

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

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

Figure 3 – Structure of safety case	19
Figure 4 – Example of system life-cycle (from IEC 62278)	21
Figure 5 – Example of design and validation portion of system life-cycle	23
Figure 6 – Arrangements for independence	24
Figure 7 – Structure of technical safety report.....	29
Figure 8 – Typical safety acceptance and approval process	31
Figure 9 – Examples of dependencies between safety cases/safety approval	32
Figure A.1 – Safety requirements and safety integrity	34
Figure A.2 – Global process overview.....	36
Figure A.3 – Example risk analysis process	37
Figure A.4 – Definition of hazards with respect to the system boundary.....	38
Figure A.5 – Example hazard control process	40
Figure A.6 – Interpretation of failure and repair times	41
Figure A.7 – Treatment of functional independence by FTA	42
Figure A.8 – Relationship between SILs and techniques	45
Figure B.1 – Influences affecting the independence of items	52
Figure B.2 – Detection and negation of single faults.....	55
Figure C.1 – Example of a 4-terminal resistor, using a hybrid thick layer technique	65
Figure D.1 – Example of a fault analysis method	83
Table A.1 – SIL-table	45
Table C.1 – Resistors.....	68
Table C.2 – Capacitors.....	69
Table C.3 – Electromagnetic components.....	69
Table C.4 – Diodes	71
Table C.5 – Transistors	72
Table C.6 – Controlled rectifiers	73
Table C.7 – Surge suppressors	74
Table C.8 – Opto-electronic components	75
Table C.9 – Filters.....	76
Table C.10 – Interconnection assemblies	76
Table C.11 – Fuses	77
Table C.12 – Switches and push/pull buttons.....	77
Table C.13 – Lamps	77
Table C.14 – Batteries.....	78
Table C.15 – Transducers/sensors (not including those with internal electronic circuitry).....	78
Table C.16 – Integrated circuits.....	78
Table D.1 – Examples of measures to detect faults in large-scale integrated circuits by means of periodic on-line testing, with comparison (SW or HW), in a 2-out-of- <i>n</i> system	84
Table E.1 – Safety planning and quality assurance activities (referred to in 5.2 and 5.3.4).....	88
Table E.2 – System requirements specification (referred to in 5.3.6)	88
Table E.3 – Safety organisation (referred to in 5.3.3)	89
Table E.4 – Architecture of system/sub-system/equipment (referred to in 5.4).....	89

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

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.

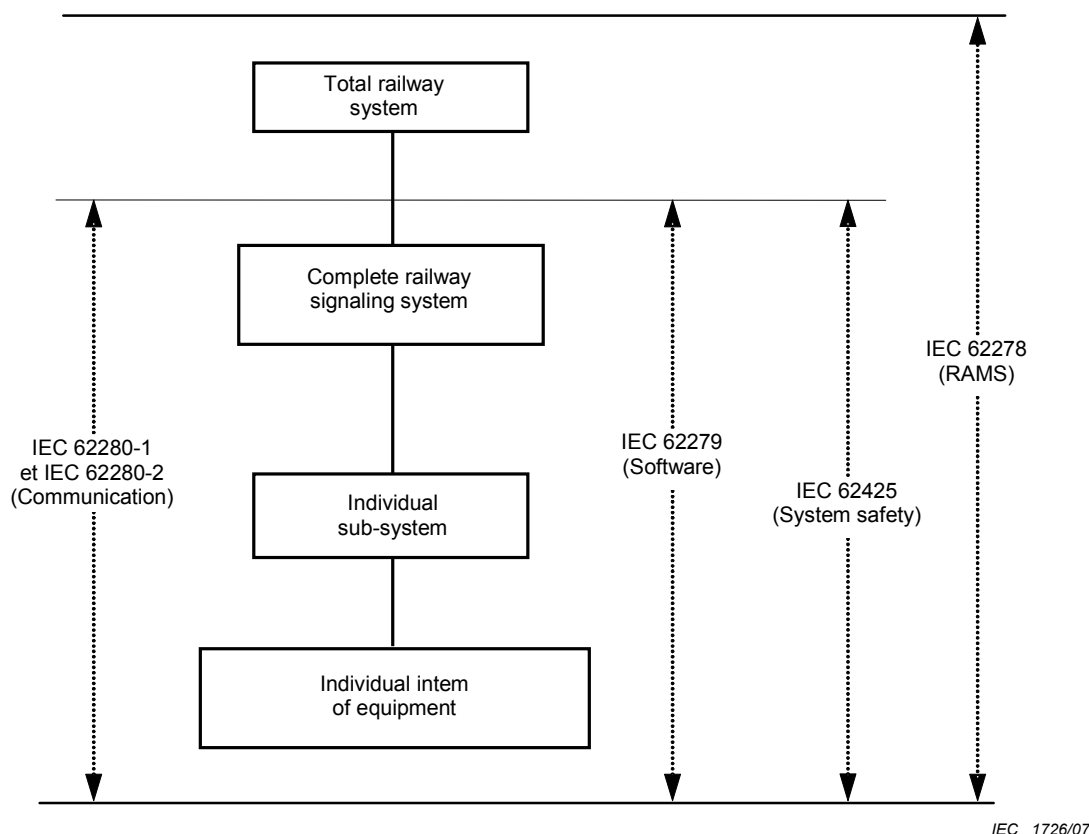


Figure 1 – Scope of the main IEC railway application standards

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

3.1.46

safety authority

the body responsible for delivering the authorisation for the operation of the safety related system

3.1.47

safety case

the documented demonstration that the product complies with the specified safety requirements

3.1.48

safety integrity

the ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period of time

3.1.49

safety integrity level

a number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

3.1.50

safety life-cycle

the additional series of activities carried out in conjunction with the system life-cycle for safety-related systems

3.1.51

safety management

the management structure which ensures that the safety process is properly implemented

3.1.52

safety plan

the implementation details of how the safety requirements of the project will be achieved

3.1.53

safety process

the series of procedures that are followed to enable all safety requirements of a product to be identified and met

3.1.54

safety-related

carries responsibility for safety

3.1.55

signalling system

particular kind of system used on a railway to control and protect the operation of trains

3.1.56

stress profile

the degree and number of external influences which a product can withstand whilst performing its required functionality

3.1.57

sub-system

a portion of a system which fulfils a specialised function

**3.1.58
system**

a set of sub-systems which interact according to a design

**3.1.59
systematic failure integrity**

the degree to which a system is free from unidentified hazardous errors and the causes thereof

**3.1.60
systematic fault**

an inherent fault in the specification, design, construction, installation, operation or maintenance of a system, sub-system or equipment

**3.1.61
system life-cycle**

the series of activities occurring during a period of time that starts when a system is conceived and ends at decommissioning when the system is no longer available for use

**3.1.62
technical safety report**

documented technical evidence for the safety of the design of a system/sub-system/equipment

**3.1.63
validation**

the activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements

**3.1.64
verification**

the activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements

3.2 Abbreviations

ATP	automatic train protection
CENELEC	European committee for electrotechnical standardisation
CCF	common-cause failure
DC	direct current
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EN	European standard
ESD	electrostatic discharge
FMEA	failure modes and effects analysis
FR	failure rate
FTA	fault tree analysis
H	hazard
HW	hardware
IEC	International electrotechnical commission
IRSE	Institution of railway signal engineers
ISO	International standards organisation
RAMS	reliability, availability, maintainability and safety

SDR	safe down rate
SDT	safe down time
SIL	safety integrity level
SW	software
THR	tolerable hazard rate
UIC	International union of railways

4 Overall framework of this standard

Clause 5 of this International Standard requires that a systematic, documented approach be taken to

- evidence of quality management,
- evidence of safety management,
- evidence of functional and technical safety,
- safety acceptance and approval.

Annex A (normative) defines the interpretation and use of safety integrity levels.

Annex B (normative) contains detailed technical requirements for safety-related systems/sub-systems/equipment.

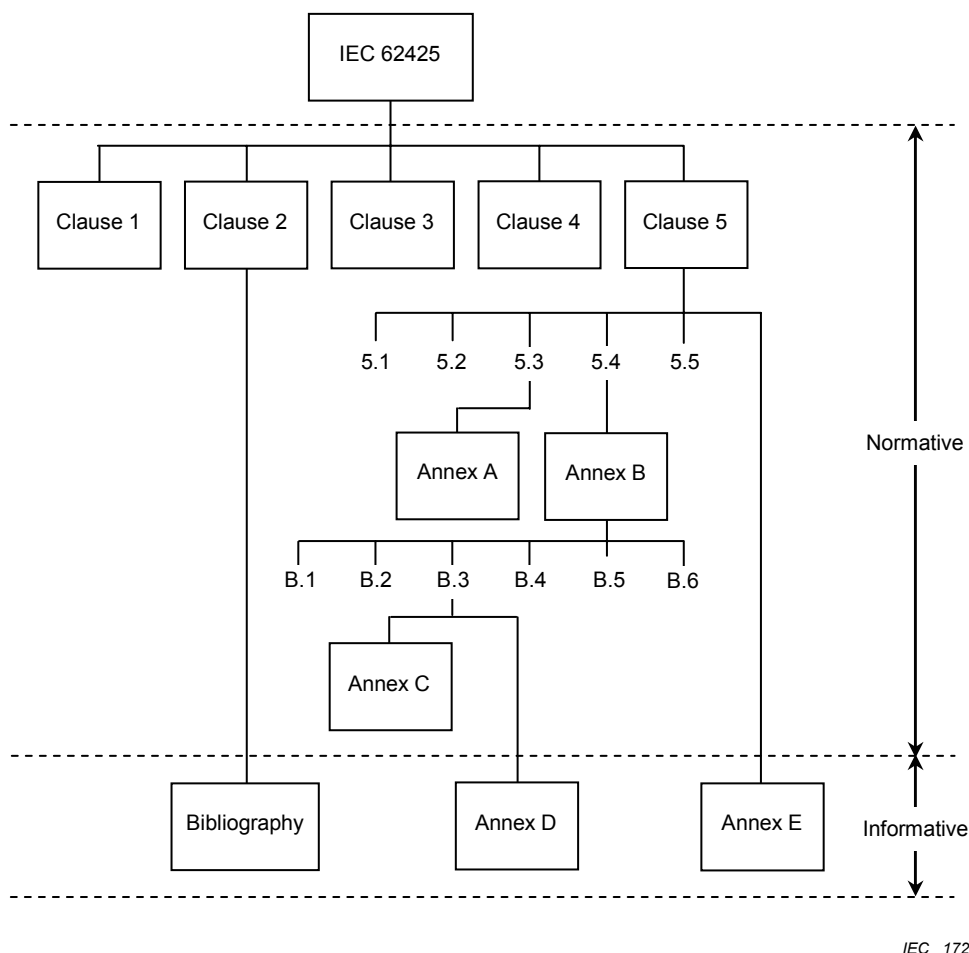
Annex C (normative) contains procedures and information for identifying the credible failure modes of hardware components.

Annex D (informative) contains supplementary technical information.

Annex E (informative) contains tables of techniques/measures to be used for various levels of safety integrity.

The bibliography contains references to documents that have been consulted during the preparation of this standard.

The structure of this standard is summarised in Figure 2.



IEC 1727/07

Figure 2 – Structure of IEC 62425

5 Conditions for safety acceptance and approval

5.1 The safety case

This standard defines the conditions that shall be satisfied in order for a safety-related electronic railway system/sub-system/equipment to be accepted as adequately safe for its intended application.

The conditions for safety acceptance are presented in this standard under three subclauses, namely

- 5.2 Evidence of quality management
- 5.3 Evidence of safety management
- 5.4 Evidence of functional and technical safety

All of these conditions shall be satisfied, at equipment, sub-system and system levels, before the safety-related system can be accepted as adequately safe.

The documentary evidence that these conditions have been satisfied shall be included in a structured safety justification document, known as the safety case. The safety case forms part of the overall documentary evidence to be submitted to the relevant safety authority in order to obtain safety approval for a generic product, a class of application or a specific application. For an explanation of the safety approval process, see 5.5.

The safety case contains the documented safety evidence for the system/sub-system/equipment, and shall be structured as follows:

– Part 1 Definition of system (or sub-system/equipment)

This shall precisely define or reference the system/sub-system/equipment to which the safety case refers, including version numbers and modification status of all requirements, design and application documentation.

– Part 2 Quality management report

This shall contain the evidence of quality management, as specified in 5.2.

– Part 3 Safety management report

This shall contain the evidence of safety management, as specified in 5.3.

– Part 4 Technical safety report

This shall contain the evidence of functional and technical safety, as specified in 5.4.

– Part 5 Related safety cases

This shall contain references to the safety cases of any sub-systems or equipment on which the main safety case depends.

It shall also demonstrate that all the safety-related application conditions specified in each of the related sub-system/equipment safety cases are

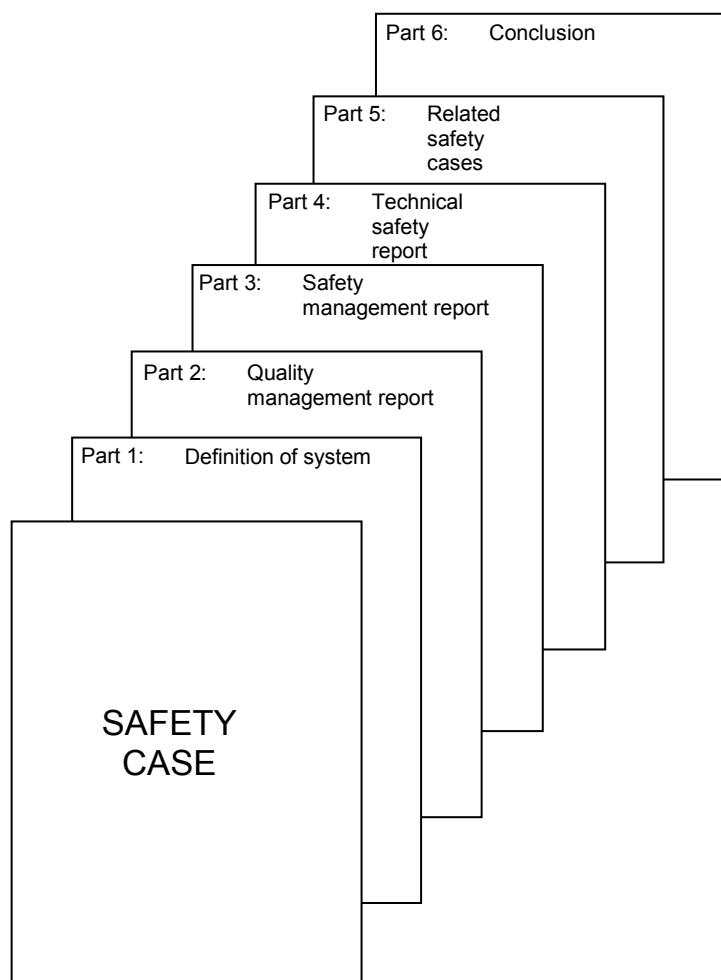
- either fulfilled in the main safety case,
- or carried forward into the safety-related application conditions of the main safety case.

– Part 6 Conclusion

This shall summarise the evidence presented in the previous parts of the safety case, and argue that the relevant system/sub-system/equipment is adequately safe, subject to compliance with the specified application conditions.

The structure of the safety case is illustrated in Figure 3.

Large volumes of detailed evidence and supporting documentation need not be included in the safety case and in its parts, provided precise references are given to such documents and provided the base concepts used and the approaches taken are clearly specified.



IEC 1728/07

Figure 3 – Structure of safety case

5.2 Evidence of quality management

The first condition for safety acceptance that shall be satisfied is that the quality of the system, sub-system or equipment has been, and shall continue to be, controlled by an effective quality management system throughout its life-cycle. Documentary evidence to demonstrate this shall be provided in the quality management report, which forms Part 2 of the safety case.

The purpose of the quality management system is to minimise the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system, sub-system or equipment.

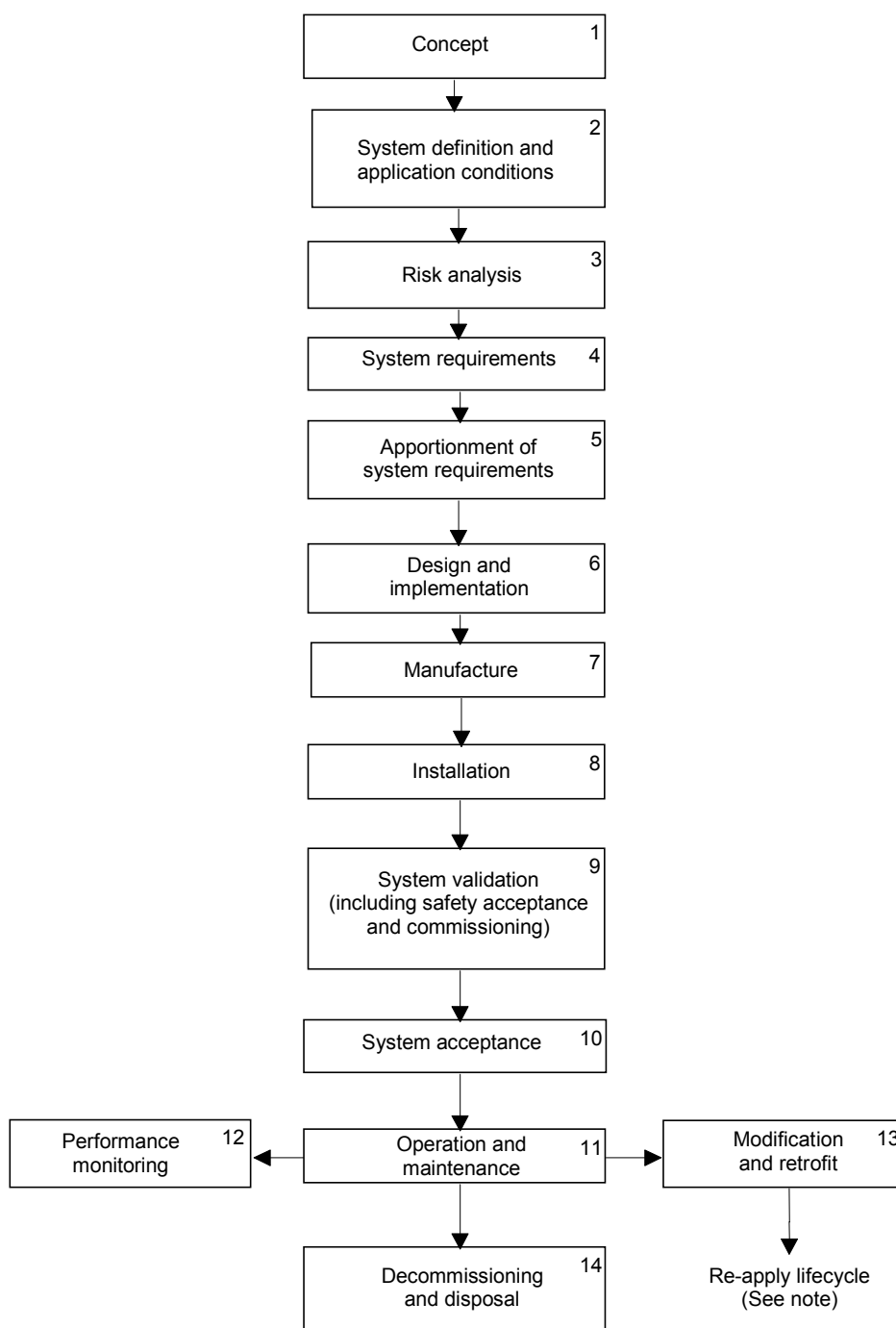
The quality management system shall be applicable throughout the system/sub-system/equipment life-cycle, as defined in IEC 62278. An example of a system life-cycle diagram (from IEC 62278) is reproduced as Figure 4.

NOTE Examples of aspects which should be controlled by the quality management system and included in the quality management report:

- organisational structure;
- quality planning and procedures;
- specification of requirements;
- design control;
- design verification and reviews;

- application engineering;
- procurement and manufacture;
- product identification and traceability;
- handling and storage;
- inspection and testing;
- non-conformance and corrective action;
- packaging and delivery;
- installation and commissioning;
- operation and maintenance;
- quality monitoring and feedback;
- documentation and records;
- configuration management/change control;
- personnel competency and training;
- quality audits and follow-up;
- decommissioning and disposal.

Compliance with the requirements for quality management is mandatory for safety integrity levels 1 to 4 inclusive (see Annex A for explanation of safety integrity levels). However, the depth of the evidence presented and the extent of the supporting documentation should be appropriate to the safety integrity level of the system/sub-system/equipment under scrutiny (see Table E.1 and Table E.8 for guidance on evidence required for each safety integrity level). The requirements for safety integrity level 0 (non-safety-related) are outside the scope of this safety standard.



IEC 1729/07

NOTE The phase at which a modification enters the life-cycle will be dependent upon both the system being modified and the specific modification under consideration.

**Figure 4 – Example of system life-cycle
(from IEC 62278)**

5.3 Evidence of safety management

5.3.1 Introduction

The second condition for safety acceptance which shall be satisfied is that the safety of the system, sub-system or equipment has been, and shall continue to be, managed by means of an effective safety management process, which should be consistent with the management

process for RAMS described in IEC 62278. The purpose of this process is to further reduce the incidence of safety-related human errors throughout the life-cycle, and thus minimise the residual risk of safety-related systematic faults. The elements of the safety management process are briefly summarised in 5.3.2 to 5.3.13 below.

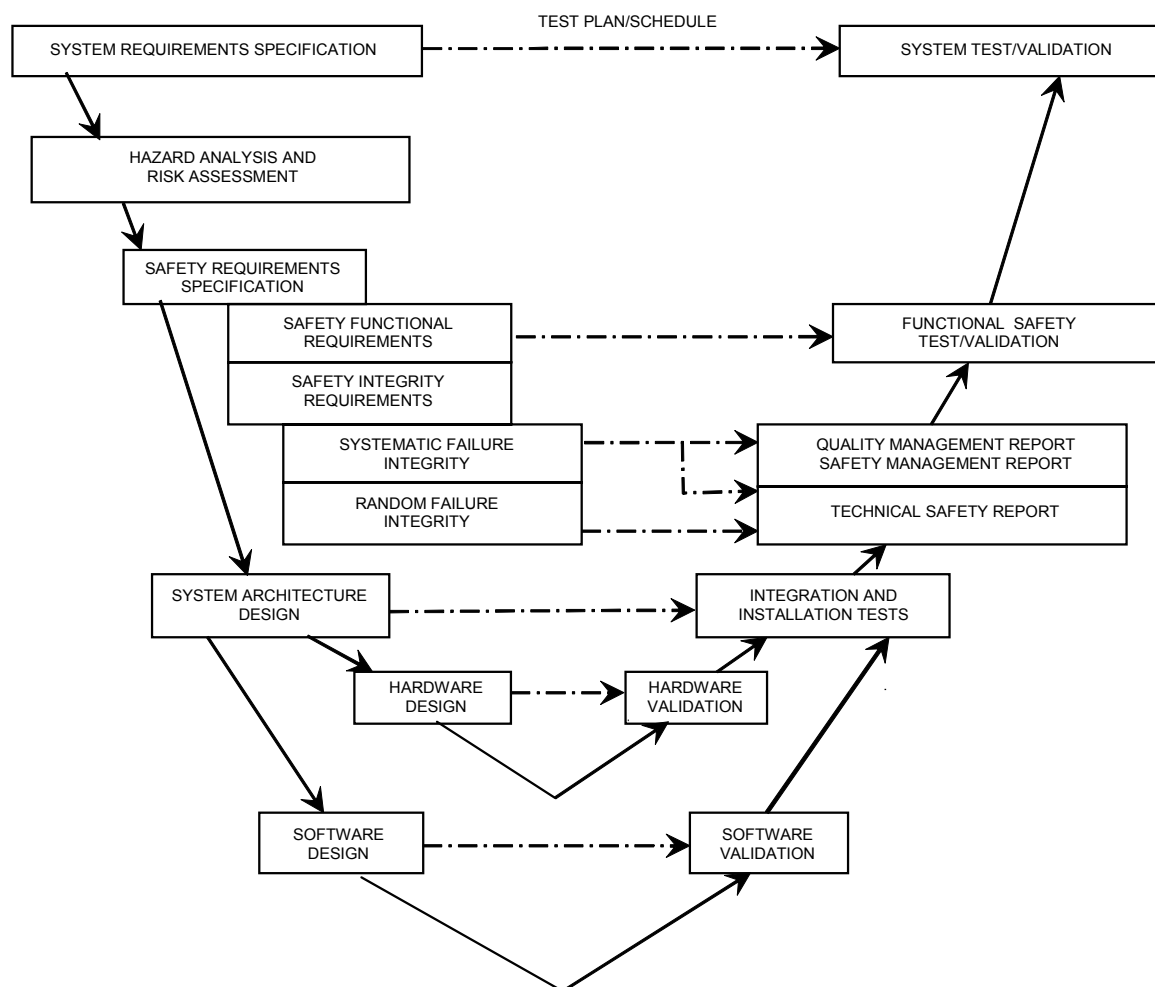
Documentary evidence to demonstrate compliance with all elements of the safety management process throughout the life-cycle shall be provided in the safety management report, which forms Part 3 of the safety case. Large volumes of detailed evidence and supporting documentation need not be included, provided precise references are given to such documents.

The use of this safety management process is mandatory for safety integrity levels 1 to 4 inclusive (see Annex A for explanation of safety integrity levels). However, the depth of the evidence presented and the extent of the supporting documentation should be appropriate to the safety integrity level of the system/sub-system/equipment under scrutiny. The requirements for safety integrity level 0 (non-safety-related) are outside the scope of this safety standard.

In all cases, the hazard analysis and risk assessment processes defined in IEC 62278 are necessary, in order to identify the required level of safety integrity for each particular situation. This includes those cases where the analysis and assessment reveal that a safety integrity level of zero may be assigned; however, once this conclusion has been reached (i.e. that the situation is non-safety-related), and provided it remains at level zero, this safety standard ceases to be applicable.

5.3.2 Safety life-cycle

The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle; this should be consistent with the system life-cycle defined in IEC 62278, which is reproduced as Figure 4. The design and validation part of the system life-cycle can be viewed as a "top-down" phase followed by a "bottom-up" phase, (i.e. a "V"-diagram), an example of which is shown in Figure 5.

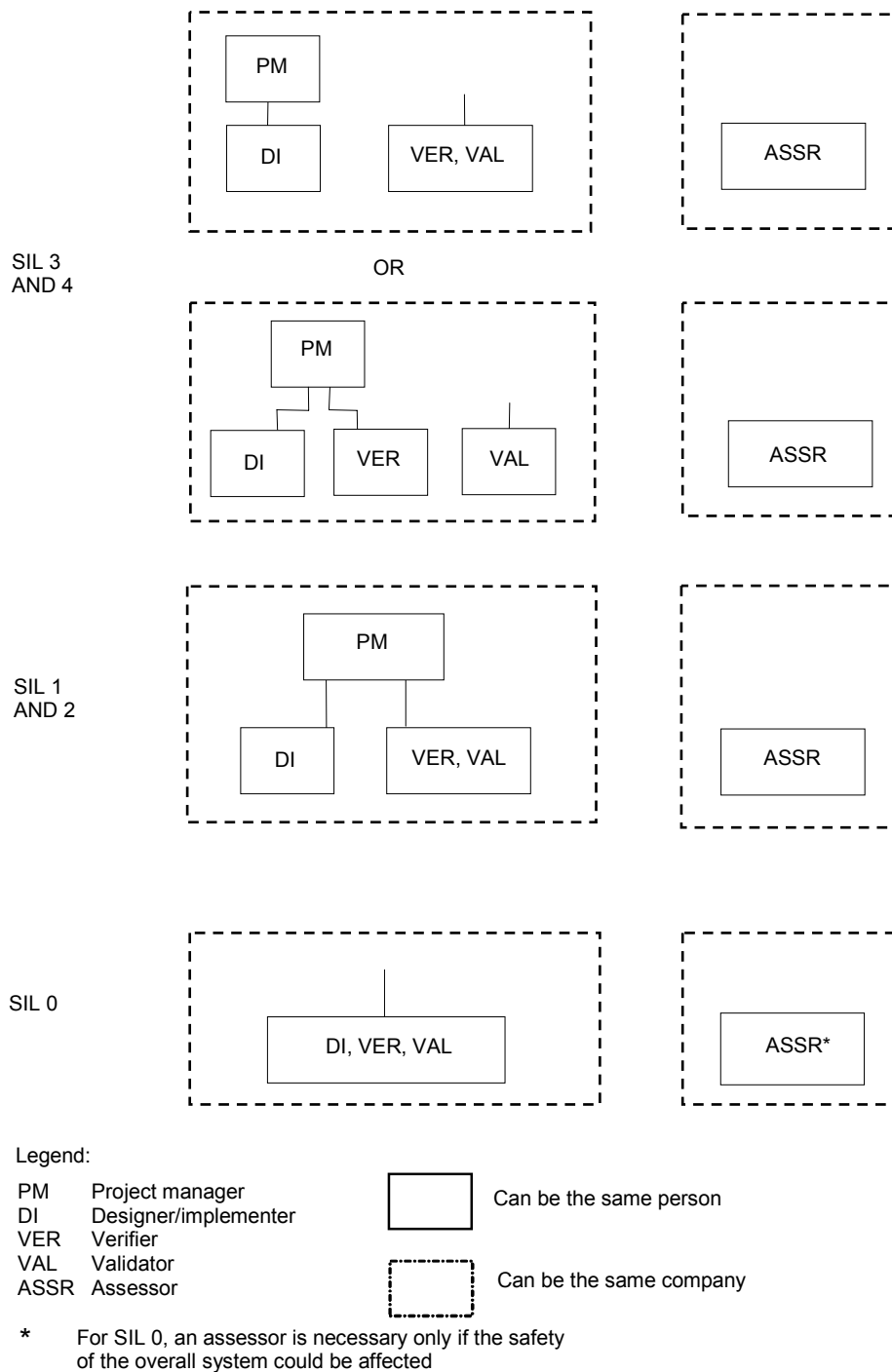


IEC 1730/07

Figure 5 – Example of design and validation portion of system life-cycle

5.3.3 Safety organisation

The safety management process shall be implemented under the control of an appropriate safety organisation, using competent personnel assigned to specific roles. Assessment and documentation of personnel competence, including technical knowledge, qualifications, relevant experience and appropriate training, shall be carried out in accordance with recognised standards. An appropriate degree of independence shall be provided between different roles, as shown in Figure 6. See also Table E.3, for guidance on the safety organisation required for each safety integrity level.



IEC 1731/07

Figure 6 – Arrangements for independence

5.3.4 Safety plan

A safety plan shall be drawn up at the start of the life-cycle. This plan shall identify the safety management structure, safety-related activities and approval mile-stones throughout the life-cycle, and shall include the requirements for review of the safety plan at appropriate intervals. The safety plan shall be updated and reviewed if subsequent alterations or additions are made to the original system/sub-system/equipment. If any such change is made, the effect on safety shall be assessed, starting at the appropriate point in the life-cycle. See Table E.1 for guidance on safety plans for each safety integrity level.

The safety plan shall deal with all aspects of the system/sub-system/equipment, including both hardware and software. IEC 62279 shall be referenced for software aspects.

The safety plan should include a safety case plan, which identifies the intended structure and principal components of the final safety case.

5.3.5 Hazard log

A hazard log shall be created and maintained throughout the safety life-cycle, as explained in IEC 62278. It shall include a list of identified hazards, together with associated risk classification and risk control information for each hazard. The hazard log shall be updated if any modification or alteration is made to the system, sub-system or equipment.

5.3.6 Safety requirements specification

The specific safety requirements for each system/sub-system/equipment, including safety functions and safety integrity, shall be identified and documented in the safety requirements specification. This shall be achieved by means of

- hazard identification and analysis,
- risk assessment and classification,
- allocation of safety integrity levels,

as explained in IEC 62278. Some information concerning safety integrity levels for railway electronic systems is contained in Annex A.

NOTE The safety requirements specification may be included in the system/sub-system/equipment functional requirements specification or may be written as a separate document. See Table E.2, for guidance on system requirements specifications for each safety integrity level.

5.3.7 System/sub-system/equipment design

This phase of the life-cycle shall create a design which fulfils the specified operational and safety requirements. A top-down, structured design methodology shall be used, with rigorously controlled and reviewed documentation. In particular, the relationship between hardware and software, as represented by the software requirements specification and software/hardware integration, shall be strictly managed, and IEC 62279 shall be adhered to. Table E.7 gives guidance on design and development of system/sub-system/equipment for each safety integrity level.

5.3.8 Safety reviews

Safety reviews shall be carried out at appropriate stages in the life-cycle. Such reviews shall be specified in the safety plan, and their results fully documented. Any alteration or extension to the system, sub-system or equipment shall also be subject to review.

5.3.9 Safety verification and validation

The safety plan shall include or reference plans for verifying that each phase of the life-cycle satisfies the specific safety requirements identified in the previous phase, and for validating the completed system/sub-system/equipment against its original safety requirements specification.

These activities shall be carried out and fully documented, including appropriate testing and safety analyses. They shall be repeated as appropriate in the event of any subsequent modification or addition to the system/sub-system/equipment.

The degree of independence necessary for the verifier and the validator shall be in accordance with the safety integrity level of the system/sub-system/equipment under scrutiny. This is

shown in Figure 6. Table E.9 gives guidance on verification and validation techniques/measures for each safety integrity level.

At the discretion of the safety authority, the assessor may be part of the supplier's organisation or of the customer's organisation but, in such cases, the assessor shall

- be authorised by the safety authority,
- be totally independent from the project team,
- report directly to the safety authority.

5.3.10 Safety justification

The evidence that the system/sub-system/equipment meets the defined conditions for safety acceptance shall be presented in a structured safety justification document known as the safety case, as explained in 5.1.

5.3.11 System/sub-system/equipment handover

Prior to handover of the system/sub-system/equipment to a railway authority, the conditions for safety acceptance and safety approval defined in 5.5 shall be satisfied, including submission of the safety case and the safety assessment report.

5.3.12 Operation and maintenance

Following handover, the procedures, support systems and safety monitoring defined in the safety plan and in Section 5 of the technical safety report (part of the safety case) shall be adhered to.

During the operational life of a system, change requests may be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation. Where a change request results in a modification which could affect the safety of the system, or associated systems, or the environment, the appropriate portion of the safety life-cycle shall be repeated to ensure that the implemented modification does not unacceptably reduce the level of safety. Table E.10 gives guidance on application, operation and maintenance for each safety integrity level.

5.3.13 Decommissioning and disposal

At the end of the operational life of a system, its decommissioning and disposal shall be carried out in accordance with the measures defined in the safety plan and in Section 5 of the technical safety report (part of the safety case).

5.4 Evidence of functional and technical safety

In addition to the evidence of quality and safety management, described in 5.2 and 5.3, a third condition shall be satisfied before a system/sub-system/equipment can be accepted as adequately safe for its intended application. This consists of technical evidence for the safety of the design, which shall be documented in the technical safety report. This document forms Part 4 of the safety case for the system/sub-system/equipment, as explained in 5.1.

The technical safety report is mandatory for safety integrity levels 1 to 4 inclusive (see Annex A for explanation of safety integrity levels). However, the depth of the information and the extent of the supporting documentation should be appropriate to the safety integrity level of the system/sub-system/equipment under scrutiny. The requirements for safety integrity level 0 (non-safety-related) are outside the scope of this safety standard.

The technical safety report shall explain the technical principles which assure the safety of the design, including (or giving references to) all supporting evidence (for example, design principles and calculations, test specifications and results, and safety analyses).

The technical safety report shall be arranged under the following headings:

a) Section 1: Introduction

This section shall provide an overview description of the design, including a summary of the technical safety principles that are relied on for safety and the extent to which the system/sub-system/equipment is claimed to be safe in accordance with this standard.

This section shall also indicate the standards (and their issues) used as the basis for the technical safety of the design. In the case of modifications or additions to equipment already in service, or in standard production, or at a completed stage of development, then, as an exception, the issues of standards used for the original design may be used as a basis, these already having been accepted in the approval of the original equipment. This may be applied only if, by taking into consideration the latest issues of the standards, further modifications to the existing equipment would be required, or unjustifiably high costs for the change would be incurred. Reasons justifying use of this statement shall be given.

b) Section 2: Assurance of correct functional operation

This section shall contain all the evidence necessary to demonstrate correct operation of the system/sub-system/equipment under fault-free normal conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements.

The following aspects shall be included, for which more detailed requirements are contained in Clause B.2:

- 2.1 System architecture description (see B.2.1 and Table E.4);
- 2.2 Definition of interfaces (see B.2.2);
- 2.3 Fulfilment of system requirements specification (see B.2.3);
- 2.4 Fulfilment of safety requirements specification (see B.2.4);
- 2.5 Assurance of correct hardware functionality (see B.2.5);
- 2.6 Assurance of correct software functionality (see B.2.6).

c) Section 3: Effects of faults

This section shall demonstrate that the system/sub-system/equipment continues to meet its specified safety requirements, including the quantified safety target, in the event of random hardware faults.

In addition, a systematic fault could still exist, despite the quality and safety management processes defined in 5.2 and 5.3. This section shall demonstrate which technical measures have been taken to reduce the consequent risk to an acceptable level.

This section shall also include demonstration that faults in any system/sub-system/equipment having a safety integrity level lower than that of the overall system, including level 0, cannot reduce the safety of the overall system.

The following headings shall be used in this section, for which more detailed requirements are contained in Clause B.3. Guidance is also given in Table E.5 and Table E.6.

- 3.1 Effects of single faults (see B.3.1);
- 3.2 Independence of items (see B.3.2);
- 3.3 Detection of single faults (see B.3.3);

- 3.4 Action following detection (including retention of safe state) (see B.3.4);
- 3.5 Effects of multiple faults (see B.3.5);
- 3.6 Defence against systematic faults (see B.3.6).

d) Section 4: Operation with external influences

This section shall demonstrate that when subjected to the external influences defined in the system requirements specification, the system/sub-system/equipment

- continues to fulfil its specified operational requirements,
- continues to fulfil its specified safety requirements (including fault conditions).

The safety case is therefore valid only within the specified range of external influences, as defined in the system requirements specification. Safety is not assured outside these limits, unless additional special measures are provided.

The methods used to withstand the specified external influences shall be fully explained and justified.

More detailed requirements are contained in Clause B.4.

e) Section 5: Safety-related application conditions

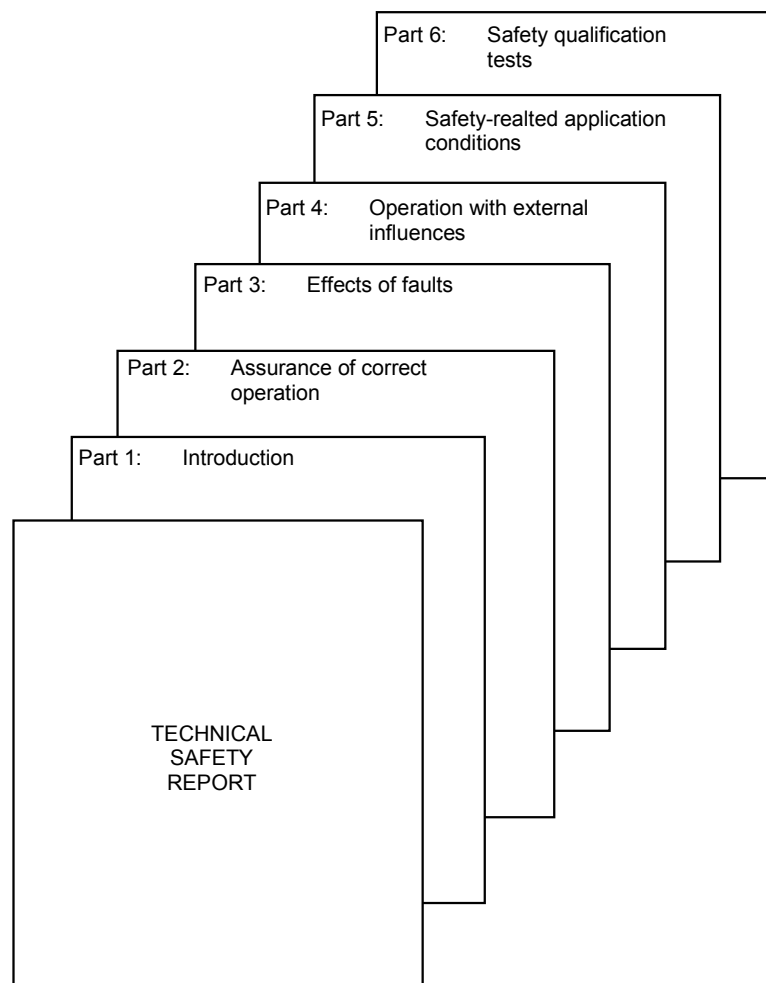
This section shall specify (or reference) the rules, conditions and constraints which shall be observed in the application of the system/sub-system/equipment. This shall include the application conditions contained in the safety case of any related sub-system or equipment.

More detailed requirements are contained in Clause B.5. Guidance is also given in Table E.10.

f) Section 6: Safety qualification tests

This section shall contain evidence to demonstrate successful completion, under operational conditions, of the safety qualification tests. These are explained in Clause B.6.

The structure of the technical safety report is illustrated in Figure 7.



IEC 1732/07

Figure 7 – Structure of technical safety report

5.5 Safety acceptance and approval

This subclause defines the safety acceptance and approval process for safety-related electronic system/sub-system/equipment. Except where considered appropriate, it does not specify who should carry out the work at each stage, since this may vary in different circumstances.

5.5.1 Introduction

As explained in 5.1, three conditions shall be satisfied before a safety-related electronic railway system/sub-system/equipment can be accepted as adequately safe for its intended application:

- evidence of quality management;
- evidence of safety management;
- evidence of functional and technical safety.

These three conditions have been explained in 5.2, 5.3 and 5.4.

The evidence of quality management, safety management and functional/technical safety shall be included in the safety case, as shown in 5.1 and Figure 3.

Three different categories of safety case can be considered:

- generic product safety case (independent of application)
A generic product can be re-used for different independent applications;
- generic application safety case (for a class of application)
A generic application can be re-used for a class/type of application with common functions;
- specific application safety case (for a specific application)
A specific application is used for only one particular installation.

It is essential to demonstrate for each "specific" application that the environmental conditions and context of use are compatible with the "generic" application conditions (see 5.5.4).

In all three categories, the structure of the safety case and the procedure for obtaining safety approval are basically the same. However, there is an additional factor for specific applications: in this category, separate safety approval is needed for the application design of the system and for its physical implementation (e.g., manufacture, installation, test, and facilities for operation and maintenance). For this reason, the safety case for specific applications shall be divided into two portions:

- the application design safety case: this shall contain the safety evidence for the theoretical design of the specific application;
- the physical implementation safety case: this shall contain the safety evidence for the physical implementation of the specific application.

Both portions shall be structured as shown in 5.1 and Figure 3.

5.5.2 Safety approval process

Before an application for safety approval can be considered, an independent safety assessment of the system/sub-system/equipment and its safety case shall be carried out, to provide additional assurance that the necessary level of safety has been achieved. Its results should be presented in a safety assessment report. The report should explain the activities carried out by the safety assessor to determine how the system/sub-system/equipment, (hardware and software) has been designed to meet its specified requirements, and possibly specify some additional conditions for the operation of the system/sub-system/equipment. The depth of the safety assessment, and the degree of independence with which it is carried out, are based on the results of the risk classification, as explained in IEC 62278. Specific tests may be required by the safety assessor in order to increase confidence.

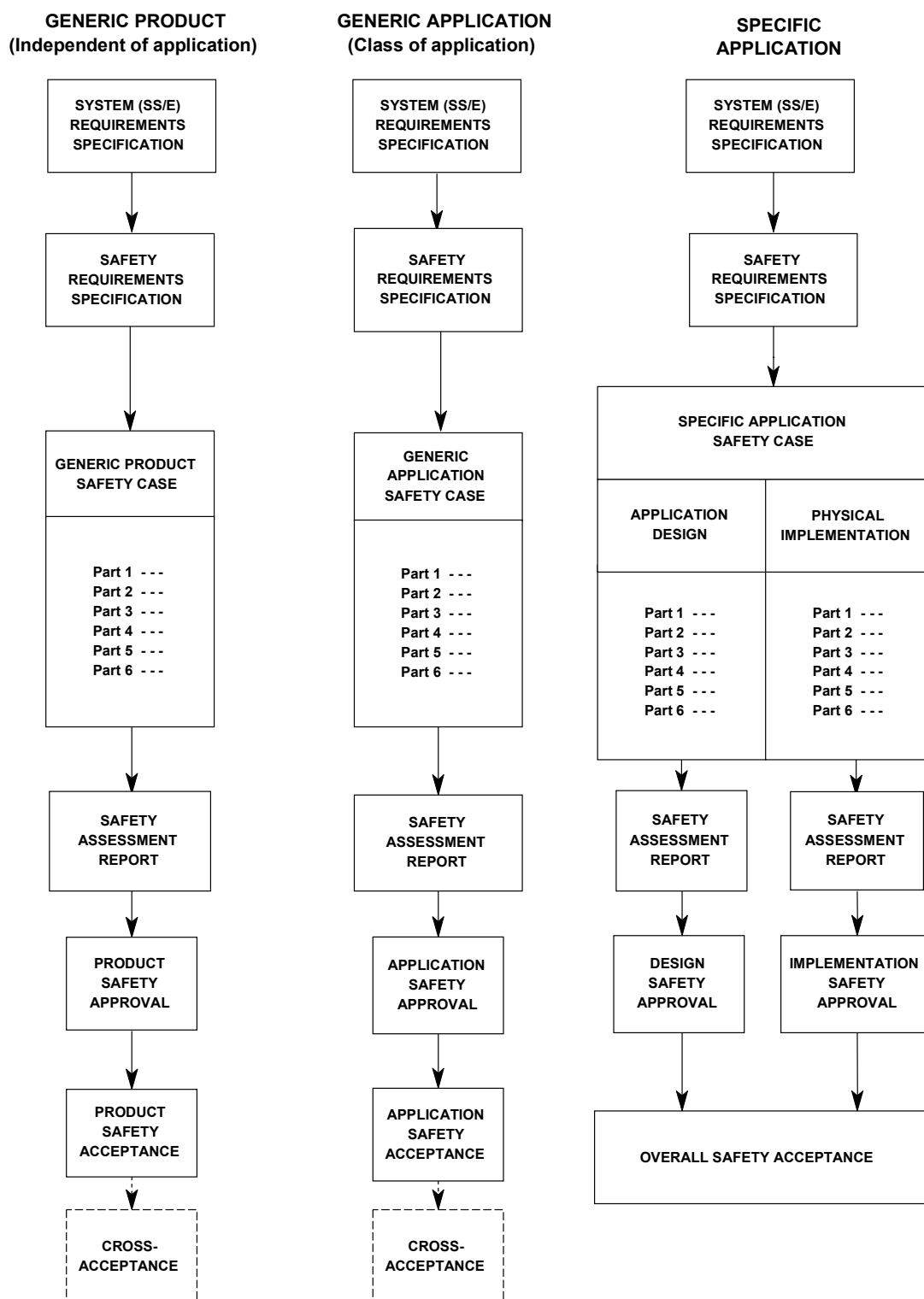
The overall documentary evidence shall consist of

- the system (or sub-system/equipment) requirements specification,
- the safety requirements specification,
- the safety case, including
 - Part 1: Definition of system/sub-system/equipment,
 - Part 2: Quality management report (evidence of quality management),
 - Part 3: Safety management report (evidence of safety management),
 - Part 4: Technical safety report (evidence of functional/technical safety),
 - Part 5: Related safety cases (if applicable),
 - Part 6: Conclusion,
- the safety assessment report.

Provided all the conditions for safety acceptance have been satisfied, as demonstrated by the safety case, and subject to the results of the independent safety assessment, the system/sub-system/equipment may be granted safety approval by the relevant safety authority. Approval may be subject to the fulfilment of additional conditions (temporary or permanent) imposed by the safety assessor.

For a generic product (i.e. independent of application), and for a generic application (i.e. class of application), it should be possible for safety approval granted by one safety authority to be accepted by other safety authorities (i.e.: cross-acceptance). This is not considered possible for specific applications.

The safety approval process, for all three categories of safety case, is illustrated in Figure 8.



IEC 1733/07

Figure 8 – Typical safety acceptance and approval process

5.5.3 After safety approval

After a system/sub-system/equipment has received safety approval, any subsequent modification shall be controlled using the same quality management, safety management and functional/technical safety criteria as would be used for a new design. All relevant documentation, including the safety case, shall be updated or supplemented by additional documentation, and the modified design shall be submitted for approval.

Once an installed system/sub-system/equipment has been commissioned, appropriate procedures, support systems and safety monitoring, as defined in the safety plan and in Section 5 of the technical safety report (part of the safety case), shall be used to ensure continued safe operation throughout its working life, including operation, maintenance, alteration, extension and eventual decommissioning. These activities shall be controlled using the same quality management, safety management and technical safety criteria as for the original design. All relevant documentation shall be kept up-to-date, including the safety case, and any alterations or extensions shall be submitted for approval.

5.5.4 Dependency between safety approvals

As mentioned in 5.1, the safety case for a system may depend on the safety cases of other sub-systems or equipment. In such circumstances, safety approval of the main system is not possible without previous safety approval of the related sub-systems/equipment.

If safety approval has been obtained for a generic product, or for a generic application, a reference may be made to this in the application for safety approval of a specific application; it is not necessary to repeat the generic approval process for each application. This dependency between safety approvals is illustrated in Figure 9.

A safety case may be based on the demonstration that the proposed specific application is technically equivalent to an existing application with specific safety approval. A new safety approval for this specific application is necessary.

It is essential to ensure in such examples of dependency that the safety-related application conditions stated in the technical safety report of each safety case are fulfilled in the higher-level safety case, or else are carried forward into the safety-related application conditions of the higher-level safety case.

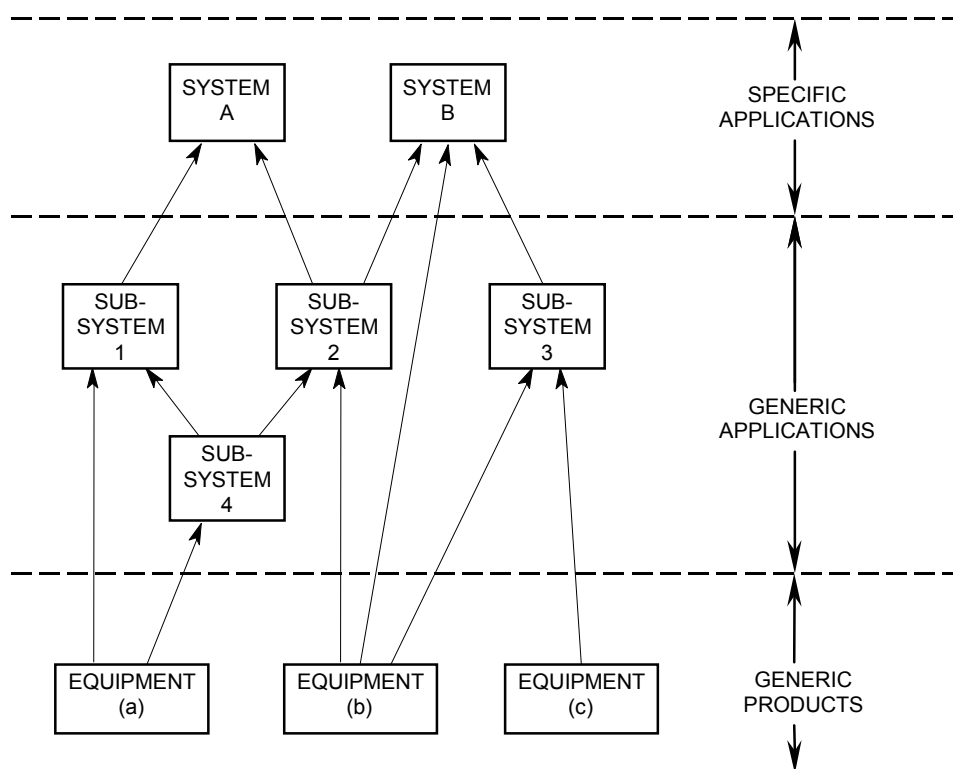


Figure 9 – Examples of dependencies between safety cases/safety approvals

IEC 1734/07

Annex A (normative)

Safety integrity levels

A.1 Introduction

This annex gives details for the derivation, allocation and implementation of safety requirements and safety integrity and the use of safety integrity levels in safety-related systems for railway application.

The tolerable hazard rates (THR) in the form of quantified safety targets for each particular railway application are the responsibility of the relevant railway authority, and are not defined by this standard.

The safety management process is defined in IEC 62278.

A.2 Safety requirements

The system requirements specification (or sub-system/equipment as appropriate) may be considered in two parts (see Figure A.1):

- requirements which are not related to safety (including operational functional requirements);
- requirements which are related to safety.

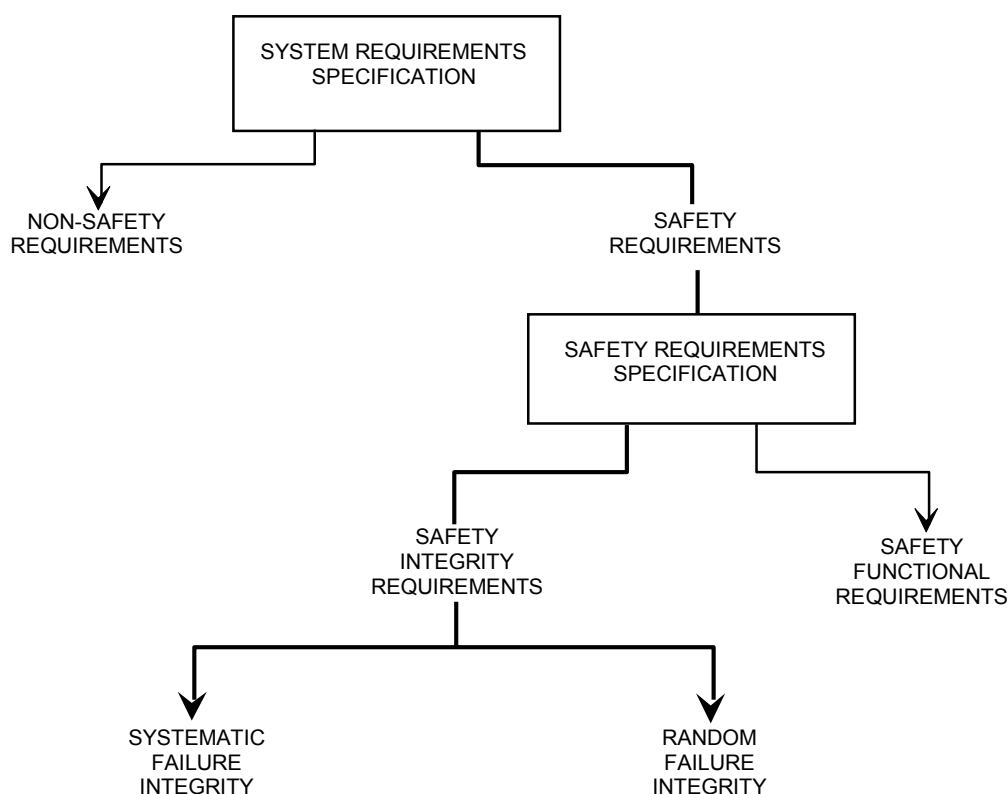
Requirements which are related to safety are usually called safety requirements. These may be contained in a separate safety requirements specification.

Safety requirements may be considered in two parts:

- safety functional requirements;
- safety integrity requirements.

Safety functional requirements are the actual safety-related functions which the system, sub-system or equipment is required to carry out.

Safety integrity requirements define the level of safety integrity required for each safety-related function.



IEC 1735/07

Figure A.1 – Safety requirements and safety integrity

A.3 Safety integrity

Safety integrity relates to the ability of a safety-related system to achieve its required safety functions. The higher the safety integrity, the lower the likelihood that it will fail to carry out the required safety functions.

Safety integrity comprises two parts (see Figure A.1):

- systematic failure integrity;
- random failure integrity.

It is necessary to satisfy both the systematic and the random failure integrity requirements if adequate safety integrity is to be achieved.

NOTE Failures caused by environmental conditions (e.g.: EMC, temperature, vibration, etc.) should be included within systematic and random failure integrity as appropriate.

Systematic failure integrity is the non-quantifiable part of the safety integrity and relates to hazardous systematic faults (hardware or software). Systematic faults are caused by human errors in the various stages of the system/sub-system/equipment life-cycle.

- EXAMPLE**
- specification errors;
 - design errors;
 - manufacturing errors;
 - installation errors;

- operation errors;
- maintenance errors;
- modification errors.

Systematic failure integrity is achieved by means of the quality management and safety management conditions specified in 5.2 and 5.3.

Technical defences against systematic faults are included in the technical safety conditions specified in 5.4.

Because it is not possible to assess systematic failure integrity by quantitative methods, safety integrity levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realisation of a system to a stated integrity level (see Annex E).

Random failure integrity is that part of the safety integrity which relates to hazardous random faults, in particular random hardware faults, which are the result of the finite reliability of hardware components.

The achievement of random failure integrity is included within the technical safety conditions specified in 5.4.

A quantified assessment of random failure integrity shall be carried out, by means of probabilistic calculations. These are based on known data for hardware component failure rates and failure modes, and disclosure times of random hardware failures. In the case of components with inherent physical properties (see Annex C), a hazardous failure rate of zero is generally assumed, although a residual risk of hazardous failure may exist and should be defended against as specified in 5.4 and B.3.6.

The allocation of safety integrity requirements and of safety integrity levels are described in Clauses A.4 and A.5 respectively.

A.4 Allocation of safety integrity requirements

A methodology to determine safety integrity requirements for railway signalling equipment, taking into account both the operational environment and the architectural design of the signalling system, shall be systematically applied.

At the heart of this approach is a well defined interface between the operational environment and the signalling system. From the safety point of view, this interface is defined by a list of hazards and associated tolerable hazard rates within the system. It should be noted that the purpose of this approach is not to limit co-operation between suppliers and railways authorities but to clarify responsibilities and interfaces.

From this interface, the analysis proceeds as follows:

- bottom-up analysis leads to the identification of the possible consequences of the hazards and the related risks; and
- top-down analysis leads to the identification of the causes of the hazards.

The global process consists of risk analysis and hazard control, see Figure A.2. The risk analysis produces tolerable hazard rates which are the input to the hazard control.

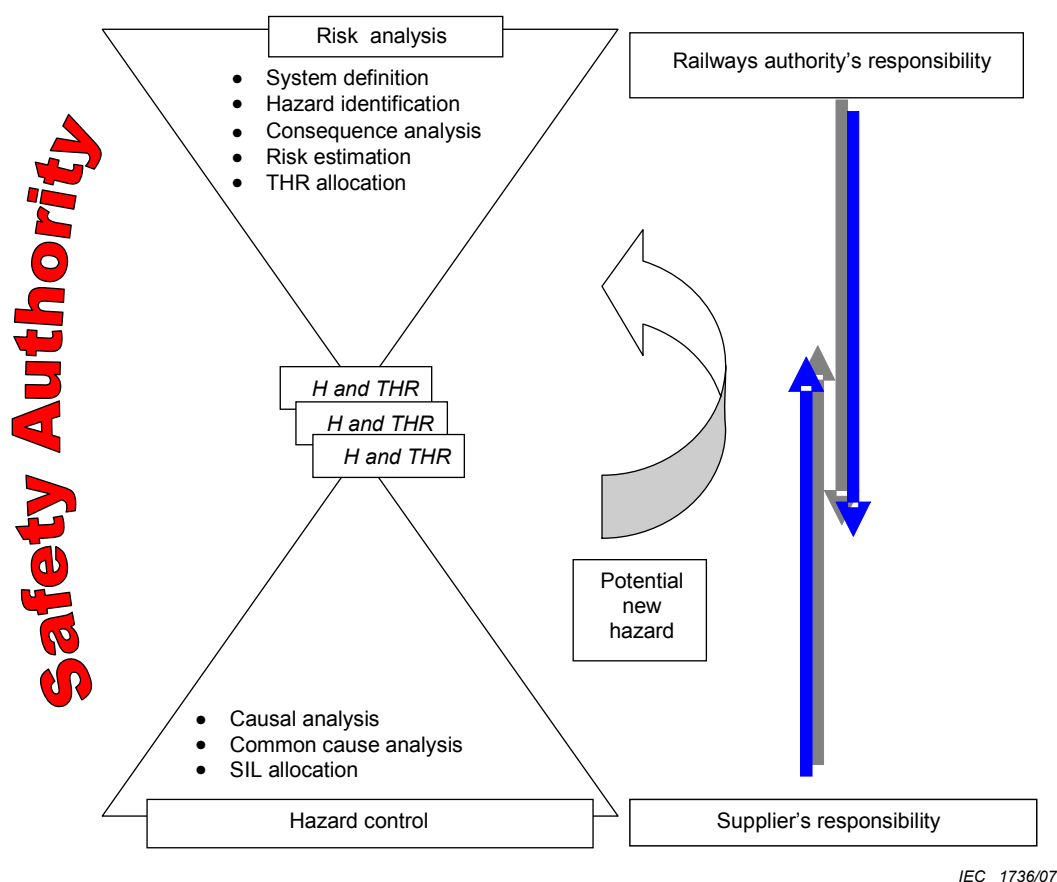


Figure A.2 – Global process overview

It is important to note that the THR is a target measure with respect to both systematic and random failure integrity. It is accepted that only with respect to random failure integrity will it be possible to quantify. Qualitative measures and judgements will be necessary to justify that the systematic integrity requirements are met. This is mainly covered by the SIL (and the measures derived from the SIL).

The safety authority shall approve both, the risk analysis and the hazard control.

NOTE In some cases, these steps are not completely independent. The hazard control can lead to system changes which offer more safety performance. The overlapping arrows in Figure A.2 show this. Hence, in these cases, the global process is iterative.

A.4.1 Risk analysis

Figure A.3 gives an example of a risk analysis process. The following subclauses explain the phase in more detail.

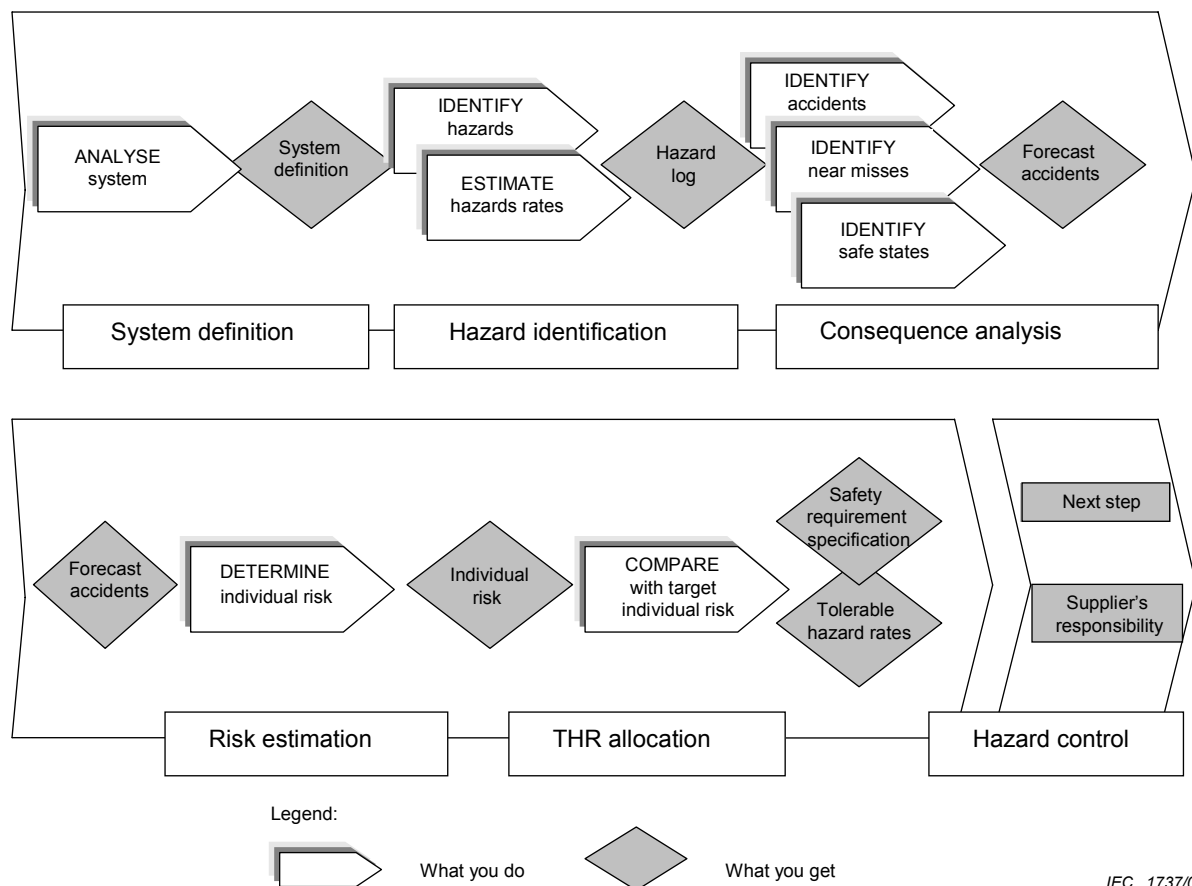


Figure A.3 – Example risk analysis process

A.4.1.1 System definition and hazard identification

It is the responsibility of the railway authority

- to define the system (independent of the technical realisation),
- to identify the hazards relevant to the system.

Hazard identification involves systematic analysis of a product, process, system or an undertaking to determine those adverse conditions (hazards) which may arise throughout the life-cycle. Such adverse conditions may have the potential for human injury or damage to the environment.

Systematic identification of hazards generally involves two phases:

- an empirical phase (exploiting past experience, e. g. checklists);
- a creative phase (proactive forecasting, e. g. brain-storming, structured what-if studies).

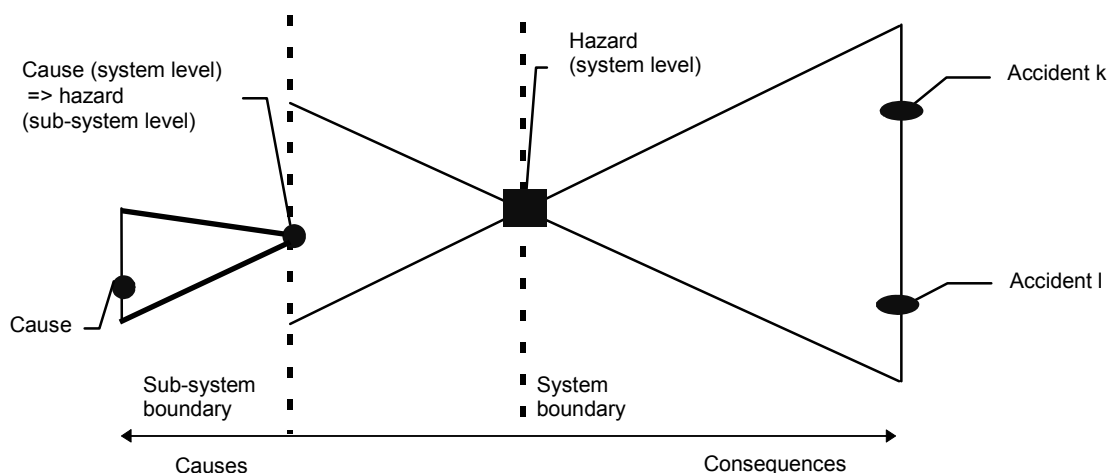
The empirical and creative phases of hazard identification complement one another, increasing confidence that the potential hazard space has been covered and that all significant hazards have been identified.

NOTE Methodologies which generate an unrealistically large number of mostly trivial or imprecisely defined hazards are wasteful of resources and can lead to a misleading or unproductive risk assessment. With the exception of large undertakings, involving many personnel, activities and equipment, a large list of hazards extending into the hundreds is unreasonable and indicative of a poorly designed or conducted study.

The hazards depend on the system definition and in particular the system boundary, which allows a hierarchical structuring of hazards with respect to systems and sub-systems. It also

means that hazard identification and causal analysis shall be performed repeatedly at several levels of detail during the system development.

Figure A.4 shows that the cause of a hazard at system level may be considered as a hazard at sub-system level (with respect to the sub-system boundary). Thus this definition enables a structured hierarchical approach to hazard analysis and hazard tracking.



IEC 1738/07

Figure A.4 – Definition of hazards with respect to the system boundary

To further ensure that the risk assessment effort is focused upon the most significant hazards, the hazards should, once identified, be ordered in terms of their perceived risk level.

All identified hazards and other pertinent information shall be recorded in a hazard log.

A.4.1.2 Consequences analysis, risk estimation and allocation of tolerable hazards rates

It is the responsibility of the railway authority

- to analyse the consequences, i.e. the losses,
- to define the risk tolerability criteria,
- to derive the tolerable hazard rates, and
- to ensure that the resulting risk is tolerable (with respect to the appropriate risk tolerability criteria).

The only requirement is that the resulting tolerable hazard rates shall be derived taking into account the risk tolerability criteria. Risk tolerability criteria are not defined by this standard, but depend on national or European legislative requirements.

The analysis methods shall either

- estimate the resulting (individual) risk explicitly, or
- derive the tolerable hazard rates from a comparison with the performance of existing systems or acknowledged rules of technology, either by statistical or analytical methods, or
- derive the tolerable hazard rates from alternative qualitative approaches, if as a result they define a list of hazards and corresponding THR.

It is important to note that this approach gives the railway authorities the freedom to define the hazards and corresponding THRs at any level, according to their particular needs. While one railway authority may set very general, high-level targets, another may set very detailed targets at the level of safety functions.

A.4.2 Hazard control

Hazard control covers the management of the implementation of the required THRs and associated safety functions.

If no THRs are provided, then either the supplier will provide these along with the system proposal to the railway authority or the railway authority and the supplier will work together to define the requirements.

Hazard control consists of performing causal analysis followed by a number of activities which can be summarised as follows:

- in the case of no defined THRs, define the safety assumptions and system functions related to the defined hazards;
- in the case of defined THRs, define the system architecture and allocate system functions within the architecture (technical solution) to meet the safety requirements;
- determine the safety integrity requirements for the sub-systems;
- complete the safety requirements specification;
- analyse the system/sub-system to meet the requirements;
- identify potential new hazards arising out of the system/sub-system design through the design and verification processes, and either ensure the new potential hazards are covered by the existing functionality or, if the new potential hazards require extra functionality or mitigation outside the system/sub-system, transfer the potential hazards back to risk analysis for further treatment;
- to determine the reliability requirements for the equipment.

The hazard control process is depicted in Figure A.5.

NOTE A well-structured hazard control contains relevant parts of a technical safety report implicitly. In this case, it is sufficient in the technical safety report to reference the hazard control.

A.4.2.1 Causal analysis

Causal analysis constitutes two key stages:

In a first phase of the causal analysis, the tolerable hazard rate for each hazard is apportioned to a functional level (system functions). The tolerable hazard rate for a function is then translated to a SIL using the SIL table. Safety integrity levels (SIL) are defined at this functional level for the sub-systems implementing the functionality.

If the railway authority has already defined the hazards and THRs with respect to safety functions, then the first phase of causal analysis is void and SILs can be immediately allocated based on the required THRs.

A sub-system, i.e. the combination of equipment, may implement a number of safety-related functions, each of which could require different safety integrity levels. Where this is the case, the sub-system shall satisfy all the required SIL levels. This can be obtained if each function meets the highest SIL or if demonstration of independence can be provided. In both cases, a common cause failure analysis shall be performed.

In a second phase of the causal analysis, the hazard rates for sub-systems are further apportioned leading to failure rates for the equipment, but on this physical or implementation level, the SIL remains unchanged. Consequently, the software SIL defined by IEC 62279 would also be the same as the sub-system SIL, except in the case of the exceptions described in IEC 62279.

The apportionment process may be performed by any method which allows a suitable representation of the combination logic, e.g. reliability block diagrams, fault trees, etc.

From risk analysis

List of hazards and THR

For each hazard

Check independence assumptions

System architecture

Undetected failure of switch-in function

Undetected failure of distant signal 1E-7

Undetected failure of light signals 7E-6

Undetected failure of barriers 7E-6

For each subsystem

SIL table

Determine THR and SIL

SIL and THR for sub-systems

Apportion hazards rates to elements

SIL and FR for elements

A.4.2.2 Common cause failure (CCF) analysis

- physical,
- functional,
- process

AVA Documents
Document Sharing Hub

A.4.2.2.1 Physical independence

Physical independence is an absolute necessity in order to make credible fault tree calculations with AND gate for random effects. Thus, in any case, a common cause failure (CCF) analysis would be necessary to assume independence.

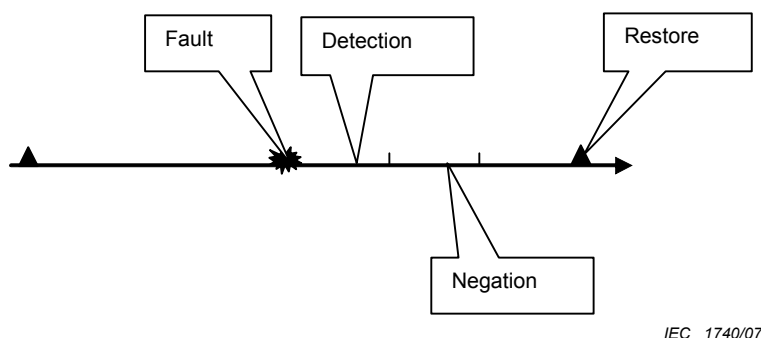
Conditions for physical independence can be found in Clauses D.2 and D.3 (informative). A sub-chapter of the safety case also deals explicitly with independence of items.

NOTE Taking a brief look at two repairable items, which are usually defined by their failure and repair rates, and a closer look at AND combinations, a different interpretation of the repair rates (or equivalent repair times) is necessary. Usually, after a fault within an item has appeared, at least two things have to happen in order to get the item working again (see Figure A.6):

- the fault is detected and negated (this means a safe state is entered);
- the item is repaired and restored.

With repair and restore time, we mean the logistic time for repair after detection, actual repair time (fault finding, repair, exchange, check) and time to restore equipment into operation. While in a reliability context usually the detection time is neglected, this time becomes important in the safety context. Safety-critical applications may not rely on self-tests or similar measures, but the detection and negation must be performed independently of the item. Sufficient failure detection and negation mechanisms should be demonstrated in the safety case.

In a safety context, generally, the actual repair and restore time can be neglected, if other control measures are taken during this period. In this case, the repair rate from reliability analysis can be interpreted as the detection and negation time, here defined as safe down time (SDT) or equivalent safe down rate (SDR).



IEC 1740/07

Figure A.6 – Interpretation of failure and repair times

Modelling the composition of two independent items in an AND-gate, the following basic formula for the (asymptotic) tolerable hazard and detection rates for highly available systems can be used, assuming that the rates are constant over time:

$$THR_S \approx \frac{FR_A}{SDR_A} \times \frac{FR_B}{SDR_B} \times (SDR_A + SDR_B) \quad SDR_S \approx SDR_A + SDR_B \quad (A.1)$$

where the FR's stand for potential hazardous failure rates.

If periodic testing times are used as detection times, then Equation (A.1) may be used with mean test times:

$$T/2 + \text{negation time} = SDT = 1/SDR.$$

This means that in order to use AND combinations properly, each item must have an independent failure detection and shut-down mechanism. If an item does not have such mechanism, then according to B.3.3, the installed lifetime of the item must be taken into account.

Another aspect, which must be taken into account in the design, and which in fact limits the free choice of parameters, is the availability of the system.

EXAMPLE Taking two identical items with a MTBF of 10 000 h and a mean detection time of 1 h (ignoring negation time), then the resulting failure rate for the parallel system (AND combination in failure logic) is 2×10^{-8} per hour. If one item has a mean detection time of 1 000 h (e. g. detection by maintenance), then the result is only 10^{-5} per hour, which is only a factor of 10 better than the MTBF of a single item. If the mean detection time for one item would be its lifetime, then the gain would become even more marginal.

Physical independence is the lowest level of independence, typically at component level. If physical independence is assured, then random integrity requirements may be apportioned to the next lower level.

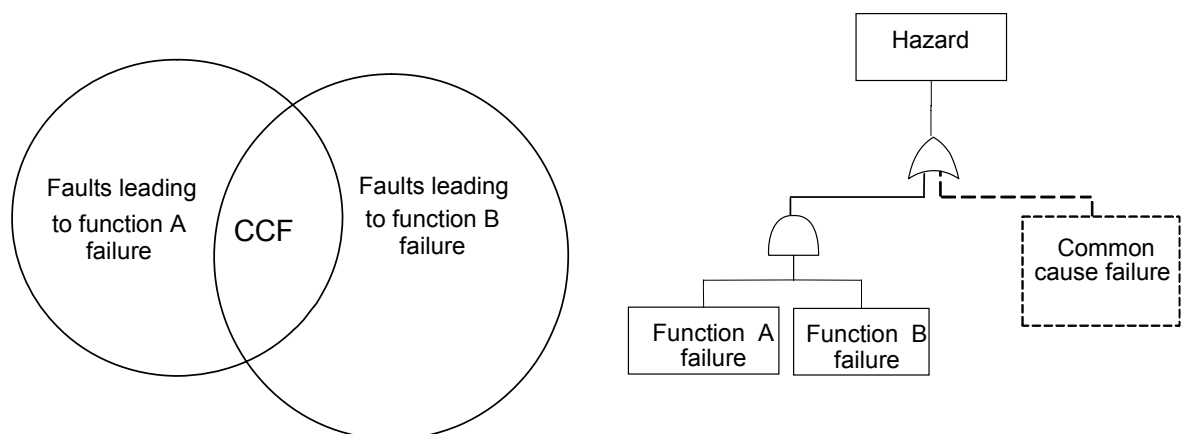
A.4.2.2.2 Functional independence

Functional independence implies that there are neither systematic nor random faults, which cause a set of functions to fail simultaneously. Thus, on this level again, a CCF analysis would be necessary in order to show that the functions are independent. In this standard, this is called independence with respect to functional influences. Random and systematic integrity requirements may be apportioned to the next lower level only if functional independence is assured.

When applying fault tree analysis to system functions, say A and B, which is the main case in the safety integrity requirements apportionment process, it shall be taken into account that using AND gates immediately creates the following safety-relevant application rules:

- the implementations of A and B shall be physically independent;
- the safe down times defined by detection and negation times for each item shall be estimated and achieved.

NOTE In general, functions are not independent, but can be further subdivided in independent sub-functions and sub-functions affected by CCF. Figure A.7 shows a generic treatment of CCF by FTA.



IEC 1741/07

Figure A.7 – Treatment of functional independence by FTA

A.4.2.2.3 Process independence

Products and systems generally emerge as a result of activities inherent in the early life-cycle processes. These broadly comprise concept, requirements specification, system design, system development, verification and validation phases which have a significant influence on the properties of the end product. It is generally agreed that higher degrees of criticality of a product or system in its environment of application demand more robust and systematic life-cycle processes. In addition, since systematic errors inherently arise during these life-cycle processes, a degree of independence is often desirable.

In a manner similar to functional and physical counterparts, independence and diversity in human resource and life-cycle processes are deemed to contribute to higher overall safety integrity for products and systems. Higher SIL requirements would therefore call for higher degrees of process and human resource independence to ensure systematic errors are avoided or minimised.

The development processes should fulfil the required SIL and ensure that there is sufficient organisational and personal independence between the development teams in order to further minimise systematic errors. For guidance on software issues, see IEC 62279.

A.4.3 Identification and treatment of new hazards arising from design

Realisation of a signalling system is likely to lead to unforeseen or undesirable properties with a potential to cause harm to people, in particular if the system or technology is new. New hazards may arise because of several aspects:

- new technology has a great potential for new hazards (lack of experience);
- emergence of hidden hazards in the existing railway system due to the introduction of a new technology (e.g. analogue to digital technology);
- new design hazard due to a lack of adequate/proper specification;
- special operation modes in an existing railway system may not fit well and may create new hazards for the operators, maintainers or other members of the staff, public, etc.;
- design errors may create new hazards, but they can often be related to the already identified ones.

These aspects may give rise to hazardous circumstances and states which require the same systematic treatment as applied to the already identified hazards.

The process for identification, processing and treatment of new hazards arising from the design or application of a system is essentially identical to the risk analysis phase. Once identified, system level hazards with a potential to affect overall system performance or cause harm to people shall be declared by the supplier to the railway authority. Depending on the perceived risks, these would require qualitative or quantitative assessment, with a view to forecast and agree on an appropriate tolerable rate (THR) for each.

NOTE Then it is possible to proceed in at least two different ways:

- it is possible to relate the new hazard to an identified one: in this case, the supplier should make sure that the resulting HR of the combination of these two hazards is still compliant with the THR that has been fixed by the railway authority. The hazard log and the safety case should trace this hazard;
- the new hazard has nothing to do with any of the identified ones: in this case, the supplier should contact the railway authority to provide all the information he has analysed about the hazard (causes, consequences, risk, etc.). The railway authority should then decide whether this new hazard could be accepted or not:
 - if not, the supplier should re-design his product/system if it is possible. If not, then additional protection measures should be implemented in order to keep the hazard and associated risk at an acceptable level;
 - if yes, then the railway authority is in charge of defining the THR of this new hazard and the supplier should provide a design compliant with this requirement;
 - for both cases, once a conclusion has been reached concerning this hazard, everything should be recorded in the hazard log and the safety case.

The THRs shall be derived for each new hazard and these will lead to updated requirements.

A.5 Safety integrity levels

A.5.1 General aspects

Safety integrity is specified as one of four discrete levels. Level 4 has the highest level of safety integrity; level 1 has the lowest. Level 0 is used to indicate that there are no safety requirements. A SIL should address qualitative appreciation of factors such as quality and safety management and technical safety conditions.

Hazards related to a system are identified and assessed with regard to their potential consequences during the risk analysis phase of the system life-cycle, as described A.4.1. This activity results (top-down) in tolerable hazard rates for each hazard. Nevertheless, a supplier may start development of generic products in a bottom-up fashion and may even achieve safety approval for a generic product safety case (without the results of any risk analysis being available), but in the end, he shall ensure that the required tolerable hazard rates (application safety case) are fulfilled. The railway authority and/or the safety authority shall determine the base line for this process.

During the next phases, the system requirements and apportionment of system requirements phases, the tolerable hazard rates are apportioned to system functions and sub-systems, respectively.

Each of these functions shall have a qualitative safety target and a quantitative target attached to them. The qualitative target shall be in the form of a safety integrity level, and shall cover systematic failure integrity. The quantitative target shall be in the form of a numerical failure rate, and shall cover random failure integrity.

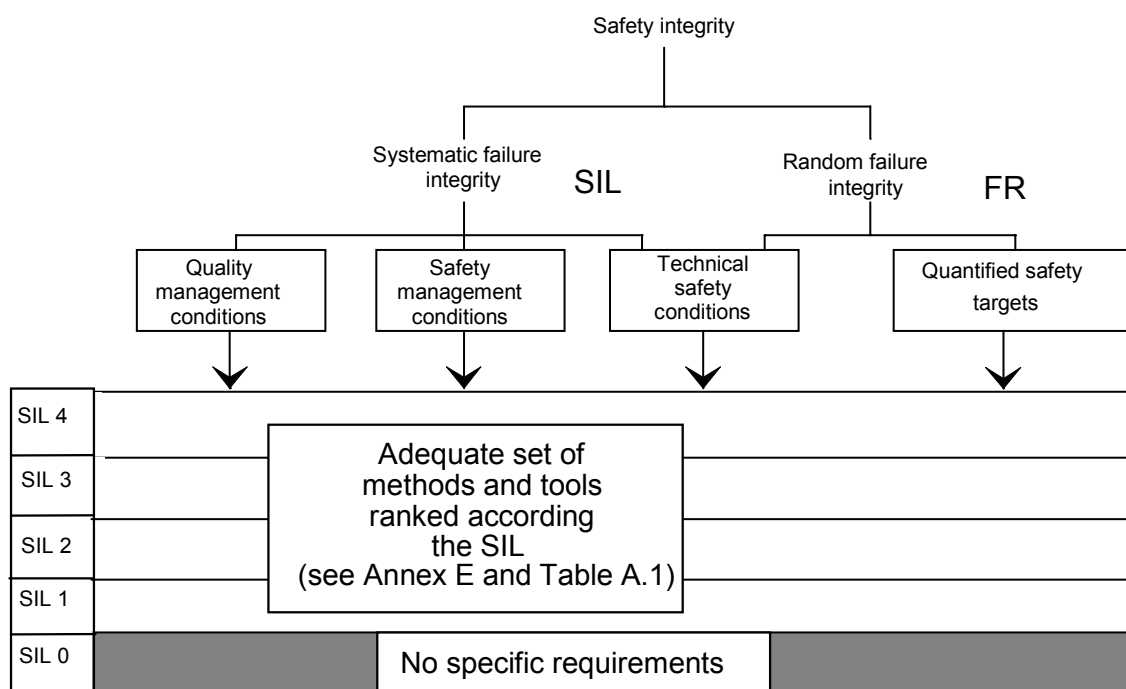
Safety-related functions within a system are implemented by sub-systems. Safety integrity levels are allocated to safety-related functions and consequently, the sub-systems implementing these functions, but no further. The safety integrity level for the equipment which is part of a sub-system, is the same as for the sub-system, unless functional independence can be demonstrated between equipment within sub-systems.

It is important to recognise that achievement of a specified safety integrity level requires compliance with all of the factors in Figure A.8, namely

- quality management conditions,
- safety management conditions,
- technical safety conditions,
- quantified safety targets.

Fulfilment of a particular quantified safety target does not, by itself, mean that the corresponding safety integrity level has been achieved. Similarly, fulfilment of the quality management, safety management and technical safety conditions associated with a particular safety integrity level does not mean that the corresponding quantified safety target, or the safety integrity level itself, have been achieved. All of the factors in Figure A.8 need to be fulfilled in order to achieve the specified safety integrity.

It is also important to understand that, whilst the quantified safety targets in Figure A.8 are those required in order to achieve the railway safety performance as described in the following paragraphs, it shall not be assumed that the target for a particular safety function can necessarily be achieved by a single sub-system or equipment. Where necessary, the required safety target shall be achieved by a combination of functions, sub-systems or equipment, as explained in this annex.



IEC 1742/07

Figure A.8 – Relationship between SILs and techniques**A.5.2 Relationship between SIL and safety targets**

This standard is based on the assumption that safety relies both on adequate measures to avoid or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failure should be balanced in order to achieve the optimum safety performance of a system. To achieve this, the concept of safety integrity levels (SIL) is used. SILs are used as a means of matching the qualitative approaches (to avoid systematic failures) with the quantitative approach (to control random failures), as it is not feasible to quantify systematic failures.

Like in many other standards, this balance is expressed in a table, which consists of a list of safety integrity levels 0, 1, 2, 3, 4 and a list of corresponding intervals or bands for tolerable hazard rates $I_0, \dots, I_4$.

The SIL table is applicable to safety-related functions or sub-systems implementing one or more of these functions. Having followed the measures and methods required for SIL x , there is no requirement to consider the systematic failures when demonstrating the THR is achieved.

The SIL table identifies the required SIL for the safety-related function from the THR. Thus, if the THR for a function F has been derived by a quantitative method, the required SIL shall be determined by the use of Table A.1.

Table A.1 – SIL-table

Tolerable hazard rate THR per hour and per function	Safety integrity level
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

A function having quantitative requirements more demanding than 10^{-9} h^{-1} shall be treated in one of the following ways:

- if it is possible to divide the function into functionally independent sub-functions, the THR can be split between those sub-functions and a SIL assigned to each sub-function;
- if the function cannot be divided, the measures and methods required for SIL 4 shall, at least, be fulfilled and the function shall be used in combination with other technical or operational measures in order to achieve the necessary THR.

NOTE In contrast to other standards, the SIL table in this standard has only one column for frequencies (formerly called high demand or continuous mode) and does not have a column for failure probabilities on demand (formerly called demand mode). The reasons to restrict to one mode are

- less ambiguity in determination of SIL,
- all demand mode systems can be modelled as continuous mode systems,
- continuous control and command signalling systems are clearly the majority in modern railway signalling applications.

The SIL table has been constructed taking into account IEC 61508-1.

Annex B (normative)

Detailed technical requirements

B.1 Introduction

As explained in 5.4, technical evidence for the safety of the system/sub-system/equipment design shall be presented in the technical safety report (which forms Part 4 of the safety case). The report shall be arranged under the following headings:

- Section 1 Introduction
- Section 2 Assurance of correct functional operation
- Section 3 Effects of faults
- Section 4 Operation with external influences
- Section 5 Safety-related application conditions
- Section 6 Safety qualification tests

Each of these has been briefly considered in 5.4. More detailed requirements for Section 2 to Section 6 of the technical safety report are contained in Clauses B.2 to B.6.

The technical safety report is mandatory for safety integrity levels 1 to 4 inclusive (see Annex A for explanation of safety integrity levels). However, the depth of the information and the extent of the supporting documentation should be appropriate to the safety integrity level of the system/sub-system/equipment under scrutiny. The requirements for safety integrity level 0 (non-safety-related) are outside the scope of this safety standard.

The structure of the technical safety report is illustrated in Figure 7.

B.2 Assurance of correct functional operation (Section 2 of the technical safety report)

This section concerns correct operation of the system/sub-system/equipment under fault-free conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements.

Some particular aspects are considered below, using the headings from 5.4.

B.2.1 System architecture description

This shall contain a general description of the system/sub-system/equipment design, in sufficient depth to convey a clear understanding of the principles and techniques which it uses.

B.2.2 Definition of interfaces

B.2.2.1 Man-machine interfaces

The man-machine interfaces consist of the following:

a) Operator

This shall describe the mechanisms by which the system/sub-system/equipment will be operated by operating and engineering personnel.

- EXAMPLE
- under normal conditions;
 - in response to alarms;
 - by use of 'help' routines.

b) Configuration

This shall describe the processes carried out by engineering personnel to configure the system/sub-system/equipment to a specific railway or application.

- EXAMPLE
- software parametering;
 - hard wiring;
 - installation techniques;
 - procedures.

c) Maintenance

This shall describe the interface mechanisms, including the use of any ancillary equipment, which will be used by maintenance personnel in the course of performing the various levels of maintenance.

More detailed information is contained in B.5.2.

B.2.2.2 System interfaces

Internal and external interfaces shall be described.

a) Internal

This shall define the functional and physical interfaces between items internal to the system/sub-system/equipment.

- EXAMPLE
- electrically clean and dirty areas;
 - internal bus structures;
 - communication links;
 - functional monitoring and correction;
 - diagnostic and health monitoring.

b) External

This shall define the functional and physical interfaces between the system/sub-system/equipment and external items.

- EXAMPLE
- sensors;
 - actuators;
 - communication links;
 - test and monitoring provisions;
 - expansion facilities.

B.2.3 Fulfilment of system requirements specification

This shall demonstrate how the operational functional requirements specified in the system/sub-system/equipment requirements specification are fulfilled by the design. All relevant evidence shall be included (or referenced).

- EXAMPLE
- design principles and calculations;
 - test specifications and results;
 - validation.