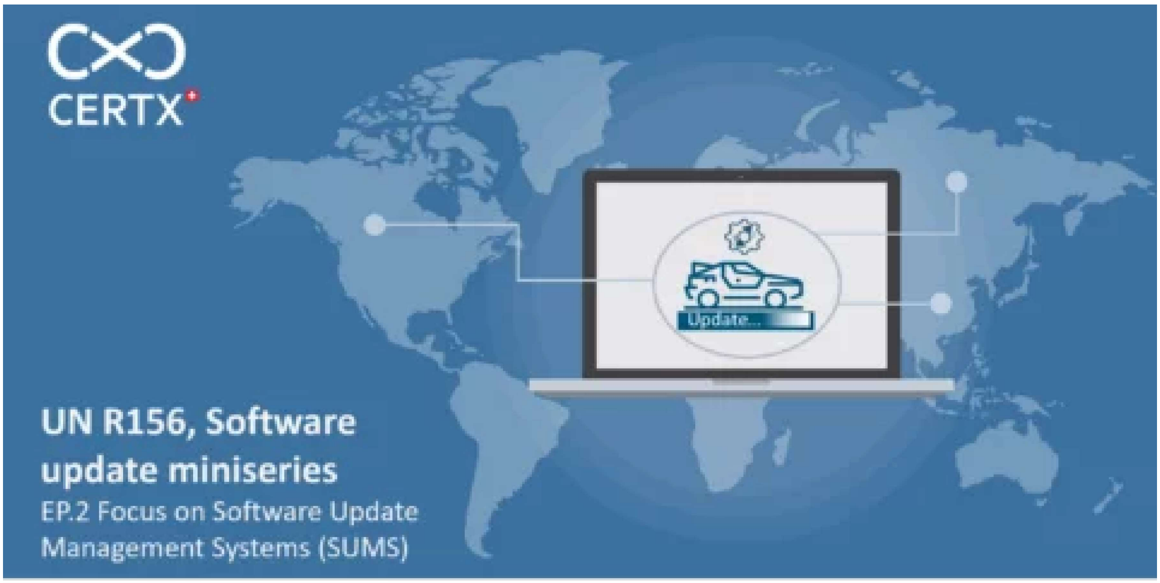
Software Update for Road Vehicles – Ep.2 – Focus on Software Update Management Systems (SUMS)

Jan 23, 2023 | Automotive, Cybersecurity

The first episode of this miniseries put an overview of the new UN ECE R156 regulation and related standard ISO 24089. This episode will focus on the management systems for the Software update required by them, so called SUMS (Software Update Management Systems). How is going to take place in every organization and its relationship with others management systems.

Miniseries history

- EP.1 Overview of UN R156 and ISO:24089
- **EP.2 Focus on Software Update Management Systems (SUMS)**
- EP.3 Focus on vehicle requirements (RXsWIN & VTA)
- … Do not hesitate to contact us for new blog post ideas.

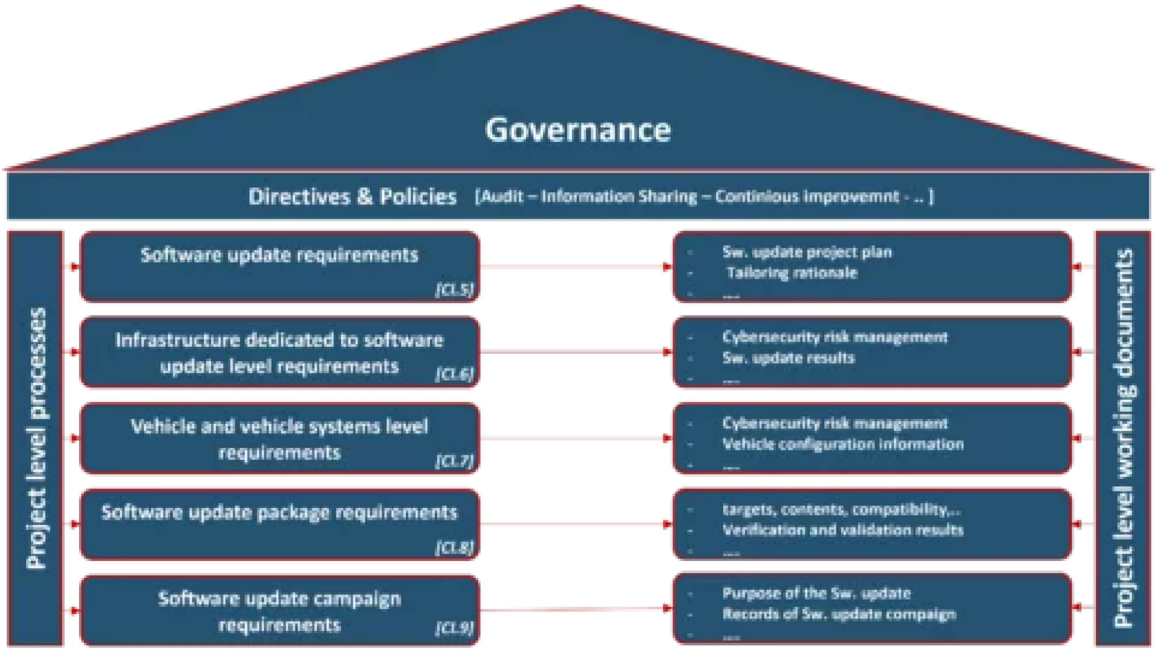

CERTX
Update...
UN R156, Software update miniseries
EP.2 Focus on Software Update Management Systems (SUMS)

Vehicles and management systems a long story

The automotive industry should already comply with requirements related to multiples management systems. From Quality management: IATF 1649, ASPICE or ISO 9001, or even security specific: ISMS (ISO 27001). Added to these well know management systems two newcomers are requested by the authorities: CSMS, Cyber Security Management Systems for Road vehicles UN R155 (aligned with ISO/SAE 21434 practices) and the SUMS. The transversality and the dependence between each management systems are explained and showed in the Blogpost “[ISO/SAE 21434] A management story”. Thus, the focus in today’s blogpost is made on the SUMS.

Adding another management systems could be considered as more processes and superfluous documents to follow. But the reality is the opposite it allows to precisely specify requirements and processes linked to Software update to improve vehicles safety, security, and reliability.

SUMS suggested structure is based on both UN R156 and ISO 24089 (currently still in FDIS release) requirements illustrated in figure below, can be compared to the CSMS structure with three typical abstraction level. The suggested approach allows to define a concise and clear document structure.


Governance
Directives & Policies [Audit – Information Sharing – Continious improvemnt - ..]
Project level processes
Software update requirements [Cl.5]
Infrastructure dedicated to software update level requirements [Cl.6]
Vehicle and vehicle systems level requirements [Cl.7]
Software update package requirements [Cl.8]
Software update campaign requirements [Cl.9]
- Sw. update project plan
- Tailoring rationale
- ....
- Cybersecurity risk management
- Sw. update results
- ....
- Cybersecurity risk management
- Vehicle configuration information
- ....
- targets, contents, compatibility,..
- Verification and validation results
- ....
- Purpose of the Sw. update
- Records of Sw. update compaign
- ....
Project level working documents

The clause identifiers [CI-X] references ISO 24089 sections for implementation guidance. Thus, they are subject to adjustments by the official release planned for mid 2023. Below the introduction to the three suggested documentation levels to be considered for SUMS establishment and operation

—

Governance level:

This category represents the top-level companies' directives. These directives set companies foundations, visions as well as top management commitment. In the context of ISO 24089 and R156 the directive contains a high-level descriptions of SUMS processes at organization level and the proof that the company complies with ISO 24089 and/or UNECE R156

—

Organization level

At organization level, processes introduced on the directive are specified. These processes include but are not limited to:

- Supporting processes (document management)
- Privacy management (the companies must ensure the privacy of customer data)
- Configuration management
- Change management process

Project level

At project level, processes are split in five categories: Generic project processes, Infrastructure processes required for the SW update, Vehicle processes required for the SW update, Software update package processes and finally software update campaign processes. These categories allow to ensure that both the infrastructure pushing the update and the vehicle getting access and processing it are ready prior to the deployment.

Generic project processes: describes and ensure that the organization develop and maintain a plan for each software update projects. This includes:

- Process that describes the Software update project plan
- Tailoring activities process
- Documentation of processes to preserve integrity of software metadata, …

Infrastructure processes: describes the infrastructure's requirement to ensure a safe, secure, and reliable software update. This includes:

- Managing cybersecurity risk
- Managing vehicle configuration information
- Performing software update campaigns
- Processing software update packages

Vehicle and vehicle systems level describes the functionality required in and for vehicle or vehicle systems. This includes

- Managing Safety and cybersecurity risk for software update in the vehicle (Reference to ISO 26262, ISO 21448, and ISO/SAE 21343)
- Managing vehicle configuration item
- Communicating to vehicle user the software update campaign information

Software update package development: describes how the software update package are verified and validates and which vehicle's type or system will receive this update package. If all elements are conformed the software update package is approved for release. This includes

- Documentation of verification and validation made
- Documentation of targets, contents, and compatibility
- Documentation of approval release

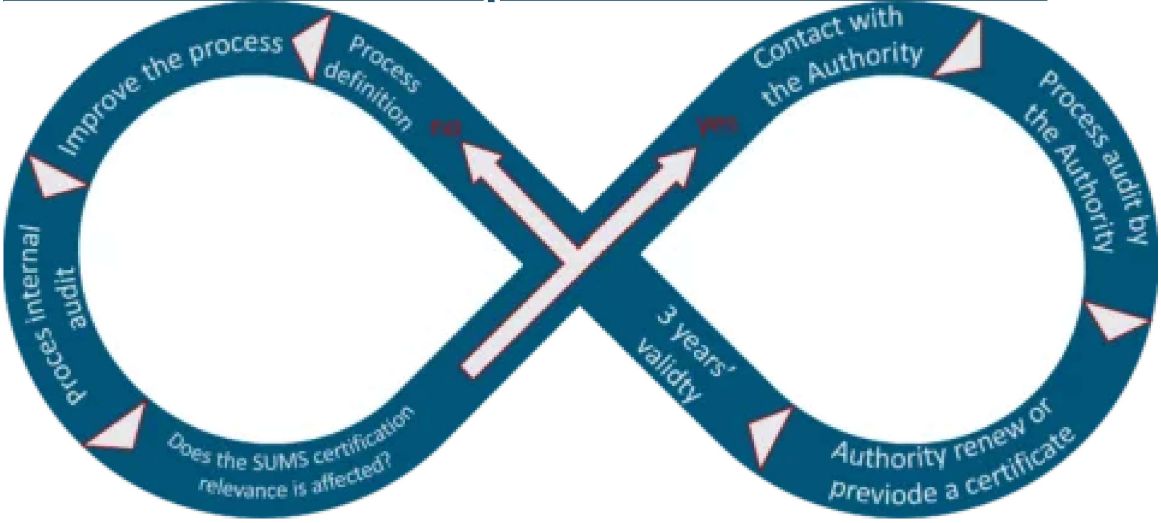
Software update campaign operations: describes the update procedure from the preparation to the completion of the campaign. This includes:

- Listing Software update campaign preparation results
- Listing Software update campaign execution results
- Logging the purpose of the campaign (target vehicles, end date, …)

SUMS Certificate for OEM

Vehicles manufactures shall certify their SUMS by an Approval Authority. The certification is based on an assessment with the Approval Authority or the Technical Service that demonstrates they have all necessary processes to comply with the UN ECE R156 regulation. Passing this assessment gives a “Certificate of Compliance for SUMS. This certificate has a validity of 3 years. After that the Approval Authority or its Technical service shall proceed to a new assessment to renew or issue a new certificate.

SUMS continuous improvement / assessment


Improve the process
Process definition
no
yes
Contact with the Authority
Process audit by the Authority
Proces internal audit
3 years' validity
Does the SUMS certification relevance is affected?
Authority renew or previode a certificate

SUMS needs to be continuously improved, based on internal/external feedback. This improvement process allows to ensure that the management system correspond to the company needs and is correctly operated throughout company activities and projects.

—

The manufacturer shall inform the Approval Authority or its Technical service in case of modification/improvement of the management system that shall affect the relevance of the certificate of compliance.

—

How can CertX support your roadmap for compliance

As a recognized certification body across the automotive industry, CertX can support your organization from different perspective, depending on your maturity and position across supply chains. Below a brief summary of services provided by our Team dedicated to cyber security & SW update team:

—

Educational support for engineers and managers

- Awareness training: tailored sessions / workshops on SW update procedures & cyber security related activities and technics
- Certifiable training: ISO/SAE 24089 Automotive Software Update Red Belt (A-SURB), ISO/SAE 21434 Automotive Cyber Security Red Belt (A-CSRB)

Gap Analysis and pre-assessment for identifying weak spots

- Evaluation of current compliance with ISO 24089 and UN R156 and/or ISO/SAE 21434 and UN R155 R156 requirements, either on organizational level (SUMS/CSMS) or product level (product-specific artefacts)
  - For OEM to prepare compliance audit/assessment with homologation authorities
  - For suppliers' readiness with upcoming requirements from OEM

Supporting services for SUMS/CSMS process design & implementation

- Support for integrating new practices into organization systems, ensuring secure handover to operating teams knowledge transfer
  - Usually based on initial gap analysis results / findings

<u>In the future</u>**: ISO 24089 – SUMS certifications**

- Independent and recognized evaluation of your SW update related process framework ISO/SAE 24089 supporting UN R156 negotiation