



**Irish Standard**  
**I.S. EN 50657:2017&A1:2023**

**Version 1.01**

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

## I.S. EN 50657:2017&A1:2023 V1.01

### The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

NSAI/... xxx: A National adoption of a Technical Regulation (TR), Technical Specification (TS), CEN and/or CENELEC Workshop Agreement (CWA).

I.S. EN 50657:2017&A1:2023 V1.01 was published under the authority of the NSAI and came into effect on: 2023-11-05

ICS number(s): 35.080, 35.240.60

NSAI  
1 Swift Square  
Northwood, Santry  
Dublin 9  
D09 A0E4  
+353 1 807 3800  
standards@nsai.ie  
[NSAI.ie](https://www.nsa.ie)

Sales  
+353 1 857 6730  
[Standards.ie](https://www.standards.ie)

Údarás um Chaighdeán Náisiúnta na hÉireann

## **National Foreword**

I.S. EN 50657:2017&A1:2023 V1.01 is the version of the NSAI adopted European document EN 50657:2017, *Railways Applications - Rolling stock applications - Software on Board Rolling Stock*, including any Corrections, Amendments etc. to EN 50657:2017.

This normative document by CEN/CENELEC the elaboration of which includes a public enquiry, followed by a Formal Vote of CEN/CENELEC national members and final ratification. This European Standard is published as an identical national standard and every conflicting national standard will be withdrawn. The content of a European Standard does not conflict with the content of any other EN (and HD for CENELEC).

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

**Conformance with this document does not of its self confer immunity from legal obligations.**

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

**I.S. EN 50657:2017&A1:2023 V1.01**

This page intentionally left blank

EUROPEAN STANDARD

**EN 50657:2017/A1**

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2023

ICS 35.080; 35.240.60

English Version

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

Applications ferroviaires - Applications du matériel roulant -  
Logiciels embarqués

Bahnanwendungen - Anwendungen für Bahnfahrzeuge -  
Software auf Bahnfahrzeugen

This amendment A1 modifies the European Standard EN 50657:2017; it was approved by CENELEC on 2023-08-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment 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 amendment 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, 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, Türkiye 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**

© 2023 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50657:2017/A1:2023 E

Contents		Page
European foreword.....		3
1	Modification to Scope .....	3
2	Modifications to Clause 5 “Software management and organization” .....	4
3	Modification to Annexes .....	4

## European foreword

This document [EN 50657:2017/A1:2023] 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) 2024-08-03
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2026-08-03

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 standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

## **1 Modification to Scope**

*Add the following note after the paragraph in 1.6:*

“NOTE This document was derived from the signalling standard EN 50128 which in many cases was also applied in Rolling Stock applications. Subclause 1.6 ensures continuity in the application of the standards, i.e., software that was developed in accordance with EN 50128 can still be re-used for new projects.”

## **2 Modifications to Clause 5 “Software management and organization”**

*Delete the following text of subclause 5.1.2.4*

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

*and replace it with the following:*

“The Assessor shall be appointed for SIL 1 – SIL 4 and may be appointed by the supplier or by the customer.”

*Delete the following text of subclause 5.1.2.5*

“The Assessor shall be independent from the supplier or, at the discretion of the Safety Authority, be part of the supplier’s organization or of the customer’s organization.”

*and replace it with the following:*

“The Assessor may be part of any stakeholder organization (e.g. supplier, customer or third-party organisation).”

## **3 Modification to Annexes**

*Delete the existing Annex ZZ and replace it with the following one:*

“

### **Annex ZZ** (informative)

#### **Relationship between this European Standard and the Essential Requirements of EU Directive (EU) 2016/797 aimed to be covered**

This European Standard has been prepared under a Commission’s standardisation request “M/483 Mandate to CEN and CENELEC for Standardisation in the field of interoperability of the rail system” to provide one voluntary means of conforming to (parts of) Essential Requirements of Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on interoperability of the rail system (recast) as specified in the relevant technical specifications for interoperability (TSI).

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZZ.1 for “Locomotives and Passenger Rolling Stock”, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive as specified in the technical specifications for interoperability (TSI), and associated EFTA regulations.



EUROPEAN STANDARD

**EN 50657**

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2017

ICS 35.080; 35.240.60

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

<b>European foreword</b>	<b>8</b>
<b>Introduction</b>	<b>9</b>
<b>1 Scope</b>	<b>12</b>
<b>2 Normative references</b>	<b>13</b>
<b>3 Terms, definitions and abbreviations</b>	<b>13</b>
3.1 Terms and definitions	13
3.2 Abbreviations	19
<b>4 Objectives, conformance and software integrity levels</b>	<b>20</b>
<b>5 Software management and organization</b>	<b>21</b>
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
<b>6 Software assurance</b>	<b>28</b>
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
<b>7</b>	<b>Software development.....</b>	<b>42</b>
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
<b>8</b>	<b>Systems configured by application data: development of application data.....</b>	<b>60</b>
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
<b>9</b>	<b>Software deployment and maintenance .....</b>	<b>64</b>
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
<b>Annex A</b>	<b>(normative) Criteria for the Selection of Techniques and Measures.....</b>	<b>69</b>
A.1	General .....	69
A.2	Clauses tables .....	70
A.3	Detailed tables .....	77
<b>Annex B</b>	<b>(normative) Key software roles and responsibilities .....</b>	<b>82</b>
<b>Annex C</b>	<b>(informative) Documents Control Summary .....</b>	<b>95</b>
<b>Annex D</b>	<b>(informative) Bibliography of techniques.....</b>	<b>97</b>
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
<b>Annex E (informative) Changes in this European Standard compared to EN 50128:2011 .....</b>	<b>133</b>
<b>Annex ZZ (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC .....</b>	<b>139</b>
<b>Bibliography .....</b>	<b>140</b>

## Figures

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

## Tables

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

<b>Table A.16 — Intentionally left empty .....</b>	<b>78</b>
<b>Table A.17 — Modelling .....</b>	<b>79</b>
<b>Table A.18 — Performance Testing .....</b>	<b>79</b>
<b>Table A.19 — Static Analysis .....</b>	<b>79</b>
<b>Table A.20 — Components .....</b>	<b>80</b>
<b>Table A.21 — Test Coverage for Code.....</b>	<b>80</b>
<b>Table A.22 — Object Oriented Software Architecture .....</b>	<b>81</b>
<b>Table A.23 — Object Oriented Detailed Design .....</b>	<b>81</b>
<b>Table B.1 — Requirements Manager Role Specification .....</b>	<b>83</b>
<b>Table B.2 — Designer Role Specification.....</b>	<b>84</b>
<b>Table B.3 — Implementer Role Specification .....</b>	<b>85</b>
<b>Table B.4 — Tester Role Specification .....</b>	<b>86</b>
<b>Table B.5 — Verifier Role Specification.....</b>	<b>87</b>
<b>Table B.6 — Integrator Role Specification .....</b>	<b>88</b>
<b>Table B.7 — Validator Role Specification.....</b>	<b>89</b>
<b>Table B.8 — Assessor Role Specification .....</b>	<b>91</b>
<b>Table B.9 — Project Manager Role Specification.....</b>	<b>93</b>
<b>Table B.10 — Configuration Manager Role Specification .....</b>	<b>94</b>
<b>Table C.1 — Documents Control Summary .....</b>	<b>95</b>
<b>Table E.1 — Correspondence between this European Standard and EN 50128:2011 .....</b>	<b>133</b>
<b>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 .....</b>	<b>139</b>

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

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.

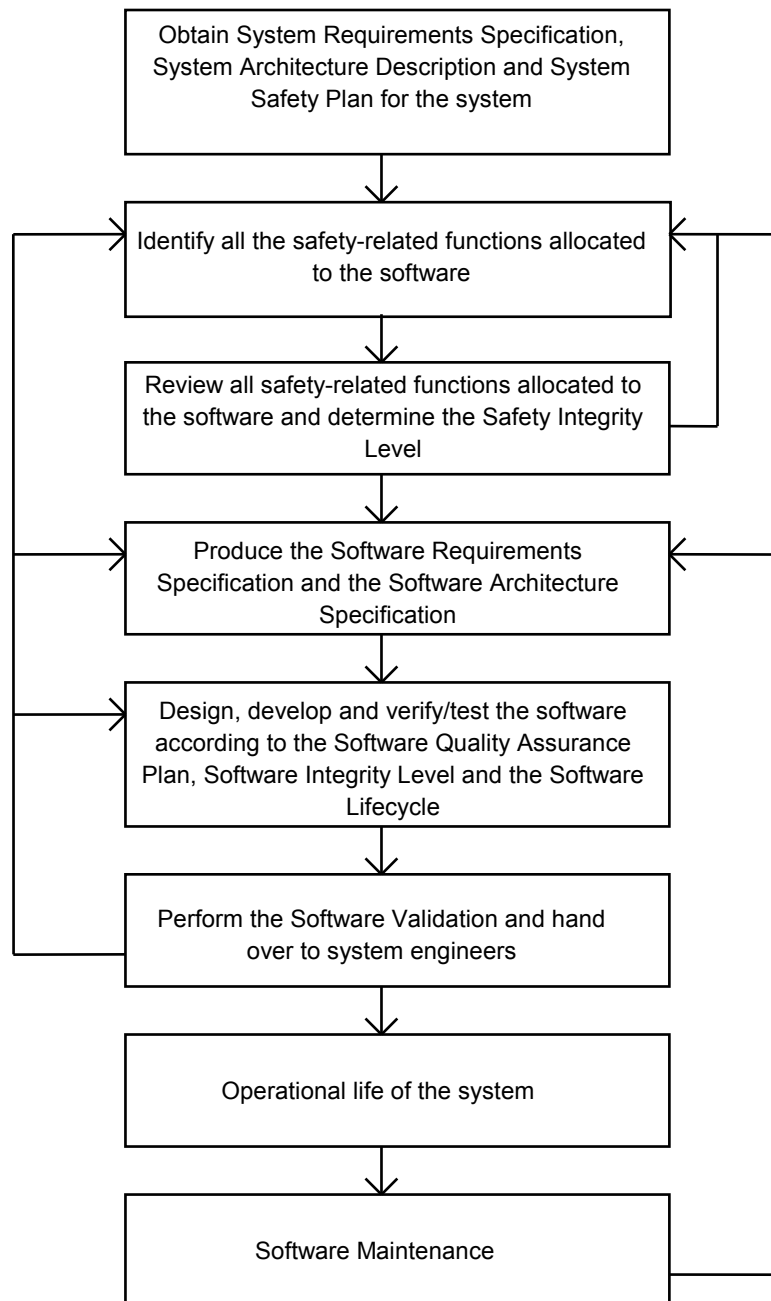
Tables have been formulated ranking various techniques/measures against the safety integrity levels 1-4 and for basic integrity. The tables are in Annex A. Cross-referenced to the tables is a bibliography giving a brief description of each technique/measure with references to further sources of information. 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.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- Looking for additional Standards? Visit Intertek Inform Infostore
  - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-