FINAL DRAFT

Technical Report

ISO/DTR 24935

Road vehicles — Software update over the air using mobile cellular network

Véhicules routiers — Mise à jour du logiciel à distance (OTA) à l'aide d'un réseau cellulaire mobile

ISO/TC **22**/SC **32**

Secretariat: **JISC**

Voting begins on:
2025-03-18

Voting terminates on:
2025-05-13

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/DTR 24935:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The electronic control units (ECUs) and their software have become major components of road vehicles in recent years. Software, in particular, must be updated as it is frequently revised.

- The need for updating software is more prominent as cybersecurity and passenger safety become more dependent on software.
- The software-update operation was usually performed at workshops, which was very inconvenient for vehicle users.

The ECUs requiring software-update operations range from a smart key to power train ECUs.

- These days, the software-update operation for ECUs has become possible even while vehicles are serviced in gas stations. Moreover, mobile cellular networks can be used to update vehicle software regardless of the vehicle location.

ISO 24089 was published as the standard for vehicle software update engineering. ISO 24089 addresses the requirements on the organization, software-update project, infrastructure level, vehicle and vehicle-systems level, software-update package and software-update campaign, among others. However, ISO 24089 does not address the actual technologies and procedures for updating software.

This document describes an actual experience involving technologies and systems for updating software using mobile cellular networks. In addition, the results of verification by mounting the ECU developed in this document on an actual vehicle are included.

Road vehicles — Software update over the air using mobile cellular network

1 Scope

This document describes use cases and activities for updating software in vehicles over the air using mobile cellular network. This document provides a case study on the use of International Standards in preparing software-update packages, managing infrastructure and operation within the vehicles.

This document includes descriptions of a reference model for software-update operations and metadata which can be used during the software-update operations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 24089, *Road vehicles — Software update engineering*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 24089 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
to archive
to store logs and records on a permanent medium such that they may be *retrieved* (3.9) at a later date

3.2
authentication
act of proving an assertion, such as the identity of a computer system user

3.3
authorization
formal permission to use a product within specified application constraints

3.4
cryptography
discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification

[SOURCE: ISO/IEC 2382:2015, 2126278]

3.5
Ethernet
communication protocol specified in ISO/IEC/8802-3:2021

3.6
metadata
data that provides information about other data

3.7
mobile cellular network
telecommunications network where the link to and from end nodes is wireless and the network is distributed over land areas called cells

3.8
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: ISO/IEC 27002:2022, 3.1.19]

3.9
to retrieve
to restore from the *archived* (3.1) data

3.10
validation
confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are achieved

[SOURCE: ISO/SAE 21434:2021, 3.1.36]

3.11
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[SOURCE: ISO/SAE 21434:2021, 3.1.37]

4 Abbreviated terms

ACC	Accessory
AVB	Audio Video Bridge
AVN	Audio Video Navigation
AVTP	Audio Video Transport Protocol
BCU	Body Control Unit
BSB	Binary Software Block
CAN	Controller Area Network
CM	Campaign Management
DoIP	Diagnostic communication over Internet Protocol
DS	Digital Signature
ECU	Electronic Control Unit
EOL	End of Line
E2E	End to End
HMI	Human Machine Interface

HSM	Hardware Security Module
ITS	Intelligent Transport Systems
IVN	In-Vehicle Network
KMIP	Key Management Interoperability Protocol
KMS	Key Management Server
LDM	Local Dynamic Map
LKAS	Lane Keeping Assist System
MAC	Message Authentication Code
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
OTA	Over The Air
OTAM	OTA Master
OTP	One Time Password
SM	Software Management
SUP	Software Update Package
SUV	Sport Utility Vehicles
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
UDS	Unified Diagnostic Services
URL	Uniform Resource Locator
VCI	Vehicle Configuration Information
VIN	Vehicle Identification Number
VM	Vehicle Management
VMG	Vehicle Mobile Gateway

5 General

5.1 Purpose

The purpose of this document is to share the technical experiences in using mobile cellular networks for updating software in vehicle ECUs, and to share the experience in the adoption of related International Standards such as ISO 24089.

5.2 Structure of this document

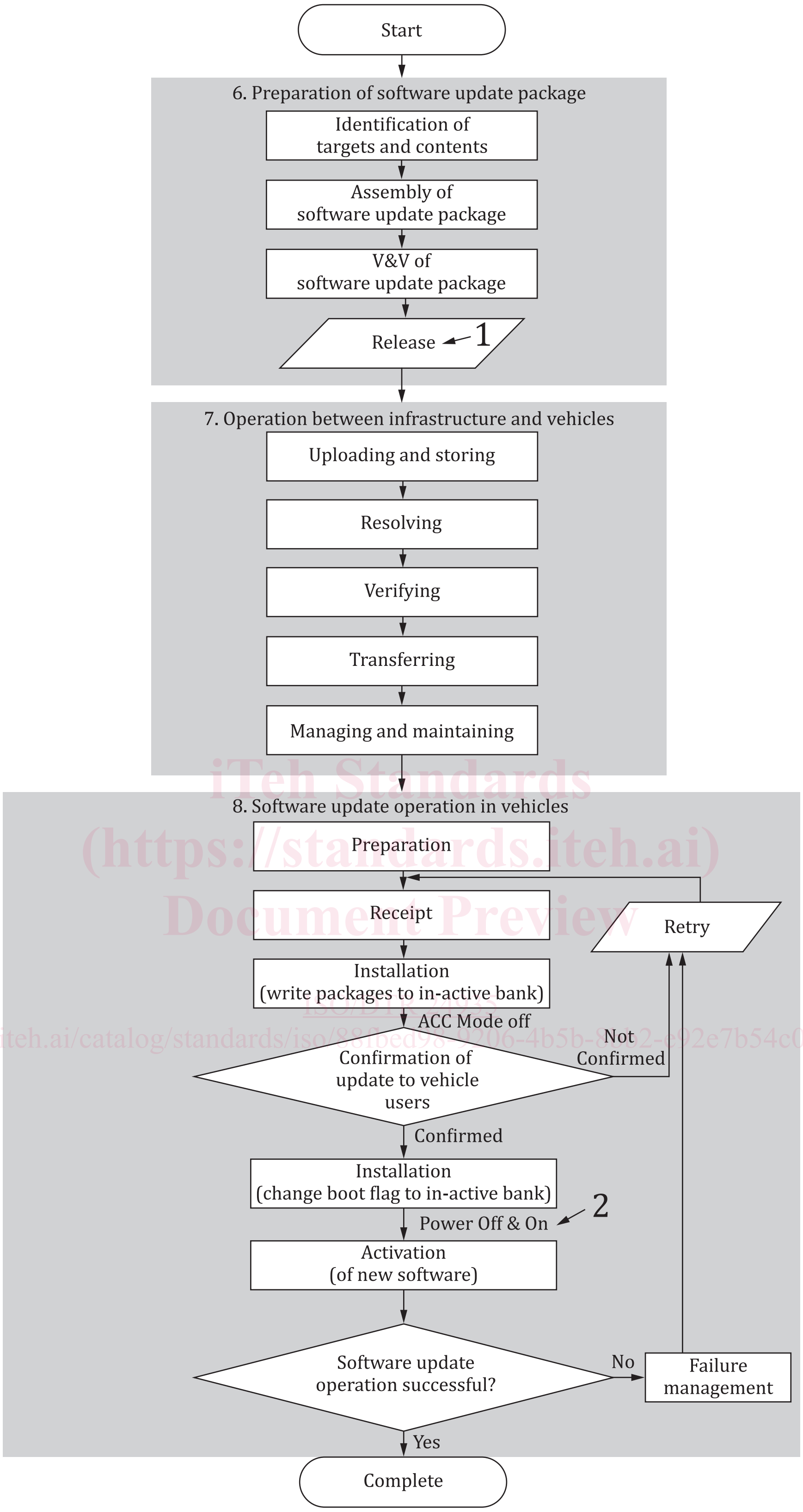
Clause 5 describes the purpose and the structure of this document. It also describes basic and cybersecurity models for the software-update operation.

Clause 6 describes the preparation of the software-update package. This clause includes roles of vehicle manufacturers and suppliers in the software-update process for vehicle ECUs.

Clause 7 describes the capabilities and functions, which are used to perform the activities during the software-update campaign in the update server. It also describes the flow of activities involved during the software-update operation.

Clause 8 describes the software-update operations. This clause includes software-update operations in the IVN.

Clause 9 describes the results of evaluating the software-update operation in actual vehicles.


Start
6. Preparation of software update package
Identification of targets and contents
Assembly of software update package
V&V of software update package
Release
1
7. Operation between infrastructure and vehicles
Uploading and storing
Resolving
Verifying
Transferring
Managing and maintaining
8. Software update operation in vehicles
Preparation
Receipt
Retry
Installation (write packages to in-active bank)
ACC Mode off
Not Confirmed
Confirmation of update to vehicle users
Confirmed
Installation (change boot flag to in-active bank)
2
Power Off & On
Activation (of new software)
Software update operation successful?
No
Failure management
Yes
Complete

Key

1 software-update packages (SUPs) are released

2 vehicle is powered off and on

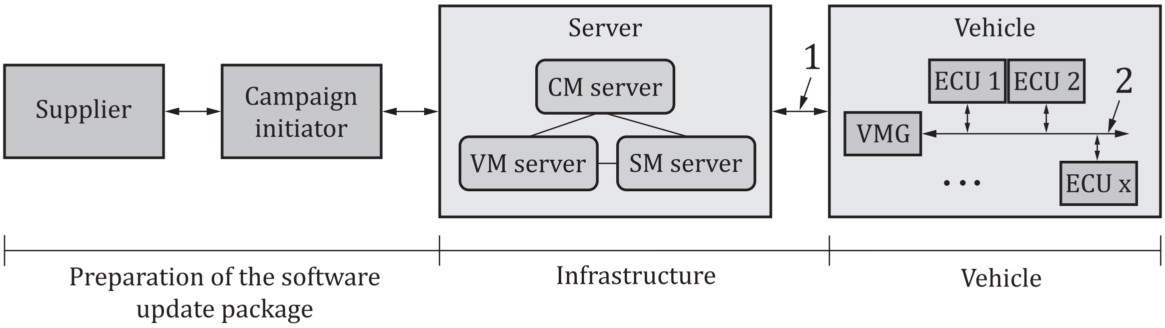
Figure 1 — Overview of software-update activities

Figure 1 shows the overview of the software-update activities and the corresponding clauses which explain the activities.

Once the SUP is ready, it is released. Then the interaction of the infrastructure and the vehicle takes place. When the vehicle is turned on (power on), the vehicle is ready to install a new SUP in ACC mode and begins to write the SUP in an in-active bank. After the ACC mode is turned off, the installation and activation take place if the vehicle user agrees to the software-update operations.

5.3 Reference model

The basic model, which is used in this document, consists of three parts: preparation of the SUP, infrastructure and vehicle (see Figure 2).



Key

1 mobile cellular network

2 in-vehicle network (e.g. CAN or automotive Ethernet)

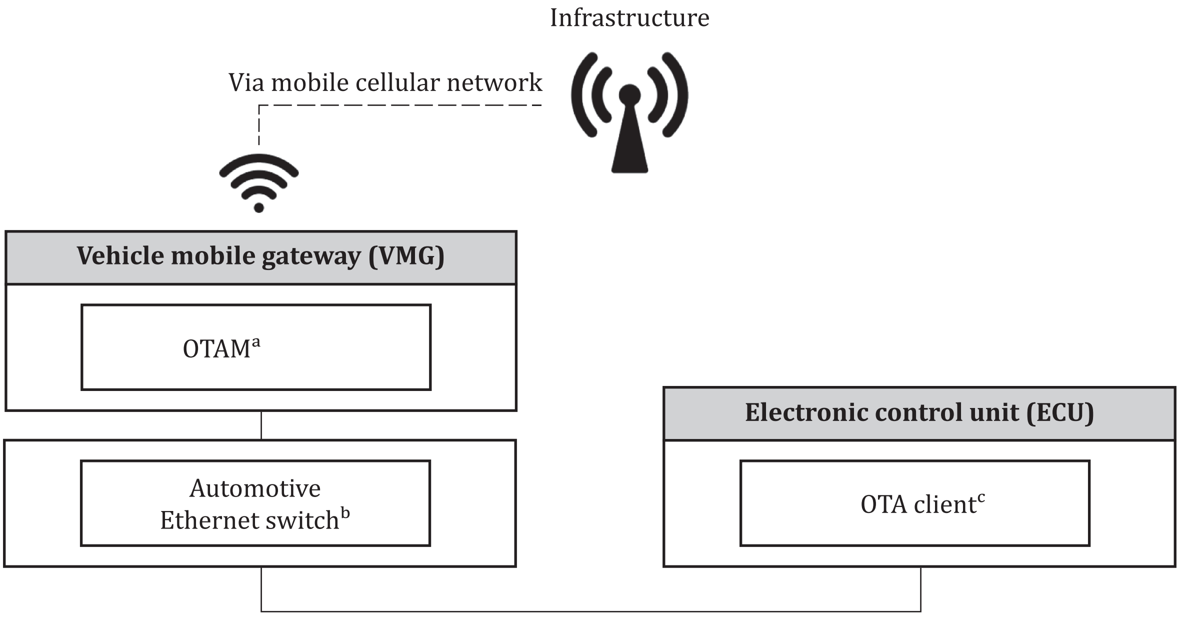
Figure 2 — Reference model for the software-update activities

The preparation of the SUP part covers the development of the software to be updated, and tools or methodologies for identifying the target vehicles whose ECU is to be updated by the software-update operation. It also addresses generation of the metadata which can be used by infrastructure or vehicles during the software-update operation, and creation of the SUP by adding appropriate additional information such as cybersecurity-related information. However, the development of the software itself is out of scope in this document.

The infrastructure includes a mobile cellular network and the update server which consists of a CM server, VM server and SM server (see Clause 7). The infrastructure covers uploading the SUP into the storage server, validating the SUP, and managing the VCI. It also performs resolving the target vehicles, communicating with the target vehicles, transferring the SUP into the recipients, and handling the result of the software-update operation.

The architecture of the vehicle is depicted in Figure 3. The software-update operation within the vehicle is managed by the VMG, which communicates with the CM server via the mobile cellular network, receives the SUP from the server, reports the result of the software-update operation to the server, checks the vehicle state, validates the received SUP, transfers the received SUP into the corresponding ECU, and checks the result of the installation and activation of software in the ECU.

In-vehicle networks typically include CAN and automotive Ethernet, which are linked through an Ethernet gateway. All ECUs to be updated by the software-update operation are connected to the automotive Ethernet network for the purpose of faster and parallel data transfer. The ECUs to be updated support a dual bank memory and UDS diagnostic communication capabilities.


Infrastructure
Via mobile cellular network
Vehicle mobile gateway (VMG)
OTAM[a]
Automotive
Ethernet switch[b]
Electronic control unit (ECU)
OTA client[c]

Key

[a] See 8.1.3.

[b] See 8.1.2.

[c] See 8.1.2 and 8.1.3.

Figure 3 — Architecture of the vehicle

5.4 Cybersecurity model

5.4.1 General

This subclause addresses the cryptographic techniques and corresponding cryptographic key management models used in this document. 5.4.2 introduces the cryptographic techniques used in this document to provide basic security services. 5.4.3 proposes solutions for supplier and vehicle manufacturer cryptographic key management models for verification and validation of the SUP.

5.4.2 Use of cryptography

Corruption or tampering of data while handling it might have safety-related impact(s) on vehicle(s). Hence, data used during preparation or software-update operation is protected by cryptographic techniques.

Cryptographic techniques used to provide or support several basic security services are as follows:

- Confidentiality
  - TLS is used to provide confidentiality in communication between vehicle manufacturers, suppliers, and vehicles. In this document, cryptographic suites providing a security strength of 128 bits or higher are utilized.
  - Cryptographic objects (e.g. certificates, private keys) used by vehicle manufacturers and suppliers are encrypted and stored in their respective KMS to prevent leakage (see 5.4.3).
- Identity authentication
  - Any access to VCI and SUPs is controlled using identity authentication. The access to the update server is allowed only to the authorized person and the vehicle that is authorized to access the corresponding SUP.

  - The OASIS KMIP is used as a protocol to communicate with the KMS. KMIP supports MFA using ID/password or additional OTP as identity authentication methods to grant access the KMS. In this document, it is possible to access the KMS using a private key/certificate that is pre-issued and securely provided by the KMS administrator.

- Integrity and source authentication

  - The SUP consists of multiple BSBs, along with the DS values for each block, as illustrated in Figure 4.

  - The DS, generated with the supplier's private key, ensures integrity and source authentication for a BSB. The recipient can verify the integrity and source of the software by performing DS verification using the supplier's certificate, which is pre-injected to the ECU's HSM.

  - The DS, generated with the vehicle manufacturer's private key, ensures integrity and source authentication for an SUP. The recipient can verify the integrity and source of the SUP by performing DS verification using the vehicle manufacturer's certificate, which is pre-injected into the VMG's HSM.

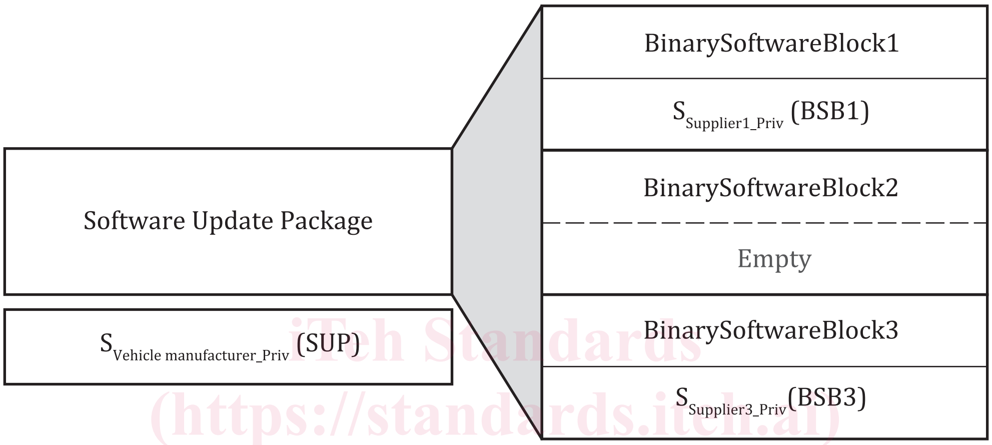

BinarySoftwareBlock1
$S_{\text{Supplier1\_Priv}}$ (BSB1)
BinarySoftwareBlock2
Empty
BinarySoftwareBlock3
$S_{\text{Supplier3\_Priv}}$(BSB3)
Software Update Package
$S_{\text{Vehicle manufacturer\_Priv}}$ (SUP)

Figure 4 — Structure of the SUP

- Authorization

  - The vehicle manufacturer's private key for the DS of SUPs is managed in a KMS located in a secure room controlled by the vehicle manufacturer, and only authorized users (e.g. developer, build server) can request signature generation.

  - The supplier's private key for the DS of software is managed in the KMS located in a secure room controlled by the supplier, and only authorized users (e.g. developer, build server) can request signature generation.

  - Keys are logically separated for each purpose and model by using the group concept, which is a system object in KMIP v.3.0.

  - Each group has its own cryptographic objects and users. Users can access only the cryptographic objects of their own group.

NOTE The user is a person or entity that uses cryptographic objects in the KMS. This can refer to developers, build servers, EOLs, etc.

- Non-repudiation

  - Vehicle manufacturers and suppliers use the non-repudiation property of DSs to protect against future legal disputes, including defects in distributed software.