A Special Feature Article
ISSUE 2 2022 JAPIA NEWS

Addressing to Automotive Cybersecurity - Requirements and Countermeasures for Parts Suppliers

Time to address automotive cybersecurity is just around the corner. The Working Party on Automated and Connected Vehicles (GRVA) of World Global Forum for Harmonization of Vehicle Regulations (WP29) of the United Nations Economic Commission for Europe's World Forum for Harmonization of Vehicle Standards has announced that the international standards for automotive cybersecurity and software updates that were approved in June 2020 came into effect in January 2021 and will be apply to new models released in Japan on or after July 1, 2022. Next-generation vehicles equipped with advanced driver assistance systems (ADAS) and automated driving technologies are expected to update and optimize software and add functions through wireless communication using OTA (over-the-air). Cybersecurity measures are essential to ensure the safety of connected cars, and automakers, as well as component manufacturers, are also required to comply with international standards.

Will apply to new vehicles released in July or later

The UN regulations on cybersecurity and software updates are the legally binding "UN-R155 CSMS" and "UN-R156 SUMS," which came into effect in January 2021. Without these certifications, cars cannot be sold in markets such as the EU and Japan. In Japan, certification will be required from July 2022 for new models with OTA updates, and from July 2024 for all models already sold.

The key point about cybersecurity is that not only automobile manufacturers but also parts suppliers, aftermarket-related companies, and service providers are required to establish a management system. This is because cybersecurity requirements are defined from vehicle development to production and post-production.

There are two main cybersecurity requirements set forth by WP29, one for "organizations" and the other for "vehicles".

The one for organizations calls for the establishment of a cybersecurity management system (CSMS). It is necessary to clarify the processes, responsibilities, and management related to vehicle cybersecurity, and to establish a system to manage cybersecurity throughout the entire life cycle of a vehicle, from planning and development to production through disposal.

In establishing this CSMS, the international standard "ISO/SAE21434" is considered to be a guideline. Following ISO/SAE21434 is the best approach to build a CSMS and will make it possible to respond to future automotive cybersecurity.

ISO/SAE 21434 is an international reference standard that summarizes the key issues in ensuring vehicle security throughout the entire life cycle of a vehicle, starting from planning and development, through design, implementation, and verification, to production, shipment, market use, and disposal. It consists of seven major elements: "overall security management," "project-specific security management," "risk assessment," "concept phase," "product development phase," "production/post-production phase," and "security activities in distributed development."

This ISO/SAE 21434 is sufficient condition for obtaining CSMS certification, although some parts of the scope of application may differ. Required by the UNR155CSMS but not covered by ISO/SAE21434 include physical damage to back-end servers which are the platform from which the car makes its network connections and data.

On the other hand, for vehicles, automakers are required to obtain type certification after developing vehicles based on the CSMS. The type certification must be obtained after risk assessment and risk mitigation measures for key components of the vehicle, product protection after shipment, and a system for monitoring and recording cyber-attacks.

UNR156SUMS is a system for safely updating the software of in-vehicle ECUs. It covers the entire vehicle life cycle, including not only the vehicle development phase but also the use phase. In order to ensure feasible and safe software updates, the requirements for organization and functionality are defined in the same way as for the CSMS.

Software updates and management are now mandatory

Organizations are required to securely maintain the documentation necessary to generate and authorize evidence of activities related to software updates, to operate a software version control identifier " RXSWIN" , and the notification of information to users.

The functional requirements stipulate that the software update function must be secure, guarantee the safety of the vehicle even if the update fails, and guarantee that the RXSWIN and software version can be read from OBD and other sources and not be tampered with.

Software updates cover the entire life cycle of a vehicle, including the manufacturing and the use phase, not just the development phase. Therefore, the documentation and evaluation methods are required to implement safe software updates at each stage must be defined, and it is necessary to demonstrate that this process is at a feasible level.

In order to identify vehicles subject to software updates, it is necessary to manage each vehicle model, including derivatives, each vehicle by identification number, and by user and maintenance status. Therefore, it is important to not only share information within the development, manufacturing, and sales departments, but also to review the process of collaboration with suppliers and dealers.

The key to vehicle management is software version management using RXSWIN. RXSWIN is an identifier to collectively manage the software of ECUs related to each regulation number of the

United Nations Regulations (UN Regulations). For example, UN12 specifies steering mechanism and UN39 specifies speedometer/odometer.

In RXSWIN, the ECUs that make up the system are numbered as a single entity. When a software update affects an approved system, it is necessary to renumber the ECUs and manage the software versions of the ECUs.

Requirements to Parts Suppliers

In complying with the UN regulations, automobile manufacturers will be asked to cooperate with parts suppliers. In particular, with regard to cybersecurity, the regulations clearly require automakers to manage parts suppliers.

Parts suppliers are essential to the development of high-quality, high-performance, cost-effective vehicles, and now that ADAS and automated driving technologies are being installed, the development of software for these advanced devices is also increasingly being handled by suppliers. In order to address vulnerabilities to cyber-attacks as early as possible, the cooperation of parts suppliers is indispensable.

The creation, continuous monitoring, and improvement of security quality cannot be implemented by the automakers alone. Therefore, it is essential to strengthen cooperation between automakers and parts suppliers, and parts suppliers will be required to take the same approaches as automakers. Parts suppliers will need to engage in many activities such as process development, setting up a system, secure development and evaluation, in-plant security, and PSIRT.

In the CSMS established by automobile manufacturers, five main requirements are summarized: "security process definition," "risk analysis / measures," "supplier management," "security inspection," and "vulnerability / incident Information and Response.

Looking at these five requirements from the supplier's perspective, "supplier management" is the very reason why automobile manufacturers require activities in compliance with UN regulations. Since the CSMS requires a process that continuously produces products with stable quality, it is highly likely that automobile manufacturers will require parts suppliers to define security processes.

Vulnerability / incident information handling will also require not only prompt countermeasures when problems are discovered, but also continuous monitoring of vulnerabilities in in-house developed software. In addition, since vehicle development based on CSMS is a condition for obtaining type certification, parts suppliers who are responsible for component development will also have an important responsibility.

The ISO/SAE 21434 guideline for CSMS requires the development of OT (Operational Technology) security to prevent unauthorized software from being installed in ECUs at manufacturing plants. Therefore, when software is installed at the supplier and delivered to the

automaker, there is a good chance that the automaker will request the status of OT security construction.

UN-R155/156 defines a general policy but does not define specific examination methods or pass/fail decisions. Therefore, in obtaining certification, automobile manufacturers themselves need to prove that they are following the policy. In vehicle development, component manufacturers are only developing systems in specific areas. Therefore, only automobile manufacturers can conduct risk analysis and security inspections of the entire vehicle.

For parts suppliers to comply with UN-R155/156, they will be required more than ever to establish a cooperative framework that extends to the early stages of vehicle development by automobile manufacturers. At the same time, the automotive parts industry, which includes many small and medium companies, faces a mountain of challenges, such as building internal organizational structures and securing the necessary human resources. How to support companies that find it difficult to take a company-wide approach is another important industry issue that needs to be resolved.