



DPC: 22/30394082 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 11 January 2022

Origin: International

Latest date for receipt of comments: 06 March 2022

Project No. 2019/00956

Responsible committee: AUE/32 Electrical and electronic components and general system aspects (Road vehicles)

Interested committees:

Title: Draft BS ISO 24089 Road vehicles - Software update engineering.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 06 March 2022

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/DIS 24089

ISO/TC 22/SC 32

Secretariat: JISC

Voting begins on:
2022-01-11

Voting terminates on:
2022-04-05

Road vehicles — Software update engineering

Véhicules routiers — Ingénierie de mise à jour du logiciel

ICS: 43.040.15

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

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.

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.

This document is circulated as received from the committee secretariat.



Reference number
ISO/DIS 24089:2022(E)

AVA Documents
Document Sharing Hub
© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 General terminology	2
3.2 Terminology for the software update operation	5
4 Organization level software update requirements	5
4.1 Objectives	5
4.2 General	6
4.3 Requirements and recommendations	6
4.4 Work products	8
5 Project level software update requirements	8
5.1 Objectives	8
5.2 General	9
5.3 Requirements and recommendations	9
5.4 Work products	10
6 Infrastructure design and development	10
6.1 Objectives	10
6.2 General	11
6.3 Requirements and recommendations	11
6.4 Work products	12
7 Vehicle and vehicle systems design and development	12
7.1 Objectives	12
7.2 General	13
7.3 Requirements and recommendations	13
7.4 Work products	15
8 Software update package development	16
8.1 Objectives	16
8.2 General	16
8.3 Requirements and recommendations	16
8.4 Work products	18
9 Software update campaign operations	18
9.1 Objectives	18
9.2 General	18
9.3 Requirements and recommendations	18
9.4 Work products	23
Bibliography	24

56 Foreword

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

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

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

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

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

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

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

Introduction

Road vehicles have been increasing their use of electronic control systems in recent years. With this has come increasing complexity of software in vehicles. As a result, software has become essential to the operation of road vehicles. This software is often updated to increase functionality and maintain the safety and cybersecurity of road vehicles. Therefore the establishment and application of software update engineering are important to ensure software quality, cybersecurity, and road vehicle safety.

Today, in-vehicle software is updated by skilled persons using specialized tools and equipment or by remote software updates. With the increased frequency of software updates it is important to have accurate current configuration information for individual vehicles to ensure software quality, cybersecurity, and road vehicle safety.

This document assigns accountability for the processes required to update software safely and securely, provides the fundamental requirements for performing those processes correctly, and producing high quality software update packages. By applying the software update engineering requirements and recommendations in this document, the following benefits can be expected:

- Safe and secure software update operations in road vehicles;
- Establishment of clear processes, including explicit goal setting, planning, auditing, process monitoring, process measurement, and process improvement;
- Shared awareness of safety and cybersecurity among related parties;
- Establish trust that software update engineering activities are based on clear and controlled processes.

Figure 1 shows the overview of this document.

Clause 4 and clause 5 define necessary organizational rules and processes.

Clause 6 and clause 7 define the software update capabilities for infrastructure and vehicles.

Clause 8 defines creation of software update packages.

Clause 9 defines the preparation and execution of software update campaigns.

In this document, clauses are structured using following idea,

- Process should be defined before actual operation
- Set of Processes should be managed as assets, i.e. documented and maintained
- Processes should be managed in higher level than each project, in order to reuse or refer established processes in other project.

1. Scope			
2. Normative references			
3. Terms and definitions			
4. Organization level software update requirements			
5. Project level software update requirements			
6. Infrastructure design and development	7. Vehicle and vehicle systems design and development	8. Software update package development	9. Software update campaign operations

Figure 1 – Overview of this document

- 111 Software update engineering activities occur throughout the life cycle of the vehicle.
- 112 It is important to apply software quality assurance, cybersecurity, and safety processes to software update
- 113 engineering activities.

Road vehicles – Software Update Engineering

1 Scope

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

These requirements and recommendations apply to the vehicle, its systems, and/or the infrastructure. Additionally, these requirements and recommendations apply to ECUs installed in road vehicles, and the creation of software update packages after the original development.

In addition, this document specifies requirements and recommendations for deployment of software update packages to road vehicles.

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

This document enables a common understanding for communicating and managing activities and responsibilities among stakeholders.

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

This document applies to organizations involved in software update engineering in road vehicles. Such organizations can include OEMs, suppliers, and their subsidiaries or contractual partners.

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--- Functional Safety --- Part 6: Product development at the software level*

ISO 26262-8, *Road Vehicles--- Functional Safety --- Part 8: Supporting processes*

ISO/SAE 21434, *Road vehicles --- Cybersecurity Engineering*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

— IEC Electropedia: available at <http://www.electropedia.org/>

3.1 General terminology

3.1.1

corrective action

action to eliminate or contain a problem or failure

3.1.2

cybersecurity

road vehicle cybersecurity

condition in which assets are sufficiently protected against threat scenarios in road vehicles, vehicle systems and/or ECUs and infrastructure supporting software update engineering.

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

[SOURCE: ISO/SAE 21434: modified - definition aligned to terms used in this document, added infrastructure, removed Note 1 to entry]

3.1.3

cybersecurity risk

effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact

[SOURCE: ISO/SAE 21434]

3.1.4

electronic control unit

ECU

embedded device in a vehicle whose software can be updated

Note 1 to entry: Replacing an ECU can be a method of updating its software.

Note 2 to entry: ECUs can be implemented on a larger computing device as virtual ECUs.

3.1.5

functional safety risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 26262-1]

3.1.6

infrastructure

services that manage software update operations, software update campaigns, documentation and/or vehicle configuration information, including both digital and manual activities

Note 1 to entry: Infrastructure can include servers, tools, and/or manual activities used in the software update operation.

Note 2 to entry: Function(s) of the infrastructure can be implemented in the vehicle and/or externally.

3.1.7

in-vehicle resources

vehicle or ECU available properties relevant for software update engineering