Software Update Management Systems According to UNECE R156

The United Nations Economic Commission for Europe (UNECE) regulations for cybersecurity (UN R155) and software update management (UN R156) have been in force since the summer of 2022.

Software Intensive Systems White Papers

Introduction

Vehicle manufacturers must set up management systems to safeguard the cybersecurity of vehicle fleets based on a methodical approach and clear structures.

Under R156, the UNECE also calls for a software update management systems (SUMS). This resource guide and the video discuss what a SUMS includes and how to set one up.

Why do you need a SUMS? Software updates are a pivotal aspect of cybersecurity because today's cybersecurity has an expiration date. After all, the community of threat actors is always advancing it skills. A year from now, they may find new ways to attack your vehicle. Your serial vehicle might have been secure when it entered production, but it may not be in the future. This is where updates come into play. One important role is to help maintain the safety of connected vehicles.

Because cybersecurity is a moving target, software updates help you keep that target in sight.

How does that work in practical terms? This resource guide answers three key questions:

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

2. How should you set up a SUMS?

3. How can a SUMS comply with regulations?

Before we go into these questions, let's look at the cybersecurity management system (CSMS) called for by the UNECE under R155. This is important because a SUMS builds on groundwork laid by a CSMS.

Like any management system, a CSMS determines responsibilities and required procedures to maintain vehicle cybersecurity. A CSMS requires comprehensive activities so that the nature of threats can be systematically monitored and evaluated. It also defines how any insights you gain should be dealt with. Here is the crux. Software updates are an important response to potential threats. A CSMS thus provides information on when and for what purpose software updates are required. If, because of an analysis, it is decided that a risk should be eliminated by providing an update, the SUMS and its processes need to be followed.

Software updates can introduce new vulnerabilities that could be exploited or cause safety issues if not properly tested and validated. Vehicle manufacturers must design their SUMS to address these concerns and thoroughly test and validate software updates before they are released.

The SUMS requires thorough preparation to make an important contribution to cybersecurity by design.

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

A software update management systems (SUMS) establishes that software updates are carried out in a safe, functional, traceable and compliant manner. Compliant manner means that the vehicle's software is and stays compliant with the respective vehicle type approval. This is the objective of R156.

This management system encompasses processes relevant to automotive security that establish that:

1. Software updates for target vehicles are identified. You need to know which cars need an update. Documentation of the vehicle configuration is key.

2. There is a check of the compatibility of software updates with the overall vehicle configuration. You need to know the effects on vehicle systems and vehicle parameters.

3. Software updates and their influence on the scope of type approval and the overall vehicle are identified. An update, as it is a change, can have an influence on the valid type approval.

4. You meet the security, safety and documentation requirements for software updates that take place in the workshop or over the air (OTA).

5. The software is available and implemented safety, and the integrity and authenticity of the software and the software update are established.

The SUMS establishes every vehicle can be reliably supplied with required updates. That’s easier said than done because you have to deal with different configurations of one vehicle type.

A SUMS deals with connected vehicles as if they're part of an overall system — with vehicles defined by their software, which includes vehicle architecture and backend servers, as shown as the diagram below.

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

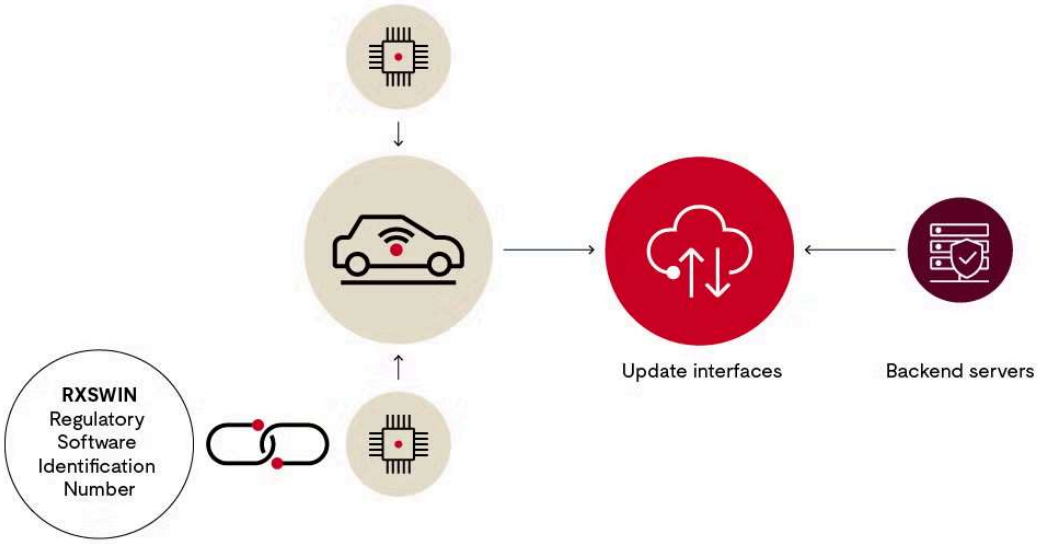


Image Scope of a software update management system.

Scope of a software update management systems (SUMS)

Configuration management is key. An identifier is needed to determine the current software-configuration status of the vehicle, including the respective components. The Regulatory Software Identification Number (RXSWIN) is a dedicated identifier, required by the authorities and defined by the vehicle manufacturer. It represents information about the type approval relevant software and its characteristics. The RXSWIN can be read out from the vehicle and allows the determination of the homologation status of individual functions and the related control units that are subject to a UNECE regulation.

For example, if a vehicle manufacturer is creating an RXSWIN for the steering system software in a vehicle that falls under UNECE Regulation No. 79. The manufacturer would use "RX79" as the first part of the RXSWIN to indicate the UNECE regulation number. The second part would be a software identification number for a specific version of the steering system software at the manufacturer.

The RXSWIN should be unique for each software version in each vehicle type, and it should be assigned by the vehicle manufacturer. The need to follow a systematic structure is also

underscored by the fact that routines must be defined, in case an update fails. If an update fails or is interrupted, you must be able to restore it to the previous state. Moreover, you must adhere to the most important protection goals of cybersecurity the confidentiality, integrity and availability of the update.

2. How should you set up a software update management system?

If a SUMS offers you a systematic method for carrying out reliable vehicle updates, then the focus lies in processes and procedures. The processes you need for this revolve around the following:

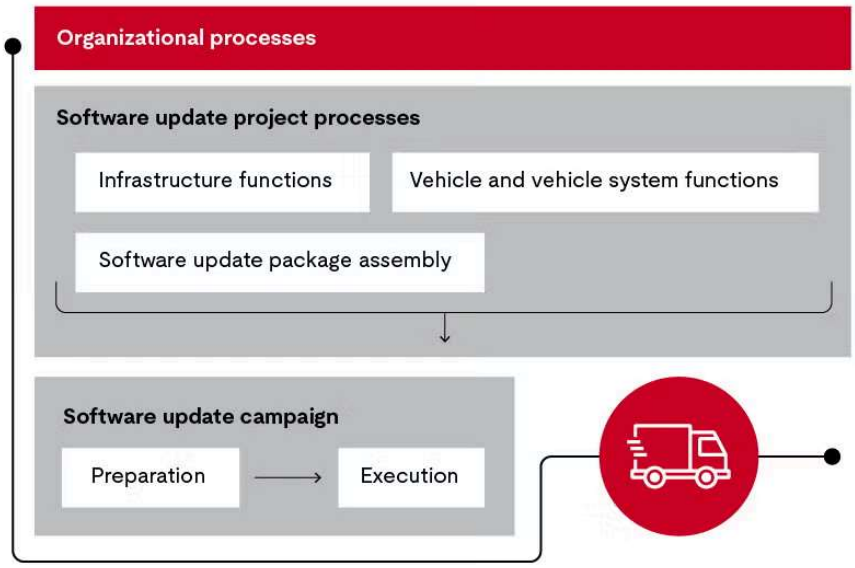
1. How should you log different versions of the hardware and software required for the vehicle type for different systems and functions?
2. Which software is important for type approval and needs a RXSWIN that must be defined and updated?
3. Are there any interdependencies, especially for software updates?
4. Which components are affected by updates, including their compatibility?
5. To what extent does a software update affect type approval or other aspects defined by legislators?
6. To what extent does an update affect functional safety or driving safety?
7. How will vehicle owners be informed of updates?
8. How will the update process itself be protected from a cybersecurity perspective?
9. How should all of these points be documented?

Aside from cybersecurity for vehicle stakeholders, the primary concern for vehicle manufacturers is legal certainty. Is everything being done 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, a threat actor finds a way to get into a system, manufacturers must provide evidence that they made every reasonable effort to protect vehicles and worked according to the standards.

The UNECE regulations also stipulate that you will be obligated to report attacks in the future.

Another challenge is that ISO 24089, Road Vehicles — Software Update Engineering, which provides more guidance for a SUMS, was only published in early 2023. UN R156 only states the required activities; how you implement those requirements in practical terms is explained in ISO 24089. To a certain extent, this regulation defines the destination while ISO 24089 gives guidance for getting there.



Structure of ISO 24089

This diagram shows that organizational processes are a prerequisite for providing quick and secure updates to the vehicle fleet in the field. All requirements, including the infrastructure, access to configuration databases and the 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 will have to be averted by releasing an update, the

software update processes must already be in place. Only then can the software update campaign be carried out on the basis of a methodical approach and clear structures.

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.

3. How can a SUMS comply with regulations?

The UNECE regulation lays down explicit requirements but leaves it up to manufacturers to determine how they meet those requirements. The SUMS is an important aspect of approval processes and homologation and needs to be certified. Like a CSMS, the SUMS must be audited and certified by a neutral body; otherwise, the vehicle will now be granted type approval.

The diagram below shows how the process works.

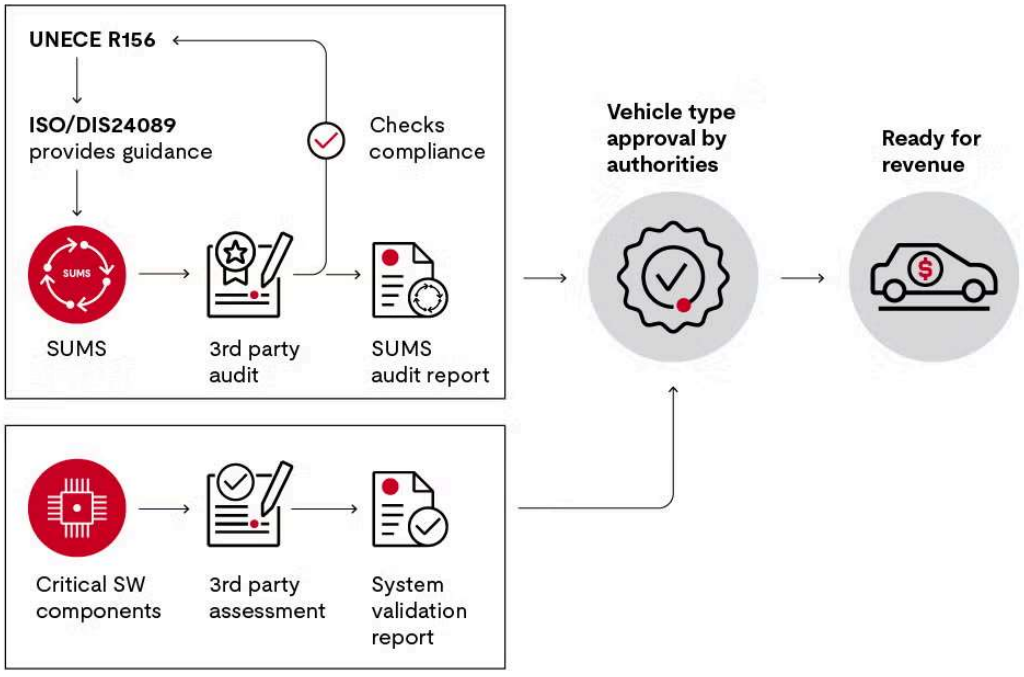


Image Vehicle type approval process

A SUMS needs to be established, for example, based on ISO 24089.

An auditor from a UNECE listed inspection body examines whether the SUMS and the activities discussed previously are carried out by your company and are suitable to meet the regulatory requirements of UN R156. If they are, you receive a certificate, which is valid for three years.

But for bringing the vehicles into the market, that is not enough. All components identified as critical must also be certified by an independent body. Manufacturers also receive a certificate for this in the form of a system validation report for each release candidate. From an approval perspective, this is where a SUMS is different from a CSMS; only the SUMS includes the additional aspect of component certification.

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

For type approval, you need:

1. A certificate for your CSMS.
2. A certificate for your SUMS.
3. Numerous certificates for relevant components.

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

Summary

This overview of the basics of a SUMS answers three key questions:

1. What is the aim of a SUMS, and what does it include?
2. How should you set up a SUMS?
3. How can a SUMS comply with regulations?

This knowledge can help you better understand UN R156 and the approach offered by ISO 24089. A good SUMS builds on the knowledge of this standard. Like any management system, however, it must be adapted to your company and the process landscape.