9 May, 2024 · 3 mins read

Compliance with UN R156: Securing Vehicle Software Updates

In the past, vehicles were purchased with a fixed set of functionalities that remained unchanged until the owner acquired a new vehicle. However, modern cars have evolved into customizable platforms with software that can be continuously updated and enhanced.

To meet the growing demand for personalization and remain competitive, manufacturers now offer advanced features that can be subscribed to and downloaded onto vehicles at any time after purchase. These functionalities, such as entertainment applications, driver assistance systems, self-driving capabilities, and others, are constantly being improved and updated.

Maintaining this kind of flexible software structure requires vehicle manufacturers to implement periodic update procedures. However, since these updates essentially alter the vehicle's software and carry a fair amount of potential risks, it is crucial that they are implemented in the most secure way possible. This is where the UNECE Regulation 156 (UN R156) comes into play, establishing a much-needed framework for secure vehicle software updates.

UN R156 Requirements

UNECE Regulation 156 establishes the minimum cybersecurity and Software Update Management System (SUMS) requirements for vehicle manufacturers. According to the regulation, manufacturers must implement the SUMS and demonstrate that they have the necessary processes in place to comply with all secure software update requirements. The requirements can be divided into two main categories:

1. **Software Update Management System Requirements:** These include securing communication channels for updates, validating software integrity, implementing access control mechanisms, and maintaining update logs for auditing purposes.

2. **Vehicle Type Requirements:** Specific rules and standards that vehicles must meet to ensure secure software updates.

As vehicles become increasingly software-defined, the ability to update their software securely and efficiently is paramount as unsecured software updates can leave vehicles vulnerable to cyber threats, such as malware infections, data breaches, or even remote control of vehicle systems. These risks can compromise vehicle safety, privacy, and security, making it essential to implement robust cybersecurity measures for software updates.

Securing Updates for UN R156 compliance

UNECE Regulation 156 requires manufacturers to implement appropriate cybersecurity measures to mitigate potential risks from software updates. These measures include:

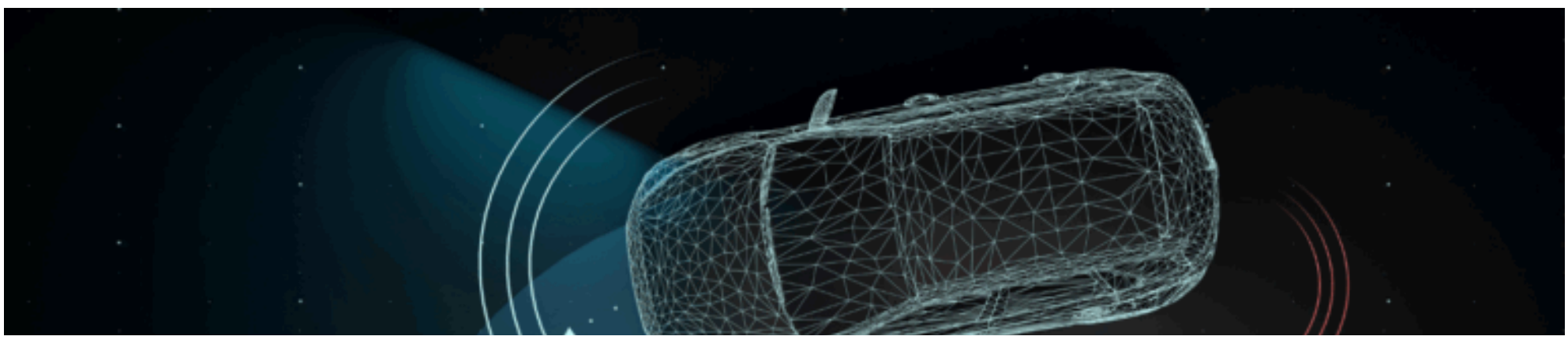
- Implementing a software update management system

- Securing communication channels for update processes
- Validating software integrity to prevent tampering
- Implementing access control mechanisms to protect against unauthorized access
- Maintaining update logs for auditing purposes

AUTOCRYPT offers a suite of in-vehicle cybersecurity products and solutions that implement the necessary security processes in line with UN R156 requirements for secure software updates. Apart from cybersecurity implementation, we also offer UN R155/156 compliance consulting services. Visit our UNECE WP.29 Consulting page to learn more and download the WP.29 regulation checklist outlining the steps for UNECE regulation compliance.

As the automotive industry continues to embrace software-defined vehicles, UN R156 plays a crucial role in ensuring the safe and secure updating of vehicle software. By establishing baseline requirements for cybersecurity and software update management systems, this regulation helps protect vehicles, their occupants, and the broader transportation ecosystem from potential cyber threats. Compliance with UNECE Regulation 156 is a critical step towards building a safer and more secure future for the automotive industry.

Related Articles



The State of Autonomous Driving in 2025

10 July, 2025

Relationship between UN R155, UN R156 and ISO/SAE 21434, ISO 24089

27 June, 2025