Understanding the WP.29 Regulatory Framework

Regulating technology advancement is a necessary process. As consumer habits change, hyperconnectivity is continuing to transform the automotive industry at a faster rate than ever before.

This creates many opportunities for vehicle manufacturers, and we are seeing a lot of new technology arise as a result.

The United Nations Economic Commission for Europe (UNECE) instituted a new regulatory framework to add more protection for consumers amidst this change. The World Forum of Harmonization of Vehicle Regulations, dubbed WP.29 for short, works on regulations covering di erent parts of the vehicle. In a recent episode of the HARMAN Experiences Per Mile podcast, I explain the new WP.29 regulation for software updates and vehicle cybersecurity and how HARMAN is helping vehicle manufacturers be compliant. This blog post highlights parts of the discussion, but you can listen to the entire podcast here.

WP.29 was created after the regulators in many countries started to acknowledge the possible risks that could be encountered as a result of having connected vehicles and particularly for those that receive software updates over the air. Although the automotive industry made changes to address cybersecurity and software updates, the adoption by various vehicle manufacturers and Tier-1 suppliers still varies, making it clear that we need to make these e orts consistent across the industry. In the last three years, WP.29 has introduced detailed guidelines for cybersecurity, data protection and software updates. Overall, the regulatory framework allows the market to introduce innovative vehicle technologies while continuously improving global vehicle safety.

While UNECE is a European agency, the regulation and harmonization e orts are worldwide. WP.29 will be applied in more than 50 countries and will a ect major automotive manufacturing hubs and markets such as the US, Germany, Japan, France and the UK.

Not only will all vehicles on the road need to comply with these regulations, so will the management system which manufacturers and their suppliers are using to

develop and maintain the vehicles. In short, compliance needs to be achieved on an organizational level—not only on a project level. The penalty for not participating is severe. If automotive manufacturers are not compliant with the regulation, they will not be able to sell vehicles.

WP.29 Regulation

The new WP.29 regulation will have a significant impact on vehicle manufacturers operating in WP.29 member countries. This regulation mandates an organizational change within OEMs to have full visibility into security risk management, including the formation of a security-minded structure with proper processes, specific roles and expertise, managerial oversight, and more.

Discover More

Marcin Biedron

OTA Product Manager at HARMAN International

Connect with the Author: LinkedIn

Vehicle manufacturers should first gain a deep understanding of the gaps between the current and the new regulatory requirements in terms of risk identification and management processes. Once the gaps are identified, a plan should be put in place to address them with maximum reuse of existing processes to create a compliant and workable process.

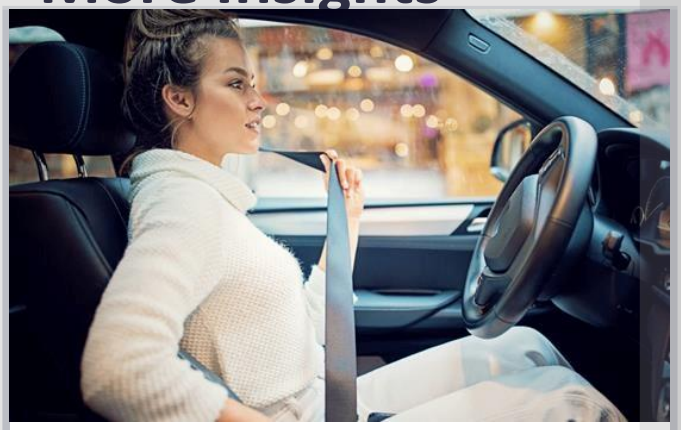
Currently, EU states, Japan and South Korea have already decided to apply the regulations to most road vehicles. The regulations will be mandatory for new vehicles from mid-2022 and mandatory for first registration of the vehicles from mid-2024 in these markets. Of course, in some countries, the timeline varies as di erent e ective dates can vary by geography.

The road to compliance can be complex. Thankfully, HARMAN has a suite of consulting packages aligned with WP.29 regulations for both software updates and automotive cybersecurity to help vehicle manufacturers understand their status and determine what is needed in order to be compliant. HARMAN has nearly a decade of automotive expertise in cybersecurity and software updating as well as a dedicated team that leads regulatory compliance. At HARMAN, we are committed to developing experiences that enhance the physical safety and digital security of

vehicle occupants, while meeting the changing needs of consumers for connected experiences.

To hear more from me on this topic, [listen to this episode of the Experiences Per Mile podcast](#).

More Insights



Why is it critical to secure the connected car?

Hackers finding are finding new ways to break into connected systems, extract sensitive information and even take control of Electronic Control Units (ECUs).

READ MORE

Virtualization for Safety and Security within a Digital Cockpit

The modern cockpit contains many driver assist functions. Virtualization reduces cost by running these functions on a single hardware platform without compromising the system safety

READ MORE