

© Copyright SEK. Reproduction in any form without permission is prohibited.

Järnvägstillämpningar – Tillämpningar för rullande materiel – Programvaror på rullande materiel

*Railway applications –
Rolling stock applications –
Software on Board Rolling Stock*

Som svensk standard gäller europastandarden EN 50657:2017. Den svenska standarden innehåller den officiella engelska språkversionen av EN 50657:2017.

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

English Version

Railways Applications - Rolling stock applications - Software on Board Rolling Stock

Applications ferroviaires - Applications du matériel roulant -
Logiciels embarqués

Bahnanwendungen - Anwendungen für Schienenfahrzeuge
- Software auf Schienenfahrzeugen

This European Standard was approved by CENELEC on 2017-05-08. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

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

Contents

Page

European foreword.....	8
Introduction.....	9
1 Scope	12
2 Normative references	13
3 Terms, definitions and abbreviations	13
3.1 Terms and definitions	13
3.2 Abbreviations	19
4 Objectives, conformance and software integrity levels.....	20
5 Software management and organization.....	21
5.1 Organization, roles and responsibilities	21
5.1.1 Objective	21
5.1.2 Requirements.....	21
5.2 Personnel competence	25
5.2.1 Objectives	25
5.2.2 Requirements.....	25
5.3 Lifecycle issues and documentation	25
5.3.1 Objectives	25
5.3.2 Requirements.....	25
6 Software assurance	28
6.1 Software testing	28
6.1.1 Objective	28
6.1.2 Input documents	28
6.1.3 Output documents.....	28
6.1.4 Requirements.....	29
6.2 Software verification.....	29
6.2.1 Objective	29
6.2.2 Input documents	30
6.2.3 Output documents.....	30
6.2.4 Requirements.....	30
6.3 Software validation.....	31
6.3.1 Objective	31
6.3.2 Input documents	31
6.3.3 Output documents.....	31
6.3.4 Requirements.....	32
6.4 Software assessment	33
6.4.1 Objective	33
6.4.2 Input documents	33
6.4.3 Output documents.....	33
6.4.4 Requirements.....	33
6.5 Software quality assurance	35
6.5.1 Objectives	35
6.5.2 Input documents	35
6.5.3 Output documents.....	35
6.5.4 Requirements.....	35
6.6 Modification and change control	38

6.6.1	Objectives	38
6.6.2	Input documents	38
6.6.3	Output documents.....	38
6.6.4	Requirements.....	38
6.7	Support tools and languages	39
6.7.1	Objectives	39
6.7.2	Input documents	39
6.7.3	Output documents.....	39
6.7.4	Requirements.....	39
7	Software development.....	42
7.1	Lifecycle and documentation for software	42
7.1.1	Objectives	42
7.1.2	Requirements.....	42
7.2	Software requirements.....	42
7.2.1	Objectives	42
7.2.2	Input documents	42
7.2.3	Output documents.....	43
7.2.4	Requirements.....	43
7.3	Architecture and Design.....	45
7.3.1	Objectives	45
7.3.2	Input documents	45
7.3.3	Output documents.....	45
7.3.4	Requirements.....	46
7.4	Component design.....	52
7.4.1	Objectives	52
7.4.2	Input documents	52
7.4.3	Output documents.....	52
7.4.4	Requirements.....	52
7.5	Component implementation and testing	54
7.5.1	Objectives	54
7.5.2	Input documents	54
7.5.3	Output documents.....	54
7.5.4	Requirements.....	54
7.6	Integration	55
7.6.1	Objectives	55
7.6.2	Input documents	55
7.6.3	Output documents.....	55
7.6.4	Requirements.....	56
7.7	Overall Software Testing / Final Validation	57
7.7.1	Objectives	57
7.7.2	Input documents	57
7.7.3	Output documents.....	57
7.7.4	Requirements.....	58
7.8	Development of Software configured by application data.....	59
7.8.1	Objective	59
7.8.2	Requirements.....	59
8	Systems configured by application data: development of application data.....	60
8.1	Objectives	60
8.2	Input documents	60
8.3	Output documents	61
8.4	Requirements	61
8.4.1	Application Development Process	61
8.4.2	Application Requirements Specification.....	62

8.4.3	Architecture and Design.....	62
8.4.4	Application Data Production.....	63
8.4.5	Application Integration and Testing.....	63
8.4.6	Application Validation and Assessment	64
8.4.7	Application preparation procedures and tools.....	64
9	Software deployment and maintenance	64
9.1	Software deployment	64
9.1.1	Objective	64
9.1.2	Input documents	64
9.1.3	Output documents.....	64
9.1.4	Requirements.....	65
9.2	Software maintenance	66
9.2.1	Objective	66
9.2.2	Input documents	66
9.2.3	Output documents.....	66
9.2.4	Requirements.....	67
Annex A	(normative) Criteria for the Selection of Techniques and Measures.....	69
A.1	General	69
A.2	Clauses tables	70
A.3	Detailed tables	77
Annex B	(normative) Key software roles and responsibilities	82
Annex C	(informative) Documents Control Summary	95
Annex D	(informative) Bibliography of techniques.....	97
D.1	Artificial Intelligence Fault Correction.....	97
D.2	Analysable Programs	97
D.3	Avalanche/Stress Testing	98
D.4	Boundary Value Analysis	98
D.5	Backward Recovery	99
D.6	Cause Consequence Diagrams.....	99
D.7	Checklists	99
D.8	Control Flow Analysis.....	100
D.9	Common Cause Failure Analysis	100
D.10	Data Flow Analysis.....	100
D.11	Data Flow Diagrams	101
D.12	Data Recording and Analysis.....	101
D.13	Decision Tables and Truth Tables	102
D.14	Defensive Programming	102
D.15	Coding Standards and Style Guide.....	103
D.16	Diverse Programming	104
D.17	Dynamic Reconfiguration.....	105
D.18	Equivalence Classes and Input Partition Testing.....	105
D.19	Error Detecting and Correcting Codes.....	106
D.20	Error Guessing.....	106
D.21	Error Seeding.....	106
D.22	Event Tree Analysis	107
D.23	Fagan Inspections.....	107

D.24	Failure Assertion Programming	107
D.25	SEEA – Software Error Effect Analysis.....	108
D.26	Fault Detection and Diagnosis	108
D.27	Finite State Machines/State Transition Diagrams.....	109
D.28	Formal Methods	110
D.28.1	General	110
D.28.2	CSP – Communicating Sequential Processes.....	110
D.28.3	CCS – Calculus of Communicating Systems.....	111
D.28.4	HOL – Higher Order Logic	111
D.28.5	LOTOS.....	111
D.28.6	OBJ	111
D.28.7	Temporal logic	112
D.28.8	VDM – Vienna Development Method.....	112
D.28.9	Z method.....	113
D.28.10	B method.....	113
D.28.11	Model Checking	114
D.29	Formal Proof	114
D.30	Forward Recovery.....	114
D.31	Graceful Degradation.....	115
D.32	Impact Analysis.....	115
D.33	Information Hiding / Encapsulation	115
D.34	Interface Testing	116
D.35	Language Subset.....	116
D.36	Memorizing Executed Cases	116
D.37	Metrics	117
D.38	Modular Approach.....	117
D.39	Performance Modelling	118
D.40	Performance Requirements.....	118
D.41	Probabilistic Testing	119
D.42	Process Simulation	119
D.43	Prototyping / Animation	120
D.44	Recovery Block	120
D.45	Response Timing and Memory Constraints.....	120
D.46	Re-Try Fault Recovery Mechanisms.....	120
D.47	Safety Bag	121
D.48	Software Configuration Management	121
D.49	Strongly Typed Programming Languages	121
D.50	Structure Based Testing	122
D.51	Structure Diagrams.....	122
D.52	Structured Methodology.....	123
D.53	Structured Programming.....	123
D.54	Suitable Programming languages.....	124
D.55	Time Petri Nets	125
D.56	Walkthroughs / Design Reviews.....	125
D.57	Object Oriented Programming	125
D.58	Traceability.....	126

D.59 Metaprogramming.....	126
D.60 Procedural programming	127
D.61 Clause intentionally left empty	127
D.62 Clause intentionally left empty	127
D.63 Clause intentionally left empty	127
D.64 Clause intentionally left empty	127
D.65 Data modelling	127
D.66 Control Flow Diagram/Control Flow Graph	128
D.67 Sequence diagram.....	129
D.68 Tabular Specification Methods	129
D.69 Application specific language.....	130
D.70 UML (Unified Modelling Language)	130
D.71 Domain specific languages.....	131
D.72 Segregation.....	131
Annex E (informative) Changes in this European Standard compared to EN 50128:2011	133
Annex ZZ (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC	139
Bibliography	140

Figures

Figure 1 — Illustrative Software Route Map	11
Figure 2 — Illustration of the preferred organizational structure	22
Figure 3 — Illustrative Development Lifecycle 1	27
Figure 4 — Illustrative Development Lifecycle 2	28

Tables

Table 1 — Relation between tool class and applicable numbered entries	42
Table A.1 — Lifecycle Issues and Documentation (5.3).....	70
Table A.2 — Software Requirements Specification (7.2)	72
Table A.3 — Software Architecture (7.3).....	73
Table A.4 — Software Design and Implementation (7.3 and 7.4)	74
Table A.5 — Verification and Testing (6.2, 7.3 and 7.4).....	75
Table A.6 — Integration (7.6)	75
Table A.7 — Overall Software Testing (6.2 and 7.7)	75
Table A.8 — Software Analysis Techniques (6.3).....	76
Table A.9 — Software Quality Assurance (6.5)	76
Table A.10 — Software Maintenance (9.2).....	76
Table A.11 — Data Preparation Techniques (8.4).....	77
Table A.12 — Coding Standards	77
Table A.13 — Dynamic Analysis and Testing	78
Table A.14 — Functional/Black Box Test	78
Table A.15 — Intentionally left empty	78

Table A.16 — Intentionally left empty	78
Table A.17 — Modelling	79
Table A.18 — Performance Testing	79
Table A.19 — Static Analysis	79
Table A.20 — Components	80
Table A.21 — Test Coverage for Code.....	80
Table A.22 — Object Oriented Software Architecture.....	81
Table A.23 — Object Oriented Detailed Design	81
Table B.1 — Requirements Manager Role Specification	83
Table B.2 — Designer Role Specification.....	84
Table B.3 — Implementer Role Specification	85
Table B.4 — Tester Role Specification	86
Table B.5 — Verifier Role Specification.....	87
Table B.6 — Integrator Role Specification	88
Table B.7 — Validator Role Specification.....	89
Table B.8 — Assessor Role Specification	91
Table B.9 — Project Manager Role Specification.....	93
Table B.10 — Configuration Manager Role Specification	94
Table C.1 — Documents Control Summary	95
Table E.1 — Correspondence between this European Standard and EN 50128:2011.....	133
Table ZZ.1 — Correspondence between this European Standard, the TSI “Locomotives and Passenger Rolling Stock” (REGULATION (EU) No 1302/2014 of 18 November 2014) and Directive 2008/57/EC	139

European foreword

This document (EN 50657:2017) has been prepared by CLC/SC 9XB, “Electrical, electronic and electromechanical material on board rolling stock, including associated software”.

The following dates are fixed:

- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2018-05-08
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2020-05-08

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.

This document adapts EN 50128:2011 (prepared by CLC/SC 9XA “Communication, signalling and processing systems”) for the application in the Rolling Stock domain. It uses the same structure and section numbering as EN 50128:2011. Where requirements of EN 50128:2011 do not apply to rolling stock, the respective text is replaced by the term “intentionally left empty”.

The main changes with respect to EN 50128:2011 are listed in Annex E.

Introduction

This European Standard is related to, and should be read in conjunction with the EN 50126 series, *Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*.

This European Standard concentrates on the methods which need to be used in order to provide software which meets the demands for software integrity which are placed upon it by these wider considerations.

This European Standard provides a set of requirements for the development, deployment and maintenance of any software intended for railway rolling stock applications. It defines requirements concerning organizational structure, the relationship between organizations 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 integrity. This European Standard addresses five software 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 integrity level will be.

NOTE 1 The concept of basic integrity used in this European Standard was first introduced in the EN 50126 series.

This European Standard has identified techniques and measures for the five levels of software integrity. The required techniques and measures for basic integrity and for the safety integrity levels 1-4 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 the EN 50126 series to define the process of specifying the safety-related functions allocated to software.

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

The EN 50126 series requires that a systematic approach is 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 the overall system safety requirements 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 level.

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 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 organization and personnel competency issues.

At the system level, the allocation of system requirements to software functions takes place. This includes the definition of the required software integrity level for the functions. The successive functional steps in the application of this European Standard are shown in Figure 1 and are as follows:

- f) 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 integrity level (7.2 and 7.3);
- g) design, develop and test the software according to the Software Quality Assurance Plan, software integrity level and the software lifecycle (7.4 and 7.5);
- h) integrate the software on the target hardware and verify functionality (7.6);
- i) accept and deploy the software (7.7 and 9.1);
- j) 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 (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 safety integrity levels 1-4 and for basic integrity. 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.

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 2 IEC/ISO standards that address IT security in depth are the ISO/IEC 27000 standards, ISO/IEC/TR 19791 and the IEC 62443 series.

It may be necessary to balance between measures against systematic errors and measures against security threats. An example is the need for fast security updates of software arising from security threats, whereas if

such software is safety related, it should be thoroughly developed, tested, validated and approved before any update.

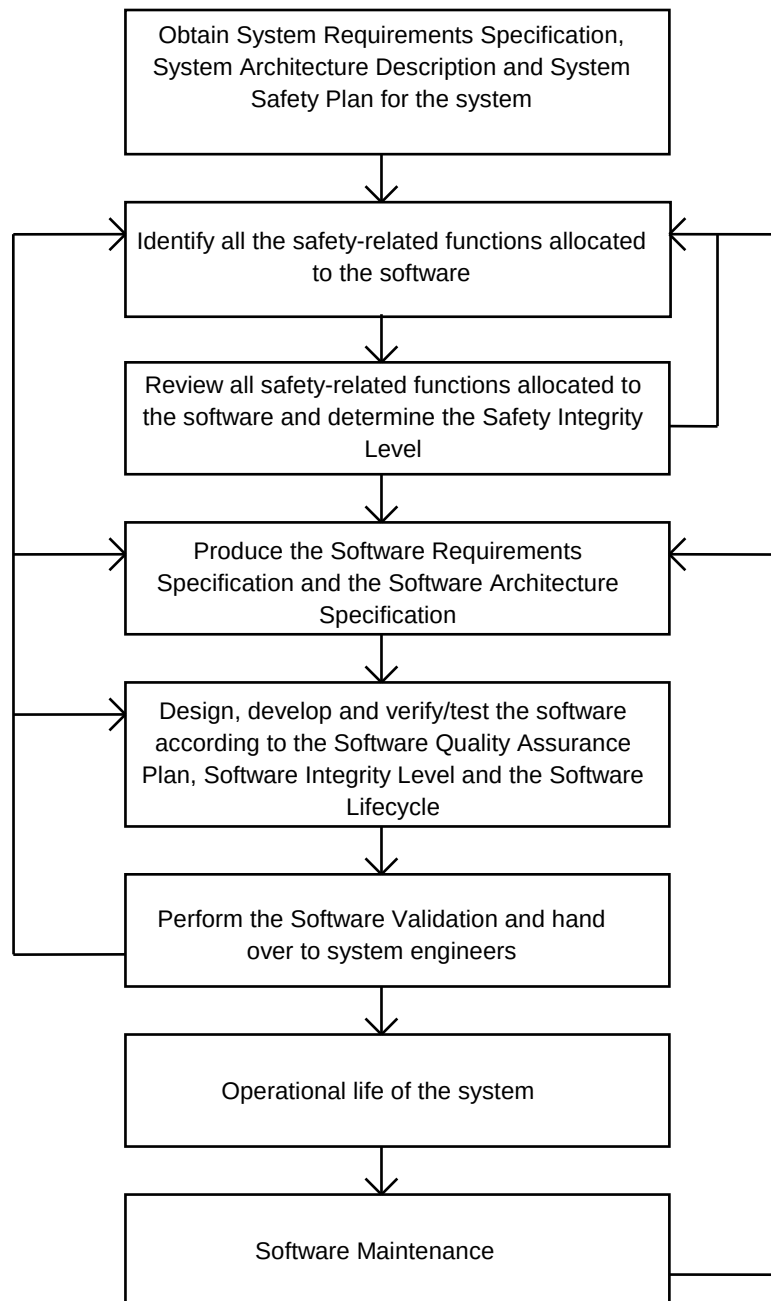


Figure 1 — Illustrative Software Route Map

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 rolling stock applications.

Outside the scope of this standard is software that:

- is part of signalling equipment (CENELEC sub-committee SC9XA applications) installed on board trains, or
- does not contribute to, and is segregated from Rolling Stock operational functions.

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 Entry intentionally left empty

1.4 This European Standard applies to safety-related as well as non-safety-related software, including for example:

- 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 a valid version of EN 50128 is considered as compliant to this standard. Software previously developed in accordance with any version of EN 50128 is also considered as compliant and not subject to the requirements on pre-existing software. For SIL1-SIL4 software under the scope of this standard, requirements included in this European Standard are equivalent to the SIL1-SIL4 software requirements of EN 50128:2011.

1.7 This European Standard considers that modern application design often makes use of software that is suitable as a basis for various applications. Such software is then configured by application data for producing the executable software for the application. This European Standard applies to such software. In addition, specific requirements for application data will be given.

1.8 Entry intentionally left empty.

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. However, application of this European Standard during upgrades and maintenance of existing software is recommended.

1.10 The relevant sections of this software standard are also applicable to programmable components (e.g. FPGA and CPLD), in addition to the applicable hardware standard (e.g. EN 50129, EN 50155, EN 61508-2). However, requirements of this software standard that are already covered by the applicable hardware standard do not need to be re-addressed.

When it is possible to exhaustively test the programmable logic for all possible inputs and internal logic states, this European Standard does not apply.

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 ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary (ISO 9000:2015)*

ISO/IEC 90003:2014, *Software engineering — Guidelines for the application of ISO 9001:2008 to computer software*