

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.



IEC 62279

Edition 2.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**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**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 45.060

ISBN 978-2-8322-2741-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	13
2 Normative references.....	14
3 Terms, definitions and abbreviations	14
3.1 Terms and definitions	14
3.2 Abbreviations	19
4 Objectives, conformance and software safety integrity levels	20
5 Software management and organisation.....	21
5.1 Organisation, 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 Life cycle 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	29
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	31
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.....	34
6.5.1 Objectives.....	34
6.5.2 Input documents	35
6.5.3 Output documents.....	35
6.5.4 Requirements	35
6.6 Modification and change control	37
6.6.1 Objectives.....	37


 (standards.iteh.ai)

[IEC 62279:2015](#)

[http://documents.iteh.ai/catalog/standards/sist/5687ec25-bbd4-48b6-b156-](http://documents.iteh.ai/catalog/standards/sist/5687ec25-bbd4-48b6-b156-498c78ccda0e/iec-62279-2015)

[498c78ccda0e/iec-62279-2015](#)

6.6.2	Input documents	37
6.6.3	Output documents	37
6.6.4	Requirements	37
6.7	Support tools and languages	38
6.7.1	Objectives.....	38
6.7.2	Input documents	38
6.7.3	Output documents.....	38
6.7.4	Requirements	38
7	Generic software development.....	41
7.1	Life cycle and documentation for generic software	41
7.1.1	Objectives.....	41
7.1.2	Requirements	41
7.2	Software requirements	42
7.2.1	Objectives.....	42
7.2.2	Input documents	42
7.2.3	Output documents.....	42
7.2.4	Requirements	42
7.3	Architecture and Design	44
7.3.1	Objectives.....	44
7.3.2	Input documents	44
7.3.3	Output documents.....	44
7.3.4	Requirements	44
7.4	Component design	50
7.4.1	Objectives.....	50
7.4.2	Input documents	50
7.4.3	Output documents.....	50
7.4.4	Requirements	50
7.5	Component implementation and testing	52
7.5.1	Objectives.....	52
7.5.2	Input documents	52
7.5.3	Output documents.....	52
7.5.4	Requirements	52
7.6	Integration	53
7.6.1	Objectives.....	53
7.6.2	Input documents	53
7.6.3	Output documents.....	53
7.6.4	Requirements	53
7.7	Overall Software Testing / Final Validation.....	54
7.7.1	Objectives.....	54
7.7.2	Input documents	54
7.7.3	Output documents.....	55
7.7.4	Requirements	55
8	Development of application data or algorithms: systems configured by application data or algorithms.....	56
8.1	Objectives.....	56
8.2	Input documents	57
8.3	Output documents.....	57
8.4	Requirements.....	57
8.4.1	Application Development Process.....	57

8.4.2	Application Requirements Specification	59
8.4.3	Architecture and Design	59
8.4.4	Application Data/Algorithms Production	59
8.4.5	Application Integration and Testing Acceptance	60
8.4.6	Application Validation and Assessment.....	61
8.4.7	Application preparation procedures and tools.....	61
8.4.8	Development of Generic Software	61
9	Software deployment and maintenance	62
9.1	Software deployment.....	62
9.1.1	Objective	62
9.1.2	Input documents	62
9.1.3	Output documents.....	62
9.1.4	Requirements	62
9.2	Software maintenance	64
9.2.1	Objective	64
9.2.2	Input documents	64
9.2.3	Output documents.....	64
9.2.4	Requirements	64
Annex A	(normative) Criteria for the selection of techniques and measures	67
A.1	General.....	67
A.2	Clauses tables	68
A.3	Detailed tables	74
Annex B	(normative) Key software roles and responsibilities	80
Annex C	(informative) Documents Control Summary.....	88
Annex D	(informative) Aim and description of techniques.....	90
D.1	Artificial Intelligence Fault Correction.....	90
D.2	Analysable Programs	90
D.3	Avalanche/Stress Testing.....	91
D.4	Boundary Value Analysis.....	91
D.5	Backward Recovery.....	92
D.6	Cause Consequence Diagrams.....	92
D.7	Checklists	92
D.8	Control Flow Analysis.....	93
D.9	Common Cause Failure Analysis	93
D.10	Data Flow Analysis.....	94
D.11	Data Flow Diagrams	94
D.12	Data Recording and Analysis.....	95
D.13	Decision Tables (Truth Tables).....	95
D.14	Defensive Programming	96
D.15	Coding Standards and Style Guide	96
D.16	Diverse Programming.....	97
D.17	Dynamic Reconfiguration.....	98
D.18	Equivalence Classes and Input Partition Testing	98
D.19	Error Detecting and Correcting Codes	98
D.20	Error Guessing.....	99
D.21	Error Seeding.....	99
D.22	Event Tree Analysis	100
D.23	Fagan Inspections.....	100

ITeh STANDARD PREVIEW

(standards.itech.ai)

<https://standards.itech.ai/catalog/standards/sist/5687ec25-bbd4-48b6-b156-498c78ccda0e/iec-62279-2015>

D.24	Failure Assertion Programming.....	100
D.25	SEEA – Software Error Effect Analysis	101
D.26	Fault Detection and Diagnosis	101
D.27	Finite State Machines/State Transition Diagrams	102
D.28	Formal Methods	102
D.28.1	General	102
D.28.2	CSP – Communicating Sequential Processes	103
D.28.3	CCS – Calculus of Communicating Systems	104
D.28.4	HOL – Higher Order Logic.....	104
D.28.5	LOTOS	104
D.28.6	OBJ	105
D.28.7	Temporal logic	105
D.28.8	VDM – Vienna Development Method.....	105
D.28.9	Z method	106
D.28.10	B method	106
D.28.11	Model Checking	107
D.29	Formal Proof.....	108
D.30	Forward Recovery.....	108
D.31	Graceful Degradation	108
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.....	118
D.54	Suitable Programming languages	118
D.55	Time Petri Nets	119
D.56	Walkthroughs / Design Reviews.....	119
D.57	Object Oriented Programming	120
D.58	Traceability	120
D.59	Metaprogramming	121
D.60	Procedural programming	121
D.61	Sequential Function Charts	122

D.62	Ladder Diagram	122
D.63	Functional Block Diagram.....	122
D.64	State Chart or State Diagram.....	122
D.65	Data modelling	123
D.66	Control Flow Diagram/Control Flow Graph	123
D.67	Sequence diagram	124
D.68	Tabular Specification Methods.....	125
D.69	Application specific language	125
D.70	UML (Unified Modeling Language).....	125
D.71	Domain specific languages.....	126
	Bibliography	127
	Figure 1 – Illustrative software route map	12
	Figure 2 – Illustration of the preferred organisational structure.....	22
	Figure 3 – Illustrative Development Life cycle 1	27
	Figure 4 – Illustrative Development Life cycle 2	28
	Table 1 – Relation between tool class and applicable subclauses	41
	Table 2 – Illustrative Relation between tool class and product SIL.....	41
	Table A.1 – Life cycle Issues and Documentation (5.3).....	68
	Table A.2 – Software Requirements Specification (7.2).....	70
	Table A.3 – Software Architecture (7.3)	71
	Table A.4 – Software Design and Implementation (7.4)	72
	Table A.5 – Verification and Testing (6.2 and 7.3, 7.5).....	72
	Table A.6 – Integration (7.6)	73
	Table A.7 – Overall Software Testing (6.2 and 7.7).....	73
	Table A.8 – Software Analysis Techniques (6.3).....	73
	Table A.9 – Software Quality Assurance (6.5).....	73
	Table A.10 – Software Maintenance (9.2)	74
	Table A.11 – Data Preparation Techniques (8.4)	74
	Table A.12 – Coding Standards.....	74
	Table A.13 – Dynamic Analysis and Testing	75
	Table A.14 – Functional/Black Box Test	75
	Table A.15 – Textual Programming Languages.....	76
	Table A.16 – Diagrammatic Languages for Application Algorithms	76
	Table A.17 – Modelling	77
	Table A.18 – Performance Testing	77
	Table A.19 – Static Analysis.....	77
	Table A.20 – Components.....	78
	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.....	80

Table B.3 – Implementer Role Specification	81
Table B.4 – Tester Role Specification.....	82
Table B.5 – Verifier Role Specification	82
Table B.6 – Integrator Role Specification.....	83
Table B.7 – Validator Role Specification.....	84
Table B.8 – Assessor Role Specification	85
Table B.9 – Project Manager Role Specification	86
Table B.10 – Configuration Manager Role Specification.....	86
Table B.11 – Quality Assurance Manager Role Specification.....	87
Table B.12 – Reviewer Role Specification	87
Table C.1 – Documents Control Summary	88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[IEC 62279:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/5687ec25-bbd4-48b6-b156-498c78ccda0e/iec-62279-2015>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING
AND PROCESSING SYSTEMS – SOFTWARE FOR RAILWAY
CONTROL AND PROTECTION SYSTEMS**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
<https://standards.iteh.ai/catalog/standards/sis/5687m35-bhd1-48bc-h156>
<https://standards.iteh.ai/catalog/standards/sis/5687m35-bhd1-48bc-h156>
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62279 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard is based on EN 50128:2011.

This second edition cancels and replaces the first edition, issued in 2002. It constitutes a technical revision.

The main technical changes with respect to the previous edition are as follows:

- requirements on software management and organisation, definition of roles and competencies, deployment and maintenance have been added;
- a new subclause on tools has been inserted in 6.7, based on IEC 61508-2:2010;
- tables in Annex A have been updated;
- a new Annex B on key software roles and responsibilities has been introduced;

- a new Annex C on document control summary has been introduced;
- Annex B on Bibliography of techniques has been revised and updated as new Annex D.

The main changes with respect to EN 50128:2011 are listed below:

- the subclause on tools in 6.7 has been updated;
- Annex B on key software roles and responsibilities has been modified.

The text of this standard is based on the following documents:

FDIS	Report on voting
9/2023/FDIS	9/2046/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

This Standard should be read in conjunction with IEC 62278:2002, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

<http://standards.iteh.ai/catalog/standards/sist/5687ec25-bbd4-48b6-b156-498c78ccda0e/iec-62279-2015>

INTRODUCTION

This Standard is part of a group of related standards. The others are IEC 62278:2002, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)* and IEC 62425:2007, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*.

IEC 62278:2002 addresses system issues on the widest scale, while IEC 62425:2007 addresses the approval process for individual systems which can exist within the overall railway control and protection system. This 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 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 should 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 Standard.

The key concept of this Standard is that of levels of software integrity. This Standard addresses five software safety integrity levels where SIL 0 is the lowest and SIL 4 the highest safety related integrity levels. The higher the risk resulting from software failure, the higher the software safety integrity level will be.

This Standard has identified techniques and measures for the five levels of software integrity. The required techniques and measures for software Safety Integrity Levels 0 to 4 are shown in the normative tables of Annex A. In this standard, 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 Standard does not give guidance on which level of software 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 functions and social and economic factors.

It is within the scope of IEC 62278 and IEC 62425 to define the process of specifying the safety functions allocated to software.

This Standard specifies those measures necessary to achieve these requirements.

IEC 62278 and IEC 62425 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 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 safety functions allocated to software and determines their safety integrity level. The successive functional steps in the application of this 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) carry out software/software and software/hardware integration 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 Standard as appropriate (9.2).

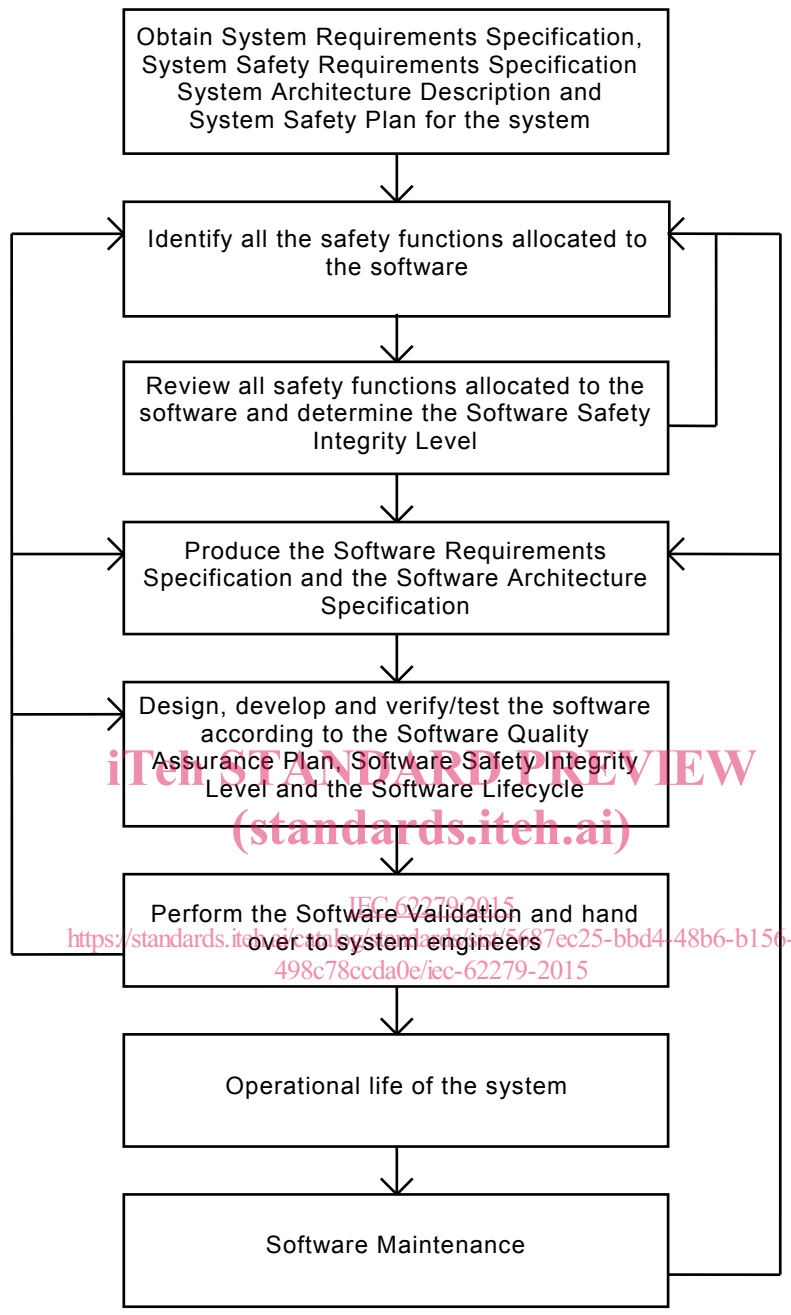
A number of activities run across the software development. These include testing (6.1), verification (6.2), validation (6.3), assessment (6.4), quality assurance (6.5) and modification and change control (6.6).

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 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. 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.



IEC

Figure 1 – Illustrative software route map

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS

1 Scope

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

1.3 This 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 safety functions. The concept of SIL 0 is introduced because uncertainty is present in the evaluation of the risk, and even in the identification of hazards. At least the SIL 0 requirements of this Standard are fulfilled for the software part of functions that have a safety impact below SIL 1.

1.4 This 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 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 Standard will be considered as compliant and not subject to the requirements on pre-existing software.

1.7 This 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 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 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 Standard will need careful consideration in any commercial situation.

1.9 This 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 analyses the