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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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 Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

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

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 It also gives information on projects, withdrawn and replaced publications.

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

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

- Electropedia: www.electropedia.org

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

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

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

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

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

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

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

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

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

- Electropedia: www.electropedia.org

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

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

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

CONTENTS

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

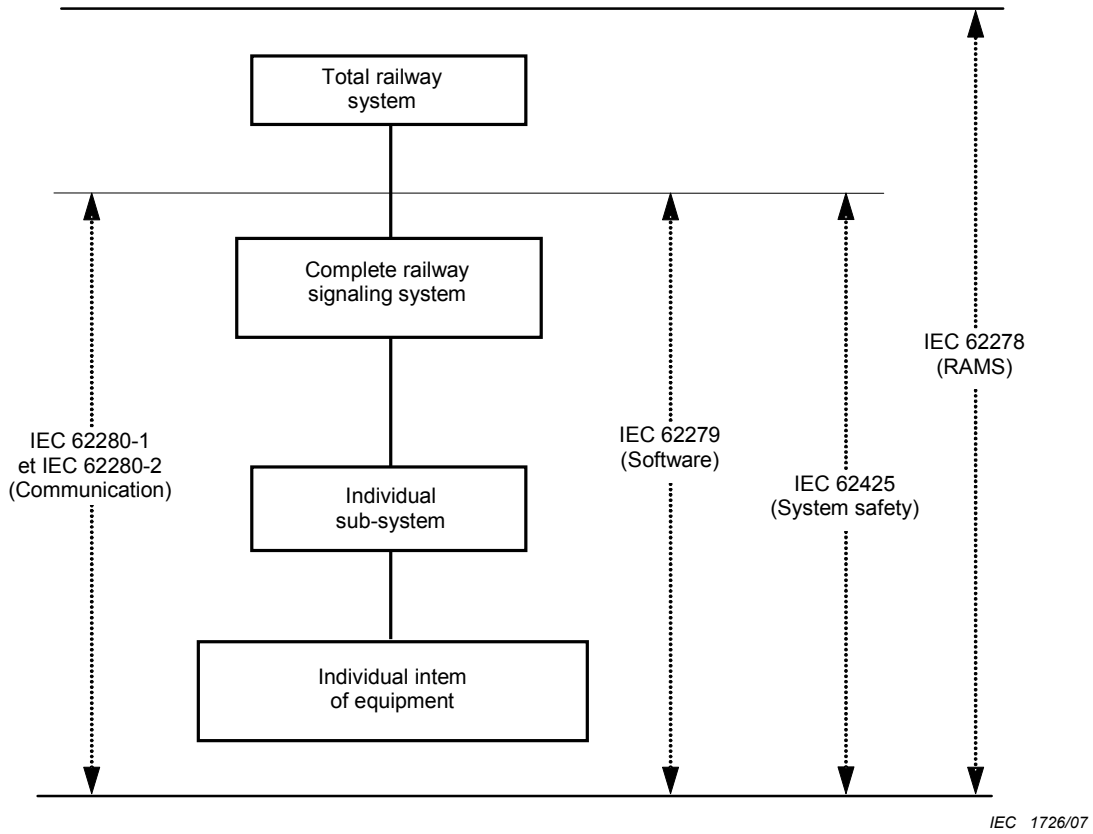


Figure 1 – Scope of the main IEC railway application standards

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*

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

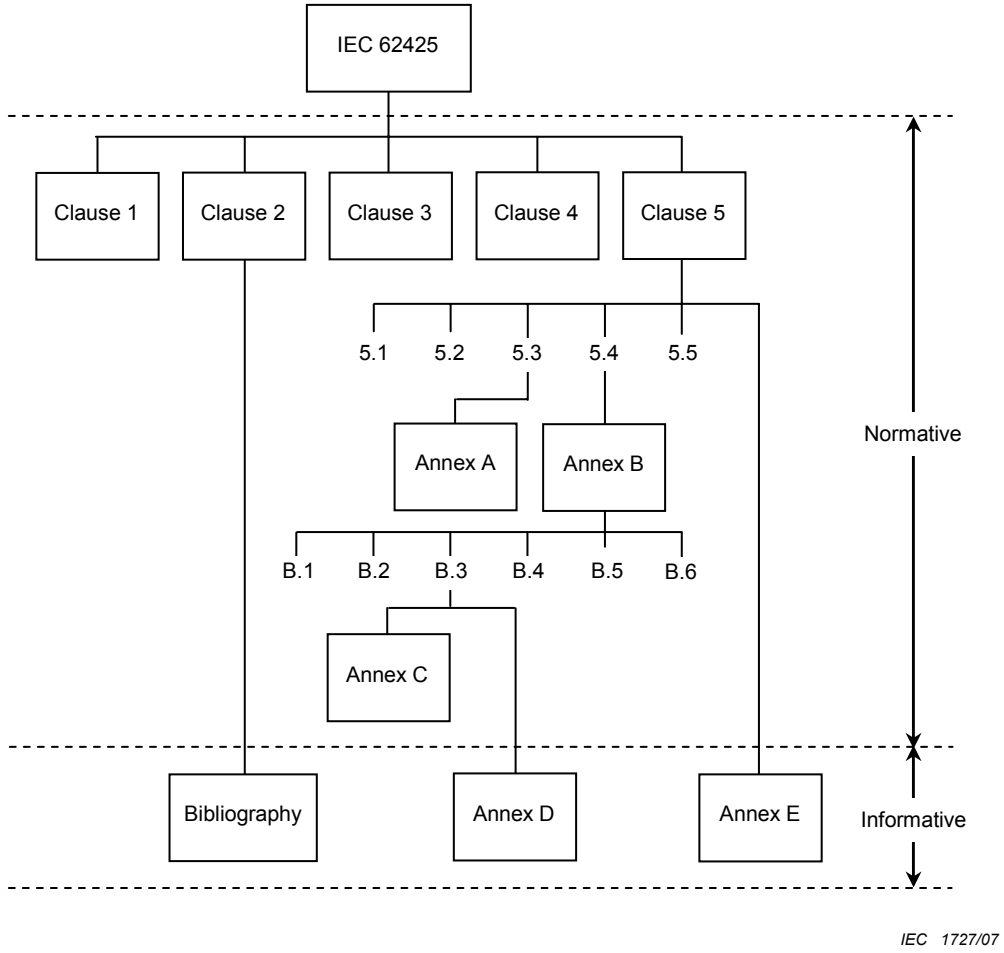


Figure 2 – Structure of IEC 62425

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

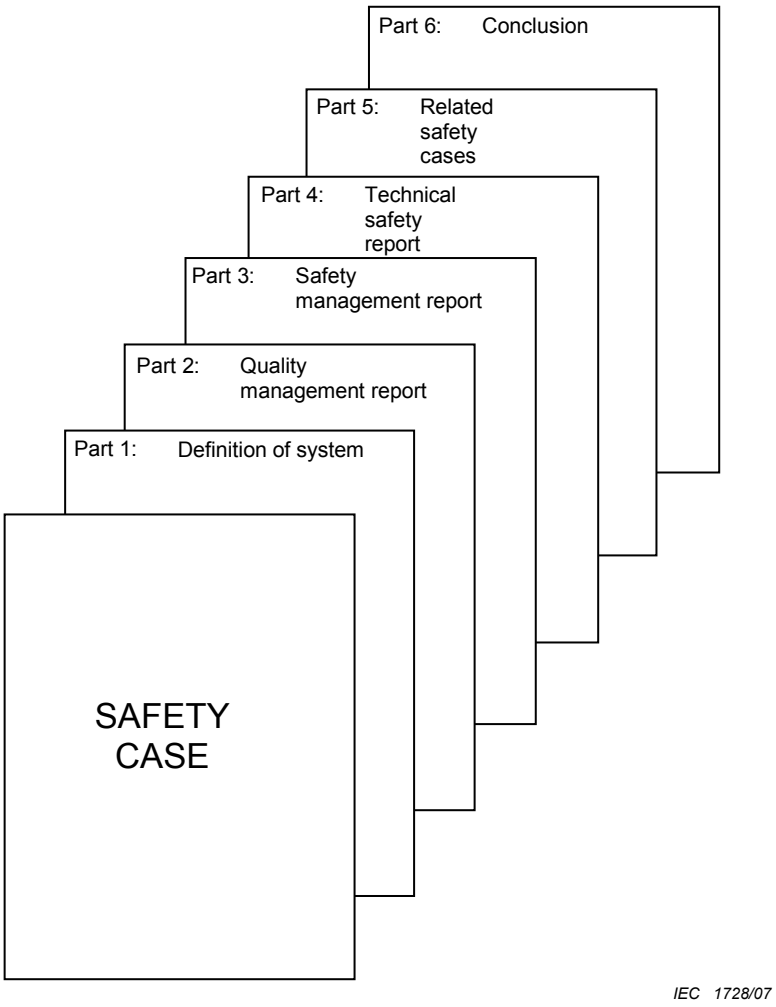


Figure 3 – Structure of safety case

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:

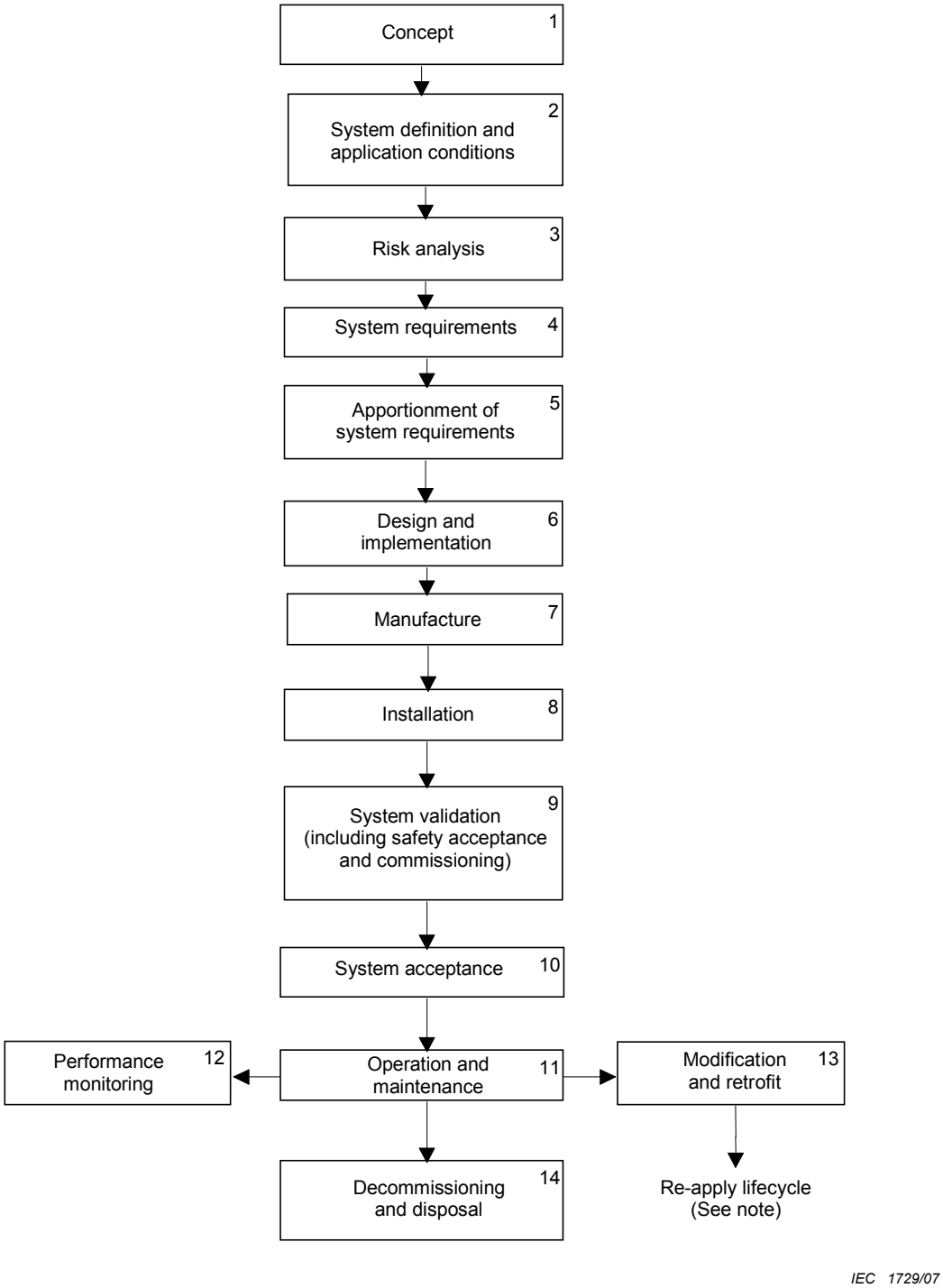
– organisational structure;
– quality planning and procedures;
– specification of requirements;
– design control;
– design verification and reviews;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

- 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.



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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

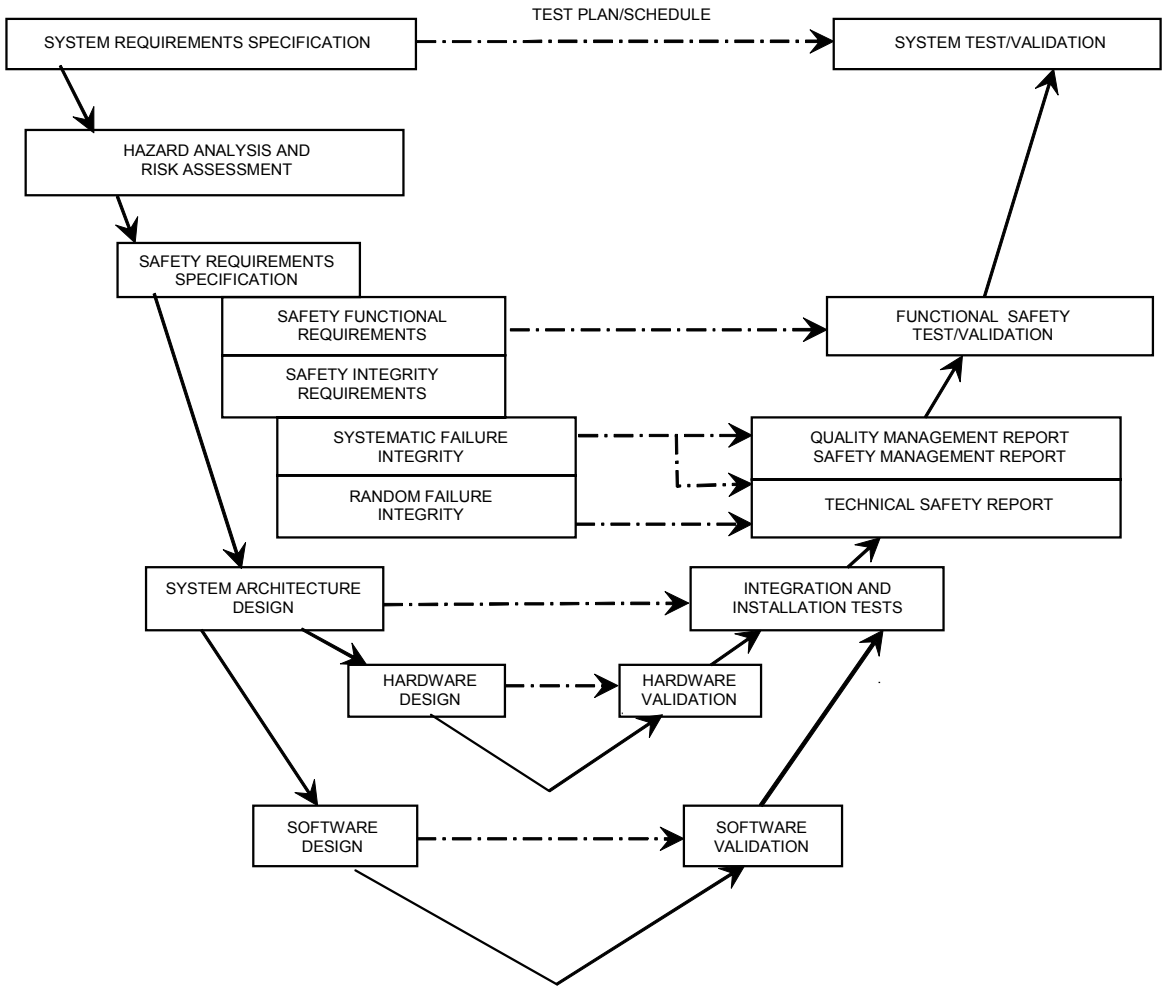


Figure 5 – Example of design and validation portion of system life-cycle

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

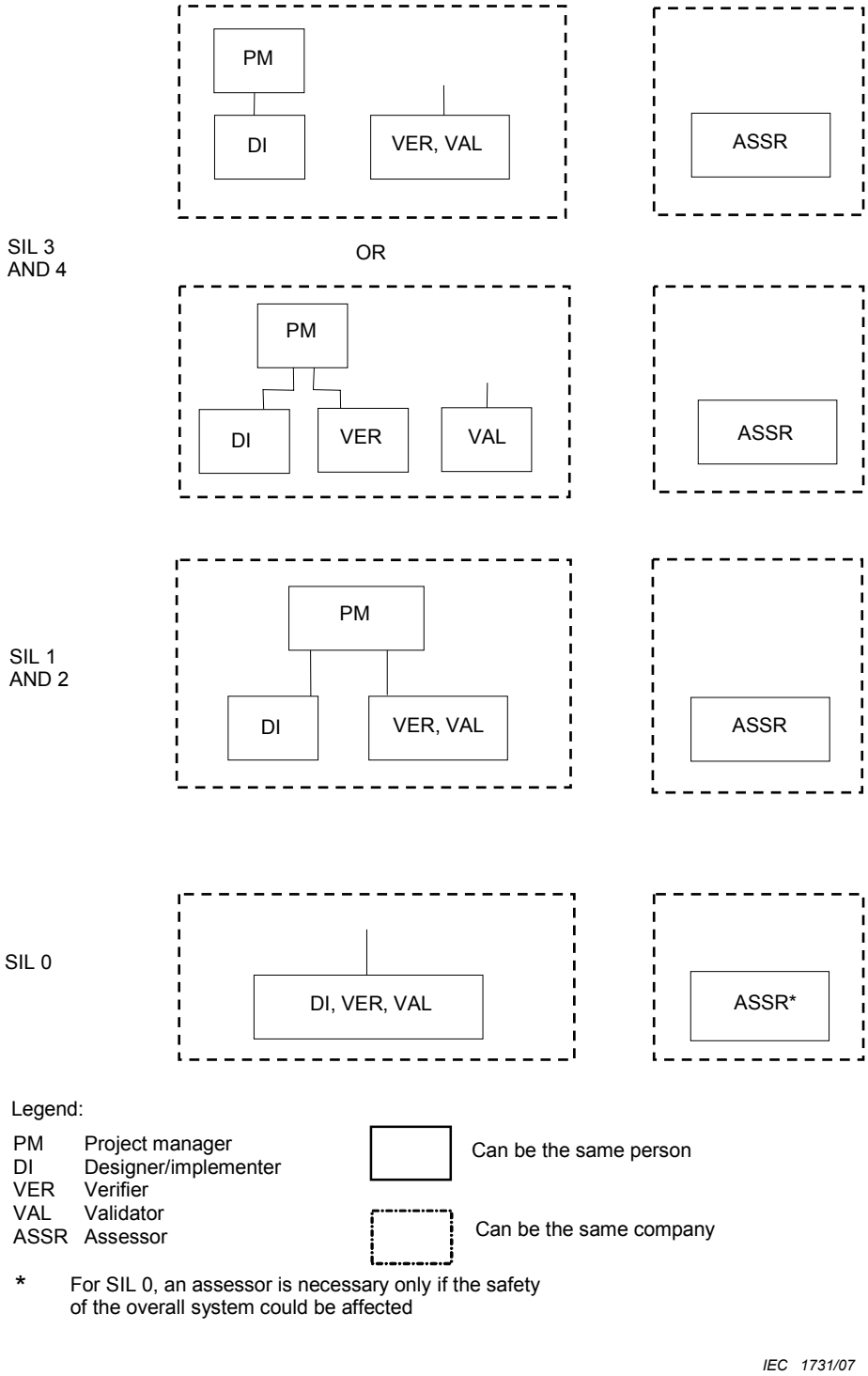


Figure 6 – Arrangements for independence

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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);

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

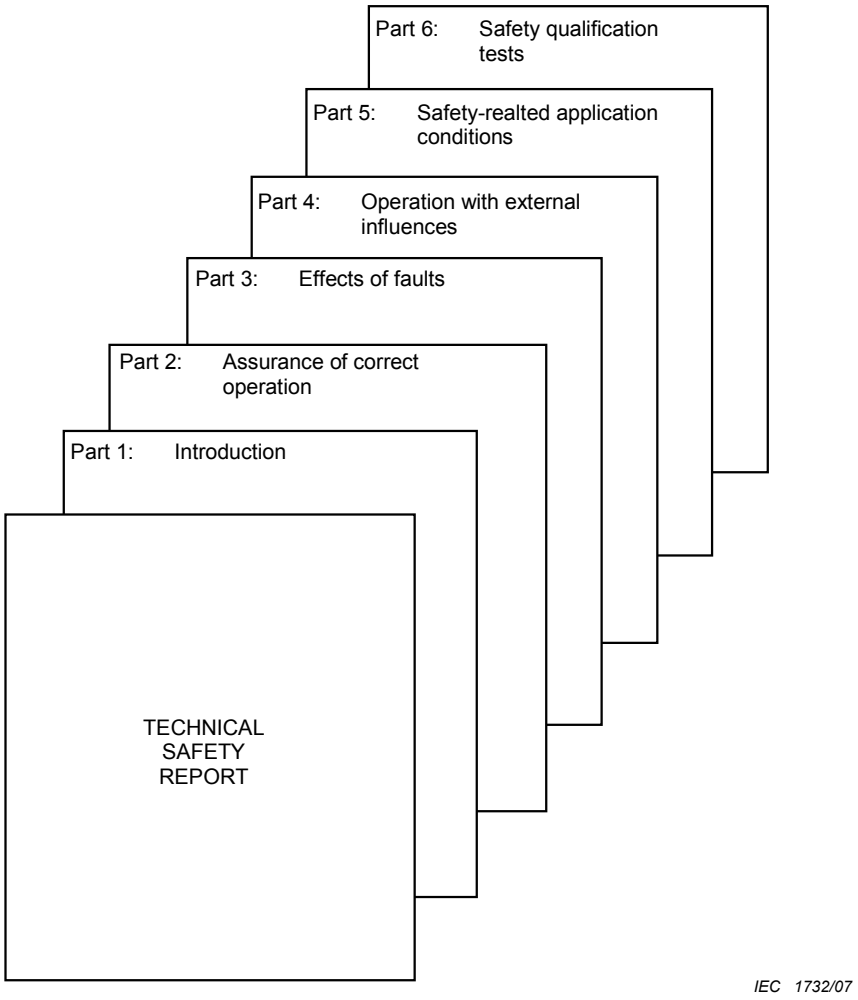


Figure 7 – Structure of technical safety report

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:

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

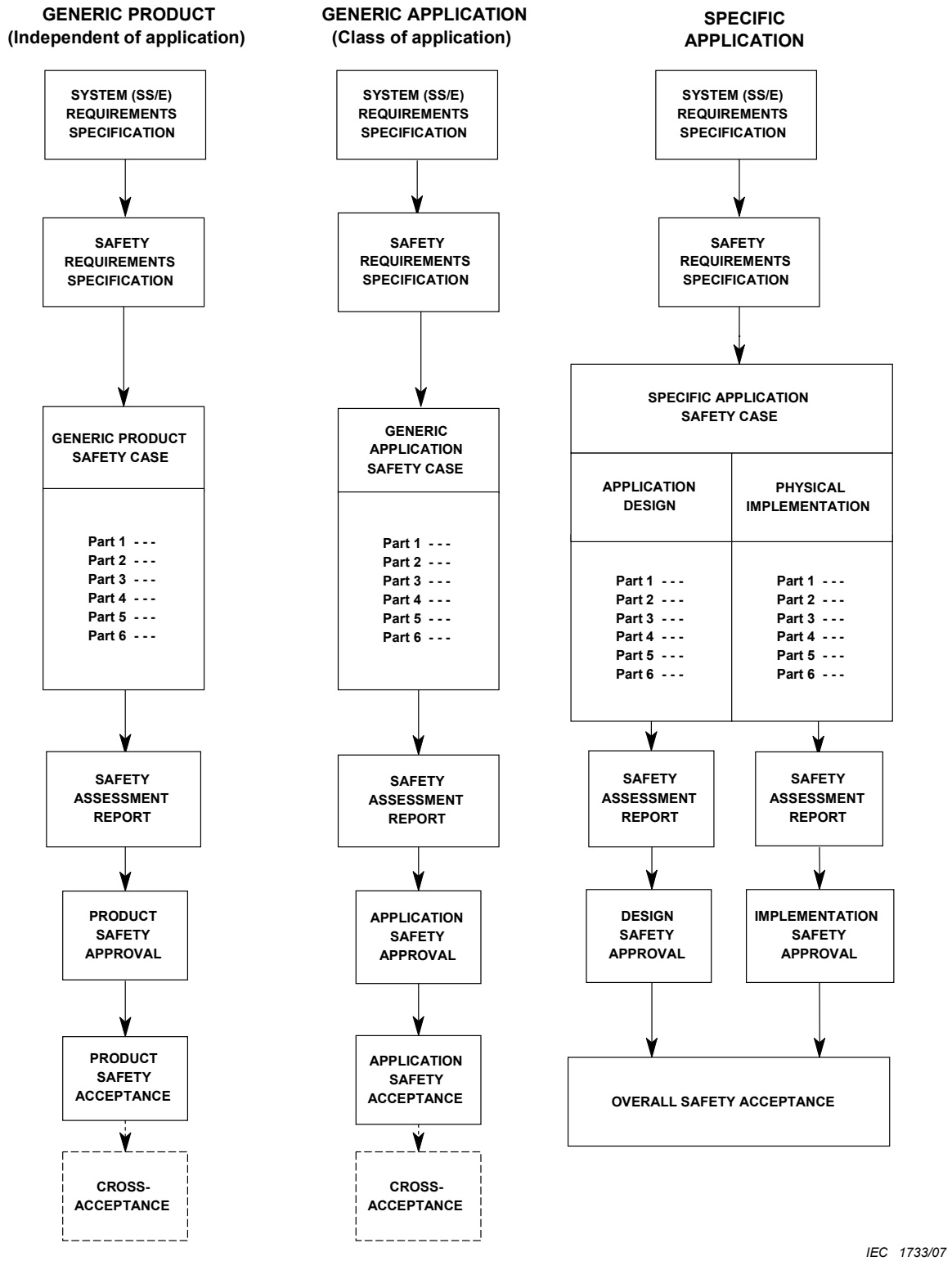


Figure 8 – Typical safety acceptance and approval process

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

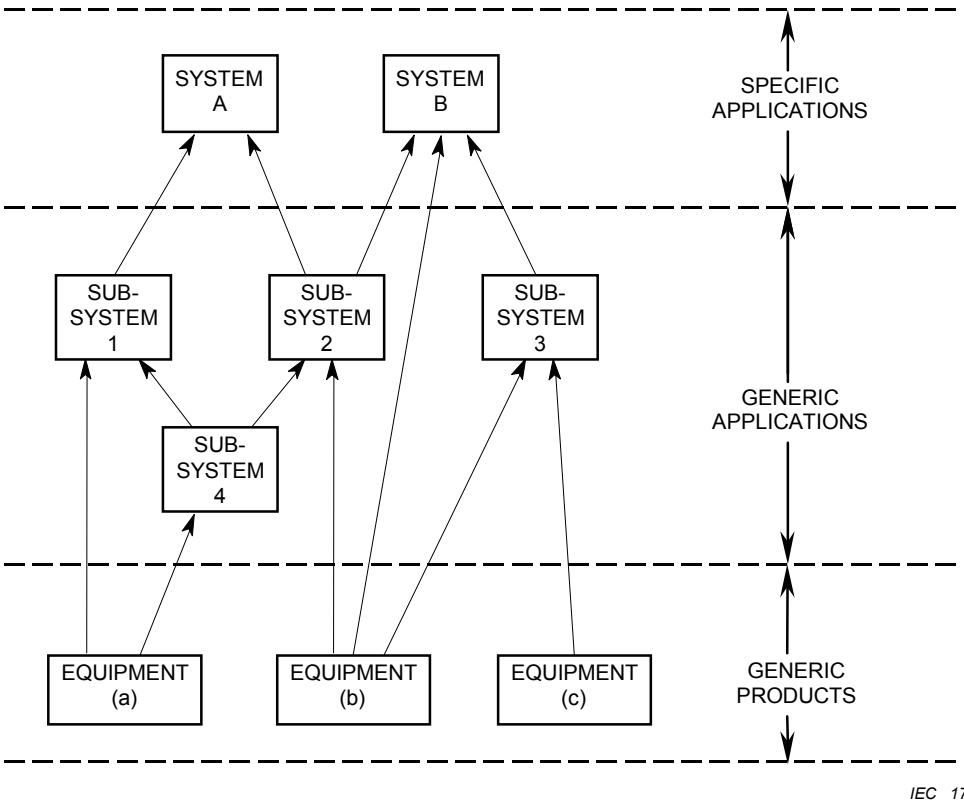


Figure 9 – Examples of dependencies between safety cases/safety approval

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

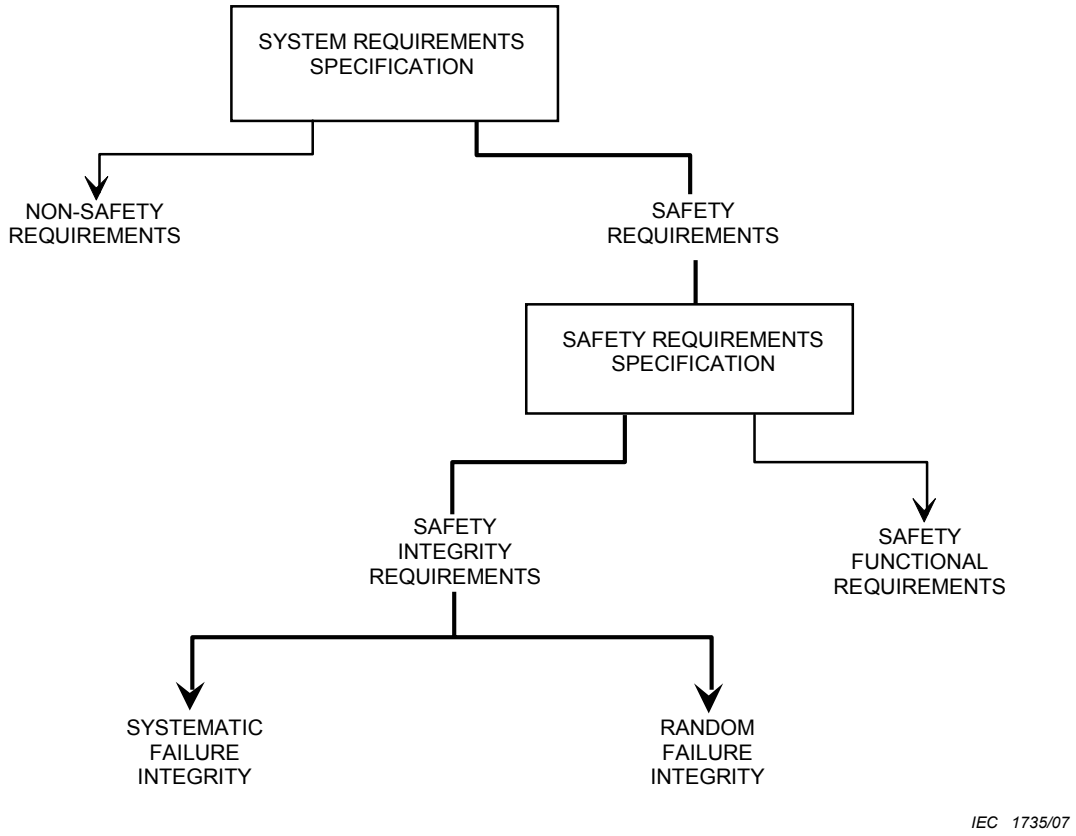


Figure A.1 – Safety requirements and safety integrity

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;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

- 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

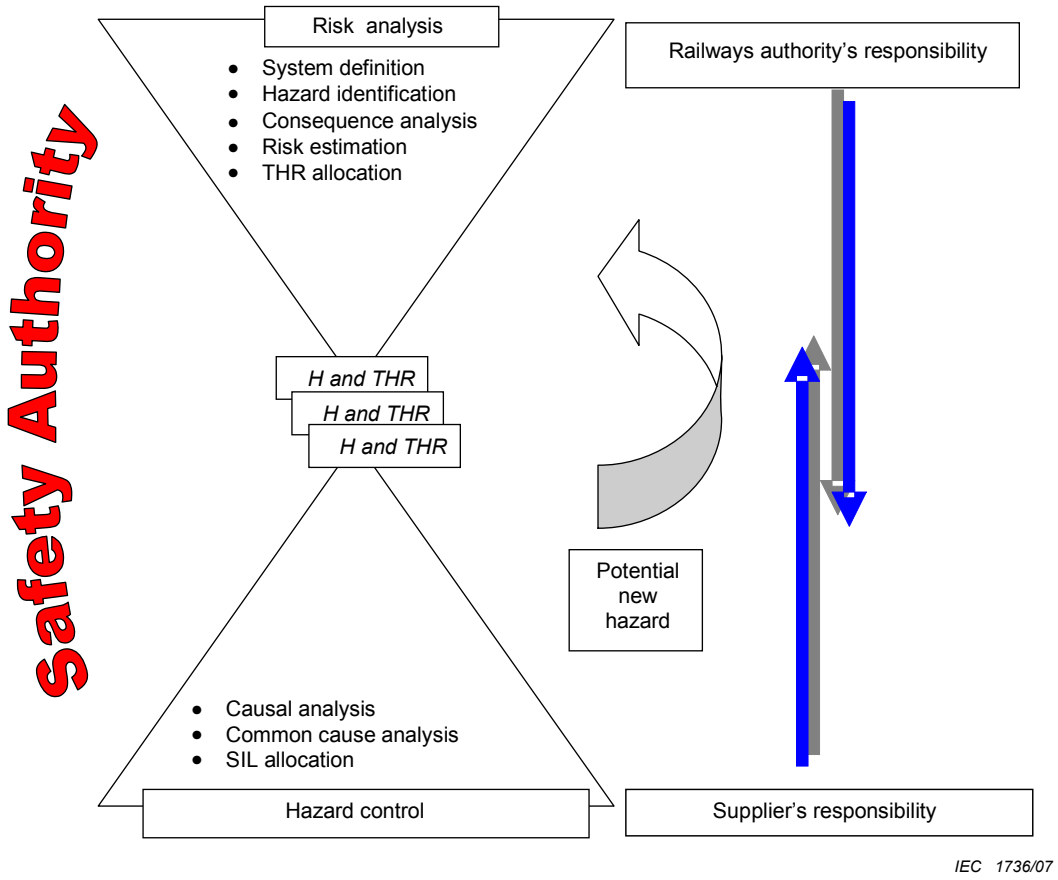


Figure A.2 – Global process overview

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

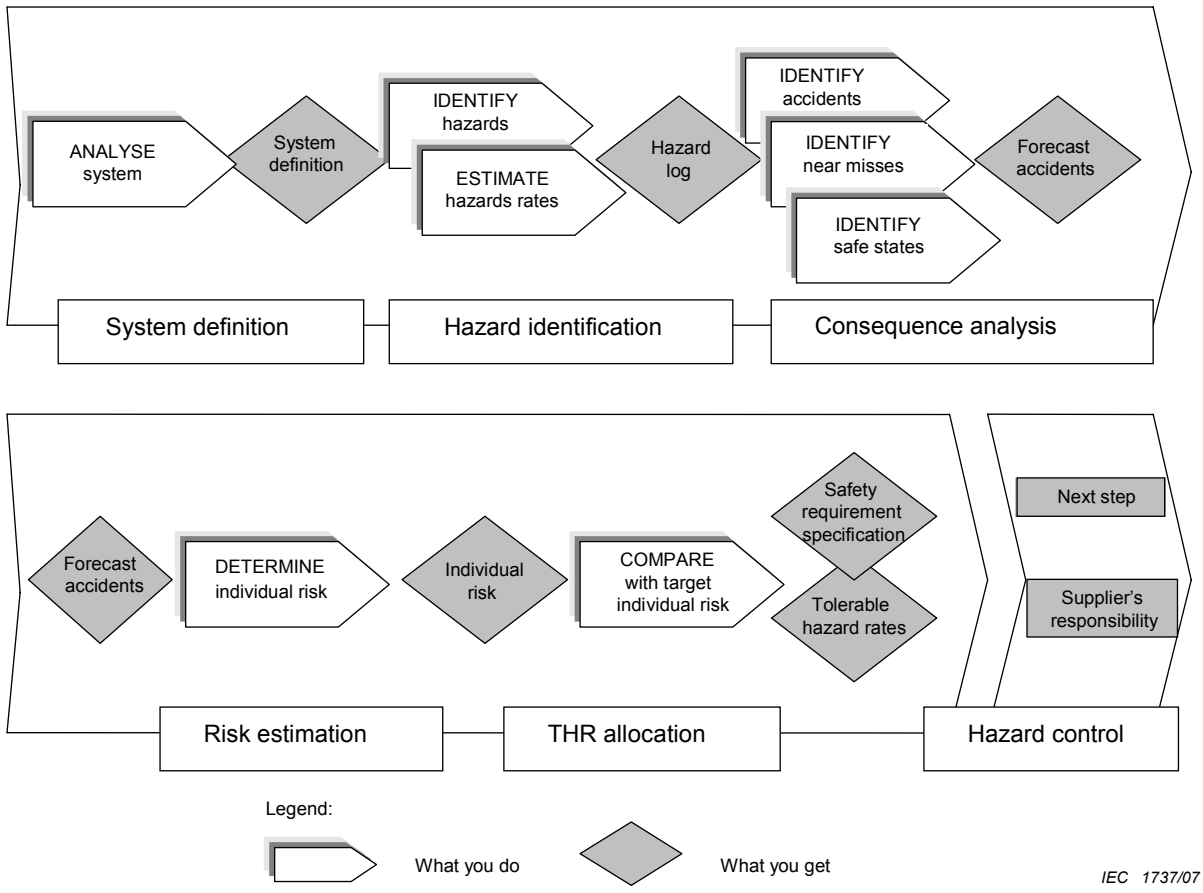


Figure A.3 – Example risk analysis process

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

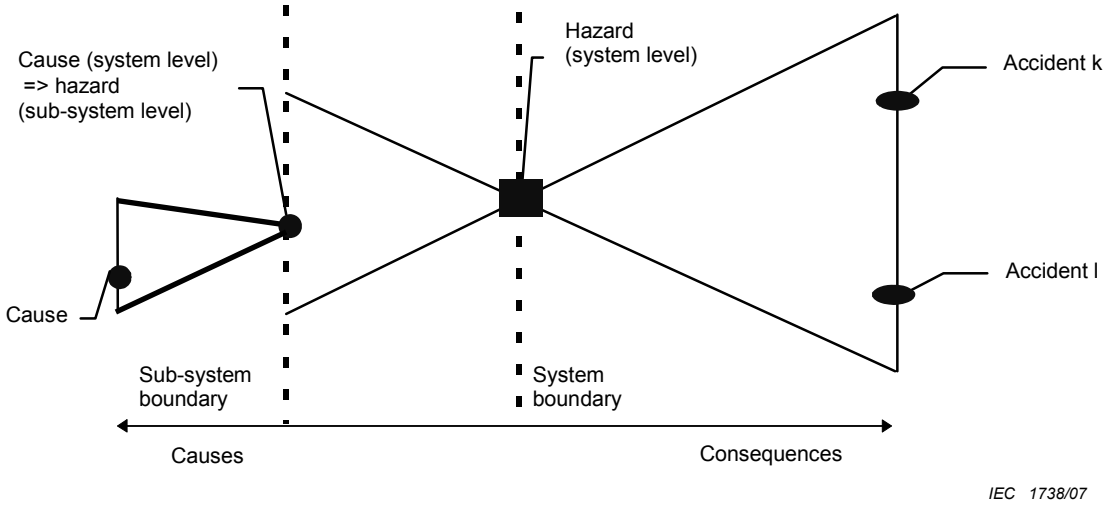


Figure A.4 – Definition of hazards with respect to the system boundary

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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, binary

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

decision diagrams, Markov models etc. In any case, particular care shall be taken when independence of items is required. While in the first phase of the causal analysis, functional independence is required (i.e. the failure of functions shall be independent with respect to systematic and random faults), physical independence is sufficient in the second phase (i.e. the failure of sub-systems shall be independent with respect to random faults). Assumptions made in the causal analysis shall be checked and may lead to safety-related application rules for the implementation.

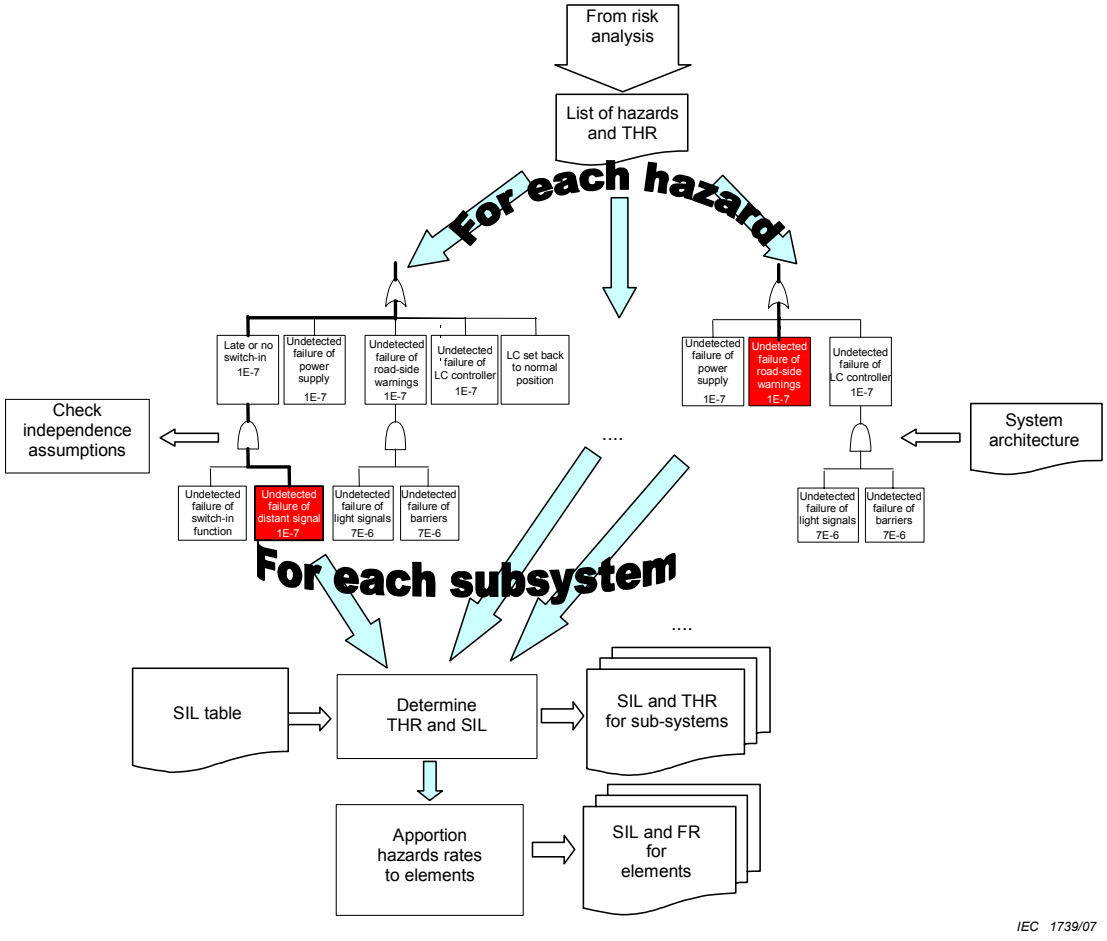


Figure A.5 – Example hazard control process

A.4.2.2 Common cause failure (CCF) analysis

Particular care has to be practised when independence claims (logical AND combinations) are used. It has to be ensured that sufficient

– physical,
– functional,
– process

independence exists between sub-systems or system functions (see B.3.2 and B.3.6). If independence cannot be demonstrated completely then the common cause failures have to be modelled at an appropriate level of detail. Additionally it shall be demonstrated that the safety-relevant application rules immediately implied by the use of AND combinations are fulfilled and checked.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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).

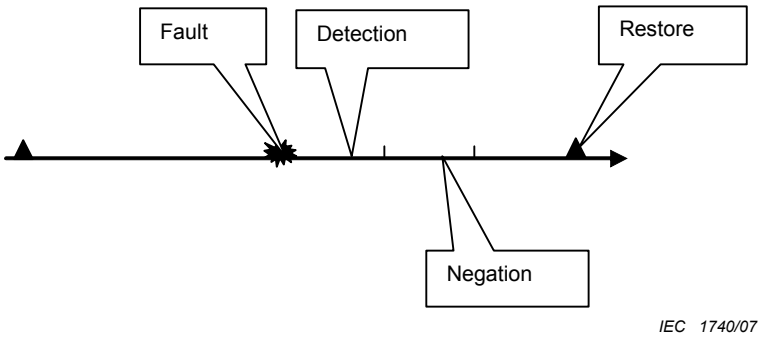


Figure A.6 – Interpretation of failure and repair times

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:

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

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:

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

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

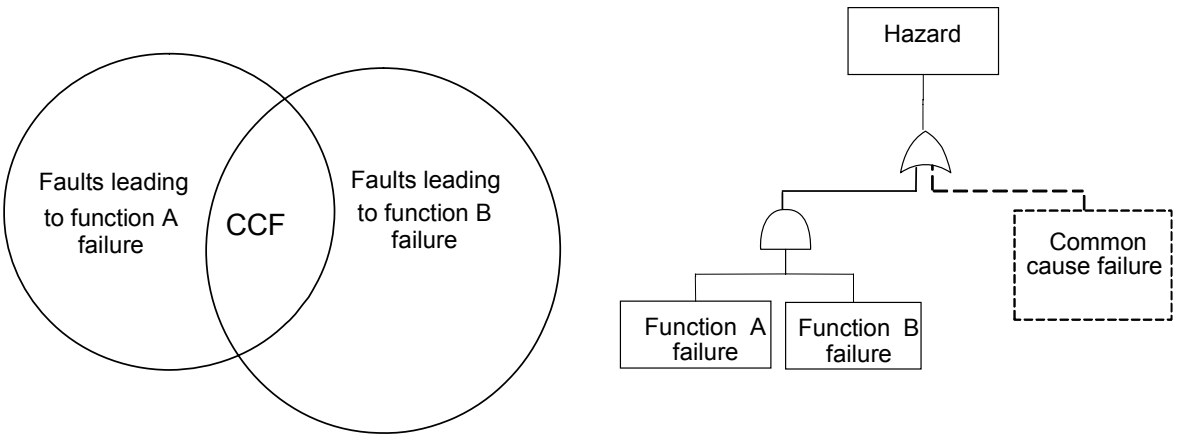


Figure A.7 – Treatment of functional independence by FTA

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

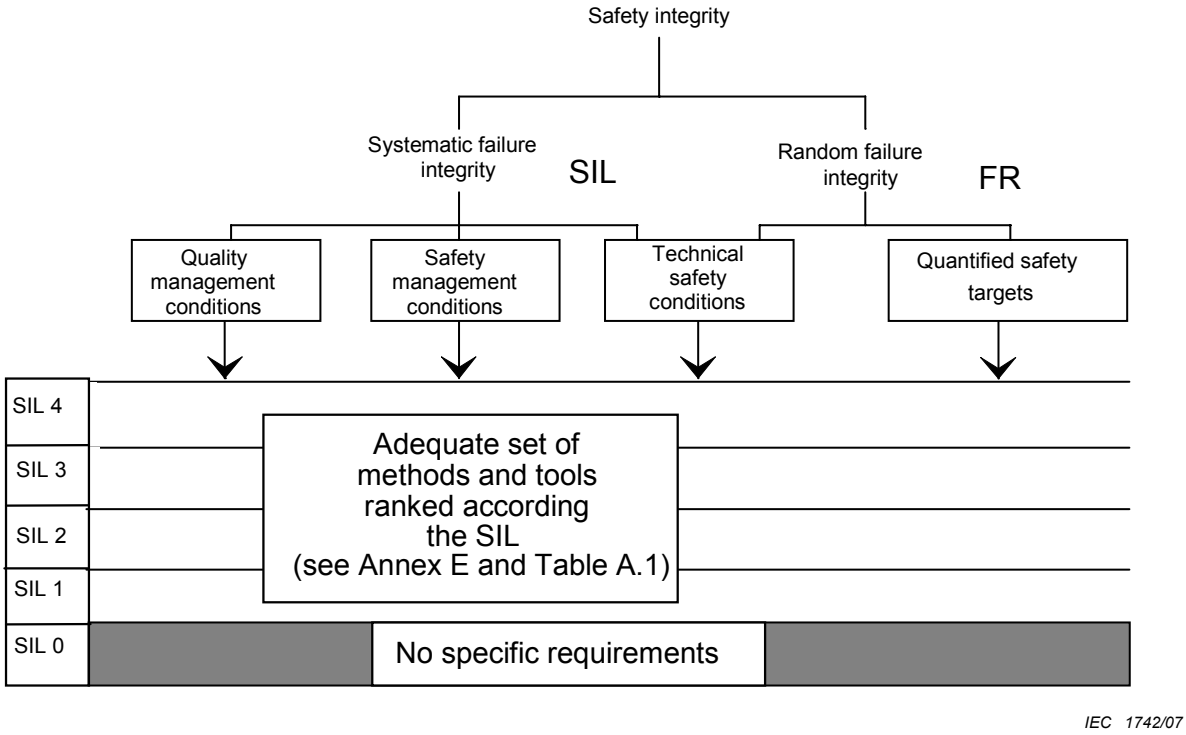


Figure A.8 – Relationship between SILs and techniques

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,..., 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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.2.4 Fulfilment of safety requirements specification

This shall demonstrate how the specified safety functional requirements are fulfilled by the design. All relevant evidence shall be included (or referenced).

EXAMPLE – design principles and calculations;
– test specifications and results;
– safety analyses and results.

B.2.5 Assurance of correct hardware functionality

This shall describe the system/sub-system/equipment hardware architecture, and explain how the design achieves the required integrity, as laid down by the requirements specification and any relevant standards, with respect to

– reliability,
– availability,
– maintainability,
– safety.

Consideration of safety may be limited to fault-free conditions, because effects of faults are dealt with elsewhere (see Clause B.3).

B.2.6 Assurance of correct software functionality

The requirements of IEC 62279 shall be complied with.

All documentation required by IEC 62279 shall be included or referenced in this section, particularly the software validation report and the software assessment report.

In addition, the interaction between hardware and software shall be explained.

NOTE Some particular topics which should receive attention include

– dependence between hardware and software,
– sequence of interaction,
– response times,
– self test routines,
– health monitoring,
– data acquisition techniques,
– graceful degradation,
– negation methods.

B.3 Effects of faults
(Section 3 of the technical safety report)

This section concerns the ability of the system/sub-system/equipment to continue to meet its specified safety requirements in the event of random hardware faults and, as far as reasonably practicable, systematic faults.

Particular aspects which shall be considered are detailed in B.3.1 to B.3.6 below, using the headings from 5.4.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.3.1 Effects of single faults

(See also guidance in Table E.4)

It is necessary to ensure that the system/sub-system/equipment meets its THR in the event of single random fault. It is necessary to ensure that SIL 3 and SIL 4 systems remain safe in the event of any kind of single random hardware fault which is recognised as possible. Faults whose effects have been demonstrated to be negligible may be ignored. This principle, which is known as fail-safety, can be achieved in several different ways:

a) composite fail-safety

   With this technique, each safety-related function is performed by at least two items. Each of these items shall be independent from all others, to avoid common-cause failures. Non-restrictive activities are allowed to progress only if the necessary number of items agree. A hazardous fault in one item shall be detected and negated in sufficient time to avoid a co-incident fault in a second item.

b) reactive fail-safety

   This technique allows a safety-related function to be performed by a single item, provided its safe operation is assured by rapid detection and negation of any hazardous fault (for example, by encoding, by multiple computation and comparison, or by continual testing). Although only one item performs the actual safety-related function, the checking/ testing/detection function shall be regarded as a second item, which shall be independent to avoid common-cause failures.

c) inherent fail-safety

   This technique allows a safety-related function to be performed by a single item, provided all the credible failure modes of the item are non-hazardous. Any failure mode which is claimed to be unlikely (for example, because of inherent physical properties) shall be justified using the procedure defined in Annex C. Inherent fail-safety may also be used for certain functions within composite and reactive fail-safe systems, for example to ensure independence between items, or to enforce shut-down if a hazardous fault is detected.

Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods. The component failure modes to be considered in the analysis shall be identified using the procedures defined in Annex C.

NOTE A top-down failure analysis method should be used, such as fault tree analysis (FTA). This should be supported, if necessary, by a bottom-up method such as failure modes and effects analysis (FMEA). See also guidance given in Table E.6.

Failure analyses shall be qualitative, and quantitative where credible data is available. Random hardware failure rates, or probabilities of component failure, should be based on field data if possible. Apportionment of an overall component failure rate between its failure modes shall be justified in the analysis.

B.3.2 Independence of items

In systems containing more than one item whose simultaneous malfunction could be hazardous, independence between items is a mandatory precondition for safety concerning single faults. Appropriate rules or guidelines shall be fulfilled to ensure this independence. The measures taken shall be effective for the whole life-cycle of the system. In addition, the system/sub-system design shall be arranged to minimise potentially hazardous consequences of loss-of-independence caused by, for example, a systematic design fault, if it could exist.

The various types of influence in a system consisting of, for example, two operating items are represented in Figure B.1. This figure may be extended to systems consisting of more than two operating items.

Where safety is reliant on the clearance and creepage distances, the minimum clearance and creepage distances shall be defined according to the application requirements (including

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

material, technology, implementation, environmental and operation conditions, failures and temporary overvoltages).

Independence could be lost by several types of influences, as explained under the following headings:

a) Type A Physical internal influences

If no physical connection exists between internal items of a system, there are neither physical nor functional influences. Therefore, internal independence is achieved.

NOTE 1 A physical connection is any medium between items, for example:
– galvanic connection;
– electromagnetic coupling.

Measures shall be taken to avoid non-intentional physical internal influences.

NOTE 2 Clause D.2 contains a range of measures for the achievement of physical internal independence (protection against influences of Type A).

b) Type B Functional internal influences

A functional influence between items is based on a physical connection. Measures shall be taken to avoid functional internal influences. This shall be achieved by means of functional internal independence (protection against influences of Type B).

NOTE 3 A functional internal influence would allow faulty information in one item to influence another item in a hazardous manner.

c) Type C Physical external influences

A physical external influence could cause a loss of physical independence between items.

NOTE 4 These could be due to, for example,
– environmental stresses such as EMI, ESD, climatic, mechanical and chemical,
– the power supply, and
– the external inputs and outputs.

Measures shall be taken to avoid non-intentional physical external influences. Clause B.4 contains requirements for external influences which shall be considered.

NOTE 5 Clause D.3 contains a range of measures for the achievement of physical external independence (protection against influences of Type C).

d) Type D Functional external influences

A functional external influence could cause a loss of functional independence between items. Measures shall be taken to avoid functional external influences. This shall be achieved by means of functional external independence (protection against influences of Type D).

NOTE 6 A functional external influence would allow faulty information from an external source to influence the system in a hazardous manner.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

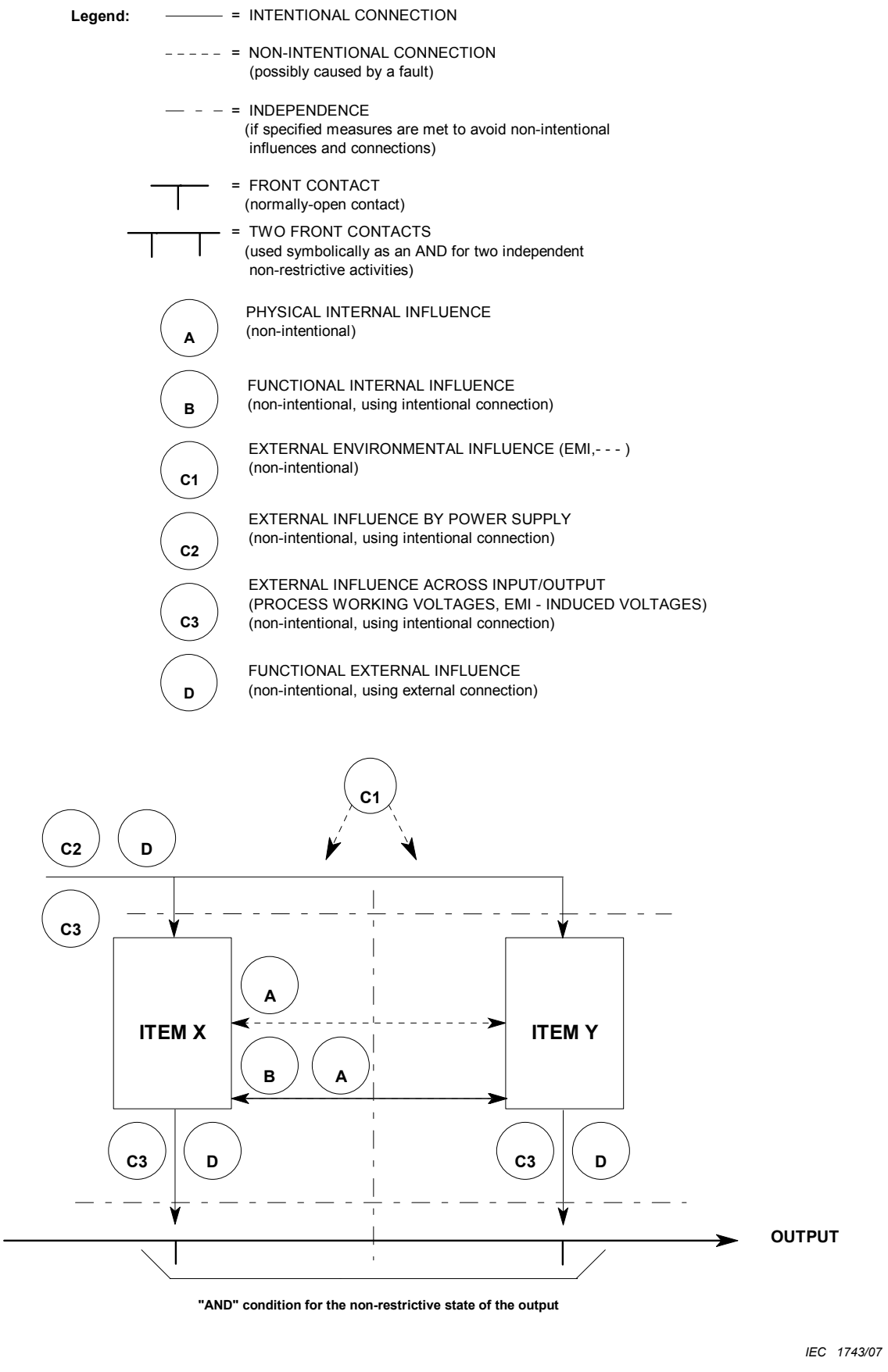


Figure B.1 – Influences affecting the independence of items

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.3.3 Detection of single faults
(See also guidance given in Table E.4)

A first fault (single fault) which could be hazardous, either alone or if combined with a second fault, shall be detected and a safe state enforced (i.e.: negated) in a time sufficiently short to fulfil the specified quantified safety target. Demonstration of this shall be achieved by a combination of failure modes and effects analysis (FMEA) and quantified assessment of random failure integrity (see Clause A.3).

In the case of composite fail-safety, this requirement means that a first fault shall be detected, and a safe state enforced, in a time sufficiently short to ensure that the risk of a second fault occurring during the detection-plus-negation time is smaller than the specified probabilistic target.

In the case of reactive fail-safety, this requirement means that the maximum total time taken for detection-plus-negation shall not exceed the specified limit for the duration of a transient, potentially-hazardous, condition.

These requirements for composite and reactive fail-safety are illustrated in Figure B.2.

The techniques used to achieve detection and negation of identified faults within the permitted time shall be shown, including supporting calculations. The sources of basic failure rate data used in the calculations (for example, hardware component failure rates) shall be identified, and the method of quantitative analysis clearly explained.

NOTE 1 The fault detection time is the test interval in the case of detection by the equipment itself, or the maintenance interval in the case of detection by staff. In the extreme case, it is the installed lifetime of the system. In the case of equipment in storage, it is the interval between periodic testing by maintenance personnel.

NOTE 2 An example of an approach to fulfilment of these requirements is contained in Clause D.4.

B.3.4 Action following detection (including retention of safe state)
(See also guidance in Table E.4)

After detection of a first fault, the system/sub-system/equipment shall enter, or continue in, a safe state. The safe state is generally (but not necessarily) more restrictive. The safe state shall be reached in a time sufficiently short that the combined detection-plus-negation time fulfils the specified safety target.

NOTE The negation time is usually the time taken for the relevant part of the system to be shut down, either automatically or by human action.

These requirements are illustrated in Figure B.2.

After detection of a first fault, and having entered the safe state, further faults shall not cancel out the safe state. Cancellation of a restrictive safe state shall occur only in a controlled manner, as part of a corrective procedure.

The system/sub-system/equipment shall remain in a safe state if further faults occur during permissible delay-times-to-repair after occurrence of a first fault. Permissible delay-times-to-repair shall be sufficiently short to fulfil the specified safety target.

B.3.5 Effects of multiple faults
(See also guidance given in Table E.4)

A multiple fault (for example, a double or triple fault) which could be hazardous, either directly or if combined with a further fault, shall be detected and a safe state enforced (i.e.: negated) in a time sufficiently short to fulfil the specified safety target. A suitable method, for example fault tree analysis (FTA), shall be used to demonstrate the effects of multiple faults. The techniques used to achieve detection-plus-negation of multiple faults within the permitted time shall be shown, including supporting calculations.

NOTE An example of an approach to fulfilment of these requirements is contained in Clause D.5.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

A common-cause failure (CCF) analysis shall be carried out, to provide assurance that a multiple fault could only occur by means of a combination of random single faults, and not as the result of a common-cause fault.

B.3.6 Defence against systematic faults

In addition to the quality and safety management techniques which are used to minimise the probability of human error (see 5.2 and 5.3), technical measures shall be taken such that if a hazardous systematic fault should exist, it would, as far as reasonably practicable, be prevented from creating an unacceptable risk.

EXAMPLE The architecture of the overall system could be configured such that, even in the event of a hazardous failure of a sub-system or item of equipment which has been designed to be safe, an accident would still be unlikely to occur.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

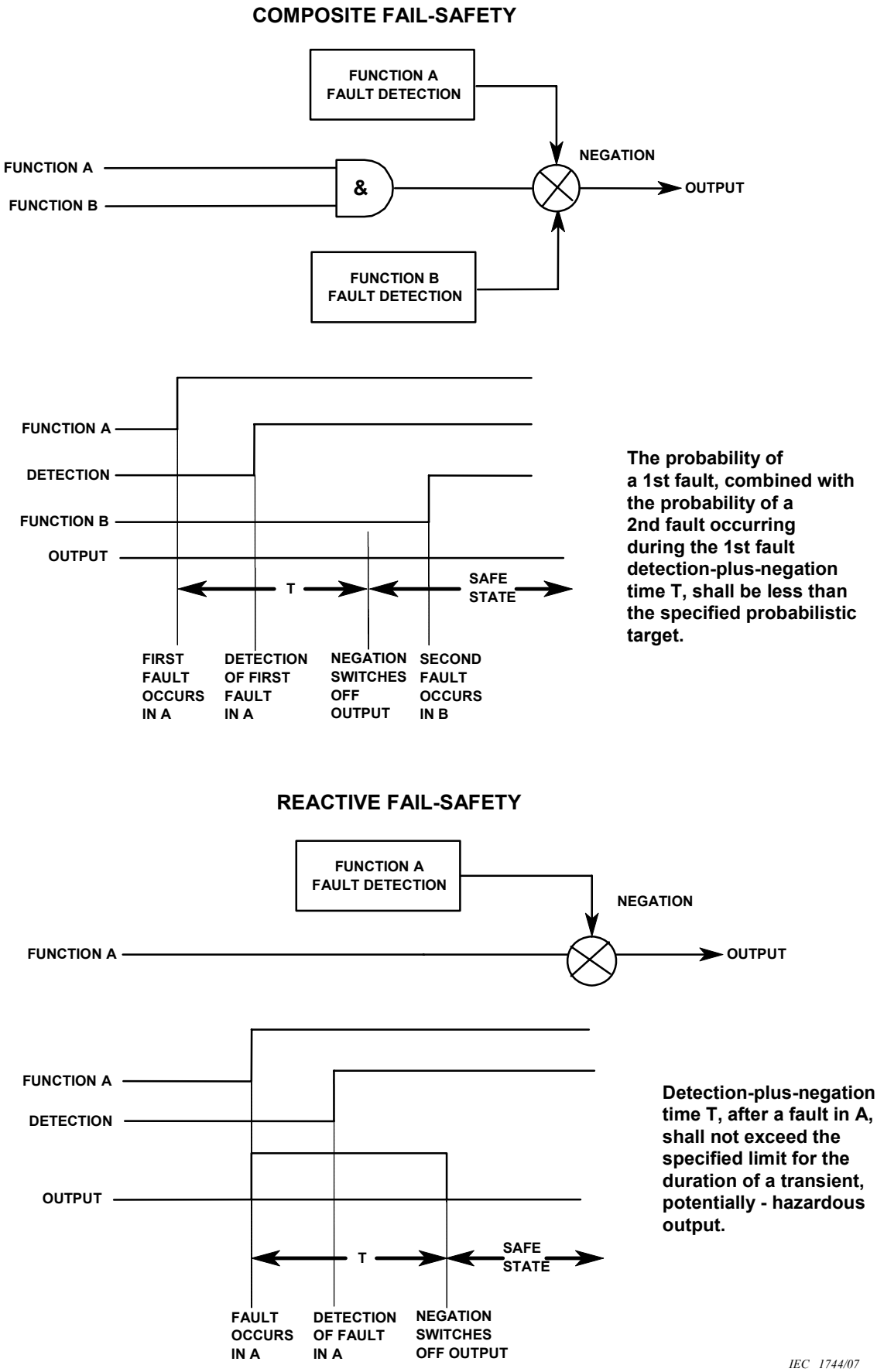


Figure B.2 – Detection and negation of single faults

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.4 Operation with external influences
(Section 4 of the technical safety report)

This section concerns the ability of the system/sub-system/equipment to operate correctly and safely when subjected to specified external influences. "Correct operation" includes fulfilment of both operational and safety requirements.

As far as reasonably practicable, safety-related systems should be designed to remain safe even if subjected to external influences outside the specified limits.

The influences which shall be considered are listed in B.4.1 to B.4.7 below. The values for different conditions listed in EN 50125-1 and EN 50125-3 shall be complied with.

Consideration shall be given to the effects of storage and transportation.

B.4.1 Climatic conditions

It shall be ensured that under the specified climatic environmental conditions, which shall be taken from EN 50125-3, safety to the required international standards is achieved.

If the railway authority specifies more severe conditions than the equipment can fulfil, the supplier can, in agreement with the customer, add measures for climatisation.

B.4.2 Mechanical conditions

It shall be ensured that under the specified mechanical environmental conditions, safety to the required international standards is achieved.

B.4.3 Altitude

It shall be ensured that at the actually occurring altitude, safety to the required international standards is achieved.

NOTE The altitude at which the system/sub-system/equipment is to function does not normally exceed 1 800 m above sea level.

B.4.4 Electrical conditions (not on vehicles)

It shall be ensured that under the specified electrical environmental conditions, safety to the required international standards is achieved.

NOTE The values quoted in IEC 62236-4 and EN 50124-1 should be used as a basis.

B.4.5 Electrical conditions (on vehicles)

It shall be ensured that under the specified electrical environmental conditions on vehicles, safety to the required international standards is achieved.

NOTE The values quoted in IEC 62236, EN 50124-1 and EN 50155 should be used as a basis.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.4.6 Protection against unauthorised access

a) Definition of access levels

The access level defines who has access, reason for access and how access is achieved, thereby guarding against unauthorised access. For each of the particular operations below, persons performing these functions will require to meet certain criteria, which shall be defined with respect to

– skill discipline,

– skill level,

– equipment-specific training.

b) Protection

With respect to the above access levels, this section shall define how protection is to be achieved.

The protective measures should guard against access which is

– accidental, by authorised persons,

– intentional, by unauthorised persons.

c) External conditions

This shall describe how protection is achieved by means additional to the equipment itself.

EXAMPLE – housing;
– security;
– accessibility.

d) Encapsulation

This shall describe how protection is achieved by the actual equipment.

EXAMPLE – covers;
– mounting;
– seals;
– coding, electrical;
– coding, mechanical;
– firmware.

B.4.7 More severe conditions

Where necessary, provision shall be made to deal with additional, more severe, conditions specified by the railway authority.

NOTE The following are examples of more severe conditions:

– condensation due to rapid variation in ambient temperatures of equipment;
– severe pollution of the air by
  - dust;
  - smoke;
  - steam;
  - corrosive chemicals;
  - salt;
  - hydrogen sulphide.

The kinds of pollutants and their concentration should be defined in the specification:

– for outdoor equipment:
  - frost;
  - rapid temperature change;
– chemical influences such as:
  - oil products;
  - organic elements;
  - weed killers;
– excessive heating from, for example, fire or solar radiation;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– action/entry of plants, insects or animals;
– accumulation of dirt and dust (conductive and/or non-conductive);
– more extreme temperature limits in some countries.

B.5 Safety-related application conditions
(Section 5 of the technical safety report)

This section shall define the rules, conditions and constraints relevant to functional safety which need to be observed in the application of the system/sub-system/equipment.

General topics which shall be considered include the following:

– configuration of programmable systems to suit specific applications;
– precautions in manufacturing, installation, testing and commissioning;
– rules and methods for maintenance and fault-finding;
– instructions for system operation;
– safety warnings and precautions;
– electromagnetic compatibility (EMC) precautions (susceptibility and emission);
– information concerning modifications and eventual de-commissioning;
– safety justification of support equipment and tools, such as test equipment, maintenance equipment and configuration tools.

Some specific topics which shall be included are listed in B.5.1 to B.5.3 below.

B.5.1 Sub-system/equipment configuration and system build

a) Configuration

If a sub-system or equipment is such that it has to be configured for each particular application, then any configuration tools and/or procedures shall be defined.

EXAMPLE
– procedural methods;
– version control;
– hardware requirements of configuration system;
– software details of configuration system;
– software maintenance;
– verification and validation;
– simulation.

b) System build

This documentation shall detail how sub-systems and equipment are built into a particular signalling system.

EXAMPLE
– version control settings;
– application control settings;
– interface settings;
– initialisation settings;
– maintenance control settings;
– manufacturing and production testing;
– system test routines;
– installation, testing and commissioning.

c) Change of functionality

If a sub-system or equipment is of sufficient generic design that it could be employed in systems for various applications, then the manner in which it is configured and set-up to

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

meet these different applications shall also be documented. Any limitations or conditions for safe use shall be fully specified.

B.5.2 Operation and maintenance

The necessary minimum maintenance to ensure continued safe and correct operation of the system/sub-system/equipment within the specified environmental conditions shall be documented in the form of an operation and maintenance plan, which shall include the following aspects:

a) operational status

The conditions that exist in each system/sub-system/equipment shall be defined to provide operating and maintenance personnel with sufficient understanding during the following situations:

1) start-up

This shall describe the start-up conditions of the system, sub-system or equipment when power is initially applied, or following shut-down due to power interruption or other cause.

NOTE This should define, for example,

– default conditions,

– initialisation period,

– self checks performed,

– manual intervention required,

– condition of outputs,

– precautions after an exceptional event, such as fire or unauthorised entry.

2) normal operation

Once the system/sub-system/equipment has successfully completed initialisation, the conditions during normal operation shall be defined.

EXAMPLE – cycle times;
– non-data routines;
– disclosure of faults.

3) changeover

If the equipment, or the system/sub-system in which it is configured, has a facility to change over to either a cold or hot standby system/sub-system, then the conditions defined in a) and b) shall be re-stated for this changeover routine. The reaction of the equipment to the changing of failed modules shall also be clearly defined.

4) shut-down

When a system, sub-system or item of equipment is shut down intentionally for a configuration change or de-commissioning, or unintentionally via a power failure, then all relevant conditions shall be defined.

EXAMPLE – default conditions;
– conditions for graceful degradation;
– safety aspects;
– procedures;
– influences on other connected systems.

b) maintenance levels

These shall be defined with respect to

– first line maintenance,

– second line maintenance by customer,

– second line maintenance by manufacturer.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

NOTE 1 "First line" is preventative maintenance and fault-finding/repair carried out on site, with "second line" being preventative maintenance and possible repair in a workshop environment, that is, off site.

c) periodic maintenance

In describing the periodic maintenance required, reference shall be made to all relevant areas.

EXAMPLE
- training;
- accessibility;
- modularity;
- interchangeability;
- spares provisions;
- storage of spares.

d) maintenance aids

For each level of maintenance, the maintenance aids available to personnel shall be defined.

NOTE 2 These aids should include, for example,

- fault diagnostics,
- interpretation of fault messages,
- fault correction.

B.5.3 Operational safety monitoring

During the operation and maintenance phase of the system life-cycle, the performance of the system/sub-system/equipment shall be monitored to ensure that the features incorporated into the design, and the assumptions made during the initial safety assessment, remain valid for the actual circumstances encountered during in-service use.

NOTE This should include, for example,

- the monitoring of safety-related performance and comparison with the predicted performance,
- the monitoring and assessment of failure reports to detect failure trends or possible hazardous failures which can be corrected, thereby improving safety and reliability,
- investigation of incident and accident reports to identify any changes required to improve the safety performance of the system.

B.5.4 Decommissioning and disposal

The technical safety precautions and procedures which will be necessary when the system/sub-system/equipment is eventually decommissioned shall be documented. This shall include consideration of possible phased introduction of replacement systems whilst the railway continues in operation.

Appropriate warnings and instructions concerning final disposal of equipment after decommissioning shall also be included.

B.6 Safety qualification tests
(Section 6 of the technical safety report)

This section shall contain evidence to demonstrate successful completion of the safety qualification tests under operational conditions.

The purpose of these tests is

- to gain increased confidence that the system/sub-system/equipment fulfils its specified operational requirements,

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– to gain increased confidence that the specified reliability and safety targets have been achieved,
– to allow systems/sub-systems/equipment to be put into operational service before final safety approval, subject to provision of appropriate precautions and monitoring.

NOTE These tests only provide increased confidence and are not the unique means for demonstration of safety.

B.6.1 Requirements

The extent and duration of the safety qualification tests shall be agreed between the railway authority and the safety authority, and shall be justified having regard to the degree of novelty and complexity associated with the system/sub-system/equipment.

Because completion of the safety qualification tests is contained within the safety case, the safety of the system is not fully assured during the test period. Therefore, appropriate precautions, procedures and monitoring shall be provided, to ensure safety of the railway during the test period.

Safety qualification tests, as defined, shall be completed before commencing operation with full responsibility for safety.

A record shall be established which explains when the system is put into service, with or without passengers, with or without precautions, and what is the authorisation level obtained at each stage (provisional or final safety approval).

B.6.2 Results

An account of the safety qualification tests, including a full description of the tests carried out and the results obtained, shall be documented in this section of the technical safety report.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annex C
(normative)

Identification of hardware component failure modes

C.1 Introduction

This annex contains procedures and information for identifying the credible failure modes of hardware components.

NOTE The tables of hardware component failure modes included in this annex have been derived from international experience and also from the following sources listed in Bibliography:

– UIC/ORE Report A155/RP12;

– MIL-HDBK-338-1A;

– German Federal Railways Mü8004;

– Reliability Analysis Center Report FMD-91.

The information in the tables may be modified, as explained in C.2 and C.5, if adequate justification is provided for such variations.

C.2 General procedure

For the purpose of analysing the results of single faults (see B.3.1), it is necessary to identify the credible failure modes of each hardware component.

Tables C.1 to C.16 contain lists of hardware component failure modes which shall be used as the basis for design and analysis, unless justification is provided for any variation. The general notes in C.5 shall be observed.

The lists are not necessarily complete, and any additional failure modes which are considered to be credible shall be added to the analysis. In such cases, the extra failure modes shall be brought to the attention of the relevant authority, so that the lists can be extended at a future date, by means of the normal CENELEC procedure.

C.3 Procedure for integrated circuits (including microprocessors)

Designs which employ integrated circuits require special treatment, since it can be difficult to predict all the credible failure modes that the device may possess. This is particularly true for programmable devices, since the failure modes that may be observed at the boundary of the device are application specific.

It is recommended that the hazardous failure modes be identified in a top-down manner for the specific application, using a technique such as fault tree analysis. (An alternative would be to use a bottom-up approach such as failure modes and effects analysis, but this method is time-consuming and it is possible that certain hazardous failure modes could be missed).

As assessment and justification shall then be made, to show that for each identified hazardous failure mode

either a) the failure mode cannot credibly occur, due to the internal software architecture or data structure,

or b) the failure mode will be externally detected and a safe state imposed within the required time. In this case, quantitative analysis shall be performed to justify the design, and a pessimistic view shall be taken whereby the hazardous failure modes are assumed to take the full component failure rate.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

NOTE Some items, such as "intelligent" sensors, employ embedded microprocessors. Such items should be assessed using the same methods as outlined above for integrated circuits.

C.4 Procedure for components with inherent physical properties

If the technique of inherent fail-safety is used (see B.3.1), full justification shall be provided for any component failure mode which is considered to be unlikely. This justification shall include, but not necessarily be limited to, the following topics:

– theoretical explanation of inherent physical properties;
– evidence of compliance with recognised quality standards;
– explanation of special construction of components;
– explanation of special mounting arrangements or other precautions for the component;
– evidence that the failure mode will not occur as a result of component ratings being exceeded (for example, because of fault or overload conditions);
– results of tests to demonstrate fail-safe behaviour of component under adverse conditions (by means of physical tests, technical justifications, or simulation);
– evidence of previous experience of reliance on the component for inherent fail-safety.

If satisfactory justification is provided, the relevant component failure modes may be excluded from the safety analysis.

It is not necessary to repeat the justification if it has already been provided in the past; it is sufficient to make reference to the previous justification report. However, if this justification includes particular conditions (for example, special mounting arrangements or means for prevention of overload), the fulfilment of these conditions shall be included in the safety case.

Previous experience indicates that some particular component failure modes are more likely to be capable of justification as unlikely; these failure modes are indicated by (*) in Tables C.1 to C.16, together with relevant guidance notes in Clauses C.6 and C.7. Other component failure modes are much less likely to be capable of justification as unlikely. Note that justification shall be provided for all failure modes which are considered to be unlikely, including those which are indicated in the tables.

C.5 General remarks concerning component failure modes

1) Tables C.1 to C.16 contain lists of credible failure modes of hardware components.
2) The failure modes are as manifested at the boundary of the components, and not the internal physical causes of the failures.
3) All listed failure modes could be intermittent.
4) Intermittent failures are caused by environmental influences such as temperature variation or mechanical stress (see relevant environmental standards). Therefore, the frequency of intermittent failures will be in accordance with these reasons.
5) Variations within the tolerances of a component's published specification are not considered to be failures.
6) It is assumed that components are operated within their published environmental limits.
7) It is assumed that components are operated within their published electrical ratings.
8) External short-circuit or leakage between terminals of a component is not considered to be a component failure. For suitable creepage and clearance distances, refer to item 10).
9) External short-circuit or leakage between different components is not considered to be a component failure. For suitable creepage and clearance distances, refer to item 10). Stable mounting and/or special fastening will be necessary if environmental conditions could change the position of a component.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

10) Where safety is reliant on clearance and creepage distances, the minimum clearance and creepage distances shall be defined according to the application requirements (including material, technology, implementation, environmental and operating conditions, failure conditions and temporary overvoltages). EN 50124-1 or IEC 60664 shall be used to determine minimum requirements based on re-inforced insulation. These requirements shall be accepted or further strengthened or complemented by the railway authority.

C.6 Additional general notes, concerning components with inherent physical properties

1) The procedure and conditions for justification of any component failure mode as unlikely are contained in Clause C.4.

2) Failure modes indicated by (*) in Tables C.1 to C.16 are those which are more likely to be capable of being justified as unlikely.

3) "Note xy" following (*) in Tables C.1 to C.16 refers to guidance notes in Clause C.7 on some factors that are relevant to possible justification of the failure mode as unlikely.

4) The general notes in Clause C.5 apply also to components with inherent physical properties, with the following additions in items 5), 6) and 7) below.

5) In addition to item 5) in Clause C.5, it is recommended that some allowance be made for variations which exceed the normal tolerances.

6) In addition to item 6) in Clause C.5, it is recommended that some allowance be made for excursions beyond the normal environmental limits.

7) In addition to item 7) in Clause C.5, a margin shall be ensured within the published electrical ratings, so that the component is protected from being overloaded.

8) Not used.

9) Not used.

C.7 Specific notes concerning components with inherent physical properties

The following notes provide guidance concerning possible justification of the failure modes identified by (*) in Tables C.1 to C.16 as unlikely.

10) The body shall have no hollows.

The resistance shall be limited to the lowest possible value (for example, no greater than 10 kΩ).

Clearance and creepage distances between the caps/connection wires at each end of the component shall at least fulfil the requirements of EN 50124-1, in accordance with its requirements for re-inforced insulation.

The component shall be coated with cement or enamel. In other cases, the coating shall be non-conductive, even at the highest temperature (including fault conditions).

The body shall be constructed of material which is non-conductive, even at the highest temperature (including fault conditions).

Additional guidance for a wire-wound resistor:

The winding of a wire-wound resistor shall have only one layer.

Short-circuit between turns of a wire-wound resistor shall be avoided by coating of the wire, and/or by physical separation of the turns.

11) The 4-terminal resistor shall be constructed in such a way that, if a fault causing interruption of the resistance material occurs, this fault would also cause interruption of at least one of the four connecting terminals.

The circuitry external to the resistor shall disclose the interruption of the terminal(s) in a fail-safe manner.

Example of a 4-terminal resistor, using a hybrid thick layer technique (see Figure C.1):

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

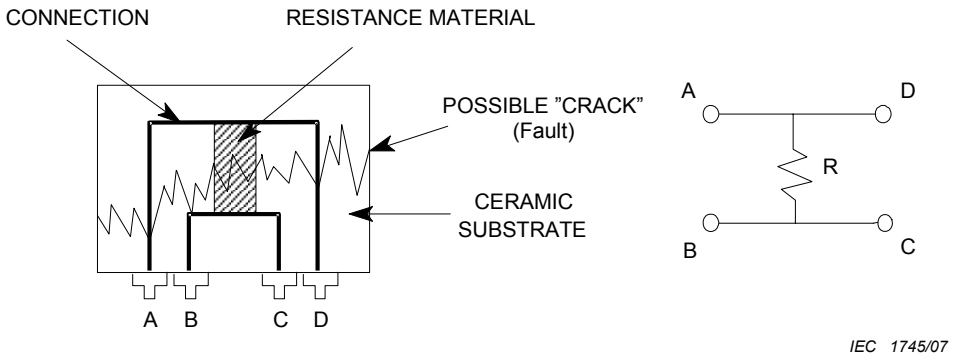


Figure C.1 – Example of a 4-terminal resistor, using a hybrid thick layer technique

12) Two terminals shall be connected independently to each side of the component.

13) The formula to calculate capacitance of a simple parallel-plate capacitor is

$$C = \varepsilon_0 \cdot \varepsilon_r \cdot \frac{A}{d}$$

where

A is the common area of plates;

d is the distance between plates;

ε_0 is the permittivity of free space;

ε_r is the relative permittivity (dielectric constant).

Justification of the failure mode as unlikely requires demonstration that none of these parameters can significantly change.

Electrolytic capacitors are not suitable for exclusion from this failure mode.

14) The capacitor shall be designed and constructed for high-voltage application in relation to the maximum possible operating voltage (including fault conditions). It shall have Class-Y specification, and self-healing properties at the working source impedance and over the working voltage range.

15) There shall be only one layer of turns, separated by means of grooves in the insulated body, or the wire shall have re-inforced insulation.

The turns shall be securely fastened.

16) Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

All windings and connections shall be securely fastened.

Power dissipation shall be limited sufficiently to prevent internal carbonisation (including fault conditions).

17) The magnetic core shall be constructed such that no significant change in reluctance of the magnetic path can occur.

18) The transfer ratio depends upon the number of turns on each winding, and on the integrity of the magnetic coupling. Therefore, it is necessary for items 15), 16) and 17) to be fulfilled.

19) The transductance and the d.c. threshold voltage depend upon the properties of the magnetic core material. Therefore, it is necessary to demonstrate that these magnetic properties cannot significantly change.

Transductance and d.c. threshold voltage also depend on the number of turns on each winding, and on the integrity of the magnetic coupling. Therefore, it is also necessary for items 15), 16) and 17) to be fulfilled.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

The output from a transductor is related to the number of ampere-turns in the control winding. It is necessary to demonstrate that, in conjunction with the associated drive circuitry, no credible failure modes of the control winding can cause an increase in the number of ampere-turns.

20) All parts of the relay or switch mechanism shall be robustly constructed and securely fastened, including

- the operating mechanism,
- the contact system,
- the magnetic circuit (if any),
- the coil(s) (if any).

Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

21) Contact materials which are not capable of being welded shall be chosen.

The risk of welding shall be further reduced by appropriate mechanical design and construction of the contacts.

The maximum current shall be limited, to ensure that the temperature of the contacts does not reach a value at which welding could occur.

22) Stability of the relay's characteristics shall be ensured by careful attention to the following factors:

- magnetic characteristics:
  - choice of magnetic material;
  - provision of a stop device to avoid permanent magnetisation of the magnetic circuit (core);
  - protection against external magnetic fields;
- electrical characteristics:
  - choice and quality of the wire and insulation;
  - quality of winding of the coil;
  - quality of terminations;
- mechanical characteristics:
  - choice and quality of materials;
  - secure fastening of all parts;
  - secure retention of all safety-related adjustments;
  - provision of adequate return force
    - using gravity (supplemented, if necessary, by springs and/or by elasticity of blades);
    - using springs (and/or by elasticity of blades), designed appropriately;
  - design and construction of the operating mechanism such that it cannot become jammed.

23) The threshold voltage of a p-n junction, such as a diode or a transistor base-emitter junction, is a function of

- minority and majority charge-carrier densities,
- boltzmann's constant (k),
- electron charge (e),
- temperature (K).

Therefore, the threshold voltage is dependent on non-variable characteristics of the p-n junction, and should be constant for a given temperature.

24) The breakdown voltage is determined by one of two possible mechanisms: Zener breakdown or avalanche breakdown. Both of these are dependent on non-variable physical characteristics of the diode, so the breakdown voltage should be constant for a given temperature.

Care shall be taken to avoid components which consist internally of two or more diodes connected in series.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Note that conduction at voltages above and below the breakdown voltage may be possible, due to shunt or series resistance, but the differential (slope) resistance in such cases would be higher than for the case of breakdown conduction.

25) The amplification (or gain, or transconductance) of a transistor, and the optical sensitivity of a photo-diode or transistor, are dependent on

– doping levels,

– thickness of the junction(s),

– life-time of charge carriers.

These parameters should remain constant, with the exception of the charge carriers' life-time, which can only decrease with time. Therefore, the amplification/sensitivity should remain constant, or possibly decrease, but not increase (has to be justified for each application).

A small possibility exists of an increase in amplification caused by pollution affecting surface doping. This can be avoided by high-quality manufacture and packaging of the component. Also this effect is only significant for very low bias currents, which shall therefore be avoided when designing circuits.

26) Light emission is a physical property related to recombination of electrons and holes when current flows in a forward-biased p-n junction.

The rate of recombination is a function of the forward current, and therefore the light emission should not increase at constant current.

Below the threshold voltage there is no significant current flow and therefore no light emission.

27) If the p-n junction is reverse biased, there will be no significant current flow below the breakdown voltage and therefore no light emission.

Above the breakdown voltage, the mechanism that allows current to flow is different to that for forward bias and should not result in emission of light.

28) For optocouplers and self-contained fibre-optic systems, the failure modes of each element shall be considered, i.e.

– light-emitting transmitter,

– optical medium,

– photo-sensitive receiver.

29) Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

The construction of the components shall be robust and stable.

Power dissipation in the component shall be limited sufficiently to prevent internal carbonisation (including fault conditions).

30) Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

The input and output drive/coupling elements shall be securely fastened.

31) The component shall be robustly constructed.

The resonator(s) shall be constructed and mounted so as to prevent change of their effective dimensions.

The resonator(s) shall be constructed of a material whose dimensions are not significantly altered by changes of temperature.

The material of the resonator(s) shall be stabilised by temperature cycling and/or pre-operation for a sufficient time.

The material of the resonator(s) shall not be over-stressed, even under fault conditions. In particular the limit of elasticity shall not be exceeded.

32) The transfer ratio is a function of the efficiency of the drive/coupling elements and the Q-factor of the filter.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

The drive/coupling elements shall be designed and constructed so as to prevent any significant increase in their efficiency.

33) The resonator(s) shall be constructed and mounted to obtain the maximum possible Q-factor, so that no subsequent improvement can occur.

34) The resonator(s) shall be constructed and mounted so as to prevent the occurrence of damping by any mechanism.

35) The insulating material shall be stable.

Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

36) The connector shall be robustly constructed.

All parts of the connector shall be securely fastened.

37) Incorrect orientation of the connector, or insertion into the wrong socket, shall be prevented by means of, for example, mechanical design or mechanical pin-coding.

Alternatively, the effects of incorrect insertion shall be rendered non-hazardous by means of, for example, electrical coding of connector pins or allocation of unique addresses/identities.

The risk shall be further reduced by means of warning labels and training of personnel.

38) The screen shall be robustly constructed and protected from excessive physical damage.

The electrical connection to the screen shall be robust and securely fastened.

39) Sufficiently robust insulation shall be provided.

Clearance and creepage distances shall fulfil at least the requirements for re-inforced insulation of EN 50124-1.

Protection shall be provided against excessive physical damage.

Protection shall be provided against electrically conductive foreign bodies.

40) The fuse and its holder shall be physically constructed and mounted so as to prevent the occurrence of a parallel short-circuit.

Means shall be provided to prevent the use of an incorrectly rated fuse.

Means shall be provided to prevent the use of a fuse with self-resetting or self-healing capability.

Table C.1 – Resistors

a) All kinds of resistor and adjustable resistor (excluding 4-terminal resistor)	
Interruption	
Short-circuit	(*) item 10
Increase of resistance value	
Decrease of resistance value	(*) item 10
Short-circuit to case	
b) Four-terminal resistor	
Interruption of each terminal	
Interruption of resistance material	(*) item 11
Short-circuit	(*) item 10
Increase of resistance value of each terminal	
Decrease of resistance value	(*) item 10
Short-circuit between two terminals of same side	(*) item 12
Short-circuit to case	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.2 – Capacitors

a) All kinds of capacitor and adjustable capacitor (excluding 4-terminal capacitor)	
Interruption	
Short-circuit	(*) item 14
Increase of capacitance	(*) item 13
Decrease of capacitance	(*) item 13
Decrease of parallel resistance	(*) item 14
Increase of series resistance	
Short-circuit to case	
b) Four-terminal capacitor	
Interruption of each terminal	
Short-circuit	
Increase of capacitance	(*) item 13
Decrease of capacitance	(*) item 13
Decrease of parallel resistance	(*) item 14
Increase of series resistance	
Short-circuit between two terminals of same side	(*) item 12
Short-circuit to case	

Table C.3 – Electromagnetic components

a) Inductor	
Interruption of winding	
Short-circuit of winding – between turns – between layers – whole winding	 (*) item 15 (*) item 16 (*) item 16
Short-circuit or decrease of insulation between winding and body	(*) item 16
Increase of resistance of winding	
Increase of inductance	(*) item 17
Decrease of inductance	(*) item 17
b) Transformer	
Interruption of any winding	
Short-circuit of any winding – between turns – between layers – whole winding	 (*) item 15 (*) item 16 (*) item 16
Short-circuit or decrease of insulation – between windings	(*) item 16
Short-circuit or decrease of insulation between – any winding and body	(*) item 16

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.3 *(continued)*

Increase of resistance of any winding	
Increase of inductance of any winding	(*) item 17
Decrease of inductance of any winding	(*) item 17
Change of transfer ratio	(*) item 18
c) Transductor (saturable reactor or magnetic amplifier)	
Interruption of any winding	
Short-circuit of d.c. winding	
Short-circuit of a.c. winding	
– between turns	(*) item 15
– between layers	(*) item 16
– whole winding	(*) item 16
Short-circuit or decrease of insulation resistance	
– between d.c. and a.c. windings	(*) item 16
– between any winding and body	(*) item 16
Increase of inductance of a.c. winding	(*) item 17
Decrease of inductance of a.c. winding	(*) item 17
Increase of transductance	(*) item 19
Decrease of transductance	
Increase of d.c. threshold voltage	
Decrease of d.c. threshold voltage	(*) item 19
d) Relay	
Interruption of any coil	
Interruption of any contact	
Short-circuit or decrease of insulation resistance	
– across open contacts	(*) item 20
– between coil and coil	(*) item 16
– between coil and contact	(*) item 20
– between coil and case	(*) item 16
– between contact and contact	(*) item 20
– between contact and case	(*) item 20
Welding of contacts	(*) item 21
Increase of contact resistance	
Increase of contact chatter time	
Increase of pick-up current	
Decrease of pick-up current	(*) item 22
Increase of drop-away current	
Decrease of drop-away current	(*) item 22
Change of pick-up to drop-away ratio	(*) item 22
Increase of pick-up time	
Decrease of pick-up time	(*) item 22
Increase of drop-away time	(*) item 22

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.3 *(continued)*

Decrease of drop-away time	(*) item 22
Relay does not pick up	
Relay does not drop away	(*) item 22
Closure of any front contact at the same time as any back contact (transient or continuous)	(*) item 22
Non-correspondence between front contacts	
Non-correspondence between back contacts	

Table C.4 – Diodes

a) Normal diode (power, signal, switching)	
Interruption	
Short-circuit	
Increase of reverse current	
Decrease of reverse breakdown voltage	
Increase of conducting-state voltage	
Decrease of conducting-state voltage	
Increase of threshold voltage	(*) item 23
Decrease of threshold voltage	(*) item 23
Short-circuit to conductive case	
b) Zener diode	
Interruption	
Short-circuit	
Increase of Zener voltage	(*) item 24
Decrease of Zener voltage	(*) item 24
Change of differential resistance	
Increase of reverse current	
Increase of forward conducting-state voltage	
Decrease of forward conducting-state voltage	
Increase of forward threshold voltage	(*) item 23
Decrease of forward threshold voltage	(*) item 23
Short-circuit to conductive case	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.5 – Transistors

a) Bipolar transistor	
Interruption – of emitter (E) – and/or base (B) – and/or collector (C)	
Short circuit – between E and B – between B and C – between E and C – between E and B and C	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and E or B or C	
Increase of d.c. and/or a.c. amplification	(*) item 25
Decrease of d.c. and/or a.c. amplification	
Increase of base-emitter conducting-state voltage	
Decrease of base-emitter conducting-state voltage	
Increase of threshold voltage V_{BE}	(*) item 23
Decrease of threshold voltage V_{BE}	(*) item 23
Decrease of break-down voltage V_{EB} or V_{CB} or V_{CE}	
Change of rise time, fall time, turn-on time, turn-off time	
Increase of leakage current I_{CB}, I_{EB}, I_{CE}	
Change of saturation voltage V_{CE}	
b) Field-effect transistor (FET)	
Interruption – of gate (G) – and/or source (S) – and/or drain (D)	
Short-circuit – between S and D – between G and D – between S and G – between S and G and D	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and S or G or D	
Increase of forward transconductance	(*) item 25
Decrease of forward transconductance	
Increase of gate threshold voltage	
Decrease of gate threshold voltage	
Decrease – of drain-source break-down voltage – of gate-source and drain-gate maximum rated voltages	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.5 *(continued)*

Change of turn-on-time and turn-off time	
Increase of leakage current I_{GS}, I_{DS}, I_{GD}	
Change of static drain to source on-state resistance	

Table C.6 – Controlled rectifiers

a) Silicon – controlled rectifier (SCR) (thyristor)	
Interruption – of gate (G) – and/or anode (A) – and/or cathode (C)	
Short-circuit – between G and C – between G and A – between A and C – between A and G and C	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and A or G or C	
Change of holding current	
Change of gate trigger current and/or of gate trigger voltage	
Decrease – of anode-cathode forward blocking voltage – of anode-cathode reverse blocking voltage – of reverse gate maximum rated voltage	
Change of turn-on time and turn-off time	
Increase of leakage current I_{AC}, I_{GC}, I_{GA}	
Change of forward static on-voltage	
b) Bidirectional thyristor (triac)	
Interruption – of gate (G) – and/or of MT1 (first current-carrying terminal) – and/or of MT2 (second current-carrying terminal)	
Short-circuit – between G and MT1 – between G and MT2 – between MT1 and MT2 – between MT1 and G and MT2	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and MT1 or G or MT2	
Change of holding current	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.6 *(continued)*

Change of gate trigger current and/or of gate trigger voltage	
Decrease of MT1-MT2 maximum rated off-state voltage and/or of gate maximum rated voltage	
Increase of leakage current MT1-MT2, G-MT1, G-MT2	
Change of static on-voltage	

Table C.7 – Surge suppressors

a) Voltage-dependent resistor (VDR) (varistor)	
Interruption	
Short-circuit	
Increase of clamp voltage	
Decrease of clamp voltage	
Increase of leakage current	
b) Protective diode (tranzorb)	
Interruption	
Short-circuit	
Increase of breakdown voltage	(*) item 24
Decrease of breakdown voltage	(*) item 24
Increase of leakage current	
Short-circuit to conductive case	
c) Gas-discharge arrester	
Interruption	
Short-circuit	
Increase of breakdown voltage	
Decrease of breakdown voltage	
Increase of leakage current	
d) Air-gap arrester	
Interruption	
Short-circuit	
Increase of breakdown voltage	
Decrease of breakdown voltage	
Increase of leakage current	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.8 – Opto-electronic components

a) Photo diode	
Interruption	
Short-circuit	
Increase of light sensitivity	(*) item 25
Decrease of light sensitivity	
Increase of leakage current	
b) Photo transistor	
Interruption	
Short-circuit	
Increase of light sensitivity	(*) item 25
Decrease of light sensitivity	
Increase of leakage current	
c) Light-emitting diode (LED)	
Interruption	
Short-circuit	
Increase of light emission (at constant current)	(*) item 26
Decrease of light emission (at constant current)	
Increase of leakage current	
Increase of threshold voltage	(*) item 23
Decrease of threshold voltage	(*) item 23
Light emission below threshold voltage	(*) item 26
Light emission with reverse polarity	(*) item 27
d) Optocoupler and self-contained fibre-optic system (see item 28)	
Short-circuit or decrease of insulation resistance – between input and output – between adjacent systems in the same case	 (*) item 29 (*) item 29
Short-circuit to casing	
Change of switching time	
Increase of current transfer ratio	(*) items 25 and 26
Decrease of current transfer ratio	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.9 – Filters

a) Crystal	
Interruption	
Short-circuit	
Change of resonant frequency	
Decrease of Q-factor	
Short-circuit to conductive case	
b) Mechanical resonator (turning fork/reed/pendulum)	
Interruption	
Short-circuit or decrease of insulation resistance – between input and output – between input or output and case	 (*) item 30 (*) item 30
Change of resonant frequency	(*) item 31
Increase of transfer ratio	(*) items 32 and 33
Decrease of transfer ratio	
Increase of Q-factor	(*) item 33
Decrease of Q-factor	(*) items 31 and 34

Table C.10 – Interconnection assemblies

a) Printed-circuit board	
Interruption or increase of resistance in one or more lines	
Short-circuit or decrease of insulation between two different lines	(*) item 35
b) Connector	
Interruption of – one or more contacts – shield	
Short-circuit or decrease of insulation resistance – between contact and contact – between contact and shell	 (*) items 35 and 36 (*) items 35 and 36
Wrong mechanical position	(*) item 37
c) Cable and wire	
Interruption or increase of resistance in one or more wires	
Interruption or increase of resistance of screen	(*) item 38
Short-circuit or decrease of insulation resistance – between wire and wire, or more than one wire – between wire or wires and screen – between wire or wires or screen and external conductive parts	 (*) item 39 (*) item 39 (*) item 39

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.10 *(continued)*

Multiple interruptions and short-circuits	(*) item 39
d) Connection – soldered, welded, wrapped, crimped, clipped, screwed	
Interruption	
Increase of resistance	
e) Fibre-optic cable	
Interruption	
Increase of attenuation	
f) Fibre-optic connector	
Interruption	
Increase of attenuation	

Table C.11 – Fuses

Interruption	
Parallel short-circuit	(*) item 40
Increase of rupture current	(*) item 40
Increase of rupture time	(*) item 40
Reconnection after rupture	(*) item 40

Table C.12 – Switches and push/pull buttons

Interruption of any contact	
Short-circuit or decrease of insulation resistance	
– across open contacts	(*) item 20
– between contact and contact	(*) item 20
– between contact and case	(*) item 20
Welding of contacts	(*) item 21
Increase of contact resistance	
Device jammed in current state	
Increase of contact chatter time	

Table C.13 – Lamps

Interruption	
Short-circuit	
Decrease of light intensity	
Short-circuit to conductive case	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table C.14 – Batteries

Interruption	
Short-circuit – of individual cell – of multiple cells – of whole battery	
Decrease of e.m.f.	
Increase of internal resistance	

Table C.15 – Transducers/sensors (not including those with internal electronic circuitry)

Interruption	
Short-circuit	
Output too high	
Output too low	
Time response too long	
Short-circuit to conductive case	

Table C.16 – Integrated circuits

a) Analogue devices	
Functional malfunction: see Clause C.3	
b) Digital devices	
Functional malfunction: see Clause C.3	
c) Microprocessors	
Functional malfunction: see Clause C.3	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annex D
(informative)

Supplementary technical information

D.1 Introduction

This annex provides examples and guidance to supplement the technical requirements contained in 5.4 and Annex B. The given requirements are only valid for SIL 3 or SIL 4.

D.2 Achievement of physical internal independence
(Protection against influences of type A, as referred to in B.3.2)

D.2.1 Primary independence

The following measures provide "primary independence" between two items whose simultaneous malfunction could be hazardous:

a) measures to avoid non-intentional galvanic connections

   (protection of internal galvanic insulation)

   1) Insulation between lines on the same layer of a printed-circuit board.

      Insulation distances (creepage distances and clearances) should be dimensioned at least according to the requirements for re-inforced insulation of EN 50124-1.

   2) Insulation between lines on different layers of a multilayer printed-circuit board.

   3) Insulation between insulated wires in the same cable.

   4) Insulation between insulated windings in the same transformer.

      Maximum temperature inside transformers should be limited (including fault conditions), to avoid carbonisation.

   5) Insulation between insulated items inside an opto-coupler.

      Maximum temperature inside opto-couplers should be limited (including fault conditions), to avoid carbonisation.

b) measures to avoid non-intentional effects via intentional connections

   (protection of internal interfaces)

   Interfaces should be protected by means of devices with inherent properties.

c) measures to avoid non-intentional effects via electromagnetic coupling

   (protection against internal cross-talk)

   Cross-talk between electronic networks should be prevented as follows:

   1) if different items are on the same printed-circuit board, they should be supplied by different power-supply networks. If not, then the impedance of the ground network should be sufficiently low to avoid cross-talk, even in the event of faults;

   2) if different lines on the same board need to be protected against cross-talk occurring between them, the necessary separation distance depends on the used technology, the coupling length and the coupling mechanism. This distance should be demonstrated for the normal operational mode by theoretical calculations and/or by practical measurements;

   3) if necessary, to avoid coupling in the event of faults, additional measures (for example, shielding or doubling of distance) should be taken. Effectiveness should be demonstrated by theoretical calculations and/or by practical measurements.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

D.2.2 Secondary independence

The following measures provide "secondary independence" between two items whose simultaneous malfunction could not be hazardous:

a) each item in a *n*-out-of-*m* system may consist of a number of independent items;

b) independence of two items whose simultaneous malfunction could be hazardous is achieved as written in D.2.1 (primary independence). These items will be referred to as "main items". Each main item can have one or more so called "additional items" checking the main item;

c) the degree of independence between a main item and an additional item may be less than written in D.2.1 and is called "secondary independence";

d) main items are independent from additional items if all possible first-fault-effected influences between them are detected before they can become hazardous through further faults;

e) the following simplifications to D.2.1 are allowed for secondary independence:

   – insulation distances (creepage distances and clearances) should be dimensioned at least according to the requirements for basic insulation of EN 50124-1;

   – protecting devices do not require inherent properties. (Only a second fault may be able to inhibit the independence between a main item and an additional item);

   – at least the power-supply network for the voltage-monitoring (additional item) should be separated from the power-supply network for the monitored main item as written in this item e).

D.3 Achievement of physical external independence
(Protection against influences of type C, as referred to in B.3.2)

The following measures provide physical external independence:

a) measures should be taken to avoid non-intentional effects by EMI/ESD disturbing correct operation, in accordance with IEC 62236-4;

b) the specified climatic conditions should normally be complied with. Measures should be taken to minimise the risk of the system being operated outside its specified climatic conditions;

c) measures should be taken to avoid non-intentional effects by mechanical stresses disturbing the correct operation:

   1) measures to ensure reliable correct operation in spite of mechanical stress-conditions agreed between the railway authority and supplier;

   2) protection should be compliant with EN 50125-1 and/or EN 50125-3 as appropriate;

d) measures should be taken to ensure reliable correct operation in spite of chemical stress-conditions agreed between the railway authority and supplier;

e) measures should be taken to avoid non-intentional operation under non-permitted power-supply voltages (protection of supply-voltages):

   1) non-permitted supply voltages (outside data-sheet values for supplied systems/ equipments/components) should be disclosed by voltage-monitoring, triggering a safe state before hazardous situations are possible;

   2) voltage-monitoring should operate correctly for the whole life-cycle. Voltage-monitoring redundancy may be necessary if disclosure of voltage-monitoring faults is not possible.

f) measures should be taken to avoid non-intentional hazardous effects caused by external voltages across input and output ports disturbing the correct operation (protection of external interfaces):

   1) worst-case external voltages should be assumed (process-voltages and all possible EMI-induced voltages on cables and lines);

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

2) clearances between live parts and exposed conductive parts/earth/circuits whose correct operation needs to be protected should be dimensioned according to surge voltages specified in EN 50124-1;

3) creepage distances between live parts and exposed conductive parts/earth/circuits whose correct operation needs to be protected should be dimensioned according to EN 50124-1 and according to maximum rated r.m.s. voltages during operation;

4) for dimensioning insulation, the larger distance (clearance or creepage distance) is decisive.

D.4 Example of a method for single-fault analysis
(As referred to in B.3.3)

NOTE 1 The information for the following items a) to f) is derived from CENELEC paper CLC/SC9XA(SEC)114 "Calculation with Mü 8004 formulas".

a) Depending on the sum "*a*" of the failure rates of the items whose simultaneous malfunctioning could be hazardous, the detection-plus-negation time t_{sf} of single faults in the respective items should not exceed the value:

$$t_{sf} \leq \frac{k}{1\,000 \times a}$$

where

k = 1 for a 2 out of 2 system;

k = 0,5 for a 2 out of 3 system.

b) The failure rates mentioned in item a) above are to be determined as a function of the stress profile dependent on the environmental conditions during operation. The stress profile depends on the application. A simplified stress profile may be taken as a basis if this has an unfavourable effect on the failure rate.

c) If within a system, sub-system or equipment comprising several items, not all combinations of two failed items would be hazardous, the fault detection time may be determined separately for the various combinations. If, in this case, different fault detection times result for one item, the shortest time is decisive.

d) Periodic tests for faults in all items should be implemented. The tests should be representative for all credible faults affecting the correct operation, and should be finished within a time < t_{sf}.

Detection of faults in large-scale integrated circuits should be compliant with Table D.1.

e) If a fault-free 2-out-of-*n* system (n = 2 or 3) is disconnected from the power supply, the fault detection may be interrupted. The duration of such a service interruption should not exceed the 400-fold value of the fault detection time which is permissible according to item a) above.

NOTE 2 This is based on the assumption that the reliability of electronic components is 20 times better when the equipment is not powered.

f) In the case of the fault detection being interrupted for a longer time than permissible according to item e) above, the system/sub-system/equipment may only be put into operation again after having been checked for multiple faults.

NOTE 3 The information for the following items g) to j) is derived from Italian railway technical standard for safety electronic systems (IS 353). This IS 353 complies with ORE A155.3 recommendation.

g) When the safety-related function is performed by a single item, the disclosure time of a wrong side failure t_{sf} is the maximum total time to detect and react in a safe way to a single fault. The disclosure time shall not exceed the specified limit for the duration of any hazardous condition. In order to avoid any hazardous condition this duration must be less than the required response time of the equipment to be controlled (by means of the single item system).

h) The response time depends on the kind of the equipment to be controlled and it is therefore application dependent.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

For example the t_{sf} could assume the following values:

t_{sf} < 100 ms, if the equipment to be controlled is a signalling relay.

i) During the time t_{sf}, the first safety related failure must be detected and it must trigger a safety reaction.

j) Periodic tests for faults should be implemented in the single item case. The tests should be representative for all faults affecting the correct operation, and should finish within a time < t_{sf}.

D.5 Example of a method for multiple-fault analysis
(As referred to in B.3.5)

NOTE The information for the following items a) and b) is derived from CENELEC paper CLC/SC9XA(sec)114 "Calculation with Mü 8004 formulas".

a) Double fault which could be hazardous if combined with a third fault.

   1) If the timely detection-plus-negation of a fault in one item is impossible or unsuitable, the chance occurrence of a further fault in a second item should be taken into account.

   2) It is necessary that simultaneous faults in two items are non-hazardous. This means that at least three independent items are necessary. They are connected such that only the malfunction of three items could be hazardous, as in a 3 out of 3-system.

   3) Depending on the sum "*a*" of the failure rates of at least three items, whose simultaneous malfunction could be hazardous, the detection-plus-negation time t_{df} for double faults should not exceed the value:

$$t_{df} \leq \frac{2}{a}$$

   4) The failure rates mentioned in c) should be determined as a function of the stress profile dependent on the environmental conditions during operation. The stress profile depends on the application. A simplified stress profile may be taken as a basis if this has an unfavourable effect on the failure rate.

   5) If, within a system, sub-system or equipment comprising several items, not all combinations of three failed items would be hazardous, the fault detection time may be determined separately for the various combinations. If, in this case, different fault detection times result for two items, the shortest time is decisive.

b) Triple fault which could be hazardous if combined with a fourth fault.

   1) If the timely detection-plus-negation of a double fault in two items is impossible or unsuitable, the chance occurrence of a further fault in a third item should be taken into account.

   2) It is necessary that simultaneous faults in three items be non-hazardous. This means that at least four independent items are necessary. They are connected such that only the malfunction of four items could be hazardous, as in a 4 out of 4-system.

   3) Measures for detection of triple faults, over and above the operational data flow and the tests during maintenance, are not required if the failure rate "*a*" does not exceed the value:

$$a \leq 2 \times 10^{-4}\ h^{-1}$$

   4) The failure rate "*a*" is the sum of the failure rates of those items whose simultaneous malfunction could be hazardous (quadruple fault).

c) Coherently with item 3) of Clause D.4, it shall not be possible for further failures to cancel out a safe reaction. This could be allowable only in a controlled manner as part of corrective maintenance actions which must be executed when the faulty section of the item is off-line.

An example of a fault analysis method can be found in Figure D.1.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

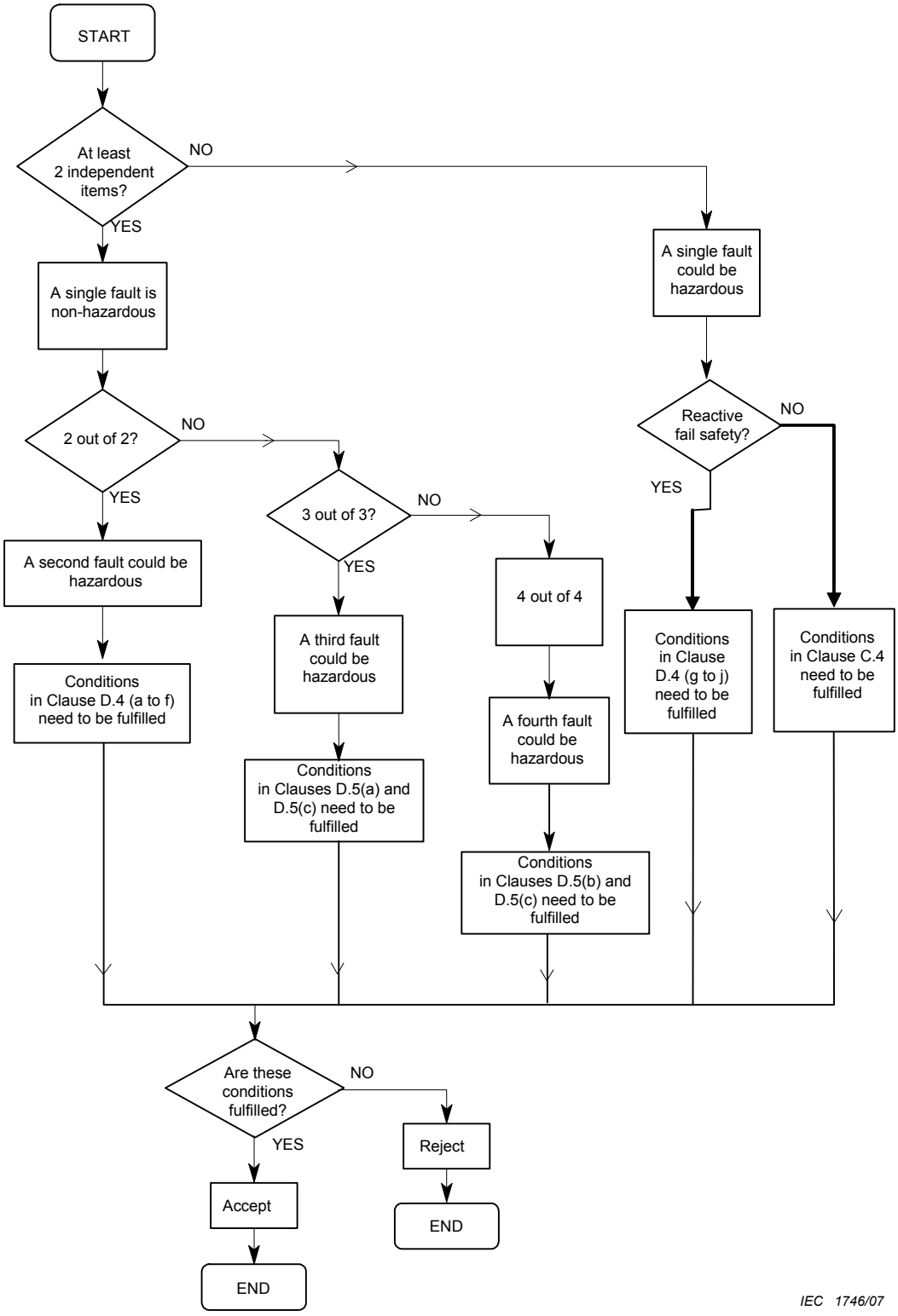


Figure D.1 – Example of a fault analysis method

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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-*n* system [1)]

Component	Malfunction	Measures
1 CPU 1.1 Register	Any, for example dependency on combinations of data bits (pattern -sensitive fault).	Using all registers (except initialisation registers) in all possible patterns (combinations of data bits). After initialising an initialisation register (e.g. interrupt control register), the correct initialised function needs to be tested. Registers greater than 8 bits may be tested by using all following combinations of data bits: ..5555....H OAAAA....H ..3333....H 9999....H 0CCCC....H 6666....H 0000....H 0FFFF....H 0F0F0....H ..0F0F....H in each on-line test period. Additional on-line tests with all combinations of data bits are necessary, distributed over several test periods (using, for example, a random number generator).
1.2 Instruction decoding and execution	Any, for example wrong decoding or wrong execution affecting registers or memories, dependent on combinations of data bits at source and/or destination.	Using one instruction of each type, testing with combinations of data bits mentioned in 1.1. Test of whether all usable system-related instructions are executable, for all conditions, sources, destinations and values of address bits (loading program counter included). Test of whether all usable system-related interrupt instructions are executable, dependent on interrupts or interrupt conditions. To test all usable system-related instructions, it is permissible to generate them in RAM and to jump to them for execution. After execution-related changing of the contents of at least one register, it is recommended to check not only the contents of concerned registers but also the contents of all other registers.
1.3 Clock	Wrong frequency	If independent clock generators are used for each computing channel, then wrong frequency in one channel can be detected by comparison. In cases of multiple faults, additional frequency monitoring may be necessary.

1) Application-independent detection of a first fault before a second fault is to be assumed.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table D.1 *(continued)*

Component	Malfunction	Measures
1.4 Reset	Additional or no reset(s)	If independent reset-generators are used for each computing channel, then a wrong reset in one channel can be detected by comparison. In cases of multiple faults, additional correct-start monitoring may be necessary.
1.5 Power supply	Wrong supply voltage	If independent power supplies are used for each computing channel, then a wrong supply voltage in one channel can be detected by comparison. In cases of no independence, or multiple faults, additional voltage monitoring may be necessary.
2 Memory 2.1 ROM	Any wrong content(s) and any wrong decoding of address(es) or control signals(s).	Reading and comparing all contents.
2.2 RAM	Any wrong content(s) after reading or writing, and any wrong decoding of address(es) or control signal(s).	Reading and comparing all contents. Writing/reading/comparing test with all combinations of data bits mentioned in 1.1. Test whether all cells are addressable (e.g. by loading a particular combination of data bits into one cell and reading/comparing all other cells of the concerned chip). The same once more by loading the inverted particular combination of data bits into the same cell. All this to be repeated for the next cell in the same manner, and so on until all cells in all RAM chips are used.
		The last described test also detects influences from each bit to each other bit in the same RAM circuit. This test may be distributed over several on- line test periods.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

E.1 Techniques and measures for safety-related electronic systems for signalling for the avoidance of systematic faults and the control of random and systematic faults

Safety integrity levels (SIL) are defined at functional level for the sub-systems implementing the functionality. This annex relates architectures, techniques and measures to avoid systematic faults and control random and systematic faults to the different safety integrity levels 1-4.

Therefore, the following tables describe the various techniques/measures against the four SILs.

It is not possible to list all individual causes of systematic faults during the life-cycle phases, because systematic faults have different effects in the different life-cycle phases and measures are dependent on the application. A quantitative analysis for the avoidance of faults is therefore not possible.

According to the system life-cycle and the safety management process described in IEC 62278 and referred to in 5.3, a number of activities shall be performed at each life-cycle phase. As described in the safety management process, the purpose of the process is to reduce further the incidence of safety related human errors throughout the life-cycle and thus minimise the residual risk of safety related systematic faults. This includes verification and quality assurance processes. The requirements for this process are listed in

Table E.1 – Safety planning and quality assurance activities (referred to in 5.2 and 5.3.4).

Following the phases 1 to 4 described in IEC 62278

Phase 1: Concept

Phase 2: System definition and application conditions

Phase 3: Risk analysis

Phase 4: System requirements

the results shall be documented in the system requirements specification, which shall take account of the techniques/measures in

Table E.2 – System requirements specification (referred to in 5.3.6).

During the preparation of a safety plan, the safety management structure shall be identified. Supporting information is given in

Table E.3 – Safety organisation (referred to in 5.3.3).

During the life-cycle phase design and implementation (phase 6), the system architecture description shall be documented with consideration to

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.4 – Architecture of system/sub-system/equipment (referred to in 5.4).

For the avoidance and control of faults caused by

– any residual design faults,
– environmental conditions,
– misuse or operating mistakes,
– any residual faults in the software,
– human factors,

techniques/measures for design features are given in

Table E.5 – Design features (referred to in 5.4).

According to the design features, the analysis of effects of faults has to identify RAM and safety constraints on hardware and software using RAMS analysis and the failure modes in Annex C.

Methods to identify and evaluate the effects of faults are given in

Table E.6 – Failure and hazard analysis methods (referred to in 5.4).

Whatever the design method is, it shall have the following features:

– clear and precise documentation;
– clear and precise expression of functionality;
– transparency, modularity and traceability;
– technological and time-related information;
– testability during verification and validation.

Techniques/measures are given in

Table E.7 – Design and development of system/sub-system/equipment (referred to in 5.3.7).

The intended design shall be documented with reference to

Table E.8 – Design phase documentation (referred to in 5.2).

and validated against the techniques/measures in

Table E.9 – Verification and validation of the system and product design (referred to in 5.3.9).

Using the hazard log, a validation test report shall be established including

– the version of the test specification used,
– the version of element (HW and SW) used,
– the tools and equipment used,
– the result of each test,
– any discrepancy between expected and actual results,
– the analysis made and the decision taken in the case of discrepancy.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

The results of the design/development phase and of the safety case will lead to application, operation and maintenance procedures which shall be documented taking into account the techniques/measures in

Table E.10 – Application, operation and maintenance (referred to in 5.3.12 and 5.4).

With each technique or measure in these tables, there is a recommendation for each safety integrity level (SIL) 1 to 4.

"HR" This symbol means that the measure or technique is highly recommended for this safety integrity level. If this technique or measure is not used, the rationale behind not using it shall be detailed.

"R" This symbol means that the measure or technique is recommended for this safety integrity level.

"-" This symbol means that the technique or measure has no recommendation for or against being used.

Table E.1 – Safety planning and quality assurance activities (referred to in 5.2 and 5.3.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Checklists	R: checklist of activities and items to be produced		R: checklist of activities and items to be produced	
2 Audit of tasks	R		HR	
3 Inspection of issues of documentation	HR: documents agreed between railway/safety authority and industry		HR: all documents	
4 Review after change in the safety plan	HR			
5 Review of the safety plan after each safety life-cycle phase	HR			

Table E.2 – System requirements specification (referred to in 5.3.6)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Separation of safety-related systems from non safety-related systems	R: well defined interfaces between safety-related systems and non safety-related systems (SRS)		HR: well defined interfaces between safety-related systems and non safety-related systems (SRS) and interface analysis	
2 Graphical description including for example block diagrams	HR		HR	
3 Structured specification	HR: manual hierarchical separation into subtasks, description of the interfaces		HR: hierarchical separation using formalised methods, automatic consistency checks, refinement down to functional level	
4 Formal or semiformal methods	-		R: computer-aided	
5 Computer aided specification tools	-	R: tools without preference for one particular design method	R: model oriented procedures with hierarchical subdivision, description of all objects and their relationship, common data base, automatic consistency check	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.2 *(continued)*

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
6 Checklists	R: prepared checklists for all safety life-cycle phases, concentration on the main safety issues		R: prepared detailed checklists for all safety life-cycle phases	
7 Hazard log	HR: Hazard log to be established and maintained throughout the system life-cycle			
8 Inspection of the specification	R		HR	
NOTE Checklists or computer aided specification tools should be used with another method since they usually state what to do (in order not to forget something), but cannot guarantee the quality of what is actually achieved.				

Table E.3 – Safety organisation
(referred to in 5.3.3)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Training of staff in safety organisation	HR: initial training in all relevant safety activities		HR: repetitive training or regular executing in all relevant safety activities	
2 Independence of roles	See Figure 6: Arrangements for independence			
Qualification of staff in safety organisation (see note)	HR: technical education or sufficient experience		HR: higher technical education or extensive experience	
NOTE Staff involved in safety activities should be competent to perform those activities (see 5.3.3).				

Table E.4 – Architecture of system/sub-system/equipment
(referred to in 5.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Separation of safety-related systems from non safety-related systems	R	R	HR	HR
2 Single electronic structure with self tests and supervision	R	R	-	-
3 Dual electronic structure	R	R	-	-
4 Dual electronic structure based on composite fail-safety with fail-safe comparison	R	R	HR	HR
5 Single electronic structure based on inherent fail-safety	R	R	HR	HR
6 Single electronic structure based on reactive fail-safety	R	R	HR	HR
7 Diverse electronic structure with fail-safe comparison	R	R	HR	HR
8 Justification of the architecture by a quantitative reliability analysis of the hardware	HR	HR	HR	HR
NOTE All techniques of the grey shaded group are alternatives, i.e. R means that at least one of these techniques is recommended.				

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.5 – Design features
(referred to in 5.4)

Techniques/Measures		SIL 1	SIL 2	SIL 3	SIL 4
1	Protection against operating errors	R: plausibility checks on each input command		HR: plausibility checks on each input command	
2	Protection against sabotage	-		R: additional organisational measures are necessary	
3	Protection against single fault for discrete components (B.3.1)	R: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties (See Annex C). EN 50124-1 requirements for basic insulation		HR: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties (see Annex C). EN 50124-1 requirements for reinforced insulation	
4	Protection against single fault for integrated circuits for digital electronic technology (B.3.1, Clause C.3)	R: stuck-at fault model	R: DC-fault model	HR: permanent and transient malfunction model on item level (examples for malfunctions of integrated circuits are defined in Table D.1)	
5	Physical independence within the safety-related architecture (B.3.2 type A and C)	R: insulation distances should be dimensioned at least according to EN 50124-1 (basic insulation)		HR: insulation distances should be dimensioned to the reinforced value according to EN 50124-1 (reinforced insulation)	
6	Detection of single faults (B.3.3)	R: revealed by deviation from normal operation	R: dependent on the safety target the time for detection -plus-negation of a single fault should be within the safety target	HR: dependent on the safety target the time for detection-plus-negation of a single fault should be within the safety target	
7	Retention of safe state (B.3.4)	R: indication to the operator the safety-related functions associated with this faulty item should not be used or relied upon		HR: automatically shut down the faulty item, sub-system or system from the process or blocking all safety-related functions of this faulty item, sub-system or system	
8	Multiple faults (B.3.5)	R: revealed by deviation from normal operation	R: dependent on the safety target the time for detection plus-negation of a multiple fault should be within the safety target	HR: dependent on the safety target, the time for detection-plus-negation of a multiple fault should be within the safety target	
9	Dynamic fault detection	R: on line dynamic testing should be performed to check the proper operation of the safety-related system and provide an indication to the operator	HR: on line dynamic testing should be performed to check the proper operation of the safety-related system and provide an indication to the operator	HR: on line dynamic testing should be performed to check the proper operation of the safety-related system and automatically shut down the faulty item, sub-system or system from the process or blocking all safety related functions of this faulty item, sub-system or system	
10	Program sequence monitoring	R: temporal or logical monitoring of the program sequence plus indication to the operator	HR: temporal or logical monitoring of the program sequence plus indication to the operator	HR: temporal and logical monitoring of the program sequence at many checking points in the program and automatically shut down the faulty item, sub-system or system from the process or blocking all safety related functions of this faulty item, sub-system or system	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.5 *(continued)*

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
11 Measures against voltage breakdown, voltage variations, overvoltage, low voltage	HR: measures against voltage breakdown, voltage variations, overvoltage, low voltage		HR: extended measures against voltage breakdown, voltage variations, overvoltage, low voltage	
12 Measures against temperature increase	HR: temperature sensor detecting over-temperature		HR: the necessity of a safety shut down it is to be investigated	
13 Software architecture	see IEC 62279		see IEC 62279	

Table E.6 – Failure and hazard analysis methods (referred to in 5.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Preliminary hazard analysis [a]	HR	HR	HR	HR
2 Fault tree analysis	R	R	HR	HR
3 Markov diagrams	R	R	HR	HR
4 FMECA	R	R	HR	HR
5 HAZOP	R	R	HR	HR
6 Cause-consequence diagrams	R	R	HR	HR
7 Event tree	R	R	R	R
8 Reliability block diagram	R	R	R	R
9 Zonal analysis	R	R	R	R
10 Interface hazard analysis	R	R	HR	HR
11 Common cause failure analysis	R	R	HR	HR
12 Historical event analysis	R	R	R	R

[a] PHA should only be considered at the early stages of the development. When precise technical information is available, during the design, the other methods should be preferred.

Table E.7 – Design and development of system/sub-system/equipment (referred to in 5.3.7)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Structured design	HR: design hierarchically broken down		HR: design hierarchically broken down and fully traceable back to requirements specification including references between specification, design, circuit diagrams and application documentation	
2 Modularisation	R: modules of limited size, each module isolated	HR: modules of limited size each module isolated	HR: use of fully validated, easily comprehensible modules of limited size, each module functionally isolated	
3 Formal or semiformal methods			R: computer-aided	
4 Computer aided design tools	-	R: computer support for complex designs	R: use of tools which are proven in use or validated, general computer-aided development	
5 Environmental studies (EMC, vibration etc.)	R	R	HR	HR

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.8 – Design phase documentation (referred to in 5.2)

	Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1	Graphical description of sub-systems	HR	HR	HR	HR
2	Description of interfaces	HR	HR	HR	HR
3	Environment (EMC, vibrations) studies	R	R	HR	HR
4	Modification procedure	HR	HR	HR	HR
5	Maintenance manual	HR	HR	HR	HR
6	Manufacturing documentation	HR	HR	HR	HR
7	Application documentation	HR	HR	HR	HR

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.9 – Verification and validation of the system and product design (referred to in 5.3.9)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Checklists	R: prepared checklists, concentration on the main safety issues		R: prepared detailed checklists	
2 Simulation		R	R	
3 Functional testing of the system	HR: functional tests, reviews should be carried out to demonstrate that the specified characteristics and safety requirements have been achieved		HR: comprehensive functional tests should be carried out on the basis of well defined test cases to demonstrate the specified characteristics and safety-requirements are fulfilled	
4 Functional testing under environmental conditions	HR: the testing of safety-related functions and other functions under the specified environmental conditions should be carried out		HR: the testing of safety-related functions and other functions under the specified environmental conditions should be carried out	
5 Surge immunity testing	HR: surge immunity should be tested to the boundary values of the real operational conditions	HR: surge immunity should be tested higher / higher limit than the boundary values of the real operation conditions		
6 Inspection of documentation	HR			
7 Ensure design assumptions are not compromised by manufacturing process	-		HR: specify manufacturing requirements and precautions, plus audit of actual manufacturing process by safety organisation	
8 Test facilities	R: designer of the test facilities should be independent from the designer of the system or product		HR: designer of the test facilities should be independent from the designer of the system or product	
9 Design review	HR: reviews should be carried out at appropriate stages in the life-cycle to confirm that the specified characteristics and safety requirements have been achieved		HR: reviews should be carried out at appropriate stages in the life-cycle to confirm that the specified characteristics and safety requirements have been achieved	
10 Ensure design assumptions are not compromised by installation and maintenance processes	HR: specify installation and maintenance requirements and precautions		HR: specify installation and maintenance requirements and precautions, plus audit of actual installation and maintenance processes by safety organisation	
11 High confidence demonstrated by use (optional where some previous evidence is not available)	R: 10 000 h operation time, at least 1 year experience with equipments in operation		R: 1 million hours operation time, at least 2 years experience with different equipments including safety analysis, detailed documentation also of minor changes during operation time	
NOTE Checklists, computer aided specification tools and inspection of the specification can be used in the verification activity of a phase.				

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Table E.10 – Application, operation and maintenance (referred to in 5.3.12 and 5.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Production of applications operational and maintenance instructions	R: all operational, application and maintenance instructions traceable back to the design including use of hazard log		HR: all operational, application and maintenance instructions traceable back to the design including use of hazard log	
2 Training in the execution of operational and maintenance instructions (see 5.4, Section 5)	HR: initial training of all operators and maintenance staff		HR: initial training plus periodic refresher training of all operators and maintenance staff	
3 Operator friendliness	HR: the interaction between the person and the system to be as simple as possible, in order to reduce the risk of human errors			
4 Maintenance friendliness	HR: separate diagnosis tools, safety-related maintenance measures as seldom as possible		HR: sufficient, sensible and simply handled diagnosis tools shall be included for unavoidable repairing measures, safety-related maintenance measures as seldom as possible or not necessary at all	
5 Protection against operating errors	R: procedural plausibility checks on each input command		HR: procedural plausibility checks on each input command	
6 Protection against sabotage	-		R: additional organisational measures are necessary	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Bibliography

NOTE The following documents were consulted during the preparation of this standard (in addition to the normative references listed in Clause 2).

HD 485 S1:1987, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) *(IEC 60812:1985)*

HD 617 S1:1992, Fault tree analysis (FTA) *(IEC 61025:1990)*

CLC/SC9XA(SEC)114, Calculation with Mü8004 formulas, August 1994

ISO 9001:1994, Quality Systems – Model for quality assurance in design, development, production, installation and servicing

TR 50451, Railway applications – Systematic allocation of safety integrity requirements (CENELEC)

UIC/ORE Report A155/RP6, Computer-based safety systems requirements specification, September 1985

UIC/ORE Report A155/RP7, The design of computer-based safety systems, April 1986

UK Health & Safety Executive, Programmable electronic systems in safety-related applications – Parts 1 and 2, 1987

UIC/ORE Report A155/RP11, Proof-of-Safety of computer-based safety systems, September 1987

UIC/ORE Report A155/RP12, Failure catalogue for electronic components, April 1988

MIL-HDBK-338-1A, Electronic reliability design handbook, October 1988

German Federal Railways Mü8004, Principles for the technical approval of signalling and communications technology, January 1991

Reliability Analysis Center Report FMD-91, Failure mode/mechanism distributions, September 1991

IRSE International Technical Committee Report No.1, Safety system validation with regard to cross-acceptance of signalling systems by the railways, January 1992

IS 353: Ferrovie dello stato servizio impianti elettrici: Norme Tecniche IS. 353 Ed. 1985: Norme Tecniche per la presentazione dei prototipi di apparecchiature elettroniche destinate agli impianti di sicurezza e segnalamento.

UIC/ORE A155.3: The use of Electronic Components for Signalling

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

SOMMAIRE

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATIONS ET DE TRAITEMENT – SYSTÈMES ÉLECTRONIQUES DE SÉCURITÉ POUR LA SIGNALISATION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62425 a été établie par le comité d'études 9 de la CEI: Matériels et systèmes électriques ferroviaires.

Elle a été soumise aux Comités Nationaux pour vote suivant la procédure par voie express, par les documents suivants:

FDIS	Rapport de vote
9/1057/FDIS	9/1087/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Ce document est basé sur la norme européenne EN 50129.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

INTRODUCTION

Le présent document est la première Norme internationale qui définit les exigences pour l'acceptation et l'approbation des systèmes électroniques relatifs à la sécurité dans le domaine de la signalisation ferroviaire. La présente norme est issue de la Norme européenne EN 50129.

Les systèmes électroniques relatifs à la sécurité pour la signalisation incluent les aspects matériels et logiciels. Pour installer des systèmes complets relatifs à la sécurité, ces deux parties sont à prendre en compte lors du cycle de vie entier du système. Les exigences concernant le matériel relatif à la sécurité et le système global sont définies dans la présente norme. Les autres exigences sont définies dans les normes CEI associées.

Le présent document est le référentiel commun pour l'acceptation et l'approbation de la sécurité des systèmes électroniques pour des applications de signalisation ferroviaire. Le but des sociétés d'exploitation ferroviaire et de l'industrie ferroviaire est de développer des systèmes ferroviaires basés sur des normes communes. Les autorités de tutelle compétentes peuvent appliquer la présente norme aux domaines pertinents qu'elles choisissent. Sur cette base, l'acceptation réciproque des approbations de la sécurité pour des sous-systèmes et équipements peut être appliquée par les différentes autorités de tutelle nationales. L'acceptation réciproque est applicable à l'approbation générique et non à des applications spécifiques.

La présente norme comprend un corps principal (Article 1 à Article 5) et des Annexes A, B, C, D et E. Les exigences définies dans le corps principal de la présente norme et dans les Annexes A, B et C sont normatives, alors que les Annexes D et E sont informatives.

La présente norme est conforme à la CEI 62278: "Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)", et utilise les sections applicables de cette dernière. La présente norme et la CEI 62278 sont basées sur le cycle de vie système et sont conformes à la CEI 61508-1, laquelle est remplacée par l'ensemble des CEI 62278/ CEI 62279/ CEI 62425, pour autant que les systèmes ferroviaires de signalisation, de télécommunications et de traitement soient concernés. Le respect des exigences de ces normes suffit à assurer la conformité à la CEI 61508-1 sans qu'une évaluation complémentaire ne soit nécessaire.

Etant donné que la présente norme concerne les preuves à fournir pour l'acceptation de systèmes relatifs à la sécurité, elle spécifie les activités du cycle de vie qui doivent être terminées avant la phase d'acceptation, puis suivies d'activités planifiées supplémentaires à réaliser après la phase d'acceptation. La justification de la sécurité pour la totalité du cycle de vie est donc exigée.

La présente norme précise quelles sont les preuves qui doivent être établies. Sauf si cela est considéré comme opportun, elle ne spécifie pas par qui il est recommandé que le travail nécessaire soit réalisé, cela pouvant varier en fonction des diverses circonstances.

Pour les systèmes relatifs à la sécurité qui comprennent de l'électronique programmable, des conditions supplémentaires sont définies, pour le logiciel, dans la CEI 62279.

Des exigences supplémentaires pour la transmission de données de sécurité sont définies dans les CEI 62280-1 et CEI 62280-2.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATIONS ET DE TRAITEMENT – SYSTÈMES ÉLECTRONIQUES DE SÉCURITÉ POUR LA SIGNALISATION

1 Domaine d'application

La présente Norme internationale est applicable aux systèmes électroniques relatifs à la sécurité (en incluant les sous-systèmes et les équipements) pour des applications de signalisation ferroviaire.

Le domaine d'application de la présente norme et ses relations avec les autres normes CEI sont illustrés à la Figure 1.

La présente norme est applicable à tous les systèmes/sous-systèmes/équipements de signalisation ferroviaire relatifs à la sécurité. Cependant, les processus d'analyse des situations dangereuses et d'évaluation des risques définis dans la CEI 62278 et dans la présente norme sont nécessaires pour tous les systèmes/sous-systèmes/équipements de signalisation ferroviaire, de manière à identifier les exigences de sécurité pour chaque situation particulière. Si l'analyse montre qu'il n'existe aucune exigence de sécurité (c'est-à-dire que la situation n'est pas relative à la sécurité), et sous réserve que la conclusion n'est pas remise en cause suite à des évolutions ultérieures, la présente norme de sécurité cesse d'être applicable.

La présente norme est applicable aux phases de spécification, de conception, de réalisation, d'installation, d'acceptation, de fonctionnement, de maintenance et de modification/ d'extension de systèmes complets de signalisation, ainsi qu'à des sous-systèmes et à des équipements faisant partie d'un système complet. L'Annexe C inclut des procédures traitant des composants électroniques.

La présente norme est applicable aux sous systèmes et équipements génériques (qu'ils soient indépendants de l'application ou prévus pour une classe particulière d'application), et aussi aux systèmes/sous-systèmes/équipements pour des applications spécifiques.

La présente norme n'est pas applicable à des systèmes/sous-systèmes/équipements existants (c'est-à-dire à ceux qui ont déjà été acceptés avant l'élaboration de la présente norme). Toutefois, dans la mesure où cela est raisonnablement possible, il convient que la présente norme soit appliquée à des modifications et à des extensions de systèmes, de sous-systèmes et d'équipements existants.

La présente norme est d'abord applicable aux systèmes/sous-systèmes/équipements qui ont été spécialement conçus et réalisés pour des applications de signalisation ferroviaire. Il est aussi recommandé de l'appliquer, dans la limite du raisonnable, à des équipements généraux ou industriels (par exemple alimentations, modems, etc.) qui sont utilisés comme partie d'un système de signalisation ferroviaire relatif à la sécurité. Dans de tels cas, il doit être, au minimum, apporté des preuves démontrant:

– soit que la sécurité ne repose pas sur cet équipement,

– soit que les fonctions en relation avec la sécurité peuvent reposer sur cet équipement.

La présente norme est applicable à la sécurité fonctionnelle des systèmes de signalisation ferroviaire. Elle n'est pas destinée à traiter de la santé des travailleurs et de la sécurité du personnel; ce sujet est couvert par d'autres normes.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

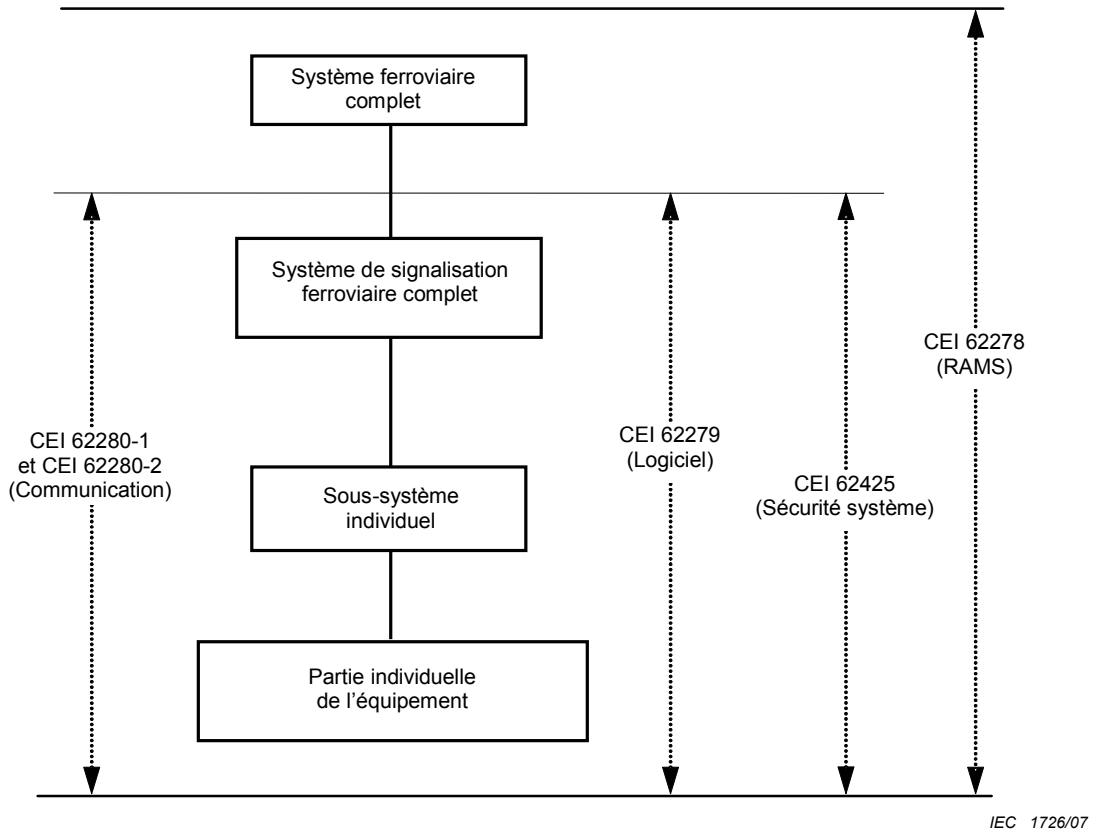


Figure 1 – Domaine d'application des principales normes ferroviaires CEI

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NOTE 1 Des références informatives additionnelles sont incluses dans la Bibliographie.

CEI 60664 (toutes les parties), *Coordination de l'isolement des matériels dans les systèmes (réseaux) à basse tension*

CEI 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 62236 (toutes les parties), *Applications ferroviaires – Compatibilité électromagnétique*

CEI 62236-4, *Applications ferroviaires – Compatibilité électromagnétique – Partie 4: Emission et immunité des appareils de signalisation et de télécommunication*

CEI 62278, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*

CEI 62279, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire*

CEI 62280-1, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

CEI 62280-2, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 2: Communication de sécurité sur des systèmes de transmission ouverts*

EN 50124-1, *Applications ferroviaires – Coordination de l'isolement – Partie 1: Prescriptions fondamentales – Distances d'isolement dans l'air et lignes de fuite pour tout matériel électrique et électronique*

EN 50125-1, *Applications ferroviaires – Conditions d'environnement pour le matériel – Partie 1: Equipement embarqué du matériel roulant*

EN 50125-3, *Applications ferroviaires – Conditions d'environnement pour le matériel – Partie 3: Equipement pour la signalisation et les télécommunications*

EN 50155, *Applications ferroviaires – Equipements électroniques utilisés sur le matériel roulant*

NOTE 2 La série EN 50124, la série EN 50125 et l'EN 50155 seront transformées en normes CEI, conformément à la stratégie de convergence entre le CE 9 de la CEI et le TC9X du CENELEC.

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations suivants s'appliquent.

3.1 Définitions

3.1.1
accident
événement ou série d'événements inattendus conduisant au décès, à des blessures, à la perte d'un système ou d'un service, ou à des dommages sur l'environnement

3.1.2
évaluation
processus d'analyse d'un produit visant à déterminer si l'autorité de conception et le chargé de validation ont réussi à aboutir à un produit qui satisfait aux exigences spécifiées et visant à formuler un jugement sur le fait que le produit répond à l'objectif attendu

3.1.3
autorisation
permission formelle d'utiliser un produit dans les limites de l'application spécifiée

3.1.4
disponibilité
aptitude d'un produit à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée

3.1.5
analyse des causes
analyse des raisons à l'origine d'une situation dangereuse

3.1.6
défaillance de mode commun
défaillance commune à des éléments qui sont prévus pour être indépendants

3.1.7
analyse des conséquences
analyse des événements susceptibles de survenir après l'occurrence d'une situation dangereuse

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.1.8
configuration
structuration et relations entre le matériel et le logiciel d'un système pour une application attendue

3.1.9
acceptation réciproque
état atteint par un produit qui a été accepté par une autorité selon les normes en vigueur et qui est acceptable par les autres autorités sans nécessité de nouvelle évaluation

3.1.10
conception
activité menée afin d'analyser et de transformer les exigences spécifiées en solutions de conceptions acceptables ayant le niveau d'intégrité de la sécurité requis

3.1.11
autorité de conception
organisme responsable de la formulation d'un choix de conception pour remplir les exigences spécifiées et de la supervision des développements ultérieurs et de la mise en marche d'un système dans l'environnement attendu

3.1.12
diversité
moyen permettant de satisfaire totalement ou partiellement aux exigences spécifiées, de plusieurs manières indépendantes et dissemblables

3.1.13
équipement
entité fonctionnelle physique

3.1.14
erreur
écart par rapport à la conception attendue pouvant conduire à un comportement ou à une défaillance inattendu(e) du système

3.1.15
de sécurité intrinsèque
concept inclus dans la conception d'un produit de sorte que, dans l'éventualité d'une défaillance, il rentre ou reste dans un état sûr

3.1.16
défaillance
écart d'un système par rapport aux performances spécifiées

NOTE Une défaillance est la conséquence d'une panne ou d'une erreur dans le système.

3.1.17
panne
état anormal pouvant conduire à une erreur dans un système

NOTE Une panne peut être aléatoire ou systématique.

3.1.18
temps de détection de panne
intervalle de temps qui commence à l'instant où une panne se produit et qui finit lorsque la panne est décelée

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.1.19
fonction
mode d'action ou d'activité par lequel le produit accomplit sa mission

3.1.20
situation dangereuse
état pouvant conduire à un accident

3.1.21
analyse des situations dangereuses
processus d'identification des situations dangereuses et d'analyse de leurs causes, ainsi que les écarts par rapport aux exigences pour limiter la probabilité d'occurrence et les conséquences des situations dangereuses à un niveau acceptable

3.1.22
registre des situations dangereuses
document dans lequel toutes les activités de gestion de la sécurité, les situations dangereuses identifiées, les décisions prises et les solutions adoptées sont enregistrées ou référencées

3.1.23
erreur humaine
action humaine (erreur), susceptible de conduire à un(e) comportement/défaillance inattendu(e) du système

3.1.24
réalisation
activité consistant à transformer les spécifications de conceptions en réalité physique

3.1.25
indépendance (fonctionnelle)
absence de tout mécanisme susceptible d'affecter le fonctionnement correct de plusieurs fonctions suite à une défaillance aléatoire ou à une erreur systématique

3.1.26
indépendance (des personnes)
non-appartenance à une même entité intellectuelle, commerciale et/ou de direction

3.1.27
indépendance (physique)
absence de tout mécanisme susceptible d'affecter le fonctionnement correct de plusieurs systèmes/sous-systèmes/équipements suite à des défaillances aléatoires

3.1.28
risque individuel
risque relatif à un seul individu

3.1.29
maintenabilité
pour une entité donnée, utilisée dans des conditions données d'utilisation, probabilité pour qu'une opération donnée de maintenance active puisse être effectuée pendant un intervalle de temps donné, lorsque la maintenance est assurée dans des conditions données et avec l'utilisation de procédures et de moyens prescrits

3.1.30
maintenance
combinaison de toutes les actions techniques et administratives, y compris les opérations de surveillance, destinées à maintenir ou à remettre une entité dans un état lui permettant d'accomplir sa fonction requise

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.1.31
passivation
forçage dans un état sûr suite à la détection d'une panne dangereuse

3.1.32
temps de passivation
intervalle de temps qui commence au moment où l'existence d'une panne est détectée et qui se termine lorsque l'état sûr a été atteint

3.1.33
produit
ensemble d'éléments, liés entre eux pour former un système/sous-système/équipement, de manière à remplir les exigences spécifiées

3.1.34
qualité
perception des attributs d'un produit par l'utilisateur

3.1.35
société d'exploitation ferroviaire
organisme répondant de l'exploitation d'un système ferroviaire sûr devant l'autorité de tutelle

3.1.36
intégrité de défaillances aléatoires
degré avec lequel un système est exempt de pannes aléatoires dangereuses

3.1.37
panne aléatoire
survenue imprévisible d'une panne

3.1.38
redondance
présence d'une ou de plusieurs mesures additionnelles, habituellement identiques, pour admettre une tolérance de pannes

3.1.39
fiabilité
capacité d'une entité à remplir une fonction requise, dans des conditions données pendant une durée donnée

3.1.40
réparation
actions destinées à rétablir, après une panne/une défaillance, un système, un sous-système ou un équipement dans l'état requis

3.1.41
risque
combinaison de la fréquence, ou de la probabilité, et des conséquences d'un événement dangereux spécifié

3.1.42
état sûr
état qui continue d'assurer la sécurité

3.1.43
sécurité
absence de niveaux de risque inacceptables

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.1.44
acceptation de la sécurité
état de sécurité donné à un produit par l'utilisateur final

3.1.45
approbation de la sécurité
état de sécurité donné à un produit par l'autorité saisie lorsque le produit a rempli un ensemble de conditions prédéterminées

3.1.46
autorité de tutelle
organisme chargé de délivrer l'autorisation de mise en service d'un système relatif à la sécurité

3.1.47
dossier de sécurité
démonstration documentée que le produit répond aux exigences de sécurité spécifiées

3.1.48
intégrité de la sécurité
aptitude d'un système relatif à la sécurité à remplir ses fonctions de sécurité requises dans toutes les conditions spécifiées, au sein d'un environnement opérationnel spécifié et pendant une durée donnée

3.1.49
niveau d'intégrité de la sécurité
nombre qui indique le degré de confiance requis pour qu'un système remplisse ses fonctions de sécurité spécifiées eu égard à ses défaillances systématiques

3.1.50
cycle de vie sécurité
ensemble supplémentaire d'activités menées en parallèle du cycle de vie système pour des systèmes relatifs à la sécurité

3.1.51
gestion de la sécurité
structure de gestion qui assure que le processus de sécurité est correctement mis en œuvre

3.1.52
plan d'assurance sécurité
détails de mise en œuvre indiquant la manière dont les exigences de sécurité du projet seront satisfaites

3.1.53
processus d'assurance sécurité
ensemble de procédures à suivre pour permettre l'identification et la satisfaction de toutes les exigences de sécurité d'un produit

3.1.54
relatif à la sécurité
qui est responsable de la sécurité

3.1.55
système de signalisation
type particulier de système utilisé dans le domaine ferroviaire pour commander, contrôler et protéger l'exploitation des trains

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.1.56
profil des contraintes
degré et nombre d'influences externes qu'un système est en mesure de supporter, alors qu'il remplit sa fonction requise

3.1.57
sous-système
partie d'un système qui remplit une fonction spéciale

3.1.58
système
ensemble de sous-systèmes ou d'éléments qui interagissent conformément à une conception

3.1.59
intégrité de défaillances systématiques
degré pour lequel un système est exempt de toute erreur dangereuse non identifiée et des causes d'erreur associées

3.1.60
panne systématique
panne inhérente à la spécification, la conception, la fabrication, l'installation, l'exploitation et la maintenance d'un système, sous-système ou équipement

3.1.61
cycle de vie système
ensemble d'activités intervenant durant la période qui commence lorsque le système est conçu et qui finit lorsqu'il est retiré du service

3.1.62
rapport de sécurité technique
preuves techniques documentaires de la sécurité de la conception d'un système, d'un sous-système ou d'un équipement

3.1.63
validation
activité qui vise à démontrer, par des essais et des analyses, que le produit remplit intégralement ses exigences spécifiées

3.1.64
vérification
activité qui vise à déterminer, par des analyses et des essais, à chaque phase du cycle de vie, que les exigences de cette phase à l'étude répondent aux sorties de la phase précédente et que le produit de la phase à l'étude répond à ses propres exigences

3.2 Abréviations

ATP	protection automatique du train (*automatic train protection*)
CENELEC	Comité européen de normalisation électrotechnique
CCF	défaillance de mode commun (*common-cause failure*)
CC	courant continu
CEM	compatibilité électromagnétique
EMI	interférence électromagnétique (*electromagnetic interference*)
EN	norme européenne
ESD	décharge électrostatique (*electrostatic discharge*)
AMDE	analyse des modes de défaillance et de leurs effets

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

FR	taux de défaillance (*failure rate*)
FTA	analyse par arbre des défauts (*fault tree analysis*)
H	situation dangereuse (*hazard*)
HW	matériel (*hardware*)
CEI	Commission électrotechnique internationale
IRSE	Institution des ingénieurs de la signalisation ferroviaire (*Institution of railway signal engineers*)
ISO	Organisation internationale de normalisation (*International standards organisation*)
RAMS	fiabilité, disponibilité, maintenabilité et sécurité (*reliability, availability, maintainability and safety*)
SDR	taux de passivation (*safe down rate*)
SDT	temps de mise en sécurité (*safe down time*)
SIL	niveau d'intégrité de la sécurité (*safety integrity level*)
SW	logiciel (*software*)
THR	taux maximal acceptable d'occurrence d'une situation dangereuse (*tolerable hazard rate*)
UIC	Union internationale des chemins de fer

4 Cadre général de la présente norme

L'Article 5 de la présente Norme internationale exige qu'une approche systématique et documentée soit réalisée en ce qui concerne:

– la preuve de la gestion de la qualité,
– la preuve de la gestion de la sécurité,
– la preuve de la sécurité fonctionnelle et technique,
– l'acceptation et l'approbation de la sécurité.

L'Annexe A (normative) définit l'interprétation et l'utilisation des niveaux d'intégrité de la sécurité.

L'Annexe B (normative) contient des exigences techniques supplémentaires pour les systèmes/sous-systèmes/équipements relatifs à la sécurité.

L'Annexe C (normative) contient des procédures et des informations afin d'identifier les modes de défaillances réalistes des composants matériels.

L'Annexe D (informative) contient des informations techniques supplémentaires.

L'Annexe E (informative) contient des tableaux de techniques/mesures à utiliser en fonction des différents niveaux d'intégrité de la sécurité.

La Bibliographie contient des références de documents qui ont été consultés lors de la préparation de la présente norme.

Le plan de la présente norme est résumé à la Figure 2.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

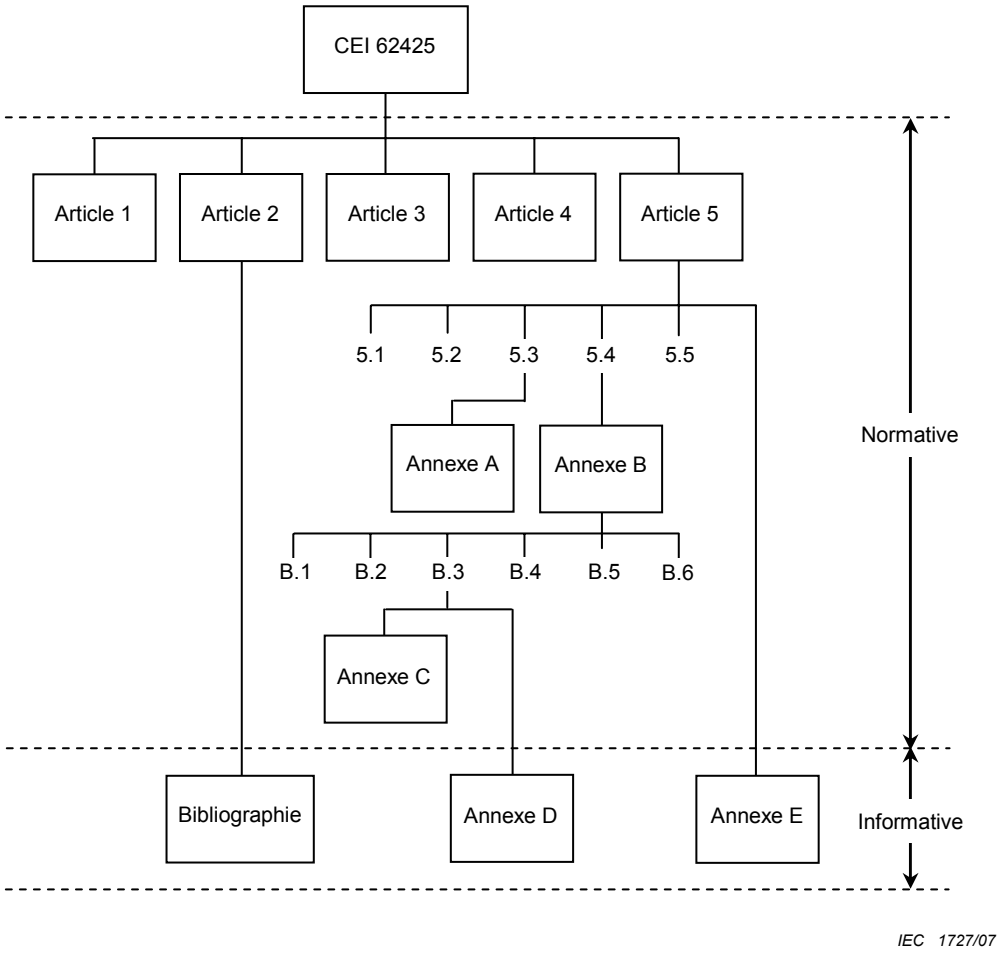


Figure 2 – Structure de la CEI 62425

5 Conditions pour l'acceptation et l'approbation de la sécurité

5.1 Le dossier de sécurité

La présente norme définit les conditions à remplir pour qu'un système/sous-système/ équipement électronique ferroviaire relatif à la sécurité puisse être accepté comme suffisamment sûr pour son utilisation attendue.

Les conditions d'acceptation de la sécurité sont présentées dans la présente norme dans trois paragraphes, intitulés

5.2 Preuve de la gestion de la qualité

5.3 Preuve de la gestion de la sécurité

5.4 Preuve de la sécurité fonctionnelle et technique

Toutes ces conditions doivent être remplies, aux niveaux équipement, sous-système et système, avant qu'un système relatif à la sécurité puisse être accepté comme suffisamment sûr.

La preuve documentaire que ces conditions ont été remplies doit faire partie d'un document structuré justificatif de la sécurité, appelé dossier de sécurité. Le dossier de sécurité fait partie de la preuve documentaire globale à soumettre à l'autorité de tutelle concernée, afin d'obtenir l'approbation de la sécurité pour un produit générique, une classe d'application ou une application spécifique. Pour une explication du processus d'approbation de la sécurité, se référer à 5.5.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Le dossier de sécurité contient la preuve documentée de la sécurité du système/sous-système/équipement et doit être structuré comme suit:

– Partie 1 Définition du système (ou du sous-système/équipement)

Cette partie doit définir précisément ou référencer le système/sous-système/équipement correspondant au dossier de sécurité, en incluant les numéros de version et l'état des modifications de toute la documentation sur les exigences, la conception et l'utilisation.

– Partie 2 Rapport de gestion de la qualité

Cette partie doit contenir la preuve de la gestion de la qualité, comme spécifié en 5.2.

– Partie 3 Rapport de gestion de la sécurité

Cette partie doit contenir la preuve de la gestion de la sécurité, comme spécifié en 5.3.

– Partie 4 Rapport de sécurité technique

Cette partie doit contenir la preuve de la sécurité fonctionnelle et technique, comme spécifié en 5.4.

– Partie 5 Dossiers de sécurité connexes

Cette partie doit contenir les références des dossiers de sécurité de tous les sous-systèmes ou équipements dont le dossier de sécurité principal dépend.

Elle doit aussi démontrer que toutes les conditions d'application relatives à la sécurité, spécifiées dans chaque dossier de sécurité connexe de sous-système/équipement, sont

- soit remplies dans le dossier de sécurité principal,
- soit reportées dans les conditions d'application relatives à la sécurité du dossier de sécurité principal.

– Partie 6 Conclusion

Cette partie doit résumer les preuves présentées dans les parties précédentes du dossier de sécurité, et justifier que le système/sous-système/équipement correspondant présente la sûreté requise, et est conforme aux conditions d'utilisation spécifiées.

Le plan du dossier de sécurité est illustré à la Figure 3.

Il n'est pas nécessaire d'inclure beaucoup de preuves et de documents détaillés dans le dossier de sécurité et ses différentes parties, pourvu que les références précises soient données à de tels documents et pourvu que les concepts de base et les démarches utilisés soient clairement spécifiés.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

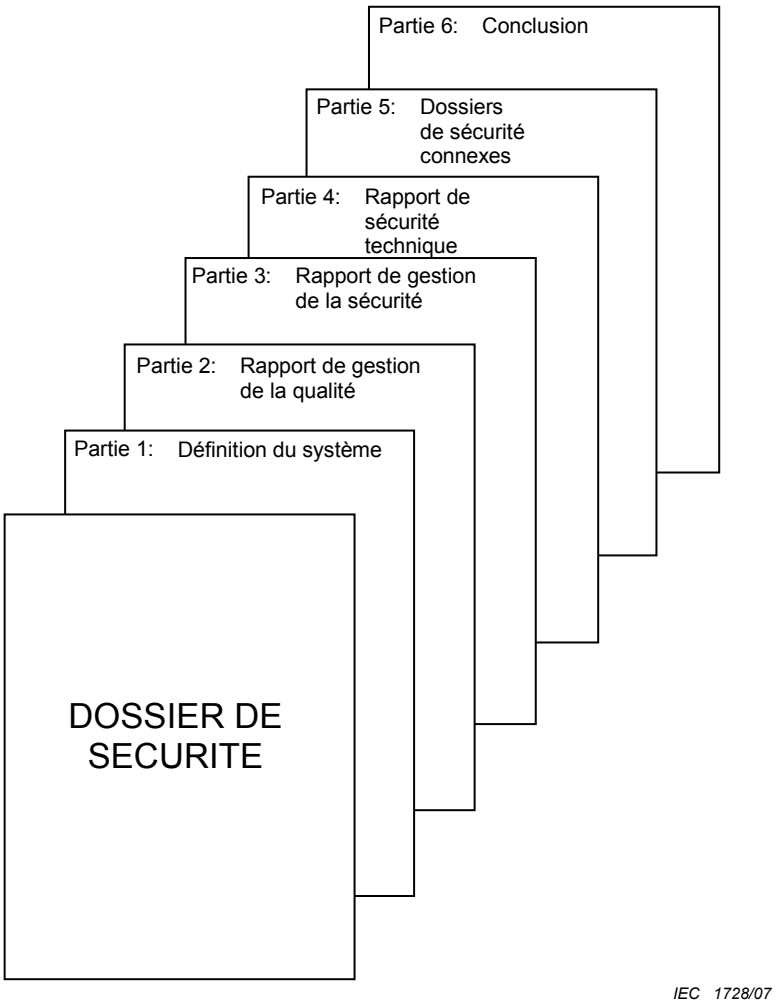


Figure 3 – Plan du dossier de sécurité

5.2 Preuve de la gestion de la qualité

La première condition pour l'acceptation de la sécurité devant être satisfaite est que la qualité du système, du sous-système ou de l'équipement a été contrôlée, et doit continuer à l'être, par un système de gestion de la qualité efficace tout au long du cycle de vie. La preuve documentaire pour le démontrer doit être fournie dans le rapport de gestion de la qualité, qui constitue la Partie 2 du dossier de sécurité.

Le but du système de gestion de la qualité est de minimiser l'incidence des erreurs humaines à chaque phase du cycle de vie et, ainsi, de réduire le risque de défauts systématiques dans le système, le sous-système ou l'équipement.

Le système de gestion de la qualité doit être applicable tout au long du cycle de vie du système/sous-système/équipement, comme défini dans la CEI 62278. Un exemple de diagramme de cycle de vie système (issu de la CEI 62278) est reproduit à la Figure 4.

NOTE Exemples de points qu'il est recommandé de contrôler par le système de gestion de la qualité et d'inclure dans le rapport de gestion de la qualité:

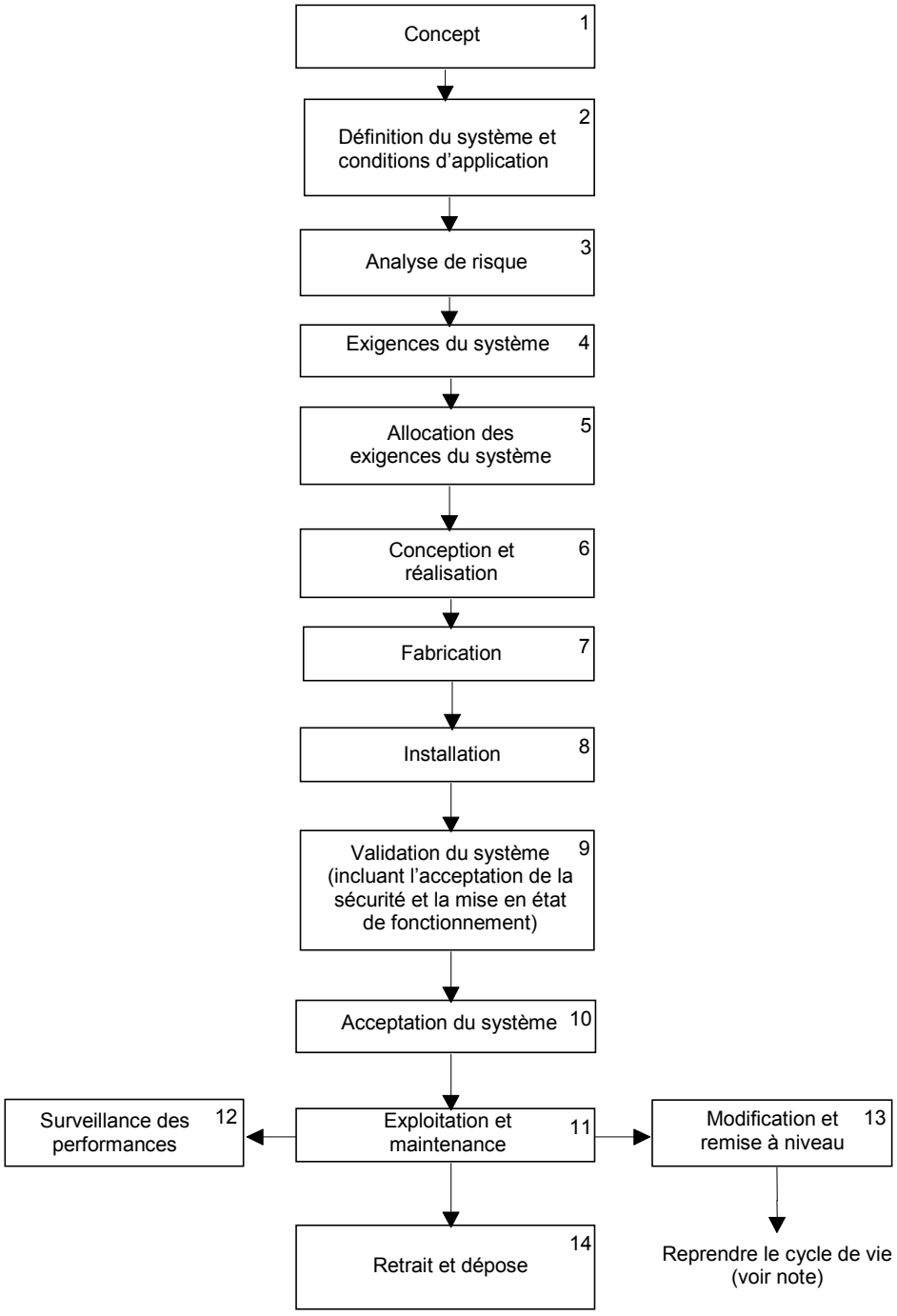
– structure de l'organisation;
– planning et procédures qualité;
– spécification des exigences;
– contrôle de la conception;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– vérification de la conception et revues;
– ingénierie applicative;
– approvisionnement et fabrication;
– identification du produit et traçabilité;
– manutention et stockage;
– inspection et essais;
– non-conformités et actions correctives;
– conditionnement et livraison;
– installation et mise en service;
– exploitation et maintenance;
– suivi de la qualité et retour d'expérience;
– documentation et enregistrements;
– gestion de la configuration/contrôle des évolutions;
– compétence du personnel et formation;
– audits qualité et leurs retombées;
– réforme et dépose.

La conformité aux exigences pour la gestion de la qualité est obligatoire pour les niveaux d'intégrité de la sécurité 1 à 4 inclus (voir l'Annexe A pour des explications sur les niveaux d'intégrité de la sécurité). Cependant, il est recommandé que le niveau de détail des preuves présentées et la couverture de la documentation de soutien soient appropriés au niveau d'intégrité de la sécurité du système/sous-système/équipement examiné (voir les Tableaux E.1 et E.8 pour une aide sur les preuves exigées pour chaque niveau d'intégrité de la sécurité). Les exigences pour le niveau d'intégrité de la sécurité 0 (non de sécurité) sont hors du cadre de la présente norme relative à la sécurité.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.



NOTE La phase au cours de laquelle une modification est introduite dans le cycle de vie dépend à la fois du système modifié et de la modification particulière considérée.

Figure 4 – Exemple de cycle de vie système (issu de la CEI 62278)

5.3 Preuve de la gestion de la sécurité

5.3.1 Introduction

La deuxième condition qui doit être remplie, pour l'acceptation de la sécurité, est que la sécurité du système, du sous-système ou de l'équipement a été, et doit continuer à être, gérée par l'intermédiaire d'un processus de gestion de la sécurité efficace, qu'il est recommandé de rendre homogène avec le processus de gestion de fiabilité, disponibilité, maintenabilité et

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

sécurité, défini dans la CEI 62278. L'objectif de ce processus est de réduire plus l'incidence des erreurs humaines ayant un impact sur la sécurité tout au long du cycle de vie et, ainsi, de minimiser le risque résiduel des défauts systématiques liés à la sécurité. Les éléments du processus de gestion de la sécurité sont brièvement résumés de 5.3.2 à 5.3.13 ci-dessous.

La preuve documentaire démontrant la conformité avec tous les éléments du processus de gestion de la sécurité tout au long du cycle de vie doit être fournie dans le rapport de la gestion de la sécurité, qui constitue la Partie 3 du dossier de sécurité. De grandes quantités de preuves détaillées et de documentations de soutien n'ont pas besoin d'y être incluses, sous réserve que des références précises soient données pour de tels documents.

L'utilisation de ce processus de gestion de la sécurité est obligatoire pour les niveaux 1 à 4 inclus d'intégrité de la sécurité (voir l'Annexe A pour une explication des niveaux d'intégrité de la sécurité). Cependant, il est recommandé que la précision des preuves et la couverture de la documentation de soutien soient appropriées au niveau d'intégrité de la sécurité du système/sous-système/équipement examiné. Les exigences pour le niveau d'intégrité de la sécurité 0 (non de sécurité) sont hors du cadre de la présente norme relative à la sécurité.

Dans tous les cas, les analyses des situations dangereuses et les processus d'évaluation des risques définis dans la CEI 62278 sont nécessaires, de manière à identifier le niveau requis d'intégrité de la sécurité pour chaque situation particulière. Cela comprend les cas où les analyses et l'évaluation mettent en évidence qu'il est possible d'assigner le niveau 0 d'intégrité de la sécurité; cependant, une fois que l'on a abouti à cette conclusion (c'est-à-dire que la situation n'est pas en rapport avec la sécurité), et sous réserve qu'elle reste au niveau 0, la présente norme relative à la sécurité cesse d'être applicable.

5.3.2 Cycle de vie sécurité

Le processus de gestion de la sécurité doit comprendre un nombre de phases et d'activités reliées entre elles afin de former le cycle de vie sécurité; il est recommandé que ce processus soit en conformité avec le cycle de vie du système défini dans la CEI 62278, qui est repris à la Figure 4. Les phases de conception et de validation du cycle de vie système peuvent être vues comme une phase "descendante" suivie d'une phase "remontante" (c'est-à-dire cycle en "V"); un exemple d'un tel cycle est montré à la Figure 5.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

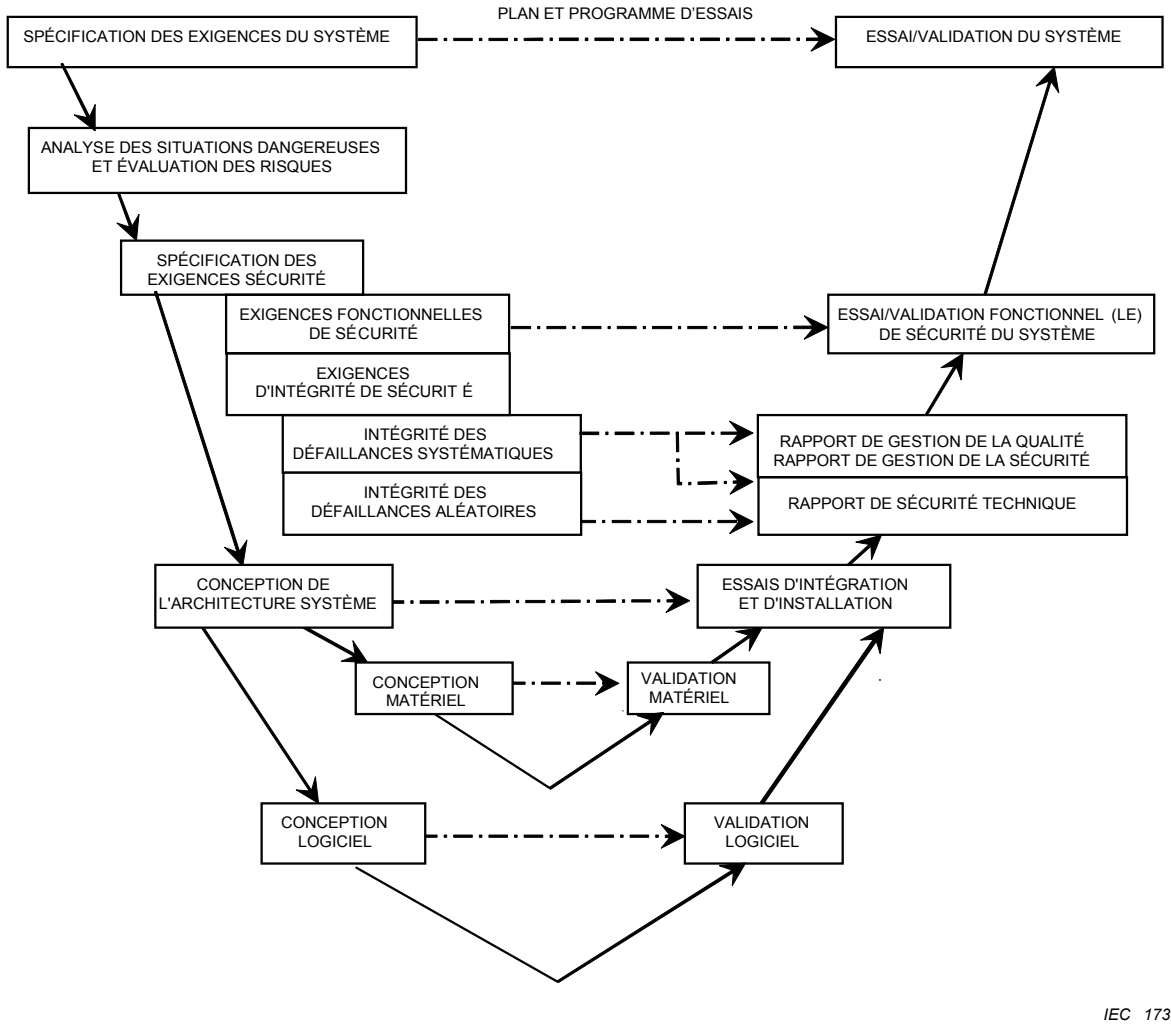


Figure 5 – Exemple de la partie conception et validation du cycle de vie système

5.3.3 Organisation sécurité

Le processus de gestion de la sécurité doit être mis en œuvre sous le contrôle d'une organisation sécurité appropriée, en utilisant du personnel compétent à qui l'on affecte des rôles spécifiques. L'évaluation et la documentation relatives à la compétence du personnel, y compris les connaissances techniques, les qualifications, l'expérience en rapport et les formations appropriées doivent être menées à bien en respectant les normes reconnues. Un degré d'indépendance approprié doit exister entre les différents rôles, comme illustré à la Figure 6. Voir aussi le Tableau E.3 pour des indications relatives à l'organisation sécurité requise pour chaque niveau d'intégrité de la sécurité.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

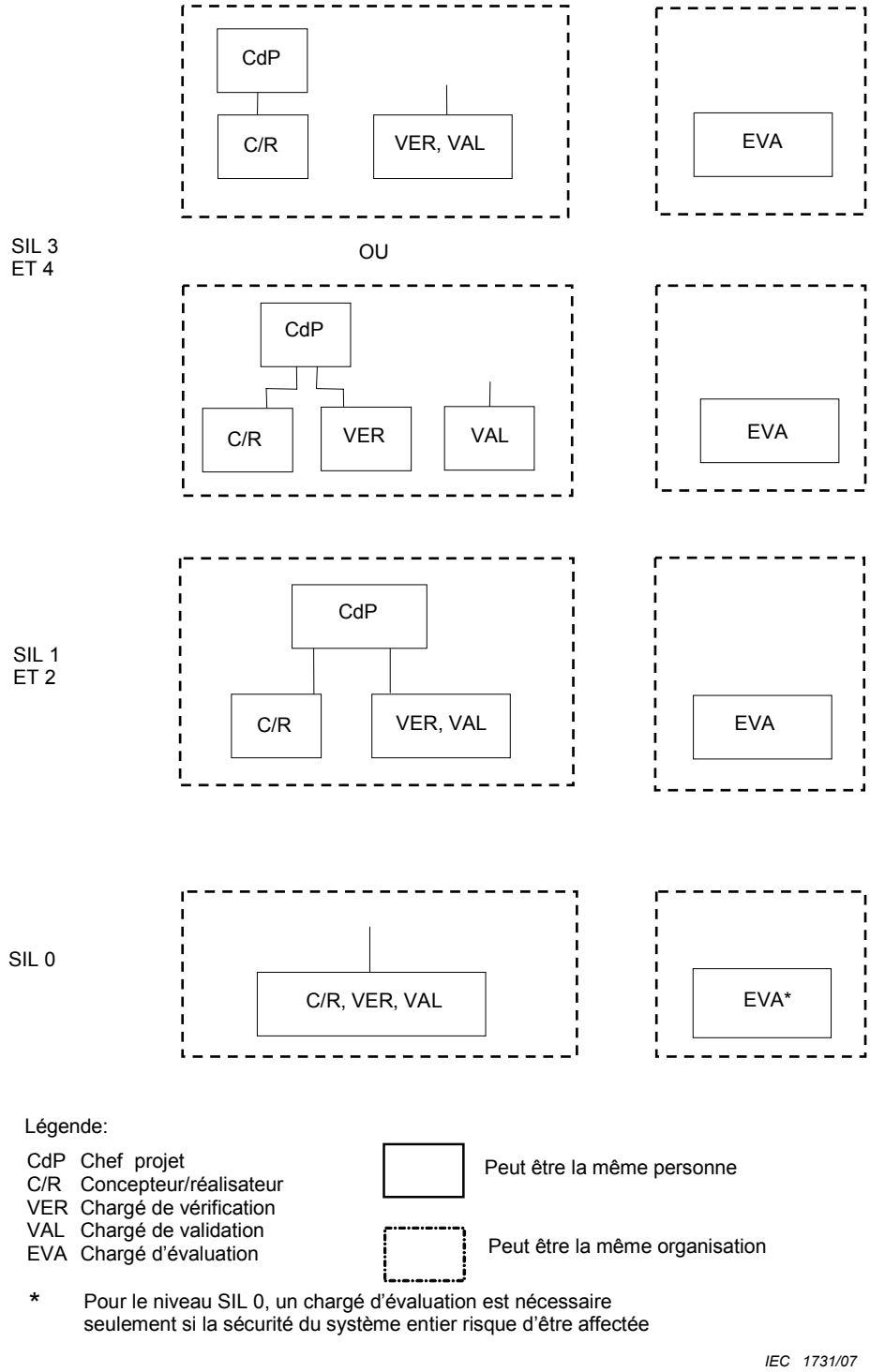


Figure 6 – Arrangements pour l'indépendance

5.3.4 Plan d'assurance sécurité

Un plan d'assurance sécurité doit être établi au début du cycle de vie. Ce plan doit identifier la structure pour la gestion de la sécurité, les activités relatives à la sécurité et des points d'approbation tout au long du cycle de vie. Il doit aussi contenir les exigences de revue du plan d'assurance sécurité avec une périodicité appropriée. Le plan d'assurance sécurité doit être mis à jour et revu si des modifications ou des ajouts ultérieurs sont faits sur le système/sous-système/équipement d'origine. Si de tels changements venaient à être effectués, les effets sur la sécurité doivent être évalués, en redémarrant depuis le point approprié du cycle de vie. Voir

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

le Tableau E.1, pour des indications relatives aux plans d'assurance sécurité pour chaque niveau d'intégrité de la sécurité.

Le plan d'assurance sécurité doit traiter de tous les aspects du système/sous-système/équipement, qu'ils soient matériels ou logiciels. Il doit être fait référence à la CEI 62279 pour ce qui concerne les logiciels.

Il est recommandé que le plan d'assurance sécurité comprenne un plan de dossier de sécurité, qui identifie la structure prévue et les composantes principales du dossier de sécurité final.

5.3.5 Registre des situations dangereuses

Un registre des situations dangereuses doit être établi et maintenu tout au long du cycle de vie sécurité, comme expliqué dans la CEI 62278. Il doit contenir une liste des situations dangereuses identifiées, avec la classification des risques associée et les informations de contrôle des risques pour chaque situation dangereuse. Le registre des situations dangereuses doit être mis à jour dès qu'une évolution ou modification est réalisée sur le système, sous-système ou équipement.

5.3.6 Spécification des exigences de sécurité

Les exigences de sécurité spécifiques à chaque système/sous-système/équipement, y compris les fonctions de sécurité et l'intégrité de la sécurité correspondante, doivent être identifiées et documentées dans la spécification des exigences de sécurité. Cela doit être réalisé à l'aide:

– de l'identification et l'analyse des situations dangereuses,

– de l'évaluation et la classification des risques,

– de l'allocation des niveaux d'intégrité de la sécurité,

comme cela est expliqué dans la CEI 62278. Des informations concernant les niveaux d'intégrité de la sécurité pour les systèmes électroniques ferroviaires sont contenues dans l'Annexe A.

NOTE Il est possible d'inclure la spécification des exigences de sécurité dans la spécification des exigences fonctionnelles du système/sous-système/équipement ou de l'écrire dans un document distinct. Voir le Tableau E.2 pour des indications relatives aux spécifications des exigences du système pour chaque niveau d'intégrité de la sécurité.

5.3.7 Conception du système/sous-système/équipement

Cette phase du cycle de vie doit aboutir à une conception qui réponde aux exigences opérationnelles et aux exigences de sécurité spécifiées. Une méthodologie structurée de conception descendante doit être utilisée avec une documentation rigoureusement contrôlée et revue. En particulier, les relations entre le matériel et le logiciel, comme représentées par la spécification des exigences du logiciel et l'intégration logiciel/matériel, doivent être gérées de façon stricte, et la CEI 62279 doit être respectée intégralement. Le Tableau E.7 donne des indications relatives à la conception et au développement d'un système/sous-système/équipement pour chaque niveau d'intégrité de la sécurité.

5.3.8 Revues de sécurité

Des revues de sécurité doivent être réalisées à des étapes appropriées du cycle de vie. De telles revues doivent être spécifiées dans le plan d'assurance sécurité, et leurs résultats totalement documentés. Toute modification ou ajout au système, sous-système ou équipement doit aussi faire l'objet de revues.

5.3.9 Vérification et validation de la sécurité

Le plan d'assurance sécurité doit comprendre des activités permettant de vérifier que chaque phase du cycle de vie répond aux exigences de sécurité spécifiques identifiées dans la phase

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

précédente, et permettant de valider le système/sous-système/équipement complet par rapport à sa spécification des exigences de sécurité d'origine.

Ces activités doivent être réalisées et totalement documentées, y compris les essais et analyses de sécurité appropriés. Elles doivent être répétées si cela est nécessaire lors de toute modification ultérieure ou ajouts éventuels au système/sous-système/équipement.

Le degré d'indépendance nécessaire pour le chargé de vérification et le chargé de validation doit être en conformité avec le niveau d'intégrité de la sécurité du système/sous-système/équipement examiné. Cela est illustré à la Figure 6. Le Tableau E.9 donne des indications concernant les techniques/mesures de vérification et de validation pour chaque niveau d'intégrité de la sécurité.

A la discrétion de l'autorité de tutelle, le chargé d'évaluation peut appartenir à l'organisation du fournisseur ou à celle du client mais, dans de tels cas, le chargé d'évaluation doit

– être autorisé par l'autorité de tutelle,
– être totalement indépendant de l'équipe projet,
– rendre compte directement à l'autorité de tutelle.

5.3.10 Justification de la sécurité

Les preuves montrant que le système/sous-système/équipement répond aux conditions définies pour l'acceptation de la sécurité doivent être présentées dans un document de justification de la sécurité structuré appelé dossier de sécurité, comme expliqué en 5.1.

5.3.11 Remise du système/sous-système/équipement

Avant de remettre le système/sous-système/équipement à la société d'exploitation ferroviaire, les conditions d'acceptation et d'approbation de la sécurité définies en 5.5 doivent être remplies, y compris la soumission du dossier de sécurité et du rapport d'évaluation de la sécurité.

5.3.12 Exploitation et maintenance

Après la remise, les procédures, les systèmes de soutien et le suivi de la sécurité définis dans le plan d'assurance sécurité et dans la Partie 5 du rapport de sécurité technique (partie du dossier de sécurité) doivent avoir été assimilés.

Durant la vie opérationnelle d'un système, il est possible que des demandes d'évolutions soient émises pour diverses raisons, toutes n'ayant pas trait à la sécurité. L'impact sur la sécurité de chaque demande d'évolution doit être évalué, en faisant référence à la partie correspondante de la documentation de sécurité. Lorsqu'une demande d'évolution aboutit à une modification susceptible d'affecter la sécurité du système, ou des systèmes associés, ou de l'environnement, la partie appropriée du cycle de vie sécurité doit être reprise afin de s'assurer que la modification mise en œuvre ne réduit pas de façon inacceptable le niveau de sécurité. Le Tableau E.10 donne des indications relatives à l'application, l'exploitation et la maintenance pour chaque niveau d'intégrité de la sécurité.

5.3.13 Retrait du service et dépose

A la fin de la vie opérationnelle du système, son retrait du service et sa dépose doivent être réalisés conformément aux mesures définies dans le plan d'assurance sécurité et dans la Partie 5 du rapport de sécurité technique (partie du dossier de sécurité).

5.4 Preuve de la sécurité fonctionnelle et technique

En plus de la preuve de la gestion de la qualité et de la sécurité, décrite en 5.2 et 5.3, une troisième condition doit être remplie avant qu'un système/sous-système/équipement puisse

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

être accepté comme présentant la sûreté requise pour son utilisation attendue. Cette condition consiste en une preuve technique de la sécurité de la conception, qui doit être documentée dans le rapport de sécurité technique. Ce document constitue la Partie 4 du dossier de sécurité du système/sous-système/équipement, comme expliqué en 5.1.

Le rapport de sécurité technique est obligatoire pour les niveaux d'intégrité de la sécurité de 1 à 4 inclus (voir l'Annexe A pour des explications sur les niveaux d'intégrité de la sécurité). Cependant, il est recommandé que le degré d'approfondissement des informations et la portée de la documentation correspondante soient appropriés au niveau d'intégrité de la sécurité du système/sous-système/équipement examiné. Les exigences pour le niveau d'intégrité de la sécurité 0 (non de sécurité) sont hors du cadre de la présente norme relative à la sécurité.

Le rapport de sécurité technique doit expliquer les principes techniques garantissant la sécurité de la conception, en incluant (ou en donnant les références) toutes les preuves de soutien (par exemple principes de conception et calculs, spécifications d'essais et résultats, et analyses de sécurité).

Le rapport de sécurité technique doit être présenté conformément au plan suivant:

a) Partie 1: Introduction

Cette partie doit fournir une description globale de la conception, en incluant un résumé des principes de la sécurité technique sur lesquels elle repose pour les aspects sécurité, et en indiquant dans quelle mesure le système/sous-système/équipement est considéré de sécurité, en accord avec la présente norme.

Cette partie doit également mentionner les normes (et leur édition) utilisées comme fondement de la sécurité technique de la conception. Dans le cas de modifications ou d'ajouts sur des équipements déjà en service, ou de la rédaction de nouvelles normes, ou à la fin d'une phase de développement, alors, exceptionnellement, les éditions des normes utilisées pour la conception d'origine peuvent être utilisées comme base, sous réserve qu'elles aient déjà été acceptées lors de l'approbation de l'équipement d'origine. Cette exception ne peut être appliquée que si la prise en compte des dernières éditions des normes venait à engendrer des modifications supplémentaires à l'équipement existant, ou si l'évolution s'avérait être d'un coût élevé injustifiable. Les raisons justifiant l'utilisation de cette possibilité doivent être fournies.

b) Partie 2: Assurance d'une exploitation fonctionnelle correcte

Cette partie doit contenir toutes les preuves nécessaires à la démonstration d'une exploitation correcte du système/sous-système/équipement dans des conditions normales exemptes de panne (c'est-à-dire en l'absence de tout défaut), en accord avec les exigences d'utilisation et de sécurité spécifiées pour l'utilisation.

Les sujets suivants, pour lesquels des exigences plus détaillées sont présentées à l'Article B.2, doivent être traités:

2.1 Description de l'architecture du système (voir B.2.1 et Tableau E.4);

2.2 Définition des interfaces (voir B.2.2);

2.3 Respect de la spécification des exigences du système (voir B.2.3);

2.4 Respect de la spécification des exigences de sécurité (voir B.2.4);

2.5 Assurance du fonctionnement correct du matériel (voir B.2.5);

2.6 Assurance du fonctionnement correct du logiciel (voir B.2.6).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

c) Partie 3: Effets des pannes

Cette partie doit démontrer que le système/sous-système/équipement continue à respecter ses exigences de sécurité spécifiées, y compris les objectifs quantifiés de sécurité, lors de l'occurrence de pannes matérielles aléatoires.

De plus, des pannes systématiques peuvent toujours exister, en dépit des processus de gestion de la qualité et de la sécurité définis en 5.2 et 5.3. Cette partie doit démontrer quelles sont les mesures techniques adoptées en vue de réduire les risques associés à un niveau acceptable.

Cette partie doit également inclure la démonstration que les pannes de tout système/sous-système/équipement ayant un niveau d'intégrité de la sécurité inférieur, incluant le niveau 0, à celui du système global ne peuvent pas réduire la sécurité du système global.

Les points suivants, pour lesquels des exigences plus détaillées sont présentées à l'Article B.3, doivent être abordés dans cette partie. Des indications sont également données dans les Tableaux E.5 et E.6.

3.1 Effets des pannes simples (voir B.3.1);

3.2 Indépendance des entités (voir B.3.2);

3.3 Détection des pannes simples (voir B.3.3);

3.4 Actions suivant la détection (incluant le maintien dans un état sûr) (voir B.3.4);

3.5 Effets des pannes multiples (voir B.3.5);

3.6 Protections contre les pannes systématiques (voir B.3.6).

d) Partie 4: Exploitation en présence d'influences externes

Cette partie doit démontrer que lorsqu'il est soumis aux influences externes définies dans les spécifications des exigences du système, le système/sous-système/équipement

– continue à respecter ses exigences d'exploitation spécifiées,
– continue à respecter ses exigences de sécurité spécifiées (incluant les conditions de pannes).

Le dossier de sécurité n'a de valeur que dans la limite spécifiée d'influences externes telle qu'elle est définie dans la spécification des exigences du système. La sécurité n'est pas garantie en dehors de ces limites, sauf si des mesures spécifiques supplémentaires sont fournies.

Les méthodes utilisées pour supporter les influences externes spécifiées doivent être complètement expliquées et justifiées.

Des exigences plus détaillées sont contenues à l'Article B.4.

e) Partie 5: Conditions d'utilisation relatives à la sécurité

Cette partie doit spécifier (ou référencer) les règles, conditions et contraintes qui doivent être observées lors de l'utilisation du système/sous-système/équipement. Elle doit inclure les conditions d'utilisation contenues dans le dossier de sécurité de tout sous-système ou équipement associé.

Des exigences plus détaillées sont contenues à l'Article B.5. Des indications sont également données au Tableau E.10.

f) Partie 6: Essais de qualification de la sécurité

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Cette partie doit contenir la preuve que les essais de qualification de la sécurité dans des conditions opérationnelles ont été complètement menés avec succès. Ces essais sont expliqués à l'Article B.6.

Le plan du rapport de sécurité technique est illustré à la Figure 7.

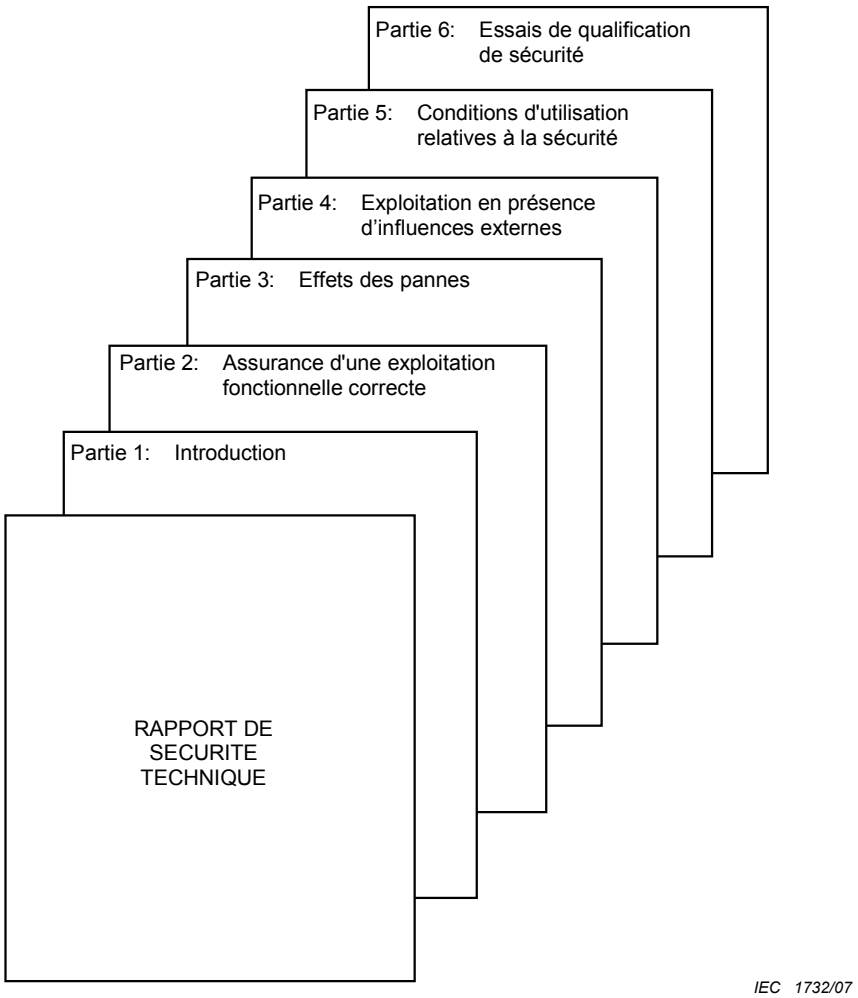


Figure 7 – Plan du rapport de sécurité technique

5.5 Acceptation et approbation de la sécurité

Le présent paragraphe définit le processus d'acceptation et d'approbation de la sécurité pour des systèmes/sous-systèmes/équipements électroniques relatifs à la sécurité. Sauf lorsque cela est considéré comme approprié, il ne spécifie pas par qui il est recommandé que le travail soit réalisé à chaque phase, cela pouvant varier en fonction des circonstances.

5.5.1 Introduction

Conformément aux explications fournies en 5.1, un système, un sous-système ou une partie d'équipement électronique ferroviaire relatif à la sécurité doit satisfaire aux trois conditions suivantes, avant de pouvoir être considéré comme présentant la sûreté requise pour son utilisation attendue:

– preuve de la gestion de la qualité;
– preuve de la gestion de la sécurité;
– preuve de la sécurité technique et fonctionnelle.

Ces trois conditions ont été expliquées en 5.2, 5.3 et 5.4.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

La preuve de la gestion de la qualité, de la gestion de la sécurité et de la sécurité fonctionnelle/technique doit faire partie du dossier de sécurité, comme montré en 5.1 et à la Figure 3.

On peut considérer trois types différents de dossiers de sécurité:

– dossier de sécurité pour les produits génériques (indépendants de l'application) Un produit générique peut être réutilisé pour diverses applications indépendantes;
– dossier de sécurité pour une application générique (pour une classe d'application) Une application générique peut être réutilisée pour une classe ou un type d'applications ayant des fonctions communes;
– dossier de sécurité pour une application spécifique (pour une application spécifique) Une application spécifique est utilisée pour une seule installation particulière.

Il est essentiel de démontrer pour chaque application «spécifique» que les conditions d'environnement et le contexte d'utilisation sont compatibles avec celles de l'application «générique» (voir 5.5.4).

Pour chacune des trois catégories, le plan du dossier de sécurité et la procédure d'obtention de l'approbation de la sécurité sont essentiellement les mêmes. Cependant, les applications spécifiques présentent une particularité: pour cette catégorie, une approbation séparée de la sécurité est nécessaire pour la conception de l'application du système et sa réalisation physique (exemple: fabrication, installation, essai et infrastructures pour l'exploitation et la maintenance). C'est pourquoi le dossier de sécurité pour les applications spécifiques doit être divisé en deux parties:

– le dossier de sécurité pour la conception de l'application: celui-ci doit contenir la preuve de la sécurité de la conception théorique de l'application spécifique;
– le dossier de sécurité de la réalisation physique: celui-ci doit contenir la preuve de la sécurité de la réalisation physique de l'application spécifique.

Les deux parties doivent être organisées comme décrit en 5.1 et à la Figure 3.

5.5.2 Processus d'approbation de la sécurité

En vue de l'approbation de la sécurité d'une application, on doit réaliser une évaluation indépendante de la sécurité du système/sous-système/équipement et de son dossier de sécurité, afin d'obtenir une assurance supplémentaire sur l'atteinte du niveau de sécurité nécessaire. Il convient que ses résultats soient présentés dans un rapport d'évaluation de la sécurité. Il convient que le rapport explique les activités qui ont été réalisées par le chargé d'évaluation de la sécurité pour déterminer comment le système, sous-système ou partie d'équipement (matériel et logiciel) a été conçu pour répondre à ses exigences spécifiées, et il peut éventuellement spécifier des conditions supplémentaires pour l'exploitation du système/sous-système/équipement. Le degré d'approfondissement de cette évaluation et le degré d'indépendance avec lequel elle a été effectuée sont fondés sur les résultats de la classification des risques, comme expliqué dans la CEI 62278. Des essais spécifiques peuvent être exigés par le chargé d'évaluation de la sécurité afin de renforcer la confiance.

La preuve documentaire globale doit comprendre

– la spécification des exigences du système (ou sous-système/équipement),
– la spécification des exigences de sécurité,
– le dossier de sécurité, comprenant

  Partie 1: Définition du système/sous-système/équipement,

  Partie 2: Rapport de la gestion de la qualité (preuve de la gestion de la qualité),

  Partie 3: Rapport de la gestion de la sécurité (preuve de la gestion de la sécurité),

  Partie 4: Rapport de sécurité technique (preuve de la sécurité fonctionnelle/technique),

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Partie 5: Dossiers de sécurité connexes (le cas échéant),

Partie 6: Conclusion,

– le rapport d'évaluation de la sécurité.

Si toutes les conditions d'acceptation de la sécurité ont été remplies, comme démontré par le dossier de sécurité, et soumises aux résultats de l'évaluation indépendante de la sécurité, le système/sous-système/équipement peut alors recevoir l'approbation de la sécurité par l'autorité de tutelle concernée. Une approbation peut faire l'objet de conditions supplémentaires (temporaires ou permanentes) imposées par le chargé d'évaluation de la sécurité.

Pour un produit générique (c'est-à-dire indépendant de l'application), et pour une application générique (c'est-à-dire classe d'application), il est recommandé que l'approbation de la sécurité accordée par une autorité de tutelle puisse être acceptée par d'autres autorités de tutelle (c'est-à-dire acceptation réciproque). Cela n'est pas considéré comme possible pour des applications spécifiques.

Le processus d'approbation de la sécurité, pour les trois catégories de dossiers de sécurité, est illustré par la Figure 8.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

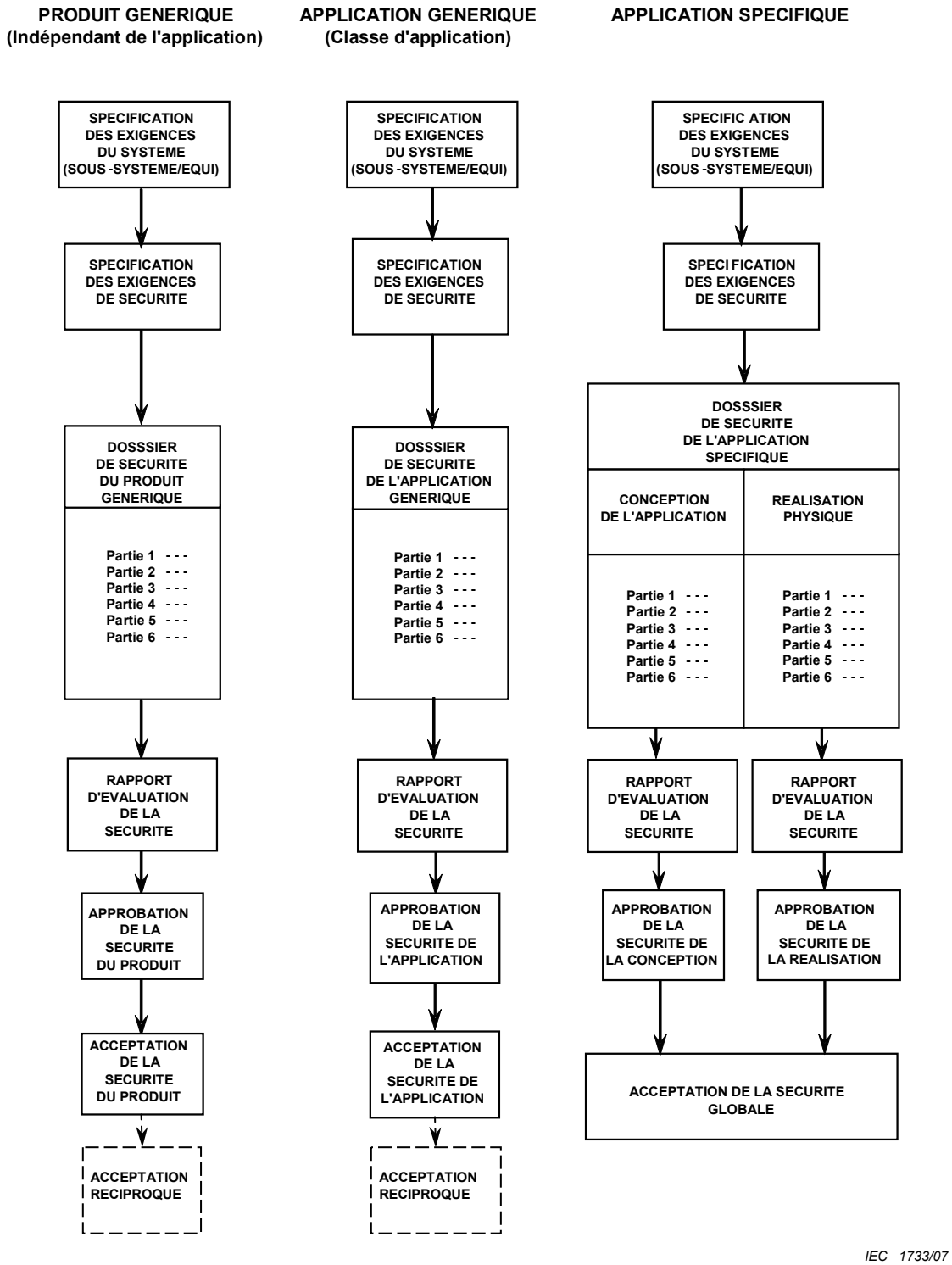


Figure 8 – Processus type d'approbation et d'acceptation de la sécurité

5.5.3 Après approbation de la sécurité

Après qu'un système/sous-système/équipement a reçu l'approbation de la sécurité, toute modification ultérieure doit être contrôlée en utilisant la même gestion de la qualité, de la sécurité et les mêmes critères de sécurité fonctionnelle/technique qui seraient utilisés pour une nouvelle conception. Toute la documentation concernée, y compris le dossier de sécurité, doit être mise à jour ou complétée par une documentation supplémentaire, et la conception modifiée doit être soumise à approbation.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Une fois qu'un système/sous-système/équipement installé a été mis en état de fonctionnement, les procédures appropriées, les systèmes de soutien et le suivi de la sécurité, comme définis dans le plan d'assurance sécurité et à la Partie 5 du rapport de sécurité technique (partie du dossier de sécurité), doivent être utilisés pour assurer une exploitation sûre continue durant toute la période d'utilisation, à savoir: l'exploitation, la maintenance, les modifications, les évolutions et le retrait du service éventuel. Ces activités doivent être contrôlées en utilisant la même gestion de la qualité, de la sécurité, et les mêmes critères de sécurité technique que pour la conception d'origine. Toute la documentation concernée doit être tenue à jour, y compris le dossier de sécurité, et toutes les modifications ou évolutions doivent être soumises à approbation.

5.5.4 Dépendance entre les approbations de la sécurité

Comme mentionné en 5.1, il est accepté que le dossier de sécurité pour un système dépende des dossiers de sécurité d'autres sous-systèmes ou équipements. Dans un tel cas, l'approbation de la sécurité du système principal n'est pas possible sans l'approbation préalable de la sécurité des sous-systèmes/équipements en relation.

Si l'approbation de la sécurité a été obtenue pour un produit générique ou pour une application générique, il est accepté de faire référence à celle-ci dans l'approbation de la sécurité pour une application spécifique; il n'est pas nécessaire de répéter le processus d'approbation générique pour chaque application. Cette dépendance entre les approbations de la sécurité est illustrée à la Figure 9.

Un dossier de sécurité peut être basé sur la démonstration que l'application spécifique proposée est techniquement équivalente à une application existante ayant déjà fait l'objet d'une approbation de la sécurité spécifique. Une nouvelle approbation de la sécurité pour cette application spécifique est nécessaire.

Il est essentiel de s'assurer pour de tels cas de dépendance que les conditions d'application relatives à la sécurité, établies dans le rapport de sécurité technique de chaque dossier de sécurité, sont remplies dans le dossier de sécurité de niveau supérieur, ou reportées dans les conditons d'application relatives à la sécurité du dossier de sécurité de niveau supérieur.

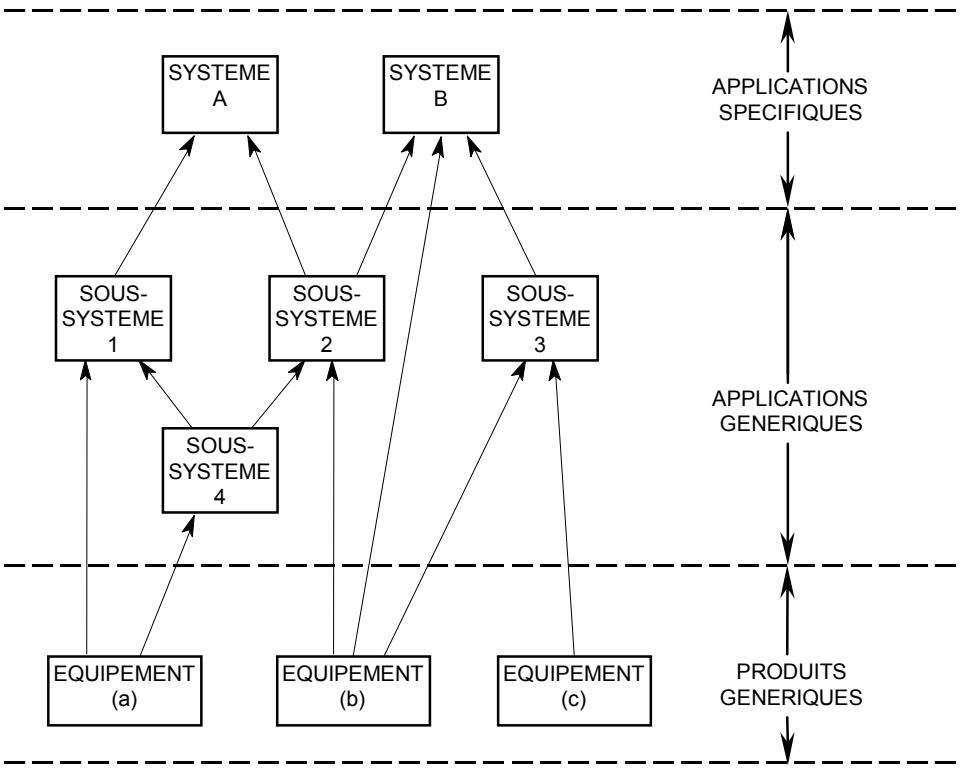


Figure 9 – Exemples de dépendances entre dossiers de sécurité/ approbation de la sécurité

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe A
(normative)

Niveaux d'intégrité de la sécurité

A.1 Introduction

La présente annexe donne des précisions pour la déclinaison, l'allocation et la prise en compte des exigences de sécurité et de l'intégrité de la sécurité et sur l'utilisation des niveaux d'intégrité de la sécurité pour les systèmes relatifs à la sécurité des applications ferroviaires.

Les taux maximaux acceptables d'occurrence d'une situation dangereuse (THR) formalisant les objectifs quantifiés de sécurité de chaque application ferroviaire particulière sont de la responsabilité de la société d'exploitation ferroviaire concernée; ils ne sont pas définis dans la présente norme.

Le processus de gestion de la sécurité est défini dans la CEI 62278.

A.2 Exigences de sécurité

La spécification des exigences du système (ou sous-système ou équipement, selon le cas) peut être considérée selon deux aspects (voir la Figure A.1):

– les exigences non relatives à la sécurité (y compris les exigences fonctionnelles opérationnelles);
– les exigences relatives à la sécurité.

Les exigences relatives à la sécurité sont généralement appelées exigences de sécurité. Celles-ci peuvent être contenues dans un document distinct appelé spécification des exigences de sécurité.

Les exigences de sécurité peuvent être constituées de deux parties:

– les exigences fonctionnelles de sécurité;
– les exigences d'intégrité de la sécurité.

Les exigences fonctionnelles de sécurité concernent les fonctions de sécurité réelles que le système, sous-système ou équipement doit accomplir.

Les exigences d'intégrité de la sécurité définissent le niveau d'intégrité de la sécurité exigé pour chaque fonction relative à la sécurité.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

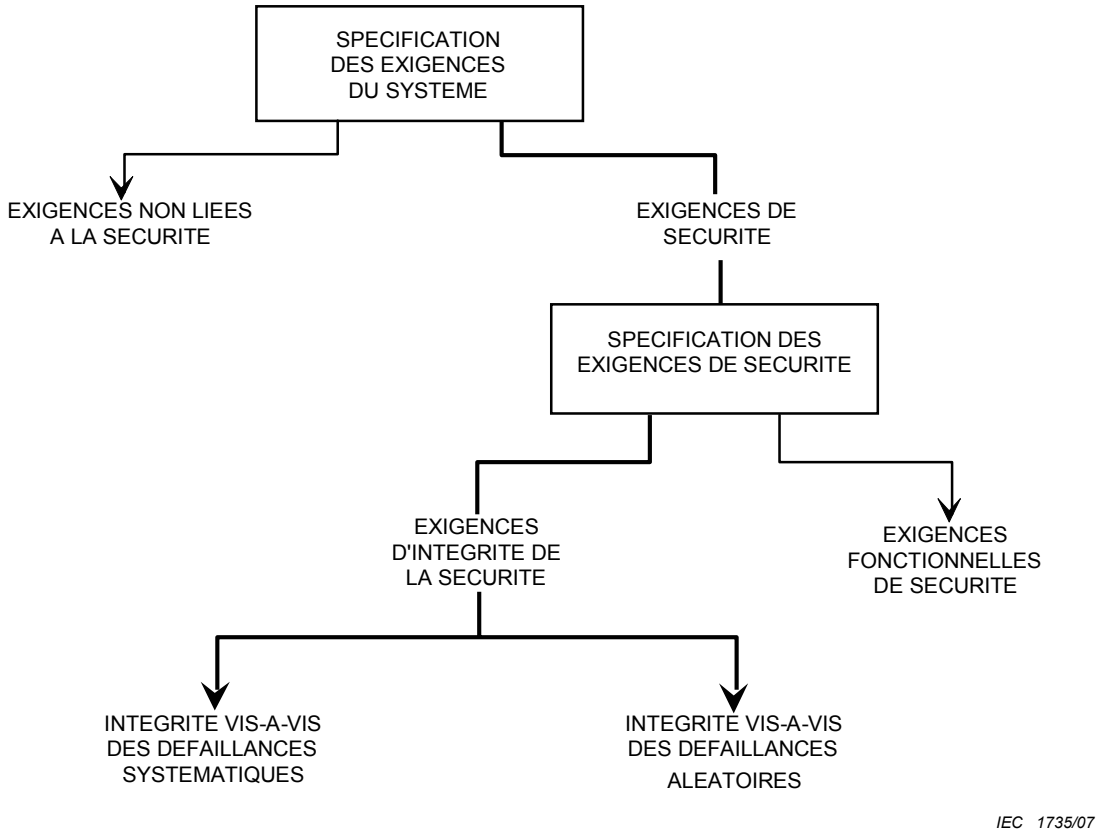


Figure A.1 – Exigences de sécurité et intégrité de la sécurité

A.3 Intégrité de la sécurité

L'intégrité de la sécurité caractérise l'aptitude d'un système relatif à la sécurité à remplir ses fonctions de sécurité requises. Plus l'intégrité de la sécurité est élevée, moins il est à craindre que le système ne remplira pas ses fonctions de sécurité requises.

L'intégrité de la sécurité comprend deux parties (voir la Figure A.1):

– l'intégrité vis-à-vis des défaillances systématiques;
– l'intégrité vis-à-vis des défaillances aléatoires.

Il est nécessaire de satisfaire à la fois aux exigences d'intégrité vis-à-vis des défaillances systématiques et aux exigences vis-à-vis des défaillances aléatoires pour atteindre l'intégrité de la sécurité adéquate.

NOTE Il est recommandé que les défaillances causées par les conditions d'environnement (par exemple: CEM, température, vibration, etc.) soient prises en compte dans l'élaboration des exigences d'intégrité de la sécurité vis-à-vis des défaillances systématiques et/ou des défaillances aléatoires, selon le cas.

L'intégrité vis-à-vis des défaillances systématiques représente la partie non quantifiable de l'intégrité de la sécurité et correspond aux erreurs systématiques dangereuses (matérielles ou logicielles). Les erreurs systématiques sont dues à des erreurs humaines à différentes phases du cycle de vie du système/sous-système/équipement.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

EXEMPLE
- erreurs de spécification;
- erreurs de conception;
- erreurs de fabrication;
- erreurs d'installation;
- erreurs d'exploitation;
- erreurs de maintenance;
- erreurs de modifications.

L'intégrité de sécurité vis-à-vis des défaillances systématiques est atteinte grâce aux dispositions de gestion de la qualité et de la sécurité spécifiées en 5.2 et 5.3.

Les mesures techniques pour se protéger des erreurs systématiques font partie des conditions de la sécurité technique spécifiées en 5.4.

Parce qu'il n'est pas possible d'évaluer l'intégrité vis-à-vis des défaillances systématiques par des méthodes quantitatives, des niveaux d'intégrité de la sécurité sont utilisés afin de regrouper différentes méthodes, divers outils et techniques qui, lorsqu'ils sont utilisés efficacement, permettent d'obtenir un niveau de confiance suffisant quant à l'adéquation de la réalisation du système à un niveau d'intégrité établi (voir l'Annexe E).

L'intégrité vis-à-vis des défaillances aléatoires est la partie de l'intégrité de la sécurité relative aux défaillances aléatoires dangereuses, en particulier les défaillances matérielles aléatoires, qui résultent de la fiabilité des composants.

L'obtention de l'intégrité vis-à-vis des défaillances aléatoires fait partie des conditions de la sécurité technique spécifiées en 5.4.

Une évaluation quantifiée de l'intégrité vis-à-vis des défaillances aléatoires doit être menée au moyen de calculs de probabilités. Ceux-ci sont basés sur des données connues de modes de défaillance et de taux de défaillance des composants matériels, ainsi que sur les instants d'apparition des défaillances matérielles aléatoires. Dans le cas des composants conçus en sécurité intrinsèque (voir l'Annexe C), on suppose généralement un taux de défaillance dangereux (contraire à la sécurité) égal à zéro, bien que le risque résiduel d'une telle défaillance puisse encore exister et il est recommandé de s'en protéger, comme cela est spécifié en 5.4 et B.3.6.

L'allocation des exigences d'intégrité de la sécurité et des niveaux d'intégrité de la sécurité est respectivement décrite aux Articles A.4 et A.5.

A.4 Allocation des exigences d'intégrité de la sécurité

Une démarche systématique pour la détermination des exigences d'intégrité de la sécurité des équipements de signalisation ferroviaire, prenant en compte à la fois l'environnement d'utilisation et le modèle architectural du système de signalisation, doit être employée.

Au cœur de cette approche, on trouve une interface bien définie entre l'environnement d'utilisation et le système de signalisation. Du point de vue de la sécurité, cette interface consiste en une liste des situations dangereuses et de leur taux maximal acceptable d'occurrence associé pour le système. Il convient de souligner que la présentation qui est faite de la démarche ne limite en rien la coopération entre les fournisseurs et les sociétés d'exploitation ferroviaire, mais a pour but de clarifier les responsabilités et les interfaces.

A partir de cette interface, la démarche se déroule comme suit:

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– analyse inductive pour identifier les conséquences possibles des situations dangereuses et les risques associés;

– analyse déductive pour identifier les causes des situations dangereuses.

Le processus global consiste en l'analyse des risques et la maîtrise des situations dangereuses (voir Figure A.2). L'analyse des risques permet de définir les taux maximaux acceptables d'occurrence d'une situation dangereuse, qui sont alors les données d'entrée de la phase de maîtrise des situations dangereuses.

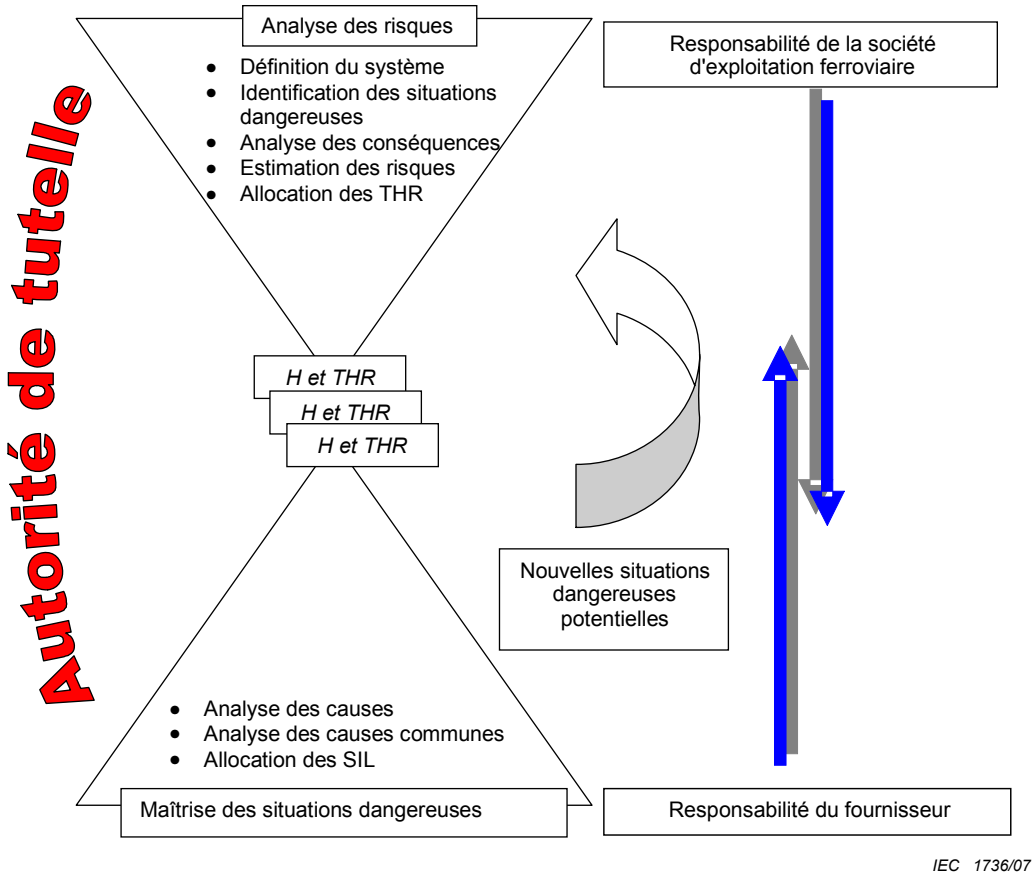


Figure A.2 – Vue d'ensemble du processus global

Il est important de noter que le taux maximal acceptable d'occurrence d'une situation dangereuse est un objectif qui tient compte à la fois de l'intégrité vis-à-vis des défaillances aléatoires et des défaillances systématiques. Il est accepté que seule l'intégrité vis-à-vis des défaillances aléatoires soit quantifiable. Des mesures qualitatives et leur appréciation seront nécessaires pour justifier du respect des exigences d'intégrité vis-à-vis des défaillances systématiques. Cela est essentiellement couvert par les niveaux d'intégrité de la sécurité (et les mesures qui en découlent).

L'autorité de tutelle doit approuver les résultats des deux analyses: analyse des risques et maîtrise des situations dangereuses.

NOTE Dans certains cas, ces deux étapes ne sont pas totalement indépendantes. La maîtrise des situations dangereuses peut amener à des modifications du système qui améliorent ses performances au niveau de la sécurité. Le recouvrement des flèches sur la Figure A.2 illustre cette éventualité. Ainsi, le processus global est itératif dans ces cas.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

A.4.1 Analyse de risques

La Figure A.3 donne un exemple du processus d'analyse des risques. Les paragraphes suivants décrivent cette phase en détail.

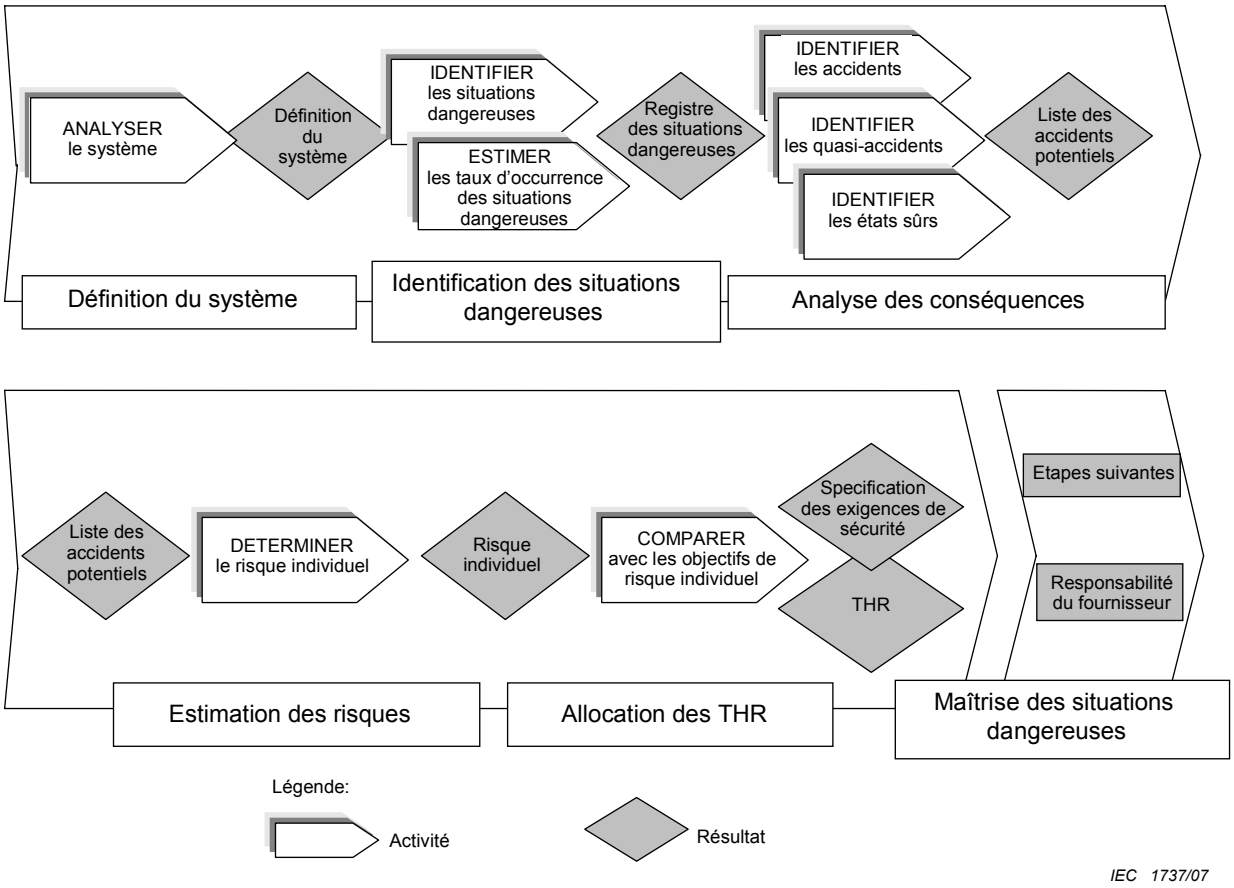


Figure A.3 – Exemple de processus d'analyse des risques

A.4.1.1 Définition du système et identification des situations dangereuses

Il est de la responsabilité de la société d'exploitation ferroviaire

– de définir le système (indépendamment de toute solution technique),
– d'identifier les situations dangereuses pertinentes pour le système.

L'identification des situations dangereuses d'un système consiste en des analyses systématiques d'un produit, d'un processus, d'un système ou toute autre activité pour déterminer les conditions défavorables (dangers) qui pourraient se produire au cours du cycle de vie du système. De telles conditions défavorables peuvent potentiellement conduire à des blessures humaines ou des dommages pour l'environnement.

L'identification systématique des situations dangereuses implique généralement deux phases:

– une phase empirique (basée sur le retour d'expérience, par exemple listes de contrôle);
– une phase créative (ou prédictive, par exemple brainstorming, études prévisionnelles structurées).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Les phases empiriques et créatives d'identification des situations dangereuses se complètent l'une l'autre, ce qui augmente la confiance que l'espace potentiel de situations dangereuses a été couvert et que toutes les situations dangereuses significatives ont bien été identifiées.

NOTE Les méthodes qui produisent, de manière inadaptée, un grand nombre de situations dangereuses, pour la plupart insignifiantes ou définies de façon imprécise, sont un gaspillage de ressources. Elles peuvent induire en erreur et mener à une évaluation des risques improductive. Hormis les projets particulièrement complexes, impliquant beaucoup de personnel, d'activités et d'équipements, une liste de plusieurs centaines de situations dangereuses est peu raisonnable et dénote une étude mal conçue ou mal conduite.

Les situations dangereuses dépendent de la définition du système et, en particulier, des limites du système, ce qui autorise une décomposition hiérarchique des situations dangereuses par rapport aux systèmes et aux sous-systèmes. Cela signifie également que l'identification des situations dangereuses et l'analyse des causes doivent être répétées à plusieurs niveaux de détail au cours du développement du système.

La Figure A.4 montre que la cause d'une situation dangereuse au niveau système peut être considérée comme une situation dangereuse de niveau sous-système (en respectant les limites du sous-système). Ainsi, cette définition permet une approche structurée hiérarchique pour le dépistage et l'analyse des situations dangereuses.

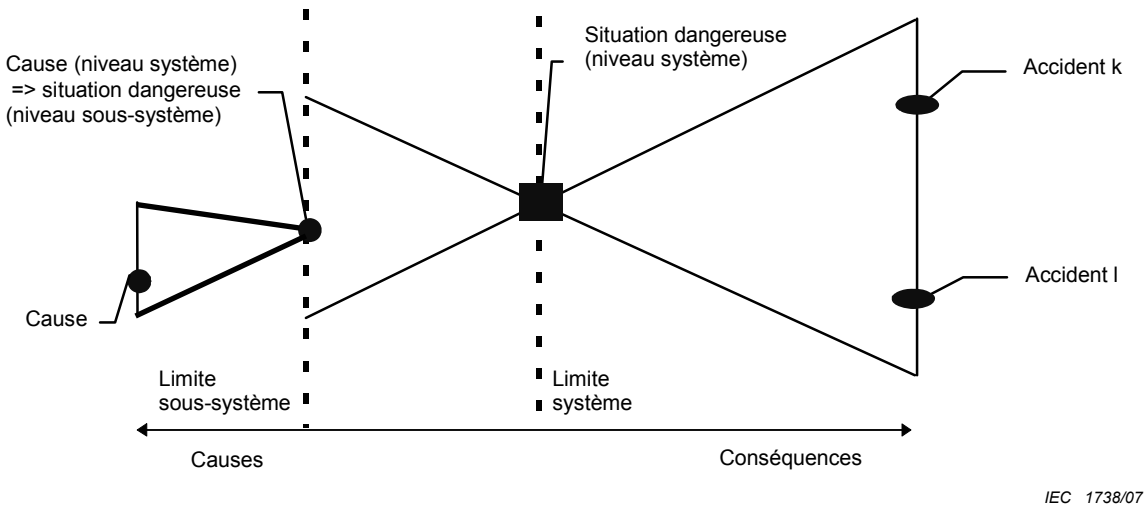


Figure A.4 – Définition des situations dangereuses par rapport aux limites du système

Pour mieux s'assurer que l'effort d'évaluation du risque est concentré sur les situations dangereuses les plus significatives, il est recommandé que celles-ci, une fois identifiées, soient classées selon leur niveau de risque perçu.

Toutes les situations dangereuses identifiées et toute autre information pertinente doivent être enregistrées dans un registre des situations dangereuses.

A.4.1.2 Analyse des conséquences, estimation des risques et allocation des taux maximaux acceptables d'occurrence d'une situation dangereuse

Il est de la responsabilité de la société d'exploitation ferroviaire

– d'analyser les conséquences, c'est-à-dire les pertes,
– de définir les critères de tolérance du risque,
– de décliner les taux maximaux acceptables d'occurrence d'une situation dangereuse, et
– de s'assurer que le risque résultant est tolérable (dans le respect des critères de tolérance du risque appropriés).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

La seule exigence est que les taux maximaux acceptables d'occurrence d'une situation dangereuse résultants doivent être déclinés en tenant compte des critères de tolérance du risque. Les critères de tolérance du risque ne sont pas définis dans la présente norme, mais dépendent d'exigences législatives nationales ou européennes.

Les méthodes d'analyse doivent, selon le cas:

– soit estimer explicitement le risque (individuel) résultant,
– soit décliner les taux maximaux acceptables d'occurrence d'une situation dangereuse par comparaison avec les performances de systèmes existants ou à partir de règles technologiques reconnues, en s'appuyant sur des méthodes statistiques ou analytiques,
– soit décliner les taux maximaux acceptables d'occurrence d'une situation dangereuse à partir d'approches qualitatives alternatives si, au final, elles définissent une liste de situations dangereuses et leurs taux maximaux acceptables d'occurrence correspondants.

Il est important de noter que cette approche donne à la société d'exploitation ferroviaire la liberté de définir les situations dangereuses et leurs taux maximaux acceptables d'occurrence d'une situation dangereuse correspondants à chaque niveau, selon leurs besoins propres. Alors qu'une société d'exploitation ferroviaire peut fixer des objectifs généraux de très haut niveau, une autre peut fixer des objectifs très détaillés au niveau des fonctions de sécurité.

A.4.2 Maîtrise des situations dangereuses

La maîtrise des situations dangereuses porte sur la gestion de la réalisation des taux maximaux acceptables d'occurrence d'une situation dangereuse requis et des fonctions de sécurité associées.

Si les taux maximaux acceptables d'occurrence d'une situation dangereuse ne sont pas fournis, soit le fournisseur les fournira avec le système qu'il propose à la société d'exploitation ferroviaire, soit cette dernière et le fournisseur travailleront ensemble pour définir les exigences.

La maîtrise des situations dangereuses consiste à réaliser une analyse des causes suivie d'un certain nombre d'activités qui peuvent être résumées ainsi:

– dans le cas où les taux maximaux acceptables d'occurrence d'une situation dangereuse ne sont pas définis, définir les hypothèses de sécurité et les fonctions du système liées aux situations dangereuses définies;
– dans le cas où les taux maximaux acceptables d'occurrence d'une situation dangereuse sont définis, définir l'architecture du système et allouer les taux maximaux acceptables d'occurrence d'une situation dangereuse aux fonctions du système correspondant à l'architecture (solution technique) pour respecter les exigences de sécurité;
– déterminer les exigences d'intégrité de la sécurité pour les sous-systèmes;
– compléter la spécification des exigences de sécurité;
– analyser le système/sous-système pour respecter les exigences;
– identifier les nouvelles situations potentiellement dangereuses apparaissant au cours de la conception du système/sous-système, au travers des processus de conception et de vérification. Ensuite, soit s'assurer que les nouvelles situations potentiellement dangereuses sont couvertes par les fonctionnalités existantes, soit, si les nouvelles situations potentiellement dangereuses exigent des fonctionnalités supplémentaires en dehors du système/sous-système, ramener les situations potentiellement dangereuses au niveau de l'analyse des risques pour un traitement complémentaire;
– déterminer les exigences de fiabilité pour le matériel.

Le processus de maîtrise des situations dangereuses est représenté à la Figure A.5.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

NOTE Une démarche de maîtrise des situations dangereuses bien structurée contient implicitement des parties essentielles d'un rapport de sécurité technique. Dans ce cas, il est suffisant de faire référence à cette démarche dans le rapport de sécurité technique.

A.4.2.1 Analyse des causes

L'analyse des causes est constituée de deux étapes clés:

Dans une première phase de l'analyse des causes, le taux maximal acceptable d'occurrence d'une situation dangereuse pour chaque situation dangereuse est réparti à un niveau fonctionnel (fonctions du système). Le taux maximal acceptable d'occurrence d'une situation dangereuse pour une fonction est alors traduit en un niveau d'intégrité de la sécurité, selon le tableau des niveaux d'intégrité de la sécurité. Les niveaux d'intégrité de la sécurité (SIL) sont définis à ce niveau fonctionnel pour les sous-systèmes qui réalisent la fonctionnalité.

Si, en ce qui concerne les fonctions de sécurité, la société d'exploitation ferroviaire a déjà défini les situations dangereuses et leurs taux maximaux acceptables d'occurrence d'une situation dangereuse, alors la première phase des analyses des causes n'a pas lieu d'être et les niveaux d'intégrité de la sécurité peuvent être directement alloués à partir des taux maximaux acceptables d'occurrence d'une situation dangereuse requis.

Un sous-système, c'est-à-dire la combinaison de plusieurs équipements, peut supporter plusieurs fonctions de sécurité, dont chacune pourrait nécessiter un niveau d'intégrité de la sécurité différent des autres. Dans ce cas, le sous-système doit satisfaire à tous les niveaux d'intégrité de la sécurité exigés. Cela peut être obtenu si chaque fonction respecte le plus haut niveau d'intégrité de la sécurité ou si la démonstration d'indépendance entre fonctions de niveaux d'intégrité de la sécurité différents peut être fournie. Dans les deux cas, une analyse des défaillances de mode commun doit être réalisée.

Dans une deuxième phase de l'analyse des causes, les taux des situations dangereuses alloués aux sous-systèmes sont à nouveau déclinés pour aboutir aux taux de défaillance des équipements mais, à ce niveau de décomposition, les niveaux d'intégrité de la sécurité restent inchangés. Par conséquent, les niveaux d'intégrité de la sécurité du logiciel tels que définis dans la CEI 62279 seraient identiques à ceux du niveau sous-système, sauf exceptions décrites dans la CEI 62279.

Le processus de répartition peut être effectué selon n'importe quelle méthode basée sur la logique combinatoire et qui permet une représentation appropriée, par exemple méthode de diagramme de fiabilité, arbres des défauts, tables de vérité, graphes de Markov, etc. Dans tous les cas, un soin particulier doit être pris lorsqu'une exigence d'indépendance est demandée. Alors que dans la première phase de l'analyse des causes, l'indépendance fonctionnelle est exigée (c'est-à-dire que les défaillances des fonctions doivent être indépendantes les unes des autres vis-à-vis des erreurs systématiques et de pannes aléatoires), l'indépendance physique est suffisante dans la deuxième phase (c'est-à-dire que les défaillances des sous-systèmes doivent être indépendantes les unes des autres vis-à-vis des pannes aléatoires). Les hypothèses faites dans l'analyse des causes doivent être vérifiées et peuvent conduire à des règles d'application de sécurité pour la phase de réalisation.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

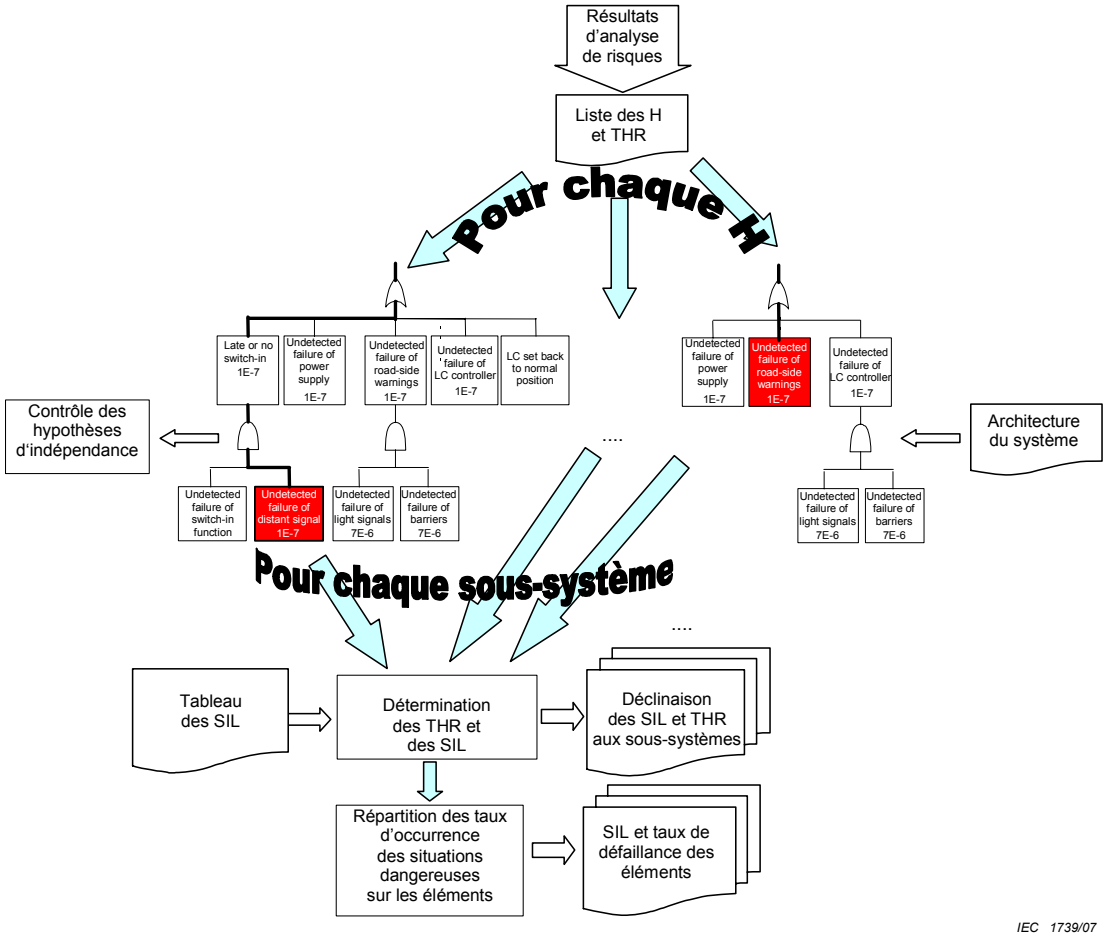


Figure A.5 – Exemple de processus de maîtrise d'une situation dangereuse (H)

A.4.2.2 Analyse de défaillance de mode commun

Un soin particulier doit être pris lorsque des affirmations d'indépendance (combinaisons de ET logiques) sont énoncées. Il est indispensable de s'assurer qu'une indépendance

– physique,
– fonctionnelle,
– de processus

suffisante existe entre les sous-systèmes ou les fonctions système (voir B.3.2 et B.3.6). Si l'indépendance ne peut pas être complètement démontrée, alors les défaillances de mode commun doivent être modélisées à un niveau de détail approprié. De plus, il doit être démontré que les règles de sécurité appropriées relevant directement de combinaisons de ET logiques sont respectées et vérifiées.

A.4.2.2.1 Indépendance physique

L'indépendance physique est une nécessité absolue pour rendre crédibles les calculs sur les arbres des défauts (par utilisation de portes ET logiques pour les effets aléatoires). Ainsi, dans tous les cas, une analyse de défaillance de mode commun est nécessaire pour démontrer l'indépendance.

Des conditions d'obtention de l'indépendance physique sont décrites aux Articles D.2 et D.3 (informatifs). Un paragraphe du dossier de sécurité traite également explicitement de l'indépendance entre éléments.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

NOTE Si l'on considère deux matériels réparables, définis généralement par leur taux de défaillance et leur taux de réparation, et si l'on regarde de plus près les combinaisons de ET logiques dans un arbre des défauts, une interprétation différente des taux de réparation (ou des temps de réparation correspondants) est nécessaire. D'habitude, après l'occurrence d'une panne d'un matériel, il faut qu'au moins deux choses se passent avant que le matériel fonctionne de nouveau (voir Figure A.6):

– la panne est détectée et un état sûr du système est atteint (passivation);

– le matériel est réparé et remis en service.

Par temps de réparation et de remise en service, on entend le temps logistique pour la réparation après la détection, le temps réel de réparation (localisation de la panne, réparation, échange, vérification) et le temps pour remettre l'équipement en service. Alors que dans un contexte fiabiliste, le temps de détection est généralement négligé, ce temps devient important dans le contexte de la sécurité. Les applications critiques de sécurité ne peuvent pas s'appuyer sur des autotests ou sur des mesures semblables, mais il faut que la détection et la passivation soient réalisées indépendamment de l'élément en panne. Il convient de démontrer dans le dossier de sécurité la suffisance des mécanismes de détection et de passivation des défaillances.

Généralement, dans un contexte de sécurité, le temps réel de réparation et de remise en service peut être négligé si d'autres mesures de contrôle sont prises pendant cette période. Dans ce cas, le taux de réparation de l'analyse fiabiliste peut être interprété comme le temps de détection et de passivation, ici défini comme le temps de mise en sécurité (SDT) ou taux de passivation équivalent (SDR).

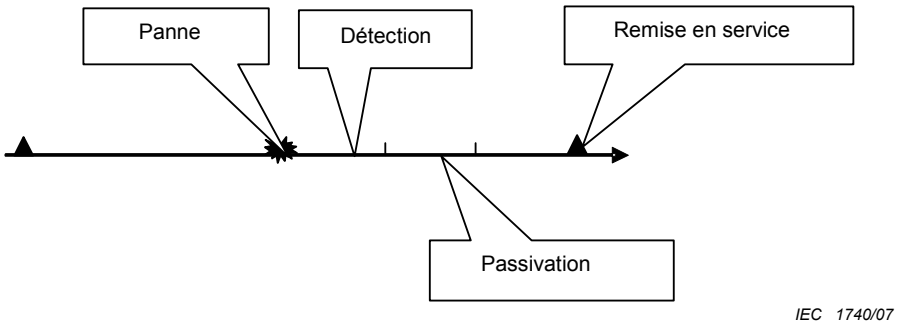


Figure A.6 – Interprétation des temps de défaillance et de réparation

Pour modéliser, à l'aide d'une porte ET logique, la composition de deux matériels indépendants, la formule de base suivante de calcul des taux (asymptotiques) maximaux acceptables d'occurrence et de détection des situations dangereuses pour des systèmes à haute disponibilité peut être employée, sous l'hypothèse que les taux sont constants au cours du temps:

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

où FR représente le taux d'occurrence des situations potentiellement dangereuses.

Si les temps d'essais périodiques sont utilisés comme temps de détection, alors on peut utiliser l'Equation (A.1) en prenant

T/2 + temps de passivation = SDT = 1/SDR comme temps moyen d'essais.

Cela signifie que pour employer correctement des combinaisons ET logiques, il faut que chaque matériel soit équipé d'un mécanisme indépendant de détection des défaillances et d'arrêt. Si un matériel n'est pas équipé d'un tel mécanisme, alors il faut que la durée de vie du matériel installé soit prise en compte, comme cela est décrit en B.3.3.

La disponibilité du système est un autre aspect qu'il faut prendre en compte dans la conception et qui limite en fait le libre choix des paramètres.

EXEMPLE Si l'on considère deux équipements identiques avec un MTBF de 10 000 h et un temps moyen de détection de 1 h (en ignorant le temps de passivation), alors le taux de défaillance résultant pour le système constitué des deux équipements en parallèle (combinaison ET dans la logique des défaillances) vaut 2×10^{-8} par heure. Si l'un des équipements a un temps moyen de détection de 1 000 h (par exemple la détection par la maintenance), alors le résultat vaut seulement 10^{-5} par heure, ce qui correspond à une amélioration d'à peine un facteur 10 du MTBF d'un équipement simple. Si le temps moyen de détection d'une défaillance d'un équipement correspond à sa durée de vie, alors le gain devient encore plus marginal.

L'indépendance physique est le niveau d'indépendance le plus bas; elle est recherchée typiquement au niveau des composants. Si l'indépendance physique est garantie, alors les

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

exigences d'intégrité vis-à-vis des défaillances aléatoires peuvent être déclinées au niveau de décomposition inférieur.

A.4.2.2.2 Indépendance fonctionnelle

L'indépendance fonctionnelle implique qu'il n'y a ni erreurs systématiques ni pannes aléatoires, qui peuvent être la cause d'une défaillance simultanée de plusieurs fonctions. Ainsi, pour ce type d'indépendance également, une analyse de défaillance de mode commun serait nécessaire dans le but de montrer que les fonctions sont indépendantes. C'est ce que l'on appelle, dans cette norme, l'indépendance vis-à-vis des influences fonctionnelles. Il est recommandé que les exigences d'intégrité vis-à-vis des défaillances aléatoires et systématiques ne soient déclinées au niveau de décomposition inférieur qu'à condition que l'indépendance fonctionnelle soit garantie.

Lors de la mise en œuvre d'une analyse par arbres des défauts sur deux fonctions systèmes, soient A et B, ce qui est le cas usuel dans le processus d'allocation d'exigences d'intégrité de sécurité, on doit considérer que l'utilisation des portes ET logiques implique immédiatement les règles de sécurité suivantes:

– la réalisation de A et celle de B doivent être physiquement indépendantes;
– les temps de mise en sécurité définis par la somme du temps de détection et du temps nécessaire à la passivation de chaque matériel doivent être définis et respectés.

NOTE En général, les fonctions ne sont pas indépendantes mais peuvent être décomposées en sous-fonctions indépendantes et en sous-fonctions affectées par des défaillances de mode commun. La Figure A.7 montre un traitement générique de défaillances de mode commun selon l'analyse par arbre des défauts.

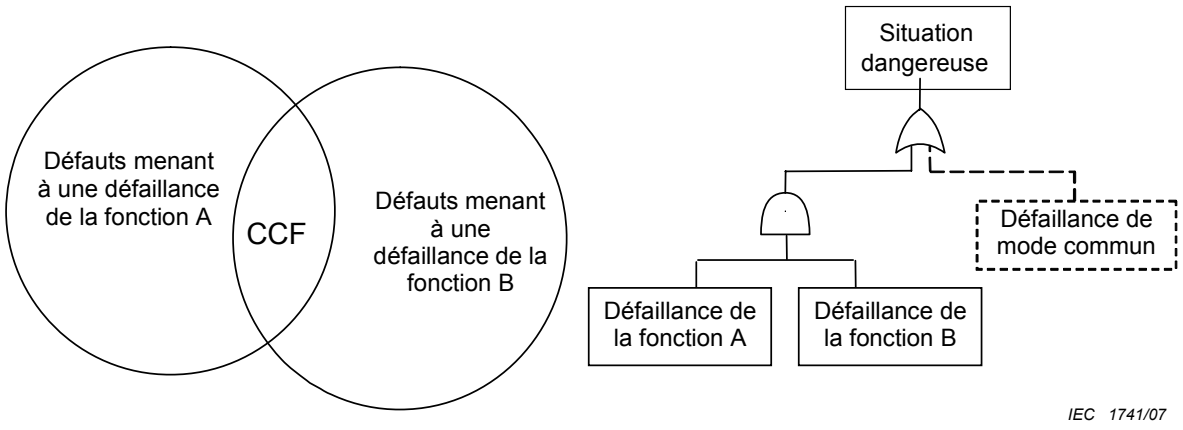


Figure A.7 – Traitement de l'indépendance fonctionnelle par analyse par arbre des défauts

A.4.2.2.3 Indépendance de processus

Les produits et les systèmes sont généralement le fruit des activités inhérentes aux premiers processus de cycle de vie. D'une manière générale, ceux-ci comprennent les phases de concept, de spécification des exigences, de conception système, de développement système, de vérification et de validation, qui ont une influence significative sur les propriétés du produit final. Il est généralement admis que plus les degrés de criticité sont élevés pour un produit ou un système dans son environnement d'application, plus les processus de cycle de vie doivent être robustes et méthodiques. De plus, comme la manifestation d'erreurs systématiques est inhérente à ces processus du cycle de vie, un degré d'indépendance entre ces processus est souvent souhaitable.

D'une manière similaire aux principes d'indépendance fonctionnelle et physique, on considère que l'indépendance et la diversité du personnel et des processus du cycle de vie contribuent globalement à une intégrité de la sécurité plus élevée des produits et des systèmes. Des

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

exigences de niveaux d'intégrité de la sécurité plus élevées requièrent ainsi des degrés plus élevés d'indépendance de processus et du personnel pour garantir que les erreurs systématiques soient évitées ou minimisées.

Il est recommandé que les processus de développement respectent les niveaux d'intégrité de la sécurité exigés et garantissent qu'il y a une indépendance suffisante au niveau de l'organisation et du personnel entre les équipes de développement dans le but de réduire au maximum les erreurs systématiques. Les dispositions d'indépendance relatives au développement des logiciels sont décrites dans la CEI 62279.

A.4.3 Identification et traitement des nouvelles situations dangereuses apparaissant au cours de la conception

La réalisation d'un système de signalisation peut éventuellement mener à des propriétés imprévues ou indésirables pouvant causer des blessures aux personnes, en particulier si le système ou la technologie sont nouveaux. De nouvelles situations dangereuses peuvent survenir pour plusieurs raisons:

– forte potentialité pour une nouvelle technologie d'être la source de nouvelles situations dangereuses (manque d'expérience);
– apparition de situations dangereuses cachées du système ferroviaire existant, en raison de l'introduction d'une nouvelle technologie (par exemple passage de l'analogique au numérique);
– nouvelle situation dangereuse au niveau de la conception en raison d'une spécification incomplète/incorrecte;
– les modes d'exploitation spécifiques d'un système ferroviaire existant peuvent ne pas être bien adaptés et peuvent créer de nouvelles situations dangereuses pour les exploitants, les mainteneurs, voire d'autres membres du personnel, le public, etc.;
– des erreurs de conception peuvent créer de nouvelles situations dangereuses mais celles-ci peuvent souvent être reliées à d'autres situations dangereuses déjà identifiées.

Ces particularités peuvent provoquer des circonstances et des états dangereux qui exigent le même traitement systématique que celui appliqué aux situations dangereuses déjà identifiées.

Le processus pour l'identification et le traitement de nouvelles situations dangereuses mis en évidence lors de la conception ou lors de l'exploitation d'un système est pratiquement identique à la phase d'analyse de risque. Une fois identifiées, les situations dangereuses de niveau système pouvant affecter les performances du système global ou pouvant causer des blessures aux personnes doivent être déclarées par le fournisseur à la société d'exploitation ferroviaire. Selon les risques perçus, celle-ci peut exiger une évaluation qualitative ou quantitative, en vue de rechercher et de s'accorder sur un taux maximal acceptable d'occurrence d'une situation dangereuse approprié pour chacune de ces situations dangereuses.

NOTE Il est alors possible de procéder selon au moins deux voies différentes:

- il est possible de rapprocher la nouvelle situation dangereuse d'une autre déjà identifiée: dans ce cas, il est recommandé que le fournisseur s'assure que le taux d'occurrence de la situation dangereuse résultant de la combinaison de ces deux situations dangereuses est toujours compatible avec le taux maximal acceptable d'occurrence d'une situation dangereuse qui a été fixé par la société d'exploitation ferroviaire. Il est recommandé que le registre des situations dangereuses et le dossier de sécurité tracent cette situation dangereuse;
- la nouvelle situation dangereuse n'a aucun rapport avec celles déjà identifiées: dans ce cas, il est recommandé que le fournisseur avertisse la société d'exploitation ferroviaire et lui donne toutes les informations sur l'analyse de la situation dangereuse qu'il a effectuée (les causes, les conséquences, le risque, etc.). Il convient alors que la société d'exploitation ferroviaire décide si cette nouvelle situation dangereuse peut être acceptée ou non:
    - si ce n'est pas le cas, il convient que le fournisseur re-conçoive son produit/système si cela est possible. Si ce n'est pas possible, il convient alors de mettre en œuvre des mesures de protection complémentaires pour maintenir la situation dangereuse et le risque associé à un niveau acceptable;
    - si c'est le cas, la société d'exploitation ferroviaire a la charge de définir le taux maximal acceptable d'occurrence de la nouvelle situation dangereuse et il convient que le fournisseur conçoive le système/produit en prenant en compte cette exigence;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

- dans les deux cas, dès que la décision concernant cette nouvelle situation dangereuse aura été prise, il convient que tout soit enregistré dans le registre des situations dangereuses et dans le dossier de sécurité.

Les taux maximaux acceptables d'occurrence d'une situation dangereuse doivent être déclinés pour chaque nouvelle situation dangereuse, ce qui mènera à la mise à jour des exigences.

A.5 Niveaux d'intégrité de la sécurité

A.5.1 Aspects généraux

L'intégrité de la sécurité est spécifiée sur une échelle de quatre niveaux discrets. Le niveau 4 correspond au niveau d'intégrité de la sécurité le plus élevé, le niveau 1 correspond au niveau le plus bas. Le niveau 0 est utilisé pour indiquer qu'il n'y a pas d'exigence de sécurité. Il est recommandé qu'un niveau d'intégrité de la sécurité fasse appel à une appréciation qualitative des facteurs tels que la gestion de la qualité et de la sécurité ainsi que les conditions techniques de la sécurité.

Les situations dangereuses liées à un système sont identifiées et évaluées en fonction de leurs conséquences potentielles, pendant la phase d'analyse des risques du cycle de vie du système (comme cela est décrit en A.4.1). Cette activité (inductive) aboutit à la définition du taux maximal acceptable d'occurrence d'une situation dangereuse pour chaque situation dangereuse. Néanmoins, un fournisseur peut commencer le développement de produits génériques d'une façon déductive et peut même obtenir une approbation de sécurité pour un dossier de sécurité de produits génériques (sans résultats d'aucune analyse des risques disponible) mais, au final, il doit garantir que les taux maximaux acceptables d'occurrence d'une situation dangereuse exigés (dossier de sécurité d'une application) sont respectés. La société d'exploitation ferroviaire et/ou l'autorité de tutelle doivent déterminer les directives de base pour ce processus.

Au cours des phases suivantes, les exigences du système et l'allocation des exigences du système, les taux maximaux acceptables d'occurrence d'une situation dangereuse sont déclinés respectivement sur les fonctions du système et sur les sous-systèmes.

Un objectif qualitatif de sécurité et un objectif quantitatif doivent être associés à chacune de ces fonctions. L'objectif qualitatif doit être exprimé sous la forme d'un niveau d'intégrité de la sécurité et doit couvrir l'intégrité vis-à-vis des défaillances systématiques. L'objectif quantitatif doit être exprimé sous la forme d'une valeur de taux de défaillance et doit couvrir l'intégrité vis-à-vis des défaillances aléatoires.

Les fonctions de sécurité au sein d'un système sont réalisées au travers des sous-systèmes. Les niveaux d'intégrité de la sécurité sont alloués aux fonctions de sécurité et par conséquent aux sous-systèmes supportant ces fonctions, mais pas à un niveau (de décomposition) inférieur. Le niveau d'intégrité de la sécurité pour un équipement au sein d'un sous-système est le même que celui du sous-système, à moins que l'indépendance fonctionnelle ne puisse être démontrée entre les équipements au sein des sous-systèmes.

Il est important de souligner que l'atteinte d'un niveau d'intégrité de la sécurité spécifié exige la conformité avec tous les facteurs présentés sur la Figure A.8, à savoir

– les dispositions de gestion de la qualité,

– les dispositions de gestion de la sécurité,

– les conditions de la sécurité technique,

– les objectifs quantifiés de sécurité.

L'atteinte d'un objectif de sécurité quantifié particulier ne signifie pas, à elle seule, que le niveau d'intégrité de la sécurité correspondant a été respecté. De la même façon, le respect des dispositions de gestion de la qualité, de la sécurité et des conditions de la sécurité technique associées à un niveau d'intégrité de la sécurité particulier ne signifie pas que l'objectif de sécurité quantifié ou le niveau d'intégrité de la sécurité lui-même correspondant a

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

été réalisé. Tous les facteurs présentés sur la Figure A.8 doivent être respectés pour atteindre l'intégrité de la sécurité spécifiée.

Il est également important de comprendre que si les objectifs de sécurité quantifiés de la Figure A.8 sont ceux qui sont exigés dans le but de tenir les performances de la sécurité ferroviaire telles qu'elles sont décrites dans les alinéas suivants, il ne doit pas être supposé que l'objectif relatif à une fonction de sécurité particulière peut nécessairement être réalisé par un seul sous-système ou équipement. Quand cela est nécessaire, l'objectif de sécurité exigé doit être réalisé par la combinaison de fonctions, de sous-systèmes ou d'équipements, comme cela est expliqué dans la présente annexe.

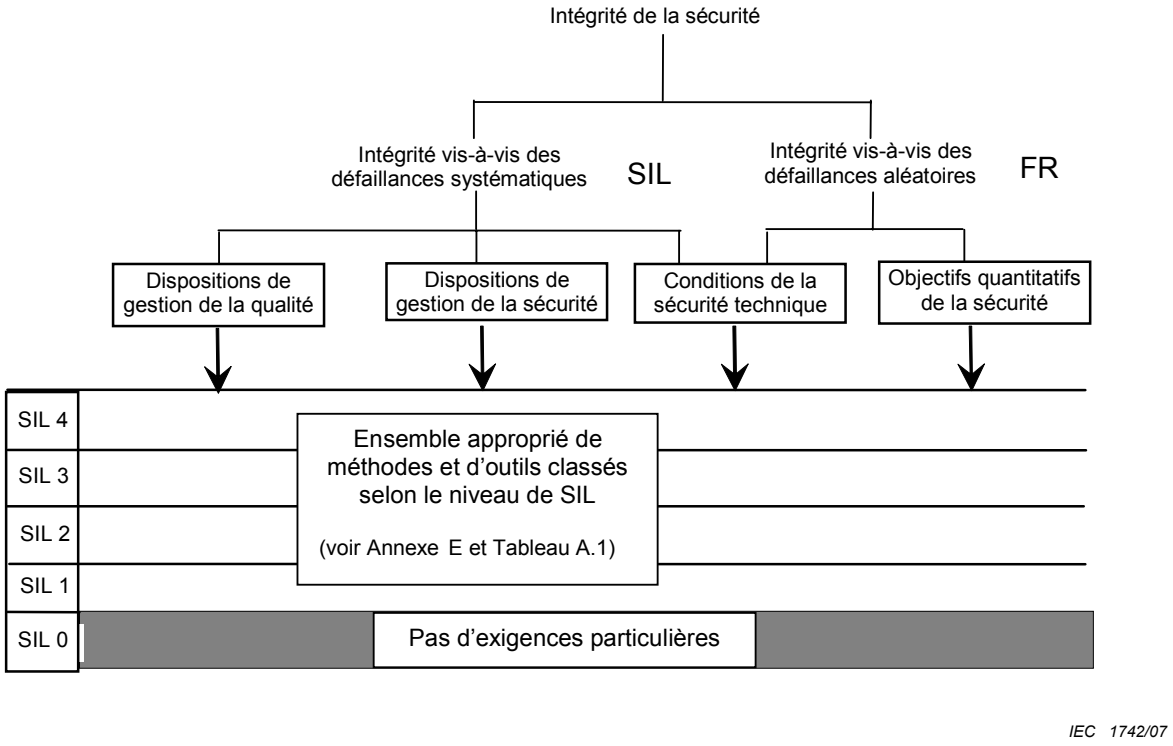


Figure A.8 – Liens entre les niveaux d'intégrité de la sécurité et les techniques

A.5.2 Liens entre les niveaux d'intégrité de la sécurité et les objectifs de sécurité

La présente norme est basée sur l'hypothèse que la sécurité repose à la fois sur l'utilisation de mesures appropriées pour éviter ou tolérer les fautes (comme garde-fous contre les défaillances systématiques) et sur l'utilisation de mesures adéquates pour maîtriser les défaillances aléatoires. Il est recommandé que les mesures prises contre les deux types de causes de défaillances soient équilibrées pour atteindre les performances optimales de sécurité d'un système. Pour ce faire, le concept de niveaux d'intégrité de la sécurité (SIL) est utilisé. Les niveaux d'intégrité de la sécurité sont utilisés comme un moyen de faire correspondre les approches qualitatives (pour éviter les défaillances systématiques) et l'approche quantitative (pour maîtriser les défaillances aléatoires), puisque la quantification des défaillances systématiques n'est pas faisable.

Comme dans beaucoup d'autres normes, cet équilibre est exprimé dans un tableau, qui consiste en une liste de niveaux d'intégrité de la sécurité 0, 1, 2, 3, 4 et une liste d'intervalles correspondants de taux maximaux acceptables d'occurrence des situations dangereuses l_0,..., l_4.

Le tableau des niveaux d'intégrité de la sécurité est applicable aux fonctions de sécurité ou aux sous-systèmes qui réalisent unes ou plusieurs de ces fonctions. Ayant suivi les mesures et les méthodes exigées pour le SIL *x*, il n'y a aucun besoin de considérer les défaillances

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

systématiques pour démontrer que le taux maximal acceptable d'occurrence d'une situation dangereuse est respecté.

Le tableau des SIL identifie le niveau d'intégrité de la sécurité exigé pour la fonction de sécurité à partir du taux maximal acceptable d'occurrence d'une situation dangereuse. Ainsi, si le taux maximal acceptable d'occurrence d'une situation dangereuse pour une fonction F a été défini selon une méthode quantitative, le niveau d'intégrité de la sécurité exigé doit être déterminé par l'utilisation du Tableau A.1.

Tableau A.1 – Tableau des SIL

Taux maximal acceptable d'occurrence d'une situation dangereuse (THR) par heure et par fonction	Niveau d'intégrité de la sécurité
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Une fonction dont les exigences quantitatives sont plus contraignantes que 10^{-9} h^{-1} doit être traitée selon l'une des manières suivantes:

– s'il est possible de décomposer la fonction en sous-fonctions indépendantes du point de vue fonctionnel, le taux maximal acceptable d'occurrence d'une situation dangereuse peut être réparti sur les sous-fonctions et un niveau d'intégrité de la sécurité peut être fixé à chacune des sous-fonctions;

– si la fonction ne peut pas être décomposée, les mesures et les méthodes exigées pour le niveau d'intégrité de la sécurité 4 doivent, au minimum, être mises en œuvre et la fonction doit être utilisée en combinaison avec d'autres mesures techniques ou opérationnelles dans le but d'atteindre le taux maximal acceptable d'occurrence d'une situation dangereuse requis.

NOTE Par rapport à d'autres normes, le tableau des niveaux d'intégrité de la sécurité de la présente norme ne contient qu'une colonne pour les fréquences (autrefois appelée mode de fonctionnement continu / forte sollicitation) et n'a pas de colonne pour des probabilités de défaillances à la sollicitation (autrefois appelée mode de fonctionnement à la sollicitation). Les raisons de la restriction à un seul mode sont les suivantes:

– moins d'ambiguïtés dans la détermination des niveaux d'intégrité de la sécurité,

– tous les systèmes dont le mode de fonctionnement est à la sollicitation peuvent être modélisés comme des systèmes à mode fonctionnement continu,

– les systèmes de commande et de contrôle de la signalisation à mode de fonctionnement continu représentent clairement la majorité des applications ferroviaires modernes.

Le tableau des niveaux d'intégrité de la sécurité a été élaboré en prenant en compte la CEI 61508-1.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe B
(normative)

Exigences techniques détaillées

B.1 Introduction

Comme expliqué en 5.4, une preuve technique démontrant la sécurité de la conception d'un système/sous-système/équipement doit figurer dans le rapport de sécurité technique (qui constitue la Partie 4 du dossier de sécurité). Le rapport doit être présenté dans les rubriques suivantes:

Partie 1 Introduction

Partie 2 Assurance d'une exploitation fonctionnelle correcte

Partie 3 Effets des pannes

Partie 4 Exploitation en présence d'influences externes

Partie 5 Conditions d'utilisation relatives à la sécurité

Partie 6 Essais de qualification de la sécurité

Chacune de ces rubriques a été brièvement traitée en 5.4. Des exigences plus détaillées concernant les Parties 2 à 6 du rapport de sécurité technique sont présentées aux Articles B.2 à B.6.

Le rapport de sécurité technique est obligatoire pour les niveaux d'intégrité de la sécurité de 1 à 4 inclus (voir l'Annexe A pour des explications sur les niveaux d'intégrité de la sécurité). Cependant, il est recommandé que le degré d'approfondissement des informations et la portée de la documentation correspondante soient appropriés au niveau d'intégrité de la sécurité du système/sous-système/équipement examiné. Les exigences pour le niveau d'intégrité de la sécurité 0 (non de sécurité) sont hors du cadre de la présente norme relative à la sécurité.

Le plan du rapport de sécurité technique est illustré à la Figure 7.

B.2 Assurance d'une exploitation fonctionnelle correcte
(Partie 2 du rapport de sécurité technique)

Cette partie concerne l'exploitation correcte du système/sous-système/équipement exempte de panne (c'est-à-dire en l'absence de tout défaut), en accord avec les exigences d'utilisation et de sécurité spécifiées.

Certains aspects particuliers sont traités ci-dessous, en utilisant les rubriques indiquées en 5.4.

B.2.1 Description de l'architecture du système

Ce paragraphe doit comprendre une description générale de la conception du système/sous-système/équipement, suffisamment précise pour permettre de comprendre clairement les principes et techniques qu'il utilise.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.2.2 Définition des interfaces

B.2.2.1 Interfaces homme-machine

Les interfaces homme-machine consistent en ce qui suit:

a) Exploitant

Cet alinéa doit décrire les mécanismes par lesquels le système/sous-système/équipement sera exploité par le personnel d'exploitation et le personnel technique.

EXEMPLE
- dans des conditions normales;
- en réponse à des alarmes;
- par l'utilisation de procédures "d'aide".

b) Configuration

Cet alinéa doit décrire les procédés utilisés par le personnel technique pour configurer le système/sous-système/équipement en vue d'une application ferroviaire spécifique.

EXEMPLE
- paramétrage du logiciel;
- câblage du matériel;
- techniques d'installation;
- procédures.

c) Maintenance

Cet alinéa doit décrire les mécanismes d'interfaces, y compris l'utilisation de tout équipement connexe qui sera utilisé par le personnel de maintenance lors de l'exécution des divers échelons de maintenance.

Des informations plus détaillées sont précisées en B.5.2.

B.2.2.2 Interfaces du système

Les interfaces internes et externes du système doivent être décrites.

a) Internes

Cet alinéa doit définir les interfaces fonctionnelles et physiques entre les entités internes du système/sous-système/équipement.

EXEMPLE
- zones neutres ou polluées électriquement;
- structures de bus internes;
- liaisons de communication;
- surveillance et correction fonctionnelles;
- diagnostic et surveillance de l'état général.

b) Externes

Cet alinéa doit définir les interfaces fonctionnelles et physiques entre les entités externes du système/sous-système/équipement.

EXEMPLE
- capteurs;
- actionneurs;
- liaisons de communication;
- appareils d'essais et de surveillance;
- infrastructures d'extension.

B.2.3 Respect de la spécification des exigences du système

Ce paragraphe doit démontrer la manière dont les exigences fonctionnelles d'utilisation spécifiées dans la spécification des exigences du système/sous-système/équipement sont respectées par la conception. Toutes les preuves qui s'y rapportent doivent être incluses (ou référencées).

EXEMPLE
- principes et calculs de conception;
- spécifications et résultats d'essais;
- validation.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.2.4 Respect de la spécification des exigences de sécurité

Ce paragraphe doit démontrer la manière dont les exigences fonctionnelles de sécurité spécifiées sont respectées par la conception. Toutes les preuves qui s'y rapportent doivent être incluses (ou référencées).

EXEMPLE – principes et calculs de conception;
– spécifications et résultats d'essais;
– analyses de sécurité et résultats.

B.2.5 Assurance du fonctionnement correct du matériel

Ce paragraphe doit décrire l'architecture matérielle du système/sous-système/équipement, et expliquer la manière dont la conception atteint l'intégrité requise, telle qu'énoncée dans la spécification des exigences et dans toute norme applicable, en ce qui concerne

– la fiabilité,
– la disponibilité,
– la maintenabilité,
– la sécurité.

Il est permis de prendre en compte la sécurité en se limitant aux conditions exemptes de pannes, car les effets des pannes sont traités par ailleurs (voir Article B.3).

B.2.6 Assurance du fonctionnement correct du logiciel

Les exigences de la CEI 62279 doivent être respectées.

Toute la documentation exigée par la CEI 62279 doit être incluse ou référencée dans cette partie, en particulier le rapport de validation du logiciel et le rapport d'évaluation du logiciel.

De plus, l'interaction entre le matériel et le logiciel doit être expliquée.

NOTE Il est recommandé de prêter une certaine attention à des thèmes particuliers, comme par exemple:
– la dépendance entre matériel et logiciel,
– la séquence de l'interaction,
– le temps de réponse,
– les programmes d'autotests,
– la surveillance de l'état général,
– les techniques d'acquisition de données,
– la dégradation progressive,
– les méthodes d'inversion logique.

B.3 Effets des pannes
(Partie 3 du rapport de sécurité technique)

Cette partie concerne l'aptitude du système/sous-système/équipement à continuer à respecter ses exigences de sécurité spécifiées en cas de pannes matérielles aléatoires et, autant que possible, en cas de pannes systématiques.

Des points particuliers qui doivent être pris en compte sont détaillés de B.3.1 à B.3.6 ci-après, en utilisant les rubriques mentionnées en 5.4.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.3.1 Effets des pannes simples

(Voir également les informations du Tableau E.4)

Il est nécessaire de s'assurer que le système/sous-système/équipement respecte son taux maximal acceptable d'occurrence d'une situation dangereuse en cas de panne aléatoire simple. Il est nécessaire de s'assurer que les systèmes de niveaux SIL 3 et SIL 4 restent dans un état de sécurité lors de l'occurrence de toute panne matérielle aléatoire simple qui est considérée comme possible. Les pannes dont les effets ont été démontrés comme négligeables peuvent être ignorées. Ce principe, qui est connu comme sécurité intrinsèque, peut être obtenu de différentes manières:

a) sécurité composite

A l'aide de cette technique, chaque fonction relative à la sécurité est réalisée par au moins deux entités. Chacune de ces entités doit être indépendante de toutes les autres, pour éviter toute défaillance de mode commun. Des activités non restrictives ne sont autorisées que lorsque le nombre suffisant d'entités est d'accord. Une panne dangereuse dans une entité doit être détectée et passivée dans un délai suffisant pour éviter une panne similaire sur une seconde entité.

b) sécurité réactive

Cette technique permet à une fonction relative à la sécurité d'être réalisée par une entité simple, à condition que son fonctionnement sûr soit assuré par une détection rapide et une passivation de toute panne dangereuse (par exemple par cryptage, calcul multiple et comparaison, ou par essai continu). Bien qu'une seule entité réalise la fonction effective relative à la sécurité, la fonction de contrôle/essai/détection doit être considérée comme une seconde entité, qui doit être indépendante pour éviter toute défaillance de mode commun.

c) sécurité intrinsèque

Cette technique permet à une fonction relative à la sécurité d'être réalisée par une seule entité, à condition que tous les modes de défaillance vraisemblables de l'entité soient non dangereux. Le fait que tout mode de défaillance soit considéré comme invraisemblable (par exemple grâce aux propriétés physiques intrinsèques) doit être justifié en utilisant la procédure définie à l'Annexe C. Il est également permis d'utiliser la sécurité intrinsèque pour certaines fonctions dans des systèmes de sécurité réactive et composite, par exemple pour assurer l'indépendance entre entités, ou pour forcer la mise à l'arrêt si une panne dangereuse est détectée.

Quelle que soit la technique ou la combinaison de techniques utilisée, l'assurance qu'aucun mode de défaillance aléatoire unique d'un composant matériel n'est dangereux doit être démontrée en utilisant les méthodes d'analyse structurée appropriées. Les modes de défaillance d'un composant à prendre en compte dans l'analyse doivent être identifiés en utilisant les procédures définies à l'Annexe C.

NOTE Il est recommandé d'utiliser une méthode d'analyse de défaillance de type descendant, telle que l'analyse par arbre des défauts (FTA). Il est également recommandé de faire appel, si nécessaire, à une méthode de type ascendant telle que l'analyse des modes de défaillance et de leurs effets (AMDE). Voir également les informations du Tableau E.6.

Les analyses de défaillances doivent être qualitatives, et quantitatives lorsque des données fiables sont disponibles. Il est recommandé que les taux de défaillance matérielle aléatoire, ou les probabilités de défaillance d'un composent, soient basés, si possible, sur des données "terrain". Une répartition d'un taux de défaillance global d'un composant entre ses modes de défaillance doit être justifiée dans l'analyse.

B.3.2 Indépendance des entités

Dans les systèmes comportant plus d'une entité dont le dysfonctionnement simultané peut présenter un danger, l'indépendance entre entités est une précondition obligatoire pour la sécurité concernant les pannes simples. Des règles ou directives appropriées doivent être respectées pour assurer cette indépendance. Les mesures prises doivent être effectives pour tout le cycle de vie du système. De plus, le système/sous-système doit être conçu de manière

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

à minimiser les conséquences potentiellement dangereuses d'une perte d'indépendance causée, par exemple, par une panne systématique due à la conception, si elle peut exister.

Les différents types d'influence dans un système constitué, par exemple, de deux entités fonctionnelles sont illustrés à la Figure B.1. Il est permis d'étendre cette figure à des systèmes constitués de plus de deux entités fonctionnelles.

Lorsque la sécurité dépend des distances d'isolement ou des lignes de fuite, leurs valeurs minimales doivent être définies en cohérence avec les exigences de l'application (en intégrant les aspects matériels, la technologie, la réalisation, les conditions d'exploitation et d'environnement, les défaillances ainsi que les surtensions temporaires).

L'indépendance peut être perdue à cause de plusieurs types d'influences, comme expliqué dans les rubriques suivantes:

a) Type A Influences physiques internes

S'il n'existe aucune liaison physique entre des entités internes d'un système, il n'existe alors ni d'influence physique ni d'influence fonctionnelle. En conséquence, l'indépendance interne est assurée.

NOTE 1 Par liaison physique, on entend tout moyen de liaison entre des entités, par exemple:
– liaison galvanique;
– couplage électromagnétique.

Des mesures doivent être prises pour éviter toute influence physique interne involontaire.

NOTE 2 L'Article D.2 contient une liste de mesures permettant d'atteindre une indépendance physique interne (protection contre les influences de type A).

b) Type B Influences fonctionnelles internes

Une influence fonctionnelle entre des entités est basée sur une liaison physique. Des mesures doivent être prises pour éviter toute influence fonctionnelle interne. Cela doit être atteint en assurant une indépendance fonctionnelle interne (protection contre les influences de type B).

NOTE 3 Une influence fonctionnelle interne permettrait qu'une information erronée issue d'une entité soit susceptible d'influencer une autre entité d'une manière dangereuse.

c) Type C Influences physiques externes

Une influence physique externe peut avoir pour conséquence une perte d'indépendance physique entre entités.

NOTE 4 Ces influences peuvent être dues, par exemple, à:
– des contraintes d'environnement telles que les interférences électromagnétiques, les décharges électrostatiques, les conditions climatiques, mécaniques et chimiques,
– l'alimentation électrique,
– les entrées et les sorties externes.

Des mesures doivent être prises pour éviter toute influence physique externe involontaire. L'Article B.4 contient des exigences concernant les influences externes à prendre en compte.

NOTE 5 L'Article D.3 comprend une liste de mesures permettant d'atteindre l'indépendance physique externe (protection contre les influences de type C).

d) Type D Influences fonctionnelles externes

Une influence fonctionnelle externe peut avoir pour conséquence une perte d'indépendance fonctionnelle entre entités. Des mesures doivent être prises pour éviter toute influence fonctionnelle externe. Cela doit être atteint en assurant une indépendance fonctionnelle externe (protection contre les influences de type D).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

NOTE 6 Une influence fonctionnelle externe permettrait qu'une information erronée issue d'une source externe influence le système d'une manière dangereuse.

Légende:

= CONNEXION INTENTIONNELLE

= CONNEXION INVOLONTAIRE
(peut être causée par une panne)

= INDEPENDANCE
(si des mesures spécifiées sont mises en œuvre pour éviter des inductions involontaires et des connexions)

= CONTACT TRAVAIL
(contact normalement ouvert)

= CONTACT TRAVAIL DOUBLE
(utilisé symboliquement comme un ET pour deux activités non-restrictives indépendantes)

A = INFLUENCE PHYSIQUE INTERNE
(involontaire)

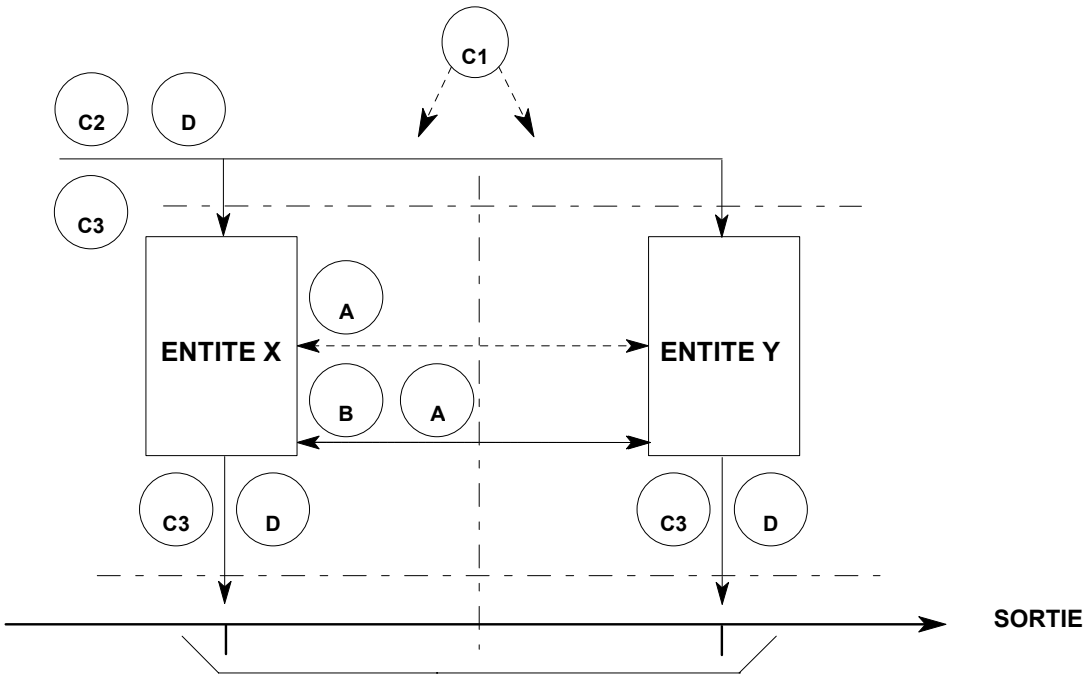
B = INFLUENCE FONCTIONNELLE INTERNE
(involontaire, utilisant une connexion intentionnelle)

C1 = INFLUENCE EXTERNE DUE A L'ENVIRONNEMENT (EMI, ...)
(involontaire)

C2 = INFLUENCE EXTERNE DUE A L'ALIMENTATION
(involontaire, utilisant une connexion intentionnelle)

C3 = INFLUENCE EXTERNE AU TRAVERS DES ENTREES/SORTIES
(TENSIONS DE FONCTIONNEMENT NORMALES, EMI-TENSIONS INDUITES)
(involontaire, utilisant une connexion intentionnelle)

D = INFLUENCE FONCTIONNELLE EXTERNE
(involontaire, utilisant une connexion externe)



IEC 1743/07

Figure B.1 – Influences affectant l'indépendance d'entités

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.3.3 Détection des pannes simples
(Voir également les informations du Tableau E.4)

Une première panne (panne simple) qui peut être dangereuse, soit seule soit combinée avec une seconde panne, doit être détectée et forcer le passage dans un état sûr (c'est-à-dire passivé) dans des délais suffisamment brefs pour atteindre l'objectif de sécurité quantifié spécifié. Une démonstration de cela doit être réalisée au moyen d'une combinaison d'une analyse des modes de défaillance et de leurs effets (AMDE) et d'une évaluation quantifiée de l'intégrité de défaillance aléatoire (voir Article A.3).

Dans le cas de la sécurité composite, cette exigence signifie qu'une première panne doit être détectée, et un état sûr forcé, dans des délais suffisamment brefs pour s'assurer que le risque d'occurrence d'une seconde panne durant la période de détection-passivation est plus petit que l'objectif de probabilité spécifié.

Dans le cas de la sécurité réactive, cette exigence signifie que le temps total maximal pris pour la détection-passivation ne doit pas excéder la limite spécifiée pour la durée d'une condition transitoire potentiellement dangereuse.

Ces exigences concernant la sécurité réactive et composite sont illustrées à la Figure B.2.

Les techniques utilisées pour obtenir une détection et une passivation de pannes identifiées dans des délais tolérables doivent être indiquées, y compris les calculs correspondants. Les sources des données fondamentales relatives aux taux de défaillance utilisées dans les calculs (par exemple taux de défaillance de composant matériel) doivent être identifiées, et la méthode de l'analyse quantitative clairement expliquée.

NOTE 1 Le temps de détection de panne est l'intervalle d'essai dans le cas d'une détection par l'équipement lui-même, ou l'intervalle de maintenance dans le cas de détection par le personnel. Dans le cas extrême, il s'agit de la durée de vie installée du système. Dans le cas d'un équipement en stockage, il s'agit de l'intervalle entre deux essais périodiques effectués par le personnel de maintenance.

NOTE 2 Un exemple d'une approche permettant le respect de ces exigences est fourni à l'Article D.4.

B.3.4 Action suivant la détection (incluant le maintien dans un état sûr)
(voir également les informations du Tableau E.4)

Après la détection d'une première panne, le système/sous-système/équipement doit passer dans un état sûr ou y rester. L'état sûr est généralement (mais non nécessairement) plus restrictif. L'état sûr doit être atteint dans un délai suffisamment bref pour que la période de détection-passivation respecte l'objectif de sécurité spécifié.

NOTE Le temps de passivation est communément le temps mis par la partie concernée du système à se mettre à l'arrêt, soit automatiquement, soit par action humaine.

Ces exigences sont illustrées à la Figure B.2.

Après détection d'une première panne, et une fois que l'état sûr a été atteint, des pannes ultérieures ne doivent pas supprimer l'état sûr. La suppression de l'état sûr restrictif ne doit se produire que d'une manière contrôlée, dans le cadre d'une procédure corrective.

Le système/sous-système/équipement doit rester dans un état sûr si des pannes ultérieures se produisent pendant les délais de réparation autorisés, suite à une première panne. Les délais de réparation autorisés doivent être suffisamment brefs pour permettre de respecter l'objectif de sécurité spécifié.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.3.5 Effets des pannes multiples

(Voir également les informations du Tableau E.4)

Une panne multiple (par exemple une double ou triple panne) qui peut présenter un danger, soit directement, soit combinée avec une panne ultérieure, doit être détectée et forcer le passage dans un état sûr (c'est-à-dire passivé) dans des délais suffisamment brefs pour atteindre l'objectif de sécurité spécifié. Une méthode appropriée, par exemple l'analyse par arbre des défauts (FTA), doit être utilisée pour démontrer les effets des pannes multiples. Les techniques utilisées pour obtenir une détection et passivation de pannes multiples dans un temps autorisé doivent être indiquées, y compris les calculs correspondants.

NOTE Un exemple d'une approche permettant le respect de ces exigences est fourni à l'Article D.5.

Une analyse de défaillance de mode commun (CCF) doit être réalisée, pour fournir l'assurance qu'une panne multiple ne peut arriver que par combinaison de pannes simples aléatoires, et non par le résultat d'une panne de mode commun.

B.3.6 Protections contre les pannes systématiques

Outre les techniques de gestion de la qualité et de la sécurité qui sont utilisées pour minimiser la probabilité d'occurrence d'une erreur humaine (voir 5.2 et 5.3), des mesures techniques doivent être prises de sorte que la présence d'une panne systématique dangereuse n'engendre pas, autant que raisonnablement réalisable, de risque inacceptable.

EXEMPLE L'architecture du système global peut être configurée de telle sorte que, même en cas d'occurrence d'une défaillance dangereuse du sous-système ou partie d'équipement conçu pour être sûr, la probabilité qu'un accident se produise reste faible.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

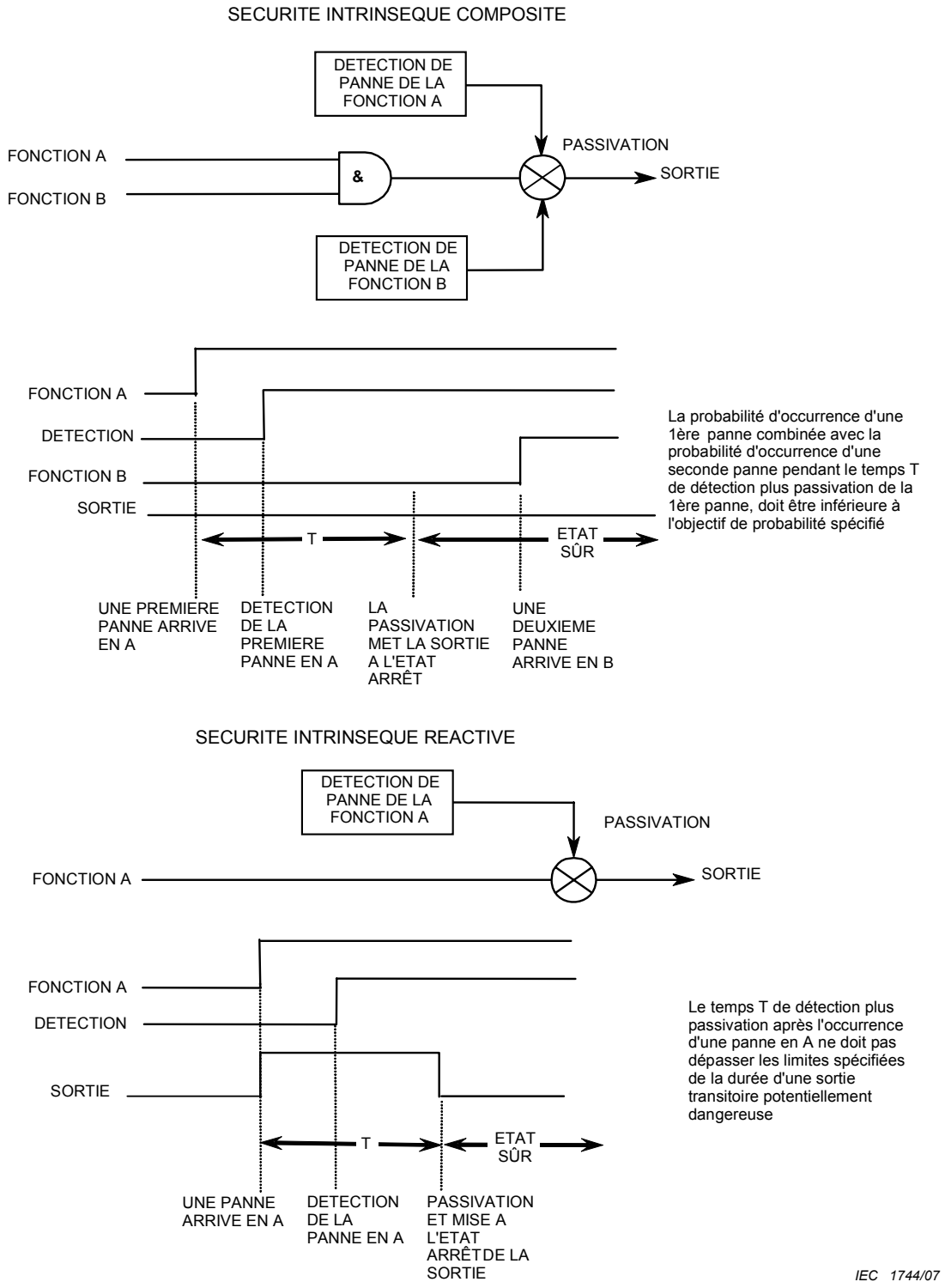


Figure B.2 – Détection et passivation de pannes simples

B.4 Exploitation en présence d'influences externes
(Partie 4 du rapport de sécurité technique)

Cette partie concerne l'aptitude d'un système/sous-système/équipement à fonctionner correctement et en toute sécurité, lorsqu'il est soumis à des influences externes spécifiées. Un "fonctionnement correct" comprend le respect des exigences fonctionnelles et de sécurité.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Autant que raisonnablement réalisable, il est recommandé de concevoir des systèmes relatifs à la sécurité pour qu'ils restent sûrs même lorsqu'ils sont soumis à des influences externes en dehors des limites spécifiées.

Les influences qui doivent être prises en compte sont énumérées de B.4.1 à B.4.7 ci-après. Les valeurs pour des conditions différentes énumérées dans l'EN 50125-1 et l'EN 50125-3 doivent être respectées.

Les conséquences du stockage et de l'acheminement doivent être prises en considération.

B.4.1 Conditions climatiques

On doit s'assurer que, dans des conditions d'environnement climatiques spécifiées, lesquelles doivent provenir de l'EN 50125-3, la sécurité soit atteinte conformément aux normes internationales en vigueur.

Si la société d'exploitation ferroviaire spécifie des conditions plus sévères que ce que l'équipement peut endurer, il est possible que le fournisseur, en accord avec le client, rajoute des mesures pour la climatisation.

B.4.2 Conditions mécaniques

On doit s'assurer que, dans des conditions d'environnement mécaniques spécifiées, la sécurité soit atteinte conformément aux normes internationales en vigueur.

B.4.3 Altitude

On doit s'assurer qu'à l'altitude réellement rencontrée, la sécurité soit atteinte conformément aux normes internationales en vigueur.

NOTE L'altitude à laquelle le système/sous-système/équipement doit fonctionner n'excède normalement pas 1 800 m au-dessus du niveau de la mer.

B.4.4 Conditions électriques (pas sur des véhicules)

On doit s'assurer que, dans des conditions d'environnement électriques spécifiées, la sécurité soit atteinte conformément aux normes internationales en vigueur.

NOTE Il est recommandé d'utiliser les valeurs indiquées dans la CEI 62236-4 et l'EN 50124-1 comme base de référence.

B.4.5 Conditions électriques (sur des véhicules)

On doit s'assurer que, dans des conditions d'environnement électriques spécifiées sur des véhicules, la sécurité soit atteinte conformément aux normes internationales en vigueur.

NOTE Il est recommandé d'utiliser les valeurs indiquées dans la CEI 62236, l'EN 50124-1 et l'EN 50155 comme base de référence.

B.4.6 Protection contre l'accès non autorisé

a) Définition des niveaux d'accès

Le niveau d'accès définit qui a droit d'accès, la raison de l'accès et la manière dont l'accès est effectué, assurant ainsi une protection contre l'accès non autorisé. Pour chacune des opérations particulières mentionnées ci-dessous, le personnel réalisant ces fonctions devra remplir un certain nombre de critères qui doivent être définis en termes de:

– domaine de compétence,

– niveau de compétence,

– formation à des équipements spécifiques.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

b) Protection

En considérant les niveaux d'accès ci-dessus, le présent paragraphe doit définir la manière dont la protection doit être atteinte.

Il est recommandé que les mesures de protection interdisent l'accès

– accidentel, par des membres autorisés du personnel,

– volontaire, par des membres non autorisés du personnel.

c) Conditions externes

Ce point doit décrire la manière dont la protection est assurée par des moyens en complément des équipements proprement dits.

EXEMPLE – enceinte;

– sécurité;

– accessibilité.

d) Encapsulation

Ce point doit décrire la manière dont la protection est assurée par l'équipement réel.

EXEMPLE – couvercles;

– montage;

– joints d'étanchéité;

– codage électrique;

– codage mécanique;

– microprogramme.

B.4.7 Conditions plus sévères

Des dispositions doivent être prises pour traiter des conditions supplémentaires plus sévères, spécifiées par la société d'exploitation ferroviaire, lorsque cela est nécessaire.

NOTE La liste suivante concerne des exemples de conditions plus sévères:

– condensation due à une variation rapide des températures ambiantes de l'équipement;

– pollution sévère de l'air à cause de
  - la poussière;
  - la fumée;
  - la vapeur;
  - les produits chimiques corrosifs;
  - le sel;
  - le sulfate d'hydrogène.

Il est recommandé de définir les types de polluants et leur concentration dans la spécification:

– pour des équipements extérieurs:
  - la gelée;
  - des variations rapides de températures;

– des influences chimiques telles que:
  - du pétrole ou dérivés;
  - des éléments organiques;
  - des désherbants;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– une chaleur excessive provenant, par exemple, du feu ou du rayonnement solaire;

– une action/présence de végétation, d'insectes ou d'animaux;

– une accumulation de poussière et de saleté (conductrice ou non);

– des limites de températures plus extrêmes dans certains pays.

B.5 Conditions d'utilisation relatives à la sécurité (Partie 5 du rapport de sécurité technique)

Cette partie doit définir les règles, conditions et contraintes associées à la sécurité fonctionnelle à observer lors de l'utilisation du système/sous-système/équipement.

Des points généraux doivent être pris en compte, y compris:

– la configuration de systèmes programmables afin de les adapter à des applications spécifiques;
– les précautions à prendre lors de la fabrication, l'installation, les essais et la mise en état de fonctionnement;
– les règles et méthodes pour la maintenance et la recherche de pannes;
– les consignes d'exploitation du système;
– les alarmes de sécurité et précautions;
– les précautions de compatibilité électromagnétique (CEM) (susceptibilité et émission);
– les informations concernant les évolutions et le retrait du service éventuel;
– une justification de la sécurité des outils et équipements de soutien, tels qu'un équipement d'essai, de maintenance et des outils de configuration.

Des points spécifiques énumérés de B.5.1 à B.5.3 ci-après doivent être pris en compte.

B.5.1 Configuration d'un sous-système/équipement et construction du système

a) Configuration

Si un sous-système ou équipement est tel qu'il doit être configuré pour chaque application particulière, alors tout outil et/ou toute procédure de configuration doi(ven)t être défini(e)(s).

EXEMPLE
– procédures;
– contrôle de la version;
– exigences matérielles du système de configuration;
– détails logiciels du système de configuration;
– maintenance du logiciel;
– vérification et validation;
– simulation.

b) Construction du système

La présente documentation doit détailler la manière dont les sous-systèmes et équipements sont construits pour obtenir un système de signalisation particulier.

EXEMPLE
– réglages de contrôle de la version;
– réglages de contrôle de l'application;
– réglages d'interfaces;
– réglages d'initialisation;
– réglages de commande de maintenance;
– essais de fabrication et de production;
– procédures d'essais du système;
– installation, essais et mise en état de fonctionnement.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

c) Changement de fonctionnalité

Si la conception d'un sous-système ou équipement est suffisamment générique pour lui permettre d'être utilisé dans des systèmes pour diverses applications, la manière dont il est configuré et mis au point pour répondre à ces différentes applications doit également être documentée. Toute limitation ou condition pour garantir une utilisation sûre doit être complètement spécifiée.

B.5.2 Exploitation et maintenance

La maintenance minimale nécessaire pour assurer une exploitation sûre, continue et correcte du système/sous-système/équipement dans des conditions d'environnement spécifiées doit être documentée sous la forme d'un plan de maintenance et d'exploitation, qui doit comprendre les points suivants:

a) état d'exploitation

Les conditions présentes dans chaque système/sous-système/équipement doivent être définies pour permettre au personnel de maintenance et d'exploitation une compréhension suffisante lors des situations suivantes:

1) démarrage

Ce point doit décrire les conditions de démarrage du système, sous-système ou équipement lorsque l'alimentation est établie, ou suite à un arrêt dû à une coupure d'alimentation ou d'autres causes.

NOTE Il est recommandé de définir, par exemple:

– des conditions implicites,

– une période d'initialisation,

– des autotests réalisés,

– une intervention manuelle requise,

– des conditions de sortie,

– des précautions après un événement exceptionnel, tel que le feu ou une entrée non autorisée.

2) fonctionnement normal

Une fois que le système/sous-système/équipement a achevé l'initialisation avec succès, les conditions lors du fonctionnement normal doivent être définies.

EXEMPLE – temps de cycle;

– procédures sans données;

– traitement des pannes.

3) commutation

Si l'équipement, ou le système/sous-système dans lequel il est configuré, dispose d'une fonction de commutation lui permettant de passer à un système/sous-système en réserve chaude ou froide, les conditions définies en a) et b) doivent alors être rétablies pour ce programme de commutation. La réaction de l'équipement au remplacement de modules défaillants doit également être clairement définie.

4) mise à l'arrêt

Quand un système, sous-système ou équipement est mis à l'arrêt volontairement pour un changement de configuration ou un retrait du service, ou involontairement suite à une défaillance d'alimentation, toutes les conditions applicables doivent alors être définies.

EXEMPLE – des conditions implicites;

– des conditions relatives à une dégradation progressive;

– des points de sécurité;

– des procédures;

– des influences envers d'autres systèmes connectés.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

b) niveaux de maintenance

Ceux-ci doivent être définis en termes de

– maintenance de premier ordre,
– maintenance de deuxième ordre, par le client,
– maintenance de deuxième ordre, par le fabricant.

NOTE 1 La maintenance de premier ordre représente la maintenance préventive et la recherche de panne/réparation menées sur le site, alors que la maintenance de deuxième ordre représente la maintenance préventive et la possible réparation réalisées en atelier hors site.

c) maintenance périodique

Pour décrire la maintenance périodique exigée, tous les domaines concernés doivent être référencés.

EXEMPLE
– formation;
– accessibilité;
– modularité;
– interchangeabilité;
– approvisionnement de pièces de rechange;
– stockage des pièces de rechange.

d) aide à la maintenance

Pour chaque niveau de maintenance, l'aide à la maintenance disponible pour le personnel doit être définie.

NOTE 2 Il est recommandé que ces moyens comprennent, par exemple

– des diagnostics de panne,

– une interprétation des messages de panne,

– une correction des pannes.

B.5.3 Surveillance de la sécurité d'exploitation

Au cours de la phase d'exploitation et de maintenance du cycle de vie du système, les performances du système/sous-système/équipement doivent être surveillées pour s'assurer que les fonctions particulières incorporées dans la conception et les hypothèses avancées lors de l'évaluation initiale de la sécurité restent valables pour les conditions réelles rencontrées pendant le service.

NOTE Il est recommandé d'inclure, par exemple,

– la surveillance des performances relatives à la sécurité et la comparaison avec les performances prévues,
– la surveillance et l'évaluation des rapports de défaillance, dans le but de détecter les tendances aux défaillances ou d'éventuelles défaillances dangereuses qui peuvent être corrigées, permettant ainsi d'améliorer la sécurité et la fiabilité,
– l'investigation des rapports d'incident et d'accident pour identifier toute modification requise pour améliorer les performances du système en matière de sécurité.

B.5.4 Retrait du service et dépose

Les précautions et procédures concernant la sécurité technique nécessaires quand le système/sous-système/équipement est par la suite retiré du service doivent être documentées. Cela doit inclure une prise en compte d'une introduction phasée éventuelle de systèmes de remplacement pendant que le système ferroviaire continue à fonctionner.

Des avertissements et instructions appropriés concernant la dépose finale de l'équipement après retrait du service doivent être également inclus.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

B.6 Essais de qualification de la sécurité
(Partie 6 du rapport de sécurité technique)

Cette partie doit contenir la preuve que les essais de qualification de la sécurité dans des conditions opérationnelles ont été complètement menés avec succès.

L'objectif de ces essais est

– d'obtenir une confiance accrue dans le fait que le système/sous-système/équipement respecte ses exigences d'exploitation spécifiées,
– d'obtenir une confiance accrue dans le fait que les objectifs de fiabilité et de sécurité spécifiés ont été atteints,
– de permettre aux systèmes/sous-systèmes/équipements de passer en service d'exploitation avant l'approbation finale de la sécurité, moyennant la fourniture de précautions appropriées et d'une surveillance.

NOTE Ces essais permettent seulement une confiance accrue et ne sont pas le seul moyen pour démontrer la sécurité.

B.6.1 Exigences

L'extension et la durée des essais de qualification de la sécurité doivent faire l'objet d'un accord entre la société d'exploitation ferroviaire et l'autorité de tutelle, et doivent être justifiées en considérant le degré d'innovation et de complexité associé au système/sous-système/équipement.

Du fait que la finalisation des essais de qualification de la sécurité est comprise dans le dossier de sécurité, la sécurité du système n'est pas complètement assurée lors de la période d'essai. En conséquence, des précautions, procédures et surveillances adéquates doivent être fournies, pour assurer la sécurité du système ferroviaire lors de la période d'essai.

Les essais de qualification de la sécurité, tels que définis, doivent être finalisés avant le commencement de l'exploitation avec une responsabilité totale de la sécurité.

Un enregistrement doit être établi pour expliquer que le système est mis en service, avec ou sans passagers, avec ou sans précautions, et ce que vaut le niveau d'autorisation obtenu à chaque phase (provisoire ou approbation finale de la sécurité).

B.6.2 Résultats

Un compte rendu des essais de qualification de la sécurité, y compris une description complète des essais menés et des résultats obtenus, doit être documenté dans la présente partie du rapport de sécurité technique.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe C
(normative)

Identification des modes de défaillance des composants matériels

C.1 Introduction

La présente annexe contient les procédures et informations nécessaires à l'identification des modes de défaillance possibles des composants matériels.

NOTE Les tableaux des modes de défaillance des composants matériels inclus dans la présente annexe ont été établis à partir de l'expérience internationale ainsi que des sources suivantes, reprises dans la Bibliographie:

– Rapport A155/RP12 UIC/ORE;

– MIL-HDBK-338-1A;

– MÜ 8004 des Chemins de Fer Fédéraux Allemands;

– Rapport du Centre d'Analyse de la Fiabilité FMD-91.

Les informations données dans les tableaux peuvent être modifiées, comme expliqué aux Articles C.2 et C.5, si des justifications adéquates sont fournies pour de telles variations.

C.2 Procédure générale

Pour réaliser l'analyse des conséquences des pannes simples (voir B.3.1), il est nécessaire d'identifier les modes de défaillance vraisemblables de chaque composant matériel.

Les Tableaux C.1 à C.16 contiennent la liste des modes de défaillance des composants matériels qui doit être utilisée comme base pour la conception et l'analyse, à moins que des justifications ne soient fournies pour toute variation. Les notes générales de l'Article C.5 doivent être prises en compte.

Ces listes ne sont pas nécessairement complètes, et tous les modes de défaillance additionnels considérés comme vraisemblables doivent être ajoutés à l'analyse. Dans ce cas, les modes de défaillance supplémentaires doivent être portés à l'attention de l'autorité compétente, de telle façon que la liste soit complétée à une date ultérieure par le moyen de la procédure normale du CENELEC.

C.3 Procédure pour les circuits intégrés (incluant les microprocesseurs)

Les conceptions qui emploient des circuits intégrés exigent un traitement spécial puisqu'il peut être difficile de prédire tous les modes de défaillance vraisemblables de tels composants. Cela est particulièrement vrai pour les composants programmables, puisque les modes de défaillance qui peuvent être observés aux bornes du composant sont spécifiques à l'application.

Il est recommandé que les modes de défaillance dangereux soient identifiés par une analyse "descendante" pour les applications spécifiques par l'utilisation d'une technique telle que l'analyse par arbre des défauts. (Une alternative pourrait être d'utiliser une approche "ascendante", telle que l'analyse des modes de défaillance et de leurs effets, mais cette méthode est coûteuse en temps et il est possible que certains modes de défaillance dangereux puissent être oubliés).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

L'évaluation et les justifications doivent être fournies afin de démontrer que, pour chaque mode de défaillance dangereux identifié,

soit a) ce mode de défaillance ne peut raisonnablement survenir, grâce à l'architecture interne du logiciel ou à la structure des données,

soit b) ce mode de défaillance sera détecté extérieurement et un état sûr sera imposé dans le temps requis. Dans ce cas, une analyse quantitative doit être réalisée pour justifier la conception, et un point de vue pessimiste doit être pris partout où les modes de défaillance dangereux sont avérés en prenant pour taux de défaillance celui du composant en entier.

NOTE Quelques composants, tels que les capteurs "intelligents", utilisent des microprocesseurs intégrés. Il est recommandé que de tels composants soient validés en utilisant les mêmes méthodes que celles décrites ci-dessus pour les circuits intégrés.

C.4 Procédure pour les composants avec propriétés physiques intrinsèques

Si la technique de la sécurité intrinsèque est utilisée (voir B.3.1), une justification complète doit être fournie pour chacun des modes de défaillance considérés comme invraisemblables. Cette justification doit inclure mais non nécessairement se limiter aux points suivants:

– explication théorique des propriétés physiques intrinsèques;
– preuve de la conformité à des normes qualité reconnues;
– explication de la construction spéciale des composants;
– explication des arrangements spéciaux et autres précautions pour le montage du composant;
– preuve que le mode de défaillance ne peut survenir lors du dépassement des taux de charge du composant (par exemple à cause d'une panne ou pour des conditions de surcharge);
– résultats d'essais démontrant le comportement "sécurité intrinsèque" du composant dans des conditions défavorables (au moyen d'essais physiques, de justifications techniques ou par simulation);
– preuve de l'expérience antérieure démontrant la confiance du composant pour la sécurité intrinsèque.

Si les justifications satisfaisantes sont fournies, les modes de défaillance du composant correspondants peuvent être exclus de l'analyse de sécurité.

Il n'est pas nécessaire de répéter la justification si elle a déjà été fournie dans le passé; il suffit de faire référence au rapport de justification antérieur. Cependant, si la justification inclut des conditions particulières (par exemple arrangements de montage spéciaux ou moyens pour éviter les surcharges), ces conditions doivent être incluses dans le dossier de sécurité et doivent être respectées.

L'expérience antérieure montre que la justification comme invraisemblable est plus probable pour certains modes de défaillance particuliers des composants; ces modes de défaillance sont indiqués par (*) dans les Tableaux C.1 à C.16, avec une référence aux notes d'explication des Articles C.6 et C.7. La justification comme invraisemblable des autres modes de défaillance non repérés par (*) est considérée comme beaucoup moins probable. Il est à noter que les justifications de tous les modes de défaillance considérés comme invraisemblables doivent être fournies, y compris pour ceux indiqués dans les tableaux.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

C.5 Remarques générales concernant les modes de défaillance des composants

1) Les Tableaux C.1 à C.16 contiennent la liste des modes de défaillance des composants matériels considérés comme vraisemblables.

2) Les modes de défaillance sont ceux qui se manifestent aux bornes des composants et non les causes physiques internes des défaillances.

3) Tous les modes de défaillance listés peuvent être intermittents.

4) Les défaillances intermittentes peuvent être causées par les influences de l'environnement telles que les variations de température ou les contraintes mécaniques (voir les normes d'environnement correspondantes). Par conséquent, la fréquence des défaillances intermittentes sera en rapport avec ces causes.

5) Les variations de tolérances précisées dans les publications de spécifications composants ne sont pas considérées comme des défaillances.

6) Il est supposé que les composants opèrent dans les limites environnementales spécifiées dans les publications.

7) Il est supposé que les composants opèrent sous des taux de charge électriques spécifiés dans les publications.

8) Les courts-circuits externes ou les fuites entre les connexions d'un composant ne sont pas considérés comme défaillances du composant. Pour les distances d'isolement et les lignes de fuite appropriées, se référer au point 10).

9) Les courts-circuits externes ou fuites entre différents composants ne sont pas considérés comme défaillances du composant. Pour les distances d'isolement et les lignes de fuite appropriées, se référer au point 10). Un montage stable et/ou une fixation spéciale sont nécessaires si les conditions d'environnement peuvent changer la position du composant.

10) Lorsque la sécurité dépend des distances d'isolement et des lignes de fuite, leurs valeurs minimales doivent être définies en cohérence avec les exigences de l'application (en intégrant les aspects matériels, la technologie, la réalisation, les conditions d'exploitation et d'environnement, les conditions de défaillance ainsi que les surtensions temporaires). Les normes EN 50124-1 ou CEI 60664 doivent être utilisées pour déterminer les exigences minimales basées sur l'isolation renforcée. Ces exigences doivent être acceptées ou davantage renforcées ou complétées par la société d'exploitation ferroviaire.

C.6 Notes générales additionnelles concernant les composants avec propriétés physiques intrinsèques

1) La procédure et les conditions nécessaires à la justification de chacun des modes de défaillance considérés comme invraisemblables sont précisées à l'Article C.4.

2) Les modes de défaillance repérés par (*) dans les Tableaux C.1 à C.16 sont ceux dont la justification comme invraisemblable est la plus probable.

3) Les "Notes xy" qui suivent l'astérisque (*) dans les Tableaux C.1 à C.16 font référence aux notes explicatives de l'Article C.7 sur quelques facteurs pertinents pour une possible justification des modes de défaillance considérés comme invraisemblables.

4) Les notes générales de l'Article C.5 s'appliquent aussi aux composants ayant des propriétés physiques intrinsèques, complétées par les points additionnels 5), 6) et 7) ci-dessous.

5) En complément du point 5) de l'Article C.5, il est recommandé de tenir compte de toute variation qui excède les tolérances normales.

6) En complément du point 6) de l'Article C.5, il est recommandé de tenir compte des excursions au-delà des limites normales de l'environnement.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

7) En complément du point 7) de l'Article C.5, une marge doit être prise par rapport aux taux de charge électriques spécifiés dans les publications, de telle façon que le composant soit protégé des surcharges.

8) Pas utilisée.

9) Pas utilisée.

C.7 Notes spécifiques concernant les composants avec propriétés physiques intrinsèques

Les notes ci-après donnent des conseils sur les justifications possibles des modes de défaillance repérés par (*) dans les Tableaux C.1 à C.16 comme étant invraisemblables.

10) Le corps du composant ne doit pas avoir de trou.

La résistance doit être limitée à la valeur la plus faible possible (par exemple, pas supérieure à 10 kΩ).

Les distances d'isolement et les lignes de fuite entre les fils de connexion à chaque extrémité du composant doivent au moins remplir les exigences de l'EN 50124-1, conformément aux exigences de l'isolation renforcée.

Le composant doit être revêtu de ciment ou d'émail. Dans d'autres cas, le revêtement ne doit pas être conducteur, même à la plus haute température (en incluant les conditions de panne).

Le corps du composant doit être réalisé en matériau non conducteur, même à la plus haute température (en incluant les conditions de panne).

Lignes directrices supplémentaires pour une résistance à couche bobinée:

L'enroulement d'une résistance à couche bobinée ne doit comporter qu'une seule couche.

Le court-circuit entre spires d'une résistance à couche bobinée doit être évité en recouvrant le fil, et/ou en séparant physiquement les spires.

11) Les résistances à quatre connexions doivent être conçues de manière telle que si une panne cause l'interruption du matériau résistif, cette panne causera aussi l'interruption d'au moins une des quatre connexions de sortie.

Les circuits extérieurs à la résistance doivent détecter l'interruption d'une ou de plusieurs connexions de manière sûre.

Exemple de résistance à quatre connexions utilisant une technique hybride couche épaisse (voir Figure C.1):

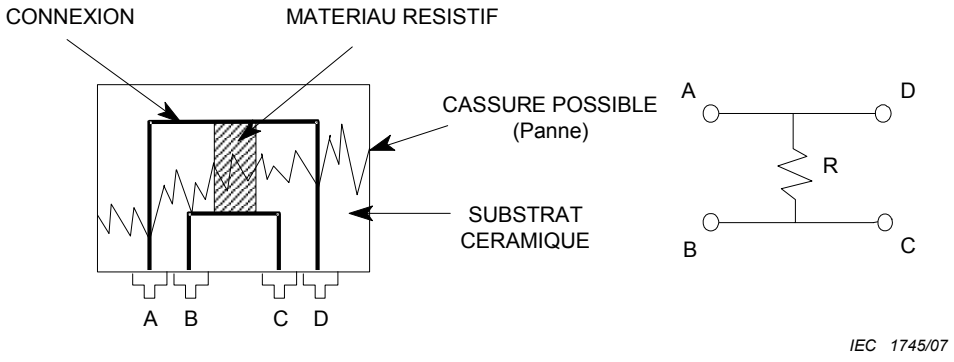


Figure C.1 – Exemple de résistance à quatre connexions utilisant une technique hybride couche épaisse

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

12) Deux bornes doivent être connectées indépendamment de chaque côté du composant.

13) La formule pour calculer la capacité d'un condensateur à simples plaques parallèles est la suivante:

$$C = \varepsilon_0 \cdot \varepsilon_r \cdot \frac{A}{d}$$

où

A est la surface commune des plaques;

d est la distance entre plaques;

ε_0 est la permittivité du vide;

ε_r est la permittivité relative (constante diélectrique).

La justification du mode de défaillance considéré comme invraisemblable exige la démonstration qu'aucun de ces paramètres ne peut changer de manière significative.

Les condensateurs électrolytiques ne peuvent prétendre à l'exclusion de ce mode de défaillance.

14) Pour les applications haute tension, les condensateurs doivent être conçus et réalisés en fonction de la tension de fonctionnement la plus élevée possible (en incluant les conditions de panne). Ces condensateurs doivent être spécifiés classe Y, et avoir des propriétés d'auto-cicatrisation à l'impédance de travail et au-delà de l'étendue de la tension de travail.

15) Il ne doit y avoir qu'une seule couche de spires, séparées par des rainures dans la carcasse isolée, ou le fil doit avoir une isolation renforcée.

Les spires doivent être fixées d'une manière sûre.

16) Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

Tous les enroulements et les connexions doivent être fixés d'une manière sûre.

La puissance dissipée doit être suffisamment limitée afin d'éviter la carbonisation interne (en incluant les conditions de panne).

17) Le circuit magnétique doit être réalisé de telle manière qu'aucun changement significatif de la réluctance du "chemin des lignes de champ magnétique" ne puisse advenir.

18) Le rapport de transfert dépend du nombre de spires de chaque enroulement et de l'intégrité du couplage du circuit magnétique. Par conséquent, il est nécessaire que les points 15), 16) et 17) soient respectés.

19) La transductance, ainsi que le seuil de tension du courant continu, dépendent des propriétés du noyau magnétique. Par conséquent, il est nécessaire de démontrer que ces propriétés magnétiques ne peuvent changer significativement.

La transductance ainsi que le seuil de tension du courant continu dépendent aussi du nombre de spires de chaque enroulement et de l'intégrité du couplage magnétique. Par conséquent, il est également nécessaire que les points 15), 16) et 17) soient respectés.

La valeur de la sortie du transducteur est fonction du nombre d'ampères-tours de l'enroulement de commande. Il est nécessaire de démontrer qu'en association avec le circuit électronique de pilotage, aucun mode de défaillance vraisemblable de l'enroulement de commande ne peut causer l'augmentation du nombre d'ampères-tours.

20) Toutes les parties du relais ou du mécanisme de commutation doivent être construites de manière robuste et être fixées de manière sûre, en incluant

– le mécanisme de travail,

– le système de contacts,

– le ou les circuits magnétiques (s'il y en a),

– la ou les bobines (s'il y en a).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

21) Les matériaux des contacts doivent être choisis de telle sorte qu'ils ne puissent être soudables.

Les risques de soudage doivent être ultérieurement réduits par une conception mécanique et une réalisation des contacts appropriées.

La valeur maximale du courant traversant les contacts doit être limitée, afin de s'assurer que la température de ces derniers n'atteigne pas celle de leur soudure.

22) La stabilité des caractéristiques du relais doit être assurée en prenant en compte les facteurs suivants:

- caractéristiques magnétiques:
  - choix du matériau magnétique;
  - mise en œuvre d'un dispositif d'arrêt pour éviter la magnétisation permanente du circuit magnétique (noyau);
  - protection contre les champs magnétiques externes;
- caractéristiques électriques:
  - choix et qualité du fil et de son isolant;
  - qualité de l'enroulement de la bobine;
  - qualité de la réalisation des sorties;
- caractéristiques mécaniques:
  - choix et qualité des matériaux;
  - fixation sûre de toutes les parties;
  - tenue sûre dans le temps de tous les réglages relatifs à la sécurité;
  - mise à disposition d'une force de rappel adéquate
    - utilisant la gravité (complétée, si nécessaire, par des ressorts et/ou par une lame élastique);
    - utilisant des ressorts (et/ou une lame élastique), conçus de manière appropriée;
  - conception et réalisation du mécanisme de travail de telle façon qu'il ne puisse pas se bloquer.

23) La tension de seuil d'une jonction p-n, telle que celle d'une diode ou la jonction base-émetteur d'un transistor, est fonction

- de la densité des porteurs de charges majoritaires et des porteurs de charges minoritaires,
- de la constante de Boltzmann (k),
- de la charge de l'électron (e),
- de la température (K).

En conséquence, la tension de seuil d'une jonction p-n est dépendante de caractéristiques non variables, et il convient de la considérer comme constante pour une température donnée.

24) La tension de claquage est déterminée par l'un des deux mécanismes possibles suivants: claquage par effet Zener ou claquage par avalanche. Les deux dépendent de caractéristiques physiques non variables de la diode; il convient donc de considérer la tension de claquage comme constante pour une température donnée.

On doit veiller à éviter l'usage de composants comportant intérieurement deux ou plusieurs diodes en série connectées ensemble.

Il est à noter que la conduction à une tension supérieure ou inférieure à la tension de claquage est possible, en raison de la présence de résistances parallèles ou série mais que, dans ce cas, la résistance différentielle (de rampe) est plus grande que lors de la conduction en claquage.

25) L'amplification (ou le gain ou la transconductance) d'un transistor et la sensibilité optique d'une photodiode ou d'un phototransistor, dépendent

- des niveaux de dopage,
- de l'épaisseur des jonctions,

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– de la durée de vie des porteurs de charges.

Il convient de considérer ces paramètres comme constants, à l'exception de la durée de vie des porteurs de charges, qui ne peut que décroître dans le temps. En conséquence, il convient de considérer que l'amplification ou la sensibilité optique sont constantes ou peuvent décroître, mais elles ne peuvent augmenter (à justifier pour chaque application).

Il existe une faible possibilité d'augmentation de l'amplification causée par la pollution venant affecter le dopage en surface. Cela peut être évité par une haute qualité de réalisation et de mise en boîtier du composant. Par ailleurs, cet effet n'est significatif que pour les très faibles valeurs du courant de distorsion, ce qui doit donc être évité lors de la conception des circuits électroniques.

26) L'émission de lumière est une propriété physique relative à la recombinaison des électrons et des trous quand le courant circule au travers d'une jonction p-n polarisée en direct.

Le taux de recombinaison est fonction du courant direct et, par conséquent, il convient que la lumière émise n'augmente pas à courant constant.

En dessous de la tension de seuil, aucun courant significatif ne circule et, par conséquent, aucune lumière n'est émise.

27) Si une jonction p-n est polarisée en sens inverse, aucun courant significatif ne circule en dessous de la tension de claquage et, par conséquent, aucune lumière n'est émise.

Au-dessus de la tension de claquage, le mécanisme qui permet au courant de circuler est différent de celui qui permet son passage en direct, et il convient qu'aucune émission de lumière n'en résulte.

28) Pour les optocoupleurs et les systèmes comportant une fibre optique, les modes de défaillance de chacun des éléments doivent être considérés, c'est-à-dire

– l'émetteur de lumière,

– le support optique,

– le récepteur photosensible.

29) Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

La construction des composants doit être robuste et stable.

La puissance dissipée dans le composant doit être suffisamment limitée afin d'éviter la carbonisation interne (en incluant les conditions de panne).

30) Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

Les éléments de couplage/pilotage des entrées et des sorties doivent être fixés d'une manière sûre.

31) Le composant doit être construit de manière robuste.

Le ou les résonateurs doivent être construits et montés afin d'éviter tout changement de leurs dimensions effectives.

Le ou les résonateurs doivent être construits avec un matériau dont les dimensions ne changent pas de manière significative avec la température.

Le matériau du ou des résonateurs doit être stabilisé par une opération préliminaire et/ou un cycle en température pendant un temps suffisant.

Le matériau du ou des résonateurs ne doit pas être surchargé, même dans les conditions de panne. En particulier, les limites d'élasticité ne doivent pas être dépassées.

32) Le rapport de transfert est fonction de l'efficacité des éléments de pilotage/couplage et du facteur Q du filtre.

Les éléments de pilotage/couplage doivent être conçus et réalisés de telle manière que leur efficacité ne puisse augmenter significativement.

33) Le ou les résonateurs doivent être construits et montés afin d'obtenir le facteur Q le plus élevé possible, de telle manière qu'aucune augmentation ne puisse survenir.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

34) Le ou les résonateurs doivent être construits et montés afin d'éviter l'apparition de tout amortissement par un mécanisme quelconque.

35) Le matériau d'isolation doit être stable.

Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

36) Le connecteur doit être construit de manière robuste.

Toutes les parties du connecteur doivent être fixées de manière sûre.

37) Le positionnement incorrect du connecteur ou son insertion dans une embase erronée doivent être évités au moyen, par exemple, de la conception mécanique ou du codage mécanique.

D'une manière alternative, les effets d'une insertion incorrecte doivent être rendus non dangereux au moyen, par exemple, du codage électrique des broches du connecteur ou de l'allocation d'adresses/identités uniques.

Les risques doivent être réduits davantage au moyen d'étiquettes d'avertissement et par une formation du personnel.

38) Les écrans doivent être construits de manière robuste et protégés de dommages physiques excessifs.

La connexion électrique de l'écran doit être robuste et fixée d'une manière sûre.

39) Une isolation suffisamment robuste doit être assurée.

Les distances d'isolement et les lignes de fuite doivent répondre au moins aux exigences concernant le renforcement de l'isolation de l'EN 50124-1.

Une protection contre les dommages physiques excessifs doit être réalisée.

Une protection contre les corps étrangers conducteurs de l'électricité doit être réalisée.

40) Le fusible et son support doivent être physiquement construits et montés de manière à éviter l'occurrence d'un court-circuit parallèle.

Des moyens doivent être mis en œuvre afin d'éviter l'utilisation d'un fusible de calibre incorrect.

Des moyens doivent être mis en œuvre afin d'éviter l'utilisation d'un fusible ayant des capacités d'autorégénération ou de réinitialisation.

Tableau C.1 – Résistances

a) Toutes sortes de résistances et de résistances ajustables (à l'exclusion des résistances à 4 connexions)	
Coupure	
Court-circuit	(*) point 10
Augmentation de la valeur de la résistance	
Diminution de la valeur de la résistance	(*) point 10
Court-circuit au boîtier	
b) Résistances à quatre connexions	
Coupure de chaque connexion	
Coupure du matériau résistif	(*) point 11
Court-circuit	(*) point 10
Augmentation de la valeur de la résistance de chaque connexion	
Diminution de la valeur de la résistance	(*) point 10
Court-circuit entre deux connexions du même côté	(*) point 12
Court-circuit au boîtier	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.2 – Condensateurs

a) Toutes sortes de condensateurs et condensateurs ajustables (à l'exclusion des condensateurs à 4 connexions)	
Coupure	
Court-circuit	(*) point 14
Augmentation de la capacité	(*) point 13
Diminution de la capacité	(*) point 13
Diminution de la résistance parallèle	(*) point 14
Augmentation de la résistance série	
Court-circuit au boîtier	
b) Condensateur à quatre connexions	
Coupure de chaque connexion	
Court-circuit	
Augmentation de la capacité	(*) point 13
Diminution de la capacité	(*) point 13
Diminution de la résistance parallèle	(*) point 14
Augmentation de la résistance série	
Court-circuit entre deux connexions du même côté	(*) point 12
Court-circuit au boîtier	

Tableau C.3 – Composants électromagnétiques

a) Inductance	
Coupure de l'enroulement	
Court-circuit de l'enroulement	
– entre spires	(*) point 15
– entre couches	(*) point 16
– de tout l'enroulement	(*) point 16
Court-circuit ou diminution de l'isolement entre l'enroulement et le circuit magnétique	(*) point 16
Augmentation de la résistance de l'enroulement	
Augmentation de l'inductance	(*) point 17
Diminution de l'inductance	(*) point 17
b) Transformateur	
Coupure de chacun des enroulements	
Court-circuit de chacun des enroulements	
– entre spires	(*) point 15
– entre couches	(*) point 16
– de tout l'enroulement	(*) point 16
Court-circuit ou diminution de l'isolement – entre enroulements	(*) point 16
Court-circuit ou diminution de l'isolement – entre chacun des enroulements et le circuit magnétique	(*) point 16
Augmentation de la résistance de chacun des enroulements	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.3 *(suite)*

Augmentation de l'inductance de chacun des enroulements	(*) point 17
Diminution de l'inductance de chacun des enroulements	(*) point 17
Changement du rapport de transformation	(*) point 18
c) Transducteur (réacteur saturable ou amplificateur magnétique)	
Coupure de chacun des enroulements	
Court-circuit de l'enroulement c.c.	
Court-circuit de l'enroulement c.a.	
– entre spires	(*) point 15
– entre couches	(*) point 16
– de tout l'enroulement	(*) point 16
Court-circuit ou diminution de la résistance d'isolement	
– entre les enroulements c.c. et c.a.	(*) point 16
– entre chacun des enroulements et le circuit magnétique	(*) point 16
Augmentation de l'inductance de l'enroulement c.a.	(*) point 17
Diminution de l'inductance de l'enroulement c.a.	(*) point 17
Augmentation de la transductance	(*) point 19
Diminution de la transductance	
Augmentation de la valeur continue (c.c.) de la tension de seuil	
Diminution de la valeur continue (c.c.) de la tension de seuil	(*) point 19
d) Relais	
Coupure de chacune des bobines	
Coupure de chacun des contacts	
Court-circuit ou diminution de la résistance d'isolement	
– à travers les contacts ouverts	(*) point 20
– entre bobines	(*) point 16
– entre bobine et contact	(*) point 20
– entre bobine et boîtier	(*) point 16
– entre contacts	(*) point 20
– entre contact et boîtier	(*) point 20
Soudage des contacts	(*) point 21
Augmentation de la résistance des contacts	
Augmentation du temps de rebondissement de contact	
Augmentation du courant d'attraction	
Diminution du courant d'attraction	(*) point 22
Augmentation du courant de chute	
Diminution du courant de chute	(*) point 22
Changement du rapport courant d'attraction/courant de chute	(*) point 22
Augmentation du temps d'attraction	
Diminution du temps d'attraction	(*) point 22
Augmentation du temps de chute	(*) point 22
Diminution du temps de chute	(*) point 22
Le relais ne monte pas	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.3 *(suite)*

Le relais ne chute pas	(*) point 22
Fermeture des contacts travail et contacts repos (transitoire ou continue)	(*) point 22
Non-correspondance (défaut de solidarité) entre contacts travail	
Non-correspondance (défaut de solidarité) entre contacts repos	

Tableau C.4 – Diodes

a) Diode normale (de puissance, de signal, de commutation)	
Coupure	
Court-circuit	
Augmentation du courant inverse	
Diminution de la tension inverse de claquage	
Augmentation de la tension à l'état de conduction	
Diminution de la tension à l'état de conduction	
Augmentation de la tension de seuil	(*) point 23
Diminution de la tension de seuil	(*) point 23
Court-circuit au boîtier conducteur	
b) Diode Zener	
Coupure	
Court-circuit	
Augmentation de la tension de Zener	(*) point 24
Diminution de la tension de Zener	(*) point 24
Changement de la valeur de la résistance différentielle	
Augmentation du courant inverse	
Augmentation de la tension à l'état de conduction directe	
Diminution de la tension à l'état de conduction directe	
Augmentation de la tension de seuil de conduction directe	(*) point 23
Diminution de la tension de seuil de conduction directe	(*) point 23
Court-circuit au boîtier conducteur	

Tableau C.5 – Transistors

a) Transistor bipolaire	
Coupure – de l'émetteur (E) – et/ou de la base (B) – et/ou du collecteur (C)	
Court-circuit – entre E et B – entre B et C – entre E et C – entre E et B et C	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.5 *(suite)*

Court-circuit entre deux connexions et coupure de la troisième connexion	
Court-circuit entre le boîtier et E ou B ou C	
Augmentation du gain c.c. et/ou c.a.	(*) point 25
Diminution du gain c.c. et/ou c.a.	
Augmentation de la tension base-émetteur à l'état de conduction	
Diminution de la tension base-émetteur à l'état de conduction	
Augmentation de la tension de seuil V_{BE}	(*) point 23
Diminution de la tension de seuil V_{BE}	(*) point 23
Diminution de la tension de claquage V_{EB} ou V_{CB} ou V_{CE}	
Changement du temps de montée, du temps de descente, du temps d'établissement et du temps de coupure de conduction	
Augmentation du courant de fuite I_{CB}, I_{EB}, I_{CE}	
Changement de la tension de saturation V_{CE}	
b) Transistor à effet de champ (FET, *Field-effect transistor*)	
Coupure – de la gâchette (G) – et/ou de la source (S) – et/ou du drain (D)	
Court-circuit – entre S et D – entre G et D – entre S et G – entre S et G et D	
Court-circuit entre deux connexions et coupure de la troisième connexion	
Court-circuit entre le boîtier et S ou G ou D	
Augmentation de la transconductance directe	(*) point 25
Diminution de la transconductance directe	
Augmentation de la tension de seuil de la grille	
Diminution de la tension de seuil de la grille	
Diminution – de la tension de claquage drain-source – des tensions assignées maximales grille-source et drain-grille	
Changement du temps d'établissement et du temps de coupure de conduction	
Augmentation du courant de fuite I_{GS}, I_{DS}, I_{GD}	
Changement de la valeur statique de la résistance drain/ source à l'état passant	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.6 – Redresseurs contrôlés

a) Redresseurs contrôlés au silicium (SCR, *Silicon – controlled rectifier*) (thyristor)	
Coupure – de la gâchette (G) – et/ou de l'anode (A) – et/ou de la cathode (C)	
Court-circuit – entre G et C – entre G et A – entre A et C – entre A et G et C	
Court-circuit entre deux connexions et coupure de la troisième connexion	
Court-circuit entre le boîtier et A ou G ou C	
Changement du courant de maintien	
Changement du courant de déclenchement de la gâchette et/ou de la tension de déclenchement de la gâchette	
Diminution – de la tension de blocage directe anode-cathode – de la tension de blocage inverse anode-cathode – de la tension assignée maximale inverse de la gâchette	
Changement du temps d'établissement et du temps de coupure de conduction	
Augmentation des courants de fuite I_{AC}, I_{GC}, I_{GA}	
Changement de la tension statique directe de conduction	
b) Thyristor bidirectionnel (triac)	
Coupure – de la gâchette (G) – et/ou de MT1 (première connexion de sortie courant) – et/ou de MT2 (seconde connexion de sortie courant)	
Court-circuit – entre G et MT1 – entre G et MT2 – entre MT1 et MT2 – entre MT1 et G et MT2	
Court-circuit entre deux connexions et coupure de la troisième connexion	
Court-circuit entre boîtier et MT1 ou G ou MT2	
Changement du courant de maintien	
Changement du courant de déclenchement de la gâchette et/ou de la tension de déclenchement de la gâchette	
Diminution des tensions assignées maximales de blocage MT1-MT2 et/ou de la tension assignée maximale de la gâchette	
Augmentation des courants de fuite MT1-MT2, G-MT1, G-MT2	
Changement de la tension statique de conduction	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.7 – Suppresseurs de surtension

a) Résistance variable avec la tension (VDR, *Voltage-dependent resistor*) (varistance)	
Coupure	
Court-circuit	
Augmentation de la tension d'écrêtage	
Diminution de la tension d'écrêtage	
Augmentation du courant de fuite	
b) Diode de protection (tranzorb)	
Coupure	
Court-circuit	
Augmentation de la tension de claquage	(*) point 24
Diminution de la tension de claquage	(*) point 24
Augmentation du courant de fuite	
Court-circuit au boîtier conducteur	
c) Dispositif de protection à gaz	
Coupure	
Court-circuit	
Augmentation de la tension de claquage	
Diminution de la tension de claquage	
Augmentation du courant de fuite	
d) Dispositif de protection à air	
Coupure	
Court-circuit	
Augmentation de la tension de claquage	
Diminution de la tension de claquage	
Augmentation du courant de fuite	

Tableau C.8 – Composants optoélectroniques

a) Photodiode	
Coupure	
Court-circuit	
Augmentation de la sensibilité lumineuse	(*) point 25
Diminution de la sensibilité lumineuse	
Augmentation du courant de fuite	
b) Phototransistor	
Coupure	
Court-circuit	
Augmentation de la sensibilité lumineuse	(*) point 25
Diminution de la sensibilité lumineuse	
Augmentation du courant de fuite	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.8 *(suite)*

c) Diode électroluminescente (DEL)	
Coupure	
Court-circuit	
Augmentation de l'émission lumineuse (à courant constant)	(*) point 26
Diminution de l'émission lumineuse (à courant constant)	
Augmentation du courant de fuite	
Augmentation de la tension de seuil	(*) point 23
Diminution de la tension de seuil	(*) point 23
Emission de lumière en dessous de la tension de seuil	(*) point 26
Emission de lumière en polarité inverse	(*) point 27
d) Optocoupleur et système optique contenant une fibre optique (voir point 28)	
Court-circuit ou diminution de la résistance d'isolement	
– entre entrée et sortie	(*) point 29
– entre systèmes adjacents dans le même boîtier	(*) point 29
Court-circuit au boîtier	
Changement du temps de commutation	
Augmentation du rapport de transfert en courant	(*) points 25 et 26
Diminution du rapport de transfert en courant	

Tableau C.9 – Filtres

a) Cristal de quartz	
Coupure	
Court-circuit	
Changement de la fréquence de résonance	
Diminution du facteur Q	
Court-circuit au boîtier conducteur	
b) Résonateur mécanique (diapason/lame/pendule)	
Coupure	
Court-circuit ou diminution de la résistance d'isolement	
– entre entrée et sortie	(*) point 30
– entre entrée ou sortie et boîtier	(*) point 30
Changement de la fréquence de résonance	(*) point 31
Augmentation du rapport de transfert	(*) points 32 et 33
Diminution du rapport de transfert	
Augmentation du facteur Q	(*) point 33
Diminution du facteur Q	(*) points 31 et 34

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.10 – Assemblages d'interconnexion

a) Circuit imprimé	
Coupure ou augmentation de la résistance d'une ou de plusieurs pistes	
Court-circuit ou diminution de l'isolement entre deux pistes différentes	(*) point 35
b) Connecteur	
Coupure – d'un ou de plusieurs contacts – du blindage	
Court-circuit ou diminution de la résistance d'isolement – entre contact et contact – entre contact et blindage	 (*) points 35 et 36 (*) points 35 et 36
Mauvais positionnement mécanique	(*) point 37
c) Câbles et fils	
Coupure ou augmentation de la résistance d'un ou de plusieurs fils	
Coupure ou augmentation de la résistance de l'écran	(*) point 38
Court-circuit ou diminution de la résistance d'isolement – entre deux fils ou plusieurs fils – entre un fil ou plusieurs fils et l'écran – entre un fil ou plusieurs fils ou l'écran et les parties conductrices externes	 (*) point 39 (*) point 39 (*) point 39
Coupures et courts-circuits multiples	(*) point 39
d) Connexion – soudée, brasée, enroulée, sertie, clipsée, vissée	
Coupure	
Augmentation de la résistance	
e) Câble à fibre optique	
Coupure	
Augmentation de l'atténuation	
f) Connecteur à fibre optique	
Coupure	
Augmentation de l'atténuation	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.11 – Fusibles

Coupure	
Court-circuit parallèle	(*) point 40
Augmentation de la valeur du courant de rupture	(*) point 40
Augmentation du temps de rupture	(*) point 40
Reconnexions après rupture	(*) point 40

Tableau C.12 – Interrupteurs et boutons-poussoirs

Coupure de chacun des contacts	
Court-circuit ou diminution de la résistance d'isolement	
– à travers les contacts ouverts	(*) point 20
– entre contacts	(*) point 20
– entre contact et boîtier	(*) point 20
Soudage des contacts	(*) point 21
Augmentation de la résistance des contacts	
Système bloqué à l'état haut	
Augmentation du temps de rebondissement de contact	

Tableau C.13 – Lampes

Coupure	
Court-circuit	
Diminution de l'intensité lumineuse	
Court-circuit au boîtier conducteur	

Tableau C.14 – Batteries

Coupure	
Court-circuit – d'un élément – de plusieurs éléments – de toute la batterie	
Diminution de la f.é.m.	
Augmentation de la résistance interne	

Tableau C.15 – Transducteurs/capteurs (n'incluant pas ceux avec un circuit électronique intégré)

Coupure	
Court-circuit	
Sortie trop haute	
Sortie trop basse	
Temps de réponse trop long	
Court-circuit au boîtier conducteur	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau C.16 – Circuits intégrés

a) Dispositifs analogiques	
Dysfonctionnement: voir Article C.3	
b) Dispositifs numériques	
Dysfonctionnement: voir Article C.3	
c) Microprocesseurs	
Dysfonctionnement: voir Article C.3	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe D
(informative)

Informations techniques supplémentaires

D.1 Introduction

La présente annexe fournit des exemples et des lignes directrices en complément des exigences techniques spécifiées en 5.4 et à l'Annexe B. Les exigences fournies sont uniquement valables pour le SIL 3 ou le SIL 4.

D.2 Obtention de l'indépendance physique interne
(Protection contre les influences de type A, telles que mentionnées en B.3.2)

D.2.1 Indépendance de premier niveau

Les mesures suivantes permettent d'obtenir une "indépendance de premier niveau" entre deux entités dont le dysfonctionnement simultané est susceptible d'engendrer une situation dangereuse:

a) mesures destinées à éviter les liaisons galvaniques involontaires

(protection de l'isolation galvanique interne)

1) Isolation entre les pistes d'une même couche de carte de circuit imprimé.

Il est recommandé que les distances d'isolation (lignes de fuite et distances d'isolement) soient au moins dimensionnées conformément aux exigences sur le renforcement de l'isolation de l'EN 50124-1.

2) Isolation entre des pistes situées sur des couches différentes d'une carte imprimée multicouches.

3) Isolation entre les fils isolés d'un même câble.

4) Isolation entre des enroulements isolés dans le même transformateur.

Il convient que la température maximale à l'intérieur des transformateurs soit limitée (également en cas de pannes), afin d'éviter la carbonisation.

5) Isolation entre des entités isolées à l'intérieur d'un coupleur optoélectronique.

Il est recommandé que la température maximale à l'intérieur des coupleurs optoélectroniques soit limitée (également en cas de pannes), afin d'éviter la carbonisation.

b) mesures destinées à éviter les effets involontaires engendrés par des liaisons volontaires

(protection des interfaces internes)

Il est recommandé que les interfaces soient protégées au moyen de dispositifs présentant des propriétés intrinsèques.

c) mesures destinées à éviter les effets involontaires engendrés par un couplage électromagnétique

(protection contre la diaphonie interne)

Il est recommandé que la diaphonie entre des réseaux électroniques numériques soit évitée comme suit:

1) si plusieurs entités se trouvent sur la même carte de circuit imprimé, il est préférable de les alimenter par des réseaux d'alimentation électrique différents. Si cela n'est pas le cas, il convient que l'impédance du réseau de terre soit suffisamment faible pour empêcher le phénomène de diaphonie, même en cas de panne;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

2) si plusieurs lignes sur la même carte nécessitent une protection contre les phénomènes de diaphonie qui se produisent entre elles, la distance de séparation nécessaire dépend de la technologie utilisée, de la longueur de couplage et du mécanisme de couplage. Il convient que cette distance soit démontrée, pour le mode d'exploitation normal, par des calculs théoriques et/ou par des mesures pratiques;

3) s'il est nécessaire d'éviter les couplages en cas de pannes, il convient de prendre des mesures additionnelles (par exemple utilisation d'un blindage ou doublement de la distance d'isolement). Il convient de démontrer leur efficacité par des calculs théoriques et/ou par des mesures pratiques.

D.2.2 Indépendance de deuxième niveau

Les mesures suivantes assurent une "indépendance de deuxième niveau" entre deux entités dont le dysfonctionnement simultané ne peut pas engendrer une situation dangereuse:

a) chaque entité dans un système "*n* parmi *m*" peut se composer d'un certain nombre d'entités indépendantes;

b) l'indépendance de deux entités dont le dysfonctionnement simultané est susceptible d'engendrer une situation dangereuse est obtenue en procédant conformément à D.2.1 (indépendance de premier niveau). Ces entités seront désignées par "entités principales". Chaque entité principale peut avoir une ou plusieurs "entités supplémentaires" servant à contrôler l'entité principale;

c) il est possible que la qualité de l'indépendance entre une entité principale et une entité supplémentaire soit inférieure à celle énoncée en D.2.1; dans ce cas, elle est désignée par "indépendance de deuxième niveau";

d) les entités principales sont indépendantes des entités supplémentaires, si toutes les influences possibles liées à une première panne entre elles sont décelées avant qu'elles ne deviennent dangereuses suite à d'autres pannes;

e) il est permis de procéder aux simplifications suivantes, par rapport à D.2.1, pour l'indépendance de deuxième niveau:

   – il convient que le dimensionnement des distances d'isolation (lignes de fuite et distances d'isolement) soit au moins conforme aux exigences de l'isolement de base de l'EN 50124-1;

   – les dispositifs de protection ne nécessitent pas de propriétés intrinsèques. (Seule une seconde panne est en mesure de compromettre l'indépendance entre une entité principale et une entité supplémentaire);

   – il convient de séparer au moins les réseaux d'alimentation électrique du système de surveillance de tension (entité additionnelle) de celui de l'entité principale surveillée, comme cela est écrit au présent point e).

D.3 Obtention de l'indépendance physique externe
(Protection contre les influences de type C, telles que mentionnées en B.3.2)

Les mesures suivantes assurent une indépendance physique externe:

a) il convient de prendre des mesures pour éviter des effets involontaires dus à des interférences électromagnétiques ou à des décharges électrostatiques perturbant l'exploitation normale, conformément à la CEI 62236-4;

b) il convient de remplir normalement les conditions climatiques spécifiées. Il convient de prendre des mesures pour minimiser le risque d'exploiter le système en dehors de ses conditions climatiques spécifiées;

c) il convient de prendre des mesures pour éviter des effets involontaires engendrés par des contraintes mécaniques perturbant l'exploitation normale:

   1) mesures pour assurer une exploitation fiable et correcte, malgré la présence de contraintes mécaniques, convenues entre la société d'exploitation ferroviaire et le fournisseur;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

2) il convient que la protection soit conforme aux exigences des EN 50125-1 et/ou EN 50125-3, selon le cas;

d) il convient de prendre des mesures pour assurer une exploitation fiable et correcte, malgré les conditions de contraintes chimiques convenues entre la société d'exploitation ferroviaire et le fournisseur;

e) il convient de prendre des mesures pour éviter une mise en fonctionnement involontaire, sous des tensions d'alimentation électrique non permises (protection des tensions d'alimentation):

1) il convient que les tensions d'alimentation non permises (en dehors des valeurs indiquées sur les fiches techniques relatives aux systèmes, aux équipements ou aux composants alimentés) soient décelées par un dispositif de surveillance de la tension électrique, assurant le passage à un état sûr avant que des situations dangereuses ne deviennent possibles;

2) il convient que le dispositif de surveillance de la tension électrique puisse fonctionner correctement pendant toute la durée du cycle de vie. Il est possible qu'une redondance du dispositif de surveillance de la tension électrique soit nécessaire, si la détection de pannes par le dispositif de surveillance de la tension n'est pas possible.

f) il convient de prendre des mesures pour éviter les effets dangereux involontaires, dus à des tensions externes entre les bornes d'entrée et de sortie, qui empêchent l'exploitation normale (protection des interfaces externes):

1) il convient de supposer la présence de tensions externes, dans le cas le plus défavorable (tensions de fonctionnement et toutes tensions possibles induites par des interférences électromagnétiques sur les câbles et les lignes);

2) il convient que le dimensionnement des distances d'isolement entre des parties sous tension et des parties conductrices exposées, une terre conductrice exposée, ou des circuits conducteurs exposés, dont le fonctionnement correct nécessite une protection, soit effectué selon les tensions de choc spécifiées dans l'EN 50124-1;

3) il convient que le dimensionnement des lignes de fuite entre des parties sous tension et des parties conductrices exposées, une terre conductrice exposée ou des circuits conducteurs exposés, dont le fonctionnement correct nécessite une protection, soit effectué conformément aux exigences de l'EN 50124-1 et conformément aux taux de tensions efficaces maximales assignées pendant l'exploitation;

4) en ce qui concerne le dimensionnement de l'isolation, il est nécessaire de choisir la plus grande distance (distance d'isolement ou ligne de fuite).

D.4 Exemple de méthode d'analyse de panne simple
(Telle que mentionnée en B.3.3)

NOTE 1 Les informations des points a) à f) suivants sont tirées du document CENELEC CLC/SC9XA(SEC)114 *Calculs avec les formules du MÜ 8004*.

a) Suivant la somme "*a*" des taux de défaillance des entités dont le dysfonctionnement simultané est susceptible d'engendrer une situation dangereuse, il est recommandé que le temps de détection plus passivation t_{sf} des pannes simples dans les entités respectives ne dépasse pas la valeur suivante:

$$t_{sf} \leq \frac{k}{1\,000 \times a}$$

où

k = 1 pour un système "2 parmi 2";

k = 0,5 pour un système "2 parmi 3".

b) Les taux de défaillance, mentionnés au point a) ci-dessus, doivent être déterminés en fonction du profil de contrainte qui dépend des conditions d'environnement pendant l'exploitation. Le profil de contrainte dépend de l'application. Il est possible de prendre un

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

profil de contrainte simplifié comme base de référence, si ce profil exerce un effet défavorable sur le taux de défaillance.

c) Si, dans un système, un sous-système ou un équipement comprenant plusieurs entités, les combinaisons de deux entités défaillantes ne sont pas toutes dangereuses, le temps de détection des pannes peut être déterminé séparément pour les diverses combinaisons. Si, dans ce cas, il existe différents temps de détection de pannes pour une seule entité, il faut choisir le temps de détection le plus court.

d) Il convient que des essais périodiques de détection de pannes de toutes les entités soient mis en œuvre. Il convient que ces essais soient représentatifs des pannes vraisemblables pouvant affecter le fonctionnement correct et qu'ils soient exécutés dans un temps inférieur à t_{sf}.

Il est recommandé que la détection de pannes dans les circuits intégrés à grande échelle soit conforme au Tableau D.1.

e) Si l'alimentation électrique d'un système "2 parmi *n*" (*n* = 2 ou 3), exempt de pannes, est coupée, il est admis que la détection de panne soit interrompue. Il est souhaitable que la durée d'une telle coupure d'alimentation ne dépasse pas 400 fois la valeur du temps de détection de panne permis, conformément au point a) ci-dessus.

NOTE 2 Cette règle est basée sur l'hypothèse selon laquelle la fiabilité des composants électroniques est 20 fois supérieure lorsque l'équipement n'est pas alimenté.

f) Dans le cas où la détection de panne est interrompue pendant une durée supérieure à la durée admissible selon le point e) ci-dessus, le système, le sous-système, ou l'équipement ne peut être remis en service qu'après avoir subi des contrôles destinés à déterminer d'éventuelles pannes multiples.

NOTE 3 Les informations des points g) à j) suivants sont tirées du document italien "Note technique des chemins de fer pour les systèmes électroniques de sécurité (IS 353)". L'IS 353 est en accord avec les recommandations du document ORE A 155.3.

g) Lorsque la fonction relative à la sécurité est réalisée par une entité unique, le temps de détection d'une défaillance contraire t_{sf} est le temps maximal total de détection et de passage à l'état sûr en cas de panne simple. Le temps de détection ne doit pas dépasser les limites de durée spécifiées pour une condition dangereuse. Afin d'éviter toute condition dangereuse, il faut que cette durée soit inférieure au temps de réponse exigé de l'équipement sous contrôle (par le biais de l'entité unique).

h) Le temps de réponse dépend du type d'équipement à contrôler, et dépend donc du type d'application.

Par exemple, le temps t_{sf} pourrait vérifier la valeur suivante:

t_{sf} < 100 ms, si l'équipement à contrôler est un relais de signalisation.

i) Durant le temps t_{sf}, il faut que la première défaillance relative à la sécurité soit détectée et qu'elle déclenche la mise à l'état sûr.

j) Il convient de mettre en œuvre des essais périodiques dans le cas d'une entité unique. Il est souhaitable que les essais soient représentatifs de toutes les défaillances pouvant affecter l'exploitation correcte, et que ces essais soient achevés dans un délai inférieur à t_{sf}.

D.5 Exemple de méthode de détection de pannes multiples
(Telle que mentionnée en B.3.5)

NOTE Les informations des points a) et b) suivants sont tirées du document CENELEC CLC/SC9XA(sec)114 *Calculs avec les formules du MÜ 8004*.

a) Panne double susceptible d'engendrer une situation dangereuse si elle est combinée à une troisième panne.

1) Si la détection d'une panne dans une entité plus sa passivation n'est pas possible dans les délais prévus, ou si elle est inadaptée, il convient de tenir compte de la probabilité qu'une autre panne se produise dans une seconde entité.

2) Il est nécessaire que des pannes simultanées se produisant dans deux entités ne soient pas dangereuses. Cela signifie qu'au moins trois entités indépendantes sont

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

nécessaires. Elles sont reliées de telle manière qu'une situation dangereuse ne peut être engendrée que si les trois entités ont un mauvais fonctionnement, comme c'est le cas dans un système "3 parmi 3".

3) Suivant la somme "*a*" des taux de défaillance d'au moins trois entités, dont le dysfonctionnement simultané est susceptible d'engendrer une situation dangereuse, il convient que le temps de détection plus passivation t_{df}, relatif aux pannes doubles, ne soit pas supérieur à la valeur suivante:

$$t_{df} \leq \frac{2}{a}$$

4) Il convient de déterminer les taux de défaillance mentionnés au point c) en fonction du profil de contrainte qui dépend des conditions d'environnement qui prédominent pendant l'exploitation. Le profil de contrainte dépend de l'application. Il est possible de prendre un profil de contrainte simplifié comme base de référence, si ce profil exerce un effet défavorable sur le taux de défaillance.

5) Si, dans un système, un sous-système ou un équipement comprenant plusieurs entités, les combinaisons de trois entités défaillantes ne sont pas toutes dangereuses, le temps de détection des pannes peut être déterminé séparément pour les diverses combinaisons. Si, dans ce cas, il existe différents temps de détection de pannes pour deux entités, il faut choisir le temps de détection le plus court.

b) Panne triple susceptible d'engendrer une situation dangereuse si elle est combinée à une quatrième panne.

1) Si la détection d'une panne double dans deux entités plus sa passivation n'est pas possible dans les délais prévus, ou si elle est inadaptée, il convient de tenir compte de la probabilité pour qu'une autre panne se produise dans une troisième entité.

2) Il est nécessaire que des pannes simultanées se produisant dans trois entités ne soient pas dangereuses. Cela signifie qu'au moins quatre entités indépendantes sont nécessaires. Elles sont reliées de telle manière qu'une situation dangereuse ne peut être engendrée que si les quatre entités ont un mauvais fonctionnement, comme c'est le cas dans un système "4 parmi 4".

3) Aucune mesure de détection de pannes triples n'est requise sur le flux de données d'exploitation et pour des valeurs supérieures à celui-ci, et au cours des essais pendant la maintenance, si le taux de défaillance "*a*" ne dépasse pas la valeur suivante:

$$a \leq 2 \times 10^{-4}\ h^{-1}$$

4) Le taux de défaillance "*a*" est la somme des taux de défaillance des entités dont le dysfonctionnement simultané est susceptible d'engendrer une situation dangereuse (panne quadruple).

c) En cohérence avec le point 3) de l'Article D.4, il ne doit pas être possible qu'une défaillance supplémentaire puisse inhiber la mise à l'état sûr. Cela ne peut être obtenu que par la mise en œuvre de contrôles lors des opérations de maintenance corrective qu'il faut exécuter lorsque la partie en panne de l'entité est hors service.

Un exemple de méthode d'analyse des défauts est donné à la Figure D.1

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

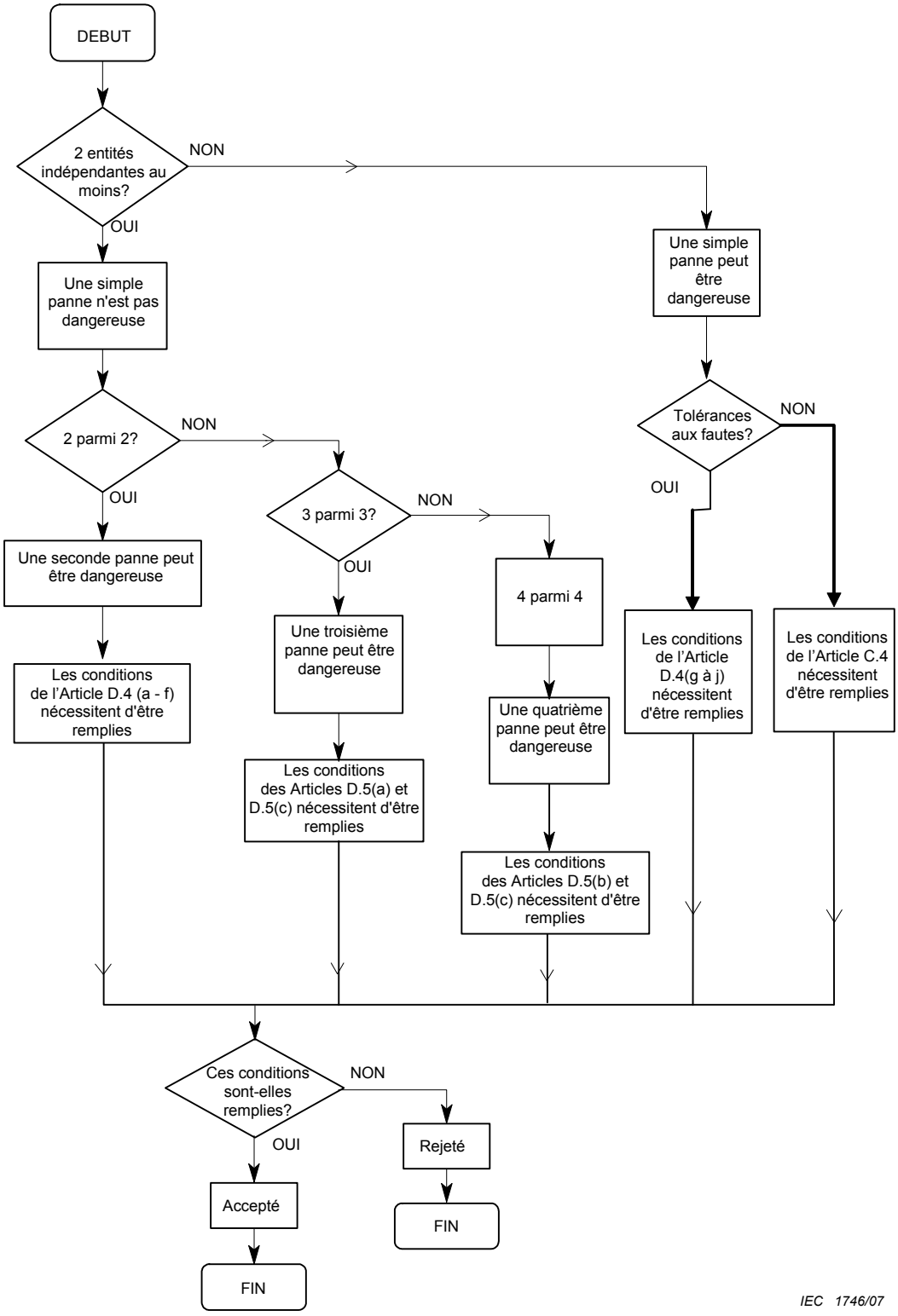


Figure D.1 – Exemple d'une méthode de détection de pannes

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau D.1 – Exemples de mesures permettant de déceler des pannes dans des circuits intégrés à grande échelle au moyen d'un essai périodique en ligne, avec comparaison (SW ou HW), dans un système "2 parmi *n*" [1)]

Composant	Dysfonctionnement	Mesures
1 Unité centrale 1.1 Registre	Par exemple, toute dépendance vis-à-vis de combinaisons de bits de données (panne sensible à une trame)	En utilisant tous les registres (excepté les registres d'initialisation) dans toutes les configurations possibles (combinaisons de données utiles). Après initialisation d'un registre d'initialisation (registre de commande d'interruptions), la fonction correcte initialisée doit être testée. Les registres supérieurs à 8 bits peuvent être testés en utilisant toutes les combinaisons suivantes de bits de données: ..5555....H OAAAA....H ..3333....H 9999....H 0CCCC....H 6666....H 0000....H 0FFFF....H 0F0F0....H ..0F0F....H au cours de chaque période d'essai en ligne. Des essais en ligne supplémentaires, avec toutes les combinaisons de données utiles, sont nécessaires; ces essais doivent être répartis sur plusieurs périodes d'essai (en utilisant, par exemple, un générateur de nombres aléatoires).
1.2 Décodage et exécution d'une instruction	Par exemple, tout décodage erroné ou exécution erronée affectant des registres ou des mémoires, selon les combinaisons de bits de données au niveau de la source et/ou de la destination.	Utiliser une instruction de chaque type, tester avec toutes les combinaisons de données utiles mentionnées en 1.1. Vérifier si toutes les instructions utiles liées au système sont exécutables, pour toutes les conditions, sources, destinations et valeurs des bits d'adresses (y compris compteur d'instructions de programmes de chargement). Vérifier si toutes les instructions utiles liées aux interruptions système sont exécutables, en fonction des interruptions ou des conditions d'interruption. Pour vérifier toutes les instructions utiles liées au système, il est permis de les créer dans la RAM et de les rappeler pour l'exécution. Après un changement lié à l'exécution du contenu d'au moins un registre, il est recommandé de ne pas limiter la vérification au contenu des registres concernés, mais de l'étendre aux contenus de tous les autres registres.
1.3 Horloge	Fréquence erronée	Si des générateurs d'horloge indépendants sont utilisés pour chaque voie de calcul, il est alors possible de déceler une fréquence erronée dans un canal en procédant par comparaison. En cas de pannes multiples, un contrôle supplémentaire des fréquences peut s'avérer nécessaire.

1) Il faut supposer une détection, indépendante de l'application, des premières pannes avant les deuxièmes.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau D.1 *(suite)*

Composant	Dysfonctionnement	Mesures
1.4 Remise à zéro	Remise(s) à zéro supplémentaire(s) ou aucune remise à zéro	Si des générateurs de remise à zéro indépendants sont utilisés pour chaque voie de calcul, il est alors possible de déceler une remise à zéro erronée dans un canal, en procédant par comparaison. En cas de pannes multiples, un contrôle supplémentaire de démarrage correct peut s'avérer nécessaire.
1.5 Alimentation électrique	Tension d'alimentation erronée	Si des alimentations électriques indépendantes sont utilisées pour chaque voie de calcul, il est alors possible de déceler une tension d'alimentation erronée dans un canal, en procédant par comparaison. En cas de non-indépendance, ou de pannes multiples, un contrôle supplémentaire de la tension peut s'avérer nécessaire.
2 Mémoire 2.1 ROM	Tout contenu erroné et tout décodage erroné d'adresse(s) ou de signal (signaux) de commande.	Lecture et comparaison de tous les contenus.
2.2 RAM	Tout contenu erroné après lecture ou écriture, et tout décodage erroné d'adresse(s) ou de signal (signaux) de commande.	Lecture et comparaison de tous les contenus. Essai d'écriture/lecture/comparaison avec toutes les combinaisons de données utiles mentionnées en 1.1. Vérifier si toutes les cellules sont adressables (par exemple en chargeant une combinaison particulière de bits de données dans une cellule et en lisant/comparant toutes les autres cellules du circuit intégré concerné). Répéter la même procédure en chargeant la combinaison particulière inversée de données utiles dans la même cellule. Toutes ces vérifications doivent être répétées pour la cellule suivante, de la même manière, et ainsi de suite, jusqu'à ce que toutes les cellules contenues dans tous les circuits intégrés de la RAM soient utilisées.
		Le dernier essai décrit permet également de déceler des influences de la part de chaque bit vers un autre bit dans le même circuit de RAM. Cet essai peut être réparti sur plusieurs périodes d'essai en ligne.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe E
(informative)

Techniques et mesures à mettre en œuvre pour éviter les pannes systématiques et contrôler les pannes systématiques et aléatoires des systèmes électroniques de signalisation relatifs à la sécurité

E.1 Techniques et mesures à mettre en œuvre pour éviter les pannes systématiques et contrôler les pannes systématiques et aléatoires des systèmes électroniques de signalisation relatifs à la sécurité

Les niveaux d'intégrité de la sécurité (SIL) sont définis au niveau fonctionnel pour les sous-systèmes réalisant la fonctionnalité. La présente annexe précise les architectures, techniques et mesures à mettre en œuvre pour éviter les pannes systématiques et contrôler les pannes systématiques et les pannes aléatoires pour les différents niveaux d'intégrité de la sécurité (SIL) 1 à 4.

En conséquence, les tableaux suivants décrivent les différentes techniques et mesures à mettre en œuvre pour les quatre niveaux de SIL.

Il n'est pas possible d'énumérer toutes les causes élémentaires des pannes systématiques durant les phases du cycle de vie, parce que les pannes systématiques ont des effets différents dans les différentes phases du cycle de vie et que les mesures à appliquer dépendent de l'application. Une analyse quantitative pour éviter les pannes systématiques n'est donc pas possible.

Conformément au cycle de vie système et au processus de gestion de la sécurité décrits dans la CEI 62278 et en 5.3, un certain nombre d'activités doit être mené à chaque phase du cycle de vie. Comme il est précisé dans le processus de gestion de la sécurité, l'objectif de ce processus est de réduire autant que possible l'incidence des erreurs humaines relatives à la sécurité tout au long du cycle de vie et donc de minimiser le risque résiduel des pannes systématiques relatives à la sécurité. Cela comprend les processus de vérification et d'assurance qualité. Les exigences de ce processus sont listées dans le:

Tableau E.1 – Activités d'assurance qualité et de planification de la sécurité (référencées en 5.2 et 5.3.4).

Selon les phases 1 à 4 décrites dans la CEI 62278

Phase 1: Conception

Phase 2: Conditions d'application et définition du système

Phase 3: Analyse de risques

Phase 4: Exigences du système

les résultats doivent être intégrés dans le document spécification des exigences du système, qui doit tenir compte des techniques/mesures dans le

Tableau E.2 – Spécification des exigences du système (référencée en 5.3.6).

Durant la préparation du plan de sécurité, la structure de la gestion de la sécurité doit être identifiée. Des informations de soutien sont données dans le

Tableau E.3 – Organisation de la sécurité (référencée en 5.3.3).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Durant la phase de conception et de réalisation du cycle de vie (phase 6), la description de l'architecture du système doit être documentée en prenant en considération le

Tableau E.4 – Architecture du système/sous-système/équipement (référencée en 5.4).

Pour éviter et contrôler les pannes causées par

– toute panne résiduelle de conception,
– les conditions d'environnement,
– des erreurs d'utilisation ou d'exploitation,
– toute panne résiduelle dans le logiciel,
– des facteurs humains,

les techniques/mesures pour les caractéristiques de conception sont données dans le

Tableau E.5 – Caractéristiques de conception (référencées en 5.4).

Conformément aux caractéristiques de conception, l'analyse des effets des pannes doit identifier les contraintes de fiabilité, disponibilité, maintenabilité et sécurité sur le matériel et le logiciel en utilisant les analyses de fiabilité, disponibilité, maintenabilité et sécurité et les modes de défaillance de l'Annexe C.

Des méthodes pour identifier et évaluer les effets des pannes sont données dans le

Tableau E.6 – Méthodes d'analyse des situations dangereuses et des défaillances (référencées en 5.4).

Quelle que soit la méthode de conception, elle doit avoir les caractéristiques suivantes:

– une documentation claire et précise;
– une expression claire et précise des fonctionnalités;
– une transparence, modularité et traçabilité;
– des informations relatives au temps et à la technologie;
– une testabilité durant la vérification et la validation.

Des techniques/mesures sont données dans le

Tableau E.7 – Conception et développement du système/sous-système/équipement (référencés en 5.3.7).

La conception projetée doit être documentée en faisant référence au

Tableau E.8 – Documentation de la phase de conception (référencée en 5.2)

et validée pour les techniques/mesures dans le

Tableau E.9 – Vérification et validation de la conception du produit et du système (référencées en 5.3.9).

En s'appuyant sur le registre des situations dangereuses, un rapport d'essai de validation doit être établi en incluant

– la version des spécifications d'essais utilisée,
– la version des éléments matériels et logiciels (HW et SW) utilisée,

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– les outils et les équipements utilisés,

– le résultat de chaque essai,

– toutes les différences entre les résultats attendus et les résultats réels,

– les analyses menées et les décisions prises dans le cas de différences constatées.

Les résultats de la phase de conception/développement et du dossier de sécurité déboucheront sur les procédures d'application, d'exploitation et de maintenance qui doivent être documentées en prenant en compte les techniques/mesures dans le

Tableau E.10 – Application, exploitation et maintenance (référencées en 5.3.12 et 5.4).

Pour chaque technique ou mesure précisées dans ces tableaux, il est fait mention d'une recommandation pour chacun des niveaux d'intégrité de la sécurité (SIL) 1 à 4.

"HR" Ce symbole signifie que la technique ou la mesure est hautement recommandée pour ce niveau d'intégrité de la sécurité. Si cette technique ou cette mesure n'est pas utilisée pour des raisons tout à fait rationnelles, celles-ci doivent être précisées.

"R" Ce symbole signifie que la technique ou la mesure est recommandée pour ce niveau d'intégrité de la sécurité.

"-" Ce symbole signifie que la technique ou la mesure n'a pas de recommandation à être ou ne pas être utilisée.

Tableau E.1 – Activités d'assurance qualité et de planification de la sécurité (référencées en 5.2 et 5.3.4)

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1 Listes de contrôle	R: liste de contrôle des activités et points qui doivent être produits		R: liste de contrôle des activités et points qui doivent être produits	
2 Audit des tâches	R		HR	
3 Inspection des versions de la documentation	HR: documents acceptés par la société d'exploitation ferroviaire ou l'autorité de tutelle et l'industrie		HR: tous les documents	
4 Revue après changement dans le plan de sécurité	HR			
5 Revue du plan de sécurité après chaque phase du cycle de vie sécurité	HR			

Tableau E.2 – Spécification des exigences du système (référencée en 5.3.6)

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1 Séparation des systèmes relatifs à la sécurité des systèmes non relatifs à la sécurité	R: interfaces bien définies entre les systèmes relatifs à la sécurité et les systèmes non relatifs à la sécurité (SRS)		HR: interfaces bien définies entre les systèmes relatifs à la sécurité et les systèmes non relatifs à la sécurité (SRS) et analyse des interfaces	
2 Description graphique incluant par exemple des blocs-diagrammes	HR		HR	
3 Spécifications structurées	HR: séparation hiérarchique manuelle en sous-tâches, description des interfaces		HR: séparation hiérarchique utilisant les méthodes formalisées, contrôle automatique de la cohérence, décomposition jusqu'à un niveau fonctionnel	
4 Méthodes formelles ou semi-formelles	-		R: assistées par ordinateur	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.2 *(suite)*

5 Outils de spécification assistés par ordinateur	-	R: outils sans aucune préférence pour une méthode de conception particulière	R: procédures orientées méthode avec subdivision hiérarchique, description de tous les objets et de leur relations, base de données commune, contrôle automatique de la cohérence
6 Listes de contrôle	R: listes de contrôle préparées pour toutes les phases du cycle de vie sécurité, en se concentrant sur les principaux problèmes de sécurité		R: listes de contrôle détaillées préparées pour toutes les phases du cycle de vie sécurité
7 Registre des situations dangereuses	HR: Registre des situations dangereuses à établir et à maintenir tout au long du cycle de vie du système		
8 Inspection des spécifications	R		HR
NOTE Il convient d'utiliser avec d'autres méthodes des listes de contrôle ou des outils de spécification assistés par ordinateur, étant donné qu'ils stipulent habituellement ce qui doit être fait (afin de ne rien oublier), mais ne peuvent garantir la qualité de ce qui est réellement réalisé.			

Tableau E.3 – Organisation de la sécurité (référencée en 5.3.3)

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1 Formation du personnel dans l'organisation de la sécurité	HR: formation initiale dans toutes les activités correspondantes de sécurité		HR: formation répétitive ou exécution régulière dans toutes les activités correspondantes de sécurité	
2 Indépendance des rôles	Voir Figure 6: Arrangements pour l'indépendance			
Qualification du personnel dans l'organisation de la sécurité (voir note)	HR: éducation technique ou expérience suffisante		HR: éducation technique de haut niveau ou expérience importante	
NOTE Il convient que le personnel impliqué dans des activités de sécurité ait la compétence nécessaire pour mener à bien ces activités (voir 5.3.3).				

Tableau E.4 – Architecture d'un système/sous-système/équipement (référencée en 5.4)

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1 Séparation des systèmes relatifs à la sécurité des systèmes non relatifs à la sécurité	R	R	HR	HR
2 Structure électronique simple avec autotests et surveillance	R	R	-	-
3 Structure électronique double	R	R	-	-
4 Structure électronique double basée sur la sécurité composite dotée d'un système de comparaison de sécurité	R	R	HR	HR
5 Structure électronique simple basée sur la sécurité intrinsèque	R	R	HR	HR
6 Structure électronique simple basée sur la sécurité réactive	R	R	HR	HR
7 Structure électronique diversifiée dotée d'un système de comparaison de sécurité	R	R	HR	HR

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.4 *(suite)*

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
8 Justification de l'architecture par une analyse quantitative de la fiabilité du matériel	HR	HR	HR	HR
NOTE Toutes les techniques précisées dans la partie grisée du tableau sont alternatives, c'est-à-dire que R signifie qu'au moins l'une de ces techniques est recommandée.				

Tableau E.5 – Caractéristiques de conception (référencées en 5.4)

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1 Protection contre les erreurs d'exploitation	R: liste de contrôle pertinente sur chacune des entrées de contrôle		HR: liste de contrôle pertinente sur chacune des entrées de contrôle	
2 Protection contre le sabotage	-		R: des mesures d'organisation additionnelles sont nécessaires	
3 Protection contre les pannes simples des composants discrets (B.3.1)	R: tous les modes de défaillance dangereux doivent être soit détectés et passivés, soit démontrés comme étant sûrs d'une manière inhérente, comme le résultat de propriétés physiques intrinsèques (voir l'Annexe C). Exigences de l'EN 50124-1 pour l'isolation de base		HR: tous les modes de défaillance dangereux doivent être soit détectés et passivés, soit démontrés comme étant sûrs d'une manière inhérente, comme le résultat de propriétés physiques intrinsèques (voir l'Annexe C). Exigences de l'EN 50124-1 pour l'isolation renforcée	
4 Protection contre les pannes simples des circuits intégrés pour la technologie à composants électroniques numériques (B.3.1, Article C.3)	R: modèle de "collage" à l'état de panne	R: modèle de panne CC	HR: modèle permanent et transitoire de dysfonctionnement au niveau entité simple (des exemples pour les dysfonctionnements des circuits intégrés sont donnés au Tableau D.1)	
5 Indépendance physique dans une architecture relative à la sécurité (B.3.2 type A et C)	R: il convient que les distances d'isolement soient au moins dimensionnées conformément à l'EN 50124-1 (isolation de base)		HR: il convient que les distances d'isolement soient dimensionnées conformément aux valeurs de l'EN 50124-1 (isolation renforcée)	
6 Détection des pannes simples (B.3.3)	R: révélées par les écarts par rapport à l'exploitation normale	R: il convient que le temps de détection plus passivation d'une panne simple, qui dépend de l'objectif de sécurité, soit dans les marges définies par l'objectif de sécurité	HR: il convient que le temps de détection plus passivation d'une panne simple, qui dépend de l'objectif de sécurité, soit dans les marges définies par l'objectif de sécurité	
7 Maintien dans un état sûr (B.3.4)	R: il convient que les indications fournies à l'opérateur ne puissent ni être utilisées ni reposer sur les fonctions relatives à la sécurité en relation avec l'entité en panne		HR: mise à l'arrêt automatique du système ou sous-système, de l'entité en panne ou blocage des fonctions relatives à la sécurité de cette entité, du système ou du sous-système en panne	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.5 *(suite)*

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
8 Pannes multiples (B.3.5)	R: révélées par les écarts par rapport à l'exploitation normale	R: il convient que le temps de détection plus passivation de pannes multiples, qui dépend de l'objectif de sécurité, soit dans les marges définies par l'objectif de sécurité	HR: il convient que le temps de détection plus passivation de pannes multiples, qui dépend de l'objectif de sécurité, soit dans les marges définies par l'objectif de sécurité	
9 Détection dynamique des pannes	R: il convient que des essais dynamiques en ligne soient réalisés pour contrôler le fonctionnement correct du système relatif à la sécurité et fournir une indication à l'opérateur	HR: il convient que des essais dynamiques en ligne soient réalisés pour contrôler le fonctionnement correct du système relatif à la sécurité et fournir une indication à l'opérateur	HR: il convient que des essais dynamiques en ligne soient réalisés pour contrôler le fonctionnement correct du système relatif à la sécurité et mettre à l'arrêt automatiquement le système ou sous-système de l'entité en panne ou bloquer toutes les fonctions de sécurité de cette entité, du système ou du sous-système en panne	
10 Surveillance des séquences du programme	R: surveillance temporelle ou logique des séquences du programme et fourniture d'indications à l'opérateur	HR: surveillance temporelle ou logique des séquences du programme et fourniture d'indications à l'opérateur	HR: surveillance temporelle et logique des séquences du programme avec de nombreux points de contrôle dans le programme et mise à l'arrêt automatique du système ou sous-système de l'entité en panne ou blocage des fonctions relatives à la sécurité de cette entité, du système ou du sous-système en panne	
11 Mesures contre les interruptions de tension, les variations de tension, les surtensions, les diminutions de tension	HR: mesures contre les interruptions de tension, les variations de tension, les surtensions, les diminutions de tension		HR: mesures étendues contre les interruptions de tension, les variations de tension, les surtensions, les diminutions de tension	
12 Mesures contre l'accroissement de la température	HR: capteur de température détectant les températures supérieures à celles spécifiées		HR: la nécessité d'une mise à l'arrêt en sécurité doit être analysée	
13 Architecture logicielle	voir la CEI 62279		voir la CEI 62279	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.6 – Méthodes d'analyse des situations dangereuses et des défaillances (références en 5.4)

	Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1	Analyse préliminaire des situations dangereuses [a]	HR	HR	HR	HR
2	Analyse par arbre des défauts	R	R	HR	HR
3	Bloc diagramme de Markov	R	R	HR	HR
4	AMDEC	R	R	HR	HR
5	HAZOP	R	R	HR	HR
6	Diagramme causes - conséquences	R	R	HR	HR
7	Arbre d'événements	R	R	R	R
8	Diagramme de fiabilité	R	R	R	R
9	Analyse par zone	R	R	R	R
10	Analyse des situations dangereuses aux interfaces	R	R	HR	HR
11	Analyse des défaillances de mode commun	R	R	HR	HR
12	Analyse des événements historiques	R	R	R	R

[a] Il est recommandé que l'analyse préliminaire des situations dangereuses ne soit envisagée qu'au début de la phase de développement. Il convient que le choix se porte sur d'autres méthodes lors de la phase de conception, si des informations techniques précises sont disponibles.

Tableau E.7 – Conception et développement d'un système/sous-système/équipement (références en 5.3.7)

	Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1	Conception structurée	HR: division hiérarchique de la conception		HR: division hiérarchique de la conception et pleine traçabilité de la spécification des exigences en incluant les références entre les spécifications, la conception, les diagrammes de circuits et la documentation de l'application	
2	Modularisation	R: modules de taille limitée, chaque module étant isolé	HR: modules de taille limitée, chaque module étant isolé	HR: utilisation de modules entièrement validés, facilement compréhensibles et de taille limitée, chaque module étant fonctionnellement isolé	
3	Méthodes formelles ou semi-formelles			R: assistées par ordinateur	
4	Outils de conception assistés par ordinateur	-	R: aide informatique pour des conceptions complexes	R: utilisation d'outils validés ou éprouvés par l'usage, développement généralisé assisté par ordinateur	
5	Etudes d'environnement (CEM, vibrations, etc.)	R	R	HR	HR

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.8 – Documentation de la phase de conception (référencée en 5.2)

	Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1	Description graphique des sous-systèmes	HR	HR	HR	HR
2	Description des interfaces	HR	HR	HR	HR
3	Etudes d'environnement (CEM, vibrations)	R	R	HR	HR
4	Procédure de modification	HR	HR	HR	HR
5	Manuel de maintenance	HR	HR	HR	HR
6	Documentation de fabrication	HR	HR	HR	HR
7	Documentation de l'application	HR	HR	HR	HR

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.9 – Vérification et validation de la conception du produit et du système (références en 5.3.9)

	Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1	Listes de contrôle	R: listes de contrôle préparées, en se concentrant sur les principaux problèmes de sécurité		R: listes de contrôle préparées dans le détail	
2	Simulation		R	R	
3	Essai fonctionnel du système	HR: il convient que des essais fonctionnels et des revues soient menés pour démontrer que les caractéristiques spécifiées et les exigences de sécurité ont été réalisées		HR: il convient que des essais fonctionnels compréhensibles soient menés sur la base de cas d'essais bien définis pour démontrer que les caractéristiques spécifiées et les exigences de sécurité sont réalisées	
4	Essai fonctionnel dans les conditions d'environnement	HR: il convient que l'essai des fonctions relatives à la sécurité et des autres fonctions, dans les conditions d'environnement spécifiées soit mené		HR: il convient que l'essai des fonctions relatives à la sécurité et des autres fonctions, dans les conditions d'environnement spécifiées, soit mené	
5	Essai de l'immunité aux surcharges	HR: il convient que l'essai de l'immunité aux surcharges soit réalisé aux limites des valeurs des conditions d'exploitation réelles	HR: il convient que l'essai de l'immunité aux surcharges soit réalisé au-delà des plus hautes limites des valeurs réelles des conditions d'exploitation		
6	Inspection de la documentation	HR			
7	Assurance que toutes les hypothèses de conception ne sont pas compromises par le processus de fabrication	-		HR: spécifier les précautions et exigences de fabrication, plus audit du procédé réel de fabrication par l'organisation de sécurité	
8	Moyens d'essai	R: il convient que le concepteur des moyens d'essai soit indépendant du concepteur du système ou du produit		HR: il convient que le concepteur des moyens d'essai soit indépendant du concepteur du système ou du produit	
9	Revue de conception	HR: il convient que des revues soient menées à des phases appropriées du cycle de vie pour confirmer que les caractéristiques spécifiées et les exigences de sécurité ont été réalisées		HR: il convient que des revues soient menées à des phases appropriées du cycle de vie pour confirmer que les caractéristiques spécifiées et les exigences de sécurité ont été réalisées	
10	Assurance que les hypothèses de conception ne sont pas compromises par les processus d'installation et de maintenance	HR: spécifier les précautions et les exigences pour l'installation et la maintenance		HR: spécifier les précautions et les exigences pour l'installation et la maintenance, plus audit des processus d'installation et de maintenance réels par l'organisation de sécurité	
11	Haute confiance démontrée par l'usage (optionnel lorsque des preuves précédentes ne sont pas disponibles)	R: 10 000 h de temps d'exploitation, au moins 1 an d'expérience avec les équipements en fonctionnement		R: 1 million d'heures de temps d'exploitation, au moins 2 ans d'expérience avec les différents équipements en incluant les analyses de sécurité, avec la documentation détaillée des changements mineurs réalisés durant le temps d'exploitation	

NOTE Des listes de contrôle, des outils de spécification assistés par ordinateur et une inspection de la spécification peuvent être utilisés pour vérifier les activités d'une phase.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Tableau E.10 – Application, exploitation et maintenance (références en 5.3.12 et 5.4)

	Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4
1	Production d'instructions pour l'exploitation des applications et leur maintenance	R: traçabilité, à partir de la conception, de toutes les instructions pour l'exploitation des applications et leur maintenance, en incluant le registre des situations dangereuses		HR: traçabilité, à partir de la conception, de toutes les instructions pour l'exploitation des applications et leur maintenance, en incluant le registre des situations dangereuses	
2	Formation à l'exécution des instructions d'exploitation et de maintenance (voir 5.4, Partie 5)	HR: formation préliminaire de tous les exploitants et de tout le personnel de maintenance		HR: formation préliminaire puis rafraîchissement périodique des connaissances de tous les exploitants et de tout le personnel de maintenance	
3	Ergonomie de l'exploitant	HR: l'interaction entre le personnel et le système se doit d'être la plus simple possible, afin de réduire le risque d'erreurs humaines			
4	Ergonomie de la maintenance	HR: outils de diagnostic séparé, mesures de maintenance relative à la sécurité aussi rares que possible		HR: des outils de diagnostic portables, suffisants, sensibles et simples doivent être inclus dans les inévitables mesures de réparation, mesures de maintenance relative à la sécurité aussi rares que possible, ou totalement exclus	
5	Protection contre les erreurs d'exploitation	R: contrôles pertinents par procédure sur chacune des entrées de contrôle		HR: contrôles pertinents par procédure sur chacune des entrées de contrôle	
6	Protection contre le sabotage	-		R: des mesures d'organisation additionnelles sont nécessaires	

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Bibliographie

NOTE Les documents suivants ont été consultés durant la préparation de la présente norme (en complément des références normatives énumérées à l'Article 2).

HD 485 S1:1987, Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE) (*CEI 60812:1985*)

HD 617 S1:1992, Analyse par arbre de panne (AAP) (*CEI 61025:1990*)

CLC/SC9XA(SEC)114, Calculation with Mü8004 formulas, August 1994

ISO 9001:1994, Systèmes qualité – Modèle pour l'assurance de la qualité en conception, développement, production, installation et prestations associées

TR 50451, Applications ferroviaires – Allocation systématique des exigences d'intégrité de la sécurité (CENELEC)

UIC/ORE Report A155/RP6, Computer-based safety systems requirements specification, September 1985

UIC/ORE Report A155/RP7, The design of computer-based safety systems, April 1986

UK Health & Safety Executive, Programmable electronic systems in safety-related applications – Parts 1 and 2, 1987

UIC/ORE Report A155/RP11, Proof-of-Safety of computer-based safety systems, September 1987

UIC/ORE Report A155/RP12, Failure catalogue for electronic components, April 1988

MIL-HDBK-338-1A, Electronic reliability design handbook, October 1988

German Federal Railways Mü8004, Principles for the technical approval of signalling and communications technology, January 1991

Reliability Analysis Center Report FMD-91, Failure mode/mechanism distributions, September 1991

IRSE International Technical Committee Report No.1, Safety system validation with regard to cross-acceptance of signalling systems by the railways, January 1992

IS 353: Ferrovie dello stato servizio impianti elettrici: Norme Tecniche IS. 353 Ed. 1985: Norme Tecniche per la presentazione dei prototipi di apparecchiature elettroniche destinate agli impianti di sicurezza e segnalamento.

UIC/ORE A155.3: The use of Electronic Components for Signalling

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.