SLOVENSKI STANDARD
oSIST prEN 50126-4:2013

01-januar-2013

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 4. del: Funkcionalna varnost - Električno/Elektronsko/Programabilni elektronski sistemi

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 4: Functional Safety - Electrical/Electronic/Programmable electronic systems

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 4: Funktionale Sicherheit - Elektrische/Elektronische/Programmierbare elektronische Systeme

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 4: Sécurité fonctionnelle - Systèmes électriques/électroniques/électroniques programmables

Ta slovenski standard je istoveten z: **prEN 50126-4:2012**

ICS:

35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50126-4:2013 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50126-4

October 2012

ICS

Will supersede EN 50129:2003

English version

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 4: Functional Safety - Electrical/Electronic/Programmable electronic systems

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 4: Sécurité fonctionnelle - Systèmes électriques/électroniques/électroniques programmables

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 4: Funktionale Sicherheit - Elektrische/Elektronische/Programmierbare elektronische Systeme

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

Contents

Page

7155

7156

Foreword

This document [prEN 50126-4:2012] 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 functional safety for E/E/PE. It is mainly based on EN 50129:2003.

This part of EN 50126 will supersede EN 50129:2003.

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).

Modifications intended to be made, mainly for part4 and 5

WG14 intended to incorporate the following modifications prior to the CENELEC-Enquiry. Due to TC9X resolution 46/11 their incorporation must be postponed to post enquiry.

Therefore, for information purposes the list is included here. The list should not preclude commenting on these issues, but should inform the reader regarding the intended direction of further changes.

The order of the points does not indicate their importance.

1	The activity-based approach from parts 1+2 will be further implemented in parts 4+5. The relationship between "activities" and "roles" will be improved.
2	With regard to verification requirements, the approach from parts 1+2 will be used for parts 4+5 as well.
3	Safety case documentation: remaining inconsistencies within part 1 and between part 1 and parts 4/5 will be rectified.
4	E/E/PE System/Software Assurance: Chapter 7 of parts 4/5 will be removed and the essence of the content moved to part 1.
5	Improve the consistency between part 4 chapter 8 and part1.
6	SIL0: the requirements will be reduced.
7	Improve consistency between part 1 and part 4 with regard to operation and maintenance.
8	Tailoring: the main text will better reflect the adaptability of the process according to the respective SIL.
9	Alignment of terms & definitions will be finalised.
10	Consistent use of terms & definitions will be improved.
11	The HW process defined in part 4 (e.g. in chapter9 and the annexes) will be revised and the same activity based approach as outlined in issues1 of this table will be applied.

7173

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 50128:2011 and EN 50129:2003 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 evaluated.

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 the EN 50126 standard 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 9000 series of International standards.

1 Scope

This part of EN 50126

- is intended to apply to all safety-related electronic (E/E/PE) railway systems/sub-system/hardware. However, the hazard analysis and risk assessment processes defined in EN 50126-1 and in this part are necessary for all railway systems/sub-systems/hardware, in order to identify any safety requirements. The relevant methods are provided by EN 50126-2. If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety-related), and provided the conclusion is not revised as a consequence of later changes, this part of EN 50126 ceases to be applicable;
- is applicable to safety-related electronic systems (including sub-systems and hardware) for railway applications;
- is primarily applicable to systems/sub-systems/hardware which have been specifically designed and manufactured for railway applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial hardware (e.g.: power supplies, modems, etc.), which is procured for use as part of a safety-related railway system. As a minimum, evidence shall be provided in such cases to demonstrate:
  - either that the hardware is not relied on for safety,
  - or that the hardware can be relied on for those functions which relate to safety;
- applies
  - to the specification, architecture, design, construction, implementation, integration, manufacturing, installation, acceptance, operation, maintenance and modification/extension phases of the system /subsystem and hardware, and also to individual sub-systems and hardware within the overall system as determined by the process in EN 50126-1 and supported by the methods in EN 50126-2.
  - to generic sub-systems and hardware (both application-independent and those intended for a particular class of application), and also to systems/sub-systems/hardware for specific applications;
- addresses railway specifics;
- 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 of EN 50126 is applicable

- to the specification and demonstration of safety 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 hardware 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;
  - for 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, railway suppliers, assessors and safety authorities.

Application of EN 50126-4 follows from SIL allocation to system/subsystem/hardware through applying the processes described in EN50126-1 and methods described by EN 50126-2. Given the relative maturity of most electrical systems, this part of EN 50126 is largely applicable to Electronic and Programmable Electronic sub-systems, systems and hardware.

NOTE Guidance on the applicability is given in the requirements of this standard.

Existing systems compliant with any version of former EN 50126, EN 50128 or EN 50129 shall not be subject of reconsideration and are considered as compliant with this standard.

Railway applications mean Command, Control & Signalling, Rolling Stock and Fixed Installations for Railways (e.g. Electric Power Supply).

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.

prEN 50126-1:2012, *Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process*

EN 50121 (all parts), *Railway applications – Electromagnetic compatibility*

EN 50124 (all parts), *Railway applications – Insulation coordination*

EN 50125 (all parts), *Railway applications – Environmental conditions for equipment*

EN 50155, *Railway applications – Electronic equipment used on rolling stock*

EN 50159, *Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems*

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 terms and definitions given in prEN 50126-1:2012 and the following apply:

3.1
change control board
entity that supervises and authorises change throughout the life cycle

3.2
hardware component
hardware component is a constituent part of a sub-system which has well-defined interfaces and behaviour with respect to the system/sub-system architecture and design and fulfils the following criteria:

a) an electrical/electronic component or assembly delivering a specific function;
b) it covers a specific subset of sub-system requirements;
c) it is clearly identified and has an independent version inside the configuration management system or is a part of a collection of components (e. g. subsystems) which have an independent version

3.3
maintenance manager
entity responsible for implementation and upkeep of maintenance procedures and standards ensuring safe and reliable performance of the system.

3.4
release note
documented record of all application and maintenance conditions for safe operation, across life cycle phases

3.5
safety manager
entity that is responsible for the correct accomplishment of the safety management

4 Abbreviations

For the purposes of this document, the following abbreviations apply.

4.1	**ASR:**	**assessor**
4.2	**BPA:**	**Bent Pin Analysis**
4.3	**CA:**	**Contingency Analysis**
4.4	**CCD:**	**Cause Consequence Diagrams**
4.5	**CCF:**	**Common Cause Failures**
4.6	**CCFA:**	**Common Cause Failure Analysis**
4.7	**CFMA:**	**Cable Failure Matrix Analysis**
4.8	**CID:**	**Class Diagram**
4.9	**CoD:**	**Component Diagram**
4.10	**COTSH**	**Commercial off the Shelf Hardware**
4.11	**CPLD :**	**Complex Programmable Logic Device**
4.12	**CPU:**	**Central Processing Unit**
4.13	**CT:**	**Certified Tool / Certified Translator**
4.14	**DA:**	**Design Analysis**
4.15	**DC:**	**Direct Current**
4.16	**DES:**	**Designer**
4.17	**DIA:**	**Design Interface Analysis**
4.18	**DRC:**	**Design Rule Check**
4.19	**DSL:**	**Domain Specific Language**
4.20	**EAM:**	**Error Avoiding Method**
4.21	**EPLD :**	**Erasable Programmable Logic Device**
4.22	**ESD:**	**Electrostatic Discharge**
4.23	**ETA:**	**Event Tree Analysis**
4.24	**ETBA:**	**Energy Trace and Barrier Analysis**
4.25	**FET:**	**Transistors-Field Effect**
4.26	**FI:**	**Fagan Inspection**
4.27	**FPGA:**	**Field-programmable Gate Array**
4.28	**FT:**	**Fault Tree**
4.29	**GD:**	**Graceful Degradation**

4.30 HAZOP: Hazard and Operability Study

4.31 HOL: Higher Order Logic

4.32 HW: Hardware

4.33 IC: Integrated Circuit

4.34 ID: Identifier

4.35 IMP: implementer

4.36 INT: integrator

4.37 LCA: Logic Cell Array

4.38 LED: Light-emitting Diode

4.39 LRU: Line Replaceable Unit

4.40 MBT: Model Based Testing

4.41 MCS: Monte-Carlo Simulation

4.42 O&SHA: Operating and Support Hazard Analysis

4.43 ORR: Operational Readiness Review

4.44 PAL: Programmable Array Logic

4.45 PD: Programmable Device

4.46 PDH Previously Developed Hardware

4.47 PHA: Preliminary Hazard Analysis

4.48 PHL: Preliminary Hazard List

4.49 PJM: project manager

4.50 PLA: Programmable Logic Array

4.51 PLD : Programmable Logic Device

4.52 RBD: Reliability Block Diagram

4.53 RCA: Root Cause Analysis

4.54 RPN: Risk Priority Number

4.55 RQM: requirements manager

4.56 SB: Safety Bag

4.57 SCA: Sneak Circuit Analysis

4.58 SCD: State Chart Diagram

4.59 SCR: Silicon-controlled Rectifier

4.60 SeD: Sequence Diagram

4.61 SoPC: System on Programmable Chip

4.62 SRAC: Safety Related Application Conditions

4.63 SSA: System Safety Analysis

4.64 STA: Static Timing Analysis

4.65 SW: Software

4.66 TL: Temporal Logic

4.67 TO: Test Oracle

4.68 TPN: Time Petri Nets

4.69 TST: tester

4.70 UML: Unified Modelling Language

4.71 VAL: validator

4.72 VDR: Voltage-dependent Resistor

4.73 VER: verifier

4.74 VHDL: Verilog Hardware Description Language

4.75 WDR: Walkthrough / Design Review

5 Overall Framework of the Part 4

This part of the EN 50126 suite of standards addresses the application of the safety life cycle to electronic hardware and integrated systems comprising electrical, electronic and programmable electronic hardware and software. The principal purpose of this suite of standards is to support the design, development, production and operation of acceptably safe products, systems and processes aimed at railway applications. In this spirit, the approval, acceptance or certification constitute a secondary potential benefit arising from compliance with this suite of standards. EN 50126-4 and EN 50126-5 of the standard suite address technology specific safety requirements and are complementary to the requirements and the framework developed in EN 50126-1 and EN 50126-2 which shall also be complied with. The standard addresses the management, organisation and overall electronic systems assurance including the safety requirements applicable to generic and configurable hardware. The system aspects of electronic system development are also addressed together with the requirements for manufacturing, deployment, operation and maintenance.

The overall scope of this standard includes electrical, electronic and programmable electronic hardware with fixed embedded logic, configurable hardware, integrated electronic systems comprising hardware and software and electronic sub-systems with fixed or configurable logic.

A part from hardware, sub-systems and integrated systems, this standard places requirements for management, organisation and the competency of the people who assume various roles in the safety life cycle of electronic hardware and systems. This is in recognition of the major impact of the organisational and competency aspects on the overall reduction of the systematic errors which are otherwise likely to remain embedded in the design and production of electronic hardware and systems.

The overall structure of this standard addresses key safety life cycle requirements in the design, development, deployment and maintenance of electrical, electronic and programmable electronic systems and hardware. Where appropriate, the structure in this standard is aligned with the software standard in EN 50126-5 to provide a familiar and systematic approach across the related disciplines.

Clauses 6 and 7 of this standard set out the common requirements for life cycle phases defined in Clauses 8-11. The chapters are structured to state the objectives, inputs, requirements and the outputs pertinent to each phase of the life cycle.