~~2022-09-06~~

ISO/~~DIS~~FDIS 24089:2022(E)

2022-10-12

ISO TC 22/SC 32/WG 12

Secretariat: JISC

Road vehicles – Software update engineering

~~DIS stage~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~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.~~

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~~www.iso.org~~

Published in Switzerland

Contents

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

Electronic control units and software of increasing complexity have become essential to the operation of road vehicles in recent years. This software is often updated to increase functionality and maintain the safety and cybersecurity of road vehicles.

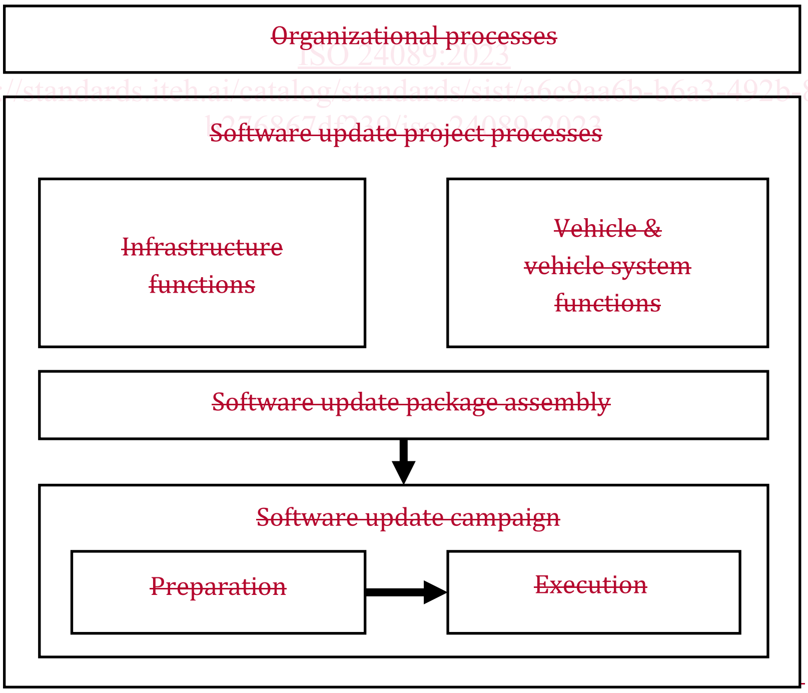
Today, in-vehicle software is updated in a workshop by skilled persons or automatically over-the-air by the vehicle user. With the increased frequency of software update campaigns, it is important to have individual vehicle configuration information. Therefore, the establishment and application of software update engineering is important to ensure software quality, cybersecurity, and safety.

Software update engineering activities occur throughout the ~~lifecycle~~life cycle of vehicles.

This document provides vocabulary, objectives, requirements, and guidelines related to software update engineering as a foundation for common understanding throughout the supply chain. By applying requirements and recommendations in this document, the following benefits can be achieved for software update engineering:

- safety and cybersecurity are addressed in software update operations in road vehicles;
- establishment of processes, including goal setting, planning, auditing, process monitoring, process measurement, and process improvement;
- shared awareness of safety and cybersecurity among related parties.

Figure 1 shows the overview of this document.


~~Organizational processes~~
~~Software update project processes~~
~~Infrastructure functions~~
~~Vehicle & vehicle system functions~~
~~Software update package assembly~~
~~Software update campaign~~
~~Preparation~~
~~Execution~~

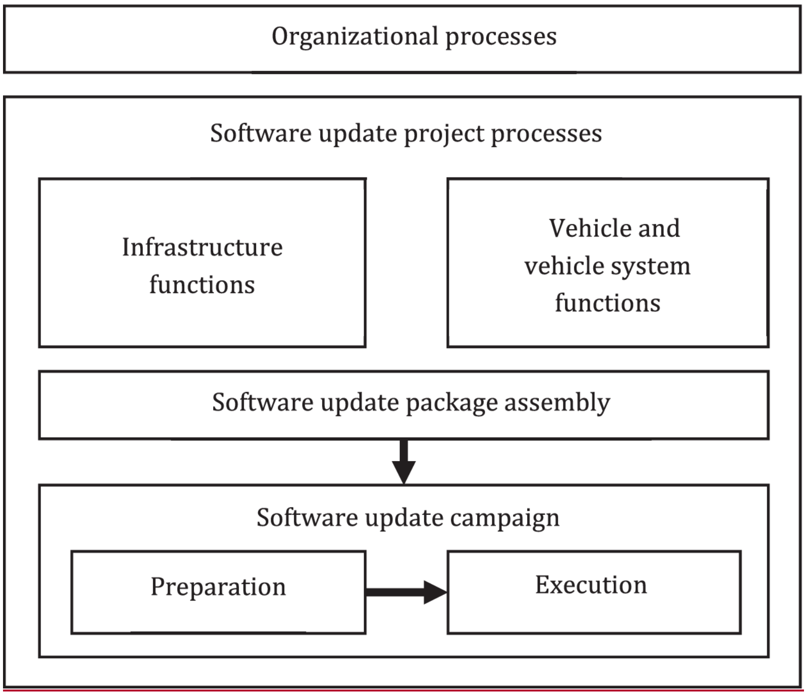

Organizational processes
Software update project processes
Infrastructure functions
Vehicle and vehicle system functions
Software update package assembly
Software update campaign
Preparation
Execution

Figure 1~~ – ~~— Overview of this document

In this document, clauses are structured using the following approach:

- each process is defined and implemented before it is executed;
- each process is established, documented~~,~~ and maintained.

This document describes the following activities:

- implementation of organizational level processes for software update engineering;
- implementation of software update project level processes for each software update project;
- definitions of functions for the vehicle and infrastructure to support the activities and processes of this document;
- assembly of software update packages using functions in the infrastructure;
- preparation and execution of software update campaigns using functions in the vehicle and infrastructure.

Road vehicles – Software update engineering

1 Scope

This document specifies requirements and recommendations for software update engineering for road vehicles on both the organizational and the project level.

This document is applicable to road vehicles whose software can be updated.

The requirements and recommendations in this document apply to vehicles, vehicle systems, ECUs, infrastructure, and the assembly and deployment of software update packages after the initial development.

This document is applicable to organizations involved in software update engineering for road vehicles. Such organizations can include vehicle manufacturers, suppliers, and their subsidiaries or partners.

This document establishes a common understanding for communicating and managing activities and responsibilities among organizations and related parties.

The development of software for vehicle functions, except for software update engineering, is outside the scope of this document.

Finally, this document does not prescribe specific technologies or solutions for software update engineering.

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 26262-6, *Road ~~Vehicles ---~~vehicles — Functional ~~Safety ---~~safety — Part 6: Product development at the software level*

ISO 26262-8, *Road ~~Vehicles ---~~vehicles — Functional ~~Safety ---~~safety — Part 8: Supporting processes*

ISO/SAE 21434, *Road vehicles ~~---~~— Cybersecurity ~~Engineering~~ engineering*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 General terminology

3.1.1
compatibility
capability of *software* (3.1.15) to be executable on *vehicle systems* (3.1.25) without conflicts

Note 1 to entry: Compatibility can be checked by *vehicle configuration information* (3.1.24).

3.1.2
condition
criteria required for a *software update operation* (3.1.19) to be completed successfully

Note 1 to entry: Conditions can include *compatibility* (3.1.1), *safe vehicle state* (3.1.13), *in-vehicle resources* (3.1.11), and external resources.

EXAMPLE The presence of a *skilled person* (3.1.14) during a software update operation~~ (3.1.19)~~.

3.1.3
corrective action
action to eliminate or contain a problem or failure

3.1.4
cybersecurity
road vehicle cybersecurity
context in which assets are sufficiently protected against threat scenarios to *vehicle systems* (3.1.25) of road vehicles and *infrastructure* (3.1.10) required to support *software update engineering* (3.1.18)

Note 1 to entry: In this document, for the sake of brevity, the term cybersecurity is used instead of road vehicle cybersecurity.

[SOURCE: ISO/SAE 21434:2021, 3.1.9, modified ~~–~~— “to items of road vehicles, their functions and their electrical or electronic components~~"~~” has been replaced by ~~"~~“to vehicle systems of road vehicles and infrastructure required to support software update engineering~~"~~” and the Note 1 to entry has been modified.]

3.1.5
cybersecurity risk
effect of uncertainty on *cybersecurity* (3.1.4) expressed in terms of attack feasibility and impact

[SOURCE: ISO/SAE 21434:2021, 3.1.29]

3.1.6
dependency
effect of *software* (3.1.15) for one *vehicle system* (3.1.25) on the same or other *vehicle systems* (3.1.25)

Note 1 to entry: A dependency can generate a *condition* (3.1.2) in the metadata of a *software update package* (3.1.20).

EXAMPLE A communication interface between two *electronic control units (ECUs)* (3.1.7).

3.1.7
ECU
electronic control unit
~~**ECU**~~
embedded device in a vehicle whose *software* (3.1.15) can be updated

3.1.8
functional safety
absence of unreasonable risk due to hazards caused by malfunctioning behaviour of *vehicle systems* (3.1.25)

[SOURCE: ISO 26262-1:2018, 3.67, modified ~~–~~— “E/E” was replaced ~~"E/E" with "~~by “vehicle~~"]~~”.]

3.1.9
functional safety risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 26262-1:2018, 3.128, modified ~~–~~— The term has been modified from ~~"~~“risk~~"~~” to ~~"~~“functional safety risk~~"~~” for the scope of this document~~]~~.]

3.1.10
infrastructure
processes and information systems managing any combination of *software update operations* (3.1.19), *software update campaigns* (3.1.16), documentation, and *vehicle configuration information* (3.1.24), including both digital and manual activities

Note 1 to entry: Infrastructure can include any combination of servers, tools, and manual activities used in the software update operation~~ (3.1.19).~~.

3.1.11
in-vehicle resource
vehicle or *electronic control unit (ECU)* (3.1.~~4~~7) available properties relevant for *software update engineering* (3.1.18)

EXAMPLE Available or remaining computational power, network capacity, RAM capacity, storage capacity, or battery capacity.

3.1.12
recipient
individual instance of a vehicle, *vehicle system* (3.1.25), or ~~*ECU*~~*electronic control unit (ECU)* (3.1.7) that receives a *software update package* (3.1.20) during a *software update campaign* (3.1.16)

3.1.13
safe vehicle state
vehicle operating mode based on *conditions* (3.1.2) for performing *software update operations* (3.1.19) without an unreasonable level of risk

Note 1 to entry: Safe vehicle state can be different depending on the *conditions* (3.1.2) required for the *software update package* (3.1.20).

Note 2 to entry: Safe vehicle state can vary based on the software update operation ~~(3.1.19) ~~step being performed.

EXAMPLE The motor is off, the parking brake is applied.

3.1.14
skilled person
individual with relevant technical education, training or experience to execute *software update operations* (3.1.19)

Note 1 to entry: A skilled person can be a mechanic in a workshop.

Note 2 to entry: A skilled person can be authorized or certified for their ~~specialised~~specialized training or be a skilled *vehicle user* (3.1.26).

[SOURCE: ISO 10209:2022, 3.14.36, modified ~~– the~~— The phrase “to enable them to perceive risks and avoid hazards occurring during use of a product” has been replaced by “to execute software update operations~~”]~~”.]

3.1.15
software

computer programs and associated data intended for *installation* (3.2.2) on vehicles, *vehicle systems* (3.1.25), or *electronic control units (ECUs)* (3.1.7), that may be dynamically written or modified during execution

[SOURCE: NIST SP 800-53, modified ~~- added "~~— The phrase “intended for installation on vehicles, vehicle systems, or electronic control units (ECUs~~"]~~)” was added.]

3.1.16
software update campaign

sequence of identifying *targets* (3.1.23) and resolving *recipients* (3.1.12); distributing *software update packages* (3.1.20); and monitoring and documenting results of *software update operations* (3.1.19)

3.1.17
software update distribution method

mechanism for delivery of a *software update package* (3.1.20) during a *software update campaign* (3.1.16)

Note 1 to entry: The software update distribution method can be wired (e.g. tool, USB flash drive), wireless (e.g. cellular or Wi-Fi) or hardware replacement.

Note 2 to entry: Hardware replacement can be replacing an ~~*ECU*~~*electronic control unit (ECU)* (3.1.7) with the effect of *software* (3.1.15) version replacement.

3.1.18
software update engineering

application of a systematic and managed approach to the processes of planning, development, and deployment of *software update packages* (3.1.20)

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.3810, modified ~~- changed "~~— “disciplined, quantifiable~~" to "~~” was replaced by “and managed~~",~~”, and ~~changed "~~“development, operation and maintenance of software~~" to "~~” was replaced by “processes of development, planning, and deployment of software update packages~~"]~~”.]

3.1.19
software update operation

steps involved in *receipt* (3.2.1), *installation* (3.2.2~~),~~) and *activation* (3.2.3) of *software update packages* (3.1.20) in a vehicle, *vehicle systems* (3.1.25), or *electronic control units (ECUs)* (3.1.7)

3.1.20
software update package

set of *software* (3.1.15) and associated metadata that is intended to be deployed to one or more vehicles, *vehicle systems* (3.1.25), or *electronic control units (ECUs)* (3.1.7)

3.1.21
software update project

set of *software update engineering* (3.1.18) activities for one or more *targets* (3.1.23)

Note 1 to entry: Activities can include developing or adapting the *infrastructure* (3.1.10), vehicle capabilities, or processes described in this document.

Note 2 to entry: A software update project can encompass multiple *software update campaigns* (3.1.16).

3.1.22
tailor, verb
to omit or perform an activity in a different manner compared to its description in this document

[SOURCE: ISO/SAE 21434:2021, 3.1.32]

3.1.23
target
one or more classes of vehicles, *vehicle systems* (3.1.25), or *electronic control units (ECUs)* (3.1.7) determined by *vehicle configuration information* (3.1.24)

3.1.24
vehicle configuration information
comprehensive accounting of hardware versions, *software* (3.1.15) versions~~,~~ and configuration parameters in a vehicle

3.1.25
vehicle system
functional group of one or more *electronic control units (ECUs)* (3.1.7) and attached hardware

Note 1 to entry: Attached hardware can be, for example, a sensor, actuator~~,~~, or light, ~~etc.~~ that is not an ECU ~~(3.1.7)~~..

EXAMPLE Braking system or infotainment system.

3.1.26
vehicle user
person operating, driving, owning or managing a vehicle

Note 1 to entry: A vehicle user can be a *skilled person* (3.1.14).

3.2 Terms related to the software update operation

3.2.1
receipt
step in the *software update operation* (3.1.19) when a tool, vehicle, *vehicle system* (3.1.25), or ~~*ECU*~~*electronic control unit (ECU)* (3.1.7) receives a *software update package* (3.1.20)

EXAMPLE 1 Downloading a software update package ~~(3.1.20).~~.

EXAMPLE 2 Transferring a software update package ~~(3.1.20)~~ using a tool.

3.2.2
installation

step in the *software update operation* (3.1.19) when the relevant parts of a *software update package* (3.1.20) are written to a vehicle, *vehicle system* (3.1.25), or ~~*ECU*~~*electronic control unit (ECU)* (3.1.7) but are not yet *activated* (3.2.3)

3.2.3
activation
step in the *software update operation* (3.1.19) when the relevant parts of an *installed* (3.2.2) *software update package* (3.1.20) become executable on a vehicle, *vehicle system* (3.1.25), or ~~*ECU*~~*electronic control unit (ECU)* (3.1.7)

EXAMPLE 1 A new automated driving function is *installed* (3.2.2) and ready for execution, but is only executed after the *vehicle user* (3.1.26) starts the function.

EXAMPLE 2 The relevant parts of a software update package ~~(3.1.20)~~ for a vehicle, vehicle system ~~(3.1.25),~~, or *ECU* (3.1.7) are installed ~~(3.2.2)~~ and executed immediately after activation without user interaction.

4 Organizational level requirements

4.1 Objectives

The objectives of this clause are to ensure that the following are performed:

a) establishing organization-specific rules and processes for software update engineering;

b) adopting quality management, functional safety management~~,~~ and cybersecurity management for software update engineering;

c) instituting and maintaining a continuous improvement process for software update engineering;

d) establishing an information sharing policy for software update engineering; and

e) performing an organizational audit for process compliance.

4.2 General

This clause covers the responsibility of the organization engaged in software update engineering to have governance in place so that the processes for software update engineering can conform to the requirements of this document. Governance includes compliance with required ISO standards as well as organizational activities such as continuous improvement, information sharing, and supporting processes. This clause also establishes auditing requirements for this document.

4.3 Requirements and recommendations

4.3.1 Governance

4.3.1.1 If the organization performs software update engineering activities, then this document applies.

4.3.1.2 The organization shall establish, document, and maintain rules and processes for software update engineering to:

~~-~~— enable the implementation of the requirements of this document;