UNECE REGULATIONS

On Cybersecurity and Software Updates: The Calm Before the Storm

Razvan Venter, Products Security Manager at Secura
January 2021
UNECE Regulations

On Cybersecurity and Software Updates: The Calm Before the Storm

The UNECE (United Nations Economic Commission for Europe) has been working in the past years on drafting two new international regulations, focused on Cybersecurity and Software Updates. The regulations have been adopted formally in June 2020, and are scheduled to enter into force from January 2021. Under the new regulations, vehicle manufacturers (OEMs) will need to satisfy the Cyber Security Management System (CSMS) and Software Updates Management System (SUMS) requirements in order to be allow to apply for type approval of specific vehicle types. The regulations will be applicable under all the UNECE member countries of the 1958 agreement, which ensures a wide global coverage.

This white paper will discuss, as an introduction, the general regulatory environment under UNECE. Furthermore, a high level view on the cybersecurity and software updates regulations requirements will be given, with specific focus on aspects which are expected to be particularly challenging for vehicle manufacturers. Finally, a conclusion and concrete timelines for the implementation are provided.

Table of Contents

1. Introduction & Background of Vehicle Regulatory Environment 3
2. The Need for Cybersecurity & Software Updates Regulations 5
3. UNECE Cybersecurity Regulation in Focus 6
   3.1 Risk Management Considerations 7
   3.2 Supply Chain Interaction Considerations 7
4. UNECE Software Updates Regulation in Focus 8
   4.1 Considerations Concerning the RXSWIN 8
5. Rules for Adoption and Timelines 9
6. Conclusion and Way Forward 10
7. Secura Supports OEMs During the Whole Journey to Compliance 11
References 12

1. Introduction and Background of Vehicle Regulatory Environment

The domain of 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, also 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, as different countries, regions or continents have slightly different rules concerning the scope and coverage of these regulations.

For example, in the United States, the access to market for the vehicles is regulated under the Federal Motor Vehicles Safety Standards. In Canada, the vehicles have to comply with the Canada Vehicle Motor Standards. In Brazil, automotive components and systems need to obtain the market access based on the regulations imposed by INMETRO.
At the same time, this does not mean 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 body that is issuing 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 put together a wide series of countries, spread across the world. Currently there are 62 member countries of the 1958 agreement, examples including most of the countries in Europe, Russia, Japan, South Korea, Australia, UK, parts of Africa and parts of the Americas.

For reference, Figure 1 provides the world distribution of the countries clustered under the 1958 agreement. These countries recognize not only the regulations, but also the vehicle type approvals (under a specific regulation) issued by each other, such that a vehicle manufacturer who is aiming to place a vehicle on the 1958 Agreement markets needs theoretically to demonstrate the compliance to the regulations only to one of the member countries of this agreement.

**Currently, there are 135 different regulations appended under the 1958 agreement**, most of them covering a single vehicle component or technology. Examples of such regulations include braking systems, vehicle lamps, steering equipment, seat belts, emissions and fuel consumption, sound emissions of tires, etc. For each vehicle type which they aim to place on a country governed by the 1958 agreement, vehicle manufacturers (OEMs) need to demonstrate compliance with all the applicable regulations. This is typically done in the form of a type approval audit conducted by a National Vehicle Approval Authority in one of the 1958 Agreement countries, which in turn 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 Cybersecurity & Software Updates Regulations

As mentioned in section 1 of this paper, there are currently 135 different UNECE regulations that OEMs need to fulfill, however all of these 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 recent years, 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 changed a bit 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 would be even hard to consider buying a vehicle that does not include, at a minimum, communication interfaces such as USB or Bluetooth, support for road navigation or hands-free connection to the mobile phone. Given this aspect, modern vehicles have become endpoints in our definition of IoT. Moreover, they have become not only connected to the users’ mobile devices, but 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 of development in relevant cyber attacks which could target such vehicles.

As the focus of the OEMs has been mostly placed 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 raised considerably the awareness of the OEMs, users, but also UNECE on the need to ensure proper regulatory requirements for cybersecurity and software updates topics. This need resulted in an effort for driving two new regulations, focused on the above mentioned topics. The drafting effort took into account the feedback and opinion of multiple OEM companies, national Approval Authorities, or specialized testing facilities. Secura has been actively involved in this process over the past years. After a few rounds of intermediate documents and validation pilot projects, the two new regulations have been officially adopted by the end of June 2020 [2], entering into force from the beginning of 2021. Under these new regulations, vehicle manufacturers will need to ensure that sufficient controls aimed to ensure the protection of cybersecurity [3] and software updates [4] aspects are embedded into the vehicles, before further making them available on the public roads. Therefore, it can be said that the race towards cybersecurity and software updates compliance has now started, and the winners of this race will be finally the whole automotive ecosystem.
3. UNECE Cybersecurity Regulation in Focus

The intention of this paper is not to dive fully into the details of the UNECE cybersecurity and software updates regulations, as these documents, including dedicated Interpretation Guides, will be made available by UNECE to the public. However, a summary of the most important requirements under these regulations will be given. The Cybersecurity regulation is split into two main parts – **Cybersecurity Management System (CSMS) Requirements and Vehicle Type requirements.** The CSMS requirement focus on the processes to be drafted and followed by the OEM during the whole life cycle of the vehicle. That being said, this covers all phases, including concept, development, production, post production monitoring, and finally decommissioning.

The list of processes required under the regulation include the main ones which could be expected from a security point of view. **This list includes processes such as:** definition of roles and responsibilities, security risk management and determination of necessary controls, configuration management, vulnerability analysis and incident response, post production patch management, or supply chain interaction. All of these processes will need to be properly documented and made available to the Approval Authority during the conducted audit. Evidence of the applicability and awareness of relevant persons to the requirements of the process will also be audited and validated. From the point of view of the vehicle type requirements, the main focus will be the validation that the documented processes have been properly applied on each type for which an approval is sought.

Among these examples 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 in place documented processes covering these topics, and be able to demonstrate during an audit that these processes are indeed applied in practice, by, for example, showing evidence of conducted risk assessments and definition of security controls. At the same time, it needs to be taken into account that these processes, as far as applicable, have to address the whole life cycle of the vehicle. 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 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 usually only integrating together components which are supplied from third parties. These components include both hardware and software, and could refer for example to ICs, ECUs, infotainment systems, specific software, etc. On top of this, modern connected vehicles also rely on cloud service providers for aspects such as 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. All the above steps require extensive periods of time, which typically result in development lifecycles which extend over 3-4 years in 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, under the new regulations also the cybersecurity of components needs to be taken into account while interacting with the supply chain. OEMs need to determine specific security requirements which need to be communicated with their providers, and afterwards need to be able to validate if the received components indeed meet these specified requirements. Finally, as the regulation asks for processes under the whole life cycle, the ability to work together with the supply chain providers in order to detect and treat new threats and vulnerabilities is also an essential one. Multiplying this by the range of hundreds independent components for which supply interaction is needed, results in a big need for efficient supply chain cybersecurity management.
4. UNECE Software Updates Regulation in Focus

The UNECE regulation of software updates will function in a similar fashion with the one focused on cybersecurity aspects. The software updates regulation will combine Software Updates Management System (SUMS) requirements, with vehicle type specific requirements. Under the SUMS part, the processes related to the development, configuration management and dispatch of software updates will need to be recorded. These processes include, at a high level:

- **Configuration management** for the various software updates
- **Linking the software update** to specific components on the vehicle, as well as to vehicle types
- **Analyzing and concluding** the impact of a new software update in terms of functionality, impacted components and impacted vehicle type evidence
- **Testing and validating** a new software update
- **Security of the software updates** delivery process (protection for the confidentiality and integrity of the update)
- **Safety concerns** during the download and execution of the update
- **Process for informing the users** about relevant aspects of the update

4.1 Considerations Concerning the RXSWIN

The Together with the software updates regulation, UNECE has proposed to the industry the adoption of the RXSWIN (Regulation “X” Software Identification Number). The RXSWIN aims to be a single version number, based on which all the software coming under a specific regulation can be clustered. For example, all the software versions residing on components in the scope of the cybersecurity regulations will be linked to a single RXSWIN number associated with the cybersecurity regulation. The usage of RXSWIN is envisioned to make easier the process of linking software versions to approved vehicle types and multiple regulations. Such a direct link is necessary in order to allow, for example, an Approval Authority or Road Authority to directly access the list of software installed on a particular vehicle and map this list against the software declared by the OEM for meeting the requirements of a specific regulation. That being said, the intention is to update the RXSWIN number only when a new software update has an impact on the compliance state with a particular regulation. Updates which don’t impact the compliance state will simply be added under the same RXSWIN.

The software updates regulation does not mandate though the usage of the RXSWIN. OEMs are allowed to use and demonstrate the compliance of their own processes for linking software versions of type approved vehicles to specific regulations. As long as such a mapping can be created and made available directly to the appropriate authorities, the requirements of the regulation can be met.
5. Rules for Adoption and Timelines

The two new UNECE regulations will come into force in January 2021. That being said, different countries under the 1958 agreement are expected to make them mandatory at slightly different dates. This decision lies with every individual country under the 1958 agreement. Currently, the EU has decided to make the new regulations mandatory for new vehicle types starting from July 2022. Japan has decided that the regulations will be mandatory directly from 2021. Finally, South Korea has decided that the requirements of the regulations will become mandatory in phases, starting from 2021. These three countries/areas have together accounted for 32 million vehicles produced in 2018 [2], being among the world leaders in this aspect.

Another important remark has been introduced by UNECE with respect to compliance state of vehicle types to the requirements of the cybersecurity regulation. It is acknowledged that full compliance will be a long process which will not be achieved directly by some of the OEMs. Due to this reason, the cybersecurity regulation introduces a buffer space with respect to the deadline. The regulation mentions that up to 1 July 2024, OEMs could choose to demonstrate compliance for their vehicle types not fully based on the requirements of the regulation concerning the CSMS, but by demonstrating that “cybersecurity was adequately considered during the development phase of the vehicle type concerned”. This buffer is aimed to allow OEMs to finalize their CSMS processes up to 2024, while not impacting their type approval process. However, after 1 July 2024, this buffer will not be further applicable.
The new UNECE regulations on cybersecurity and software updates will address areas which were previously not in scope of road vehicles international regulations. With the increase in vehicle connectivity, and the rise of associated vulnerabilities and threats, the new regulations are expected to have a positive impact on the whole ecosystem. Still, the requirements of the new regulations will ask the OEMs to have well-structured and documented processes related to cybersecurity and software updates 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 regulations are expected to come into force in 2021 and already be required for new vehicle types in the EU from July 2022. Considering this, the time is already short for OEMs to finalize their compliance state and be ready for type approval. Attention should be already given to potential gaps in the used processes, as these will take specific actions, and especially time to solve. OEMs have still however time to determine their current posture against the requirements of the regulations (for example through conducting preliminary gap analysis), and then switch their focus towards addressing the determined gaps.

It is expected that the first period after the moment when the regulations become mandatory for new types will be slightly challenging, however the long term effect will be a positive one. With the wide global recognition and adoption of the UNECE regulations, it is moreover expected that other non-UNECE countries will take the example and further implement own solutions to address these modern-day threats.
Secura Supports OEMs During the Whole Journey to Compliance

Secura is currently one of the Technical Services with experience in working together with the Dutch Road Authority RDW in demonstrating compliance against the two new UNECE regulation. This experience is gathered by being involved early in the development of the regulations, providing feedback and input in the development of the dedicated Interpretation Guides and performing multiple pre-audits on international OEMs.

OEMs have currently time to implement the last changes before the regulations go live, in order to ensure compliance. Therefore, it is essential to identify at this point in time any potential gaps in the documented processes of developed vehicle times. Secura can support OEMs with tailored pre-audits, specifically designed to highlight such potential gaps. The pre-audits are executed based on a mature auditing process.

The main phase of the service represents the gap analysis audit. This audit is aimed to fully simulate a future official UNECE audit, with the purpose of identifying potential gaps. These gaps are clearly documented in the resulting audit report, offering the OEM the possibility to efficiently address them in time. The possibility for further support in addressing the identified gaps is also available.

Once type approval audits for cybersecurity and software updates will become mandatory in the countries under UNECE, Secura will be among the very few companies able to conduct official audits. The official audit will follow the same regulation requirements which are targeted in the preparatory pre-audit, therefore this can ensure a smooth combined service for OEMs. Secura can therefore be the one-stop-shop in terms of UNECE regulations preparation, gap analysis and official type approval audits. Feel free to get in contact with us to explore possible ways of providing tailored support.

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: LinkedIn, Twitter, Facebook

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

3. Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cybersecurity and cyber security management system, 23 June 2020
4. Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software updates and software updates management system, 31 March 2020.