Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation
INTERNATIONAL STANDARD

NORME INTERNATIONALE

Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation
CONTENTS

FOREWORD.......................................................................................................................5
INTRODUCTION.....................................................................................................................7

1 Scope..........................................................................................................................8
2 Normative references........................................................................................................9
3 Terms, definitions and abbreviations...............................................................................10
  3.1 Definitions .............................................................................................................10
  3.2 Abbreviations.........................................................................................................15
4 Overall framework of this standard..................................................................................16
5 Conditions for safety acceptance and approval................................................................17
  5.1 The safety case .....................................................................................................17
  5.2 Evidence of quality management............................................................................19
  5.3 Evidence of safety management .............................................................................21
    5.3.1 Introduction ...............................................................................................21
    5.3.2 Safety life-cycle .........................................................................................22
    5.3.3 Safety organisation ....................................................................................23
    5.3.4 Safety plan ................................................................................................24
    5.3.5 Hazard log .................................................................................................25
    5.3.6 Safety requirements specification ........................................................................25
    5.3.7 System/sub-system/equipment design ..........................................................25
    5.3.8 Safety reviews .............................................................................................25
    5.3.9 Safety verification and validation ..................................................................25
    5.3.10 Safety justification .....................................................................................26
    5.3.11 System/sub-system/equipment handover ....................................................26
    5.3.12 Operation and maintenance ........................................................................26
    5.3.13 Decommissioning and disposal ..................................................................26
  5.4 Evidence of functional and technical safety ..................................................................26
  5.5 Safety acceptance and approval ..............................................................................29
    5.5.1 Introduction ...............................................................................................29
    5.5.2 Safety approval process ..............................................................................30
    5.5.3 After safety approval ....................................................................................32
    5.5.4 Dependency between safety approvals ..........................................................32

Annex A (normative) Safety integrity levels ...........................................................................33
Annex B (normative) Detailed technical requirements ................................................................47
Annex C (normative) Identification of hardware component failure modes .................................62
Annex D (informative) Supplementary technical information ..................................................79
Annex E (informative) Techniques and measures for safety-related electronic systems for signalling for the avoidance of systematic faults and the control of random and systematic faults ..............................................................................................................86

Bibliography.......................................................................................................................95

Figure 1 – Scope of the main IEC railway application standards..............................................9
Figure 2 – Structure of IEC 62425 .....................................................................................17
Table E.5 – Design features (referred to in 5.4) ................................................................. 90
Table E.6 – Failure and hazard analysis methods (referred to in 5.4) ................................. 91
Table E.7 – Design and development of system/sub-system/equipment (referred to in
5.3.7) ................................................................................................................................. 91
Table E.8 – Design phase documentation (referred to in 5.2) ............................................. 92
Table E.9 – Verification and validation of the system and product design (referred to in
5.3.9) .................................................................................................................................. 93
Table E.10 – Application, operation and maintenance (referred to in 5.3.12 and 5.4) ......... 94
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.

5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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 62425 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

It was submitted to the National Committees for voting under the Fast Track Procedure as the following documents:

<table>
<thead>
<tr>
<th>FDIS</th>
<th>Report on voting</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/1057/FDIS</td>
<td>9/1087/RVD</td>
</tr>
</tbody>
</table>

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 document is based on EN 50129.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.
The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site 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.
INTRODUCTION

This standard is the first International Standard defining requirements for the acceptance and approval of safety-related electronic systems in the railway signalling field. This standard is derived from the European Standard EN 50129.

Safety-related electronic systems for signalling include hardware and software aspects. To install complete safety-related systems, both parts within the whole life-cycle of the system have to be taken into account. The requirements for safety-related hardware and for the overall system are defined in this standard. Other requirements are defined in associated IEC standards.

This standard is the common base for safety acceptance and approval of electronic systems for railway signalling applications. The aim of railway authorities and railway industry is to develop railway systems based on common standards. The safety authorities having jurisdiction can apply this standard to the relevant matters they choose. On this basis, cross-acceptance of safety approvals for sub-systems and equipment can be applied by the different national safety authorities. Cross-acceptance is applicable to generic approval, not to specific applications.

The standard consists of the main part (Clause 1 to Clause 5) and Annexes A, B, C, D and E. The requirements defined in the main part of the standard and in Annexes A, B and C are normative, whilst Annexes D and E are informative.

This standard is in line with, and uses relevant sections of IEC 62278: "Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)". This standard and IEC 62278 are based on the system life-cycle and are in line with IEC 61508-1, which is replaced by the set of IEC 62278/ IEC 62279/ IEC 62425, as far as railway communication, signalling and processing systems are involved. Meeting the requirements in these standards is sufficient to ensure that further compliance to IEC 61508-1 need not be evaluated.

Because this standard is concerned with the evidence to be presented for the acceptance of safety-related systems, it specifies those life-cycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. Safety justification for the whole of the life-cycle is therefore required.

This standard is concerned with what evidence is to be presented. Except where considered appropriate, it does not specify who should carry out the necessary work, since this may vary in different circumstances.

For safety-related systems which include programmable electronics, additional conditions for the software are defined in IEC 62279.

Additional requirements for safety-related data communication are defined in IEC 62280-1 and IEC 62280-2.
RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED ELECTRONIC SYSTEMS FOR SIGNALLING

1 Scope

This International Standard is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications.

The scope of this standard, and its relationship with other IEC standards, are shown in Figure 1.

This standard is intended to apply to all safety-related railway signalling systems/sub-system/equipment. However, the hazard analysis and risk assessment processes defined in IEC 62278 and this standard are necessary for all railway signalling systems/sub-systems/equipment, in order to identify any safety requirements. If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety-related), and provided the conclusion is not revised as a consequence of later changes, this safety standard ceases to be applicable.

This standard applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete signalling systems, and also to individual sub-systems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

This standard applies to generic sub-systems and equipment (both application-independent and those intended for a particular class of application), and also to systems/sub-systems/equipment for specific applications.

This standard is not applicable to existing systems/sub-systems/equipment (i.e. those which had already been accepted prior to the creation of this standard). However, as far as reasonably practicable, this standard should be applied to modifications and extensions to existing systems, sub-systems and equipment.

This standard is primarily applicable to systems/sub-systems/equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (i.e.: power supplies, modems, etc.), which is procured for use as part of a safety-related signalling system. As a minimum, evidence shall be provided in such cases to demonstrate

- either that the equipment is not relied on for safety,
- or that the equipment can be relied on for those functions which relate to safety.

This standard is applicable to the functional safety of railway signalling systems. It is not intended to deal with the occupational health and safety of personnel; this subject is covered by other standards.
2 Normative references

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

NOTE 1 Additional informative references are included in the Bibliography.

IEC 60664 (all parts), Insulation coordination for equipment within low-voltage systems


IEC 62236 (all parts), Railway applications – Electromagnetic compatibility

IEC 62236-4, Railway applications – Electromagnetic compatibility – Part 4: Emission and immunity of the signalling and telecommunications apparatus

IEC 62278, Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)

IEC 62279, Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems

IEC 62280-1, Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems

IEC 62280-2, Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems
3 Terms, definitions and abbreviations

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

3.1 Definitions

3.1.1 accident
an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

3.1.2 assessment
the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose

3.1.3 authorisation
the formal permission to use a product within specified application constraints

3.1.4 availability
the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided

3.1.5 causal analysis
analysis of the reasons how and why a particular hazard may come into existence

3.1.6 common-cause failure
failure common to items which are intended to be independent

3.1.7 consequence analysis
analysis of events which are likely to happen after a hazard has occurred

3.1.8 configuration
the structuring and interconnection of the hardware and software of a system for its intended application