SLOVENSKI STANDARD
SIST EN 50126-1:2018

01-januar-2018

Nadomešča:
SIST EN 50126-1:2001
SIST EN 50126-1:2001/AC:2013

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 1. del: Generični procesi RAMS

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS Prozess

Applications ferroviaires Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1: Processus FMDS générique

Ta slovenski standard je istoveten z: **EN 50126-1:2017**

ICS:

03.120.01	Kakovost na splošno	Quality in general
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50126-1:2018 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50126-1

October 2017

ICS 29.280; 45.020

Supersedes EN 50126-1:1999

English Version

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1: Processus FMDS générique

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS Prozess

This European Standard was approved by CENELEC on 2017-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard 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 European Standard 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.

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.

CENELEC

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 50126-1:2017 E

Contents

Page

European foreword

This document (EN 50126-1:2017) has been prepared by CLC/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) 2018-07-03
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2020-07-03

This document supersedes EN 50126-1:1999 which has been technically revised.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*" consists of the following parts:

— Part 1: Generic RAMS process;

— Part 2: System approach to safety.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

Introduction

EN 50126-1:1999 was aimed at introducing the application of a systematic RAMS management process in the railway sector. Through the application of this standard and the experiences gained over the last years, the need for revision and restructuring became apparent with a need to deliver a systematic and coherent approach to RAMS applicable to all the railway application fields Command, Control and Signalling (Signalling), Rolling Stock and Electric power supply for Railways (Fixed Installations).

The revision work improved the coherency and consistency of the standard, the concept of safety management and the practical usage of EN 50126, and took into consideration the existing and related Technical Reports as well.

This European Standard provides railway duty holders and the railway suppliers, throughout the European Union, with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS.

Processes for the specification and demonstration of RAMS requirements are cornerstones of this standard. This European Standard promotes a common understanding and approach to the management of RAMS.

EN 50126 forms part of the railway sector specific application of IEC 61508. Meeting the requirements in this European Standard together with the requirements of other suitable standards is sufficient to ensure that additional compliance to IEC 61508 does not need to be demonstrated.

With regard to safety, EN 50126-1 provides a Safety Management Process which is supported by guidance and methods described in EN 50126-2.

EN 50126-1 and EN 50126-2 are independent from the technology used. As far as safety is concerned, EN 50126 takes the perspective of safety with a functional approach.

The application of this standard can be adapted to the specific requirements for the system under consideration.

This European Standard can be applied systematically by the railway duty holders and railway suppliers, throughout all phases of the life cycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The system-level approach developed by this European Standard facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This European Standard promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAMS and cost for railway applications. Adoption of this European Standard will support the principles of the European Single Market and facilitate European railway inter-operability.

In accordance with CENELEC editing rules [1)], mandatory requirements in this standard are indicated with the modal verb “shall”. Where justifiable, the standard permits process tailoring.

Specific guidance on the application of this standard for Safety aspects is provided in EN 50126-2. EN 50126-2 provides various methods for use in the safety management process. Where a particular method is selected for the system under consideration, the mandatory requirements for this method are by consequence mandatory for the safety management of the system under consideration.

This European Standard consists of the main part (Clause 1 to Clause 8) and Annexes A, B, C, D and ZZ. The requirements defined in the main part of the standard are normative, whilst Annexes are informative.

1) CEN/CENELEC Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2017-02), Annex H.

1 Scope

This part 1 of EN 50126

- considers RAMS, understood as reliability, availability, maintainability and safety and their interaction;
- considers the generic aspects of the RAMS life cycle. The guidance in this part can still be used in the application of specific standards;
- defines:
  - a process, based on the system life cycle and tasks within it, for managing RAMS;
  - a systematic process, tailorable to the type and size of the system under consideration, for specifying requirements for RAMS and demonstrating that these requirements are achieved;
- addresses railway specifics;
- enables conflicts between RAMS elements to be controlled and managed effectively;
- does not define:
  - RAMS targets, quantities, requirements or solutions for specific railway applications;
  - rules or processes pertaining to the certification of railway products against the requirements of this standard;
  - an approval process for the railway stakeholders.

This part 1 of EN 50126 is applicable to railway application fields, namely Command, Control and Signalling, Rolling Stock and Fixed Installations, and specifically:

- to the specification and demonstration of RAMS for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined subsystems and components within these major systems, including those containing software; in particular:
  - to new systems;
  - to new systems integrated into existing systems already accepted, but only to the extent and insofar as the new system with the new functionality is being integrated. It is otherwise not applicable to any unmodified aspects of the existing system;
  - as far as reasonably practicable, to modifications and extensions of existing systems already accepted, but only to the extent and insofar as existing systems are being modified. It is otherwise not applicable to any unmodified aspect of the existing system;
- at all relevant phases of the life cycle of an application;
- for use by railway duty holders and the railway suppliers.

It is not required to apply this standard to existing systems which remain unmodified, including those systems already compliant with any former version of EN 50126.

The process defined by this European Standard assumes that railway duty holders and railway suppliers have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within EN ISO 9001.

2 Normative references

Not applicable.

3 Terms and definitions

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

3.1
acceptance
status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose

3.2
accident
unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

[SOURCE: IEC 60050-821: FDIS2016, 821-12-02]

3.3
approval
permission for a product or process to be marketed or used for stated purposes or under stated conditions

Note 1 to entry: Approval can be based on fulfilment of specified requirements or completion of specified procedures.

[SOURCE: EN ISO/IEC 17000:2004, 7.1]

[SOURCE: IEC 60050-902:2013, 902-06-01]

3.4
assurance
confidence in achieving a goal being pursued. Declaration intended to give confidence

3.5
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

Note 1 to entry: Whilst “audit” applies to management systems, “assessment” applies to conformity assessment bodies as well as more generally.

[SOURCE: EN ISO/IEC 17000:2004, 4.4, modified – The references to other terms within ISO/IEC 17000 have been replaced by hyperlinks to entries in the IEV.]

[SOURCE: IEC 60050-902:2013, 902-03-04]

3.6
availability, <of a product>
ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[SOURCE: IEC 60050-821: FDIS2016, 821-05-82, modified]

3.7
basic integrity
integrity attribute for safety related function with a TFFR higher than (less demanding) 10^{-5} [h^{-1}] or non-safety-related function.

3.8
collective risk
risk, resulting from e.g. a product, process or system, to which a population or group of people is exposed

Note 1 to entry: Collective risk is not to be confused with risk of multiple victim accident.

Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group. However, the collective risk divided by the number of individuals will only provide the average individual risk.

Note 3 to entry: A group of people could be, for example, rail staff working in a restaurant car or all passengers using a particular network.

3.9
commercial off-the-shelf product
product defined by market-driven need, commercially available and whose fitness for purpose has been deemed acceptable by a broad spectrum of commercial users

[SOURCE: EN 50128:2011, 3.1.3, modified]

3.10
common cause failure
failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause

[SOURCE: IEC 60050-192:2015, 192-03-18]

3.11
compliance
state where a characteristic or property of a product, system or process satisfies the specified requirements

3.12
configuration management
process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation

[SOURCE: IAEA 3, modified]

[SOURCE: IEC 60050-395:2014, 395-07-52]

3.13
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

[SOURCE: IEC 60050-821: FDIS2016, 821-12-14]

3.14
corrective maintenance
maintenance carried out after fault detection to effect restoration

Note 1 to entry: Corrective maintenance of software invariably involves some modification.

[SOURCE: IEC 60050-192:2015, 192-06-06]

3.15
design
activity applied in order to analyse and transform specified requirements into acceptable solutions

[SOURCE: IEC 60050-821: FDIS2016, 821-12-16, modified]

3.16
deterministic
expresses that a behaviour can be predicted with certainty

Note 1 to entry: A deterministic event in a system can be predicted with certainty from preceding events which are either known or are the same as for a proven equivalent system.

3.17
diversity
existence of two or more different ways or means of achieving a specified objective

Note 1 to entry: Diversity is specifically provided as a defence against common cause failure. It can be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

[SOURCE: IEC 60050-395:2014, 395-07-115]

3.18
entity
person, group or organisation who fulfils a role as defined in this standard

3.19
equivalent fatality
expression of fatalities and weighted injuries and a convention for combining injuries and fatalities into one figure for ease of evaluation and comparison of risks

3.20
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.21
failure, <of an item>
loss of ability to perform as required

Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

[SOURCE: IEC 60050-192:2015, 192-03-01, modified Note 1 to entry has been omitted]

[SOURCE: IEC 60050-821:FDIS2016, 821-11-19]

Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

3.22
failure mode
manner in which failure occurs

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.23
failure rate
limit of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t, t + Δt) and the duration of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval

Note 1 to entry: For applications where distance travelled or number of cycles of operation is more relevant than time then the unit of time can be replaced by the unit of distance or cycles, as appropriate.

Note 2 to entry: The term “failure rate” is often used in the sense of “mean failure rate” defined in IEV 192-05-07.

[SOURCE: IEC 60050-821:FDIS2016]

3.24
fault, <in a system>
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

[SOURCE: IEC 60050-821:FDIS2016, 821-11-20]

3.25
function, <of an item>
specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input

Note 1 to entry: A function can be specified or described without reference to the physical means of achieving it.

[SOURCE: IEC 60050-821:FDIS2016, 821-12-25, modified]

3.26
functional safety
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351, 351-57-06]

3.27
generic product
product independent of applications, fulfilling predefined boundary conditions, interfaces and functionality (black box)

EXAMPLE: Examples point machines, axle counters, real-time operating systems, fail-safe computer platform without application software.

[SOURCE: IEC 60050-821:FDIS2016, 821-01-57]

3.28
hazard
condition that could lead to an accident

Note 1 to entry: The equivalent definition in [IEC 60050-903:2013, 903-01-02] refers to "harm" instead of "accident".

3.29
hazard analysis
process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level

Note 1 to entry: Similar process aspects are also considered in risk assessment. In this standard the term is applied in life cycle phases after “requirements specification”.

[SOURCE: IEC 60050-821: FDIS2016, 821-11-23]

3.30
hazard log
document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced

[SOURCE: IEC 60050-821:FDIS2016, 821-12-27]

3.31
hazard rate
rate of occurrence of a hazard

Note 1 to entry: For detailed mathematical understanding of "rate" refer to the definition of "failure rate".

3.32
implementation
activity applied in order to transform the specified designs into their realization

[SOURCE: IEC 60050-821:FDIS2016, 821-12-29, modified]

3.33
independent safety assessment
process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit for its intended purpose in relation to safety

Note 1 to entry: Requirements for independence are defined in this European Standard.

3.34
individual risk
risk, resulting from e.g. a product, process or system, to which an individual person is exposed

Note 1 to entry: Individual risk is not to be confused with risk of single victim accidents.

Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group. However, the collective risk divided by the number of individuals will only provide the average individual risk.

3.35
integration
process of assembling the elements of a system according to the architectural and design specification, and the testing of the integrated unit

3.36
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

EXAMPLE A typical system lifecycle consists of: concept and definition; design and development; construction, installation and commissioning; operation and maintenance; mid-life upgrading, or life extension; and decommissioning and disposal.

Note 1 to entry: The stages identified will vary with the application.