IEC 62425

Edition 1.0 2007-09

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

IEC 62425:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62425

Edition 1.0 2007-09

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 45.060 ISBN 2-8318-9310-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED ELECTRONIC SYSTEMS FOR SIGNALLING

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:

FDIS	Report on voting
9/1057/FDIS	9/1087/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 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 (e.g.: 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.

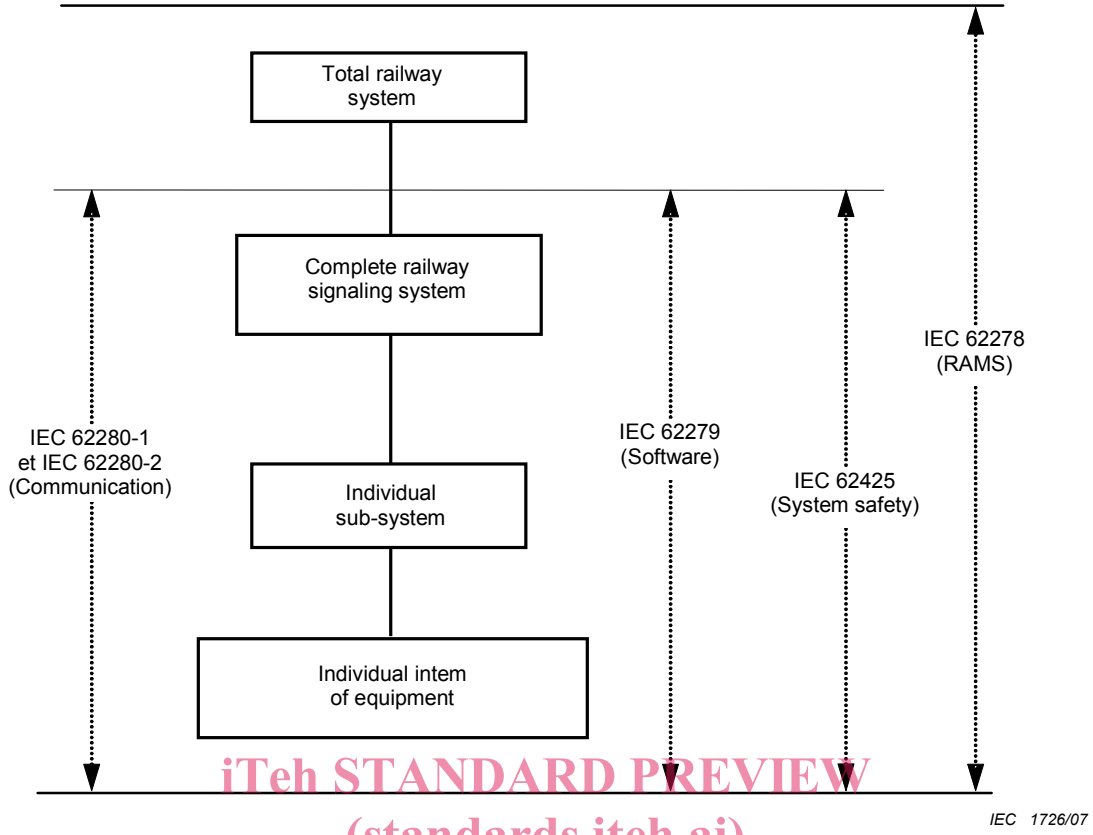

Figure 1 – Scope of the main IEC railway application standards

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 61508-1, *Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements*

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*

EN 50124-1, *Railway applications – Insulation coordination – Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment*

EN 50125-1, *Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock*

EN 50125-3, *Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications*

EN 50155, *Railway applications – Electronic equipment used on rolling stock*

NOTE 2 EN 50124 (series), EN 50125 (series) and EN 50155 will be converted to IEC standards according to the merging strategy between IEC TC9 and CENELEC TC9X.

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

3.1.9
cross-acceptance
the status achieved by a product that has been accepted by one authority to the relevant standards and is acceptable to other authorities without the necessity for further assessment

3.1.10
design
the activity applied in order to analyse and transform specified requirements into acceptable design solutions which have the required safety integrity

3.1.11
design authority
the body responsible for the formulation of a design solution to fulfil the specified requirements and for overseeing the subsequent development and setting-to-work of a system in its intended environment

3.1.12
diversity
a means of achieving all or part of the specified requirements in more than one independent and dissimilar manner

3.1.13
equipment
a functional physical item

3.1.14
error
a deviation from the intended design which could result in unintended system behaviour or failure

3.1.15
fail-safe
a concept which is incorporated into the design of a product such that, in the event of a failure, it enters or remains in a safe state

3.1.16
failure
a deviation from the specified performance of a system

NOTE A failure is the consequence of a fault or error in the system.

3.1.17
fault
an abnormal condition that could lead to an error in a system

NOTE A fault can be random or systematic.

3.1.18
fault detection time
time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected

3.1.19
function
a mode of action or activity by which a product fulfils its purpose

3.1.20
hazard
a condition that could lead to an accident

3.1.21
hazard analysis
the process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level

3.1.22
hazard log
the document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced

3.1.23
human error
a human action (mistake), which can result in unintended system behaviour/failure

3.1.24
implementation
the activity applied in order to transform the specified designs into their physical realisation

3.1.25
independence (functional)
freedom from any mechanism which can affect the correct operation of more than one function as a result of either systematic or random failure

3.1.26
independence (human)
freedom from involvement in the same intellectual, commercial and/or management entity

3.1.27
independence (physical)
freedom from any mechanism which can affect the correct operation of more than one system/sub-system/equipment as a result of random failures

3.1.28
individual risk
a risk which is related to a single individual only

3.1.29
maintainability
the probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources

3.1.30
maintenance
the combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform its required function

3.1.31
negation
enforcement of a safe state following detection of a hazardous fault

3.1.32
negation time
time span which begins when the existence of a fault is detected and ends when a safe state is enforced

3.1.33
product
a collection of elements, interconnected to form a system/sub-system/equipment, in a manner which meets the specified requirements

3.1.34
quality
a user perception of the attributes of a product

3.1.35
railway authority
the body with the overall accountability to a safety authority for operating a safe railway system

3.1.36
random failure integrity
the degree to which a system is free from hazardous random faults

3.1.37
random fault
unpredictable occurrence of a fault

3.1.38
redundancy
the provision of one or more additional measures, usually identical, to provide fault tolerance

3.1.39
reliability
the ability of an item to perform a required function under given conditions for a given period of time

3.1.40
repair
measures for re-establishing the required state of a system/sub-system/equipment after a fault/failure

3.1.41
risk
the combination of the frequency, or probability, and the consequence of a specified hazardous event

3.1.42
safe state
a condition which continues to preserve safety

3.1.43
safety
freedom from unacceptable levels of risk of harm

3.1.44
safety acceptance
the safety status given to a product by the final user

3.1.45
safety approval
the safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions