SLOVENSKI STANDARD
oSIST prEN 50126-5:2013

01-januar-2013

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 5. del: Funkcinalna varnost - Programska oprema

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 5: Functional Safety - Software

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) -- Teil 5: Funktionale Sicherheit - Software

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 5: Sécurité fonctionnelle - Logiciel

Ta slovenski standard je istoveten z: **prEN 50126-5:2012**

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 50126-5:2013 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50126-5

October 2012

ICS 29.280; 45.020

Will supersede EN 50128:2011

English version

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 5: Functional Safety - Software

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 5: Sécurité fonctionnelle - Logiciel

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 5: Funktionale Sicherheit - Software

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: 21755

Ref. No. prEN 50126-5:2012 E

13001 # Contents

13001 Page

13047 **Figures**

13054 **Tables**

13091

13092 # Foreword

13093 This document [prEN 50126-5:2012] has been prepared by CLC/TC 9X "Electrical and electronic
13094 applications for railways".

13095 This document is currently submitted to the Enquiry.

13096 EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability,*
13097 *Maintainability and Safety (RAMS)*" consists of the following parts:

13098 – Part 1: Generic RAMS process;

13099 – Part 2: Systems approach to safety;

13100 – Part 4: Functional safety – Electrical/Electronic/Programmable electronic systems;

13101 – Part 5: Functional safety – Software.

13102 This new edition of EN 50126 (all parts) will supersede EN 50126-1:1999, CLC/TR 50126-2:2007,
13103 CLC/TR 50126-3:2008, EN 50128:2011 and EN 50129:2003.

13104 This part of EN 50126 will supersede EN 50128:2011.

13105 This document has been prepared under a mandate given to CENELEC by the European Commission
13106 and the European Free Trade Association, and supports essential requirements of EU Directive(s).

13107 This European Standard supports the European Railway Directive 2004/49/EC (Railway Safety Directive)
13108 and the Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety
13109 method on risk evaluation and independent assessment as referred to in Article 6(3)(a) of Directive
13110 2004/49/EC of the European Parliament and of the Council.

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.

13111

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 European Standards and the experiences gained over the recent 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 Fixed Installations.

The revision work improved the coherence and consistency of the European 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.

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/EP technology of railway applications and their application depends on 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 European Standard shall 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 independent 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 interoperability.

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 European Standard is consistent with the application of quality management requirements contained within the ISO 9000 series of International standards.

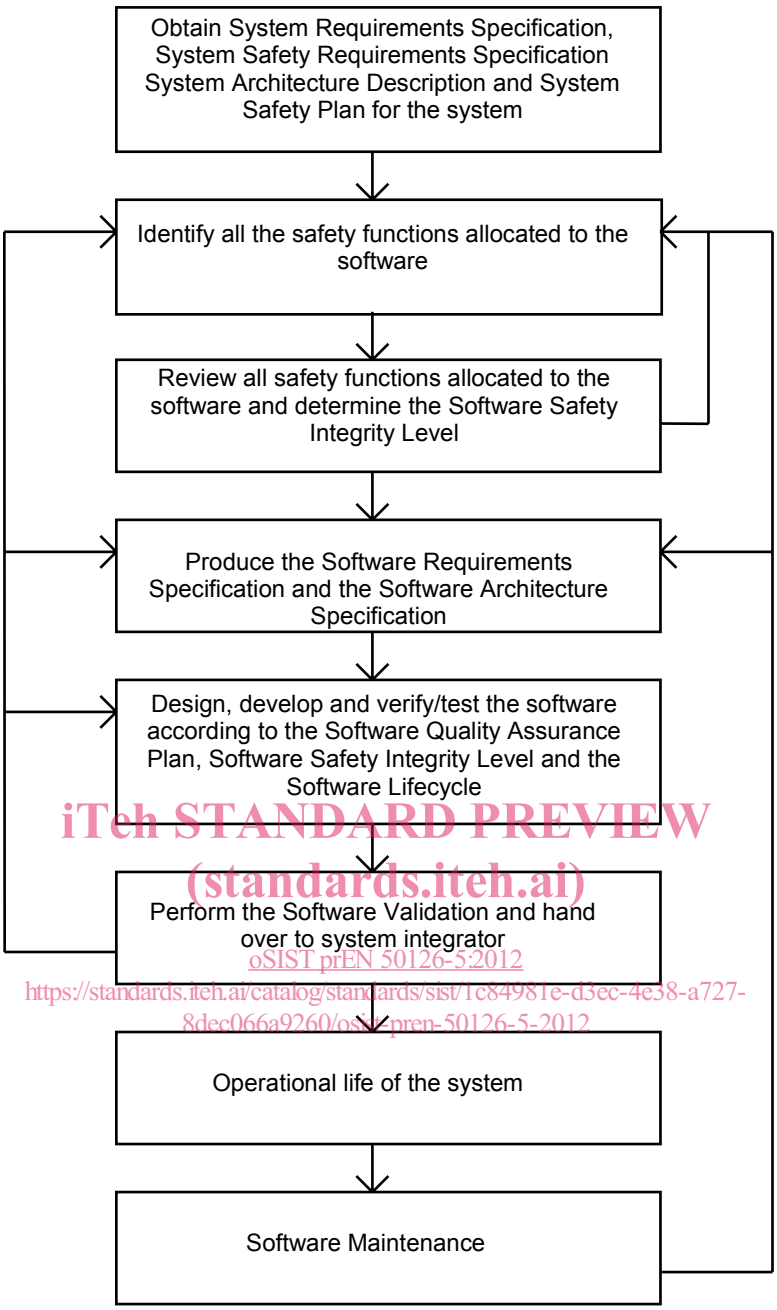
With the term document this European Standard rather means technical contents and not necessarily single physical documents. Such technical contents can arbitrarily be combined to physical documents dependent on the needs of the specific project. Technical contents can also be omitted in the process-tailoring step which should take place in the early planning phase of a project. The omission of technical

13159 contents has however to be justified with technical arguments. The tailoring process is best documented
13160 in a Project Document List, declaring which documents with which technical contents are planned to be
13161 created, by whom and in which phase of the project. Omitted technical contents should be highlighted
13162 and the omission justified.

13163 The current state-of-the-art is such that neither the application of quality assurance methods (so-called
13164 fault avoiding measures and fault detecting measures) nor the application of software fault tolerant
13165 approaches can guarantee the absolute safety of the software. The proof of the absence of faults, in
13166 reasonably complex safety-related software, especially the absence of specification and design faults is
13167 currently a formidable if not unattainable task. Adopting a systematic principled process and employing
13168 competent resources constitute current best practice in software development. The principles applied in
13169 developing high integrity software include, but are not restricted to

13170 – top-down design methods,
13171 – modularity,
13172 – verification of each phase of the development lifecycle,
13173 – verified components and component libraries,
13174 – clear documentation and traceability,
13175 – auditable documents,
13176 – validation,
13177 – assessment,
13178 – configuration management and change control and
13179 – appropriate consideration of organisation and personnel competency issues.

13180 This European Standard does not mandate the use of a particular software development lifecycle.
13181 However, illustrative lifecycle and documentation sets are given in 6.3, Figure 3 and Figure 4 and in 8.1.



13182

13183 **Figure 1 – Illustrative Software Route Map**

13184 # 1 Scope

13185 This part of EN 50126

13186 • is intended to apply to all safety-related software aimed at electronic railway systems/sub-system.
13187 The relevant methods are provided by EN 50126-2. If analysis reveals that no safety requirements
13188 exist (i.e. the situation is non-safety-related), and provided the conclusion is not revised as a
13189 consequence of later changes, this part of EN 50126 ceases to be applicable;

13190 • specifies the process and technical requirements for the development of software for programmable
13191 electronic systems for use in railway monitoring, control and protection applications. These systems
13192 can be implemented using dedicated microprocessors, programmable logic controllers,
13193 multiprocessor distributed systems, larger scale central processor systems or other architectures.

13194 • is applicable exclusively to software and the interaction between software and the system/sub-
13195 system of which it is part.

13196 This European Standard

13197 • is primarily applicable to software which have been specifically designed and developed for railway
13198 applications. It should also be applied, as far as reasonably practicable, to general-purpose or
13199 industrial software which is procured for use as part of a safety-related railway system. As a
13200 minimum, evidence shall be provided in such cases to demonstrate:

13201 - either that the software is not relied on for safety,

13202 - or that the software can be relied on for those functions which relate to safety;

13203 • applies

13204 - to the specification, architecture, design, development, implementation, integration, installation,
13205 acceptance, deployment, operation, maintenance and modification/extension phases of the
13206 software in a system /subsystem. It also applies to individual sub-systems within the overall
13207 system as determined by the process in EN 50126-1 and supported by the methods in
13208 EN 50126-2,

13209 - to generic sub-systems (both application-independent and those intended for a particular class of
13210 application), and also to systems/sub-systems for specific applications;

13211 • does not define

13212 - RAMS targets, quantities, requirements or solutions for specific railway applications

13213 - rules or processes pertaining to the certification of railway products against the requirements of
13214 this European Standard

13215 - an approval process by the safety authority;

13216 • does not specify requirements for ensuring system security.

13217 This part EN 50126 is applicable

13218 • to the specification and demonstration of safety for all software in railway applications and at all
13219 levels of such an application, as appropriate, from complete railway systems to major systems and to
13220 individual and combined sub-systems within these major systems; in particular:

13221 - to new systems;

13222 - to new systems integrated into existing systems in operation prior to the creation of this European
13223 Standard, although it is not generally applicable to other aspects of the existing system;

13224 - for modifications of existing software on systems in operation prior to the creation of this
13225 European Standard, although it is not generally applicable to other aspects of the existing system.

- at all relevant phases of the lifecycle of an application;
- for use by railway duty holders, railway suppliers, assessors and safety authorities;

- to all safety related software used in railway control and protection systems, including
  1. application programming,
  2. operating systems,
  3. support tools,
  4. firmware.

Application programming comprises high level programming, low level programming and special purpose programming (for example: Programmable logic controller ladder logic).

- not relevant for software that has been identified as having no impact on safety, i.e. software of which failures cannot affect any identified safety functions.

This European Standard also addresses the use of pre-existing software and tools. Such software may be used, if the specific requirements in 7.6.4.12 and 8.3.4.1.6 on pre-existing software and for tools in 7.9 are fulfilled.

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 European Standard.

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

Application of EN 50126-5 builds on the results in applying the methods described by EN 50126-2.

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

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.

EN 50126-1:1999 + corr. May. 2006 + corr. May. 2010, *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process*

EN 50129:2003 + corr. May. 2010, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

EN ISO 9000, *Quality management systems – Fundamentals and vocabulary (ISO 9000)*

EN ISO 9001, *Quality management systems – Requirements (ISO 9001)*

ISO/IEC 90003:2004, *Software engineering – Guidelines for the application of ISO 9001:2000 to computer software*

ISO/IEC 9126 (all parts), *Software engineering – Product quality*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50126-1:1999 and the following apply.

3.1
independent assessment
process of analysis to determine whether software, which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements and to form a judgement as to whether the software is fit for its intended purpose. Safety assessment is an independent assessment focused on but not limited to the safety properties of a system

3.2
component
constituent part of software, which has well-defined interfaces and behaviour with respect to the software architecture and design and fulfils the following criteria:

– it is designed according to “Components” (see Table A.20);
– it covers a specific subset of software requirements;
– 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
configuration manager
entity that is responsible for implementing and carrying out the processes for the configuration management of documents, software and related tools including change management

3.4
customer
entity which purchases a railway control and protection system including the software

3.5
programmable logic controller
solid-state control system which has a user programmable memory for storage of instructions to implement specific functions

3.6
robustness
ability of an item to detect and handle abnormal situations

3.7
supplier
entity that designs and builds a railway control and protection system including the software or parts thereof

3.8
system safety integrity level
classification number which indicates the required degree of confidence that an integrated system comprising hardware and software will meet its specified safety requirements

4 Abbreviations

For the purposes of this document, the abbreviations given in EN 50126-1:1999 and below apply.

ASR	Assessor
COTS	Commercial off-the-shelf
DES	Designer
HR	Highly Recommended
IMP	Implementer
INT	Integrator

13307	JSD	Jackson System Development Method
13308	M	Mandatory
13309	MASCOT	Modular Approach to Software Construction, Operation and Test
13310	MBSA	Model Based Safety Assessment/Assurance
13311	NR	Not Recommended
13312	PM	Project Manager
13313	R	Recommended
13314	RQM	Requirements Manager
13315	SDL	Specification and Description Language
13316	SFC	Sequential Function Charts
13317	SOM	Service Oriented Modelling
13318	SSADM	Structured Systems Analysis & Design Methodology
13319	TST	Tester
13320	V&V	Verification and Validation
13321	VAL	Validator
13322	VER	Verifier

13323 5 Overall framework of EN 50126-5

13324 This part of the EN 50126 suite of European Standards addresses the application of the safety life cycle
13325 to the development of software for incorporation in electronic hardware and integrated systems
13326 comprising electrical, electronic and programmable electronic hardware. The principal purpose of this
13327 suite of European Standards is to support the design, development, production and operation of
13328 acceptably safe products, systems and processes aimed at railway applications. In this spirit, the
13329 approval, acceptance or certification constitute a secondary potential benefit arising from compliance with
13330 this suite of European Standards. EN 50126-4 and EN 50126-5 of the European Standard suite address
13331 technology specific safety requirements and are complementary to the requirements and the framework
13332 developed in EN 50126-1 and EN 50126-2 which shall also be complied with. This European Standard
13333 addresses the management, organisation and overall assurance of software aimed at electronic systems
13334 including the safety requirements applicable to generic and algorithmic software.

13335 The overall scope of this European Standard includes software developed for incorporation in electronic
13336 and programmable electronic hardware systems with fixed or configurable logic.

13337 Apart from software, this European Standard places requirements for management, organisation and the
13338 competency of the people who assume various roles in the safety life cycle of software. This is in
13339 recognition of the major impact of the organisational and competency aspects on the overall reduction of
13340 the systematic errors which are otherwise likely to remain embedded in the design and production of
13341 software.

13342 The overall structure of this European Standard addresses key safety life cycle requirements in the
13343 design, development, deployment and maintenance of software for electronic and programmable
13344 electronic systems. Where appropriate, the structure in this European Standard is aligned with the
13345 hardware and system standard in EN 50126-4 to provide a familiar and systematic approach across the
13346 related disciplines.

13347 Clauses 6 and 7 of this European Standard set out the common requirements for life cycle phases
13348 defined in Clauses 8-10. These clauses are structured to state the objectives, inputs, requirements and
13349 the outputs pertinent to each phase of the life-cycle.

13350 Clause 6 sets out the generic management and organisational requirements, pertinent to software for
13351 electronic systems, addressing documentation, roles, requisite competencies, responsibilities of key
13352 personnel and the required independence between the roles.

Clause 7 sets out the generic software assurance requirements addressing quality management, safety management, configuration and change management and support tools.

Clause 8 sets out the requirements for the development of generic software addressing architecture, design, implementation, integration, installation and commissioning and validation. It additionally provides requirements and guidelines for development of Software Safety Cases.

Clause 9 sets out the requirements for the development of software systems configured by application data or algorithm addressing architecture, design, implementation, integration, testing, installation and commissioning and validation. Many of the requirements of the generic software are equally applicable to configurable variants.

Clause 10 sets out the requirements for a systematic approach to the safe deployment, operation and maintenance of safety related software in railways. It details the requisite processes that have to be implemented to ensure safe software is safely put into use and safely maintained throughout its operational life.

The annexes to this European Standard provide normative and informative requirements and guidance considered supplementary to the main sections of this European Standard. These comprise guidance on selection of techniques and measures, key safety roles and competencies for development of software, multi-core programming, guidance on the structure of Software Safety Cases and an updated generic bibliography of the software and system design and development techniques.

6 Software Management and Organisation

6.1 Organisation, Roles and Responsibilities

6.1.1 Objective

6.1.1.1 To ensure that all personnel who have responsibilities for the software are organised, empowered and capable of fulfilling their responsibilities.

6.1.2 Requirements

6.1.2.1 As a minimum, the supplier shall implement EN ISO 9001, Clauses 4 and 5, dealing with the organisation and management of the personnel and responsibilities.

6.1.2.2 Responsibilities shall be compliant with the requirements defined in Annex B and assessed.

6.1.2.3 The personnel assigned to the roles involved in the development or maintenance of the software shall be recorded in the Quality Managenent Report or in another document referenced by the Quality Managenent Report.

6.1.2.4 An Assessor shall be appointed by the supplier, the customer or the Safety Authority.

6.1.2.5 The assessor may be part or not of the supplier organization, but shall be in any case independent from the project organizations (Design, Testing, Integration, Safety, Verification and Validation). National legislation / Safety Authority may ask for additional independence requirements.

NOTE The independent assessment body may be identified by national legislation.

6.1.2.6 The Assessor shall be given authority to perform the independent assessment of the software.

6.1.2.7 The Validator shall give agreement/disagreement for the software release.

6.1.2.8 Throughout the software lifecycle, the parties involved shall be independent, in accordance with 6.1.2.9 to 6.1.2.13, to the extent required by software SIL.