SLOVENSKI STANDARD
oSIST prEN 50126-1:2013

01-januar-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 FDMS générique

Ta slovenski standard je istoveten z: **prEN 50126-1:2012**

ICS:

29.280	Električna vlečna oprema	Electric traction equipment
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50126-1:2013 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50126-1

October 2012

ICS 45.020

Will supersede EN 50126-1:1999 (partially), CLC/TR 50126-2:2007, CLC/TR 50126-3:2008

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 FDMS générique

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

This draft European Standard is submitted to CENELEC members for CENELEC enquiry.
Deadline for CENELEC: 2013-03-29.

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

If this draft becomes a European Standard, 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.

This draft European Standard 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, 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.

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Project: 21752

Ref. No. prEN 50126-1:2012 E

Contents

Page

Foreword

This document [prEN 50126-1:2012] has been prepared by CLC/TC 9X "Electrical and electronic applications for railways".

This document is currently submitted to the Enquiry.

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: Systems approach to safety;

– Part 4: Functional safety – Electrical/Electronic/Programmable electronic systems;

– Part 5: Functional safety – Software.

This new edition of EN 50126 (all parts) will supersede EN 50126-1:1999, CLC/TR 50126-2:2007, CLC/TR 50126-3:2008, EN 50128:2011 and EN 50129:2003.

This part of EN 50126 covers the RAMS process. It is mainly based on EN 50126-1:1999.

This part of EN 50126 will supersede EN 50126-1:1999 (together with prEN 50126-2:2012), CLC/TR 50126-2:2007 and CLC/TR 50126-3:2008.

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).

Introduction

EN 50126-1:1999 was produced to introduce the application of a systematic RAMS management process in the railway sector. For safety-related electronic systems for signalling, EN 50128 and EN 50129 were produced. Through the application of these standards 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 Signalling, Rolling Stock and Electric power supply for Railways (Fixed Installations).

The revision work improved the coherency and consistency of the standards, 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 is the railway sector specific application of IEC 61508. Meeting the requirements in this European Standard 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. EN 50126-4 and EN 50126-5 provide guidance specific to safety-related E/E/PE technology of railway applications. Their application is determined through the application of the general RAMS process of EN 50126-1 and through the outcome of the safety-related methods described in EN 50126-2. As far as safety is concerned, EN 50126 takes the perspective of functional safety. This does not exclude other aspects of safety. However, these are not the focus.

The aims set for revision of EN 50126 required a better understanding of the systems approach and improved methods for applying the safety management process described in EN 50126-1. EN 50126-2 provides this guidance.

The application of this standard should be adapted to the specific requirements of 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 systems-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.

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 the ISO 9001.

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 in the case of process tailoring is provided in 7.3 of EN 50126-1. 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 of this method are by consequence mandatory for the safety management of the system under consideration.

1) CENELEC “Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2009-08), 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 is still applicable 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 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 by the safety authority;
- does not specify requirements for ensuring system security.

This part 1 of EN 50126 is applicable

- 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 sub-systems and components within these major systems, including those containing software; in particular:
  - to new systems;
  - to new systems integrated into existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system;
  - to modifications of existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects 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 including those systems already compliant with any version of former EN 50126, EN 50128 or EN 50129, which remain unmodified. Railway applications mean Command, Control & Signalling, Rolling Stock and Electric Power Supply for Railways (Fixed Installations).

In this standard the term hardware refers to E/E/PE components or systems. If non E/E/PE hardware is meant, this is specifically mentioned.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9001, Quality management systems – Requirements

ISO/IEC GUIDE 51, Safety aspects – Guidelines for their inclusion in standards

3 Terms and definitions

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

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

3.2
accident
an unintended event or series of events resulting in loss of human health or life, damage to property or environmental damage

Note 1 to entry: The term includes losses from accidents arising within a short time scale (e.g. collision, explosion) and also those incurred over the long-term (e.g. release of a toxic substance).

3.3
application conditions
those conditions which need to be met in order for a system to be safely integrated and safely operated.

Note 1 to entry: Application conditions can for example be: operational restrictions (e.g. speed limit, maximum duration of use) operational rules, maintenance restrictions (e.g. requested maintenance intervals) or environmental conditions.

3.4
approval
the legal act, often focused on safety, to allow a product, system or process to be placed into service

Note 1 to entry: A legal act can be performed by an authorised entity (i.e. a NOBO)

3.5
assessment
process to form a judgement on whether a product, system or process meets the specified requirements, based on evidence

Note 1 to entry: Independence of assessment is only necessary where explicitly specified.

3.6
assessor
an entity that carries out an assessment

Note 1 to entry: Independence of the assessor is only necessary where explicitly specified.

3.7
assurance
confidence in achieving a goal being pursued. Declaration intended to give confidence

3.8
audit
a documented, systematic and independent examination to determine whether the procedures specific to the requirements

- comply with the planned arrangements,
- are implemented effectively and
- are suitable to achieve the specified objectives

3.9
availability
the ability of a product 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

Note 1 to entry: Figure B.1 (Annex B) illustrates the concept of availability and clarifies the correct use of contributory terms.

3.10
collective risk
a 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 multiple 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.

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.

3.11
commercial off-the-shelf software
software defined by market-driven need, commercially available and whose fitness for purpose has been deemed acceptable by a broad spectrum of commercial users

3.12
common cause failure
failures of different items resulting from the same cause and where these failures are not consequences of each other

3.13
compliance
a state where a characteristic or property of a product, system or process satisfies the specified requirements

3.14
configuration management
a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, to control changes to those characteristics, to record and report change processing and implementation status and to verify compliance with specified requirements

3.15
consequence analysis
to analyze the consequences of each hazard up to accidents and losses

3.16
corrective maintenance
the maintenance carried out after fault recognition and intended to put a product into a state in which it can perform a required function

3.17
data-driven software
software configured by data and/or algorithms for producing the executable software for an application by making use of an existing generic software

3.18
designer
an entity that analyses and transforms specified requirements into acceptable design solutions which have the required safety integrity

3.19
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.

3.20
diversity

a means of achieving all or part of the specified requirements in more than one independent and dissimilar manner

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

3.21
entity
a person, group or organisation who fulfil a role as defined in this standard

3.22
equivalent fatality
an 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

3.23
error
a 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.

3.24
fail-safe
a concept which is incorporated into the design of a product such that, in the event of a failure, it enters or remains in a safe state

3.25
failure
the termination of the ability of an item to perform a required function

Note 1 to entry: After failure the item has a fault.

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

3.26
failure mode
a predicted or observed manner in which the product, system or process under consideration can fail

3.27
failure rate
the limit, if this exists, 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 length 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: Failure rates are often assumed as constant. This is not always valid, e.g. for components subject to wear out (mechanical, pneumatic, electromechanical, etc.).

3.28
fault
the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions

Note 1 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure (e.g. in case of a design fault).

3.29
fault detection time
time span which begins at the instant when a failure occurs and ends when the existence of the fault is detected

3.30
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

3.31
firmware
an ordered set of instructions and associated data stored in a way that is functionally independent of main storage

3.32
function
a specified action or activity which may 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.

3.33
functional safety
the perspective of safety focused on the functions of a system

Note 1 to entry: Functional safety does not only consider normal operation.

Note 2 to entry: Functional safety can be based on safety functions as well as on safety-related functions.

3.34
generic product
product (hardware and/or software) which can be used for a variety of installations, either without making any changes or purely trough the configuration of the hardware or the software (for example by the provision of application-specific data and/or algorithms)

3.35
hazard
a condition that could lead to an accident

3.36
hazard analysis
an analysis comprising hazard identification, causal analysis and common cause analysis

3.37
hazard log
the document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced

Note 1 to entry: The Hazard Log compiles evidence on the implementation of safety requirements regarding all identified hazards, thus supporting the demonstration of completeness of the safety assurance activities

Note 2 to entry: A "hazard record" is an extract of the hazard log that is suitable for transferring between stakeholders.

3.38
hazard rate
the rate of occurrence of a hazard

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

3.39
implementation
the activity applied in order to transform the specified designs into their realisation

3.40
implementer
the entity that carries out implementation

3.41
independence (functional)
freedom from any mechanism which can affect the correct operation of more than one function as a result of either systematic or random failure

3.42
independence (physical)
freedom from any mechanism which can affect the correct operation of more than one system/subsystem/ equipment as a result of random failures

3.43
individual risk
a 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 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.

3.44
infrastructure manager