UNECE reveals how new regulations will improve security

Elle Farrell-Kingsley dives deep into how UNECE's R.155 and other regulations will improve automotive cyber security for connected cars

According to Upstream Security Global's Automotive Cybersecurity report, connected vehicles are expected to account for a quarter of all passenger cars worldwide by 2023. By 2025, this figure could reach 86% of the global automotive market. While connected components and systems are essential to enhancing the future of mobility, advancing autonomous vehicles (AVs) and providing better user experiences will introduce additional vulnerabilities and entry points for potential hackers.

The ever-growing cyber threat continues to develop. According to the AV-TEST Institute, the number of malicious programmes has increased dramatically over the last decade, from roughly 65 million in 2011 to approximately 1.1 billion in the last quarter of 2020.

The connected vehicle opens up new avenues for malicious attacks

As the automotive industry becomes more connected with more data and software, the profitability, likelihood, and subsequent danger of automotive cyber attacks will increase.

WP.29

In response to these predicted threats, the World Forum for Harmonization of Vehicle Regulations (WP.29), hosted by UNECE, has been developing new automotive regulations. WP.29 is the intergovernmental platform responsible for the regulatory frameworks regarding the safety and environmental performance of vehicle subsystems and parts.

Any country that is part of the United Nations (UN) or regional economic integration organisations set up by a member may participate and contribute to WP.29. Governmental and non-governmental organisations (NGOs) may also serve in a consultative capacity in WP.29 or its subsidiary working groups.

A key strength of cooperation under WP.29, as stated by UNECE, is the ability to unlock the benefits of innovation at scale, enabling the safe and widespread introduction of new technologies. As part of WP.29's international regulatory work on vehicle automation, a significant focus has been on establishing minimum requirements for cyber security and managing risks as hackers seek to access electronic systems and data, threatening vehicle safety and consumer privacy.

Consequently, this led to the development and adoption of UN Regulations on Cybersecurity and Software Updates in June 2020, which applies to passenger cars, vans, trucks, and buses. Specifically, these regulations were developed and adopted as "UN Regulations" under the 1958 Agreement, which is based on the mutual recognition of certified vehicles, subsystems and parts among countries that are party to the agreement.

Regulation 155

The UN Regulation No. 155 has been in place since January 2021, aiming to increase the pressure on the automotive industry to address cyber security. The regulation states: "It is the OEM's responsibility to identify and manage risks related to its Tier 1/Tier 2 or other suppliers."

R.155 was developed and adopted by governments working together as part of WP.29–with input from stakeholders involved in automotive regulations and cyber security, including manufacturers and IT experts. "This was in response to the growing recognition of cyber security risks as vehicles become increasingly connected with major cyber cases," says Francois Guichard, Secretary to the Working Party on Automated/Autonomous and Connected Vehicles under the World Forum for Harmonization of Vehicle Regulations. He is the official leading the UN's work in this area.

Automotive cyber security breaches have been making headlines for years. One of the more recent incidents, in January 2022, saw a 19-year-old hack into a number of Tesla cars around the world. Although he reported these issues to Tesla and offered solutions, the hacker David Colombo claimed he could access more than 25 Teslas. This vulnerability allowed him to remotely access multiple Tesla features, including unlocking doors and windows and starting keyless driving across at least 13 countries, making the risks of connected cars very apparent.

> "We hope that the good start will continue and that more UN Member States will apply this regulation and benefit from its provisions

Policymaking

To create new policies, WP.29 meets three times a year, and its expert sub-groups meet between these sessions to discuss and develop proposals. This approach means regulations are often amended to follow technical progress and developments in countries.

"This is the fruit of over 70 years of cooperation between countries," Guichard tells *Automotive World*. In addition to improving safety and reducing vehicle environmental

impact, Guichard also forecasts that the harmonised approach will achieve a large economy of scale for the automotive sector, notably through the system of mutual recognition reached by the 1958 Agreement. Incidentally, this was also the starting point for these regulations.

"UN regulations also play an important role in fostering innovation and help to bring the benefits of developments in automotive technologies to the widest possible audience," he says. This can be seen in the area of vehicle automation, where WP.29 recently amended a regulation to extend automated driving to up to 130 km/h in certain conditions as part of the "step by step" approach guided by UNECE's framework, which places safety at the core of developments in this area for the future of mobility.

Harmonising regulations

UN regulation No. 155 came into force in January 2021, and from July 2022 the requirements within the UNECE member countries apply to all new vehicles for type approval; from July 2024 they will apply to all vehicles. The UNECE explains that "OEMs in most major markets are already implementing these regulations."

To achieve a best practice, the regulations are best applied in harmony, says Guichard: "UN Regulation No. 156 on Software Update Management Systems and Software Updates is an example of how our harmonised regulatory approach facilitates innovation for the benefit of governments and consumers." Together with Regulation No.155 on Cybersecurity, the UNECE envisions these regulations will establish precise performance and audit requirements for vehicle manufacturers. These are the first ever internationally harmonised and binding norms in this area.

With many industry concerns surrounding the security of the increasingly connected car, could these standardised regulations extend globally?

Euro-centric?

From July 2022, system type approval for cyber security will be mandatory in all new vehicles in the EU. But will other countries follow suit? "The UK, the EU, Japan, Korea and other countries were all involved in developing and adopting UN regulation No. 155," says Guichard. "China is looking into transposing the regulation into its national standards, and some major US manufacturers are also applying it or plan to do so."

"We hope that the good start will continue and that more UN Member States will apply this regulation and benefit from its provisions," he concludes. There are currently 54 countries that are signatories to this regulation.

UN R.155 has contributed to some crucial changes in the cyber world. According to a McKinsey study, the need to strengthen automotive cyber security will trigger investments–from US$4.9bn in 2020 to US$9.7bn in 2030, with a CAGR of over 7% per year. The framework offered by the UN Regulations, and the efforts needed to meet the stringent requirements of UN R.155, are spurring significant innovation and new economic opportunities among suppliers, IT, software, and services companies.