# Software Update Management System

Learn how to implement a software update management system according to UN R156 and ISO 24089.

Contact us

Software Intensive Systems Resource Library

The United Nations Economic Commission for Europe (UNECE) regulations for cybersecurity (UN R155) and software update management (UN R156) came into force in 2022, requiring automotive original equipment manufacturers (OEMs) to set up a software update management system (SUMS) with a methodical approach and clear structures to safeguard the cybersecurity of vehicles.

Software updates are an important aspect of cybersecurity. The latest cybersecurity efforts quickly become obsolete as threat actors continually advance their skills in exploiting vulnerabilities in connected vehicles. A serial vehicle may have been secure when it entered production, but that does not guarantee its security in the future. Therefore, updates play an important role in maintaining the security of connected vehicles.

Keep reading to learn:

- The aim of a SUMS
- What a SUMS includes
- Best practices for setting up a SUMS
- How to meet SUMS regulatory requirements, including UN R156 requirements

# The software update management system

The software update management system (SUMS) builds on the groundwork laid by a cybersecurity management system (CSMS), which is required by UN R155. The CSMS determines responsibilities and procedures needed to maintain vehicle cybersecurity. It requires comprehensive activities so that threats can be systematically monitored and evaluated. UN R155 also defines how the manufacturers should deal with any insights they gain.

A CSMS thus provides information about when and why software updates — an important response to potential threats — are required. If it is determined that a cyber risk should be mitigated by providing an update, the SUMS and its required processes need to be followed.

However, software updates, if not properly tested and validated, can introduce new vulnerabilities that could be exploited by threat actors or cause safety issues. Automotive OEMs must design their SUMS to address these concerns and that software updates are thoroughly tested and validated before they are released.

The SUMS requires thorough preparation and contributes to cybersecurity by design.

# What is the aim of a SUMS, and what does it include?

The SUMS helps establish that software updates are carried out safely, functionally, traceably and compliant with UN R156 and the vehicle type approval requirements.

This management system encompasses automotive security processes that help establish that:

- Software updates for target vehicles are identified and the vehicle configuration is documented
- The compatibility software updates with the overall vehicle configuration is checked so that the update’s effects on vehicle systems and parameters are understood

Software updates and their impact on type approval and the overall vehicle are identified

You meet the security, safety and documentation requirements for software updates that are completed in the shop or over the air (OTA).

The software is available and implemented safely

The software and update have integrity and authenticity

The SUMS helps establish that every vehicle can be reliably supplied with required updates; this can be challenging because there are often multiple configurations of one vehicle type.

A SUMS deals with connected vehicles as part of an overall system, with vehicles defined by their software, in addition to vehicle architecture that includes the backend servers. This is shown in the diagram below.

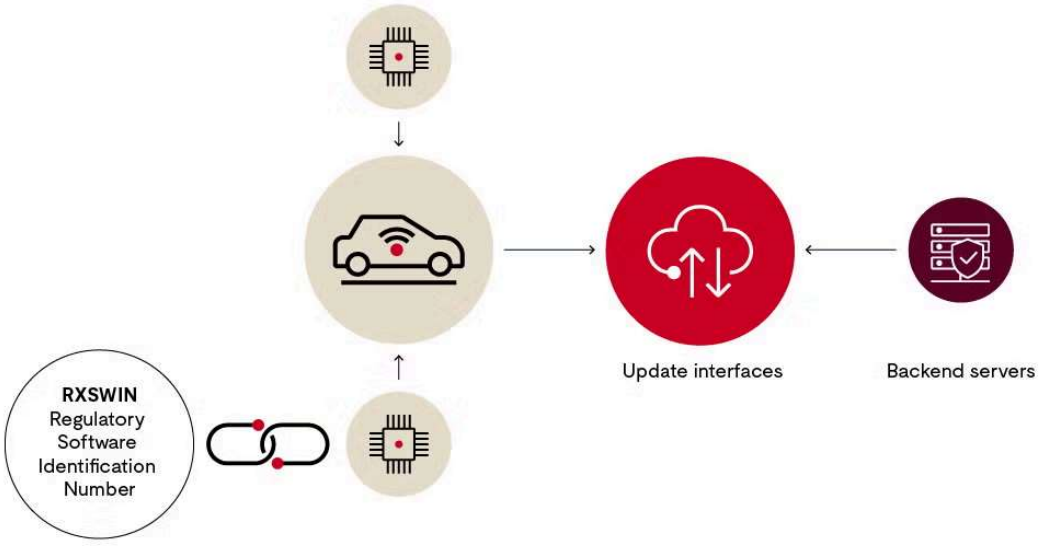



**Image** Scope of a software update management system.

At the center of the system is the software-defined vehicle. The various control units for the car body, chassis, safety aspects and gateways have interfaces, through which they are connected to backend servers.

Managing diverse configurations is important. An identifier helps establish that the vehicle's software configuration, including respective components, can be determined. The Regulatory Software Identification Number (RXSWIN) is a dedicated identifier that represents

information about the type approval relevant software and its characteristics. This identifier is required by the authorities and defined by the vehicle manufacturer. The RXSWIN should be unique for each software version in each vehicle type. It can be read out from the vehicle and enables the determination of the homologation status of individual functions and the related control units that are subject to a UNECE regulation.

Following a systematic structure and defined routine is critical in case an update fails. In case of an update failure or interruption, the previous state must be able to be restored again. Moreover, the most important goals of cybersecurity — the protection of confidentiality, integrity and update availability — must be adhered to.

# How should you set up a software update management system?

An effective SUMS provides a systematic method for carrying out reliable vehicle updates. The required processes and procedures relate to the following aspects:

- How to log multiple hardware and software versions needed for the vehicle type for different systems and functions.
- Which software is important for type approval and needs a RXSWIN.
- Defining and updating the RXWIN.
- Interdependencies, especially when it comes to software updates.
- Which components affected by updates.
- How components' compatibility is impacted by updates.
- The extent to which a software update affects type approval or other aspects defined by legislators.
- The extent to which an update affects functional safety or driving safety.
- How vehicle owners will be informed of updates.

How the update process is protected from a cybersecurity perspective.

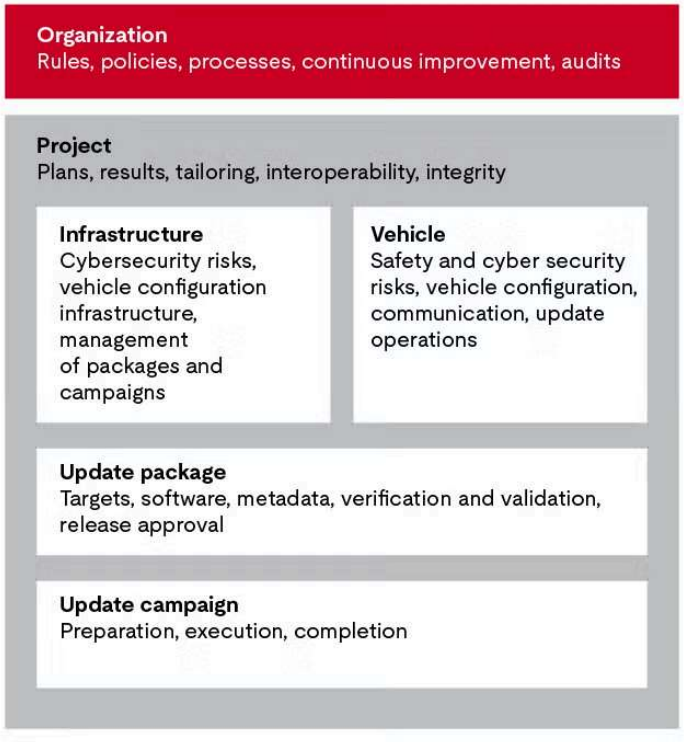
How these points shall be documented.

Aside from cybersecurity for vehicle stakeholders, the primary concern for vehicle manufacturers is legal certainty. Are appropriate measures being taken to keep the vehicle safe? How will you deal with the complexity of the connected vehicle with different configurations changing over time?

If, despite all efforts, a threat actor finds a way to get into a system, manufacturers must provide evidence that they made every reasonable effort to protect the vehicle and worked in compliance with the standards. The UNECE regulations also stipulate that manufacturers will be obligated to report attacks starting in July 2024.

Another challenge is that while UN R156 specifies required activities, it does not identify how manufacturers should implement the requirements. However, ISO 24089, Road Vehicles-Software Update Engineering, published in 2023, provides guidance on the practical implementation of the required activities.

**Software update management system overview**



This diagram shows that organizational processes are a prerequisite for providing timely, secure updates to the vehicle in the field. All requirements, including infrastructure, access to configuration databases and RXSWIN, must be planned, developed and provided to coincide with the timing of vehicle development. This is also part of security by design. If a decision is made that a risk must be averted by releasing an update, the software update processes already must be in place. Only then, employing a methodical approach and clear structures, can the software update campaign be carried out.

A management system should follow a “Plan–Do–Check–Act” (PDCA) process. Processes should be regularly evaluated for effectiveness and efficiency. This includes audits by independent inspection bodies.

# SUMS Regulations

*Note: The information provided on this web page does not, and is not intended to, constitute legal advice.*

UN R156 provides explicit requirements but leaves it up to manufacturers how to meet those requirements. SUMS is an important aspect of approval processes and homologation and needs to be certified. Like the CSMS, the SUMS must be audited and certified by a neutral body for the vehicle to be granted type approval.

The following diagram illustrates the process.

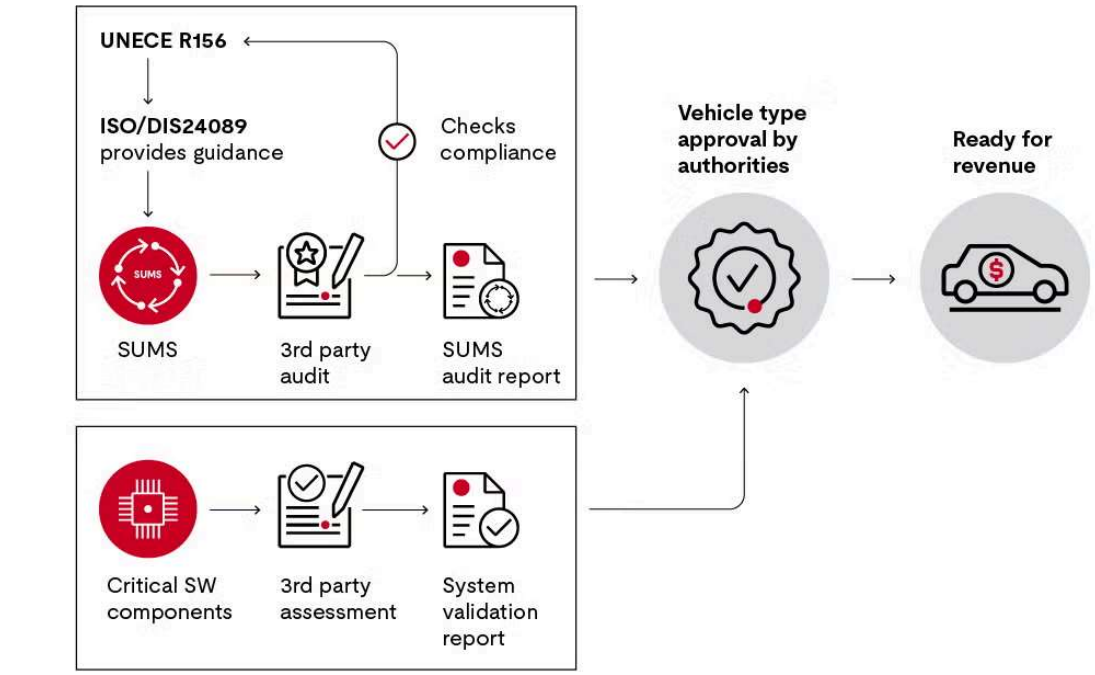



**Image** Vehicle type approval process

The diagram shows that a SUMS adhering to ISO 24089 guidance must be established.

An auditor from a UNECE listed certification body confirms whether the SUMS and related activities are carried out by the company and are suitable to meet the regulatory requirements of UN R156. If they meet requirements, the manufacturer receives a certificate, which is valid for three years.

However, to bring vehicles to market, there are additional requirements. All components identified as critical must be certified by an independent body. Manufacturers receive a certificate for each critical component in the form of a system validation report. The requirement for component certification is a key difference between the approval process for the SUMS as compared to the CSMS.

The manufacturer needs type approval from the national approvals administration before production starts. The authorities will check that all necessary certificates are in place and confirm if they have been audited by an independent body.

For type approval, the manufacturer needs:

1. A certificate for the CSMS.
2. A certificate for the SUMS.
3. A certificate for each component identified as critical.

Once all requirements have been met, the vehicle will receive its type approval and homologation. Then it is permissible to sell the vehicle.

An effective SUMS complies with UN R156 and builds on the guidance in ISO 24089. However, you must apply guidance and adapt your SUMS to your company’s specific situation and overarching process landscape.