SLOVENSKI STANDARD
SIST EN 50128:2011/oprAA:2019

01-junij-2019

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

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

Ta slovenski standard je istoveten z: **EN 50128:2011/prAA:2019**

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/oprAA:2019 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
EN 50128:2011

prAA

March 2019

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 draft amendment prAA, if approved, will modify the European Standard EN 50128:2011; it is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2019-06-21.

It has been drawn up by CLC/TC 9X.

If this draft becomes an amendment, 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.

This draft amendment was established by CENELEC 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.

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

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.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Project: 68080

Ref. No. EN 50128:2011/prAA:2019 E

Content

European foreword

This document (EN 50128:2011/prAA:2019) has been prepared by SC 9XA, “Communication, signaling and processing systems”, of Technical Committee CENELEC TC 9X, “Electrical and electronic applications for railways”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

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*”.

1 General Changes

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

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

Use of the term “EN 50126-1” is replaced by “EN 50126-1 and EN 50129-2”.

The term “assessment” in the standard is meant as “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.

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): Generic RAMS Process

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

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

EN ISO 9000, Quality management systems – Fundamentals and vocabulary

EN ISO 9001, Quality management systems – Requirements

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

ISO/IEC 9126 series, Software engineering – Product quality

5 Modifications to 3.1, Terms and definitions

Replace 3.1.9 (deleted) with:

3.1.51
error, < in software >
defect, mistake or inaccuracy in the development process which 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, 3.20 and adapted for software

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

Note 1 to entry: A fault for 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
all software developed prior to the application currently in question is classed as pre-existing software

Note 1 to entry: That 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:

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

Note 1 to entry: software is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties can be of functional or non-functional nature.

[SOURCE: IEC 60050-821:2017, 821-12-60, modified – “safety functions” has been replaced with “safety-related functions”. The note 1 to entry has been added.]

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: Validation is normally performed during the final stage of development, under defined operating conditions, although it can also be performed in earlier stages.

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

[SOURCE: IEC 60050-192:2015, 192-01-18]

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 EN50126-1):

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.

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 address

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.

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

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.