Nederlandse norm

NEN-EN 50129

(en)

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

Spoorwegen en soortgelijk geleid vervoer - Communicatie, seinwezen en procesleiding - Veiligheidsgerelateerde elektronische systemen voor het seinwezen

Vervangt NEN-EN 50129:2003;
NEN-EN 50129:2003/C1:2010;
NEN-EN 50129:2016 Ontw.;
NPR-CLC/TR 50451:2007;
NPR-CLC/TR 50506-1:2008;
NPR-CLC/TR 50506-2:2010

ICS 93.100

december 2018

Als Nederlandse norm is aanvaard:
- EN 50129:2018,IDT

Koninklijk Nederlands Elektrotechnisch Comité
Normcommissie 364009 'NEC 9 - Elektrisch materieel, systemen en elektronische toepassingen voor spoorwegen en soortgelijk geleid vervoer'

©2018 Koninklijk Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50129

November 2018

ICS 93.100

Supersedes CLC/TR 50451:2007, CLC/TR 50506-1:2007, CLC/TR 50506-2:2009, EN 50129:2003

English Version

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

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik

This European Standard was approved by CENELEC on 2018-06-07. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 50129:2018 E

EN 50129:2018

Contents **Page**

European foreword

This document (EN 50129:2018) has been prepared by CLC/SC 9XA “Communication, signalling and processing systems” of CLC/TC 9X “Electrical and electronic applications for railways”.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2019-05-23
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2021-11-23

This document supersedes EN 50129:2003.

CLC/TR 50451:2007, CLC/TR 50506-1:2007 and CLC/TR 50506-2:2009 are withdrawn by the time the present Publication is published.

The significant technical changes with respect to EN 50129:2003 are the following:

— A better alignment with the life cycle phases described in EN 50126-1:2017 has been made;

  — Clause 5 describes the requirements that apply to the development of safety-related electronic systems (until phase 9 of the life cycle),

  — Clause 8 focuses on the requirements for safety acceptance and approval of safety-related electronic systems and subsequent phases;

— Requirements and guidance have been added in Clause 6 on the following topics:

  — reuse of pre-existing systems,

  — safety-related tools,

  — impact of IT security threats on functional safety,

  — specific application safety cases;

— Requirements for the structure and content of the safety case are now defined in a dedicated Clause 7;

— Annex A has been aligned with EN 50126-2:2017 for the specification and allocation of safety integrity requirements;

— The content of former Annex D has been merged with Annex B, and has been changed from informative to normative;

— The status of the Annex E has been changed from informative to normative;

— An Annex F has been added as an informative annex on User Programmable Integrated Circuits.

A more detailed comparison of changes between EN 50129:2003 and this document can be found in Annex G.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

The structure of this document is described in Clause 4.

This document is intended to be used in conjunction with EN 50126-1:2017, "*Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process*", EN 50126-2:2017, "*Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety*", and EN 50128:2011, "*Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*".

This document has been prepared under the Mandate M/483 given to CENELEC by the European Commission and the Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method (CSM) for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 (with the subsequent amendment, Commission Implementing Regulation (EU) No 2015/1136 of 13 July 2015).

Introduction

This document defines requirements for the acceptance of safety-related electronic systems in the railway signalling field.

The aim of European railway duty holders and of European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of Safety Approvals for systems, subsystems or equipment by the different national railway duty holders is necessary. This document is the common European base for safety acceptance of electronic systems for railway signalling applications.

Cross-acceptance is aimed at the acceptance of generic products or generic applications that can be used for a number of different specific applications, and not at the acceptance of any single specific application. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will refer to this document.

This document is concerned with the evidence to be presented for the acceptance of safety-related systems. However, it specifies not only those life cycle activities which need to be completed before the acceptance stage, but also the additional planned activities to be carried out afterwards. In this way, safety justification will cover the whole life cycle.

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

Safety-related electronic systems for signalling include hardware and software aspects. To develop complete safety-related systems, both aspects need to be taken into account throughout the whole life cycle of the system. The requirements for the overall safety-related electronic system and for its hardware aspects are defined in this document. Other requirements are defined in associated CENELEC standards: for safety-related systems which include software, see EN 50128; for safety-related data communication, see EN 50159.

This document consists of Clauses 1 to 8, which form the main part, and Annexes A, B, C, D, E, F, G and ZZ. The requirements defined in the main part of this document and in Annexes A, B, C and E are normative, whilst Annexes D, F, G and ZZ are informative.

This document is in line with, and uses relevant sections of:

— EN 50126-1:2017, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process,*

— EN 50126-2:2017, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety.*

This document is based on the system life cycle described in EN 50126-1, EN 50126-2 and is in line with the EN 61508 series. EN 50126-1, EN 50126-2, EN 50128, EN 50129 comprise the railway sector equivalent of the EN 61508 series so far as Railway Communication, Signalling and Processing Systems are concerned. When compliance with these documents has been demonstrated, further evaluation of compliance with the EN 61508 series is not required.

1 Scope

This document is applicable to safety-related electronic systems (including subsystems and equipment) for railway signalling applications.

This document applies to generic systems (i.e. generic products or systems defining a class of applications), as well as to systems for specific applications.

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

This document is applicable only to the functional safety of systems. It is not intended to deal with other aspects of safety such as the occupational health and safety of personnel. While functional safety of systems clearly can have an impact on the safety of personnel, there are other aspects of system design which can also affect occupational health and safety and which are not covered by this document.

This document applies to all the phases of the life cycle of a safety-related electronic system, focusing in particular on phases from 5 (architecture and apportionment of system requirements) to 10 (system acceptance) as defined in EN 50126-1:2017.

Requirements for systems which are not related to safety are outside the scope of this document.

This document is not applicable to existing systems, subsystems or equipment which had already been accepted prior to the creation of this document. However, so far as reasonably practicable, it should be applied to modifications and extensions to existing systems, subsystems and equipment.

This document is primarily applicable to systems, subsystems or equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, so far as reasonably practicable, to general-purpose or industrial equipment (e.g. power supplies, display screens or other commercial off the shelf items), which is procured for use as part of a safety-related electronic system. As a minimum, evidence should be provided in such cases (more information is given in 6.2) 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 document is aimed at railway duty holders, railway suppliers, and assessors as well as at safety authorities, although it does not define an approval process to be applied by the safety authorities.

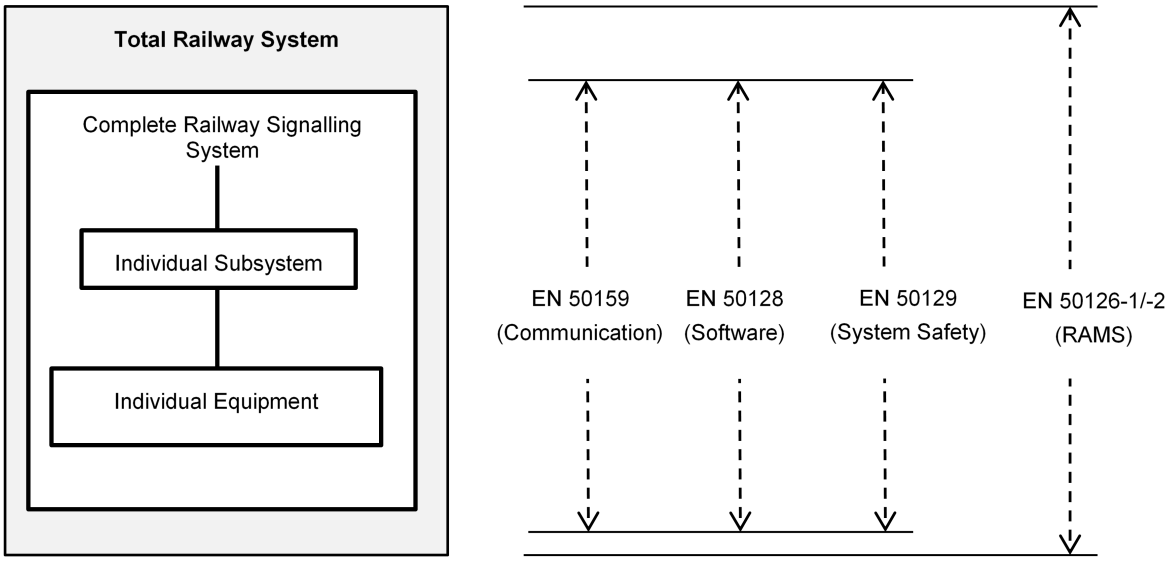


Figure 1 — Scope of the main CENELEC railway application standards

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

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: Rolling stock and on-board equipment*

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

EN 50126-1:2017, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process*

EN 50126-2:2017, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety*

EN 50128, *Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*

EN 60664-1, *Insulation coordination for equipment within low-voltage systems — Part 1: Principles, requirements and tests (IEC 60664-1)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

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

[SOURCE: IEC 60050-821:2017, 821-12-02]

3.1.2
basic integrity
integrity attribute for safety-related functions with a TFFR higher than (less demanding) 10^{-5} h^{-1} or for non-safety-related functions

Note 1 to entry: In this document Basic Integrity requirements relate only to safety-related functions. If a non-safety-related function has been given basic-integrity requirements on the basis of the process described in EN 50126-2:2017, no additional requirements are defined in this document.

[SOURCE: EN 50126-1:2017, 3.7, modified – The note 1 to entry has been added.]

3.1.3
causal analysis
analysis of the reasons how and why a particular hazard can come into existence

[SOURCE: IEC 60050-821:2017, 821-12-07]

3.1.4
common-cause failures
failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause

[SOURCE: IEC 60050-192:2015, 192-03-18]

3.1.5
configuration
structuring and interconnection of the hardware and software of a system for its intended application

[SOURCE: IEC 60050-821:2017, 821-12-12]

3.1.6
consequence analysis
analysis of events which are likely to happen after a hazard has occurred

[SOURCE: IEC 60050-821:2017, 821-12-14]

3.1.7
cross-acceptance
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

[SOURCE: IEC 60050-821:2017, 821-12-15]

3.1.8
design
activity applied in order to analyse and transform specified requirements into acceptable solutions

[SOURCE: IEC 60050-821:2017, 821-12-16, modified – The end of the definition “design solutions which have the required safety integrity level” has been replaced by “solutions”.]

3.1.9
diversity
existence of two or more different ways or means of achieving a specified objective

Note 1 to entry: Diversity is specifically provided as a defence against common cause failure. It can be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

[SOURCE: IEC 60050-395:2014, 395-07-115]

3.1.10
DC fault model
fault category that includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines, and for integrated circuits, short circuit between any two connections (pins)

3.1.11
electronic component
hardware component
electronic device that cannot be taken apart without destruction or impairment of its intended use

EXAMPLE: Resistors, capacitors, diodes, integrated circuits, hybrids, application specific integrated circuits, wound components and relays.

[SOURCE: IEC 60050-904:2014, 904-01-09, modified – “hardware component” has been added as a synonym.]

3.1.12
equipment
single apparatus or set of devices or apparatuses, or the set of main devices of an installation, or all devices necessary to perform a specific task

Note 1 to entry: Examples of equipment are a power transformer, the equipment of a substation, measuring equipment.

[SOURCE: IEC 60050-151:2001, 151-11-25]

3.1.13
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.1.14
fail-safe
able to enter or remain in a safe state in the event of a failure

[SOURCE: IEC 60050-821:2017, 821-01-10]

3.1.15
failure, <of an item>
loss of ability to perform as required

Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

Note 3 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

[SOURCE: IEC 60050-821:2017, 821-11-19, modified – The note 3 to entry has been added.]

3.1.16
failure rate
limit of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval (t, t + Δt) and the duration of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval

Note 1 to entry: For applications where distance travelled or number of cycles of operation is more relevant than time then the unit of time can be replaced by the unit of distance or cycles, as appropriate.

Note 2 to entry: The term “failure rate” is often used in the sense of “mean failure rate” defined in IEV 192-05-07.

[SOURCE: IEC 60050-821:2017, 821-12-21]

3.1.17
fault**, <in a system>**
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

[SOURCE: IEC 60050-821:2017, 821-11-20]

3.1.18
fault detection time
time interval between failure and detection of the resulting fault

[SOURCE: IEC 60050-192:2015, 192-07-11]

3.1.19
function**, <of an item>**
specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input

Note 1 to entry: A function can be specified or described without reference to the physical means of achieving it.

[SOURCE: IEC 60050-821:2017, 821-12-25, modified — The specific use “of a product” and the definition have been made more general, the note 1 to entry has been added.]

3.1.20
functional safety
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351, 351-57-06]

3.1.21
hazard**, <in railway>**
condition that could lead to an accident

Note 1 to entry: The equivalent definition in IEC 60050-903:2013, 903–01–02 refers to “harm” that, with respect to “accident”, does not include loss of system or service.

3.1.22
hazard analysis
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

[SOURCE: IEC 60050-821:2017, 821-11-23]

3.1.23
hazard log
document in which hazards identified, decisions made, solutions adopted, and their implementation status are recorded or referenced

[SOURCE: IEC 60050-821:2017, 821-12-27]

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

[SOURCE: IEC 60050-821:2017, 821-12-29, modified: "physical" has been removed as adjective of "realization".]

3.1.25
independence of roles
freedom from involvement in the same intellectual, commercial and/or management entity

3.1.26
independent safety assessment
process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety

[SOURCE: EN 50126-1:2017, 3.33, modified – The note 1 to entry has been omitted.]

3.1.27
maintenance
combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required

Note 1 to entry: Management is assumed to include supervision activities.

[SOURCE: IEC 60050-192:2015, 192-06-01]

3.1.28
negation
enforcement of a safe state following detection of a hazardous fault

[SOURCE: IEC 60050-821:2017, 821-12-38]

3.1.29
negation time
time interval which begins when the existence of a fault is detected and ends when a safe state is enforced

[SOURCE: IEC 60050-821:2017, 821-12-39]

3.1.30
pre-existing item
item that already exists and that was not developed specifically for the current project

3.1.31
product, <in railway>
collection of elements, interconnected to form a system, a subsystem or an equipment, in a manner which meets the specified requirements

[SOURCE: IEC 60050-821:2017, 821-12-40, modified — The specific use "in signalling" has been made more general with "in railway".]

3.1.32
railway duty holder
body with the overall accountability for operating a railway system within the legal framework

3.1.33
random failure integrity
degree to which a system is free from hazardous random faults

Note 1 to entry: This definition can be read as "integrity from failures due to random faults".

[SOURCE: IEC 60050-821:2017, 821-12-45, modified – The note 1 to entry has been added.]

3.1.34
random fault
unpredictable occurrence of a fault

[SOURCE: IEC 60050-821:2017, 821-12-46]

3.1.35
redundancy, <in a system>
provision of more than one means for performing a function

[SOURCE: IEC 60050-192: 2015, 192-10-02]

3.1.36
reliability, <of an item>
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures.

[SOURCE: IEC 60050-192:2015, 192-01-24]

3.1.37
repair
direct action taken to effect restoration

Note 1 to entry: Repair includes fault localization (SOURCE: IEC 60050-192:2015, 192-06-19), fault diagnosis (SOURCE: IEC 60050-192:2015, 192-06-20); fault correction (SOURCE: IEC 60050-192:2015, 192-06-21); and function checkout (SOURCE: IEC 60050-192:2015, 192-06-22).

[SOURCE: IEC 60050-192:2015, 192-06-14]

3.1.38
risk
combination of the probability of occurrence of accident and the severity of that accident

Note 1 to entry: The equivalent definition in IEC 60050-351:2013, 351-57-03 refers to "harm" that, with respect to "accident", does not include loss of system or service.

[SOURCE: IEC 60050-351:2013, 351-57-03, modified — "harm" has been replaced with "accident" and the note 1 to entry has been added.]

3.1.39
safe state
condition which continues to preserve safety

[SOURCE: IEC 60050-821:2017, 821-12-49]

3.1.40
safety
freedom from unacceptable risk

[SOURCE: IEC 60050-903:2013, 903-01-19]

3.1.41
safety acceptance
safety status given to a product by the final user

[SOURCE: IEC 60050-821:2017, 821-12-50]

3.1.42
safety approval
safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions

[SOURCE: IEC 60050-821:2017, 821-12-51]

3.1.43
safety authority
body responsible for delivering the authorization for the operation of the safety-related system

[SOURCE: IEC 60050-821:2017, 821-12-52]

3.1.44
safety case
documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements

[SOURCE: IEC 60050-821:2017, 821-12-53]

3.1.45
safety integrity
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 duration

[SOURCE: IEC 60050-821:2017, 821-12-54]

3.1.46
safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems

[SOURCE: EN 50126−1:2017, 3.70, modified – The notes to entry have been removed.]

3.1.47
safety life cycle
additional series of activities carried out in conjunction with the system life cycle for safety-related systems

[SOURCE: IEC 60050-821:2017, 821-12-55]

3.1.48
safety plan
documented set of time scheduled activities, resources and events serving to implement the organization, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

[SOURCE: IEC 60050-821:2017, 821-12-57]

3.1.49
safety process
series of procedures that are followed to enable all safety requirements of a product to be identified and met

[SOURCE: IEC 60050-821:2017, 821-12-58]

3.1.50
safety-related
carries responsibility for safety

[SOURCE: IEC 60050-821:2017, 821-01-73]

3.1.51
signalling system
system to ensure the safe movement of trains

Note 1 to entry: For the purposes of this document, railway signalling applications encompass all systems which control and protect train movements by conveying instructions or warnings to trains or trackside systems. Where a signalling system includes subsystems or equipment on board of the train, this document is intended to apply up to the interface with the braking system, traction control system or other relevant train systems.

[SOURCE: IEC 60050-821:2017, 821-01-03, modified — The end of the definition "by means of one or more of the following: lineside indications, wayside/onboard data exchange, indications given in the driver's cab" has been omitted and the note 1 to entry has been added.]

3.1.52
stress profile
degree and number of external influences which a system can withstand whilst performing its required functionality

[SOURCE: IEC 60050-821:2017, 821-12-65]

3.1.53
subsystem
part of a system, which is itself a system

[SOURCE: IEC 60050-192:2015, 192-01-04]

3.1.54
system
set of interrelated elements considered in a defined context as a whole and separated from their environment

[SOURCE: IEC 60050-351:2013, 351-42-08, modified — The Notes to entry have been omitted.]

3.1.55
system life cycle
activities occurring during a given time interval that starts when a system is conceived and ends when the system is no longer available for use, is decommissioned and is disposed of

[SOURCE: IEC 60050-821:2017, 821-12-66]

3.1.56
systematic failure integrity
degree to which a system is free from hazardous systematic faults

Note 1 to entry: This definition can be read as "integrity from failures due to systematic faults", in analogy with source IEC 60050-821:2017, 821-12-46, where "random" is replaced by "systematic"

[SOURCE: IEC 60050-821:2017, 821-12-68, modified — "unidentified hazardous errors and the causes thereof" has been replaced with "hazardous systematic faults" and the note 1 to entry has been added.]

3.1.57
systematic fault, <in signalling>
inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment

[SOURCE: IEC 60050-821:2017, 821-12-69]

3.1.58
technical safety report
documented technical evidence for the safety of the design of a system, subsystem or equipment

Note 1 to entry: The technical safety report is part of the safety case.

[SOURCE: IEC 60050-821:2017, 821-12-70, modified – The note 1 to entry has been added.]

3.1.59
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The term "validated" is used to designate the corresponding status.

Note 2 to entry: The use conditions for validation can be real or simulated.

Note 3 to entry: In design and development, validation concerns the process of examining an item to determine conformity with user needs.

Note 4 to entry: Validation is normally performed during the final stage of development, under defined operating conditions, although it can also be performed in earlier stages.

Note 5 to entry: Multiple validations can be carried out if there are different intended uses.

[SOURCE: IEC 60050-192:2015, 192-01-18]

3.1.60
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The term "verified" is used to designate the corresponding status.

Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement.

Note 3 to entry: Verification is conducted at various stages of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that stage.

[SOURCE: IEC 60050-192:2015, 192-01-17, modified — The note 3 to entry has been modified, "In the case of software," has been deleted and "software and its constituents" has been replaced by "system and its constituents".]

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

CCF Common Cause Failure

COTS Commercial Off The Shelf

DES Designer

DT Down Time, $T_D + T_N + T_R$

EMC ElectroMagnetic Compatibility

EMI ElectroMagnetic Interference

ESD ElectroStatic Discharge

FFR Functional Failure Rate

FMEA Failure Modes and Effects Analysis

FR Failure Rate

FTA Fault Tree Analysis

HAZOP HAZard and OPerability study

HW Hardware

GASC Generic Application Safety Case

GPSC Generic Product Safety Case

IP Intellectual Property

ISA Independent Safety Assessor

MTBF Mean Time Between Failure

PC Programmable Component

PM Project Manager

RAMS Reliability, Availability, Maintainability and Safety

SASC Specific Application Safety Case

SDR Safe Down Rate, inverse of SDT

SDT Safe Down Time, $T_D + T_N$

SIL Safety Integrity Level

SW Software

SRAC Safety-Related Application Condition

TFFR Tolerable Functional (unsafe) Failure Rate

THR Tolerable Hazard Rate

T_D Detection time, interval between failure and fault detection

T_N Negation time, interval between fault detection and fault negation

T_R Repair time, interval between fault negation and fault repair

UIC International Union of Railways

UPIC User Programmable Integrated Circuit

VAL Validator

VER Verifier

4 Overall framework of this document

Clause 5 of this document describes requirements for a systematic, documented approach to:

— quality management,

— safety management,

— functional and technical safety.

Clause 6 describes requirements for supporting elements such as:

— reuse of pre-existing items,

— safety-related tools for electronic systems,

— physical security and IT-security.

Clause 7 describes the safety case including:

— the general structure,

— the technical safety report,

— guidance for specific application safety cases and for dependencies between safety cases.

Clause 8 describes the system safety acceptance process and the following subsequent phases:

— operation and maintenance;

— modification and retrofit;

— decommissioning and disposal.

Annex A (normative) defines the interpretation and use of Safety Integrity Levels.

Annex B (normative) contains detailed technical requirements for safety-related systems, subsystems or equipment.

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

Annex D (informative) contains an example of THR/TFFR/FR apportionment and SIL allocation.

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

Annex F (informative) contains guidance on User Programmable Integrated Circuits.

Annex G (informative) provides traceability of changes between EN 50129:2003 and this document.

Annex ZZ (informative) provides relationship between this document and the Essential Requirements of EU Directive 2008/57/EC.

Bibliography contains references to documents that have been consulted during the preparation of this document.

The structure of this document is illustrated in Figure 2.

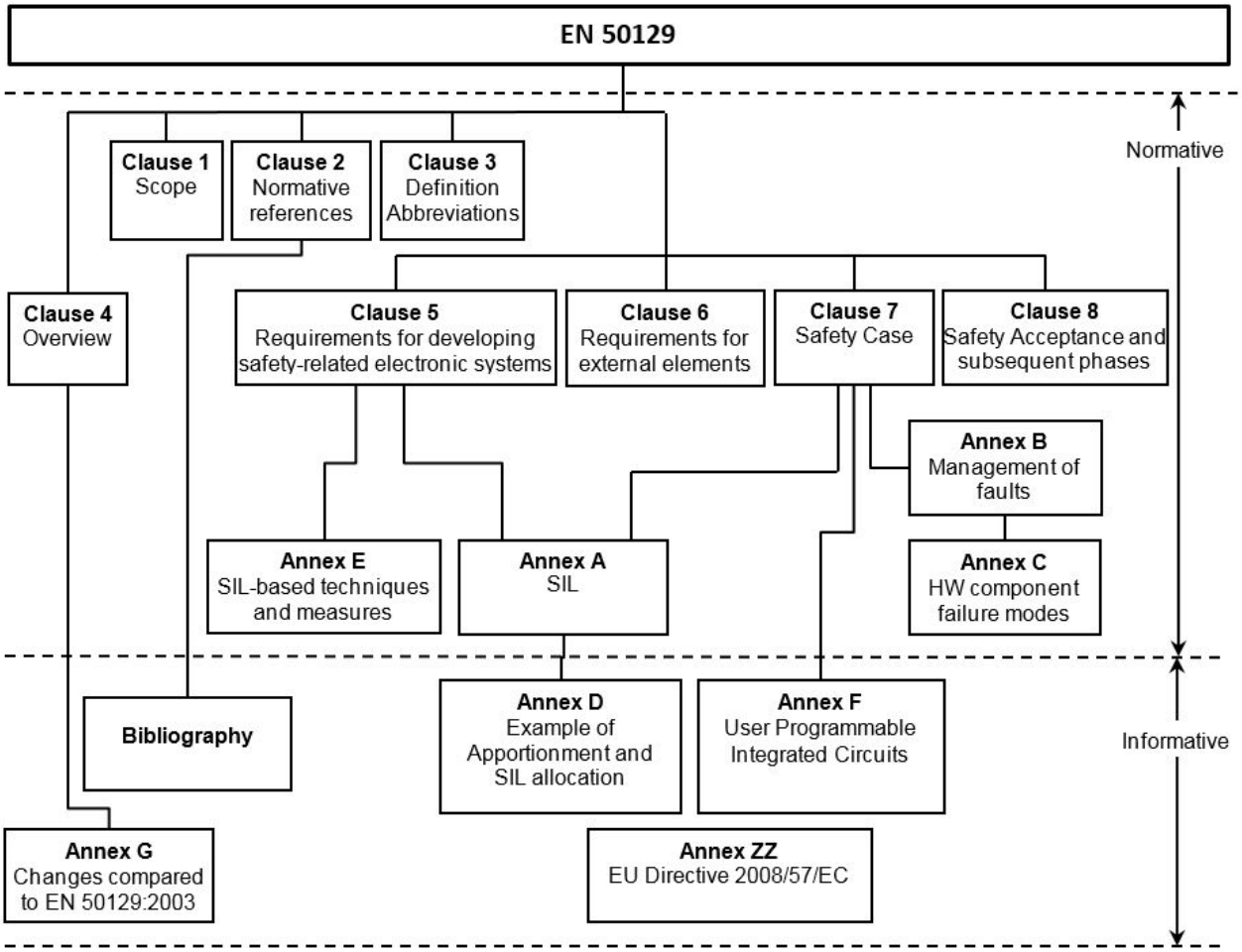


Figure 2 — Structure of EN 50129

5 Requirements for developing safety-related electronic systems

5.1 Introduction

The conditions to be satisfied in order for a safety-related electronic railway system, subsystem or equipment to be accepted as adequately safe for its intended application are:

— fulfilment of quality management process requirements (see 5.2);

— fulfilment of safety management process requirements (see 5.3);

— fulfilment of functional and technical safety requirements and technical evidence for the safety of the design (see 7.2).

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 in order to obtain safety acceptance for a generic product, a class of applications, or a specific application.

5.2 The quality management process

The first prerequisite for safety acceptance is that the quality of the system, subsystem or equipment has been, and continues to be, controlled by an effective quality management system throughout its life cycle.

The purpose of the quality management system is to minimize the incidence of human errors and to improve process performance at each stage of the life cycle, and thus to reduce the risk of systematic faults.

The quality management system shall be applicable throughout the system, subsystem or equipment life cycle, as defined in EN 50126-1. An example of a system life cycle diagram (from EN 50126-1:2017) is reproduced as Figure 3 of this document.

The quality management system should be compliant to EN ISO 9001.

NOTE: Examples of aspects which are typically controlled by the quality management system and included in the Quality Management Report:

— organizational structure;

— quality planning and procedures;

— specification of requirements;

— design control;

— design verification and reviews;

— application engineering;

— procurement and manufacture;

— product identification and traceability;

— handling and storage;

— inspection and testing;

— non-conformance and corrective action;

— packaging and delivery;

— installation and commissioning;

— operation and maintenance;

— quality monitoring and feedback;

— documentation and records;

— configuration management/change control;

— personnel competency and training;

— quality audits and follow-up;

— decommissioning and disposal.

The quality management process shall be applied to all safety-related systems.

Quality management requirements for non-safety-related systems are outside the scope of this document.

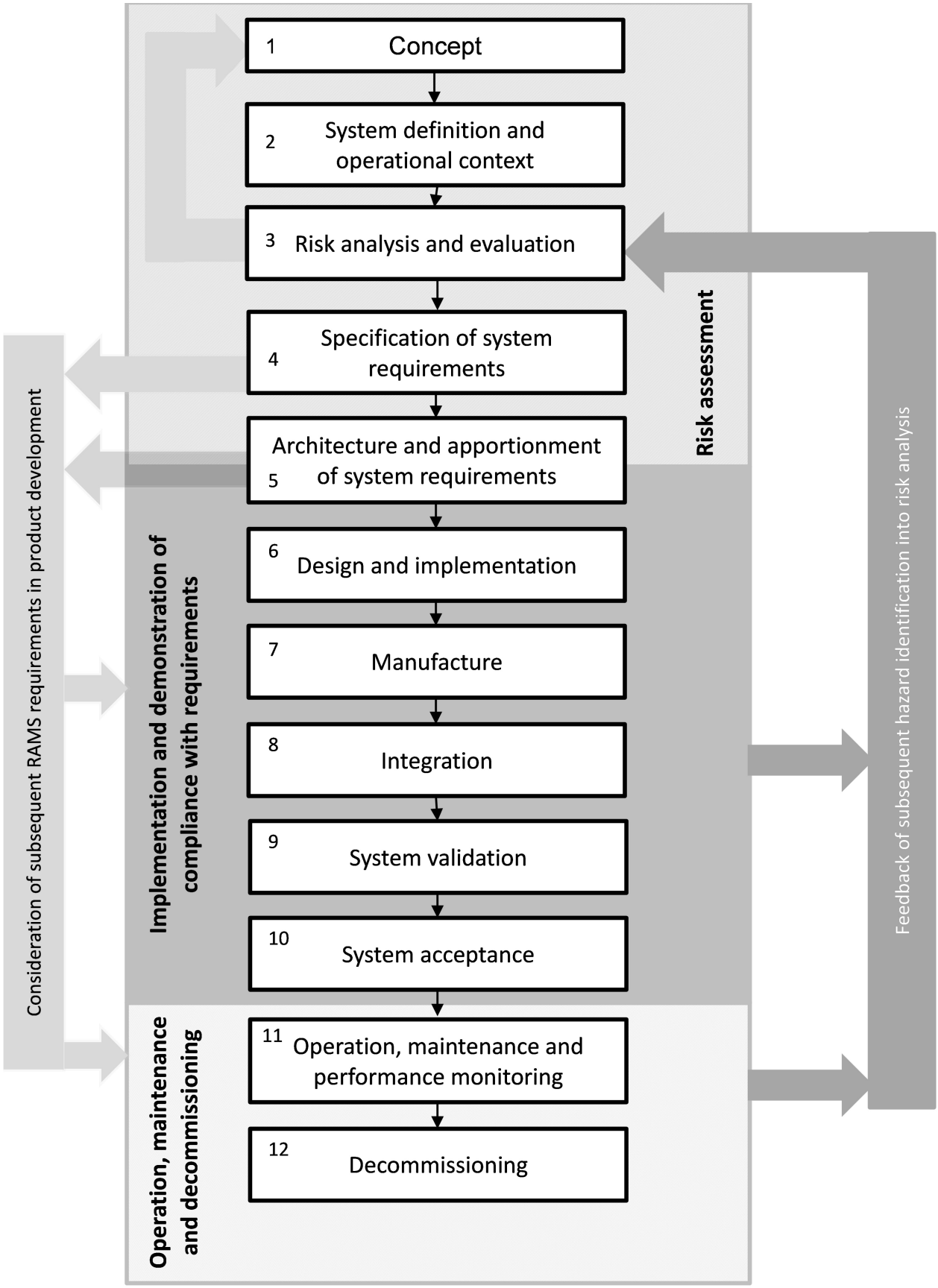


Figure 3 — Example of system life cycle (from EN 50126-1:2017)

5.3 The safety management process

5.3.1 Introduction

The second prerequisite for safety acceptance is that the safety of the system, subsystem or equipment has been, and continues to be, managed by means of an effective safety management process, consistent with the management process for RAMS described in EN 50126-1 and EN 50126-2.

As previously said, the quality management system aims at reducing the risk of systematic faults. The safety management process aims at minimizing the residual risk of safety-related systematic faults and security threats (including IT-Security threats) so far as safety is concerned. The elements of the safety management process are briefly summarized in 5.3.2 to 5.3.14.

The safety management process shall be applied to all safety-related systems. However, the depth of the evidence presented and the extent of the supporting documentation will be appropriate to the degree of safety integrity required to the functions under scrutiny, whether it be Basic Integrity or SIL 1 to SIL 4. See Annex A and Annex E for an explanation of these levels.

Risk Assessment and Hazard Control processes, defined in EN 50126-1 and EN 50126-2, are always necessary in order to identify the appropriate degree of safety integrity for each particular function. This includes those cases where the analysis and assessment reveal that a function can be classified as not safety-related; once this conclusion has been reached, this safety standard ceases to be applicable.

5.3.2 Guideline for structuring documentation

Accurate, clear and complete documentation is essential to ensuring the verification of safety evidence. It is important to ensure that generic guidelines for documentation are defined, covering the following aspects:

— specification of a documentation plan;

— checklists for the contents of documents;

— determination of the form of the document;

— management of the documentation, e.g. with the help of a computer-aided and organized project library.

Measures which can be applied to individual documents or groups of documents include:

— separation of documentation of requirements from development documentation (including internal inspection);

— grouping of development documentation in accordance with the safety life cycle. Some plans and reports which are called for by this document (such as validation, maintenance, operational plans) are not specific to safety and can be grouped with existing project documents, provided that requirements on independence of roles are fulfilled;

— definition of standardized templates, from which the documents can be compiled;

— clear identification of the constituent parts of the documentation;

— formalization of the revision update;

— selection of clear and intelligible means of description, e.g.:

  — formal notation for logical functions,

— natural language for introductions, justifications and representations of intentions,

— graphical representations of examples,

— semantic definition of graphical elements,

— glossary;

— facilitation of impact analysis and updating in case of modification (document breakdown structure);

— avoidance of redundancies.

All safety-related documents, including design documents, shall be classified in accordance with their confidentiality requirements including document storage, access conditions and modification traceability.

5.3.3 Safety life cycle

The safety management process consists of a number of phases and activities, which are linked to form the safety life cycle. The safety management process shall be consistent with the system life cycle defined in EN 50126-1 and EN 50126-2 (see Figure 3).

The design part of the system life cycle can be viewed as a "top-down" sequence of phases followed by integration and validation part as "bottom-up" phases: this is called a "V" representation, an example of which is shown in Figure 4.

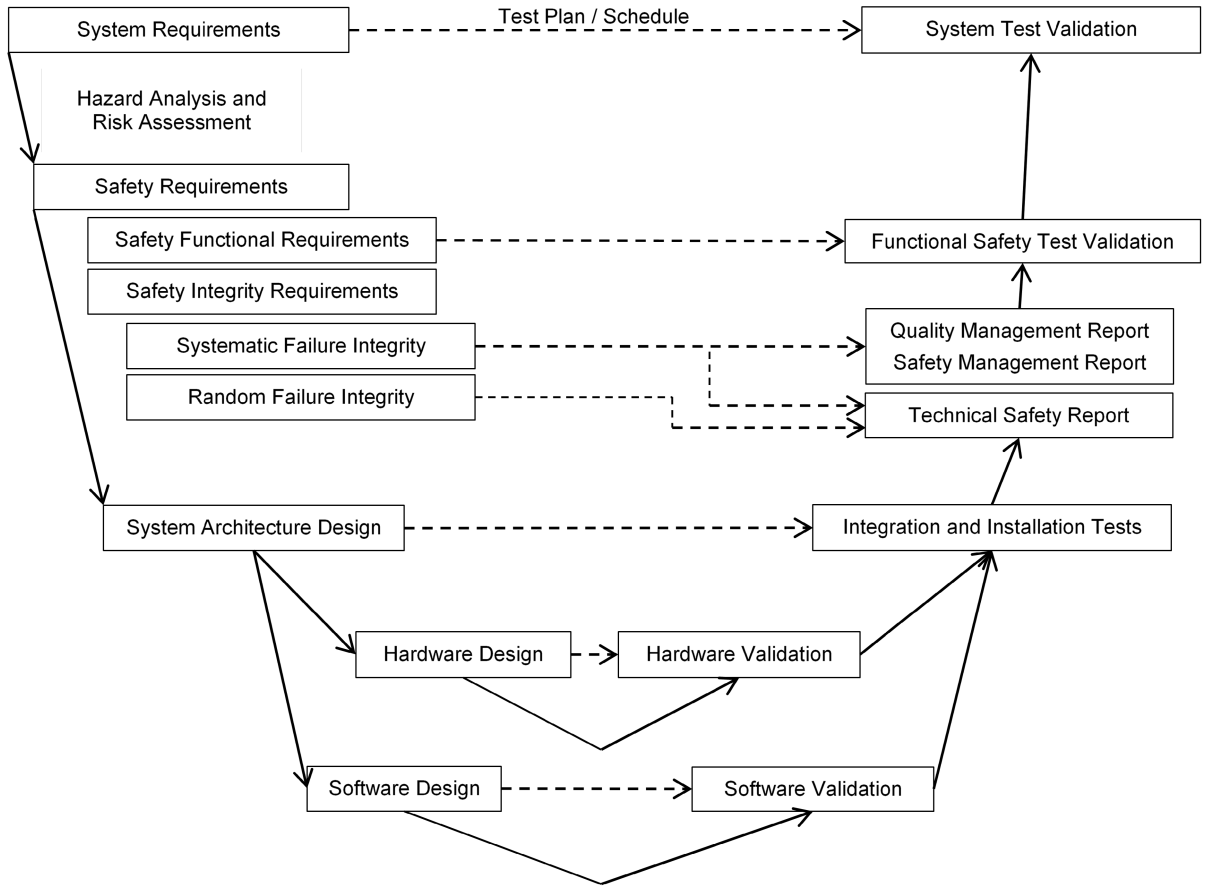


Figure 4 — Example of design and validation portion of system life cycle

5.3.4 Safety organization

5.3.4.1 General requirements

The safety management process shall be implemented under the control of an appropriate safety organization.

Personnel shall be competent to perform the roles they undertake.

Assessment and documentation of personnel competence, including technical knowledge, qualifications, relevant experience and appropriate training, shall be carried out.

A record shall be maintained of the personnel assigned to the roles involved in the development or modification of the system, subsystem or equipment.

An appropriate degree of independence shall be provided between different roles, as defined in 5.3.4.2. These arrangements apply to all the life cycle phases; in some cases they are scaled in accordance with the required degree of safety integrity.

5.3.4.2 Independence of roles

In early phases (phases 1 to 4), the general requirements for independence of roles given in EN 50126-2:2017, 7.2 shall be applied.

For phases 5 to 10, the following requirements apply.

The "project team" is defined as the set of roles comprising typically: project manager, designer, verifier and validator. The Independent Safety Assessor is considered as a role external to the project team.

NOTE In this document, "verifier" and "validator" are terms used to indicate the entities that carry out safety verification and safety validation respectively (see 5.3.10, 5.3.11).

For any SIL from 1 to 4 and for Basic Integrity, the organizational structure of the project team shall comply with the following requirements:

a) A person who is Designer shall not be Verifier for the same system, subsystem or equipment.

b) A person who is Designer shall not be Validator.

c) The Validator shall be given sufficient autonomy and responsibility to reach an independent judgement of the completeness, adequacy and fulfilment of the safety requirements. The Validator shall inform the Project Manager about this judgment.

d) A person who is Validator may also perform the role of Verifier. In this case, as for all other development activities, the safety verification and safety validation outputs shall be reviewed by another competent person.

In addition, for SIL 3 and SIL 4, the organizational structure of the project team shall comply with the following requirement:

e) The Validator shall not report to the Project Manager.

The Independent Safety Assessor shall not report to the Project Manager and shall not be part of the project team. However, the Independent Safety Assessor may be part of any stakeholder organization (e.g. supplier, infrastructure manager, operator) (see 5.3.15).

Requirements on independence of roles are illustrated in Figure 5.

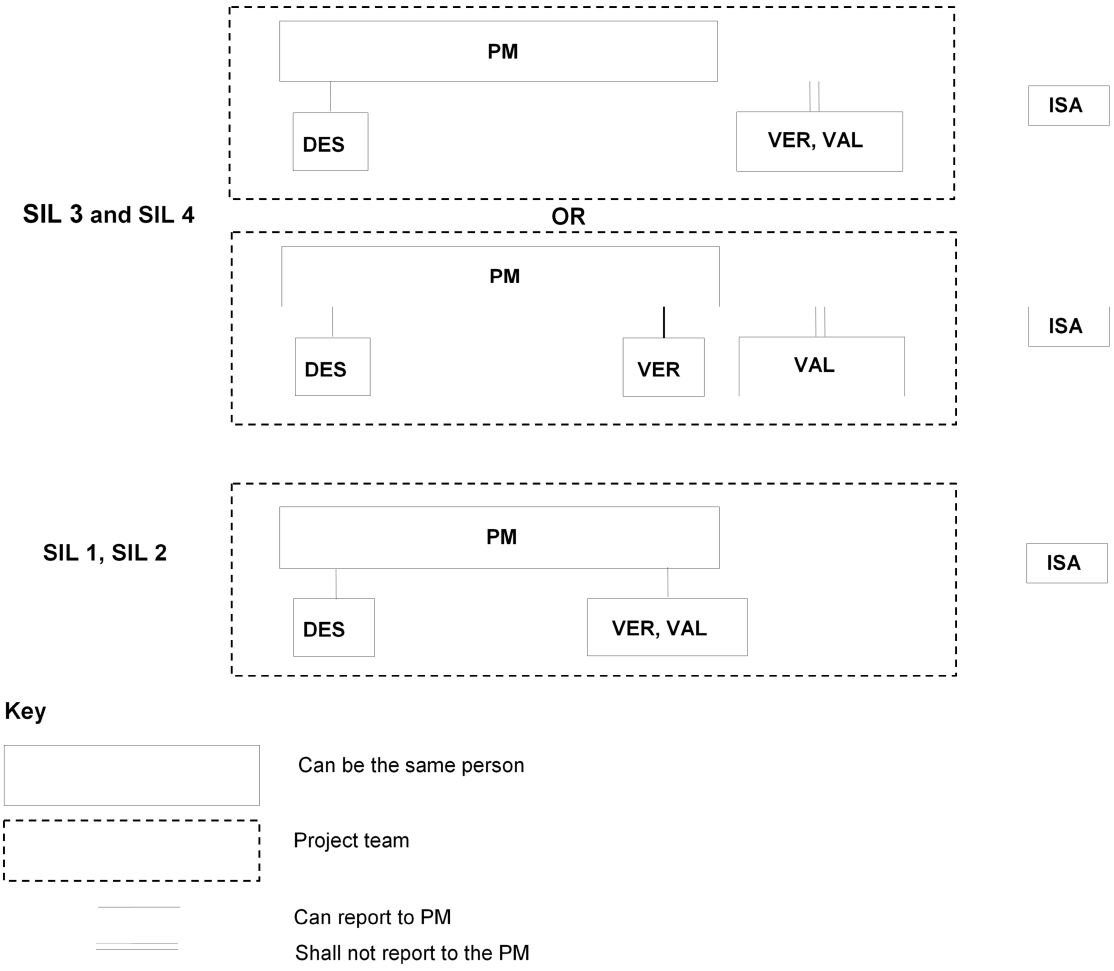


Figure 5 — Independence of Roles for different SILs

5.3.5 Safety plan

A Safety Plan shall be drawn up in the early phases of the safety life cycle, as explained in EN 50126-1:2017, 7.3.2.3. This plan shall identify the structure of the safety management organization, safety-related activities and milestones throughout the life cycle, and shall include requirements for its review at appropriate intervals.

The Safety Plan shall be updated and reviewed if subsequent alterations or additions are made to the original system, subsystem or equipment. If any such change is made, the effect on safety shall be assessed, starting at the appropriate point in the safety life cycle.

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

The Safety Plan shall deal with all aspects of the system, subsystem or equipment, including both hardware and software. EN 50128 shall be referenced for software aspects.

The Safety Plan should include a Safety Case Plan which identifies the scope of the Safety Case, its structure, the possible underlying safety cases, the people responsible and the timescale for its production.

The Safety Plan shall include or reference safety verification planning for verifying that each phase of the life cycle satisfies the specific safety requirements identified in the previous phase, and safety validation

planning for validating the completed system/subsystem/equipment against its original Safety Requirements Specification.

5.3.6 Hazard log

A Hazard Log shall be created and maintained throughout the safety life cycle, as explained in EN 50126-1 and EN 50126-2. 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 alteration or addition is made to the system, subsystem or equipment.

5.3.7 Safety requirements specification

The specific safety requirements for each system, subsystem or equipment, including requirements for safety functions and associated safety integrity requirements, are identified and documented in the safety requirements specification. This is achieved, as explained in EN 50126-1 and EN 50126-2, by means of:

— Hazard Identification and Analysis,

— Risk Assessment,

—- allocation of Safety Integrity Levels.

See A.2 for a possible classification of safety requirements.

The safety requirements specification may be included in the system, subsystem or equipment functional requirements specification or may be written as a separate document.

See Table E.2 for guidance on safety requirements specifications for each Safety Integrity Level.

5.3.8 System design for safety

During life cycle phases 5 (architecture and apportionment of system requirements) and 6 (design and implementation) a design shall be created 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 the software/hardware integration specification) shall be strictly managed, and the standard EN 50128 shall be adhered to.

During life cycle phases 5 and 6, targets for tolerable failure rates are given on the basis of the selected architecture, and Safety Integrity Levels allocated to functions, as explained in Annex A.

At least the following documentation shall be provided:

— description of system architecture and functional behaviour (this can be a system architectural design specification refining the previous safety requirements specification);

— safety-related design principles;

— description of interfaces;

— modification procedures;

— manufacturing documentation for this system;

— application documentation.

NOTE: Maintenance capability and achievement of maintenance goals strongly depend on how the system is designed. "Design for maintainability" is an important aspect of the development life cycle and can be characterized by

adoption of design techniques and measures such as: structured design, interface property definition and verification, modularity, preparation for obsolescence treatment or for evolution of the technology (see also Annex E).

The Tables E.5 and E.7 give guidance, for each Safety Integrity Level, on design and development of the system, subsystem or equipment.

5.3.9 Safety operation and maintenance plan

The operational and maintenance activities necessary to ensure continued safe and correct functioning of the system, subsystem or equipment within the specified environmental conditions shall be planned in the form of an Operation and Maintenance Plan.

Rules, conditions and constraints for operational safety monitoring shall be documented. They shall describe those aspects which need to be monitored during the operation and maintenance phase in order 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 can 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.

5.3.10 Safety verification

The objective of safety verification is to demonstrate that the deliverables of each phase meet in all respects the safety-related requirements of that phase.

Scope, activities and methodologies of safety verification, from concept to integration life cycle phases, shall be planned and documented.

In each life cycle phase, safety verification activities shall include the following:

— evaluation of the correctness and adequacy of the hazard analyses;

— verification of the deliverables of the phase for compliance with the deliverables of former phases;

— verification of the deliverables and inspection of the documentation, for compliance with the requirements for the phase in question;

— evaluation of the adequacy of the methods, tools and techniques used within the phase;

— evaluation of the correctness, consistency and adequacy of test cases and executed tests.

Hazard analyses, testing and documental review are the main activities within safety verification.

Hazard analyses, test plans and test specifications for safety verification shall either be written by the verifier or reviewed and agreed by the verifier.

Test plans and test reports shall be established and shall include:

— responsibility for test definition and execution;

— version of the test specification used;

— version of element (HW and SW) used;

— tools and equipment used;

— version of configuration data used;

— version of tools used;

— test results, including any discrepancies between expected and actual results.

Results of the planned safety verification activities shall be documented, including:

— identity and configuration of the items verified;

— items which do not conform to the specifications;

— detected errors or deficiencies;

— the fulfilment of, or deviation from, the safety verification planning;

— summary of the verification results, highlighting those results that have to be forwarded for further and more detailed analysis.

Table E.8 gives guidance on safety verification techniques and measures for each Safety Integrity Level.

5.3.11 Safety validation

The objective of safety validation is to demonstrate that:

— the safety-related requirements are specified, implemented and verified;

— the system under consideration fulfils the related safety target and is suitable for its intended use within the defined environment.

Scope, activities and methodologies of safety validation in all relevant life cycle phases shall be planned and documented.

The safety validation planning shall define or reference a summary justification of the validation strategy chosen, including consideration of:

— manual or automated techniques or both;

— static or dynamic techniques or both;

— analytical or statistical techniques or both;

— testing in a real or simulated environment or both.

The validator may require or perform reviews, analyses and tests, at appropriate stages in the safety life cycle, to confirm that the specified characteristics and safety requirements have been achieved. Hazard analyses, test plans and test specifications for safety validation shall either be written by the validator or reviewed and agreed by the validator.

The validator shall ensure that design concepts are not compromised by manufacturing, installation, maintenance and operation processes. To this aim, the validator shall review requirements, safety-related application conditions and precautions, and audit these processes.

The validator shall evaluate the processes of development, installation, commissioning and safety verification and make a statement on different aspects such as:

— conformity with the requirements defined in this document;

— consistency of plans, reports and deliverables;

— correctness of the results;

— adequacy of the system under consideration for meeting its safety requirements.

Results of the safety validation activities shall be documented in a safety validation report.

The safety validation report shall identify and name:

— the version of the system under consideration;

— documents and other items used for the validation;

— processes, technical support tools and equipment used, along with calibration data;

— the simulation models used if any.

The safety validation report shall evaluate:

— completeness of tracing of requirements in development and verification;

— completeness of validation of requirements by tests and/or analyses.

The safety validation report shall record and justify:

— deviations from the validation planning;

— deviations between expected and actual results of the tests and/or analyses;

— non-compliances, safety constraints and safety-related application conditions derived from these deviations.

The safety validation report shall present a conclusion based on the validation results and state whether the system under consideration is fit for its intended use in the defined environment, with respect to safety.

Table E.8 gives guidance on safety validation techniques and measures for each Safety Integrity Level.

5.3.12 Safety qualification tests

The purpose of the safety qualification tests is to:

— increase confidence that the system, subsystem or equipment fulfils its specified operational requirements,

— increase confidence that the specified reliability and safety targets will be achieved,

— allow systems, subsystems or equipment to be put into operational service before final safety approval, subject to provision of appropriate precautions and monitoring.

The extent and duration of the safety qualification tests shall be agreed between the railway duty holder and the supplier, and shall be justified having regard to the degree of novelty and complexity associated with the system, subsystem or equipment.

Specific Application Safety Cases may refer to other Specific Application Safety Cases in order to avoid test duplication. Before the qualification tests, a record shall be produced explaining conditions and restrictions to be followed in order to control any residual hazards.

The safety of the system is not fully assured during the test period because it depends on evidence from the safety qualification tests. Therefore appropriate precautions, procedures and monitoring shall be provided, to protect from possible hazards not yet closed.

The defined safety qualification tests shall be completed before commencing operation of the system with full responsibility for safety.

Following qualification tests, a statement shall be produced to record the conditions to operate the system and what authorization level has been obtained (provisional or final safety approval).

An account of the safety qualification tests, including a full description of the tests carried out and the results obtained, shall be documented in Section 6 of the Technical Safety Report (see 7.2).

5.3.13 Management of Safety-Related Application Conditions

A necessary pre-requisite in the development of safety-related systems is the management of Safety-Related Application Conditions (SRACs).

This subclause covers the general requirements for the establishment and verification of SRACs.

The SRACs establish the assumptions and conditions that need to be satisfied to mitigate risks when the system under consideration is integrated in an overall system. Correct handling of SRACs is a precondition for safe integration.

Compliance with SRACs supports the safety demonstration and is thus a necessary part of the superordinate level Safety Case. SRACs whose observance is necessary to the continued safe operation of the system shall be passed on to the final user (Operator / Maintainer).

NOTE 1 Systems which are more generic usually require more SRACs due to the unknown usage conditions of the system and the resulting constraints and assumptions necessary on safety analysis.

NOTE 2 If an item has many SRACs, then there are many dependencies with other items, and the effort needed to integrate the item in a wider system can be high. The modular design of a system using several suppliers could need significant workload to ensure adequate management of SRACs.

This effort can be decreased by avoiding aspects such as the following:

— declaring SRACs that in fact are not SRACs (e.g. information on system characteristics),

— declaring SRACs that could have been avoided through design,

— SRACs requiring information that is incomplete or missing,

— SRACs that are impossible or unreasonable to apply,

— SRACs with insufficient clarity for the user, e.g. due to language problems or ambiguities,

— SRACs erroneously considered as applied but not actually implemented, leading to safety deficiencies.

Each SRAC shall be linked to at least one hazard.

NOTE 3 This means that, if a SRAC is not fulfilled, a hazard can occur as a consequence; or that the probability that a hazard occurs can significantly increase. If such a hazard cannot be identified, then either the rule is not a SRAC or the hazard analysis is not complete.

Hazards could be identified that are not adequately handled within the boundaries of the item. In these cases an SRAC shall be created whenever a safety requirement cannot be completely fulfilled (and related hazards closed).

NOTE 4 No SRAC is required when the related hazard is being avoided by compliance to general legal or normative rules relevant for the intended use of the item (i.e. the Safety Case does not need to repeat SRACs that are general legal/normative rules to be followed by the users).

The SRACs shall:

— be uniquely identifiable (at least within an organization) both in records/documents and support tools used in the project;

— have an identified receiver or class of receivers or entity (e.g. application engineer, operator, maintainer);

— be self-evident (e.g. understandable without access to other documents), unambiguous, complete, suitable for auditing;

— not contain references that the receivers of the SRACs are not able to access;

— be consistent in all languages in which they are written.

The SRACs should:

— have a short title so to support sorting and analysis of contents;

— be kept to the minimum necessary list, eliminating redundancies among them;

— be available in a language known by the user who is asked to comply with them;

— be compiled within a single separate document;

— be provided with examples of how it might be possible to comply with them or, where known, how compliance has been handled in previous projects.

Within SRAC management, SRACs imported from related Safety Cases shall be shown to have been either closed, with relevant evidence being provided, or re-exported (completely or partially) to subsequent users.

The same processes for traceability, verification and validation should be used as for safety requirements.

An example of a template that may be used for writing SRACs is provided in Table 1.

Table 1 — Example of SRAC template

Identifier	Unique identifier
Title	Short title (useful to promptly recall or sort out the SRAC)
Origin	Indication of originating activity / document
Hazard(s)	Indication of related hazard(s)
Receiver	Indication of phase/entity (e.g. application design, installation, maintenance) receiving the SRAC
Text	Text of the SRAC
Verification	Examples of how it might be possible to comply with the SRAC (test, inspection, specific documentation). Examples based on past projects experience can be given where/when available

5.3.14 Safety justification

The evidence that the system, subsystem or 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 Clause 7.

5.3.15 Independent safety assessment

Independent safety assessment is the formation of a judgement, separate from and independent of any system design, development, operational and maintenance personnel.

The independent safety assessment shall assess whether:

1) the requirements given in the present document have been complied with;

2) the safety process has been adequately implemented;

3) the system under consideration is fit, from the point of view of safety, for its intended purpose.

The independent safety assessment is not restricted to document review. The independent safety assessment may be performed by more than one Independent Safety Assessor.

The Independent Safety Assessor shall be accepted by the railway duty holder in accordance with the legal framework, or have acceptance within the legal framework.

The Independent Safety Assessor shall be free to decide on the appropriate assessment methods, such as interviews, analyses, audits, witnessing tests, physical inspections.

The Independent Safety Assessor should ensure as soon as possible that appropriate persons are notified when a safety concern outside the Assessor's remit is identified.

For Basic Integrity, the Independent Safety Assessor shall only evaluate the conformity and correctness of the process up to the SIL allocation (life cycle phases 4 and 5). No further activity is needed.

NOTE For further information regarding Basic Integrity see Annex A and EN 50126-2:2017.

Results from the independent safety assessment shall be presented in a report. The report shall explain the activities carried out by the Independent Safety Assessor to determine whether the system under consideration has been designed in a way that meets its specified requirements. The report may specify possible additional conditions for the operation of the system.

6 Requirements for elements following different life cycles

6.1 Introduction

The safety of the system under consideration can rely on the specific properties of elements that have their own life cycle independent of the safety life cycle (see 5.3.3):

— use of pre-existing systems which have been already developed and cannot be changed for the system under consideration (see 6.2);

— tools which are used off-line with respect to the system under consideration (see 6.3);

— IT-Security, which is managed within its own framework (see 6.4).

All these supporting elements can have influence on functional safety; evidence of their contribution shall be integrated in the overall Safety Case (see Clause 7).

6.2 Use of pre-existing items

6.2.1 Introduction

This subclause sets out the issues associated with use of "pre-existing items" (items that already exist and that were not developed for the current project) which both:

1) are complex (in the sense that a complete and deterministic functional model of the item is not possible or not completely available); and

2) have not been developed in accordance with this document or to its previous versions.

NOTE 1 Items here considered can vary from equipment to subsystems or even complete systems. For instance: monitors, modems/switches/routers, operating systems, electronic boards, industrial or personal computers, etc.

As for other types of items:

— hardware components are considered non-complex and are not addressed here. For these components there is no need to express specific requirements in addition to those already given in the rest of this document (see Annex C);

— items that were compliant with previous versions of this document, when developed, shall be accepted without additional demonstration.

Not having been developed in accordance to this document, pre-existing items could have one or more of the following deficiencies.

— Lack of process evidence:

  — evidence of quality management and safety management is missing or at least not provided in a structured safety case;

  — sufficient freedom from systematic faults is not ensured, because the development process was not oriented to functional safety.

— Lack of technical evidence:

  — evidence of functional and technical safety is missing or at least not provided in a structured safety case;

  — some properties and functionalities are completely or partially unknown, or not guaranteed from the safety point of view;

  — control of systematic and random failures is not ensured, because the design was not safety-oriented and no embedded measures for fault tolerance and fault management were provided.

Due to these deficiencies, using pre-existing items to realize a safety-related function within the system under consideration would normally not be efficient, since the safety demonstration could be particularly onerous. There are however two classes of items for which reuse can still be efficient:

a) complete pre-existing systems that perform one or more safety-related functions and were developed in accordance with other safety standards.

In this case, the above potential deficiencies could be mostly formal and identifying and managing possible gaps could be deemed feasible. See 6.2.2.

b) pre-existing equipment, that performs only part of a safety-related function.

In this case, the above potential deficiencies shall be treated in accordance with 6.2.3.

NOTE 2 This is the case, for instance, of COTS (i.e. products used within the market in large quantities). Use of COTS has often no practicable alternatives, since development of bespoke products could be too expensive, or ineffective to defend against systematic faults due to the limited railway market, or even impossible to get, due to the highly advanced technology.

6.2.2 Requirements for use of complete pre-existing systems

To use complete pre-existing systems that perform one or more safety-related functions and were developed in accordance with other safety standards, the following requirements apply.

1) Existing evidence shall be traced.

2) Identified gaps shall be closed in accordance with the requirements of this document.

3) In case of SIL 1 to SIL 4, an independent safety assessment shall guarantee that these measures have been applied sufficiently to get compliance with this document.

6.2.3 Requirements for use of pre-existing equipment

When using pre-existing equipment that performs only part of a safety-related function, the equipment shall be correctly integrated in the technical and procedural safety management. To this end, the following requirements apply.

1) A minimum set of information shall be available:

   — functionality;

   — interfaces;

   — hardware and/or software constraints;

   — failure rate of the equipment;

   — environmental conditions and other conditions of use.

2) The equipment shall be identified, included in the overall system definition and put under configuration control.

3) The hazardous functional failure modes shall be identified. These failure modes should be identified by an interface hazard analysis. An alternative would be to use a Failure Modes and Effects Analysis, but this method might not be feasible in many cases due to excessive complexity of the equipment or lack of information on its design (e.g. in a case where only the minimum set of information is available).

4) For each hazardous functional failure mode identified at the boundary of the equipment, that would require a safety-related function with a safety integrity level from 1 to 4 or Basic Integrity, the following alternatives apply:

   4.1) it shall be demonstrated that the hazardous functional failure mode cannot credibly occur, due to the internal architecture, the data structure or inherent physical properties; or

   4.2) complete safety demonstration shall be provided for the pre-existing equipment in accordance with the required SIL; or

   4.3) the failure mode shall be externally negated and a safe state shall be enforced within the required time to fulfil the required safety target.

NOTE: This is in analogy to what is required in B.3.1.

5) Failure modes observed at the boundary of the equipment are not always traceable to their actual causes. Therefore, for any equipment performing a SIL function, when it is not possible to identify the components of the equipment having a failure mode contributing to the hazard, the full failure rate of

the equipment is used. This failure rate shall be demonstrated to be compatible with the TFFR required for the complete function.

6) At the system level, when the pre-existing equipment is integrated in the system under consideration, all design, safety verification, safety validation and assessment activities shall be performed encompassing the pre-existing equipment as a black-box.

7) For all SIL, a strategy shall be defined to manage the possible effects of product changes (e.g. disable automatic software updates).

6.3 Safety-related tools for electronic systems

This subclause deals with tools which perform or support activities in any of the life cycle phases, and which can directly or indirectly affect safety.

Tools that can directly affect safety are those tools which generate outputs that contribute to the design or implementation of a safety-related function, and whose errors could directly lead to a systematic hazardous fault in the product or application.

Tools that can indirectly affect safety are those tools which support the safety verification of the design or implementation of a safety-related function, and whose errors do not directly lead to a systematic hazardous fault in the product or application, but rather might affect the detection of other errors from other sources.

EXAMPLE 1 Tools which might directly affect safety:

a) Transformation or translation tools that convert a system and/or software / hardware component design representation (e.g. a diagram) from one abstraction level to another;

b) tools which generate detailed designs from a combination of generic rules and specific application data and parameters. Such tools for signalling systems would include tools for designing block-sectioning and safety distances and tools for generating signalling control tables;

c) circuit design tools which calculate component parameter values and tolerances needed to meet a given performance specification;

d) tools that produce or maintain data which are required to define parameters and to instantiate system and/or software/hardware components functions, e.g. transmission rates, clock rates, communication parameters, measuring instruments, calibration tools;

e) some verification and validation tools used within an integrated development framework, such as modelling tools and formal checkers.

EXAMPLE 2 Tools which might indirectly affect safety:

a) verification and validation tools, such as testing tools;

b) diagnostic tools used to maintain and monitor the system and/or software/hardware components under operating conditions;

c) configuration control tools such as version control tools;

d) tools for managing and tracing requirements;

e) tools to assist safety case preparation, e.g. text, spread sheets or diagram editors;

f) measuring instruments (physical or electrical);

g) standard office software.

Support tools for software development are out of scope of this subclause and covered by EN 50128.

Tools should be selected in accordance with needs related to development or manufacturing activities relating to system software/hardware. The selected tools should be able to cooperate. In this context, tools cooperate if the outputs from one tool have suitable contents and format for automatic input to a subsequent tool, thus minimizing the possibility of introducing human errors in the reworking of intermediate results.

The availability of suitable tools to supply their services over the whole lifetime of the system should be considered.

Additionally, for those tools that can directly affect safety, the following requirements apply:

1) Hazard identification and hazard analysis shall be applied to the tools and the processes in which they are used, in order to identify how they might affect safety and to define related safety requirements.

2) The safety validation of the respective generic product, generic application or specific application shall confirm that all tools and related processes meet their safety requirements and have been correctly applied in the related life cycle activities.

3) One of the following techniques shall be followed:

   a) Verification of tool output

   To achieve verification of the output, the output is subjected to a combination of tests, analyses and checks (including reading and visual inspection), which are capable of ensuring the correctness of the output to an extent consistent with the target Safety Integrity Level. In particular, the following applies to all tests, analyses and checks.

   — Testing has a sufficiently high coverage of the functions and of their domains.

   — Test, checks and analyses are applied to the output and are shown to be capable of detecting the types of errors which might result from the tool.

   b) Tool proven in use

   A tool is proven in use if the following conditions apply.

   — It has been confirmed and periodically checked by analysis, examination and provision of objective evidence that the tool is suitable for the purpose for which it is to be used.

   — There is sufficient qualitative evidence from previous use to show that the output of the tool can be trusted, including a suitable combination of documented history of successful use (project and applications realized, list of anomalies, identification of successive versions).

   c) Tool proven by analysis and testing

   The tool is proven by analysis and testing; results are documented addressing:

   — the version of the tool and the specification or the manual being used;

   — the tool functions being analysed and tested;

   — testing tools and equipment used;

   — test cases and their results for subsequent analysis;

— discrepancies between expected and actual results;

— the conclusions, stating either that the tool has passed the analysis and test or the reasons for its failure and/or the conditions under which the tool can be used.

d) Tool diversity

Tool diversity is achieved by one or more of the following means.

— Use of two diverse tools to perform the same function, with comparison of their outputs.

— Use one tool to perform the function and feed its output into a diverse tool which regenerates the input data provided to the first tool, with comparison of the original and regenerated input data.

— Use one tool to perform the function and subject its output to verification of results by an independent tool, which is diverse from the first tool because it works in accordance with different principles, for example a rule-checking tool to confirm that the output conforms to all relevant rules (e.g. rules for the positioning of balises).

e) Tool with appropriate SIL

The tool has been designed, implemented and validated to achieve the level of safety integrity needed to fulfil the safety requirements defined for the tool.

6.4 Physical security and IT-Security

There are two kinds of threats resulting from unauthorized access to signalling equipment:

1) Physical security threats.

   It is established good practice to protect systems from direct access to signalling equipment, which could allow unauthorized persons to cause (intentionally or unintentionally) functional safety hazards.

2) IT-Security threats.

   Modern IT communication concepts result in the need to protect those systems also against logical access via IT systems.

   EXAMPLE: An IT communication system might enable a remote attacker to manipulate a signalling system and affect functional safety.

IT-Security is a rapidly evolving field. IT-Security can affect not only the service but also functional safety of a signalling system. However, there is no inherent relationship between security and safety requirements.

Several standards exist which give detailed advice on how to deal with IT-Security threats. These standards are also valuable when considering impacts on functional safety, which are simply additional effects of threats generally regarded within IT-Security.

This document does not specify the requirements for the development, implementation, maintenance and/or operation of security policies, security services or security systems, for which appropriate IT-Security standards are applicable.

NOTE 1 IEC/ISO standards that address IT-Security in depth are ISO 27000ff, ISO/IEC/TR 19791 and the IEC 62443 series.

NOTE 2 Measures used to achieve a certain SIL will not necessarily ensure security and, on the other side, the concept of SIL is not intended to be applied to IT-Security requirements.

NOTE 3 Typical consideration of security versus safety is the need for fast security updates of SW arising from security threats, whereas if such SW is safety-related, it is thoroughly developed, tested, validated and approved before any update.

IT-Security threats shall be managed during the Risk Assessment and Hazard Control (or existing analyses shall be referenced), if an impact of IT-Security issues on functional safety is reasonably foreseeable and cannot be excluded by simple arguments (e.g. a system having no connection to untrusted networks).

Measures addressing security shall be recorded or referenced in the Safety Case (section 4.5 of the Technical Safety Report, as described in 7.2).

NOTE 4 Similar to systematic errors, probabilistic evaluation of IT-Security threats is considered infeasible.

NOTE 5 Requirements for safety-related data communication, given in EN 50159, cover some aspects of IT-Security.

7 The Safety Case: structure and content

7.1 The Safety Case structure

The essential evidence to be satisfied before the system under consideration can be accepted as adequately safe for its intended applications comprises:

— evidence of quality management;

— evidence of safety management;

— evidence of functional and technical safety.

The Safety Case contains this documented safety evidence for the system, subsystem or equipment under consideration.

Figure 6 — Structure of Safety Case

Detailed evidence and supporting documentation need not to be included in the Safety Case, provided precise references are given to such documents and provided the base concepts used and the approaches taken are clearly specified. Those referenced documents shall be made available to the independent safety assessor.

The structure of the Safety Case is illustrated in Figure 6.

The Safety Case shall be arranged under the following headings:

Part 1 — Definition of system

This shall precisely define or reference the system, subsystem or equipment to which the Safety Case refers, including version numbers and modification status of all requirements, design and application documentation.

When the Safety Case is issued or re-issued due to a change or reconfiguration, a delivery sheet or a release note reporting the complete configuration shall be referenced here. The delivery sheet or release note shall also list the current and previous versions of all the modified products and applications.

Part 2 — Quality Management Report

This part shall provide documentary evidence to demonstrate the effectiveness of the quality management system, as specified in 5.2.

Part 3 — Safety Management Report

This part shall provide documentary evidence to demonstrate compliance with all elements of the safety management process throughout the life cycle, as specified in 5.3.

Part 4 — Technical Safety Report

This part shall provide technical evidence for the safety of the design. For detailed requirements see 7.2.

Part 5 — Related Safety Cases

This part shall contain references to the Safety Cases of any system, subsystems or equipment on which the system under consideration depends.

It shall also demonstrate that all the safety-related application conditions specified in those Safety Cases have been either:

— fulfilled in the system under consideration; or

— carried forward as safety-related application conditions (and therefore recorded in Section 5 of the Technical Safety Report, see 7.2).

When the Safety Case includes other Generic (Product or Application) Safety Cases, the version of the related products/applications shall be reported here.

Part 6 — Conclusion

This shall summarize the evidence presented in the previous parts of the Safety Case, and argue that the relevant system, subsystem or equipment is adequately safe, subject to compliance with the specified application conditions.

7.2 The Technical Safety Report

Technical evidence for the safety of the design shall be documented in the Technical Safety Report, which forms Part 4 of the Safety Case.

The depth of the information and the extent of the supporting documentation should be appropriate to the Safety Integrity Level.

For safety-related Basic Integrity functions, the detailed structure given in this subclause is not required for the Technical Safety Report. However, the following requirements apply and shall be covered in a Technical Safety Report:

— fulfilment of system and safety requirements of these functions shall be demonstrated, e.g. by reference to a validation report;

— fulfilment of TFFRs shall be justified;

— environmental conditions and SRACs shall be specified;

— safety-related Basic Integrity functions shall be part of the safety qualification tests.

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 structure of the Technical Safety Report is illustrated in Figure 7.

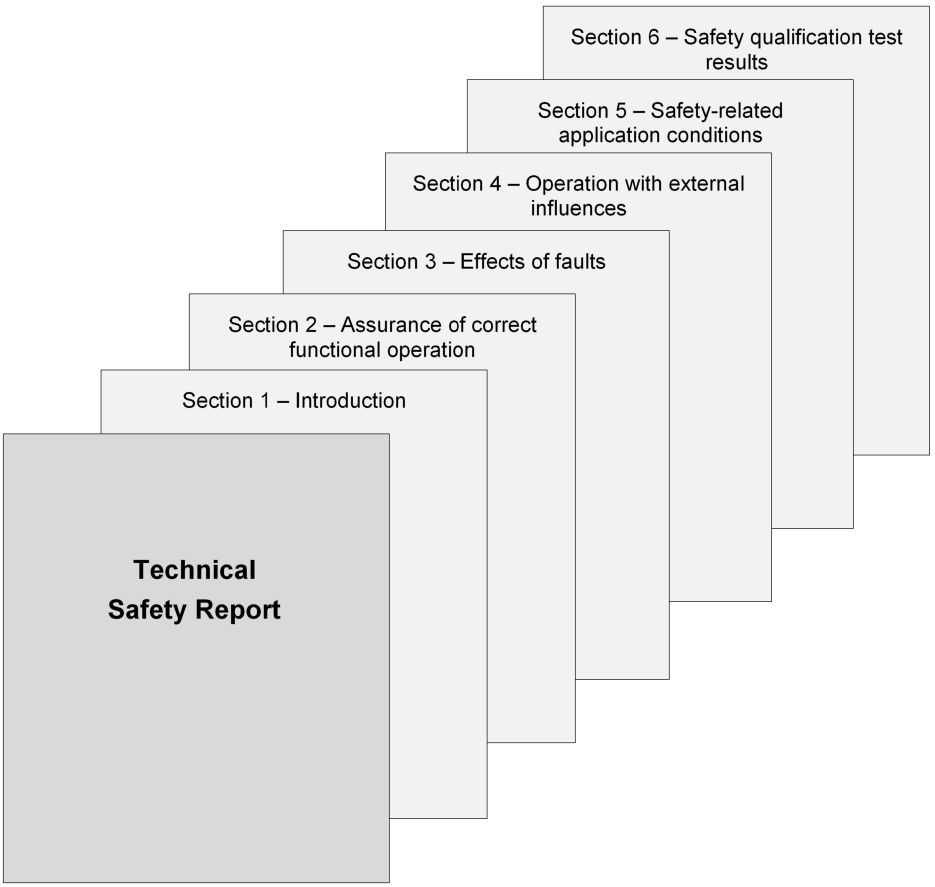


Figure 7 — Structure of Technical Safety Report

The Technical Safety Report shall be arranged under the following headings.

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, subsystem or equipment is claimed to be safe in accordance with this document.

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, in standard production, or at a completed stage of development, the issues of standards used for the original design may exceptionally be used as a basis where these have already been accepted in the approval of the original equipment. This may be applied only where taking into consideration the latest issues of the standards would require further modifications to existing equipment, or where disproportionately high costs for the change would be incurred. Reasons justifying the use of this statement shall be given.

Section 2: Assurance of correct functional operation

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

The following aspects shall be included.

Section 2.1 System architecture description

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

Section 2.2 Definition of interfaces

1) Man-machine interfaces

   a) Operator

      This shall describe the mechanisms by which the system, subsystem or equipment will be operated by operating and engineering personnel.

      EXAMPLE 1 *Mechanisms:*

      — 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, subsystem or equipment to a specific railway or application.

      EXAMPLE 2 Configuration process:

      — software parametrization;

      — 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 the Operation and Maintenance Plan.

2) System interfaces

   a) Internal

      This shall define the functional and physical interfaces between items internal to the system, subsystem or equipment.

      EXAMPLE 3 Internal interfaces:

      — 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, subsystem or equipment and external items.

EXAMPLE 4 External interfaces:

— sensors;

— actuators;

— communication links;

— test and monitoring provisions;

— expansion facilities.

Section 2.3 Fulfilment of system requirements specification

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

EXAMPLE 5 Evidence:

— design principles and calculations;

— test specifications and results;

— validation.

Section 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 6 Safety-related evidence:

— design principles and calculations;

— test specifications and results;

— safety analyses and results.

Section 2.5 Assurance of correct hardware functionality

This shall describe the hardware architecture, and explain how the design achieves the required functionality, as laid down by the requirements specification and by 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 in Section 3.

Section 2.6 Assurance of correct software functionality

For safety-related systems which include software, the requirements of EN 50128 shall be complied with.

For programmable components see Annex F. The results of software validation report (see EN 50128) shall be included or referenced in this section.

In addition, the interaction between hardware and software shall be explained. Detailed requirements for Hw/Sw integration are given in EN 50128.

NOTE 1 Particular topics which need attention include:

— dependence between hardware and software,

— sequence of interaction,

— response times,

— self test routines,

— health monitoring,

— data acquisition techniques,

— graceful degradation,

— negation methods.

Section 3: Effects of faults

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

Since a systematic fault could still exist, despite the quality and safety management processes (see 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, subsystem or equipment having a Safety Integrity Level lower than that of the overall system, including Basic Integrity and non-safety-related functions, cannot reduce the safety of the overall system.

NOTE 2 To prevent the non-safety-related functions of the system from influencing the safety-related ones in undesired ways, an interface analysis can be used to identify the need of separation.

The following headings shall be used in this section:

Section 3.1 Effects of single faults

Section 3.2 Independence of items

Section 3.3 Detection of single faults

Section 3.4 Action following detection (including retention of safe state)

Section 3.5 Effects of multiple faults

Section 3.6 Defence against systematic faults

More detailed requirements are contained in Annex B. Guidance is also given in Table E.5 and Table E.6.

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

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

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

The influences to be considered are listed in Sections 4.1 to 4.6 as described 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.

Section 4.1 Climatic conditions

This section shall demonstrate that safety to the required European standards is achieved under the specified climatic environmental conditions taken from EN 50125-3.

If the railway duty holder specifies more severe conditions than the equipment can fulfil, the supplier can, in agreement with the railway duty holder, demonstrate safety on the basis of measures to control the ambient climate of the system under consideration.

Section 4.2 Mechanical conditions

This section shall demonstrate that safety to the required European standards is achieved under the specified mechanical environmental conditions.

Section 4.3 Altitude

This section shall demonstrate that safety to the required European standards is achieved at the altitude at which the system, subsystem or equipment is actually used.

NOTE 3 The altitude at which the system, subsystem or equipment is to function does not normally exceed 1 800 m above sea level.

Section 4.4 Electrical conditions

This section shall demonstrate that safety to the required European standards is achieved under the specified electrical environmental conditions.

The values quoted in EN 50114-4 and EN 50124-1 should be used as a basis. For systems on vehicles, the values quoted in EN 50124-1, EN 50121-3 (series) and EN 50155 should be used as a basis.

Section 4.5 Protection against unauthorized access

Both physical security threats (the following items from 1.1 to 1.4) and IT-Security threats (item 2) shall be addressed, as required in 6.4 (requirements regarding Physical security and IT-Security).

1) Physical security

1.1) Definition of access levels

This section shall define the access levels: who has access, reason for access and how access is achieved, thereby guarding against unauthorized access. Persons performing functions within each access level shall be required to meet appropriate criteria defined in terms of:

— skill discipline,

— skill level,

— equipment-specific training.

1.2) Protection

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

The protective measures should guard against unauthorized access which is

— accidental, by authorized persons,

— intentional, by unauthorized persons.

1.3) External conditions

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

EXAMPLE 7

Protection against external conditions:

— housing (collocation in the building);

— accessibility.

1.4) Equipment housing

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

EXAMPLE 8

Equipment housing:

— covers;

— mounting;

— seals;

— coding, electrical;

— coding, mechanical;

— firmware recognition.

2) IT-Security

This section shall describe how IT-Security threats which have the potential to affect safety-related functions have been evaluated and how protection against them has been achieved.

Section 4.6 More severe conditions

Where necessary, this section shall describe provisions made to deal with additional, more severe, conditions specified by the railway duty holder.

NOTE 4 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.

— 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;

— action/entry of plants, insects or animals;

— accumulation of dirt and dust (conductive and/or non-conductive);

— more extreme temperature limits in some countries.

Section 5: Safety-related application conditions

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

This shall include the application conditions contained in the Safety Case of any related systems, which are not fulfilled, yet.

The topics considered shall 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;

— versions compatibility for Software and Configuration Data.

Some specific topics which shall be included are listed in Sections 5.1, 5.2 and 5.3.

Guidance is also given in 5.3.13 and Table E.9.

Section 5.1 System configuration and system build

1) System configuration

If a system, subsystem or equipment needs to be configured for each particular application, then any configuration tools and/or procedures shall be defined.

If a system, subsystem or equipment is of sufficient generic design that it could be employed in systems for various applications, then the way in which it is configured and set-up to meet these different applications shall also be documented. Any limitations or conditions for safe use shall be fully specified.

EXAMPLE 9

Configuration aspects:

— procedural methods;

— version control;

— hardware requirements of configuration system;

— software details of configuration system;

— software maintenance;

— simulation;

— configuration data specification (interface between the configurable data and the system);

— version of configuration data.

2) System build

This section shall detail how systems, subsystems and equipment are built into a particular signalling system.

EXAMPLE 10

System build:

— version control settings;

— application control settings;

— interface settings;

— initialization settings;

— maintenance control settings;

— manufacturing and production testing;

— system test routines;

— installation, testing and commissioning;

— data configuration tool required for system build;

— data configuration tool version required for system build.

Section 5.2 SRACs for operation, maintenance and safety monitoring

The technical safety precautions and procedures to operate and maintain the system, subsystem or equipment shall be extracted from the Operation and Maintenance Plan (or referred to, in a traceable way) (see 5.3.9) and documented in this section, which shall include the following aspects:

1) operational status

The conditions that exist in each system, subsystem or equipment shall be defined to provide operating and maintenance personnel sufficient understanding during the following situations:

a) start-up

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

EXAMPLE 11

— default conditions,

— initialization period,

— self-checks performed,

— manual intervention required,

— condition of outputs,

— precautions after an exceptional event, such as fire or unauthorized entry.

b) normal operation

Once the system, subsystem or equipment has successfully completed initialization, the conditions during normal operation shall be defined.

EXAMPLE 12

— cycle times;

— non-data routines;

— disclosure of faults.

c) changeover

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

d) shut-down

When a system, subsystem or 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 13

— default conditions;

— conditions for graceful degradation;

— safety aspects;

— procedures;

— influences on other connected systems.

2) maintenance levels

These shall be defined with respect to:

— first line maintenance by the maintainer,

— second line maintenance by the maintainer,

— second line maintenance by supplier.

NOTE 5 "First line" is preventive maintenance and fault-finding/repair carried out on site, with "second line" being preventive maintenance and possible repair in a workshop environment.

3) periodic maintenance

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

EXAMPLE 14

— training;

— accessibility;

— modularity;

— interchangeability;

— spares provision;

— storage of spares.

4) maintenance aids

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

EXAMPLE 15

These aids can include, for example,

— fault diagnostics,

— interpretation of fault messages.

Section 5.3 SRACs for decommissioning and disposal

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

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

Section 6: Safety qualification test results

This section shall contain evidence demonstrating successful completion, under operational conditions, of the safety qualification tests. These are explained in 5.3.12.

7.3 Generic and Specific Safety Cases

In terms of safety processes, the development of a system can be classified into three types:

— Generic Product.

The system is considered from a generic point of view, applicable to different classes of applications. Analyses are carried out within an operational context which is application-independent. The safety process is typically completed with Phase 7 (Manufacture), as explained in 8.1.

— Generic Application.

The system is considered suitable for a class of application. Analyses are carried out within an operational context which is application-dependent. The safety process is typically interrupted within Phase 7 (manufacture of first equipment) and includes the definition of the application design process.

— Specific application.

The system is considered for a specific application, including its physical implementation (see 7.4).

Three different categories of Safety Case can be defined in accordance with these types of development, namely: Generic Product Safety Case (GPSC), Generic Application Safety Case (GASC) and Specific Application Safety Case (SASC).

7.4 Provisions for the Specific Application Safety Case

When a Specific Application Safety Case is written on the basis of the Generic Application Safety Case, it shall address the following two aspects:

a) the application design, and

b) the physical implementation.

If a stand-alone Specific Application Safety Case is established it shall include all information required from a GPSC or GASC viewpoint.

For the application design, the main focus is to show that the design is based on correct specifications and input data, that it is adequate to fulfil the safety requirements of the specific application, and that it adheres to the applicable safety-related application conditions. The following shall be provided:

— evidence of the correctness and accuracy of the inputs used to elaborate the data at system level, in relation to the aspects of the railway system they describe;

— evidence that the application design and deployment processes ensure that the correct data is implemented in the application under consideration;

— evidence used to elaborate the data at system level, the application design, and the deployment process are compliant with the safety-related application conditions of the generic products or generic application.

For the physical implementation, the main focus is to show that the application provides the correct functionality, that it fulfils its safety requirements, and that all safety-related application conditions are either fulfilled or correctly addressed to operation and maintenance of the specific application. The following evidence shall be provided:

— evidence that the manufacturing and installation records are compliant with the safety-related application conditions for the generic products/applications which have been used;

— all the data preparation results, including the results of analysis and testing activities carried out as part of safety verification and safety validation;

— evidence of correct manufacturing and installation, together with results of on-site tests and commissioning, in order to prove the coherence of the installed system with the defined one (i.e. as-built versus as-designed).

The Safety Case structure, as described in 7.1 and 7.2, is suitable and sufficient for Generic Products and Generic Applications. For Specific Applications, that structure may be tailored, expanded or reduced in accordance with specific needs.

In particular:

— if separate safety approvals are needed for the application design and for its physical implementation, two separate safety cases can be produced, each of them structured as described in 7.1 and 7.2;

— otherwise, these two aspects can be merged in a single Specific Application Safety Case.

In cases where there are several similar specific applications (e.g. based on the same process of configuring generic products), a Generic Application Safety Case can be produced, describing the system before its configuration in relation to the application under consideration and justifying the rules for configuring the generic product, products of generic applications to specific applications or classes of applications. The Specific Application Safety Cases can then be written on the basis of the Generic Application Safety Case. Several aspects (and related sections of the safety case) may be omitted if not applicable because already covered in the Generic Application Safety Case. Either GASC or SASC shall contain a justification of the safety of the process used for configuring the generic application to specific applications or classes of applications.

7.5 Dependencies between Safety Cases

In some instances the Safety Case for a system will depend on the Safety Cases of other referenced systems, subsystems or equipment. For instance, if an independent safety assessment has been carried

out for a generic product, or for a generic application, a reference may be made to this, without repeating the assessment, when assessing the specific application that makes use of those generic parts.

Figure 8 shows two examples of the various possible usages of Safety Cases.

In Example 1, an overall European Rail Traffic Management System for a specific line (ERTMS Line #1) is addressed in a Specific Safety Case, embracing also a railway Interlocking system (IXL system #3) and an Automatic Train Control (ATC System #2). No other Safety Cases are reused or referenced. This means that the two subsystems (interlocking and ATC) are being developed within this application and do not rely on previous acceptance.

In Example 2, the IXL system for a specific station #4 is based on a generic application supporting the deployment of a class of similar stations. In its turn, the generic IXL system re-uses a generic signal actuator. Hence the Specific Application Safety Case is based on two Generic Safety Cases.

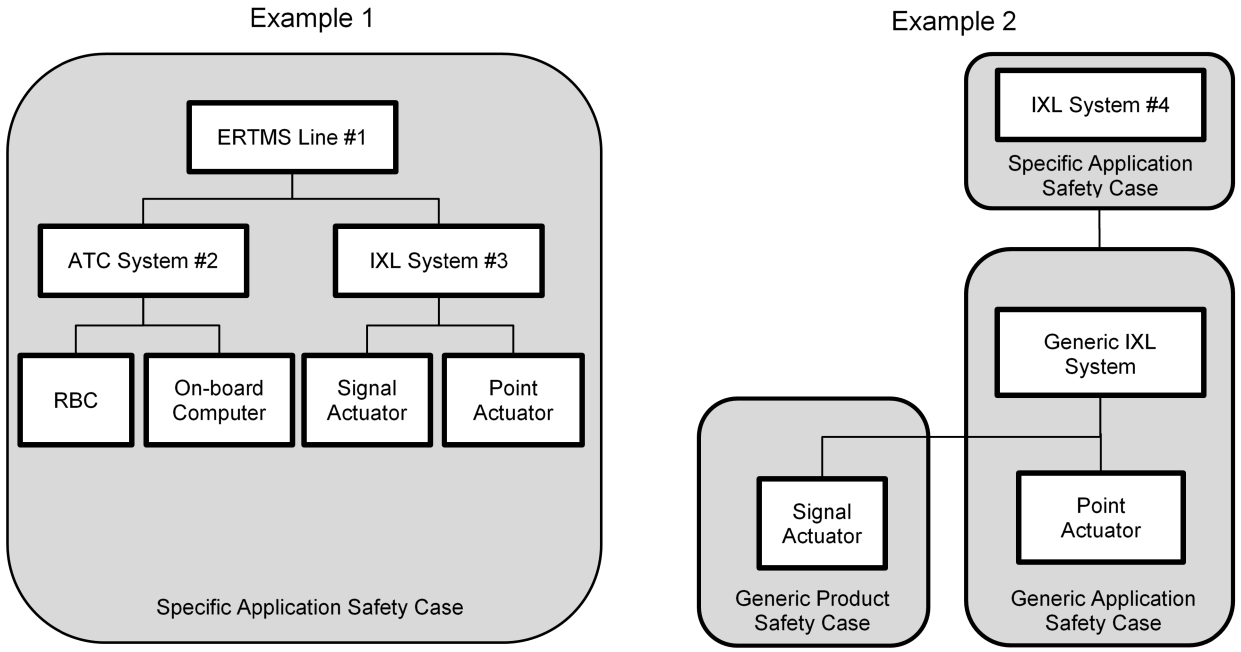


Figure 8 — Examples of different usage of Safety Cases

8 System safety acceptance and subsequent phases

8.1 System safety acceptance process

Prior to handover of the system, subsystem or equipment to a railway duty holder, the requirements for safety acceptance defined in this subclause shall be satisfied, including submission of the Safety Case and of the independent safety assessment report.

The present document does not specify who carries out the work at each stage of the safety acceptance process, since this can vary in different circumstances.

The overall documentary evidence for safety acceptance consists of:

— the system requirements specification;

— the risk assessment outcomes;

— the safety requirements specification;

— the safety case;

— the independent safety assessment report.

Provided all the conditions for safety acceptance have been satisfied and demonstrated, and subject to the results of the independent safety assessment, the system under consideration is granted safety acceptance by the railway duty holders responsible for its incorporation or final use. Acceptance can be subject to the fulfilment of additional conditions imposed by the legal framework.

When using a previously accepted Generic Product or a Generic Application in the context of a Specific Application, safety acceptance should be based on existing related independent safety assessment (i.e. cross-acceptance). No cross-acceptance shall be possible for Specific Applications.

Two examples of safety acceptance processes covering the three categories of Safety Case are illustrated in Figure 9.

These examples are consistent with those given in Figure 8; here the intention is to show a particular instance of tailoring, typically applied for reusing electronic products and related generic application activities.

On the left of Figure 9, a Specific Application Safety Process follows a life cycle where all the phases are executed for a single and unique system.

On the right of Figure 9, a Specific Application Safety Process (lower right) gets contributions from a Generic Application Safety Process and a Generic Product Safety Process. This could be the case for a configurable electronic system, where the process of application design and physical realization is established once (as a generic application) and then applied/reused for a set of specific applications.

In the middle of Figure 9, the Generic Product Safety Process is shown. When a safety case for Generic Product (i.e. independent of application), or a Generic Application (i.e. class of application) is developed, a validation activity for the system under consideration usually performed in phase 9 “system validation” of the system life cycle, shall be also performed at the end of life cycle phase 7 “Manufacture” considering also the manufacturing of the first item.

Within the Generic Product Safety Process:

a) the product is designed and implemented to meet the safety requirements;

b) plans or SRACs are established, in the context of safety, for future life cycle tasks, including:

   — installation;

   — commissioning;

   — operation and maintenance, including definition of operation and maintenance procedures;

   — data acquisition and assessment during operation;

   — decommissioning;

NOTE 1 Plans established within this phase are often generic and customized in later phases for the specific application needs (e.g. language, specific operational/maintenance framework).

c) the manufacturing process is defined, verified, established and executed on the first production series equipment;

d) related type testing (including environmental stress screening and inspection/testing of RAMS-related failure modes) is performed together with the overall testing for demonstration of the correct functional operation.

So far as the Generic Application Safety Process is concerned (upper right in Figure 9), activities end up in life cycle phase 7. This because, as for generic products, the generic applications involved in a specific application are accepted together with, and at the same time as, the acceptance of the first specific application.

With respect to the Generic Product safety process, in addition to the above activities a), b), c) and d), the following one takes place:

e) an application design process (including related procedures and tools) is prepared, validated and established.

NOTE 2 This is typically the case of electronic Interlocking systems, where the generic software, hardware and data (e.g. signalling principles) as well as the related data preparation, manufacturing, installation and commissioning procedures for specific layouts are included in a GA process and then executed for the different Specific Applications in the SA processes. The evidence of the first part is given in a GASC and of the second part in the subsequent respective SASCs. This tailoring simplifies the safety demonstration for SA, by reusing all the evidence already established for GA up to life cycle phase 6.

Finally, evidence of safety qualification tests collected, where deemed required, during the operation of the first specific application will be included in an update of SA/GA/GP Safety Cases, as first editions would not have been able to address this evidence.

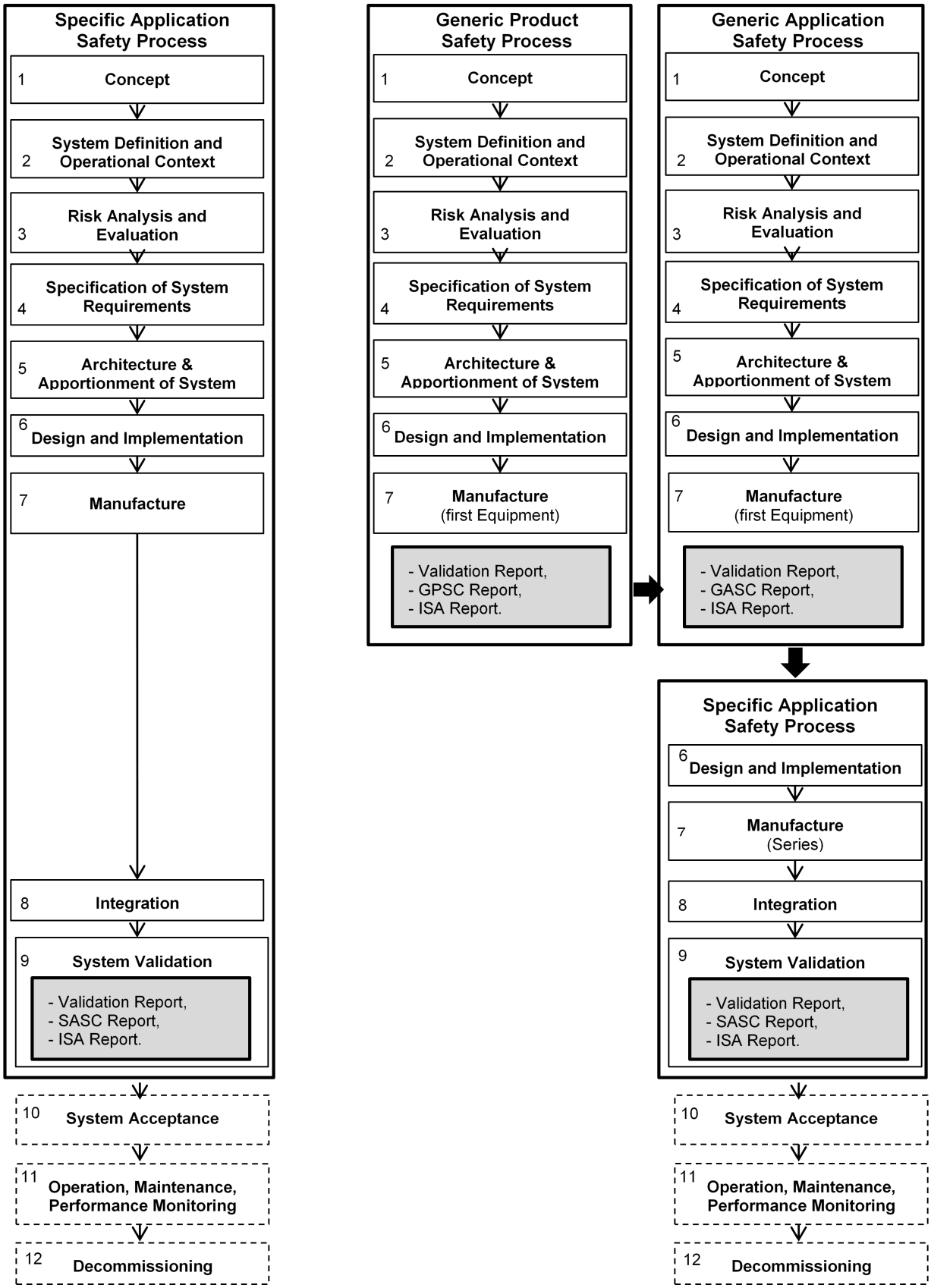


Figure 9 — Examples of different safety acceptance processes

8.2 Operation, maintenance and performance monitoring

Following handover, the procedures, support systems and safety monitoring defined in the Operation and Maintenance Plan and in Section 5.2 of the Technical Safety Report (part of the Safety Case) shall be adhered to.

Appropriate procedures, support systems and safety monitoring 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 quality management, safety management and technical safety criteria in order not to reduce the achieved level of safety.

Table E.9 gives guidance on Application, Operation and Maintenance for each Safety Integrity Level.

8.3 Modification and retrofit

During the operational life of a system, change requests can 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.

Modifications 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.

8.4 Decommissioning and disposal

At the end of the operational life of a system, its decommissioning and disposal shall be carried out under consideration of the measures defined in Section 5.3 of the Technical Safety Report (see 7.2).

These measures shall be incorporated in the maintenance manuals.

Annex A
(normative)

Safety Integrity Levels

A.1 Introduction

This annex gives details for the specification, 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 duty holder, and are not defined in this document.

The overall Risk Assessment and safety management processes are defined in EN 50126-1 and EN 50126-2.

A.2 Safety requirements

Requirements specification can be considered in two parts (see Figure A.1):

— requirements which are not related to safety, and

— 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 can, in turn, be divided in two parts:

— functional safety requirements;

— other safety requirements (e.g. occupational health and safety, fire safety).

Functional safety requirements describe the actual safety-related functions which are required to be carried out. Functional safety requirements are comprehensive of safety integrity requirements, which define the degree of safety integrity required for each safety-related function.

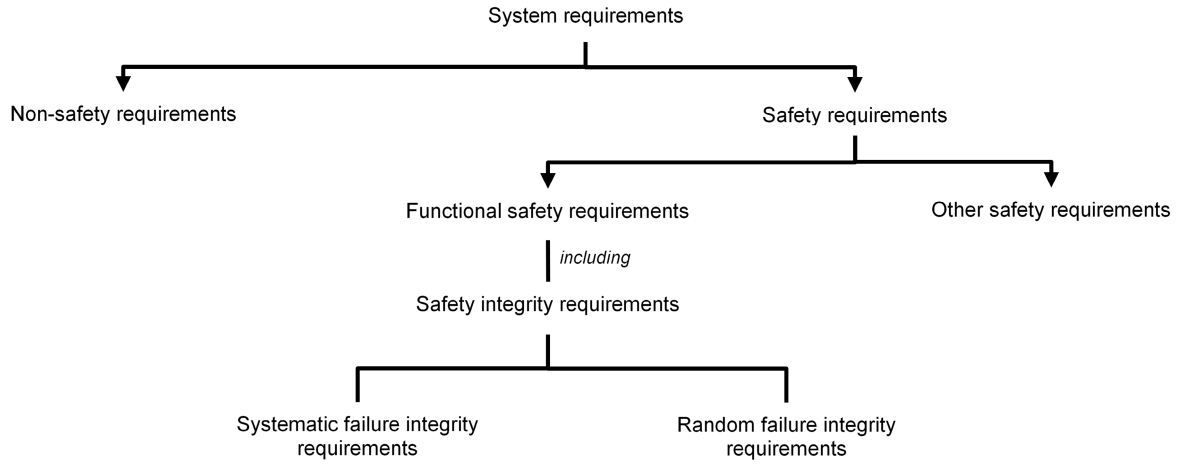


Figure A.1 — Safety requirements and safety integrity

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.

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, subsystem or equipment life cycle.

EXAMPLE:

— specification errors;

— design errors;

— manufacturing errors;

— installation errors;

— operation errors;

— maintenance errors;

— modification errors.

Systematic failure integrity is achieved by means of the quality management, safety management and technical defences.

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.

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

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 realization of a system to a stated integrity level (for guidance see Annex E).

Random failure integrity is the only part of safety integrity that can be quantified. A quantified assessment of random failure integrity is 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.

Despite the probabilistic calculations and assumptions, a residual risk of hazardous failure could still exist. This is why the achievement of random failure integrity is also included within the technical safety conditions and qualitative measures, specified in this document by means of the Safety Integrity Levels.

A.4 Determination of safety integrity requirements

A.4.1 General

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 there is a well-defined interface between the operational environment and the signalling system.

Typically this interface represents also the boundary of responsibilities between the railway duty holder and the supplier. This interface is not intended to limit cooperation but to clarify responsibilities and interactions.

From the safety point of view this interface is defined by a list of hazards and associated tolerable hazard rates within the system.

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 shall consist of Risk Assessment and Hazard Control, see Figure A.2. The Risk Assessment produces Tolerable Hazard Rates (THR) which are the input to the Hazard Control.

Both the Risk Assessment and the Hazard Control shall undergo an independent safety assessment.

NOTE 1 In some cases, these steps are not completely independent. The Hazard Control can lead to system changes which offer more safety performance. The curved arrow in Figure A.2 shows this. Hence, in these cases the global process is iterative.

NOTE 2 During each project, responsibilities are clarified unambiguously to avoid gaps. The overlapping arrows in Figure A.2 show the necessary cooperation between the stakeholders in the safety requirements specification.

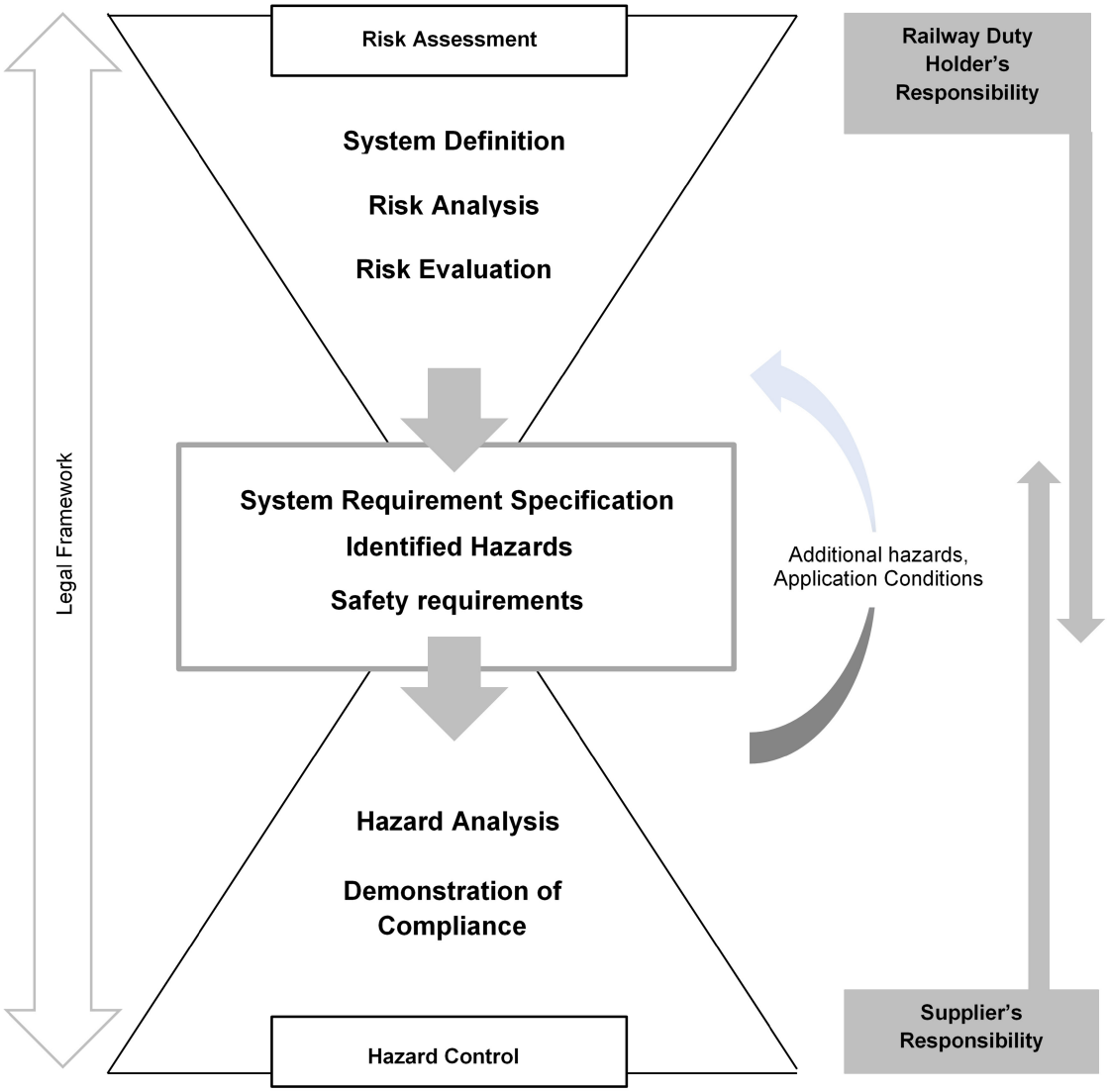


Figure A.2 — Global process overview

A.4.2 Risk Assessment

A.4.2.1 General

The aim of the Risk Assessment is to refine the product hazards, identify their causes and consequences, evaluate the risk, and define the mitigation strategy in compliance with the allocated safety target.

Risk Assessment includes:

1) System definition,

2) Risk analysis,

3) Risk evaluation.

NOTE Typically within the Hazard Control for an electronic system the techniques and measures implemented will address reduction of risk on the basis of occurrence frequencies and not of reduction of consequences.

A.4.2.2 System definition

The scope of the System Definition should include consideration of the functions and the interfaces defined for the item under consideration together with the related operation and maintenance context (independent of the technical realization).

In the case of a generic product/application development, the supplier makes assumptions about context, interfaces and related hazards. These assumptions shall then be defined as safety-related application conditions to be observed in the integration of the generic product/application in a wider system, unless they are shown to be already considered within the user processes.

A.4.2.3 Risk analysis

Risk analysis includes:

1) hazard identification;

2) consequence analysis (analysis of the consequences, i.e. the losses).

The first step of the risk analysis is hazard identification, i.e. identification of the hazards relevant to the system.

Hazard identification involves a systematic analysis of a product, process, system or an undertaking to determine those adverse conditions (hazards) which can arise throughout the life cycle. Such adverse conditions can 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 deductive phase (proactive forecasting, e.g. brain-storming, structured what-if studies, HAZOP, FMEA).

The empirical and deductive 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 often a waste of resources and can result in a misleading or unproductive risk analysis. 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 subsystems. It also means that the hazard identification will be performed repeatedly at several levels of detail during the system development.

Figure A.3 shows that the cause of a hazard at system level can be considered as a hazard at subsystem level (with respect to the subsystem boundary). Thus this definition enables a structured hierarchical approach to hazard analysis and hazard tracking.

To further ensure that the risk analysis 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.

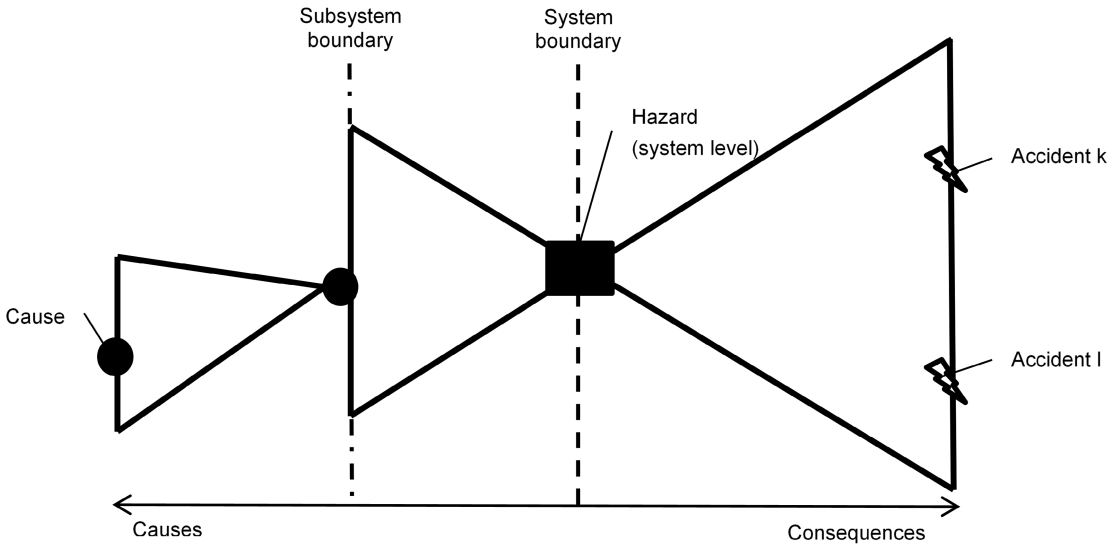


Figure A.3 — Definition of hazards with respect to the system boundary

A.4.2.4 Risk evaluation

The final activity during Risk Assessment is risk evaluation, that is derivation of the Tolerable Hazard Rates (THRs) and ensuring that the resulting risk is tolerable, with respect to the appropriate risk acceptance criteria.

The resulting THRs shall be derived, taking into account the risk acceptance criteria. Risk acceptance criteria are not defined by this document, but depend on national or international legislative requirements.

The analysis methods shall:

— 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, 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 THRs.

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

A.4.3 Hazard Control

A.4.3.1 General

Hazard Control shall demonstrate management and implementation of the required THRs with associated safety functions.

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

Hazard Control consists of a number of activities which can be summarized as follows:

— define the safety assumptions and system functions related to the defined hazards;

— define the system architecture and allocate system functions within the architecture (technical solution) to meet the safety requirements including the defined THRs;

— perform the hazard analysis (or causal analysis), to evaluate the possible causes of hazards;

— determine the safety integrity requirements for the functions of the system;

— complete the safety requirements specification;

— analyse the system to meet the requirements;

— identify potential new hazards arising out of the system design through the design and safety 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, transfer the potential hazards back to Risk Assessment for further treatment;

— determine the reliability requirements for the equipment.

Assumptions made in the hazard analysis shall be checked and may lead to safety-related application conditions for the implementation (more details in A.4.3.3).

Failures caused by environmental conditions (e.g. EMC, temperature, vibration, etc.) shall be considered within the hazard analysis.

NOTE 1 The Hazard Control process is typically planned in phases where the safety requirements are first refined and completed (as part of a hazard analysis) and then the system is analysed and verified for compliance as part of subsequent safety activities.

NOTE 2 A well-structured and documented Hazard Control contains relevant parts of a Technical Safety Report implicitly. In this case, it is sufficient to reference in the Technical Safety Report to the Hazard Control documentation.

The Hazard Analysis process is depicted in Figure A.4.

With reference to Figure A.4, hazard analysis constitutes two key stages:

1) Apportionment of THR down to the determination of TFFR and SIL (see A.4.3.2);

2) Apportionment of hazardous failure rates (see A.4.3.3).

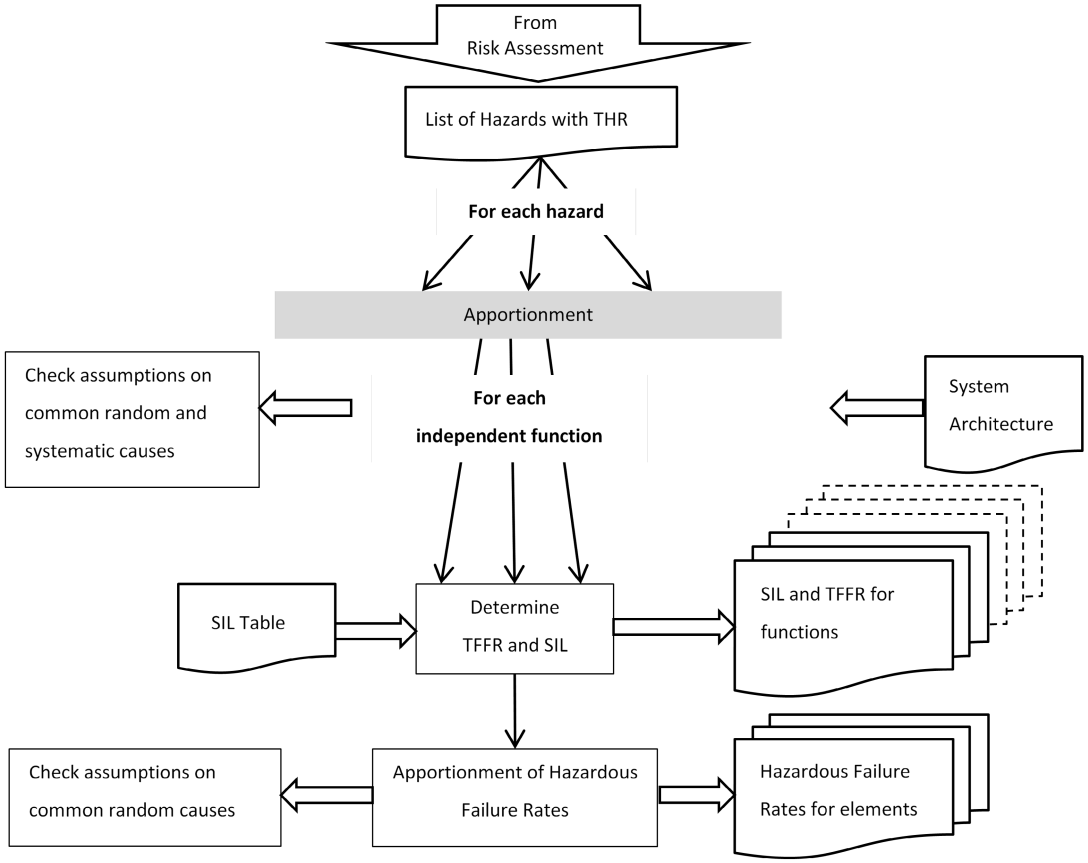


Figure A.4 — Example of a Hazard Analysis process

A.4.3.2 Determination of TFFR and SIL

Safety integrity requirements, expressed at the system level for each hazard as THR, are linked to a specific functional composition defined by the selected system architecture and therefore translated into TFFR for each of the functions involved:

1) The hazard shall be associated to a functional failure of a function or a set of functions.

2) As a consequence, the THR shall determine the tolerable functional failure rate(s) (TFFR(s)) for the identified function(s).

3) Since the possible causes of the functional failure can be both systematic and random, the TFFR is considered a target of the minimum systematic and random safety integrity of the involved function. The TFFR shall therefore be associated to an integrity level (SIL or Basic Integrity) using the SIL table (Table A.1 in A.5.2).

If the relationship between hazards and functions is one-to-one, for each hazard with related quantitative target, the quantitative safety integrity requirement (expressed as THR) shall be completely allocated to the function that protects against that hazard (TFFR).

NOTE 1 THR and TFFR are identical in case of a single function causing the hazard, e.g. movement of a point.

This process may continue down to the level of the last independent functions. This is the level at which two (or more) functions control the same hazard, being however completely independent. This means that:

a) from a functional perspective, any of them is able to counteract the hazard, regardless of the presence or absence of the other one, even though with different efficiency;

NOTE 2 For example, the control of barriers and the control of lights at a level crossing may operate differently with respect to the hazard of trespassing. On the contrary, this is not the case of cooperating functions, e.g. a control function and its protection function, or the calculation of the braking curve and the braking command itself.

b) from an implementation perspective, there is an objective to eliminate common causes of failure, either systematic or random (see A.4.3.4 for further explanation).

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 decision diagrams, Markov models etc. In any case particular care shall be taken when independence of items is required.

NOTE 3 THR and TFFR can also be derived by means other than explicit risk estimation (in line with EN 50126-2), e.g. the requirements could be part of a code of practice or they could be derived by comparison with similar reference system, as explained in A.4.2.4.

TFFR shall be used for SIL determination, at the latest at the level of the last independent functions.

A subsystem can implement a number of safety-related functions, each of which could require different Safety Integrity Levels. Where this is the case, the subsystem shall satisfy all the required Safety Integrity Levels. This may be obtained by either each function meeting the highest SIL or by demonstration of absence of unintended influence.

An example of THR/TFFR/FR apportionment and SIL allocation is provided in Annex D.

A.4.3.3 Apportionment of hazardous failure rates

In a second phase of the causal analysis, the hazard rates for subsystems are further apportioned leading to failure rates for the elements, but on this physical or implementation level the SIL (or Basic Integrity) remains unchanged.

Consequently the SIL adopted by EN 50128 for the safety-related software is the same as the function SIL.

NOTE 1 SIL 0 as defined in EN 50128:2011 is sufficient to satisfy Basic Integrity requirements for safety-related software functions.

While in the first phase of the causal analysis demonstration of complete independence is required for logical AND-combination (i.e. the failure of functions shall be independent with respect to systematic and random faults), independence with respect to random faults is sufficient in the second phase.

Hazardous failure rate is used for any further necessary allocation of random integrity requirements to physical components. Such components inherit their SIL from the TFFR level.

NOTE 2 Typically each independent function protecting from hazard(s) within a signalling system is executed by several physically independent elements where the TFFR is further apportioned as hazardous failure rates (while SIL stands unchanged as inherited from function/TFFR), e.g. a signal preventing train from entering an occupied route is set in accordance with the status of several track circuits (each one of them being a physically independent component with an hazardous failure rate lower than TFFR).

A.4.3.4 Independence among functions

Independence implies that there are neither systematic nor random faults, which cause a set of functions to fail simultaneously. This includes both

— freedom from hazardous common random causes and

— freedom from hazardous common systematic causes.

When a hazard results from the failure of two or more independent functions (i.e. logical AND combinations), the following rules shall be applied.

— Freedom from common random and systematic causes shall be demonstrated by CCF analysis.

— Each function shall be able to prevent the hazard; therefore a failure of one of the independent functions shall not lead to the hazard.

— The functions shall be diverse (i.e. use different functional approaches or technology) so as to avoid common causes leading to the hazard.

— Safety integrity of each independent function shall not rely on the results (e.g. outputs) of the other independent function(s).

NOTE 1 A first function providing input to a second one is a source of common cause failure for the overall output, in terms of safety target allocation/quantification or fault tree analyses (e.g. an interlocking system providing track circuits states to a radio block centre/automatic train protection function for the elaboration of movement authorities). This case corresponds to a OR gate where the TFFRs quantified for each constituent function are summed providing the overall hazard rate.

— A fault in any function shall be detected and a safe state enforced within a time compatible with the THR/TFFR of the higher level hazard or function. This detection should be provided by a means independent of the function under consideration.

As a precondition for this, the fault detection mechanisms of each function shall have a coverage of faults potentially leading to hazards when combined with others which is sufficient to achieve the THR/TFFR of the higher level hazard or function.

If these requirements are assured, random and systematic integrity requirements may be apportioned to the next lower level.

NOTE 2 In general, functions are not independent but can be further subdivided in independent sub-functions and sub-functions affected by CCF. Figure A.5 shows a generic treatment of CCF by FTA. The figure shows that two functions can always be made independent if their common causes are separated from the residual functions.

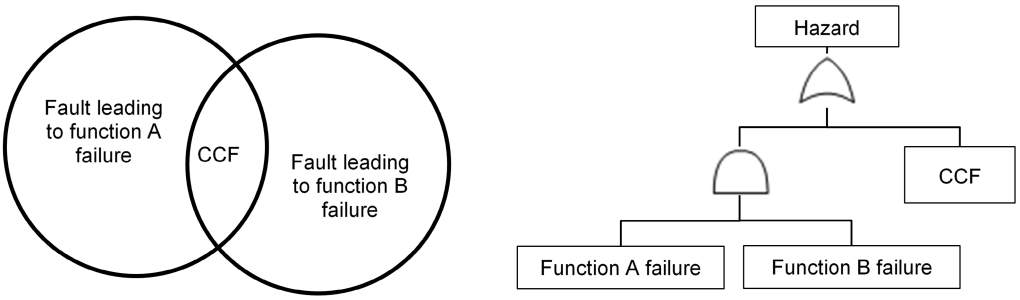


Figure A.5 — Treatment of CCF by FTA

TFFR apportionment may be only applied if the common systematic failures are non-hazardous. This is not feasible for identical redundancy architectures, typically used for composite fail-safe systems. In these cases, TFFR is not apportioned further and the logical AND relationship is only applied to FR apportionment to reflect the independence against random failures. Independence regarding systematic errors is not required.

A.4.3.5 Independence from common random causes

Fault tree calculations which include a logical AND relationship for random effects are only meaningful where there is independence from common random causes. Thus, in any case a common cause failure (CCF) analysis would be necessary to justify any assumption of independence.

This independence is a property claimed where no hazard can be caused by stochastic (galvanic connection, EMC, etc.) or non-stochastic physical influences of common cause between two functions (or items), detailed requirements for this are provided in Annex B.

NOTE Random effects due to physical influences are stochastic for any events which are represented by statistics regardless of their underlying probability distribution. These events are typically represented, within electronic technology, by exponential distributions (component failures). Random effects also cover cases governed by different probabilities/laws.
For example a switchover of a redundant power supply could occur weekly as a proof-test but this could lead to a surge or inrush current, common to all downstream subsystems, which is systematically occurring. These aspects are also covered, as random effects, by common cause analysis of physical influences.

If independence from common random causes is ensured, random integrity requirements may be apportioned to the next lower level.

When applying fault tree analysis to system functions, which is the most common situation in the process of apportioning safety integrity requirements, the usage of logical AND relationships shall be subject to the following safety-relevant conditions:

— the implementations of the system functions shall be independent from common random causes;

— the safe down times defined by detection and negation times for each function shall be estimated and achieved.

A.4.3.6 Independence from common systematic causes

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 and system development, together with the respective verification and validation activities, all of which have a significant influence on the properties of the end product. It is generally agreed that more robust and systematic life cycle processes are needed where a product or system has higher degrees of criticality in its application environment. In addition, since systematic errors inherently arise during these life cycle processes, a degree of independence is often desirable.

In a manner similar to their physical counterpart, independence and diversity in human resources 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 minimized.

If the THR/TFFR of a first level hazard/function is apportioned in less demanding TFFRs leading to lower SILs by using two independent functions, the life cycle phases before the definition of the two functions (system definition, risk analysis, requirements specification, architecture and apportionment of system requirements), as well as the life cycle phases that follow the implementation of the two functions (integration, system validation) could be a source of common causes of failure for those two functions. For this reason, these phases shall be managed in accordance with the SIL of the first level hazard/function.

The development processes shall fulfil the required SIL and ensure that there is sufficient organizational and personal independence between the development teams in order to further minimize systematic errors. For guidance on software issues see EN 50128.

A.4.4 Identification and treatment of new hazards arising from design

Realization of a signalling system can lead to unforeseen properties with a potential to cause harm to people, in particular if the system or technology is novel. New hazards can arise because of several factors:

— new technology has a potential (lack of experience) for unforeseen hazards or for new hazardous failure modes;

— emergence of hidden hazards in the existing railway system due to the introduction of a new technology (e.g. from analogue to digital technology);

— new design hazards due to a lack of adequate/proper specification;

— special operation modes in an existing railway system could not fit well and create new hazards for the operators, maintainers or other members of the staff, public, etc.;

— design errors might create new hazards but they can often be related to ones that have already been identified.

These factors can give rise to hazardous circumstances and states which require the same process to be applied as for all other hazards already identified.

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 Assessment process. 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 duty holder. Depending on the perceived risks, these hazards would require qualitative or quantitative assessment, with a view to estimating and agreeing an appropriate tolerable rate (THR) for each.

If it is possible to relate the new hazard to one which has already been identified, the supplier should confirm that the resulting hazard rate of the combination of these two hazards remains compliant with the THR fixed by the railway duty holder. The new hazard shall be traced in the hazard log and the safety case.

If the new hazard is not connected to any of the hazards which have already been identified, the supplier shall provide the railway duty holder with all of the information that has been obtained by the hazard analysis (causes, consequences, risk, etc.). The railway duty holder shall then decide whether this new hazard is relevant. If the new hazard is relevant, then the railway duty holder and supplier are responsible for finding agreement to mitigate properly the risk.

A full record of the analysis and decisions concerning any new hazard shall be included in the hazard log and referenced to in the safety case.

A.5 Allocation of SILs

A.5.1 General aspects

The degree of safety integrity for a safety-related function is expressed as one of four discrete Safety Integrity Levels (SIL, from SIL 1 to SIL 4) or as Basic Integrity. SIL 4 has the highest level of safety integrity; Basic Integrity the lowest.

NOTE In EN 50129:2003 the term “SIL 0” was introduced to indicate non-safety-related functions. This term is no longer used and non-safety-related functions are just referred to as such.

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 Assessment of the system, as described in A.4.2. This activity results in tolerable hazard rates for each hazard. Nevertheless, as described in A.4.3, 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). Within the deployment of a specific application, it shall be ensured that the required tolerable hazard rates coming from the risk analysis are fulfilled. The railway duty holder and/or the safety authority shall determine the base line for this process.

During the next phases 5 and 6 (“Specification of system requirements” and “Architecture and apportionment of system requirements”, in accordance with the life cycle phases described in EN 50126-1), the tolerable hazard rates are apportioned to system functions as TFFR. The TFFR is the target for the minimum safety integrity of the function, and shall be associated to a SIL (1 to 4) or to the Basic Integrity. Each of these levels shall have qualitative and quantitative requirements attached to them (see Figure A.6). The quantitative requirements (including the TFFR) are relevant for random failure integrity. The qualitative requirements (methods and tools) shall cover systematic and random failure integrity.

Having followed the measures and methods required for a given SIL, the systematic failures need not to be reconsidered when demonstrating the TFFR is achieved.

It is important to recognize that achievement of a specified Safety Integrity Level requires compliance with all of the factors in Figure A.6, 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.6 need to be fulfilled in order to achieve the specified safety integrity.

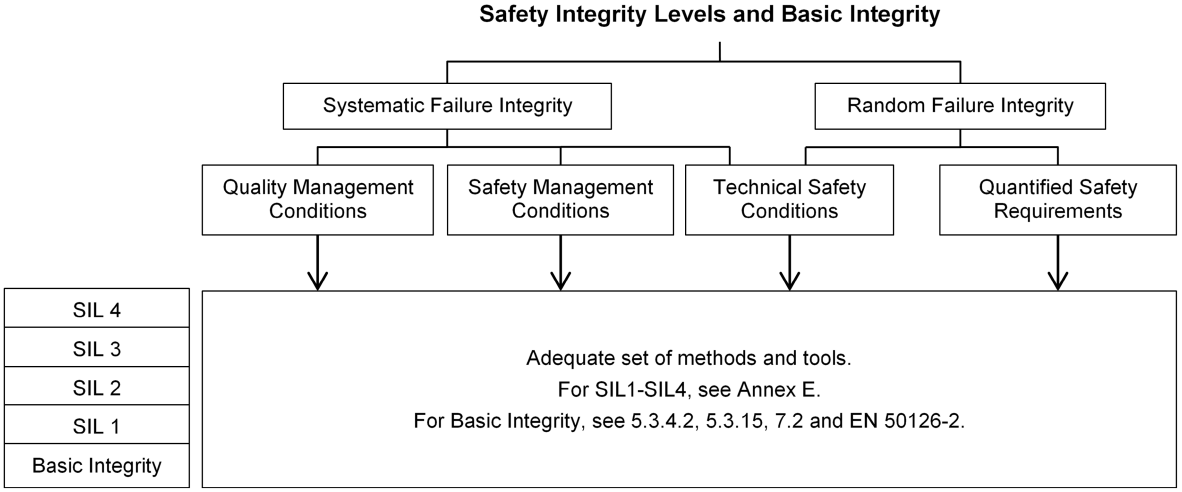


Figure A.6 — Relationship between SILs and techniques

A.5.2 Relationship between SIL and associated TFFR

This document is based on the assumption that safety relies both on adequate measures to avoid or tolerate systematic failures 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 1, 2, 3, 4 and a list of corresponding intervals or bands for tolerable functional failure rates.

The SIL table identifies the required SIL for the safety-related function from the TFFR. Thus, after the TFFR for a function has been derived by a quantitative method, the required SIL shall be determined by the use of the following table.

Table A.1 — The SIL table

TFFR per hour and per function	Safety Integrity Level
$10^{-9} \leq TFFR < 10^{-8}$	4
$10^{-8} \leq TFFR < 10^{-7}$	3
$10^{-7} \leq TFFR < 10^{-6}$	2
$10^{-6} \leq TFFR < 10^{-5}$	1

NOTE In contrast to other standards the SIL table in this document 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.

A safety-related function having quantitative requirements more demanding (lower) 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 TFFR can be apportioned between those sub-functions (allocating TFFR to these functions) and a SIL allocated to each of them;

— 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 TFFR.

A safety-related function having quantitative requirements less demanding (higher) than 10^{-5} h^{-1} shall fulfil the requirements for Basic Integrity. These requirements are provided in 5.3.4.2, 5.3.15, 6.2.3, 7.2 and EN 50126-2.

Techniques and measure to be used for SIL from 1 to 4 are provided in Annex E.

Annex B
(normative)

Management of faults for safety-related functions

B.1 Introduction

This annex concerns the ability of the system, subsystem or equipment to continue to meet its specified safety requirements in the event of random hardware faults and, as far as reasonably practicable, systematic faults.

The annex is structured as follows:

— B.2 General concepts

— B.3 Effects of faults

Within B.3, subclauses (B.3.x) are structured in accordance with the headings of the Technical Safety Report Section 3 (as defined in 7.2):

— B.3.1 Effects of single faults

— B.3.2 Independence of items

— B.3.3 Detection of single faults

— B.3.4 Action following detection

— B.3.5 Effects of multiple faults

— B.3.6 Defence against systematic faults

B.2 General concepts

B.2.1 Detection and negation times

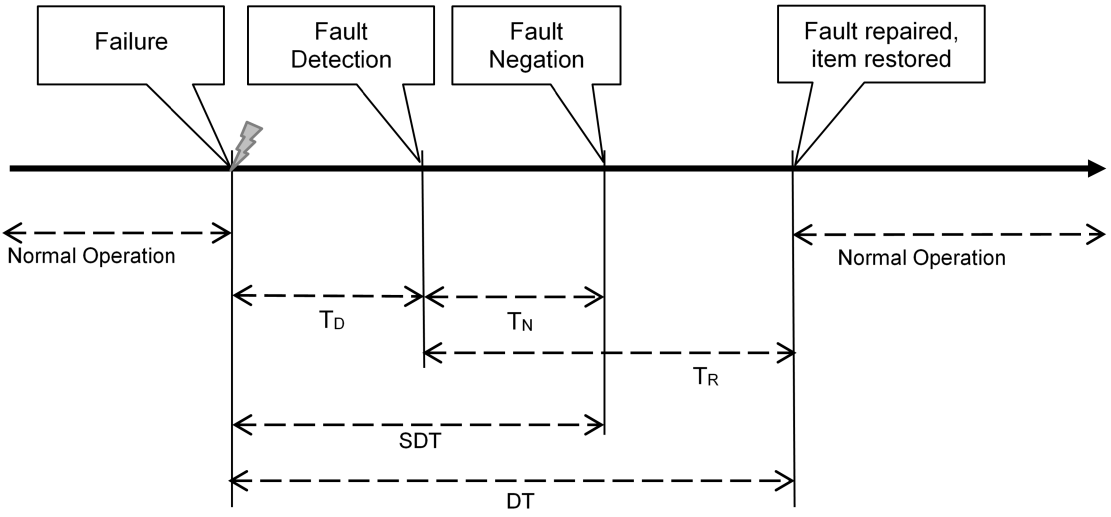


Figure B.1 — Detection and negation times

After a failure within an item has appeared, normal operation will be restored only when the following two events have taken place:

— the fault is detected and negated (this means a safe state is enforced);

— the fault is repaired and the item restored.

Detection time (T_D)

The fault detection time is the test interval in the case of detection by automatic and periodic testing, or the maintenance interval in the case of detection by staff. If no measures for detection are specified, implemented or planned, the fault detection time is the lifetime of the system.

In the case of equipment in storage, it can be linked to the interval between periodic testing by maintenance personnel.

Where fault detection is achieved through operational use, the fault detection time is mean time between uses.

While in a reliability context the detection time is usually not significant, this time becomes important in the safety context. Safety-critical applications might not rely on self-tests or similar measures, but the detection and negation might be performed independently of the item. Sufficient failure detection and negation mechanisms shall be demonstrated in the safety case.

Negation time (T_N)

The negation time is the time taken for the relevant part of the system to enforce a safe state, either automatically or by human action.

Detection plus negation times are defined here as Safe Down Time (SDT).

The Safe Down Time is the time required to detect and negate the last fault before the output becomes hazardous with respect to the defined TFFR. The SDT can have different meanings for different

architectures: in the case of composite fail-safety the system remains in a safe state, but an additional failure could be hazardous (if the first one is not negated); in the case of reactive fail-safety the system could result in a transient permissive output. See Figure B.4 for SDT in the context of composite fail-safety and Figure B.5 for SDT in the context of reactive fail-safety.

Repair time (T_R)

After fault detection, there is the time to repair (logistic time plus actual repair time: fault finding, repair, exchange, check up to restore equipment into operation).

Time between a failure and the next restore into operation is called Down Time (DT).

In a safety context generally the actual repair time can be neglected, as control measures are taken to enter and stay in an enforced safe state.

NOTE In some cases, (especially for components with low safety requirements), the negation occurs through the restoration of the item, therefore SDT = DT (no safe degraded operation exists, degraded operation is unsafe, or at least less safe than prior to the failure).

B.2.2 Composition of two independent items

For two items A and B implementing a function F, in the hypothesis that dangerous failures can be detected, and the two items are restorable, the following basic formula for the asymptotic hazardous functional failure rate (FFR) may be used:

$$FFR \approx \frac{FR_A}{SDR_A} \times \frac{FR_B}{SDR_B} \times (SDR_A + SDR_B) \quad \text{(B.1)}$$

NOTE The formula is an approximation that can be derived for a simple 2oo2 active redundant system with restorable elements (see e.g. IEC 61165:2006, Fig. B.7). In that case the down time (DT) would be used instead of the safe down time (SDT). By using SDR (inverse of SDT), it represents an upper bound (being therefore more conservative).

The formula becomes, when A and B are identical:

$$FFR \approx \frac{2FR^2}{SDR} = 2FR^2 \times SDT = 2FR^2 \times (T_D + T_N) \quad \text{(B.2)}$$

Validity of these formulas relies on the following assumptions which need to be justified for each application of the formulas:

— the rates are constant over time,

— any faults which could be hazardous if combined with a second fault are detected and negated,

— hazardous common cause failures (CCF) can be neglected,

— FR x SDT << 1

EXAMPLES

Taking two identical items with a MTBF of 10 000 hours (FR = 10^{-4}) and a SDT of 1 hour, then the resulting failure rate for the parallel system (AND combination in failure logic) is $2x10^{-8}$ per hour.

If SDT is 1 000 hours (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. Note however that this result is affected by large approximation error: in fact in this case the condition FR x SDT << 1 is no longer respected.

If SDT would be the lifetime, then the gain would become even more marginal.

B.3 Effects of faults

B.3.1 Effects of single faults

Any safety-related function shall meet its TFFR in the event of random fault.

It is necessary to ensure that SIL 3 and SIL 4 systems remain safe in the event of any kind of single hazardous random hardware fault which is recognized 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 three different ways:

1) 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 can progress only if the necessary numbers 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, in relation with the TFFR target.

   Hazardous random faults that could be dormant, causing errors only under particular conditions, shall be detected by online periodical monitoring.

2) reactive fail-safety

   This technique allows a safety-related function to be performed by a single item, provided its safe operation is ensured 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 can be regarded as a second item, which shall be independent to avoid common-cause failures.

3) 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.

   To use this technique the following requirements shall be applied:

   — The effect of every credible failure mode (and relevant combinations of failure modes) of each component identified in Annex C shall be identified, analysed, demonstrated as non-hazardous through physical tests, technical justifications or simulation. Dedicated failure tests might be necessary to confirm the effect of credible failure modes.

   — Any failure mode which is claimed to be incredible (for example, because of inherent physical properties) shall be justified using the procedure defined in Annex C. In this case, the hazard occurrence can be considered negligible and a hazardous failure rate of zero may be assumed.

   Inherent fail-safety can also be used for certain parts 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.

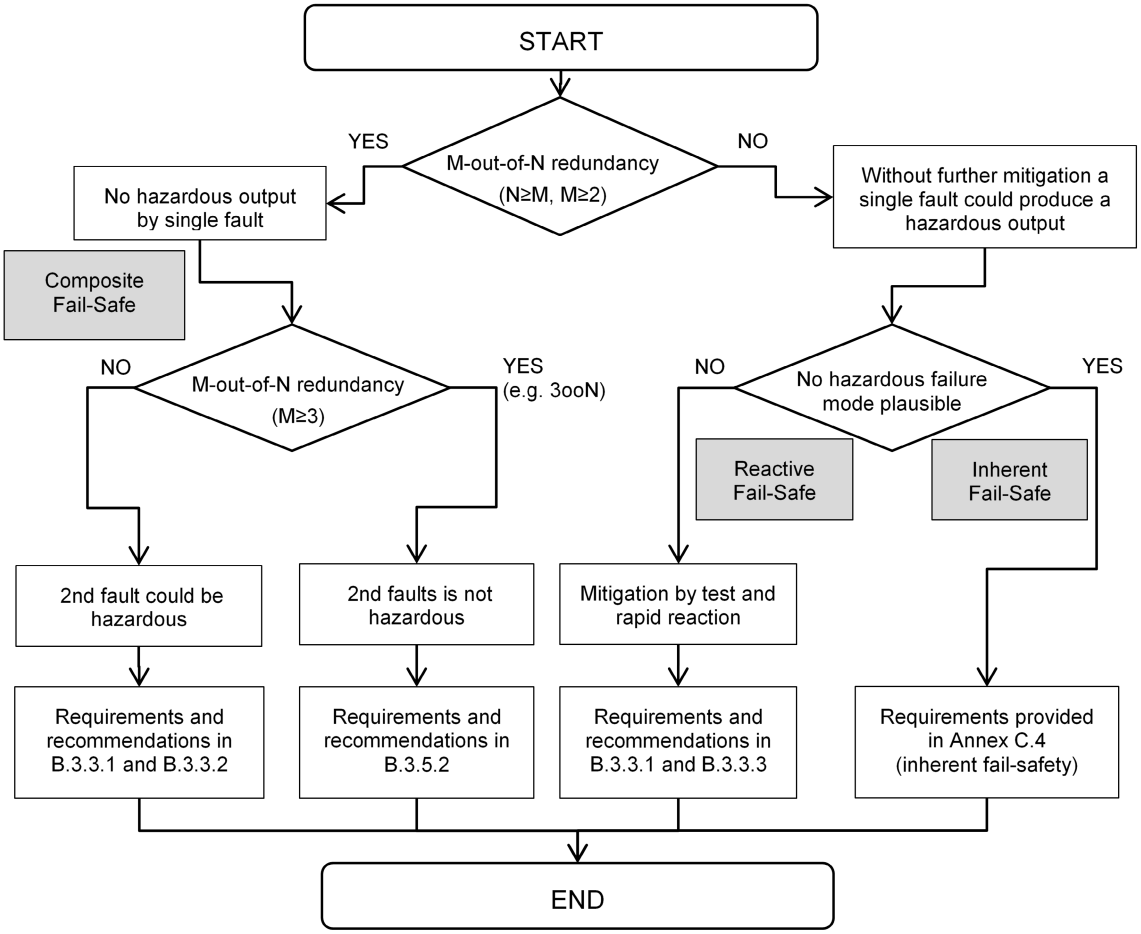
Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods.

The component failure modes to be considered in the analysis shall be identified using the procedures defined in Annex C.

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 also quantitative where credible data are 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.

A flow-chart showing the application of the three different kinds of fail-safety, and related applicable provisions, is given in Figure B.2.



NOTE M-out-of-N redundancy means redundancy wherein at least m of the total n items function and therefore meet the requirements.

Figure B.2 — Single and multiple fault control

B.3.2 Influences between items

B.3.2.1 General requirements

In systems containing items whose simultaneous malfunction could be hazardous, independence between items is a mandatory precondition for safety concerning single random faults.

This is applicable to Composite Fail-Safety (independence between the two items performing the safety-related function) as well as to Reactive Fail-Safety (independence between the item performing the function and the checking/testing/detection function).

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 design shall be arranged to minimize potentially hazardous consequences of loss of independence caused, for instance, by a systematic design fault.

As an example, the various types of influence in a system consisting of two operating items are represented in Figure B.3. This figure can be extended to systems consisting of more than two operating items.

In accordance with Figure B.3, several types of influences can be identified:

— Internal influences

  Type A: physical internal influences

  Type B: functional internal influences

— External influences

  Type C: physical external influence

  Type D: functional external influences

Functional influences (types B and D) are influences via transmitted information (e.g. data or signals): this is the case when faulty information in one item influences another item in a hazardous manner. Protection against those influences requires specific measures to be defined on a case by case basis.

Types A and C are influences resulting from other physical causes, as further detailed in the following subclauses.

B.3.2.2 Type A for SIL 3 and SIL 4

If no physical connection exists between internal items of a system, there are no physical influences. Therefore, internal independence is achieved.

NOTE A physical connection is any medium between items, for example:

— galvanic connection;

— electromagnetic coupling.

This is a condition hardly reachable in reality, so measures shall be taken to avoid non-intentional physical internal influences.

These measures may be scaled in case of "primary" or "secondary" independence.

Independence of two items whose simultaneous malfunction could be hazardous is called "primary independence". Related items are referred to as "main items".

A N-out-of-M system consists of M independent main items. Each main item can have one or more so-called "additional items" checking the main item. The degree of independence between a main and an additional item is called "secondary independence".

Secondary independence may be less stringent than primary independence, since simultaneous malfunction between a main item and an additional item would not be hazardous, provided that any fault of a main item is detected before it can become hazardous through further faults of another main item.

The following recommendations are given for primary independence.

1) Measures should be taken to avoid non-intentional galvanic connections (protection of internal galvanic insulation). Insulation distances (creepage distances and clearances) should be dimensioned at least in accordance with the requirements for reinforced insulation of EN 50124-1.

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

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

c) Insulation between insulated wires in the same cable.

d) Insulation between insulated windings in the same transformer. Maximum temperature inside transformers should be limited (including fault conditions), to avoid carbonization.

e) Insulation between insulated items inside an opto-coupler. Maximum temperature inside opto-couplers should be limited (including fault conditions), to avoid carbonization.

2) Measures should be taken to avoid non-intentional effects via intentional connections (protection of internal interfaces).

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

3) Measures should be taken to avoid non-intentional effects via electromagnetic coupling (protection against internal cross-talk).

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

   a) 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.

   b) If different lines on the same board need to be protected against cross-talk occurring between them, the necessary separation distance depends on the technology used, 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.

   c) 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.

The following simplifications to primary independence are given for secondary independence.

1) Insulation distances (creepage distances and clearances) should be dimensioned at least in accordance with the requirements for basic insulation of EN 50124-1.

2) 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).

3) Voltage monitoring is recommended. At least the voltage-monitoring (additional item) should not be influenced by the faults of the power-supply (i.e. main item).

B.3.2.3 Type C for SIL 3 and SIL 4

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

NOTE 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. Subclause 7.2 (Section 4 of the Technical Safety Report) contains requirements for external influences which shall be considered.

The following recommendations are given to provide physical external independence.

1) Measures should be taken to avoid non-intentional effects of EMI/ESD disturbing correct operation, in accordance with EN 50121-4.

2) The specified climatic conditions should normally be complied with. Measures should be taken to minimize the risk of the system being operated outside its specified climatic conditions.

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

   a) measures should be taken to ensure reliable correct operation in spite of mechanical stress-conditions;

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

4) Measures should be taken to ensure reliable correct operation under chemical stress-conditions.

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

   a) non-permitted supply voltages (outside data-sheet values for supplied systems, subsystems or equipment) should be disclosed by voltage-monitoring triggering an enforced safe state before hazardous situations are possible;

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

6) 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):

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

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

   c) creepage distances between live parts and exposed conductive parts/earth/circuits whose correct operation needs to be protected should be dimensioned at least in accordance with EN 50124-1 and considering maximum rated r.m.s. voltages during operation;

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

B.3.2.4 Type A and C for SIL 1 and SIL 2

For SIL 1/SIL 2 functions, the same recommendations as given for SIL 3/SIL 4 functions (see B.3.2.2 and B.3.2.3) apply, with the following exceptions:

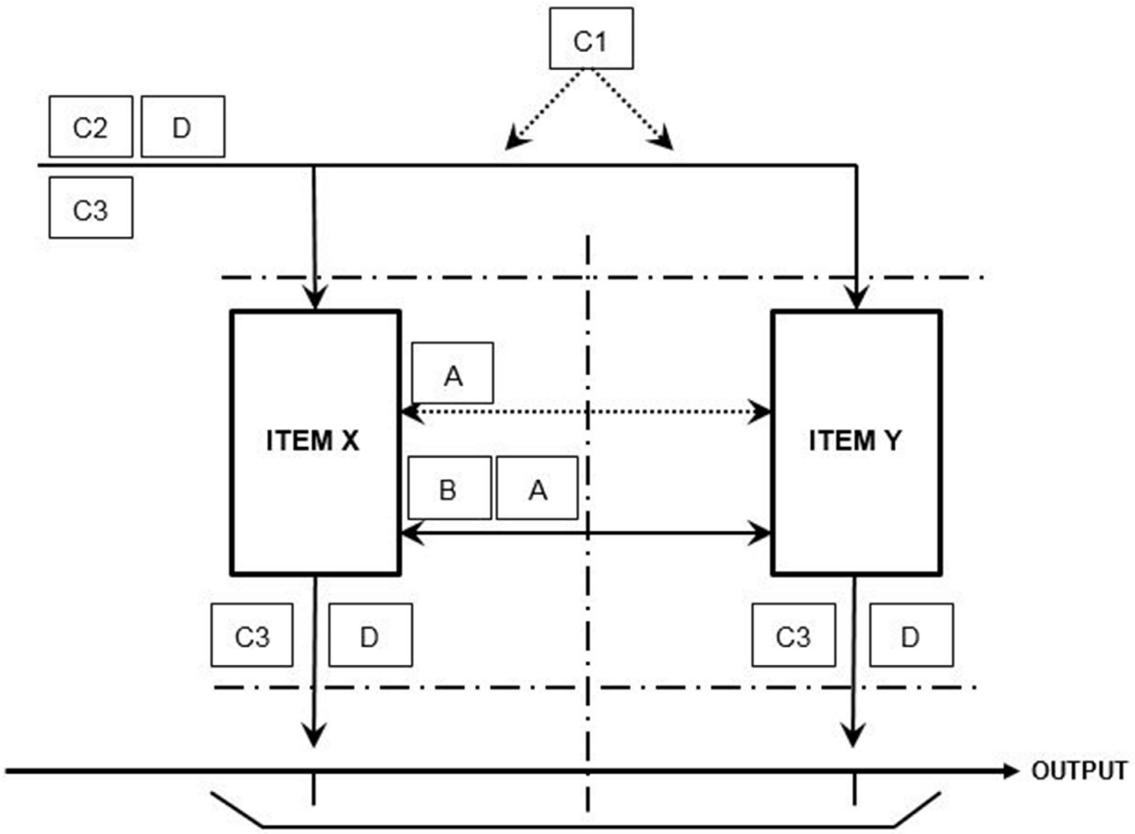
1) the European Standard EN 50124-1 requirements for basic insulation may be applied, provided that failures related to rupture of insulation do not exceed the specified TFFR;

2) protecting devices may not require inherent fail-safety properties, provided that failures related to loss of protection do not exceed the specified TFFR;

3) voltage monitoring may not be present, provided hazardous faults related to power supply do not exceed the specified TFFR.

Legend:

- Intentional connection
- Non-intentional connection (possibly caused by a fault)
- Independence (if specified measures are met to avoid non-intentional influences and connections)
- Front contact (normally-open contact)
- Two front contacts (used symbolically as an AND for two independent non-restrictive activities)
- A — Physical internal influence (non-intentional)
- B — Functional internal influence (non-intentional, using intentional connection)
- C1 — External environmental influence (EMI, ...) (non-intentional)
- C2 — External influence by power supply (non-intentional, using intentional connection)
- C3 — External influence across input/output (process working voltages, EMI-induced voltages) (non-intentional, using intentional connection)
- D — Functional external influence (non-intentional, using external connection)



"AND" condition for the non-restrictive state of the output

Figure B.3 — Influences affecting the independence of items

B.3.3 Detection of single faults

B.3.3.1 General requirements

A first fault (single fault) which could be hazardous, either alone or if combined with a second fault, shall be detected and negated, i.e. a safe state is enforced and then retained in a time sufficiently short to fulfil the specified quantitative 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, e.g. by using Fault Tree Analysis (FTA) (see Table E.6).

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 Figures B.4 and B.5.

The techniques used to achieve detection and negation of single 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.

Single random faults which could be hazardous shall be detected and negated by technical means or by operational or maintenance procedures.

For SIL 3 and SIL 4 function, single random faults which could be hazardous should be detected and negated by technical means.

B.3.3.2 Provisions for SIL 3/SIL 4 composite fail-safety functions (dual electronic structure)

This subclause applies to single-fault detection in composite (2-out-of-N) fail-safety.

In order to properly use AND combinations between two independent items X and Y, each item shall have an independent failure detection and negation mechanism. For item X (or Y), this mechanism may be performed by item Y (or X). If an item does not have such mechanism, then the installed lifetime or periodic test interval of the item shall be taken into account.

1) Periodic tests for faults in all items should be implemented. The tests should be representative for all credible faults affecting the safe operation, and should be finished within a time < SDT.

   Detection of faults in integrated circuits should be compliant with Table B.1.

   If independent failure detection is performed by periodic testing, evidence shall be given that faults not covered by periodic tests are not hazardous (i.e. these faults are demonstrated to be safe, alone or combined with others).

2) For two items A and B, whose simultaneous malfunctioning could be hazardous, having same or comparable safe down times SDT (SDT = SDT_A = SDT_B), this SDT should not exceed the value:

$$SDT \leq \frac{TFFR}{2(FR_A \times FR_B)} \tag{B.3}$$

   The following Formula (B.5) can be derived from Formula (B.3).

With the following assumptions:

— If $T_D >> T_N$: 1/SDR = SDT = $(T_D + T_N) \approx T_D$

— if a periodic test with T_T (testing time) is used,

T_D can be considered, on average,

equal to $T_T/2$, therefore: 1/SDR = SDT = $(T_D + T_N) \approx T_D = T_T/2$

the Formula (B.1) becomes:

$$FFR \approx (FR_A \times FR_B) \times T_T \quad \text{(B.4)}$$

This can be used to dimension T_T, given a target TFFR for which FFR < TFFR:

$$T_T < \frac{TFFR}{(FR_A \times FR_B)} \quad \text{(B.5)}$$

An alternative approach for the definition of SDT is given in the German Mü8004 principles (see Bibliography). The basic rule for dangerous double faults is given by:

$$SDT \leq \frac{k}{1000(FR_A + FR_B)} \quad \text{(B.6)}$$

where k depends on the system configuration:

k = 1 for a 2 out of 2 system;

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

When $FR_A = FR_B = FR$, Formulas (B.3) and (B.6) are equivalent if

$$\frac{TFFR}{FR} = \frac{k}{1000} \quad \text{(B.7)}$$

Typically the first term of this equivalence is higher than the second one and therefore the Mü8004 Formula (B.6) can be considered more conservative than Formula (B.3).

3) The failure rates mentioned in item 2) of this list 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 leads to a conservative result (higher failure rate).

4) If, within an electronic system 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 adopted.

5) If an electronic system free from random faults 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 in accordance with item 2) of this list. When needed, all the periodic tests implemented should then be executed at start-up, or alternatively the system should be thoroughly tested off-line in a controlled manner before restoring operation.

NOTE To evaluate the testing time it can be considered that the reliability of electronic components is 20 times better when the equipment is not powered.

B.3.3.3 Provisions for SIL 3/SIL 4 reactive fail-safety functions

The following provisions apply to single-fault detection in reactive fail-safety.

1) When the safety-related function is performed by a single item, the detection and negation time of a wrong side failure (SDT) is the maximum total time to detect and react in a safe way to all single faults affecting the safe operation. This time shall not exceed the specified limit for the duration of any hazardous condition.

   EXAMPLE:
   SDT could assume the following value, in order to avoid any hazardous condition:

   SDT < 100 ms, if the controlled equipment is a signalling relay with larger rise time.

2) During the time SDT, the first safety-related failure shall be detected and it shall trigger a safety reaction.

3) Integrity of the checking/testing/detection function (second item) shall be ensured throughout the lifetime of the system, leading to safe state in case of its loss.

B.3.4 Action following detection (retention of safe state)

For SIL 3 and SIL 4, after detection of a first fault, the system, subsystem or 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.

These requirements are illustrated in Figures B.4 and B.5 and Table E.4.

After detection of a first fault, and having enforced 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, subsystem or 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.

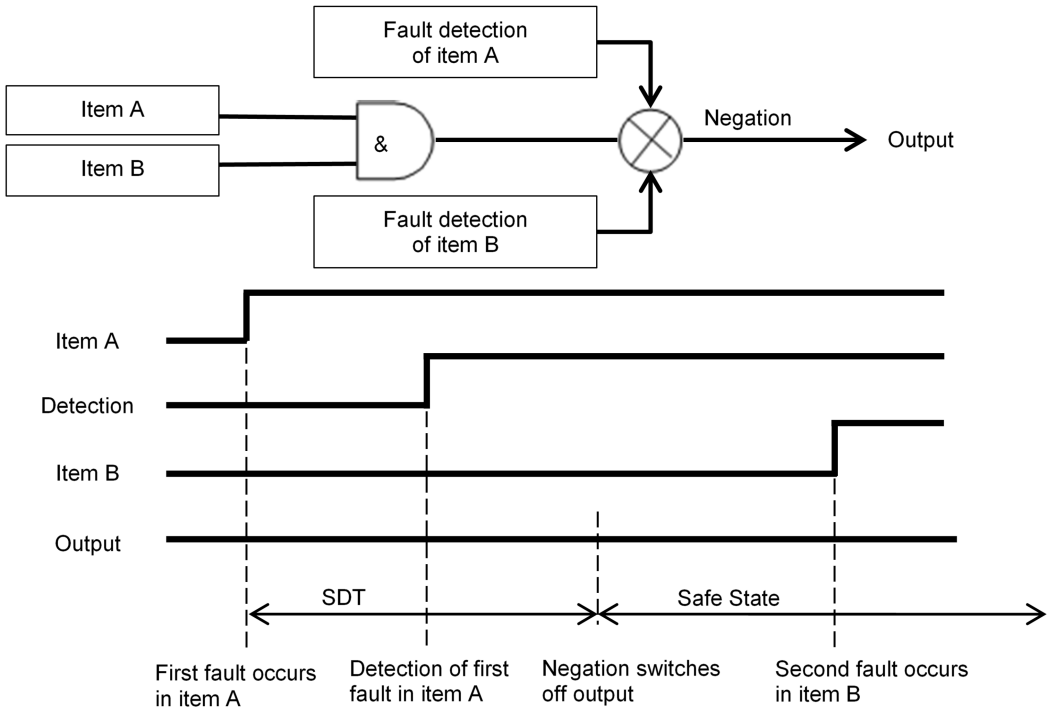


Figure B.4 — Detection and negation of single faults – Composite Fail-Safety

With reference to Figure B.4, the probability of a first fault, combined with the probability of a second fault occurring during the first fault detection-plus-negation time (SDT), shall be less than the specified probabilistic target.

NOTE Fault detection of item A is typically performed by item B and vice versa.

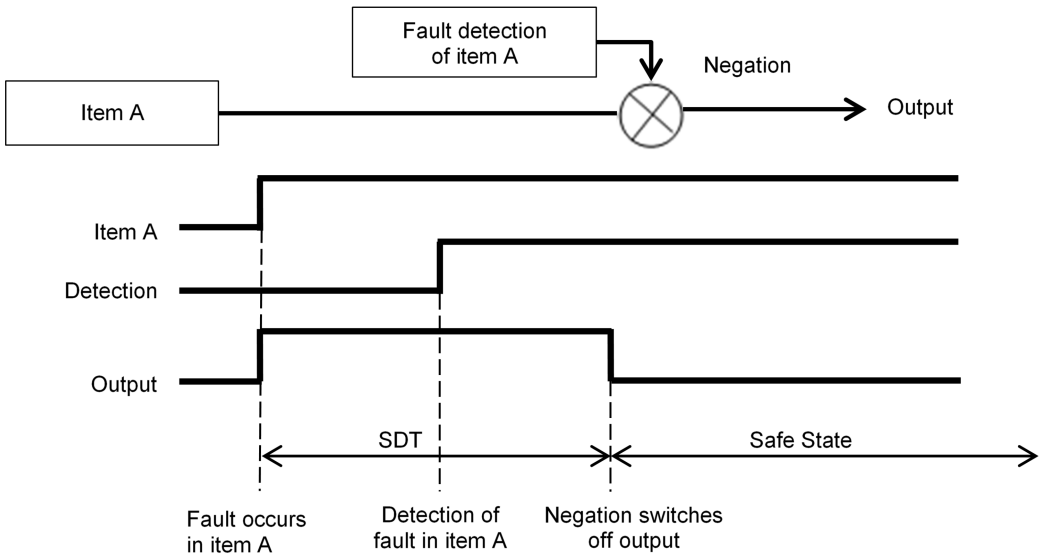


Figure B.5 — Detection and negation of single faults – Reactive Fail-Safety

With reference to Figure B.5, detection-plus-negation time SDT after a fault in function A shall not exceed the specified limit for the duration of a transient, potentially hazardous output.

B.3.5 Effects of multiple faults

B.3.5.1 General requirements

Multiple faults (for example, double or triple faults) which could be hazardous, either directly or if combined with a further fault, shall be detected and negated, i.e. a safe state is enforced and then retained in a time sufficiently short to fulfil the specified quantified safety target.

A suitable method, for example Fault Tree Analysis (FTA), shall be used to demonstrate the effects of multiple faults (see Table E.6).

The techniques used to achieve detection and negation of multiple faults within the permitted time shall be shown, including supporting calculations.

A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance that a hazardous 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.3.5.2 Provisions for SIL 3/SIL 4 composite fail-safety functions (multiple electronic structure)

The following measures provide conditions for multiple-fault detection in composite fail-safety (electronic systems with more than three independent items, i.e. 3-out-of-N and higher tolerances).

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 other items should be taken into account.

2) Simultaneous faults in two items should be non-hazardous. This means that at least three independent items are necessary.

3) Periodic tests for faults should be implemented. The tests should be representative for all credible faults affecting the safe operation, and should be finished within a time < SDT.

   Detection of faults in integrated circuits should be compliant with Table B.1.

   NOTE Periodic tests could be limited to the dangerous faults identified within the "DC fault model", i.e. stuck-at faults, stuck-open, open or high impedance outputs and short circuits between signal lines.

4) Depending on the sum of the failure rates ($FR_A+FR_B+FR_C$) of at least three identical items (A, B, C), whose simultaneous malfunction could be hazardous, the detection-plus-negation time SDT for double faults should not exceed the value:

$$SDT \leq \frac{2}{FR_A + FR_B + FR_C} \tag{B.8}$$

   This engineering rule is derived from to Mü8004 rules and should be used for definition of the SDT. This rule is considered as aligned with current practices and conservative with respect to analytical formula for combination of three or more faults where Formula (B.1) does not apply.

5) 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 of each item (FR) does not exceed the value:

$$FR \leq 2 \times 10^{-4}\ h^{-1} \tag{B.9}$$

6) The failure rates mentioned in 4) 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.

7) If within a system 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 adopted.

Table B.1 — Measures to detect faults in integrated circuits by means of periodic online testing (1 of 2)

component	Failure Modes	Measures
CPU		
Register, Internal RAM	DC fault model for data and addresses Dynamic crossover for memory cells Change of information (including those caused by soft errors, see NOTE 1) No, wrong or multiple addressing	One of the following diagnostic measures should be implemented depending on the architecture: - Comparator (HW): The signals of independent processing units are compared cyclically by a hardware comparator and enable the detection of a first fault. The comparator may itself be externally tested or inherently fail-safe. - Reciprocal comparison by software: Two processing units exchange data (including results, intermediate results and test data) reciprocally. A comparison of the data are carried out using software in each unit, and detected differences enable a safe state to be triggered. - Majority Voter (HW): A voting unit using the majority principle is used to detect and negate a first fault (i.e. negation of faulty channel). The voter may itself be externally tested or inherently fail-safe. - Coded processing (single item): Processing units or software can be designed with special coding strategy ensuring fault detection. Another item should be present to ensure negation of fault. - Other measures can be defined, provided evidence of detection of listed failures modes is demonstrated. Efficiency of comparison techniques depends on the extent of data or signals which are compared, in relation with the faults to be detected.
Instruction decoding and execution	No definite failure assumption	
Program counter, stack pointer	DC fault model Change of addresses (including those caused by soft errors)	
Clock	Incorrect frequency Period jitter	One of the following diagnostic measures should be implemented: - Comparison of clocks signals or results (e.g. counter) between channels of a M-out-of-N architecture. - Time monitoring by an independent item (e.g. watchdog). This item may itself be externally tested or inherently fail-safe.
Reset	DC fault model Drift and oscillation Individual components do not initialize to reset state	If independent reset-generators are used for each processing unit, then a wrong reset in one channel can be detected by comparison.

Table B.1 — Measures to detect faults in integrated circuits by means of periodic online testing (2 of 2)

component	Failure Modes	Measures
Memory		
Invariable	All faults that affect data in the memory	One of the following diagnostic measures should be implemented: — signature using a cyclic redundancy check (CRC) algorithm with the resulting value being at least two words in size (16-bit). — block replication: The address space is duplicated in two memories. The first memory is operated in the normal manner. The second memory contains the same information and is accessed in parallel to the first. The outputs are compared and a failure message is produced if a difference is detected. In order to detect certain kinds of bit errors, the data are stored inversely in one of the two memories and inverted once again when read.
Variable	DC fault model for data and addresses Dynamic cross-over for memory cells Change of information caused by soft errors No, wrong or multiple addressing	A combination of the following diagnostic measures (for explanations see EN 61508-7:2010, A.5) should be implemented and justified against the applicable failure modes: — RAM test "galpat" (or "transparent Galpat") — RAM test "Abraham" — Double RAM with HW/SW comparison and read/write test — Error Detecting or Correcting Memories Codes (e.g. EDC/ECC), see NOTE 2. Other measures can be defined, provided evidence of detection of listed failures modes is demonstrated.
Power supply (for integrated circuits)	DC fault model drift and oscillation	If independent power supplies are used for each computing channel, then a wrong supply voltage in one channel should be detected by comparison. In cases of no independence, or multiple faults, additional voltage monitoring should be necessary.

NOTE 1 A soft error is an issue that causes a temporary condition that alters stored data or processing in an unintended way. Causes of soft errors are: alpha particles from package decay, neutrons, external EMI noise and internal cross-talk.

NOTE 2 The effectiveness of the RAM monitoring with a modified Hamming code, or detection of data failures with error detection correction codes (EDC/ECC) depends on the inclusion of the address into the Hamming code, and relies on respective measure to detect multi-bit common cause faults, e.g. multiple addressing (multiple row select, multiple local to global bit line switches activated), production row and column replacement (production yield measure to mask production faults). It is therefore necessary to analyse coverage of this technique and define additional measures if necessary.

B.3.6 Defence against systematic faults

In addition to the quality and safety management techniques which are used to minimize the probability of human error (see 5.2 and 5.3), technical measures shall be taken such that in the event of a hazardous systematic fault 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 subsystem or equipment which has been designed to be safe, an accident would still be unlikely to occur.

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 European experience and also from the following sources listed in Bibliography:

— UIC/ORE Report A155/RP12

— MIL-HDBK-338B

— German Federal Railways Mü8004

— Reliability Analysis Center Report, Failure Mode / Mechanism Distribution, FMD-2013

— IEC 61709

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.15 contain lists of hardware component failure modes which shall be used as a basis for design and analysis, unless justification is provided for any variation. The general provisions 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 additional failure modes shall be drawn 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

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

The hazardous failure modes shall be identified and the following techniques should be used:

— top-down approach, using a technique such as Fault Tree Analysis;

— bottom-up approach, using Failure Modes and Effects Analysis.

The combination of both approaches is more efficient than a single method.

An 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 hardware design and/or 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; or

c) only for SIL 1 and SIL 2, if the occurrence of the identified failure modes can be kept within the TFFR, no detection and negation detection are necessary. Also in this case a pessimistic view shall be taken whereby the hazardous failure modes are assumed to take the full component failure rate.

For SIL 3 and SIL 4, also intermittent and transient failure modes shall be considered.

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 incredible. This justification shall include, but not necessarily be limited to, the following topics:

— theoretical explanation of inherent physical properties;

— evidence of compliance with recognized quality standards;

— explanation of special construction of the component;

— 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 the 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.

The justification needs not to be repeated 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 incredible; these failure modes are indicated by the relevant guidance in the footnotes of Tables C.1 to C.15. However, justification shall be provided for all failure modes which are considered to be incredible, including those which are indicated in the tables.

C.5 General provisions concerning component failure modes

(1) Tables C.1 to C.15 contain lists of credible failure modes of hardware components.

(2) Guidance concerning possible justification of the failure modes in Tables C.1 to C.15 as incredible is given in the tables Footnotes.

(3) The failure modes are as manifested at the boundary of the components, and not the internal physical causes of the failures.

(4) The listed failure modes that are affected by environmental influences, such as temperature variation or mechanical stress, shall be considered intermittent. Therefore the frequency of intermittent failures shall be in accordance with the relevant environmental standards.

(5) Variations within the tolerances of a component's published specification are not considered to be failures. For justification of any component failure mode as incredible, some allowance should be made for variations which exceed the normal tolerances.

(6) It is assumed that components are operated within their published environmental limits. For justification of any component failure mode as incredible, some allowance should be made for excursions beyond the normal environmental limits.

(7) It is assumed that components are operated within their published electrical ratings. For justification of any component failure mode as incredible, a margin shall be ensured within the published electrical ratings, so that the component is protected from being overloaded.

(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 (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 (10). Stable mounting and/or special fastening shall be necessary if environmental conditions could change the position of a component.

(10) Where safety is reliant on insulation distances, the minimum insulation distances shall be defined in accordance with the application requirements (including material, technology, implementation, environmental and operating conditions, failure conditions and temporary overvoltages). For the minimum clearance and creepage distances, EN 50124-1 standards shall be used to determine minimum requirements based on reinforced insulation. EN 60664-1 shall be used to determine minimum requirements for solid insulation, based on double or reinforced insulation. These requirements may be further strengthened or complemented, if not suitable for a specific application.

(11) “Short circuit to case” failure mode is considered not applicable if the case is not conductive.

(12) The components that employ embedded microprocessors, such as the “intelligent” sensors, shall be analysed using the same methods for integrated circuits given in C.3.

Table C.1 — Resistors

A) All kinds of resistor and adjustable resistor excluding 4-terminal resistor	
Interruption	
Short-circuit	(a)
Increase of resistance value	
Decrease of resistance value	(a)
Short-circuit to case	
B) Four-terminal resistor	
Interruption of each terminal	
Interruption of resistance material	(b)
Short-circuit	(a)
Increase of resistance value of each terminal	
Decrease of resistance value	(a)
Short-circuit between two terminals of same side (between B and C or A and D)	(c)
Short-circuit to case	

(a) The body shall have no hollows.

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 reinforced insulation.

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

The component shall be coated with cement or enamel.

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.

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

The coating shall be non-conductive, even at the highest temperature including fault conditions.

(b) 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.

(c) Two terminals of the resistor shall be connected independently to each side of the component.

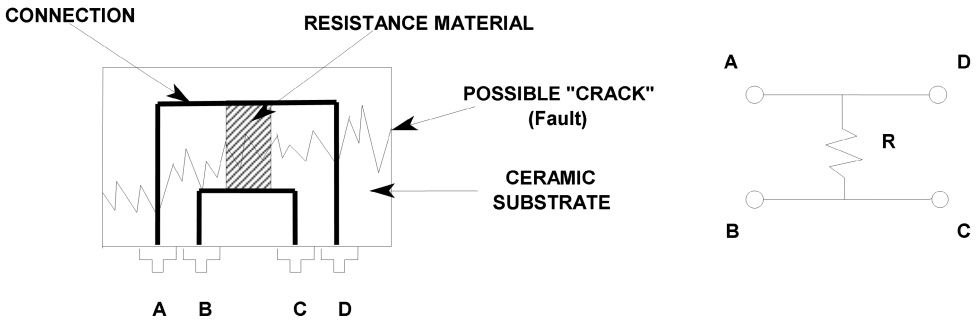


Figure C.1 — Four terminals resistor fault

Table C.2 — Capacitors

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

a) 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, with electrical and mechanical characteristics to guarantee double or reinforced insulation (following EN 50124-1) and self-healing properties at the working source impedance and over the working voltage range.

(b) Justification of the failure mode as incredible requires demonstration that both geometrical and dielectric parameters cannot significantly change.

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

(c) Two terminals of the capacity shall be connected independently to each side of the component.

Table C.3 — Electromagnetic components

(A) Inductor	
Interruption of winding	
Short-circuit of winding:	
- between turns	(a)
- between layers	(b)
- whole winding	(b)
Short-circuit or decrease of insulation	
- between winding and body	(b)
Increase of resistance of winding	
Increase of inductance	(c)
Decrease of inductance	(c)
(B) Transformer	
Interruption of any winding	
Short-circuit of any winding:	
- between turns	(a)
- between layers	(b)
- whole winding	(b)
Short-circuit or decrease of insulation	
- between winding	(b)
Short-circuit or decrease of insulation	
- between any winding and body	(b)
Increase of resistance of any winding	
Increase of inductance of any winding	(c)
Decrease of inductance of any winding	(c)
Change of transfer ratio	(d)
(C) Transductor (saturable reactor or magnetic amplifier)	
Interruption of any winding	
Short-circuit of DC winding	
Short-circuit of AC winding:	
- between turns	(a)
- between layers	(b)
- whole winding	(b)
Short-circuit or decrease of insulation resistance:	
- between DC and AC windings	(b)
- between any winding and body	(b)
Increase of inductance of AC winding	(c)
Decrease of inductance of AC winding	(c)
Increase of transductance	(e)
Decrease of transductance	
Increase of DC threshold voltage	

Decrease of DC threshold voltage	(e)

(D) Relay	
Interruption of any coil	
Interruption of any contact	
Short-circuit or decrease of insulation resistance:	
- across open contacts	(f)
- between coil and coil	(b)
- between coil and contact	(f)
- between coil and case	(b)
- between contact and contact	(f)
- between contact and case	(f)
Welding of contacts	(g)
Increase of contact resistance	
Contact chatter	
Increase of pick-up current	
Decrease of pick-up current	(h)
Increase of drop-away current	
Decrease of drop-away current	(h)
Change of pick-up to drop-away ratio	(h)
Increase of pick-up time	
Decrease of pick-up time	(h)
Increase of drop-away time	(h)
Decrease of drop-away time	(h)
Relay does not pick up	
Relay does not drop away	(h)
Closure of any front contact at the same time as any back contact (transient or continuous)	(h)
Non-correspondence between front contacts	
Non-correspondence between back contacts	

(a) There shall be only one layer of turns, separated by means of grooves in the insulated body, or the wire shall have double or reinforced insulation following EN 50124-1 and solid insulation.

The turns shall be securely fastened in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.).

(b) Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1 and solid insulation.

All windings and connections shall be securely fastened in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.).

Power dissipation shall be limited sufficiently to prevent internal carbonization, including fault conditions.

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

(d) 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 (a), (b) and (c) to be fulfilled.

(e) The transductance and the DC threshold voltage depend upon the properties of the magnetic core material. Therefore it shall be demonstrated that these magnetic properties cannot significantly change.

Transductance and DC threshold voltage also depend on the number of turns on each winding, and on the integrity of the magnetic coupling. Therefore it is necessary for (a), (b) and (c) to be fulfilled.

The output from a transductor is related to the number of ampere-turns in the control winding. It shall be demonstrated 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.

(f) All parts of the relay or switch mechanism shall be robustly constructed and securely fastened in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.), 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 double or reinforced insulation of EN 50124-1.

(g) Contact materials shall be chosen which are not capable of being welded. Alternatively, the maximum current shall be limited, to ensure that the temperature of the contacts does not reach a value at which welding could occur.

The risk of welding shall be further reduced by appropriate mechanical design and construction of the contacts. If a relay of type N is compliant to EN 50578, all requirements given in this note are assumed to be already satisfied.

(h) 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 magnetization 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);
- Design and construction of the operating mechanism such that it cannot become jammed.

For relays compliant to EN 61810-3 the failure mode “Closure of any front contact at the same time as any back contact (transient or continuous)” can be excluded without any further justification.

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	(a)
Decrease of threshold voltage	(a)
Short-circuit to conductive case	
(B) Zener diode	
Interruption	
Short-circuit	
Increase of Zener voltage	(b)
Decrease of Zener voltage	(b)
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	(a)
Decrease of forward threshold voltage	(a)
Short-circuit to conductive case	

(a) 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.

(b) 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.

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.

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 DC and/or AC amplification	(a)
Decrease of DC and/or AC amplification	
Increase of base-emitter conducting-state voltage	
Decrease of base-emitter conducting-state voltage	
Increase of threshold voltage V_{BE}	(b)
Decrease of threshold voltage V_{BE}	(b)
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	(a)
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	
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	

(a) 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.

(b) 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.

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	
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	(a)
Decrease of breakdown voltage	(a)
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	

(a) 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.

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.

Table C.8 — Opto-electronic components (1 of 2)

(A) Photo diode	
Interruption	
Short-circuit	
Increase of light sensitivity	(a)
Decrease of light sensitivity	
Increase of leakage current	
(B) Photo transistor	
Interruption	
Short-circuit	
Increase of light sensitivity	(a)
Decrease of light sensitivity	
Increase of leakage current	
(C) Light-emitting diode (LED)	
Interruption	
Short-circuit	
Increase of light emission (at constant current)	(b)
Decrease of light emission (at constant current)	
Increase of leakage current	
Increase of threshold voltage	(c)
Decrease of threshold voltage	(c)
Light emission below threshold voltage	(b)
Light emission with reverse polarity	(d)
Change of chromaticity of multicolour LED	

(D) Optocoupler and self-contained fibre-optic system	
Light emission with reverse polarity	
Short-circuit or decrease of insulation resistance: - between input and output - between adjacent systems in the same case	 (e) (e)
Short-circuit to casing	
Change of switching time	
Increase of current transfer ratio	(a) (b)
Decrease of current transfer ratio	
The failure modes of each element shall be considered, i.e. - photo diode - optical medium - photo transistor	

(a) 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.

(b) 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 can be assumed not to increase at constant current.

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

(c) 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.

(d) 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 can be assumed not to result in emission of light.

(e) Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1.

The construction of the component shall be robust and stable in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.).

Power dissipation in the component shall be limited sufficiently to prevent internal carbonization, including fault conditions.

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	 (a) (a)
Change of resonant frequency	(b)
Increase of transfer ratio	**(c) (d)**
Decrease of transfer ratio	
Increase of Q-factor	(d)
Decrease of Q-factor	**(b) (e)**

(a) Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1.

The input and output drive/coupling elements shall be securely fastened in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.).

(b) The component shall be robustly constructed in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.).

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 stabilized by temperature cycling and/or pre-operation for a sufficient time.

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

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

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

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

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

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	(a)
(B) Connector	
Interruption of: - one or more contacts - shield	
Short-circuit or decrease of insulation resistance:	

- between contact and contact	(a) (b)
- between contact and shell	(a) (b)
Wrong mechanical position	(c)
(C) Cable and wire	
Interruption or increase of resistance in one or more wires	
Interruption or increase of resistance of screen	
Short-circuit or decrease of insulation resistance:	
- between wire and wire	(d)
- between wire or wires and screen	(d)
- between wire or wires or screen and external conductive parts	(d)
Multiple interruptions and short-circuits	(d)
(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	

(a) The insulating material properties shall be stable for the whole life of the component.

For the minimum clearance and creepage distances, EN 50124-1 standards shall be used to determine minimum requirements based on double or reinforced insulation. EN 60664-1 shall be used for solid insulation requirements based on reinforced insulation or double insulation.

(b) The connector shall be robustly constructed and all parts securely fastened, in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.)

(c) 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.

(d) Sufficiently robust insulation shall be provided.

Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1.

Protection shall be provided against excessive physical damage.

Protection shall be provided against electrically conductive foreign bodies.

Table C.11 — Fuses

Interruption	
Parallel short-circuit	(a)
Increase of rupture current	(a)
Increase of rupture time	(a)
Reconnection after rupture	(b)
(a) 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. Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1. **(b) The fuse shall not have self-resetting or self-healing capability.**	

Table C.12 — Switches and push/pull buttons

Interruption of any contact	
Short-circuit or decrease of insulation resistance: - across open contacts - between contact and contact - between contact and case	 (a) (a) (a)
Welding of contacts	(b)
Increase of contact resistance	
Device jammed in current state	
Contact chatter	
Closure of any front contact at the same time as any back contact (transient or continuous)	
Non-correspondence between front contacts	
Non-correspondence between back contacts	
(a) All parts of the relay or switch mechanism shall be robustly constructed and securely fastened in order to comply with the severity of environmental stress conditions defined by the related applicable standards (e.g. mechanical vibrations, temperature cycles, etc.), 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 double or reinforced insulation of EN 50124-1. **(b) Contact materials shall be chosen which are not capable of being welded. Alternatively, the maximum current shall be limited, to ensure that the temperature of the contacts does not reach a value at which welding could occur.** The risk of welding shall be further reduced by appropriate mechanical design and construction of the contacts.	

Table C.13 — Lamps

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

Table C.14 — Batteries

Interruption	
Short-circuit: - of individual cell - of multiple cells - of whole battery	
Decrease of electromotive force	
Increase of internal resistance	

Table C.15 — Transducers/sensors (excluding those with internal electronic circuitry)

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

Annex D
(informative)

Example of THR/TFFR/FR apportionment and SIL allocation

In the following, an example is given to illustrate the quantitative breakdown of THR/TFFR/FR with a fault tree method, and the related SIL allocation.

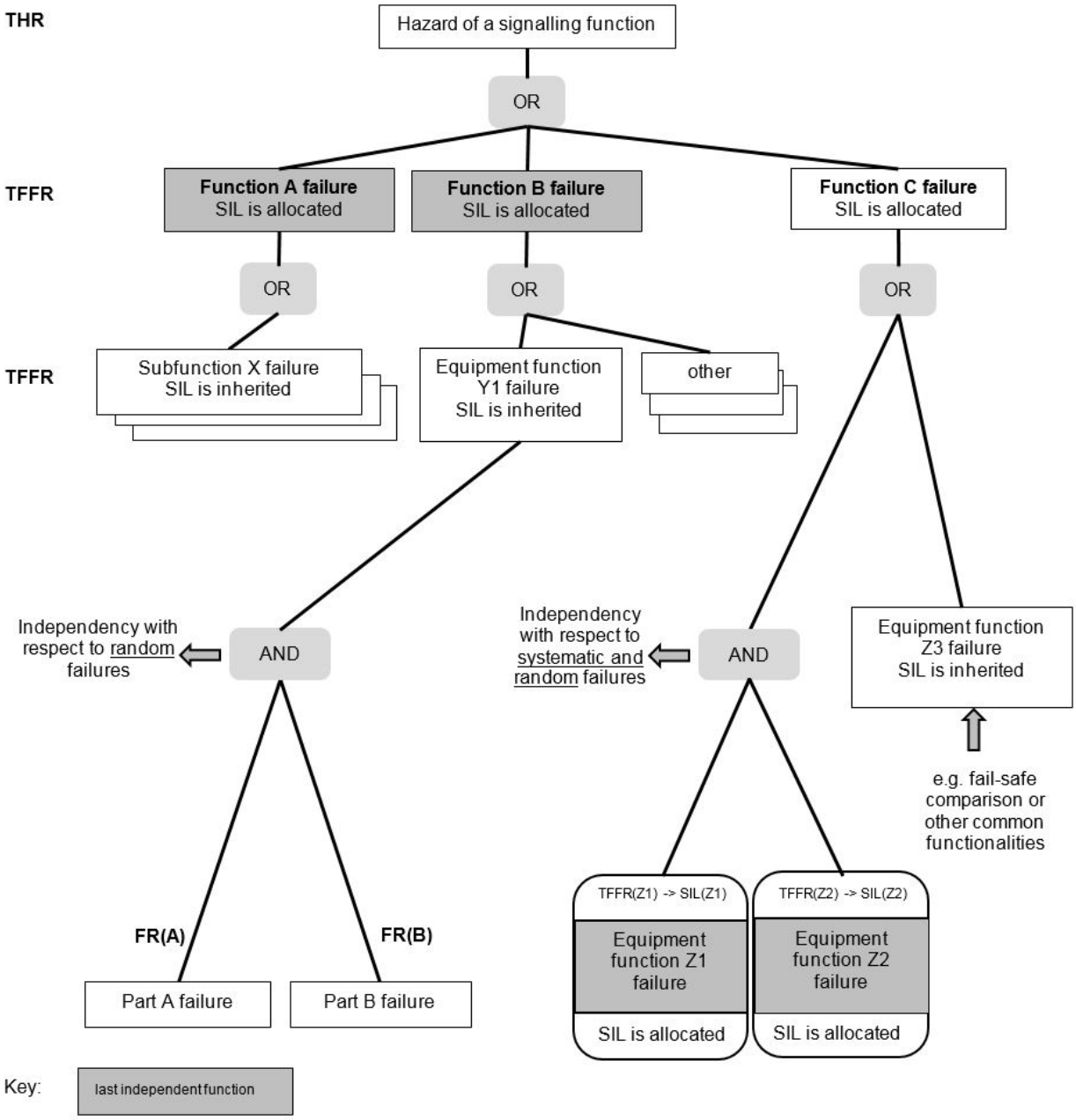


Figure D.1 — Example of THR/TFFR/FR breakdown and related SIL allocation

A higher or lower number of hierarchy levels can exist, depending on the application.

In the example, Function A, B and C failures can individually lead to the signalling system failure, which is considered the hazard being analysed, with an associated THR. The quantitative target for these functions (TFFR) is therefore more demanding than THR. The TFFR derived for these three functions leads to a SIL allocation, which is then a priori inherited by downstream sub-functions.

Function A is then performed by a set of subsystems performing subfunctions X, whose failures can individually cause the function to fail (e.g. track circuits whose failures can lead to a loss of the train detection function over a route).

Function B is performed by different subsystems and in particular:

— Equipment function Y1 (composite fail-safety architecture, where two parts are independent with respect to random faults, i.e. requirements of A.4.3.5 apply) and other equipment;

Function C is performed by different equipment functions and in particular:

— Equipment functions Z1 and Z2 that are to be demonstrated as being independent with respect to systematic and random faults (i.e. requirements of A.4.3.4, A.4.3.5 and A.4.3.6 apply);

— Equipment function Z3 that is implementing a fail-safe comparison between Z1 and Z2, as well as their common functionalities (e.g. elaboration of common inputs to Z1 and Z2).

NOTE Equipment function Z3 is not required if two completely independent equipments prevent the hazard without a need of comparison (e.g. both activate the brake independently).

The AND gate on the left, representing the combination of the two channels of Equipment function Y1, indicates independence only with respect to random faults: therefore TFFR is not further apportioned and SIL is inherited.

The AND gate on the right, comprising equipment Z1 and Z2, indicates independence with respect to both systematic and random causes, allowing further apportionment of TFFR and allocation of lower SILs.

Equipment function Z3, that represents the fail-safe comparison of Z1 and Z2 and their common functionalities, inherits the SIL from Function C.

Annex E
(normative)

Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults

E.1 Introduction

Safety Integrity Levels (SIL) are defined for safety-related functions. This annex sets out architectures, techniques/measures for the system/subsystems/equipment implementing those functions. Such techniques/measures can be used to avoid systematic faults and to control random and systematic faults, and are related to the Safety Integrity Levels 1 to 4.

The tables in this annex describe the various techniques/measures and makes recommendations regarding their use for each of the four SILs. The recommendations are graded as HR", "R", "-" and "NR". The meaning of these terms is as follows:

"HR" This symbol means that the measure or technique is Highly Recommended for this safety integrity level.

"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.

"NR" This symbol means that the technique or measure is positively Not Recommended for this safety integrity level.

If a technique or measure that is "HR" is not used the rationale behind not using it shall be detailed, unless an approved combination of techniques is selected.

If this technique or measure that is "NR" is used then the rationale behind using it shall be detailed.

Table E.1 — Safety planning and quality assurance activities

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 EN 50126-1 and EN 50126-2 and referred to in 5.3 of this document 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. Requirements for these activities are given in the main part of this document and referenced in Table E.1.

Table E.2 — Safety requirements specification

(referred to in 5.3.7)

Following the life cycle phases 1 to 4 described in EN 50126-1:

— Phase 1: Concept

——Phase 2: System definition and operational context

— Phase 3: Risk analysis and evaluation

— Phase 4: Specification of system requirements,

the results shall be documented in the safety requirements specification, which shall take account of the techniques/measures in Table E.2.

Table E.3 — Safety organization

During the preparation of a Safety Plan the safety management structure shall be identified. Requirements for these activities are given in the main part of this document and referenced in Table E.3.

Table E.4 — Architecture of system, subsystem or equipment

(referred to in B.3.4)

During the life cycle phase 5 (Architecture and apportionment of system requirements) and phase 6 (Design and implementation), the system architecture description shall be documented with consideration to Table E.4.

Table E.5 — Design features

(referred to in 5.3.8 and 7.2)

The Table E.5 gives techniques/measures for the avoidance and control of faults caused by

— random events;

— any residual design faults;

— environmental conditions;

— misuse or operating mistakes;

— any residual faults in the software;

— human factors.

Table E.6 — Failure and hazard analysis methods

(referred to in 7.2, B.3.1,B.3.3 and B.3.5.1)

In accordance with 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.

Table E.7 — Design and development of system, subsystem or equipment

(referred to in 5.3.8)

Design method 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.

Table E.8 — Safety verification and validation of the system

(referred to in 5.3.10 and 5.3.11)

The intended design shall be verified and validated with the techniques/measures provided in Table E.8.

Table E.9 — Application, operation and maintenance

(referred to in 8.2 and 7.2)

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 provided in Table E.9.

E.2 Tables of techniques and measures

Table E.1 — Safety planning and quality assurance activities

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Checklists	See 5.3.2				
2 Audit of tasks	See 5.3.11				
3 Inspection of issues of documentation	See 5.3.10				
4 Definition and review of safety plan	See 5.3.5				

Table E.2 — Safety requirements specification

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Graphical description, e.g. block diagrams	**R**	**R**	**HR**	**HR**	
2 Structured specification	**HR**	**HR**	**HR**	**HR**	(a)
3 Formal or semiformal specification	**-**	**-**	**HR**	**HR**	(b)
4 Computer aided specification tools	**-**	**R**	**R**	**R**	(c)

Approved combinations of techniques for SIL 3 and SIL 4 are:

- 1 and 2, or
- 2 and 3 (in case of semiformal specification), or
- 3 (in case of formal specification).

(a) In order to reduce complexity, it is recommended that a structured requirements specification is developed through a hierarchical structure of refined requirements. This technique structures the functional specification into partial requirements such that the simplest possible, visible relations exist between the latter. This analysis is successively refined until small clear requirements can be distinguished. The result is a hierarchical structure of requirements which provide a framework for the specification of the complete black-box functional and safety requirements. This method emphasizes the interfaces of the requirements and is particularly effective for avoiding interface specification errors.

(b) Formal or semi-formal specification provides a means of developing a description of a system based on a structured notation during the specification phase. Formal specifications are based on mathematical models of the system function and/or structure. Formal specification generally includes a verification process based on mathematical analyses to ensure the consistency of the resultant specification model. Semi-formal specification is recommended to express parts of a specification unambiguously and consistently, so that some mistakes, omissions and wrong behaviour can be detected. For semi-formal specification, in some cases the description can be analysed by machine or animated to display various aspects of the system behaviour.

	For formal and semiformal methods see EN 61508-7:2010.
(c)	Model oriented procedures with hierarchical subdivision, description of all objects and their relationship, common database, and automatic consistency check.

Table E.3 — Safety Organization

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Training of staff in safety organization	See 5.3.4.1				
2 Independence of roles	See 5.3.4.2 including Figure 5				
3 Qualification of staff in safety organization	See 5.3.4.1				

Table E.4 — Architecture of system, subsystem or equipment

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Separation of safety-related functions from non-safety-related functions to prevent unintended influences	See 7.2, “Section 3 of the Technical Safety Report”				
2 single electronic structure with self-tests and supervision	**R**	**R**	**NR**	**NR**	(a)
3 single electronic structure based on inherent fail-safety	**R**	**R**	**HR**	**HR**	(b)
4 single electronic structure based on reactive fail-safety	**R**	**R**	**HR**	**HR**	(c)
5 Dual electronic structure	**R**	**R**	**NR**	**NR**	(d)
6 Dual electronic structure based on composite fail-safety with fail-safe comparison	**R**	**R**	**HR**	**HR**	(e)
7 Diverse electronic structure with fail-safe comparison	**R**	**R**	**HR**	**HR**	(f)

For a given SIL all techniques of the grey shaded group are alternatives, i.e. at least one of these techniques should be chosen. For a given safety-related function, several techniques may be combined so as to address all kinds of faults affecting the function. Techniques 2 to 7 include also architectures where additional electronic structures are used for availability purposes (e.g. 2oo3).

(a) Technique 2 differs from a reactive fail-safe solution (technique 4) in these aspects:

1. the function and its checking/testing/detection might be not independent;

2. negation can depend on the actions of the operator or the maintainer.

Due to these possibilities, there is no assurance that the system remains safe in case of any single fault; therefore, being not fail-safe, the technique is not applicable for SIL 3 and SIL 4 functions. It is nevertheless necessary to ensure that occurrence of these single faults is considered within the safety target quantification and related TFFR.

(b) Inherent fail-safety is addressed in B.3.1 and C.4.

(c) Reactive fail-safety is addressed in B.3.1 and B.3.3.3.

(d) Technique 5 differs from a composite fail-safe solution (techniques 6 or 7) in these aspects:

1. the channels might be not completely independent;

2. comparison might be performed by a non-fail-safe voter;

3. negation can depend on the actions of to the operator or the maintainer.

Due to these possibilities, there is no assurance that the system remains safe in case of any single fault; therefore, being not fail-safe, the technique is not applicable for SIL 3 and SIL 4 functions. It is nevertheless necessary to ensure that occurrence of these single faults is considered within the safety target quantification and related TFFR.

(e) Composite fail-safety is addressed in B.3.1 and B.3.3.2.

(f) Technique 7 differs from technique 6 in these aspects:

1. the electronic structures have some technically diverse components/parts;

2. diverse components/parts can be demonstrated to fail differently in case of systematic faults and common cause influences.

Table E.5 — Design features

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Protection against operating / maintenance errors	**R**	**R**	**HR**	**HR**	(a)
2 Operator / maintainer friendliness to reduce the probability of human errors	**HR**	**HR**	**HR**	**HR**	(b)
3 Protection against single faults for discrete components	See B.3.1 and Annex C				
4 Protection against single faults for integrated circuits for digital electronic technology	See B.3.1, C.3 and, for SIL 3 and SIL 4, Table B.1				
5 Detection of single faults	See B.3.1 and B.3.3				
6 Multiple faults	See B.3.5				
7 Dynamic fault detection	See B.3.3.1				
8 Retention of safe state	See B.3.3.1 and B.3.4				
9 Program sequence monitoring	**R**	**HR**	**HR**	**HR**	(c)
10 Measures against voltage breakdown, voltage variations, overvoltage, low voltage	**R**	**R**	**HR**	**HR**	(d)
11 Control of temperatures outside specified range	**HR**	**HR**	**HR**	**HR**	(e)
12 Software architecture and design	See EN 50128				
13 Protection against sabotage (physical and IT-Security threats)	See 6.4				

(a) Wrong inputs (value range, electrical characteristics, time, consistency) should be detected via plausibility or consistency checks.

(b) Reduce the risk of human errors related to the interaction between the human (operator or maintainer) and the system by:

- limiting human intervention and

- avoiding unnecessary complexity.

(c) Temporal monitoring: external timing elements with a separate time base (for example watch-dog timers) are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that the triggering points are correctly placed in the program.

Logical monitoring: the correct sequence of the individual program sections is monitored using software (counting procedure, key procedure) or using external monitoring facilities. It is important that the checking points are placed in the program correctly.

Temporal and logical monitoring can be combined: e.g. a temporal facility monitoring the program sequence is retriggered only if the sequence of the program sections is also executed correctly.

(d) Overvoltage or under voltage is detected early enough so that the internal state can be saved in non-volatile memory (if necessary), and so that all outputs can be set to a safe condition by the power-down routine, or that all outputs can be switched to a safe condition, or there is a switch-over to a second power unit.

(e) Control of temperature ranges:

It is the operator's responsibility to operate the system within its specified temperature range (Safety Application Condition). Additionally, control of adherence to specified temperature range should protect the system in case of internal failures, e.g. failure of the cooling components, or temporary erroneous operation outside the specified range. Temperature control can be achieved by analysis of causes and safety effects or by technical measures like temperature supervision.

For SIL 3 and SIL 4, the need of a negation should be investigated.

Table E.6 — Failure and hazard analysis methods

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Failure Mode and Effects Analysis (FMEA)	**HR**	**HR**	**HR**	**HR**	(a)
2 Hazard and operability studies (HAZOP)	**HR**	**HR**	**HR**	**HR**	(b)
3 Fault tree analysis	**HR**	**HR**	**HR**	**HR**	(c)
4 Markov diagrams	**HR**	**HR**	**HR**	**HR**	(d)
5 Reliability block diagram	**R**	**R**	**R**	**R**	(e)
6 Zonal analysis	**R**	**R**	**R**	**R**	(f)
7 Common cause failure analysis	**HR**	**HR**	**HR**	**HR**	(g)
8 Historical event analysis	**R**	**R**	**R**	**R**	(h)
9 Cause-consequence diagrams	**R**	**R**	**R**	**R**	(i)
10 Event tree	**R**	**R**	**R**	**R**	(l)

For a given safety-related function, several techniques may be combined so as to address all kinds of faults affecting the function.

For SIL 1 and SIL 2, approved combination of techniques is:

- 1 or 2 (for Hazard Identification and Analysis, referred to in 5.3.7), and
- 3 or 4 (for quantification of Safety Targets), and
- 7 (in case of composite or reactive fail-safety; not deemed necessary in case of inherent fail-safety as the safety function is performed by a single item).

For SIL 3 and SIL 4, approved combination of techniques is:

- 1 or 2 (for Hazard Identification and Analysis, referred to in 5.3.7), and
- 3 or 4 (for quantification of Safety Targets), and
- 1 (at component level following Annex C, if no complete detection of functional failure modes can be demonstrated at higher level), and
- 7 (in case of composite or reactive fail-safety; not deemed necessary in case of inherent fail-safety as the safety function is performed by a single item).

(a) See as a reference EN 60812

(b) See as a reference EN 61882

(c) See as a reference EN 61025

(d) See as a reference EN 61165

(e) See as a reference EN 61078

(f) See as a reference EN 61508-7

(g) See as a reference EN 60812 and EN 61025

(h) See as a reference EN 61508-7

(i) See as a reference EN 31010

(l) See as a reference EN 62502

Table E.7 — Design and development of system, subsystem or equipment

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Structured design	**HR**	**HR**	**HR**	**HR**	(a)
2 Graphical description including for example block diagrams	**HR**	**HR**	**HR**	**HR**	
3 Modularization	**R**	**R**	**HR**	**HR**	(b)
4 Formal or semiformal design specification	**-**	**-**	**HR**	**HR**	(c)
5 Computer aided design tools	**-**	**-**	**R**	**R**	(d)
6 Environmental studies (EMC, vibration, etc.)	See 7.2 Section 4				

(a) In order to reduce complexity, a structured design specification using a hierarchical structure of refined design elements is recommended. This structure emphasizes internal interfaces and is particularly effective for avoiding interface failures. For SIL 3 and SIL 4, the design should be fully traceable back to the requirements specification and include references between specification, design, circuit diagrams and application documentation. See also Table E.1 footnote (a).

(b) Modularization aims to reduce complexity and avoid failures related to interfacing between subsystems. The system is subdivided in modules of restricted size and functionality, and interfaces are detailed.

(c) Formal or semi-formal design specification provides a means of developing a description of an item based on a structured notation during the design phase. Formal design specifications are based on mathematical models of the item's function and/or structure. Formal design specification generally includes a verification process based on mathematical analyses to ensure the consistency of the resultant design model. Semi-formal design specification is recommended as a means of representing parts of a design specification unambiguously and consistently, so as to aid the detection of mistakes, omissions and incorrect behaviour. For some types of semi-formal design specification, the description can be analysed by machine or animated to display various aspects of the behaviour of the item.

(d) See also 6.3.

Table E.8 — Safety verification and validation of the system, subsystem or equipment

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Simulation	-	R	R	R	
2 Formal verification	-	-	R	R	
3 Functional testing of the system	HR	HR	HR	HR	(a)
4 Functional testing under environmental conditions	HR	HR	HR	HR	(b)
5 Design audit	R	R	HR	HR	
6 Design review	HR	HR	HR	HR	
7 Statistical confidence demonstrated by use (field experience)	R	R	R	R	(c)
8 Inspection of documentation	HR	HR	HR	HR	(d)
9 Ensure design assumptions are not compromised by manufacturing process	See 5.3.10 and 5.3.11				
10 Test facilities	See 5.3.10 and 5.3.11				
11 Ensure design assumptions are not compromised by installation and maintenance processes	See 5.3.10 and 5.3.11				

(a) Functional tests are carried out to demonstrate that the specified characteristics and safety requirements are fulfilled. Representative configuration data are included in functional tests. See also 5.3.10 and 5.3.11.

(b) Safety-related functions are tested under the specified environmental conditions (e.g. EN 50125-3) in order to demonstrate absence of physical external influences. See also 5.3.10 and 5.3.11.

(c) Statistical confidence should be considered optional and recommended where some previous evidence is not available. It needs to be based on use of components, subsystems or equipment, which have been shown by experience to have no hazardous faults when used, essentially unchanged, over a sufficient period of time in numerous different applications. Particularly for complex components with a multitude of possible functions (for example operating system, integrated circuits), the developer shall pay attention to those functions which have actually been tested by field experience. In the example of self-test routines for fault detection: if no break-down of the hardware occurs within the operating period, the routines cannot be said to have been tested, since they have never performed their fault detection function.

For field experience to apply, the following requirements should be fulfilled:

– unchanged specification;

– at least 10 systems in different applications;

– at least 10^5 operating hours and at least one year of service history.

The field experience is demonstrated through documentation of the vendor and/or operating company. This documentation should contain at least

– the designation of the system and its component, including version control for hardware;

– the users and time of application;

– the operating hours;

– the procedures for the selection of the systems and applications procured to the proof;

– the procedures for fault detection and fault registration as well as fault removal.

Regarding field experience from different applications, see also EN 61508-7:2010, B.5.4.

(d) Checklists, computer aided specification tools and inspection of the specification can be used in the verification activity of a phase.

Table E.9 — Application, operation and maintenance

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Production of applications operational and maintenance manuals and instructions	**HR**	**HR**	**HR**	**HR**	(a)
2 Training in the execution of operational and maintenance instructions	**HR**	**HR**	**HR**	**HR**	(b)
3 Maintenance friendliness	**HR**	**HR**	**HR**	**HR**	(c)
4 Protection against sabotage — physical threats	**R**	**R**	**R**	**R**	(d)
5 Protection against sabotage – IT-Security threats	**R**	**R**	**R**	**R**	(d)

(a) Safety-related operational, application and maintenance instructions should be traceable back to the design, including use of hazard log.

(b) Training should be extended to all operators and maintenance staff. See 7.2, Section 5.

(c) See 8.2

(d) See 6.4

Annex F
(informative)

Guidance on User Programmable Integrated Circuits

F.1 Introduction

F.1.1 Purpose

This annex, being informative, gives only additional information intended to assist the understanding or use of the document. It does not contain requirements or permissions. For any technique or measure, different levels of recommendations (NR, not recommended; R, recommended; HR, highly recommended) are given for different SILs. However, due to the informative status of the present annex, these recommendations must be understood as descriptive of the current status of the art.

This annex specifies the process and practical methods for the development of configuration for User Programmable Integrated Circuits (UPIC in the following). It is aimed at use in any area where there are safety implications. UPIC can also be defined as hardware items that are configured by a hardware description language.

This annex is intended as additional guidance that can be used for UPIC (especially configuration) with respect to non-configurable HW (e.g. microprocessors). Then all the clauses in the present standard applicable for non-configurable HW are also applicable to UPICs.

In addition, it includes guidance on the way to integrate UPICs within a safety architecture.

UPICs are commonly defined by the following acronyms:

— FPGA (field-programmable gate array);

— PLD (programmable logic device);

— EPLD (erasable programmable logic device);

— CPLD (complex programmable logic device);

— PAL (programmable array logic);

— PLA (programmable logic array);

— LCA (logic cell array).

F.1.2 Terminology and context

A UPIC is composed of at least 2 items:

— UPIC Hardware: It is an integrated circuit which is included within the hardware development process in compliance with Annex B and Annex C, considering relevant techniques and measures according Annex E.

— UPIC configuration: This is the configuration of the UPIC hardware. It is made by connecting logic circuits present in the UPIC hardware, as defined by a hardware description language. This configuration is not within the scope of EN 50128 and is the main subject of the present annex.

UPIC configuration can be divided into logic components. A logic component is a constituent part of UPIC configuration which has well-defined interfaces and behaviour with respect to the UPIC configuration architecture and design.

UPIC's design is often based on “IP Cores”, reusable units of logic that is the intellectual property (IP) of one party.

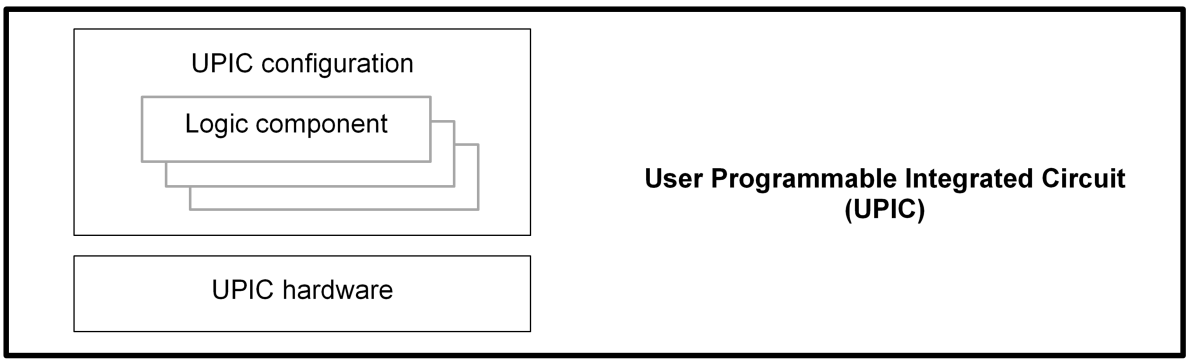


Figure F.1 — UPIC architecture

Where the UPIC is able to run SW (e.g. usage of soft processor cores), the SW is developed following the requirements of EN 50128.

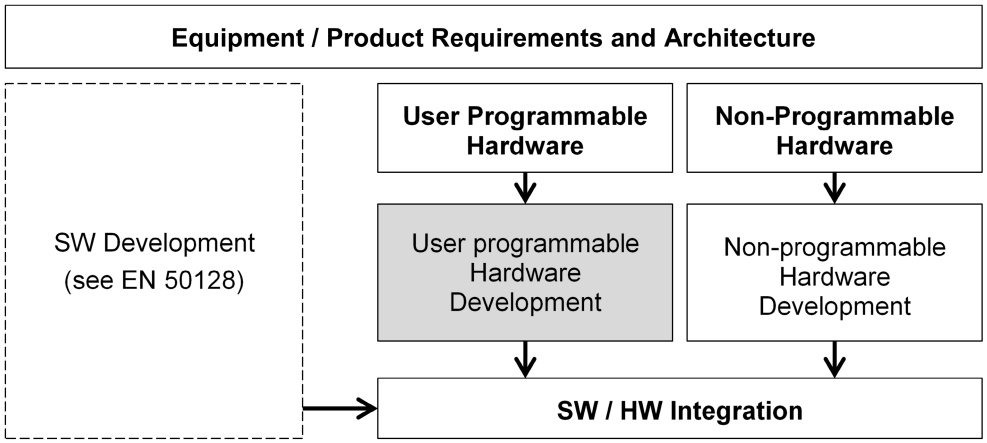


Figure F.2 — UPIC Development Context

F.2 UPIC life cycle

F.2.1 General

The UPIC development is carried out following the allocation done in the hardware requirements and architecture phase (see Figure F.3).

This annex covers a process suitable to be used within a framework-based development cycle, e.g. System on User Programmable Integrated Circuit (SoUPIC) or System on Chip (SoC), throughout reuse of pre-existing components (i.e. Intellectual Property Cores).

A life cycle model for the development of UPIC configuration is selected in compliance with general prescriptions defined in Clause 5.

Two examples of life cycle models customised for UPIC development are shown in Figure F.3 and Figure F.4.

Figure F.3 shows an example of top-down life cycle with design of dedicated logic components (new).

Figure F.4 shows a hybrid top-down / bottom-up life cycle where a set of IP Cores (pre-existing) are reused to cover requirements of an overall UPIC.

The two approaches might co-exist for a UPIC, for instance within an overall configuration that uses standard IP Cores for application-independent function (e.g. online tests of data structures integrity) and requires development of new logic components or functions which are addressing specific application requirements.

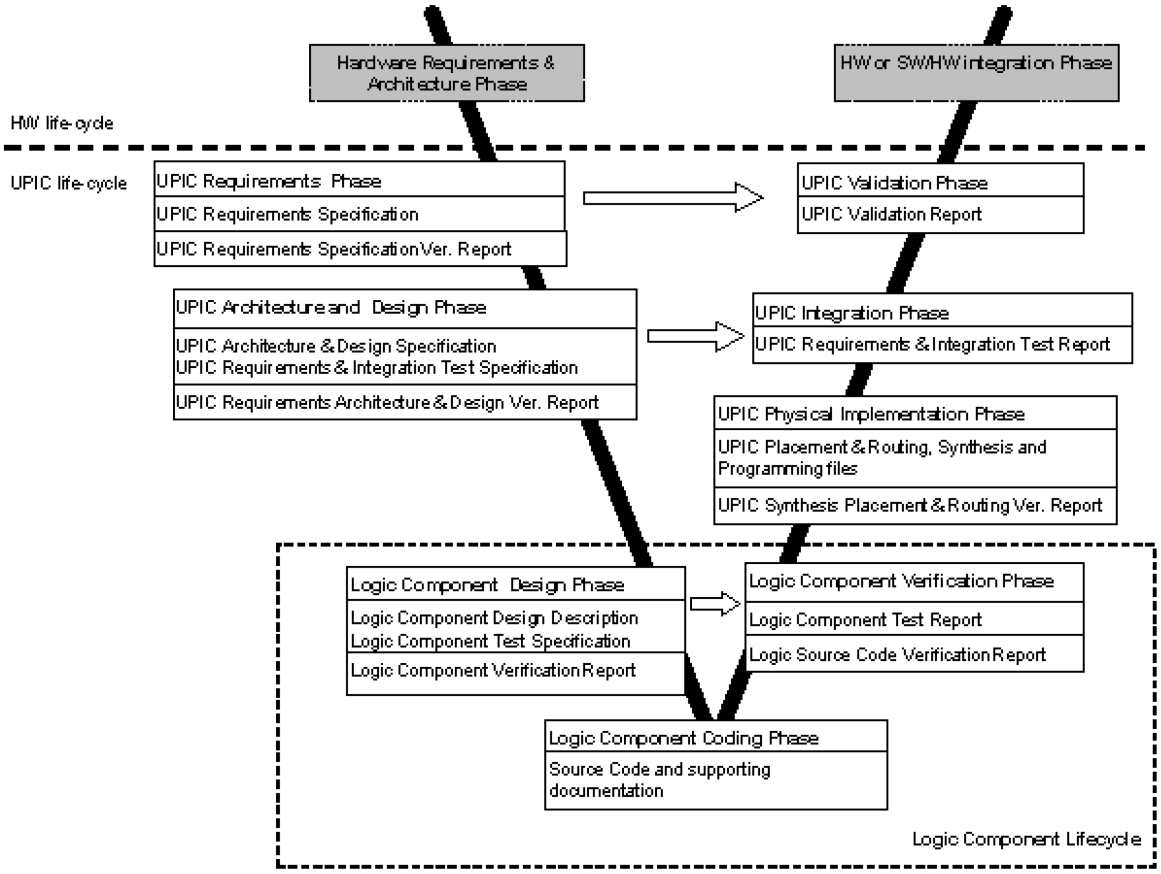


Figure F.3 — Example of UPIC development life cycle

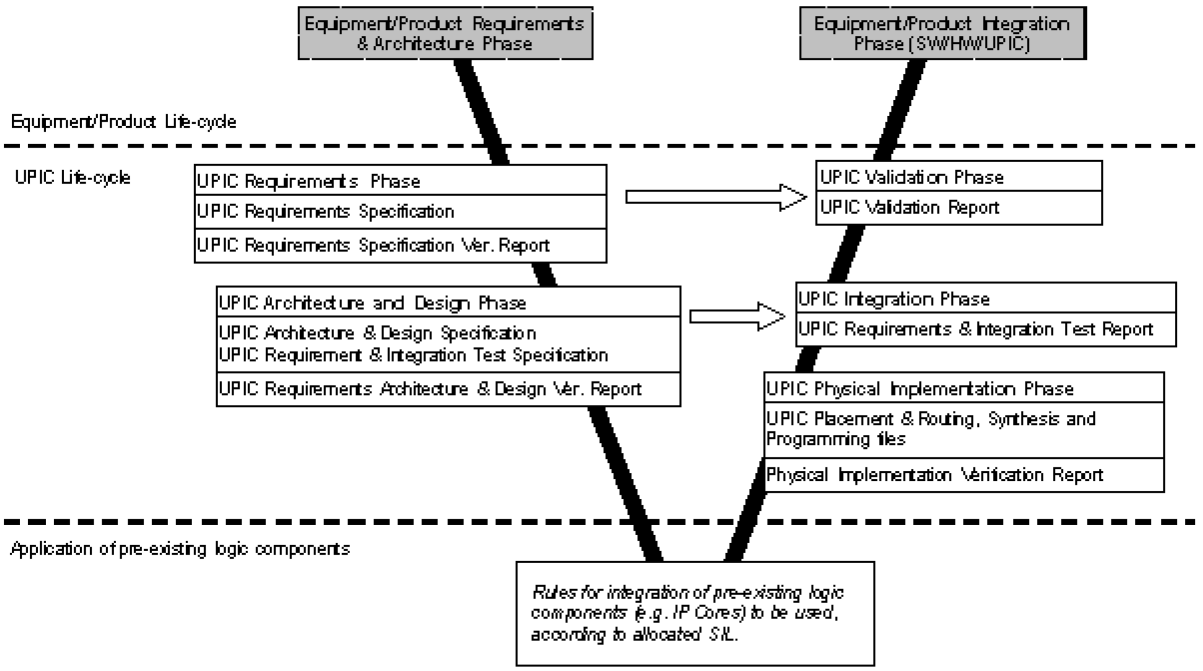


Figure F.4 — Example of UPIC development life cycle with pre-existing components

An example of the documentation set to be established is given in Table F.1.

With reference to Table F.1, the contents of different documents / reports of tasks carried out are typically merged or split according to the specific functional and reuse needs. In the table, the example of documentation is defined so as to provide evidence of execution of T&M necessary to achieve a high systematic failure integrity in complex cases. For simple UPICs it should be reduced for a simple UPIC (see also F.3.3.1).

Table F.1 — Example of documentation generated during each phase

Phase	**Document/task** (see Figures F.3 and F.4)
UPIC Requirements	UPIC Requirements Specification
	UPIC Requirements Specification Verification Report
UPIC Architecture and Design	UPIC Architecture and Design Specification
	UPIC Requirements and Integration Test Specification
	UPIC Requirements Architecture and Design Verification Report
Logic Component Design	Logic Component Design Specification
	Logic Component Test Specification
	Logic Component Verification Report
Logic Component Coding	Source code and supporting documentation
Logic Component Verification	Logic Component Test Report
	Logic Component Source Code Verification Report
UPIC Physical Implementation	UPIC Placement and Routing, Synthesis and Programming files
	UPIC Synthesis Placement and Routing Verification Report
UPIC Integration	UPIC Requirements and Integration Test Report
UPIC Validation	UPIC Validation Report

F.2.2 Organization, roles, responsibilities and personnel competencies

Organization, roles and responsibilities related to the development of UPIC are managed in compliance with the requirements defined in 5.3.4.2.

F.2.3 UPIC Requirements

The UPIC Requirements express the required functions, modes of operation, external interfaces and properties of the UPIC configuration being developed (including safety integrity level).

The description of external interfaces addresses:

— data structures and related transmission protocols;

— definition and description of boundary values for exchanged data;

— behaviour when the boundary value is exceeded;

— for time-critical input and output data:

  — time constraints and requirements for correct operation;

  — management of exceptions;

— interfaces timings and synchronisation.

The UPIC Requirements need to be complete, self-consistent, unambiguous, verifiable/testable, maintainable, feasible and traceable back to all the input documents.

Failure behaviour is documented or referenced (e.g. system level documentation).

Any constraints between the UPIC and the hardware/software are documented or referenced (e.g. system level documentation).

UPIC Requirements include self-tests necessary to ensure integrity of UPIC Hardware, as defined in the System Hazard Analysis.

Any non-safety functions which the UPIC is required to perform are part of the UPIC Requirements.

F.2.4 UPIC Architecture and Design

The UPIC Architecture Specification identifies all logic components (including IP Cores if reused).

The main algorithms and sequencing between components are defined within the UPIC Architecture including data paths, clocks and resets management (e.g. clock domains crossing, metastability mitigation).

For each logic component the architecture specification identifies:

— whether the component is new or existing;

— whether the components has been previously validated and if so its validation conditions;

— the safety integrity level of the functions performed by the component.

NOTE For simple functions unique-component architecture may be adopted provided that verification and validation activities can be executed to the extent required.

Logic components (to be defined and used as such):

— cover a defined subset of overall UPIC requirements;

— are clearly identified and independently versioned inside the configuration management system.

In case of use of pre-existing logic components (e.g. IP Cores), the architecture specification provides the evidence according to F.2.11. Use of these clauses substitutes the follow-up of phases listed in the following for Logic Components (i.e. Design, Coding and Testing).

Where the UPIC consists of logic components of different safety integrity levels then all of the components are treated as belonging to the highest of these levels unless there is evidence of independence between the higher safety integrity level components and the lower safety integrity level components. This evidence is typically recorded in the UPIC Architecture.

The UPIC Architecture Specification includes the definition of all Interfaces between logic components.

The description of internal interfaces addresses:

— data structures and related transmission protocols;

— definition and description of boundary values for exchanged data;

— behaviour when the boundary value is exceeded;

— for time-critical input and output data:

  — time constraints and requirements for correct operation;

  — management of exceptions;

— interfaces timings and synchronisation.

F.2.5 Logic Component Design

The Logic Component Design addresses:

a) identification of all lowest logic units (e.g. functions) traced back to the upper level;

b) detailed algorithms and data structures;

c) resolution of metastability and clock domain crossing.

F.2.6 Logic Component Coding

The UPIC implementation constraints instantiate the implementation requirements as defined in UPIC Architecture and Design Specification (timing, metastability, load, mapping, pin-out, segregation etc.).

F.2.7 Logic Component Verification

The UPIC Logic source code is verified for its readability, non-ambiguity and testability and a dedicated set of rules is defined and used.

F.2.8 UPIC Physical Implementation

The process of UPIC physical implementation (synthesis, placement, routing and layout) is generally performed by support tools provided by the UPIC vendor or another software manufacturer. UPIC implementation, following synthesis, is described using selected logic diagrams. These will then be put through an automated place-and-route procedure to generate a pinout, which will be used to interface with the external environment. During this phase related verification, as per selected Techniques/Measures, is then carried out.

F.2.9 UPIC Integration

The UPIC Requirements & Integration testing covers all the information provided within the UPIC Requirements and UPIC Architecture.

F.2.10 UPIC Validation

The UPIC Validation includes the confirmation that each combination of techniques or measures (selected according to F.3.3) is appropriate to the defined UPIC safety integrity level. It includes an evaluation of the overall effectiveness of the combination of techniques and measures adopted, taking account of the size and complexity of the UPIC produced and taking into account the actual results of verification and validation activities.

All constrains on use of the UPIC are recorded to allow integration of the UPIC within the target HW (e.g. information on usage, self-dynamic test, functional modes).

F.2.11 Requirements for use of pre-existing logic components

The use of pre-existing logic components (e.g. IP Cores or COTS soft cores) follows the requirements provided in 6.2.

F.3 Detailed technical requirements for UPIC

F.3.1 Guidance on safety architecture

The following provides guidance on how SIL is allocated in a product development based on UPICs and on which related safety architecture principles apply.

Definition of safety functional requirements and related SIL allocation for the UPIC is done at a higher level (e.g. within System/Subsystem/Equipment Hazard Analysis).

NOTE Safety requirements for UPIC typically include: design requirements to protect against common mode failures, and self-tests to be implemented with the maximum allowed execution period according to the safety target.

According to the SIL allocated to safety functional requirements:

— If SIL 3 or SIL 4 is allocated to the UPIC functions: requirements indicated in F.3.2 apply, to be implemented according to the process and related techniques chosen.

— If SIL 1 or SIL 2 is allocated to the UPIC functions: no generic fail-safety requirements apply (a subset of hazardous single faults can be accepted, if their occurrence is within quantitative safety target). Suitable requirements to achieve a defined quantitative safety target are defined within the product development and implemented according to the process and related techniques chosen.

— If the processed information is safety-related but protected by external elements (i.e. all failures of the UPIC are detectable by external monitoring measures), the UPIC itself can be considered as non-safety-related use of components implementing safety functions that are not controlled by an external function of applicable SIL is to be avoided.

F.3.2 Protection against random faults – architectural principles

Similarly to non-programmable HW components the implementation of SIL 3 and SIL 4 safety-related functions within a UPIC implies special care, using composite or reactive fail-safe techniques or data transmission coding strategy protection related techniques.

— **SIL 3 & 4 UPIC development**

Similarly to non-programmable HW components, it is necessary to ensure that SIL 3 and SIL 4 systems, whose functions are carried out by UPIC, remain safe in the event of any kind of single random hardware fault which is recognised as possible. This principle, which is known as fail-safety, can be achieved for UPICs in two different ways:

a) Composite fail-safety structure;

b) Reactive fail-safety structure;

NOTE As UPIC failure modes are not known, it is not deemed possible to demonstrate that each of them is non-hazardous (or justified as incredible). Thus the inherent fail-safe principle is not deemed applicable.

— **Composite fail-safety structure**

The same clauses relating to composite fail-safe architecture apply as for non-programmable HW (where each elaboration channel can be singularly implemented within a dedicated UPIC).

— **Reactive fail-safety structure**

The same clauses of reactive fail-safe architecture for non-programmable HW apply (where each part of the architecture, i.e. the processing of the safety function and the output checking/testing/detection, can be singularly implemented within a dedicated UPIC).

F.3.3 Protection against systematic faults – (techniques/measures)

F.3.3.1 Applicable Techniques and measures

The applied combination of techniques or measures is documented, with one or more techniques or measures being selected unless the notes attached to the table provide other requirements. These notes can include reference to approved techniques or approved combinations of techniques.

It is important to consider:

— the consistency of the chosen techniques and measures, and how well they complement each other;

— which techniques and measures are appropriate for every phase of the development life cycle;

— which techniques and measures are most appropriate for the specific problems encountered during the development of each different safety-related system.

Appropriate techniques/measures are selected according to the safety integrity level. Alternative or equivalent techniques/measures are indicated by a letter following the number. At least one of the alternative or equivalent techniques/measures is applied.

NOTE 1 Hard cores which may be embedded in FPGAs/CPLDs are treated in the same way as the corresponding components in Annex C (e.g. C.3 for identification of failure modes of integrated circuits).

NOTE 2 Where high level synthesis is used (i.e. to define functional behaviour in a SW language like C or C++ and translate to an HDL), related activities are addressed as SW coding, following the requirement of EN 50128. In this case the requirements for support tools will apply also to the synthesis part (similarly to that already defined for SW code compilation).

Decisions concerning the set of techniques and measures to be used only impact the development process applied to the UPIC configuration for control of systematic faults and do not influence the architectural features of the overall system embedding the UPIC for control of random faults.

Depending on UPIC complexity a complete or simplified set of techniques and measures for development is used, see Figure F.5.

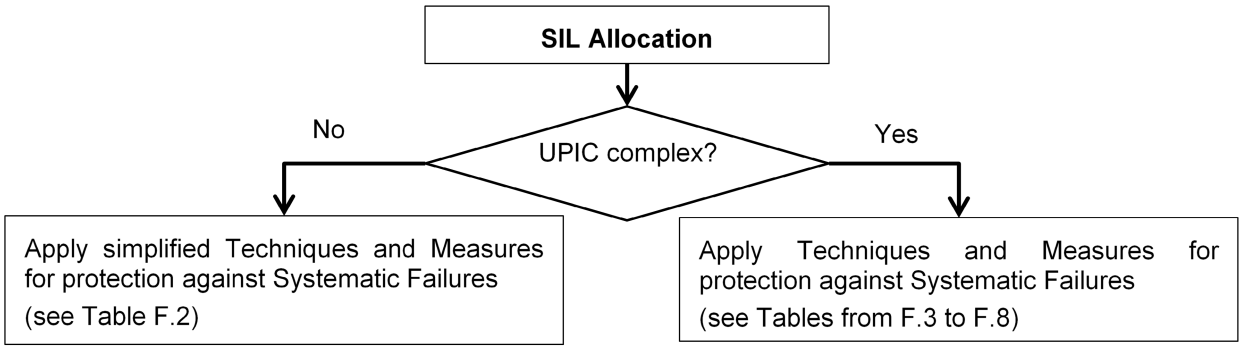


Figure F.5 — UPIC development techniques/measures

A UPIC is identified as simple only if a comprehensive combination of tests and analyses can ensure component validation. This is deemed sufficient as all internal states are therefore observable (i.e. the configured UPIC is equivalent to a simple non-programmable HW circuit).

In all other cases the UPIC is considered as complex.

NOTE 1 An example of a simple UPIC configuration (not complex) is a linear feedback shift register implemented within a CPLD/FPGA.

NOTE 2 Within typical modern safety applications the UPIC configuration used is complex.

F.3.3.2 Techniques and measures for simple UPIC

Techniques and measures for simple UPIC are given in Table F.2.

Table F.2 — Simplified techniques/measures for protection against systematic failures

Technique/Measure	SIL 1/2	SIL 3/4
Exhaustive functional and black-box tests	**HR**	**HR**
Identification and analysis of all failure modes of the UPIC	**R**	**HR**

F.3.3.3 Techniques and measures for complex UPIC

Techniques and measures for complex UPIC are given in Tables F.3, F.4 and F.5 and described in Tables F.6, F.7 and F.8.

Table F.3 — Design and Verification (including all activities before synthesis)

	Technique/Measure	SIL 1	SIL 2	SIL 3	SIL 4	Typical V-Cycle phase allocation
1	Structured description	**HR**	**HR**	**HR**	**HR**	Requirements, Architecture and Design
2	Design description in HDL	**HR**	**HR**	**HR**	**HR**	Component Coding
3	Schematic entry	**-**	**-**	**NR**	**NR**	Component Design
4	Application of a widely used design environment	**HR**	**HR**	**HR**	**HR**	Requirements, Architecture and Design
5	Functional test on component level (using for example HDL test benches)	**HR**	**HR**	**HR**	**HR**	Component Verification
6	Restricted use of asynchronous constructs	**HR**	**HR**	**HR**	**HR**	Component Design
7	Design for testability	**R**	**R**	**R**	**R**	Component Design
8	Modularisation	**R**	**R**	**HR**	**HR**	Component Design
9	Coverage of the verification scenarios (test benches)	**R**	**R**	**HR**	**HR**	Component Verification
10	Observation of coding guidelines	**HR**	**HR**	**HR**	**HR**	Component Coding
11	Documentation of simulation results	**HR**	**HR**	**HR**	**HR**	Component Verification
12a	Code inspection	**R**	**R**	**HR**	**HR**	Component Verification
12b	Walk-through	**R**	**R**	**HR**	**HR**	Component Verification

Table F.4 — Synthesis

	Technique/Measure	SIL 1	SIL 2	SIL 3	SIL 4	Typical V-Cycle phase allocation
13	Internal consistency checks	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
14	Check of IC vendor requirements and constraints	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
15	Documentation of synthesis constraints, results and tools	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
16	Application of widely used synthesis tools	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
17	Application of widely used libraries / UPIC technologies	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
18	Script based procedure	**R**	**R**	**HR**	**HR**	UPIC Physical implementation

Table F.5 — Placement, routing and layout generation

	Technique/Measure	SIL 1	SIL 2	SIL 3	SIL 4	Typical V-Cycle phase allocation
19	Static timing analysis of the critical paths (STA)	**HR**	**HR**	**HR**	**HR**	UPIC Integration
20a	*Verification of the gate netlist against a reference model by simulation*	**HR**	**HR**	**HR**	**HR**	UPIC Integration
20b	Comparison of the gate netlist with the reference model (formal equivalence check)	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
21	Design rule check	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation
22	Application of a widely used design environment	**HR**	**HR**	**HR**	**HR**	UPIC Physical implementation

Table F.6 — Description of techniques for design

	Technique/Measure	Description
1	Structured description	Description of the circuit functionality with HDL. An easily recognizable and modular structure is suggested. Each component is implemented likewise in the same fashion and is described in such a way that it is easily readable with clearly defined sub-functions. A strict distinction between implemented function and interconnection is suggested, i.e. the component, which is implemented by instancing other sub components, contains explicitly interconnections of the instanced components and does not contain any circuit logic.
2	Design description in HDL	Functional description at high abstraction level in hardware description language, for example VHDL or Verilog. The applied hardware description language allows functional and/or application oriented description and is abstracted from later implementation details. Data flows, branches, arithmetical and/or logical operations are implemented by assignment and operators of the hardware description language, without manual conversion in logical gates of the applied library.
3	Schematic entry	Description of the circuit functionality by schematic entry of the circuit plan. The functions to be realized are implemented by instancing (importing) the elementary logical circuit elements such as AND, OR, NOT along with macros consisting of complex arithmetical and logical functions, which are then interconnected. Complex circuits are partitioned considering the functional viewpoints and can be distributed on different drawings, which are hierarchically interconnected. The interconnection signals are uniquely defined and have explicit signal names over the entire hierarchy. The use of global signals (Labels) is avoided as far as applicable.
4	Application of a widely used design environment *(This technique is derived from 6.3 and adapted to technology specific aspects of UPICs).*	Most of the tools used for designing UPICs comprise sophisticated software, which cannot be assumed to operate without faults with respect to its correct functionality and it is also quite likely that faults might occur due to faulty operation. Therefore widely used tools are preferred for designing UPICs. This implies: – Application of tools which have been used (in a comparable software version) over a long period of time or by a large number of users in various projects with equivalent complexity. – Adequate experience of each UPIC designer with the operation of the tool over a long period of time. – Use of commonly used tools (adequate number of users) so that information regarding known failures with work around (version control with “Bug-List”) is available. This information is readily integrated in design flow and helps to avoid systematic failures. – The consistency check of the internal tool database and the plausibility check avoid faulty output data. Standard tools check the consistency of the internal database, for example the consistency of database between synthesis- and place-and-route-tool, in order to operate with unique data. The consistency check is an inherent attribute of the tool under use and the designer has limited influence on it. Therefore, if the possibility of manual consistency check is provided, the designer is expected to use it adequately.

	Technique/Measure	Description
5	Functional test on component level (using for example HDL test benches)	Verification of the implemented function — for example by simulation — at component level. The component under test will be instanced in a typical virtual test environment known as “test bench” and stimulated by the test pattern contained in the code. A sufficient high coverage of specified function including all special cases if they exist is at least required. Automatic verification of output sequence by the code of “test bench” is preferred to manual inspection of output signals.
6	Restricted use of asynchronous constructs	Asynchronous constructs such as SET and RESET signals derived over combinatorial logic are susceptible during synthesis and produce circuits with spikes or inverse timing sequence and therefore will have to be avoided. Also insufficient modelling may not be interpreted correctly by the synthesis tool, which causes ambiguous results during simulation. Additionally asynchronous constructs are poorly testable or not at all testable, so that the test coverage of production and online test is effectively reduced. The implementation of completely synchronous design with limited number of clock signals is therefore suggested. In systems with multiphase clocks, all the clocks are derived from one central clock. Clock input of sequential logic is always supplied exclusively by the clock signal, which does not contain any combinatorial logic. Asynchronous SET and RESET inputs of sequential cells are always supplied by synchronous signals that do not contain any combinatorial logic. Master SET and RESET are synchronised using at least two Flip-flops.
7	Design for testability	Design for testability is governed by the avoidance of – asynchronous constructs – latches and on-chip tri-state signals – wired-and / wired-or logic and redundant logic. The combinatorial depth of the sub circuits plays an important role during the testing. The test pattern required for a complete test increases exponentially with the combinatorial depth of the circuit. Therefore, circuits with high combinatorial depth are only poorly testable with adequate means.
8	Modularisation	Modularisation provides distinct partitioning of the total functionality in different components with limited functions so that transparency of components with precisely defined interface is established. Every subsystem, at all levels of the design, is clearly defined and is of restricted size (only a few functions). The interfaces between subsystems are kept as simple as possible and the cross-section (i.e. shared data, exchange of information) is minimized. The complexity of individual subsystems is also restricted.
9	Coverage of the verification scenarios (test benches)	The quality of the verification scenarios that is defined during the functional test, i.e. the applied test pattern (stimuli) to verify specified functions including all special cases, if they exist, is qualitatively and/or quantitatively documented. During a quantitative approach the achieved test coverage and the depth of the applied functional tests is documented. The resulting coverage meets the levels established for each of the coverage metrics. Any exception will be documented. In the case of a qualitative approach, the number of verified code lines, states or branches (“Code coverage”) of the circuit code to be verified is estimated.

	Technique/Measure	Description
10	Observation of coding guidelines	Syntactic coding rules help to create an easily readable code and allow a better documentation including version control. Typically, the rules for organizing and commenting the instruction blocks can be mentioned here. Semantic coding rules help avoid typical implementation problems by avoidance of constructs that lead to faulty synthesis with ambiguous implementation of the circuit function. Typical rules are for example the avoidance of asynchronous constructs or constructs that produce unpredictable timing sequence. In general the use of latches or coupling of data with clock signals lead to such ambiguities. Design guidelines are suggested to avoid systematic design failures during the UPIC development process. A coding style in certain aspect limits the design efficiency, but offers in return the advantage of failure avoidance during the UPIC development process. These are in particular: – avoidance of typical coding infirmity or failure; – restrictive usage of problematic constructs that produce ambiguous synthesis results; – design for testability; – transparent and easy to use code.
11	Documentation of simulation results	All the data needed for the functional simulation at component, chip or system level is well documented and archived with the following aims: – To repeat the simulation at any later phase in turn key fashion. – To demonstrate the correctness and completeness of all functions specified. The following database is archived for this purpose: – Simulation set-up including complete software of the applied tools, for example simulator, synthesizer with corresponding version and the necessary simulation library; – Testbench files, test stimuli, compilation and run scripts; – Log file of the simulation with full details regarding the time of simulation, applied tools with version and complete report of the work around if it was necessary; – All relevant simulation results inclusive signal flow, especially in case of manual inspection and documentation of acquired results.
12a	Code inspection	Review of circuit description is carried out by: – Checking the coding style; – Verification of the described functionality against the specification; – Checking for defensive coding, error and exception handling.
12b	Walk-through	A code walk-through consists of a walk-through team selecting a small set of test cases, representative sets of inputs and corresponding expected outputs for the program. The test data are then manually traced through the logic of the program. As a stand-alone measure, it is applied only to the circuits with very low complexity. If the HDL-Simulation cannot be carried out completely, the completeness of the walk-through and the quality of the achieved results are expected to have the equivalent quality that will be achieved by a HDL-simulation.

Table F.7 — Description of techniques for synthesis

	Technique/Measure	Description
13	Internal consistency checks	The consistency check is an inherent attribute of the tool under use and the designer has limited influence on it. Therefore, if the possibility of manual consistency check is provided, the designer should use it adequately.
14	Check of IC vendor requirements and constraints	A careful checking of the vendor requirements and constraints for example minimum and maximum fan-in and fan-out, maximum wire length (line delay), maximum slew rate of the signals, clock skew and so on by the synthesis tool enhances the reliability of the product. Besides the importance of the requirements for the production process, their violation has a great impact on the validity of the applied models that are used for the simulation. Thus any violation of the vendor requirements and constraints leads to faulty simulation results producing undesired functionality.
15	Documentation of synthesis constraints, results and tools	The documentation of all the synthesis constraints and results is indispensable for the following reasons: – to reproduce the synthesis at any later phase. – to generate an independent synthesis results for verification. Essential documents are: – Synthesis set-up including the applied tools and synthesis software with the actual version, the applied synthesis library and the defined constraints and scripts. – Synthesis log file with the time remark, applied tool with version and complete documentation of the synthesis. – The generated netlist with estimated time delays.
16	Application of widely used synthesis tools *(This technique is derived from 6.3 and adapted to technology specific aspects of UPICs).*	Tool based mapping of the HDL source code of circuit functionality by connection of the suitable gates and circuit primitives of the target UPIC library. The selected implementation out of a variety of possible implementations that fulfil the desired functionality depends on the most optimal result that is derived by the synthesis constraints such as timing (clock rate) and chip area. During synthesis phase any automatic optimisation done by tools themselves is avoided.
17	Application of widely used libraries / UPIC technologies	The synthesis and simulation target library for the development of a UPIC are derived from a common database and, therefore, are not independent. A systematic failure such as: – ambiguity between real and modelled behaviour of the circuit elements, – insufficient modelling for example of set-up and hold time, (one of the typical examples). Therefore widely used technologies and target libraries are used for the design of UPICs that perform safety functions. This means: – The application of target libraries that have been used over a significant long time in projects with comparable complexity and clock rating. – Availability of the technology and corresponding target library over a sufficient long period, so that enough modelling accuracy of the library can be expected.
18	Script based procedure	Automatic and script based control of the synthesis cycles including the definition of the applied constraints. Besides providing a precise documentation of a complete synthesis constraint, it helps to

Technique/Measure	Description
	reproduce the netlist after the alteration of the HDL source code under identical conditions.

Table F.8 — Description of techniques for placement, routing and layout generation

	Technique/Measure	Description
19	Static timing analysis of the critical paths (STA)	Static Timing Analysis (STA) analyses all the paths of a netlist (circuit) generated by the synthesis and/or placement, routing and layout tool considering the back-annotation, i.e. estimated line delays by the tool, as well as gate delays without performing the actual simulation. Therefore it allows in general a complete analysis of the timing constraint of the entire circuit, identifying the critical timings to be used to characterise the safe response time. The circuit to be tested is analysed under best- and worst-case conditions operating at maximum specified clock rate and accounting for applicable clock jitter and duty cycle skew. The number of non-relevant timing paths can be limited to a certain minimum by adopting a suitable design technique. It is suggested that the method used to report the results should be investigated, analysed and defined before beginning with the design. It can be assumed that STA covers explicitly all the existing timing paths if a) The timing constraints are properly specified. b) The circuit under test contains only such timing paths that can be analysed by STA tools, i.e. generally the case with full synchronous circuits. c) Gate and interconnection (wire) delay are considered.
20a	Verification of the gate netlist against a reference model by simulation	The applied stimuli for the verification of the circuit by simulation correspond exactly to the stimuli applied during the functional test on component or top level. The stimuli are derived to test the circuit in such a fashion that it will cover a high percentage of the timing constraints and include worst case timing paths. The functional verification is primarily performed by observing the outputs of the chip. This can be automated by comparing the output signals of the circuit with an adequate reference model or HDL source code of the circuit. This test is known as a "regression test" and is preferred to a manual check of the output signals. By applying this measure the functional behaviour of only those paths are verified which are actually stimulated during the simulation. The test coverage can, therefore, only be as good as during the original functional test at component-level or top-level. It is possible to complement this measure with a formal equivalence test. In all cases a functional verification of the HDL source code is carried out with the final netlist generated by the synthesis tool.
20b	Comparison of the gate netlist with the reference model (formal equivalence check)	Comparison of the circuit functionality described by the HDL source code with the circuit functionality of the gate netlist generated by synthesis. The tools based on the formal equivalence principle are capable of verifying the functional equivalence of a different representation form of the circuit, for example HDL description or netlist description. When applying this measure a functional simulation is not necessary, and an independent functional check is feasible. The successful application of this measure can only be guaranteed, if the applied tool is capable of proving complete equivalence and all the discrepancies reported are evaluated either by manual inspection or automatically.

	Technique/Measure	Description
21	Design rule check	Verification of the generated layout with respect to design rules.
22	Application of a widely used design environment	See Table F.6, entry 4.

Annex G
(informative)

Changes at this document compared to EN 50129:2003

This document supersedes EN 50129:2003. The changes have also taken into account the relationship to the standards EN 50126-1:2017 and EN 50126-2:2017.

Table G.1 — Clauses and subclauses — correspondence with EN 50129:2003

EN 50129:2018	EN 50129:2003	Type of Change
Foreword	**Foreword**	Updated
Introduction	**Introduction**	Updated
1	**1**	Updated
2	**2**	Updated
3	**3**	Updated
3.1	3.1	Updated, references to IEV added, alignment with EN 50126-1
3.2	3.2	Modification, new abbreviations
4	**4**	Updated
5	**5, B, Tables E**	See below
5.1	5.1 (part of)	Improved content from two subclauses
5.2	5.2	Life cycle following EN 50126-1
5.3.1	5.3.1	Small modifications
5.3.2	Table E.1	New subclause on documentation
5.3.3	5.3.2	Small modifications
5.3.4	5.3.3, Table E.3	Updated, Basic Integrity
5.3.5	5.3.4, 5.3.8, Table E.1	Updated
5.3.6	5.3.5	Updated
5.3.7	5.3.6, Table E.2	Updated
5.3.8	5.3.7	Focus on safety
5.3.9	B.5.3	Content from normative Annex
5.3.10	5.3.9, Tables E.1, E.8	Improvement on verification
5.3.11	5.3.9, Tables E.1, E.8	Improvement on validation
5.3.12	B.6	Content from normative Annex
5.3.13	−/−	New subclause on SRAC
5.3.14	5.3.10	Updated
5.3.15	−/−	New subclause on ISA
6	**−/−**	New clause on "Requirements for elements

EN 50129:2018

EN 50129:2018	EN 50129:2003	Type of Change
		following different life cycles" addressing: — Use of pre-existing items — Safety-related tools for electronic systems — Physical security and IT-Security
7	**5.1, 5.4, 5.5, B**	New clause on "The Safety Case: structure and content"
7.1	5.1 (the most of)	Updated
7.2	5.4, B.1	Updated
7.2 Section 1	5.4	Updated
7.2 Section 2	5.4, B.2	Updated
7.2 Section 3	5.4, Table E.4	Updated
7.2 Section 4	5.4, B.4, Table E.7	Updated
7.2 Section 5	5.4, B.5 (except B.5.3)	Updated
7.2 Section 6	5.4, B.6 (part of)	Updated
7.3	5.5.1	Updated
7.4	5.5.1	Updated, new text on SASC
7.5	5.5.4	Updated
8	**5 (part of)**	New clause on "System safety acceptance and subsequent phases"
8.1	5.5.2	Updated
8.2	5.3.12, 5.5.3	Updated, content merged
8.3	5.3.12, 5.5.3	Updated, content merged
8.4	5.3.13	Updated
A	**A**	Updated
A.1	A.1	Updated
A.2	A.2	Updated
A.3	A.3	Updated
A.4	A.4	Updated
A.5	A.5	Updated, Basic Integrity
B	**B, D**	Updated, merging Annexes B and D
B.1	B.1	Update
B.2.1	A.4.2.2.1, B.3.3 (parts of)	Updated
B.2.2	A.4.2.2.1	Updated
B.3.1	B.3.1, Table E.5	Updated
B.3.2.1	B.3.2	Updated
B.3.2.2	B.3.2, D.2	Updated, content merged

EN 50129:2018	EN 50129:2003	Type of Change
B.3.2.3	B.3.2, D.3	Updated, content merged
B.3.2.4	−/−	New content
B.3.3.1	B.3.3, Table E.5	Updated
B.3.3.2	D.4	Updated
B.3.3.3	D.4	Updated
B.3.4	B.3.4, Table E.5	Updated
B.3.5.1	B.3.5	Updated
B.3.5.2	D.5	Updated
B.3.6	B.3.6	Updated
C	**C**	Updated
C.1	C.1	Updated
C.2	C.2	Updated
C.3	C.3	Updated
C.4	C.4	Updated
C.5	C.5, C.6	Updated
−/−	C.7	Text directly included in Tables C.1 to C.15, for better readability
D	**−/−**	New text
−/−	**D**	Merged with Annex B
E	**E**	Updated as normative, improved structure Tables updated, Content aligned with main part, Tables modified and restructured
F	**−/−**	New text
Bibliography	Bibliography	Updated

Table G.2 — Figures and tables — correspondence with EN 50129:2003

EN 50129:2018	EN 50129:2003	Type of Change
Figures		
Figure 1	Figure 1	Updated
Figure 2	Figure 2	Updated
Figure 3	Figure 4	Updated
Figure 4	Figure 5	Unchanged
Figure 5	Figure 6	Updated
Figure 6	Figure 3	Unchanged
Figure 7	Figure 7	Unchanged
Figure 8	–/–	New
Figure 9	Figure 8	Updated
Figure A.1	Figure A.1	Updated
Figure A.2	Figure A.2	Updated
–/–	Figure A.3	Removed
Figure A.3	Figure A.4	Updated
Figure A.4	Figure A.5	Updated
Figure A.5	Figure A.7	Unchanged
Figure A.6	Figure A.8	Updated
Figure B.1	Figure A.6	Updated
Figure B.2	Figure D.1	Updated
Figure B.3	Figure B.1	Updated
Figure B.4	Figure B.2	Split in two Figures
Figure B.5	Figure B.2	Split in two Figures
Figure C.1	Without name	Unchanged
Tables		
Table 1	–/–	New content
Table A.1	Table A.1	Updated
Table B.1	Table D.1	Updated
Tables C.1 to C.15	Tables C.1 to C.15	Updated
–/–	Table C.16	Text included in subclause C.5
Tables E.1 to E.9	Tables E.1 to E.9	Updated
–/–	Table E.10	Content moved to 5.3.4.1, 5.3.8
Tables F.1 to F.8	–/–	New

Annex ZZ
(informative)

Relationship between this European standard and the essential requirements of EU Directive 2008/57/EC [2008 OJ L191] aimed to be covered

This European Standard has been prepared under a Commission's standardization request relating to harmonized standards in the field of the Interoperability of the rail system within the European Union, M/483, to provide one voluntary means of conforming to essential requirements of Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the harmonization of the laws of the Member States relating to the interoperability of the rail system within the Community [2008 OJ L191].

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZZ.1 for "Control-Command and Signalling", confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

Table ZZ.1 — Correspondence between this European Standard, the CCS TSI (COMMISSION REGULATION (EU) 2016/919 of 27 May 2016) and Directive 2008/57/EC

Essential Requirements of Directive 2008/57/EC	Chapter / § / points of CCS TSI	Clause(s) / sub-clause(s) of this EN	Remarks / Notes
1. General Requirements 1.1 Safety 1.1.1 1.1.3 2. Requirements specific to each sub-subsystem 2.3. Control Command and signalling 2.3.1 Safety	3.2. Specific Aspects of the Control-Command and Signalling Subsystems 3.2.1. Safety 4.2. Functional and technical specifications of the Subsystems 4.2.1. Control-Command and Signalling safety characteristics relevant to interoperability 4.2.1.1. Safety 6.2. Interoperability constituents 6.2.1. Assessment procedures for Control-Command and Signalling Interoperability Constituents 6.2.3. Assessment requirements 6.3. Control-Command and Signalling Subsystems	5. Requirements for developing safety-related electronic systems 6. Requirements for elements following different life cycles 7. The Safety Case: structure and content 8. System safety acceptance and subsequent phases Annex A Safety Integrity Levels Annex B Management of faults for safety-related functions Annex C Identification of hardware component failure modes Annex E Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults	The standard EN 50129:2003 is referenced in the CCS TSI (Clause 6.2.3)

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

The documents listed in this bibliography were consulted during the preparation of this document. Note that the documents listed in bibliography could have been updated.

EN 50121 (series), *Railway applications – Electromagnetic compatibility*

EN 50124-2, *Railway applications – Insulation coordination – Part 2: Overvoltages and related protection*

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

EN 31010, *Risk management – Risk assessment techniques*

EN 50159, *Railway applications – Communication, signalling and processing systems — Safety-related communication in transmission systems*

EN 61025, *Fault tree analysis (FTA)*

EN 61078, *Analysis techniques for dependability — Reliability block diagram and Boolean methods*

EN 61165, *Application of Markov techniques*

EN 60812, *Failure Mode and Effects analysis (FMEA and FMECA)*

EN 61508 (all parts), *Functional safety of electrical/electronic/ programmable electronic safety-related systems (IEC 61508 series)*

EN 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2010)*

EN 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures (IEC 61508-7:2010, modified)*

EN 61882, *Hazard and operability studies (HAZOP studies) — Application guide*

EN 62502, *Analysis techniques for dependability — Event tree analysis (ETA)*

IEC 60664 (series), *Insulation coordination for equipment within low-voltage systems*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

IEC 61709, *Electric components — Reliability — Reference conditions for failure rates and stress models for conversion*

IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

IEC 61025:2006, *Fault tree analysis (FTA)*

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

EN ISO 9001, *Quality management systems — Requirements (ISO 9001)*

R009-004, Railway applications – Systematic allocation of safety integrity requirements (CENELEC Report) Substituted by CLC/TR 50451:2007

CLC/TR 50451:2007, *Railway applications — Systematic allocation of safety integrity requirements*

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-338B, Military handbook: Electronic reliability design handbook, October 1998

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

Reliability Information Analysis Center Report FMD 2013

Failure mode/mechanism distributions, 2013

Waarom betaalt u voor een norm?
Normen zijn afspraken voor en door de markt, zo ook deze norm. NEN begeleidt het gehele normalisatieproces. Van het bijeenbrengen van partijen, het maken en vastleggen van de afspraken en het bieden van hulp bij de toepassing van de normen. Om deze diensten te kunnen bekostigen betalen alle belanghebbende partijen die aan tafel zitten voor het normalisatieproces, en u als gebruiker voor normen en trainingen. NEN is een stichting en heeft geen winstoogmerk.

Wat is nu precies de toegevoegde waarde van normen?
Stelt u zich eens voor … u wilt in het buitenland geld pinnen, maar uw bankpas past niet. Of uw nieuwe telefoon herkent uw simkaart niet. De samenstelling van de benzine over de grens is anders waardoor u niet kunt tanken. Het dagelijks leven zou zonder goede afspraken over producten, processen en diensten een stuk complexer zijn.

Het maken en vastleggen van afspraken door belanghebbende partijen noemen we het normalisatieproces. Normalisatie had vanouds betrekking op techniek en producten. Nu worden steeds vaker normen voor diensten ontwikkeld. Zo zijn er afspraken op het gebied van gezondheidszorg, schuldhulpverlening, kennisintensieve dienstverlening, externe veiligheid en MVO.

Normen zorgen voor verbetering van producten, diensten en processen; qua veiligheid, gezondheid, efficiëntie, kwaliteit en duurzaamheid. Dit ziet u op de werkvloer, in de omgang met elkaar en in de samenleving als geheel. Organisaties die normalisatie onderdeel van hun strategie maken, vergroten hun professionaliteit, betrouwbaarheid en concurrentiekracht.

Wat doet NEN?
NEN ondersteunt in Nederland het normalisatieproces. Als een partij zich tot NEN richt met de vraag om een afspraak tot stand te brengen, gaan wij aan de slag. We onderzoeken in hoeverre normalisatie mogelijk is en er interesse voor bestaat. Wij nodigen vervolgens alle belanghebbende partijen uit om deel te nemen. Een breed draagvlak is een randvoorwaarde. De afspraken komen op basis van consensus tot stand en worden vastgelegd in een document. Dit is meestal een norm. Afspraken die in een NEN-norm zijn vastgelegd mogen niet conflicteren met andere geldige NEN-normen. NEN-normen vormen samen een coherent geheel. Een belanghebbende partij kan een producent, ondernemer, dienstverlener, gebruiker, maar ook de overheid of een consumenten- of onderzoeksorganisatie zijn. De vraag is niet altijd om een norm te ontwikkelen. Vanuit de overheid komt regelmatig het verzoek om te onderzoeken of er binnen een bepaalde sector of op een bepaald terrein normalisatie mogelijk is. NEN doet dan onderzoek en start afhankelijk van de uitkomsten een project. Deelname staat open voor alle belanghebbende partijen. NEN beheert ruim 30.000 normen. Dit zijn de in Nederland aanvaarde internationale (ISO, IEC), Europese (EN) en nationale normen (NEN). In totaal zijn er ruim 800 normcommissies actief met in totaal bijna 5.000 normcommissieleden. Een goed beheer van de omvangrijke normencollectie en de afstemming tussen nationale, Europese en internationale normcommissies vereisen dan ook een zeer goede infrastructuur.

Betalen kleine organisaties net zoveel als grote organisaties?
Het uitgangspunt is dat alle partijen die deelnemen aan het normalisatieproces een evenredig deel betalen. De normcommissieleden kunnen onderling andere afspraken maken. Zo worden er wel eens afspraken gemaakt dat de grote partijen een groter deel betalen dan de kleinere bedrijven. De prijzen voor normen zijn voor iedereen gelijk. De kosten voor licenties zijn afhankelijk van de omvang van een organisatie en het aantal gebruikers.

Voordelen van normalisatie en normen
Gegarandeerde kwaliteit | Veiligheid geborgd | Bevordert duurzaamheid | Opschalen en vermarkten van nieuwe innovatieve producten | Meer (internationale) handelsmogelijkheden | Verhoogde effectiviteit en efficiëntie | Onderscheidend in de markt.

Voordelen van deelname
Invloed op de (internationale en Europese) afspraken | Als eerste op de hoogte van veranderingen | Netwerk; ook op Europees en internationaal niveau | Kennisvergroting.