecurity in the past years, and started incorporating it in their processes. In this case, OEMs can simply continue to identify the remaining gaps with respect to the R155 regulation, and address these gaps one by one, until a compliance state is achieved.

Secura is a recognized Technical Service for offering UNECE R155 certification for vehicle manufacturers, under the Dutch (E4) and Cyprus (E49) road authorities. Our services cover the full range of R155, starting from initial trainings and workshops, all the way to consultancy and, of course, the final certification audits.





4.2 The "Standards Based Approach"

There are cases when the OEMs have not taken cybersecurity into account (too extensively) in their processes during the last years. That is easily explainable by the fact that R155 regulation has been adopted very recently, and previously the focus was on safety of the vehicles. In such circumstances, going with compliance method based on international standards could be the best option for OEMs. Two relevant standards will be further discussed: ISO 21434 and TISAX.

ISO 21434 standard has been developed in a very similar timeframe with the R155 regulation. The drafting group of people for these two publications has a good overlap as well. The main intention of the standard is to become a clear and useful companion for vehicle manufacturers and automotive suppliers who intent to achieve compliance with the R155 regulation.

ISO 21434 has been developed based on a structure that is very similar to the one used for ISO 26262. ISO 26262, an automotive safety oriented standard, has already been adopted and used by a large number of OEMs in the past years. By using a similar structure and set of requirements, one of the objectives of ISO 21434 is to allow the OEMs to implement cybersecurity directly on top of their existing safety related processes.

ISO 21434 is a process-oriented standard, which can be applied by the OEMs in order to obtain a set of final deliverables, which would allow to address both the CSMS requirements, as well as the vehicle type requirements of the R155 regulation.

The standard consists of several sections, which include:

- Processes related to secure development, production and postproduction of vehicles and components;
- Security governance, training and competences management;
- Incident response;
- Security vulnerabilities monitoring and vulnerabilities management;
- Security focused risk assessment and definition of mitigations;
- Security testing and validation;
- Supply chain interaction and management;
- Decommissioning processes.

The standard requires that each category of processes should be implemented and documented by the OEMs. Then the evidence needed to demonstrate that the process is applied in practice for the vehicle or component in scope can be created.

For example, the risk assessment requirements define the methodology that the manufacturer needs to have in place to conduct risk assessments as well as the work products (deliverables) that need to be drafted to demonstrate all the results of the process. Most of the times, the effort needed to have all the deliverables in place will be much higher than the effort needed to establish and document the process. Keeping the risk assessment example, imagine that the risk assessment will need to be performed for all of the relevant items (e.g. ECUs, or backend components) of the vehicle in scope.

However, despite the fact that it requires quite a bit of effort and time to fully implement ISO 21434 standard in a correct and complete way, the results will be very valuable for the OEMs or suppliers. For the OEMs, it will result in a clear set of evidence that can be used directly during the type approval and CSMS audits organized by the Approval Authority. For the suppliers, it will create a common language based on which they can easily understand the requirements of the OEMs, and follow-up in a quick manner with the required set of evidence. Furthermore, for vehicle manufacturers that have not yet considered security in their processes before, starting with the ISO 21434 standard implementation could be the easiest way to begin.

The TISAX standard was drafted and intensely supported by the German automotive industry. Before the regulations such as R155 or standards such as ISO 21434 were in place, several German vehicle manufacturers wanted to have a standardized way to ensure that their suppliers have taken security into account sufficiently, therefore increasing the trust in them as a company. TISAX is strongly inspired by ISO 27001, and is an organization-focused standard rather than a product related standard. That being said, if a vehicle manufacturer or a supplier follows (and is certified) based on TISAX, it means that their organization is taken security strongly into account. That is an important and critical benefit in terms of increasing trust of the organization. However, important to remember that a TISAX certificate does not cover the security of the product or the service offered by the organization, and separate agreements (such as request for risk assessment or test results) should be put in place between the OEM and the supplier.

Considering all of the above, TISAX and ISO 21434 standards are complementary to each other, and both can be very valuable in their own ways to automotive industry. An ISO 21434 compliance and certificate can directly help organizations to demonstrate compliance with R155 regulation, and, especially for suppliers, allow them to easily interact with the OEMs and provide the required evidence. A TISAX certificate allows the suppliers to demonstrate importance of cybersecurity at their organization, and therefore prove that they can be a trusted partner for the OEMs.

Secura can support vehicle manufacturers and automotive suppliers with a full range of services related to ISO 21434 and TISAX standards such as official certification audits as well as training and pre-audit preparation.

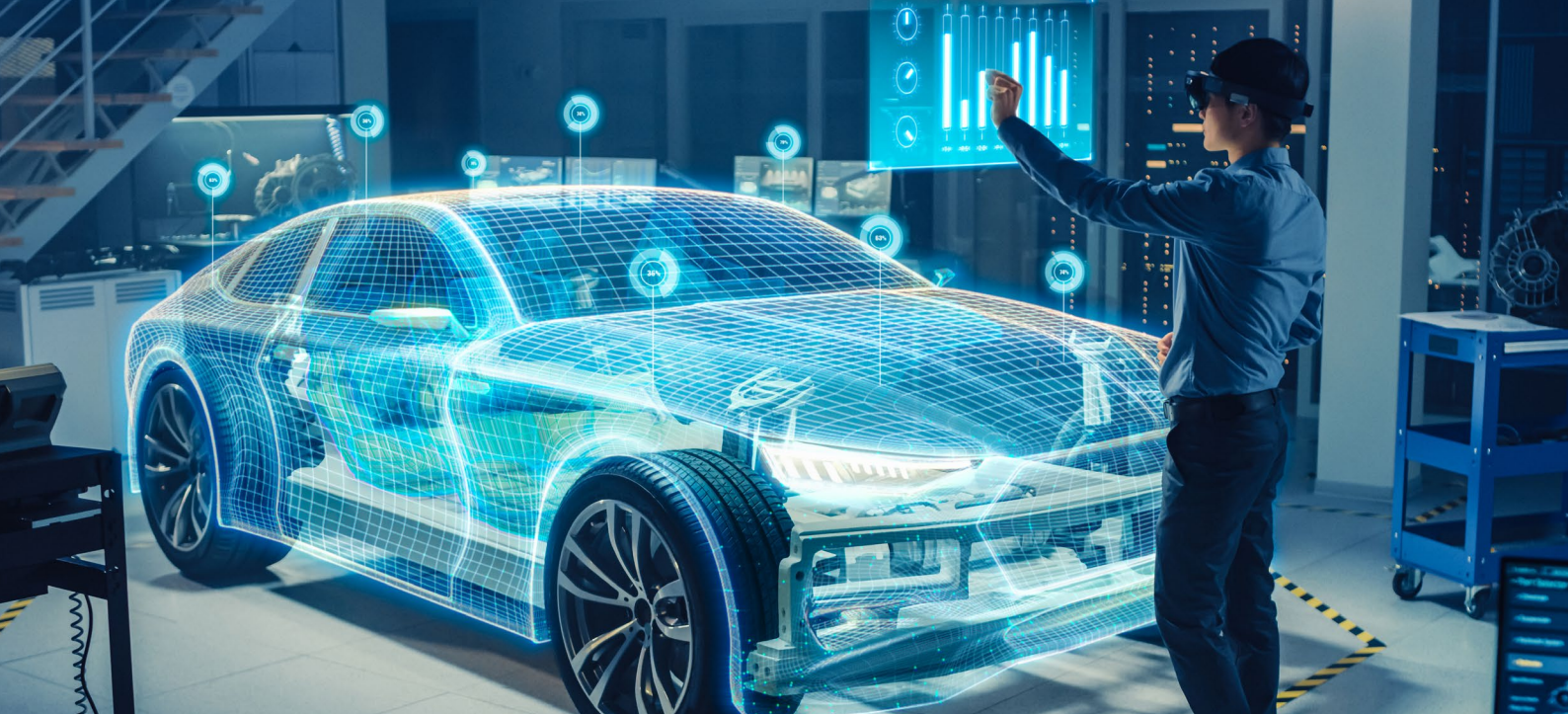
5. Conclusion and the Way Forward

The new UNECE regulation on cybersecurity will address areas which were previously not in scope for international road vehicle regulations. With increasing vehicle connectivity and a rise of associated vulnerabilities and threats, the new regulation is expected to have an overall positive impact on the automotive ecosystem.

The new regulation will require the OEMs to have well-structured and documented processes related to cybersecurity issues. While some of these processes might be directly available and in place, others will require careful consideration in order to ensure a compliance state.

The regulation has come into force in 2021 and will be mandatory for new vehicle types in the EU starting from July 2022. Considering these timelines, OEMs need to address the remaining gaps very carefully and timely in order to be ready for the type approval. It is expected that the initial period when the regulation becomes mandatory will be challenging, but the long-term effect will be a positive one. With the global recognition and adoption of the UNECE regulation, it is also expected that other non-UNECE countries will take this as an example and will further implement their own solutions to address these modern-day threats.

Finally, as discussed above in this article, internationally recognized standards such as ISO 21434 or TISAX could come as useful resources for OEMs and suppliers. Such standards can be used to create a common language between these two parties, but also allow them to understand easier what processes and deliverables need to be achieved for UNECE R155 compliance.



References




1. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, last accessed 08.02.2022
2. <https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll>, last accessed 08.02.2022
3. UNECE Regulations on Cybersecurity and Software Updates - The Calm Before the Storm, Author: Razvan Venter, paper presented at ESCAR 2021

About Secura

Secura has worked in information security and privacy for over two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organizations with up-to-date knowledge to work toward a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Follow us on:   

Contact us today at
info@secura.com or
visit secura.com for
more information.

SUBSCRIBE

TO OUR NEWSLETTER

