MAY 07, 2024:

As the demand for software defined vehicles (SDV) continues to increase there is a greater need to safeguard them with the adequate cybersecurity controls to strike the right balance between software advancements and embedding security into the SDV ecosystem.

To secure the software systems of these vehicles, the European Union (EU) announced a new United Nations Economic Commission for Europe (UNECE) WP.29 cybersecurity regulation. The aim of the regulation is to holistically secure the vehicles from emerging cybersecurity attacks throughout their lifecycle, starting from development, going through production, while it's on the road, and during its post-production service time.

- Vehicle cybersecurity risk management
- Vehicle security - by - design principles
- Vehicle cybersecurity incident management
- Secure updates and patch management

What are R155 and R156 regulations under WP.29?

- **R155** is focused on establishing a Cybersecurity Management System (CSMS) to protect, detect and respond to cyber-attacks.
- **R156** is focused on establishing a Software Update Management System (SUMS) to ensure that all software updates to vehicles are securely managed.

A well established CSMS ensures that cybersecurity risks pertaining to vehicles are adequately managed. It also ensures that adequate mitigation measures implemented to secure the vehicle from emerging threats and vulnerabilities.

Like IT, vehicle software also requires updates on a periodic basis to ensure that new features and critical security updates are installed in a timely manner. SUMS manages these updates and ensures that cyber security threats to the vehicles are addressed.

Implementing and complying with R155 and R156 regulations

The regulations enacted by the UN are a legal binding and a vehicle OEM requires explicit type approval to sell into a market under any region. Once the certification is attained by an OEM for a region, they can sell the vehicles to all countries under its jurisdiction. OEM can gain the certification from an independent third-party auditor.

Due to its legal implications, if the OEMs don't obtain the certification, then it may result in prevention of sale of non-compliant vehicles in the region.

The cybersecurity requirements under the text heavy R155 and R156 regulations are quite exhaustive and overwhelming to the automotive community to decipher. The below concise summary would help them gauge the critical requirements and make informed decisions about security compliance.

Requirements for CSMS:

- A well-defined CSMS process should be documented.
- Ensure that the process apply to the development, production, and post-production of vehicles.
- Define a process to manage vehicle cybersecurity risks.
- Verify that the risks identified are adequately managed.
- Adequate cybersecurity testing of a vehicle type.
- Ensure that the risk assessment is kept current.
- Ensure processes mitigate cyber threats and vulnerabilities which require a response within a reasonable timeframe.
- Ensure processes continually monitor for, detect, and respond to cyber-attacks, cyber threats, and vulnerabilities on vehicle types.
- Identify and manage supplier-related risks.

Requirements for SUMS:

- Ensure there is a well-defined SUMS process is in place.
- A repository of all initial and updated software versions should be maintained.
- Assess, identify, and record if a software update will adversely affect any other systems required for the safe and continued operation of the vehicle.
- Maintain adequate documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance.
- Adequate processes should be defined to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated.
- Update processes should be securely protected to reasonably prevent them from being compromised, including development of the update

delivery system.

Navigating the WP.29 Regulation for a Secured Future of Mobility

There are several automotive cybersecurity standards and regulations e.g., ISO 21434, WP.29, ISO 24089, and SAE J3061, and more. There are various cybersecurity controls that are common in these standards and regulations. If a common cybersecurity control is implemented for a particular standard, it means that the same artifact can be used to demonstrate compliance with another automotive regulatory requirement. This ensures that the OEMs are not over-burdened with multiple cybersecurity compliance requirements.

About the Author

Akhilesh Soni
Principal Consultant, Tech Mahindra

Akhilesh is a cybersecurity architect with 16+ years of diversified experience in the field of cloud security, data security, application security, security operations, identity and access management, OT/IoT security, endpoint security, governance, risk management, and compliance.

MORE