BSI Standards Publication

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


It should be noted that this standard is presently undergoing further revision to expand its remit to cover software applications within the context of the whole railway system, including, but not limited to, rolling stock, fixed installations as well as signalling systems. When revised it is planned that EN 50128 will become a part of the new suite of EN 50126 railway standards.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to CENELEC text carry the number of the CENELEC amendment. For example, text altered by CENELEC amendment A2 is indicated by \[ \text{A2} \].

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

A list of organizations represented on this committee can be obtained on request to its committee manager.

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

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 13395 0

ICS 35.240.60; 45.020; 93.100

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2011.

Amendments/corrigenda issued since publication

<table>
<thead>
<tr>
<th>Date</th>
<th>Text affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 April 2014</td>
<td>Implementation of CENELEC corrigendum February 2014: dow date extended to 2017-04-25 in European foreword</td>
</tr>
<tr>
<td>31 August 2020</td>
<td>Implementation of CENELEC amendment A2:2020</td>
</tr>
</tbody>
</table>
Railway applications -
Communication, signalling and processing systems -
Software for railway control and protection systems

This European Standard was approved by CENELEC on 2011-04-25. 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 Central Secretariat 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 Central Secretariat 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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.
Contents

Forewords .............................................................................................................................................. 6
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 ............................................................. 17
5 Software management and organisation ............................................................................................. 18
  5.1 Organisation, roles and responsibilities ......................................................................................... 18
  5.2 Personnel competence ................................................................................................................... 21
  5.3 Lifecycle issues and documentation ................................................................................................. 22
6 Software assurance .............................................................................................................................. 24
  6.1 Software testing ............................................................................................................................. 24
  6.2 Software verification ....................................................................................................................... 26
  6.3 Software validation .......................................................................................................................... 28
  6.4 Software assessment ....................................................................................................................... 29
  6.5 Software quality assurance ............................................................................................................. 31
  6.6 Modification and change control .................................................................................................... 33
  6.7 Support tools and languages .......................................................................................................... 34
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 .......................................................................................... 50
  7.6 Integration ....................................................................................................................................... 51
  7.7 Overall Software Testing / Final Validation ..................................................................................... 53
8 Development of application data or algorithms: systems configured by application data or algorithms .......................................................................................................................... 55
8.1 Objectives ................................................................................................................. 55
8.2 Input documents ......................................................................................................... 56
8.3 Output documents ....................................................................................................... 56
8.4 Requirements ................................................................................................................ 56
9 Software deployment and maintenance ....................................................................... 61
  9.1 Software deployment .................................................................................................. 61
  9.2 Software maintenance ............................................................................................... 63
Annex A (normative) Criteria for the Selection of Techniques and Measures ................. 66
  A.1 Clauses tables ........................................................................................................... 67
  A.2 Detailed tables .......................................................................................................... 69
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 ......................................................................................... 92
  D.4 Boundary Value Analysis ....................................................................................... 92
  D.5 Backward Recovery ................................................................................................. 93
  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 ............................................................................................... 95
  D.11 Data Flow Diagrams ............................................................................................. 95
  D.12 Data Recording and Analysis .............................................................................. 96
  D.13 Decision Tables (Truth Tables) ........................................................................... 96
  D.14 Defensive Programming ....................................................................................... 97
  D.15 Coding Standards and Style Guide .................................................................... 97
  D.16 Diverse Programming .......................................................................................... 98
  D.17 Dynamic Reconfiguration .................................................................................... 99
  D.18 Equivalence Classes and Input Partition Testing .................................................. 99
  D.19 Error Detecting and Correcting Codes ............................................................... 99
  D.20 Error Guessing ..................................................................................................... 100
  D.21 Error Seeding ....................................................................................................... 100
  D.22 Event Tree Analysis ............................................................................................. 100
  D.23 Fagan Inspections ................................................................................................. 101
  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 ............................................ 103
  D.28 Formal Methods .................................................................................................. 103
  D.29 Formal Proof ....................................................................................................... 109

BS EN 50128:2011+A2:2020
EN 50128:2011+A2:2020

- 3 -

Bibliography. 130
Figures

Figure 1 – Illustrative Software Route Map ......................................................................................................... 10
Figure 2 – Illustration of the preferred organisational structure ........................................................................ 19
Figure 3 – Illustrative Development Lifecycle 1 .................................................................................................. 23
Figure 4 – Illustrative Development Lifecycle 2 .................................................................................................. 24

Tables

Table 1 - Relation between tool class and applicable sub-clauses ............................................................................. 38
Table A.1 – Lifecycle Issues and Documentation (5.3) ......................................................................................... 67
Table A.2 – Software Requirements Specification (7.2) ....................................................................................... 69
Table A.3 – Software Architecture (7.3) .................................................................................................................. 70
Table A.4 – Software Design and Implementation (7.4) ..................................................................................... 71
Table A.5 – Verification and Testing (6.2 and 7.3) ................................................................................................. 72
Table A.6 – Integration (7.6) .................................................................................................................................. 72
Table A.7 – Overall Software Testing (6.2 and 7.7) ............................................................................................ 72
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) ........................................................................................................... 73
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 ............................................................................................................. 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
European 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".

Foreword to amendment A1

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.
POLICY STATEMENT DEFINING ASHRAE'S CONCERN FOR THE ENVIRONMENTAL IMPACT OF ITS ACTIVITIES

ASHRAE is concerned with the impact of its members' activities on both the indoor and outdoor environment. ASHRAE's members will strive to minimize any possible deleterious effects on the indoor and outdoor environment of the systems and components in their responsibility while maximizing the beneficial effects these systems provide, consistent with the accepted standards and the practical state of the art.

ASHRAE's short-range goal is to ensure that the systems and components within its scope do not impact the indoor or outdoor environment to a greater extent than specified by the standards as established by itself and other responsible bodies.

As an ongoing goal, ASHRAE will, through its Standards Committee and extensive technical committee structure, continue to generate up-to-date standards where appropriate and adopt, recommend, and promote those new and revised standards developed by other responsible organizations.

Through its Handbook, appropriate chapters will contain up-to-date standards and design considerations as the material is systematically revised.

ASHRAE will take the lead with research and dissemination of environmental information of its primary interest and will seek out and disseminate information from other responsible organizations that is pertinent, as guides to updating standards.

The effects of the design and selection of equipment and systems will be considered within the scope of the system's intended use and expected misuse. The disposal of hazardous materials, if any, will also be considered.

ASHRAE's primary concern for environmental impact will be at the site where equipment within ASHRAE's scope operates. However, energy source selection and the possible environmental impact due to the energy source and energy transportation will be considered where possible. Recommendations concerning energy source selection should be made by its members.

Foreword to amendment A2

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.


- 7 -

BS EN 50128:2011+A2:2020
EN 50128:2011+A2:2020
Introduction

This European Standard is part of a group of related standards. The others are EN 50126-1:1999 "Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process", BS 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 50129:2003 "Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling".

EN 50126-1 and EN-50126-2 address 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 0 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 0-4 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, 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, 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 safety-related functions 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.

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.
Obtain System Requirements Specification, System Safety Requirements Specification, System Architecture Description and System Safety Plan for the system

Identify all the safety-related functions allocated to the software

Review all safety-related functions allocated to the software and determine the Software Safety Integrity Level

Produce the Software Requirements Specification and the Software Architecture Specification

Design, develop and verify/test the software according to the Software Quality Assurance Plan, Software Safety Integrity Level and the Software Lifecycle

Perform the Software Validation and hand over to system engineers

Operational life of the system

Software Maintenance

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 safety-related functions.

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.

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