

**RAUDTEEALASED RAKENDUSED. SIDE-,
SIGNALISATSIOONI- JA ANDMETÖÖTLUSSÜSTEEMID.
RAUDTEE JUHTIMIS- JA TURVANGUSÜSTEEMIDE
TARKVARA**

**Railway applications - Communication, signalling and
processing systems - Software for railway control and
protection systems**

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

See Eesti standard EVS-EN 50128:2011+A1:2020 sisaldab Euroopa standardi EN 50128:2011 ingliskeelset teksti ja selle paranduse AC:2014 ja muudatuse A1:2020 ingliskeelset teksti.	This Estonian standard EVS-EN 50128:2011+A1:2020 consists of the English text of the European standard EN 50128:2011 and its corrigendum AC:2014 and amendment A1:2020.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas. Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 17.06.2011, muudatus A1 07.02.2020.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation. Date of Availability of the European standard is 17.06.2011, for A1 07.02.2020.
Parandusega AC lisatud või muudetud tekst on tähistatud püst-kriipsuga lehe välisveerisel. Sellesse standardisse on muudatus A1 sisse viidud ja tehtud muudatused tähistatud kahekordse püstkriipsuga lehe välisveerisel. Muudatusega A2 lisatud või muudetud teksti algus ja lõpp on tekstis ära märgitud märgenditega A2 A2 . Standard on kättesaadav Eesti Standardikeskusest.	The start and finish of text introduced or altered by amendment AC is marked by a vertical line on the outer row of the page. The amendment A1 has been incorporated into this standard and changes have been marked by a double vertical line on the outer row of the page. The start and finish of text introduced or altered by amendment A2 is indicated in the text by symbols A2 A2 . The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.240.60; 45.020; 93.100

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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 European Standard was approved by CENELEC on 2011-04-25. Amendment A1 was approved by CENELEC on 2019-07-23. Amendment A2 was approved by CENELEC on 2020-06-22. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European standard and its amendments 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 and its amendments A1 and A2 exist 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

Contents

Foreword	6
Amendment A1 European foreword	7
Amendment A2 European foreword	7
Introduction	8
1 Scope	11
2 Normative references	12
3 Terms, definitions and abbreviations	12
3.1 Terms and definitions	12
3.2 Abbreviations	17
4 Objectives, conformance and software safety integrity levels	18
5 Software management and organisation	19
5.1 Organisation, roles and responsibilities	19
5.2 Personnel competence	22
5.3 Lifecycle issues and documentation	23
6 Software assurance	25
6.1 Software testing	25
6.2 Software verification	27
6.3 Software validation	28
6.4 Software assessment	30
6.5 Software quality assurance	32
6.6 Modification and change control	34
6.7 Support tools and languages	35
7 Generic software development	38
7.1 Lifecycle and documentation for generic software	38
7.2 Software requirements	38
7.3 Architecture and Design	41
7.4 Component design	47
7.5 Component implementation and testing	49
7.6 Integration	50
7.7 Overall Software Testing / Final Validation	52
8 Development of application data or algorithms: systems configured by application data or algorithms	54
8.1 Objectives	54
8.2 Input documents	55
8.3 Output documents	55
8.4 Requirements	55
9 Software deployment and maintenance	60
9.1 Software deployment	60
9.2 Software maintenance	62

Annex A (normative) Criteria for the Selection of Techniques and Measures	65
A.1 Clauses tables	66
A.2 Detailed tables	74
Annex B (normative) Key software roles and responsibilities	80
Annex C (informative) Documents Control Summary	89
Annex D (informative) Bibliography of techniques	91
D.1 Artificial Intelligence Fault Correction	91
D.2 Analysable Programs.....	91
D.3 Avalanche/Stress Testing	91
D.4 Boundary Value Analysis.....	92
D.5 Backward Recovery	92
D.6 Cause Consequence Diagrams.....	93
D.7 Checklists.....	93
D.8 Control Flow Analysis	94
D.9 Common Cause Failure Analysis	94
D.10 Data Flow Analysis	94
D.11 Data Flow Diagrams	95
D.12 Data Recording and Analysis	95
D.13 Decision Tables (Truth Tables).....	96
D.14 Defensive Programming	96
D.15 Coding Standards and Style Guide	97
D.16 Diverse Programming	98
D.17 Dynamic Reconfiguration.....	98
D.18 Equivalence Classes and Input Partition Testing	99
D.19 Error Detecting and Correcting Codes	99
D.20 Error Guessing.....	99
D.21 Error Seeding.....	100
D.22 Event Tree Analysis.....	100
D.23 Fagan Inspections	100
D.24 Failure Assertion Programming	101
D.25 SEEA – Software Error Effect Analysis	101
D.26 Fault Detection and Diagnosis.....	102
D.27 Finite State Machines/State Transition Diagrams	102
D.28 Formal Methods	103
D.29 Formal Proof	108
D.30 Forward Recovery	108
D.31 Graceful Degradation.....	109
D.32 Impact Analysis.....	109
D.33 Information Hiding / Encapsulation	109
D.34 Interface Testing	110
D.35 Language Subset.....	110
D.36 Memorising Executed Cases	110
D.37 Metrics	111
D.38 Modular Approach	111
D.39 Performance Modelling.....	112

D.40 Performance Requirements.....	112
D.41 Probabilistic Testing.....	113
D.42 Process Simulation	113
D.43 Prototyping / Animation.....	114
D.44 Recovery Block.....	114
D.45 Response Timing and Memory Constraints	114
D.46 Re-Try Fault Recovery Mechanisms	115
D.47 Safety Bag	115
D.48 Software Configuration Management	115
D.49 Strongly Typed Programming Languages	115
D.50 Structure Based Testing	116
D.51 Structure Diagrams.....	116
D.52 Structured Methodology.....	117
D.53 Structured Programming.....	117
D.54 Suitable Programming languages	118
D.55 Time Petri Nets	119
D.56 Walkthroughs / Design Reviews.....	119
D.57 Object Oriented Programming.....	119
D.58 Traceability.....	120
D.59 Metaprogramming.....	121
D.60 Procedural programming	121
D.61 Sequential Function Charts	121
D.62 Ladder Diagram	121
D.63 Functional Block Diagram.....	122
D.64 State Chart or State Diagram	122
D.65 Data modelling.....	122
D.66 Control Flow Diagram/Control Flow Graph.....	122
D.67 Sequence diagram.....	124
D.68 Tabular Specification Methods	124
D.69 Application specific language	124
D.70 UML (Unified Modeling Language).....	125
D.71 Domain specific languages.....	125

Annex ZZ (informative) Relationship between this European standard and the essential requirements of EU Directive 2016/797/EU [2016 OJ L138] aimed to be covered.....	127
--	------------

Bibliography.....	128
--------------------------	------------

Figures

Figure 1 – Illustrative Software Route Map	10
Figure 2 – Illustration of the preferred organisational structure.....	20
Figure 3 – Illustrative Development Lifecycle 1	24
Figure 4 – Illustrative Development Lifecycle 2	25

Tables

Table 1 - Relation between tool class and applicable sub-clauses	38
A2 Table A.1 – Lifecycle Issues and Documentation (5.3).....	66
Table A.2 – Software Requirements Specification (7.2).....	68
Table A.3 – Software Architecture (7.3)	69
A2 Table A.4 – Software Design and Implementation (7.3, 7.4, and 7.5) A2	70
A2 Table A.5 – Verification and Testing (6.2 and 7.4) A2	71
A2 Table A.6 – Integration (7.3 and 7.6) A2	71
A2 Table A.7 – Overall Software Testing (6.2 and 7.2) A2	72
Table A.8 – Software Analysis Techniques (6.3)	72
Table A.9 – Software Quality Assurance (6.5)	73
Table A.10 – Software Maintenance (9.2)	73
Table A.11 – Data Preparation Techniques (8.4)	73
Table A.12 – Coding Standards	74
Table A.13 – Dynamic Analysis and Testing	74
Table A.14 – Functional/Black Box Test.....	75
Table A.15 – Textual Programming Languages	75
Table A.16 – Diagrammatic Languages for Application Algorithms	76
Table A.17 – Modelling	76
Table A.18 – Performance Testing	76
Table A.19 – Static Analysis	77
Table A.20 – Components	77
Table A.21 – Test Coverage for Code	78
Table A.22 – Object Oriented Software Architecture	79
Table A.23 – Object Oriented Detailed Design	79
Table B.1 – Requirements Manager Role Specification.....	80
Table B.2 – Designer Role Specification	81
Table B.3 – Implementer Role Specification	82
Table B.4 – Tester Role Specification	83
Table B.5 – Verifier Role Specification	84
Table B.6 – Integrator Role Specification	85
Table B.7 – Validator Role Specification	86
Table B.8 – Assessor Role Specification.....	87
Table B.9 – Project Manager Role Specification	88
Table B.10 – Configuration Manager Role Specification.....	88
Table C.1 – Documents Control Summary	89
Table ZZ.1 - Correspondence between this European Standard, the TSI “Control-Command and Signalling” (REGULATION (EU) No 2016/919 of 27 May 2016) and Directive 2016/797/EU [2016 OJ L138]	127

Foreword

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways. .

It was submitted to the Formal Vote and was approved by CENELEC as EN 50128 on 2011-04-25.

This document supersedes EN 50128:2001.

The main changes with respect to EN 50128:2001 are listed below:

- requirements on software management and organisation, definition of roles and competencies, deployment and maintenance have been added;
- a new clause on tools has been inserted, based on EN 61508-2:2010;
- tables in Annex A have been updated.

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

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2012-04-25 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2017-04-25 |

This European Standard should be read in conjunction with EN 50126-1:1999 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process*" and EN 50129:2003 "*Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*".

Amendment A1 European foreword

This document (EN 50128:2011/A1:2020) has been prepared by CLC/SC 9XA "Communication, signalling and processing systems".

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) 2020-08-07
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2020-08-07

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.

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.

A2 Amendment A2 European foreword

This document (EN 50128:2011/A2:2020) has been prepared by SC 9XA, "Communication, signalling and processing systems", of Technical Committee CENELEC 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) 2021-06-22
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2023-06-22

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*".

EE NOTE 1 The term "assessment" in the standard means "independent safety assessment" as per definition of EN 50126-1:2017, 3.33.

EE NOTE 2 All statements qualified by the words "software safety integrity level" are applicable also to Basic Integrity. **A2**

Introduction

This European Standard is part of a group of related standards. The others are **EN 50126-1** "Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process" and EN 50129:2003 "Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling".

EN 50126-1 and **EN 50126-2** addresses system issues on the widest scale, while EN 50129 addresses the approval process for individual systems which can exist within the overall railway control and protection system. This European Standard concentrates on the methods which need to be used in order to provide software which meets the demands for safety integrity which are placed upon it by these wider considerations.

This European Standard provides a set of requirements with which the development, deployment and maintenance of any safety-related software intended for railway control and protection applications shall comply. It defines requirements concerning organisational structure, the relationship between organisations and division of responsibility involved in the development, deployment and maintenance activities. Criteria for the qualification and expertise of personnel are also provided in this European Standard.

The key concept of this European Standard is that of levels of software safety integrity. This European Standard addresses five software safety integrity levels where **Basic Integrity** is the lowest and 4 the highest one. The higher the risk resulting from software failure, the higher the software safety integrity level will be.

This European Standard has identified techniques and measures for the five levels of software safety integrity. The required techniques and measures for software safety integrity levels **Basic Integrity** to 4 are shown in the normative tables of Annex A. In this version, the required techniques for level 1 are the same as for level 2, and the required techniques for level 3 are the same as for level 4. This European Standard does not give guidance on which level of software safety integrity is appropriate for a given risk. This decision will depend upon many factors including the nature of the application, the extent to which other systems carry out safety-related functions and social and economic factors.

It is within the scope of **EN 50126-1** and **EN 50126-2** and EN 50129 to define the process of specifying the safety-related functions allocated to software.

This European Standard specifies those measures necessary to achieve these requirements.

EN 50126-1 and **EN 50126-2** and EN 50129 require that a systematic approach be taken to

- a) identify hazards, assessing risks and arriving at decisions based on risk criteria,
- b) identify the necessary risk reduction to meet the risk acceptance criteria,
- c) define an overall System Safety Requirements Specification for the safeguards necessary to achieve the required risk reduction,
- d) select a suitable system architecture,
- e) plan, monitor and control the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety integrity.

As decomposition of the specification into a design comprising safety-related systems and components takes place, further allocation of safety integrity levels is performed. Ultimately this leads to the required software safety integrity levels.

The current state-of-the-art is such that neither the application of quality assurance methods (so-called fault avoiding measures and fault detecting measures) nor the application of software fault tolerant approaches can guarantee the absolute safety of the software. There is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults.

The principles applied in developing high integrity software include, but are not restricted to

- top-down design methods,
- modularity,
- verification of each phase of the development lifecycle,
- verified components and component libraries,
- clear documentation and traceability,
- auditable documents,
- validation,
- assessment,
- configuration management and change control and
- appropriate consideration of organisation and personnel competency issues.

The System Safety Requirements Specification identifies all **A2** safety-related functions **A2** allocated to software and determines their system safety integrity level. The successive functional steps in the application of this European Standard are shown in Figure 1 and are as follows:

- a) define the Software Requirements Specification and in parallel consider the software architecture. The software architecture is where the safety strategy is developed for the software and the software safety integrity level (7.2 and 7.3);
- b) design, develop and test the software according to the Software Quality Assurance Plan, software safety integrity level and the software lifecycle (7.4 and 7.5);
- c) integrate the software on the target hardware and verify functionality (7.6);
- d) accept and deploy the software (7.7 and 9.1);
- e) if software maintenance is required during operational life then re-activate this European Standard as appropriate (9.2).

A number of activities run across the software development. These include testing (6.1), verification (6.2), validation (6.3), assessment (6.4), quality assurance (6.5) and modification and change control (6.6).

Requirements are given for support tools (6.7) and for systems which are configured by application data or algorithms (Clause 8).

Requirements are also given for the independence of roles and the competence of staff involved in software development (5.1, 5.2 and Annex B).

This European Standard does not mandate the use of a particular software development lifecycle. However, illustrative lifecycle and documentation sets are given in 5.3, Figure 3 and Figure 4 and in 7.1.

Tables have been formulated ranking various techniques/measures against the software safety integrity levels 0-4. The tables are in Annex A. Cross-referenced to the tables is a bibliography giving a brief description of each technique/measure with references to further sources of information. The bibliography of techniques is in Annex D.

A2 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. **A2**

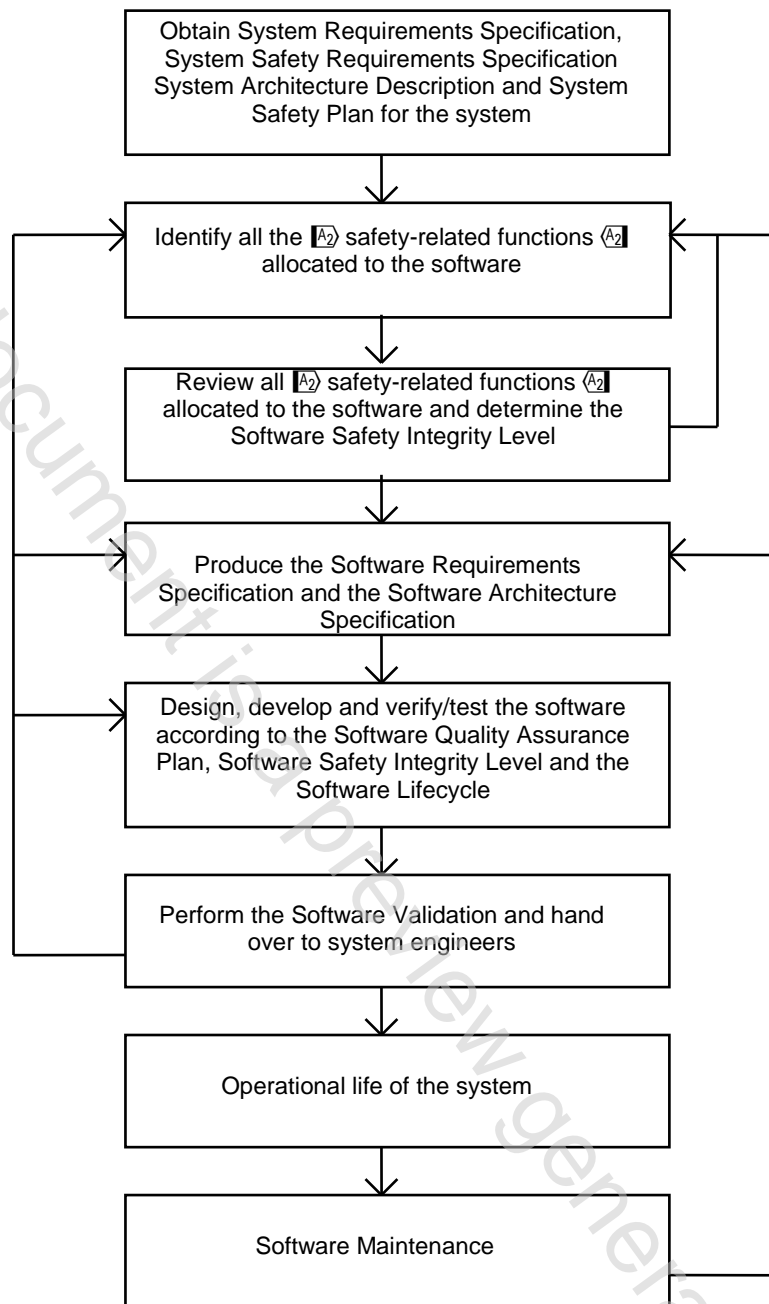


Figure 1 – Illustrative Software Route Map

1 Scope

1.1 This European Standard specifies the process and technical requirements for the development of software for programmable electronic systems for use in railway control and protection applications. It is aimed at use in any area where there are safety implications. These systems can be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.

1.2 This European Standard is applicable exclusively to software and the interaction between software and the system of which it is part.

1.3 This European Standard is not relevant for software that has been identified as having no impact on safety, i.e. software of which failures cannot affect any identified **A2** safety-related functions **A2**.

1.4 This European Standard applies to all safety related software used in railway control and protection systems, including

- application programming,
- operating systems,
- support tools,
- firmware.

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

1.5 This European Standard also addresses the use of pre-existing software and tools. Such software may be used, if the specific requirements in 7.3.4.7 and 6.5.4.16 on pre-existing software and for tools in 6.7 are fulfilled.

1.6 Software developed according to any version of this European Standard will be considered as compliant and not subject to the requirements on pre-existing software.

1.7 This European Standard considers that modern application design often makes use of generic software that is suitable as a basis for various applications. Such generic software is then configured by data, algorithms, or both, for producing the executable software for the application. The general Clauses 1 to 6 and 9 of this European Standard apply to generic software as well as for application data or algorithms. The specific Clause 7 applies only for generic software while Clause 8 provides the specific requirements for application data or algorithms.

1.8 This European Standard is not intended to address commercial issues. These should be addressed as an essential part of any contractual agreement. All the clauses of this European Standard will need careful consideration in any commercial situation.

1.9 This European Standard is not intended to be retrospective. It therefore applies primarily to new developments and only applies in its entirety to existing systems if these are subjected to major modifications. For minor changes, only 9.2 applies. The assessor has to analyse the evidences provided in the software documentation to confirm whether the determination of the nature and scope of software changes is adequate. However, application of this European Standard during upgrades and maintenance of existing software is highly recommended.

A2 1.10 For the development of User Programmable Integrated Circuits (e.g. FPGA and CPLD) guidance is provided in EN 50129:2018, Annex F. **A2**

2 Normative references

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

^{A2} 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

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

EN ISO 9000:2015, Quality management systems – Fundamentals and vocabulary

EN ISO 9001:2015, Quality management systems – Requirements

ISO/IEC 90003:2014, Software engineering – Guidelines for the application of ISO 9001 to computer software

ISO/IEC 25000 series, Systems and software engineering – Systems and software Quality Requirements and Evaluation ^{A2}

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1

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 focused on but not limited to the safety properties of a system

3.1.2

assessor

entity that carries out an assessment

3.1.3

commercial off-the-shelf (COTS) software

software defined by market-driven need, commercially available and whose fitness for purpose has been demonstrated by a broad spectrum of commercial users

3.1.4

component

a 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