

ISO/SAE 21434 Automotive Cybersecurity Lifecycle Management

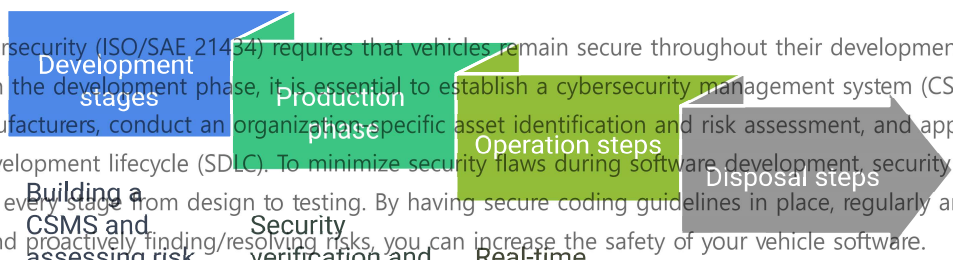
ISO/SAE 21434

Automotive Cybersecurity Lifecycle Management

Hello Engineers! This is Hermes Solution. Today, we'll take a look at the lifecycle management of automotive cybersecurity (ISO/SAE 21434) and what security activities are required at each stage.

With the rapid development of autonomous driving technology, automotive cybersecurity is no longer an option, but a requirement. Cars have evolved to utilize a variety of electronic control units (ECUs) and communication technologies, and in the future, over-the-air software updates (OTA) and real-time data collection are expected to become more prevalent. As a result, it is essential to have a security posture that is in line with international standards and regulations such as UN Regulation 155 (UNECE R155), UN Regulation 156 (UNECE R156), ISO/SAE 21434 and ISO 24089.

Automotive Cybersecurity Lifecycle
: From Development to Decommissioning



Automotive cybersecurity (ISO/SAE 21434) requires that vehicles remain secure throughout their development, production, and operation. In the development phase, it is essential to establish a cybersecurity management system (CSMS) for automotive manufacturers, conduct an organization-specific asset identification and risk assessment, and apply secure coding and a secure development lifecycle (SDLC). To minimize security flaws during software development, security checks should be performed at every stage from design to testing. By having secure coding guidelines in place, regularly analyzing code vulnerabilities, and proactively finding/resolving risks, you can increase the safety of your vehicle software.

Security verification procedures are important during the production phase. To prevent various security threats that may occur on the vehicle assembly line (e.g., attacks on the manufacturing process, hacking of test equipment, etc.), the vulnerabilities of the product should be checked by various methods: penetration testing, fuzzing testing, etc. In addition, vehicle security should be tested in an environment that corresponds to actual driving conditions by combining real vehicle-based and simulated security testing.

In the operational phase, a real-time security monitoring and response system should be in place to detect and respond to threats in real time. Security management of internal and external vehicle communications and over-the-air (OTA) updates is also essential, and intrusion detection and threat monitoring systems should be applied. In addition, a software update and maintenance system should be established during the operation phase to ensure continuous vehicle safety.

Finally, the disposal phase requires procedures to securely erase user and vehicle data. It is important to maintain the security of the vehicle by eliminating security vulnerabilities and thoroughly validating the security of reusable electronics.

A reliable way to assess automotive security

The question "How do we assess this security, and how do we prove it is reliable?" is critical. UNECE R155 and ISO/SAE 21434 require automotive manufacturers to establish their own security assessment and certification scheme, with key assessment areas including

- CSMS operation and validation: verifying the level of organization-wide cybersecurity management
- Security Vulnerability Analysis: Analysis of vehicle networks/ECUs/communication modules
- Communication-OTA update security assessment: Verification of safety, integrity of OTA system
- Data protection and privacy management: Encryption/access control of data generated in autonomous driving

Automotive cybersecurity ratings are gradually being introduced in the US and Europe. This is an objective way of indicating the security level of a vehicle, which helps build consumer trust and increase manufacturer accountability.

Securely applying over-the-air software updates (OTA)

In autonomous vehicles, software must be constantly updated, and one of the biggest risks is OTA security.

1. Prevent security vulnerabilities

- Encrypt (SSL/TLS) the communication between the OTA server and the vehicle, and use signature verification to prove the authenticity of the update file.
- Perform security scans or integrity verification before and after updates to prevent malware injection.

2. Compliance with international standards

- Standardize software update procedures based on international standards for OTA security, such as ISO 24089.
- Adopt industry-recognized authentication/encryption technologies to increase the reliability of updates.

3. Safety-convenience balance

- When performing updates, vehicle owners should consider not only convenience, but also safety (such as limiting updates while driving).



Autonomous vehicles generate and collect a large amount of data while driving. This data includes location, video, personal information, and more, and requires strict legal and ethical protection.

- Protecting personal data and managing privacy
 - It is necessary to clearly define the purpose and scope of the information collected from the vehicle and who uses it (manufacturer, service provider, etc.).
 - Minimize the exposure of personal information by applying encryption/access restriction measures in accordance with privacy laws and, if necessary, anonymization procedures.
- Encrypt and securely store data
 - Encrypt data in transit between the vehicle and cloud servers to prevent it from being intercepted or forged or altered in the middle.
 - Especially for autonomous cooperative driving (vehicle-to-object communication, vehicle-to-server communication, etc.), it is essential to apply secure protocols (TLS, IPsec, etc.).

Securing the automotive future, now is the time to prepare

Automotive cybersecurity (ISO/SAE 21434) is becoming increasingly important with the development of autonomous driving technologies. Security and data protection is no longer an option, but a necessity, and requires active cooperation between automakers and governments. A cybersecurity assessment system based on international standards and software update management techniques that are legislated will create a safer autonomous driving environment.

In this article, we've looked at automotive cybersecurity (ISO/SAE 21434) lifecycle management. As the era of autonomous driving approaches, security and data protection are becoming essential. In response, it is important that manufacturers and governments work closely together to drive technology development and legislation.

Cybersecurity and software update safety are essential for the commercialization of Level 4 and higher autonomous driving. Cybersecurity assessment systems and software update management technologies that are aligned with international standards (UNECE R155, R156) will help create a safe autonomous driving environment.