SLOVENSKI STANDARD
SIST EN 50128:2011/A2:2020

01-oktober-2020

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Programska oprema za železniške krmilne in zaščitne sisteme - Dopolnilo A2

Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire

SIST Preview
(https://ecommerce.sist.si)
SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

Ta slovenski standard je istoveten z: EN 50128:2011/A2:2020

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50128:2011/A2:2020 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 50128:2011/A2:2020

SIST Preview
(https://ecommerce.sist.si)

SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

SIST EN 50128:2011/A2:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50128:2011/A2

July 2020

ICS 35.240.60; 45.020; 93.100

English Version

Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme

This amendment A2 modifies the European Standard EN 50128:2011; it was approved by CENELEC on 2020-06-22. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This amendment exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

SIST Preview
(https://ecommerce.sist.si)

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50128:2011/A2:2020 E

SIST EN 50128:2011/A2:2020

Content

European foreword 3
1 General Changes 4
2 Modification to the Introduction 4
3 Modification to the Scope 4
4 Modification to Clause 2, Normative references 4
5 Modifications to 3.1, Terms and definitions 5
6 Modifications to Clause 4, Objectives, conformance and software safety integrity levels 6
7 Modifications to Clause 5, Software management and organization 7
8 Modifications to 6.2, Software verification 7
9 Modifications to 6.3, Software validation 7
10 Modifications to 6.4, Software assessment 7
11 Modifications to 6.5, Software quality assurance 8
12 Modifications to 6.7, Support tools and languages 8
13 Modifications to Clause 7, Generic software development 9
14 Modifications to Clause 8, Development of application data or algorithms: systems configured by application data or algorithms 9
15 Modifications to Clause 9, Software deployment and maintenance 10
16 Modifications to Annex A, Criteria for the Selection of Techniques and Measures 11
17 Modifications to Annex C 14

SIST Preview
(https://ecommerce.sist.si)

SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

SIST EN 50128:2011/A2:2020

European foreword

This document (EN 50128:2011/A2:2020) has been prepared by SC 9XA, “Communication, signalling and processing systems”, of Technical Committee CENELEC TC 9X, “Electrical and electronic applications for railways”.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2021-06-22
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2023-06-22

The EN 50128:2011 standard was amended to align with EN 50126-1:2017, EN 50126-2:2017 and EN 50129:2018. In addition, some technical mistakes were corrected and some clarifications were added.

This European Standard should be read in conjunction with EN 50126-1:2017 “*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process”,* EN 50126-2:2017 *“Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety*” and EN 50129:2018 “*Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*”.

SIST Preview
(https://ecommerce.sist.si)

SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

SIST EN 50128:2011/A2:2020

1 General Changes

All occurrences of SIL 0 within EN 50128:2011 are replaced with Basic Integrity (EN 50126-1:2017, 3.7).

All occurrences of safety function(s) are replaced with safety-related function(s).

Use of the term “EN 50126-1” is replaced by “EN 50126-1 and EN 50126-2”.

The term “assessment” in the standard means “independent safety assessment” as per definition of EN 50126-1:2017, 3.33.

All statements qualified by the words “software safety integrity level” are applicable also to Basic Integrity.

2 Modification to the Introduction

The following paragraph is added at the end of the Introduction:

This European Standard does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet security requirements that may be needed by the safety-related system. IT security can affect not only the operation but also the functional safety of a system. For IT security, appropriate IT security standards should be applied.

NOTE IEC/ISO standards that address IT security in depth are ISO 27000 series, ISO/IEC TR 19791 and the IEC 62443 series.

3 Modification to the Scope

The following subclause 1.10 is added:

1.10 For the development of User Programmable Integrated Circuits (e.g. FPGA and CPLD) guidance is provided in EN 50129:2018, Annex F.

SIST Preview
(https://standards.iteh.ai)

4 Modification to Clause 2, Normative references

Replace the list of normative references by the following:

EN 50126-1:2017, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process

SIST EN 50128:2011/A2:2020
https://standards.iteh.ai/catalog/standards/sist/ccb9ccb6-5ea532910c1f/sist-en-50128-2011-a2-2020

EN 50126-2:2017, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety

EN 50129:2018, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

EN ISO 9000:2015, Quality management systems – Fundamentals and vocabulary

EN ISO 9001:2015, Quality management systems – Requirements

ISO/IEC 90003:2014, Software engineering – Guidelines for the application of ISO 9001 to computer software

ISO/IEC 25000 series, Systems and software engineering – Systems and software Quality Requirements and Evaluation

SIST EN 50128:2011/A2:2020

5 Modifications to 3.1, Terms and definitions

Replace 3.1.9 (deleted) with:

3.1.51
error, <in software>
defect, mistake or inaccuracy that could result in a deviation from the intended performance or behaviour of the software

Note 1 to entry: definition is derived from EN 50126-1:2017, 3.20 and adapted for software (caused by systematic fault, e.g. human error, in line with EN 50126-1:2017 3.20 Note 2).

3.1.52
fault
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault in software is systematic.

[SOURCE: IEC 60050-821:2017, 821-11-20, modified – The note 1 to entry has been modified.]

Replace 3.1.10 with:

3.1.10
failure, <of an item>
loss of ability to perform as required

Note 1 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

[SOURCE: IEC 60050-821:2017, 821-11-19, modified – The notes 1 and 2 have been omitted. A new note 1 to entry has been added.]

Replace 3.1.17 with:

3.1.17
pre-existing software
software developed prior to the application currently in question

Note 1 to entry: This includes commercial off-the-shelf software, open-source software and software previously developed but not in accordance with this European Standard.

[SOURCE: EN 50126-1:2017, 3.43, modified – The end of the definition has been moved to the note 1 to entry.]

Definition 3.1.26 replaced by:

3.1.26
risk, <for railway RAMS>
combination of expected frequency of loss and the expected degree of severity of that loss

[SOURCE: EN 50126-1:2017, 3.57]

Definition 3.1.27 replaced by:

3.1.27
safety
freedom from unacceptable risk

[SOURCE: IEC 60050-903:2013, 903-01-19]

Definition 3.1.28 replaced by:

3.1.28
safety authority
body responsible for delivering the authorization for the operation of the safety-related system

[SOURCE: IEC 60050-821:2017, 821-12-52]

Remove the term 3.1.29 and its definition (see also General Changes).

Definition 3.1.30 replaced by:

SIST Preview
(https://ecommerce.sist.si)
SIST EN 50128:2011/A2:2020

SIST EN 50128:2011/A2:2020

3.1.30
safety-related software
software which performs safety-related functions

[SOURCE: IEC 60050-821:2017, 821-12-60, modified – “safety functions” has been replaced with “safety-related functions”.]

Definition 3.1.46 replaced by:

3.1.46
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The term “validated” is used to designate the corresponding status.

Note 2 to entry: The use conditions for validation can be real or simulated.

Note 3 to entry: In design and development, validation concerns the process of examining an item to determine conformity with user needs.

Note 4 to entry: intentionally deleted

Note 5 to entry: Multiple validations can be carried out if there are different intended uses.

[SOURCE: IEC 60050-192:2015, 192-01-18, modified – The note 4 is not relevant for software]

Definition 3.1.48 replaced by:

3.1.48
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The term “verified” is used to designate the corresponding status.

Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement.

Note 3 to entry: Verification is conducted at various life cycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that life cycle phase.

[SOURCE: IEC 60050-192:2015, 192-01-17, modified – The note 3 to entry has been modified.]

Add the following 3.1.50 (in line with EN 50126-1):

3.1.50
safety-related
carries responsibility for safety

[SOURCE: IEC 60050-821:2017, 821-01-73]

6 Modifications to Clause 4, Objectives, conformance and software safety integrity levels

4.4 is replaced by:

4.4 At least the Basic Integrity requirements of this European Standard shall be fulfilled for the software part of functions that have a safety impact below SIL 1.

NOTE Basic Integrity requirements can also be used for development of non safety-related software.

SIST Preview
(https://ecommerce.sist.si)
SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

SIST EN 50128:2011/A2:2020

7 Modifications to Clause 5, Software management and organization

In 5.1.2.10 bullet n) replace as follows:

n) A person who is Validator may also perform the role of Verifier, but still maintaining independence from the Project Manager. In this case, as for all other development activities, the Validator/Verifier outputs shall be reviewed by another competent person.

In 5.1.2.11 bullet m) replace as follows:

m) A person who is Validator may also perform the role of Verifier, Integrator and Tester. In this case, as for all other development activities, the Validator/Verifier outputs shall be reviewed by another competent person.

8 Modifications to 6.2, Software verification

In 6.2.3, Output documents, Bullet 3) is replaced by:

3) Software Planning Verification Report

In 6.2.4, Requirements, 6.2.4.10 is replaced by:

6.2.4.10 A Software Planning Verification Report shall be written, under the responsibility of the Verifier, on the basis of the input documents from 6.2.2. The Software Planning Verification Report shall be reviewed by the Validator.

The requirement in 6.2.4.11 refers to the Software Planning Verification Report.

6.2.4.11 is replaced by:

6.2.4.11 Once the software plans have been established (Software Quality Assurance Plan, Software Configuration Management Plan, Software Verification Plan, Software Validation Plan, and Software Maintenance Plan) verification shall confirm

a) that the software plans meet the general requirements for readability and traceability in 5.3.2.7 to 5.3.2.10 and in 6.5.4.14 to 6.5.4.17 as well as the specific requirements in 6.2.4.3 to 6.2.4.9,

b) the internal consistency of the software plans,

c) the coherency of the software plans.

The results shall be recorded in a Software Planning Verification Report.

SIST Preview
(https://ecommerce.sist.si)
SIST EN 50128:2011/A2:2020
https://ecommerce.sist.si/catalog/standards/sist/ac9ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

9 Modifications to 6.3, Software validation

In 6.3.3, Output documents:

Remove 3) Software Validation Verification Report

Remove 6.3.4.12, 6.3.4.13 and 6.3.4.14

10 Modifications to 6.4, Software assessment

In 6.4.3, Output documents:

Remove 3) Software Assessment Verification Report

Remove 6.4.4.6 and 6.4.4.7

SIST EN 50128:2011/A2:2020

11 Modifications to 6.5, Software quality assurance

In 6.5.3, Output documents:

Remove 3) Software Quality Assurance Verification Report

In 6.5.4, Requirements:

6.5.4.3 is replaced by:

6.5.4.3 A Software Quality Assurance Plan shall be written on the basis of the input documents from 6.5.2.

Remove 6.5.4.7 and 6.5.4.8.

12 Modifications to 6.7, Support tools and languages

6.7.4.4 is replaced (based on EN 50129:2018, 6.3) by:

6.7.4.4 For each tool in class T3, evidence shall be available that the output of the tool conforms to the specification of the output or failures in the output are detected. Evidence may be based on the same steps necessary for a manual process as a replacement for the tool and an argument presented if these steps are replaced by alternatives (e.g. validation of the tool). Evidence shall be based on one or more of the following techniques.

a) a suitable combination of history of successful use, for which the following conditions apply:

- It has been confirmed and periodically checked by analysis, examination and provision of objective evidence that the tool is suitable for the purpose for which it is to be used.

- There is sufficient qualitative evidence from previous use to show that the output of the tool can be trusted, including a suitable combination of documented history of successful use (project and applications realized, list of anomalies, identification of successive versions).

SIST Preview
(https://ecommerce.sist.si)

b) tool validation as specified in 6.7.4.5,

c) tool diversity, which is typically obtained by using one of the possibilities below:

https://ecommerce.sist.si/catalog/standards/sist/ae93ed9d-3882-49e7-a5cb-5ea532910c1f/sist-en-50128-2011-a2-2020

- Use of two diverse tools to perform the same function, with comparison of their outputs.

- Use one tool to perform the function and feed its output into a diverse tool which regenerates the input data provided to the first tool, with comparison of the original and regenerated input data.

- Use one tool to perform the function and subject its output to verification of results by an independent tool, which is diverse from the first tool because it works in accordance with different principles, for example a rule-checking tool to confirm that the output conforms to all relevant rules (e.g. rules for the positioning of balises).

d) compliance with the safety integrity levels derived from the risk analysis of the process and procedures including the tools,

e) other appropriate methods for avoiding or handling failures introduced by tools (e.g. verification of tool output).

NOTE 1 As an example the use of a non-trusted compiler can be justified as follows.

The object code produced by the compiler has been subjected to a combination of tests, checks and analyses which are capable of ensuring the correctness of the code to the extent that it is consistent with the target Safety Integrity Level. In particular, the following applies to all tests, checks and analyses.

- Testing has been shown to have a sufficiently high coverage of the implemented code. If there is any code unreachable by testing, it has been shown by checks or analyses that the function concerned is executed correctly when the code is reached on the target.