



BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of EN 50129:2018, incorporating corrigendum April 2019. It supersedes PD CLC/TR 50451:2007, PD CLC/TR 50506-1:2007, PD CLC/TR 50506-2:2009 and BS EN 50129:2003, which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 539 04568 0

ICS 93.100

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2018.

Amendments/corrigenda issued since publication

Date	Text affected
31 May 2019	Implementation of CENELEC corrigendum April 2019: Section 4.4 of subclause 7.2 corrected

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

Contents	Page
European foreword	5
Introduction	7
1 Scope	8
2 Normative references	9
3 Terms, definitions and abbreviations	10
3.1 Terms and definitions	10
3.2 Abbreviations	20
4 Overall framework of this standard	21
5 Requirements for developing safety-related electronic systems	22
5.1 Introduction	22
5.2 The quality management process	23
5.3 The safety management process	26
6 Requirements for elements following different life cycles	36
6.1 Introduction	36
6.2 Use of pre-existing items	36
6.3 Safety-related tools for electronic systems	39
6.4 Physical security and IT-Security	41
7 The Safety Case: structure and content	42
7.1 The Safety Case structure	42
7.2 The Technical Safety Report	44
7.3 Generic and Specific Safety Cases	55
7.4 Provisions for the Specific Application Safety Case	55
7.5 Dependencies between Safety Cases	56
8 System safety acceptance and subsequent phases	57
8.1 System safety acceptance process	57
8.2 Operation, maintenance and performance monitoring	61
8.3 Modification and retrofit	61
8.4 Decommissioning and disposal	61
Annex A (normative) Safety Integrity Levels	62
A.1 Introduction	62
A.2 Safety requirements	62
A.3 Safety integrity	63
A.4 Determination of safety integrity requirements	64
A.4.1 General	64
A.4.2 Risk Assessment	65
A.4.3 Hazard Control	67

A.4.4	Identification and treatment of new hazards arising from design	72
A.5	Allocation of SILs	73
A.5.1	General aspects	73
A.5.2	Relationship between SIL and associated TFFR	74
Annex B	(normative) Management of faults for safety-related functions	77
B.1	Introduction	77
B.2	General concepts	78
B.2.1	Detection and negation times	78
B.2.2	Composition of two independent items.....	79
B.3	Effects of faults	80
B.3.1	Effects of single faults	80
B.3.2	Influences between items	81
B.3.3	Detection of single faults	87
B.3.4	Action following detection (retention of safe state)	90
B.3.5	Effects of multiple faults	92
B.3.6	Defence against systematic faults	95
Annex C	(normative) Identification of hardware component failure modes	96
C.1	Introduction	96
C.2	General procedure	96
C.3	Procedure for integrated circuits.....	96
C.4	Procedure for components with inherent physical properties.....	97
C.5	General provisions concerning component failure modes	97
Annex D	(informative) Example of THR/TFFR/FR apportionment and SIL allocation	117
Annex E	(normative) Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults	119
E.1	Introduction	119
E.2	Tables of techniques and measures	121
Annex F	(informative) Guidance on User Programmable Integrated Circuits.....	130
F.1	Introduction	130
F.1.1	Purpose	130
F.1.2	Terminology and context	131
F.2	UPIC life cycle.....	132
F.2.1	Organization, roles, responsibilities and personnel competencies.....	134
F.2.2	UPIC Requirements.....	134
F.2.3	UPIC Architecture and Design.....	135
F.2.4	Logic Component Design	136
F.2.5	Logic Component Coding	136
F.2.6	Logic Component Verification.....	136

F.2.7	UPIC Physical Implementation	136
F.2.8	UPIC Integration	136
F.2.9	UPIC Validation	136
F.2.10	Requirements for use of pre-existing logic components	136
F.3	Detailed technical requirements for UPIC.....	136
F.3.1	Guidance on safety architecture	136
F.3.2	Protection against random faults – architectural principles	137
F.3.3	Protection against systematic faults – (techniques/measures)	137
Annex G	(informative) Changes at this document compared to EN 50129:2003.....	147
Annex ZZ	(informative) Relationship between this document and the Essential Requirements of EU Directive 2008/57/EC.....	151
Bibliography		153

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.

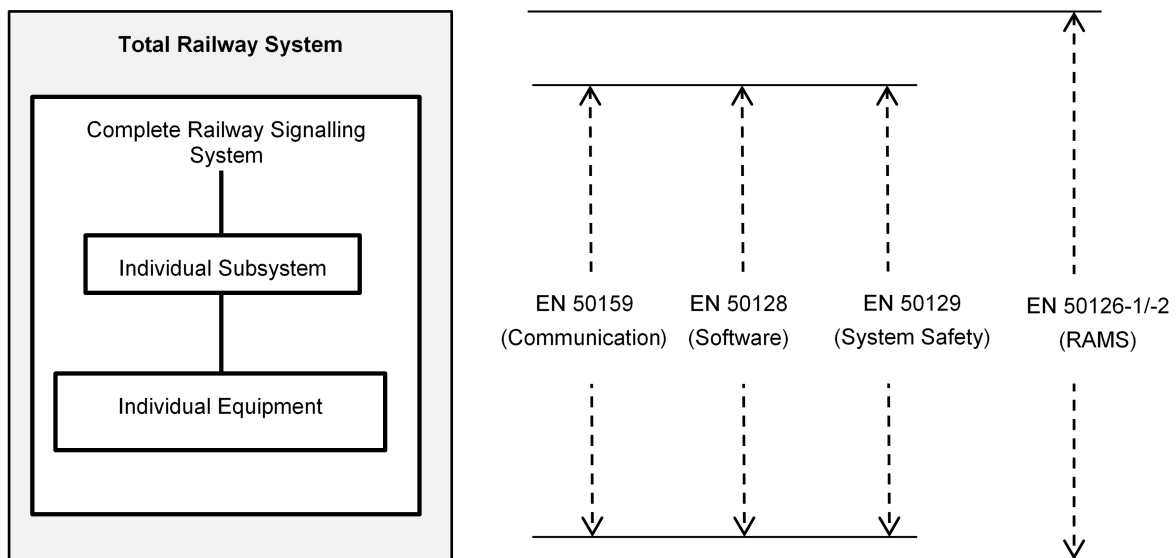


Figure 1 — Scope of the main CENELEC railway application standards

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 $(t, t + \Delta t)$ 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 IEC 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.

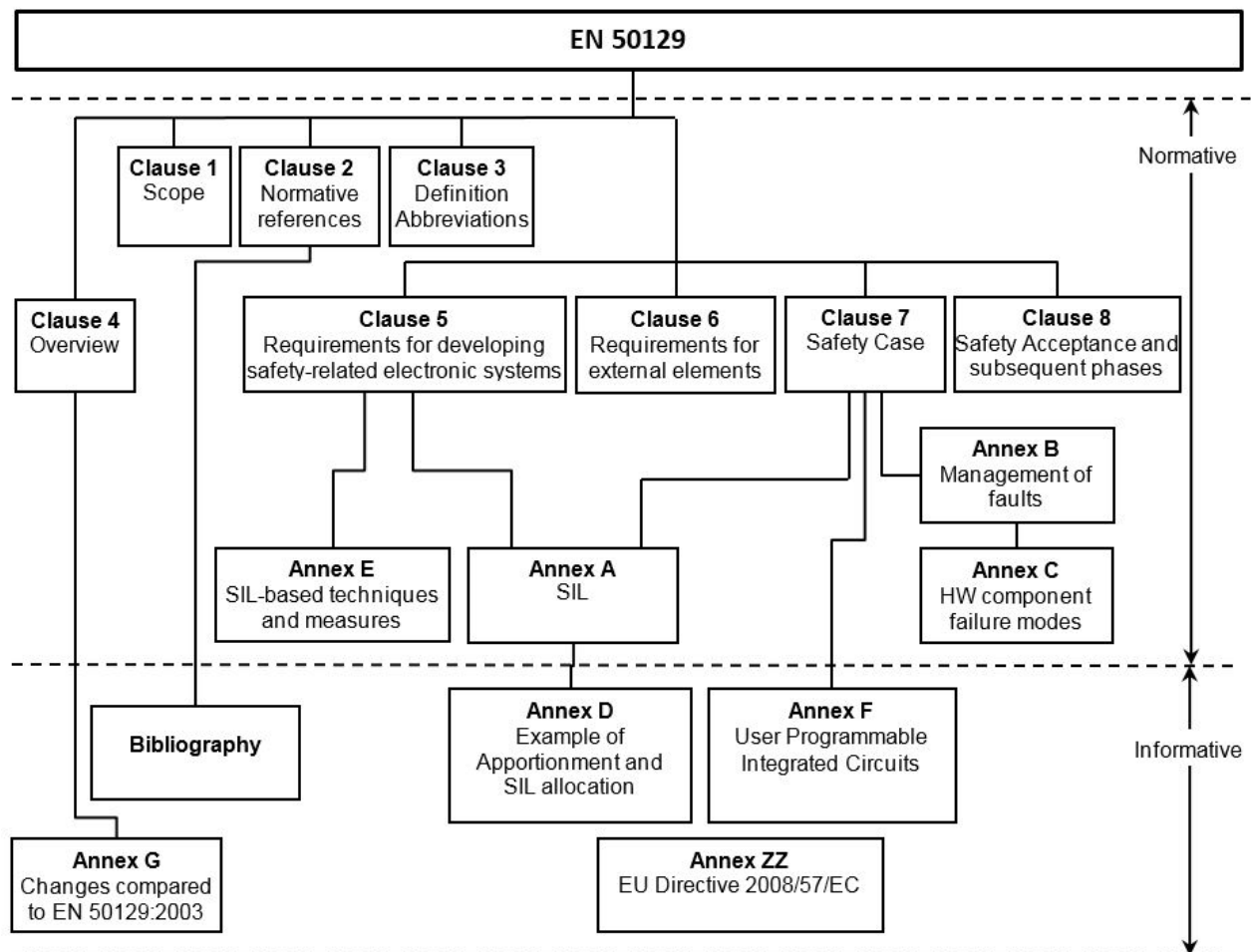


Figure 2 — Structure of EN 50129

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.

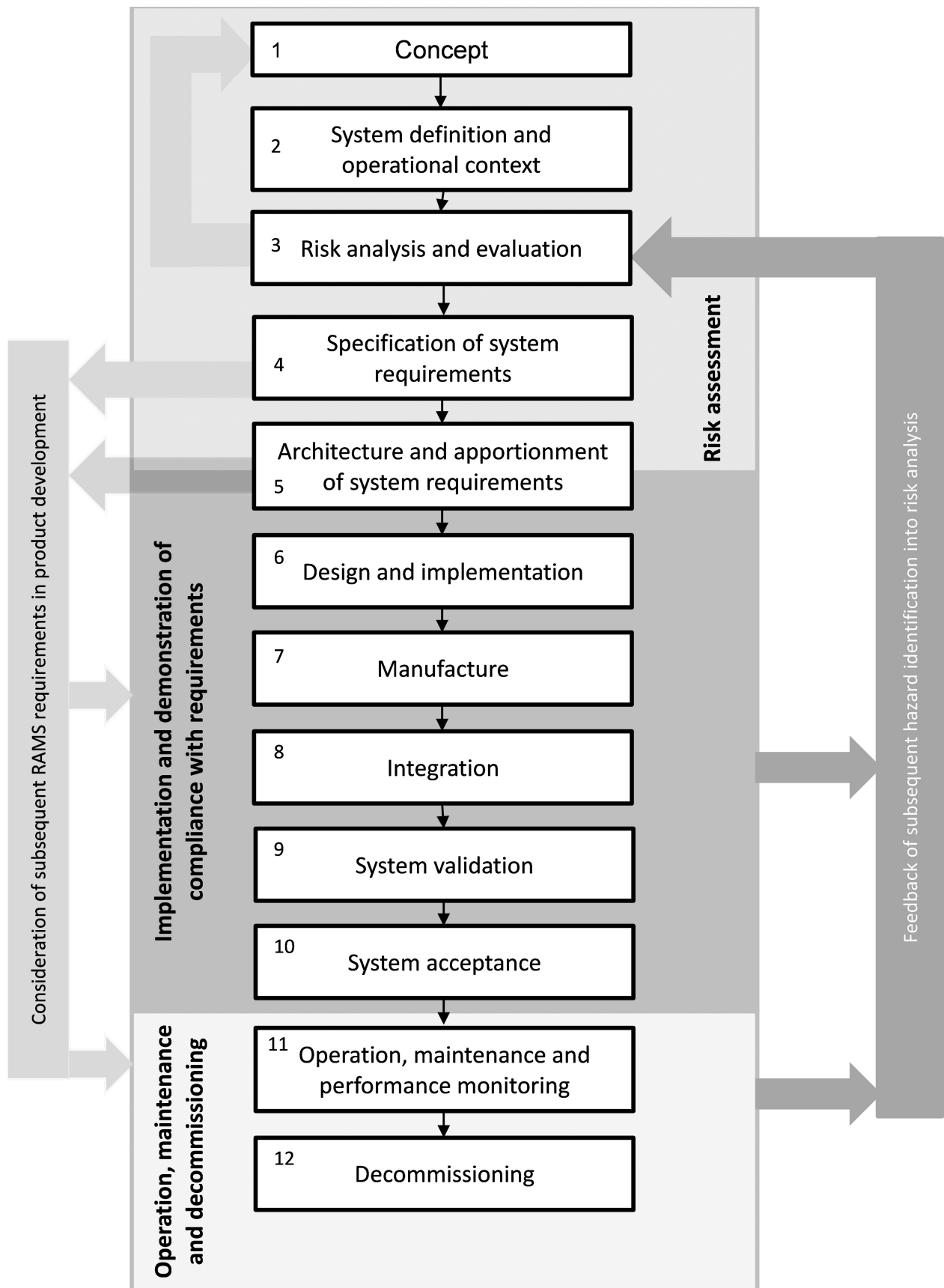


Figure 3 — Example of system life cycle (from EN 50126-1:2017)

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.

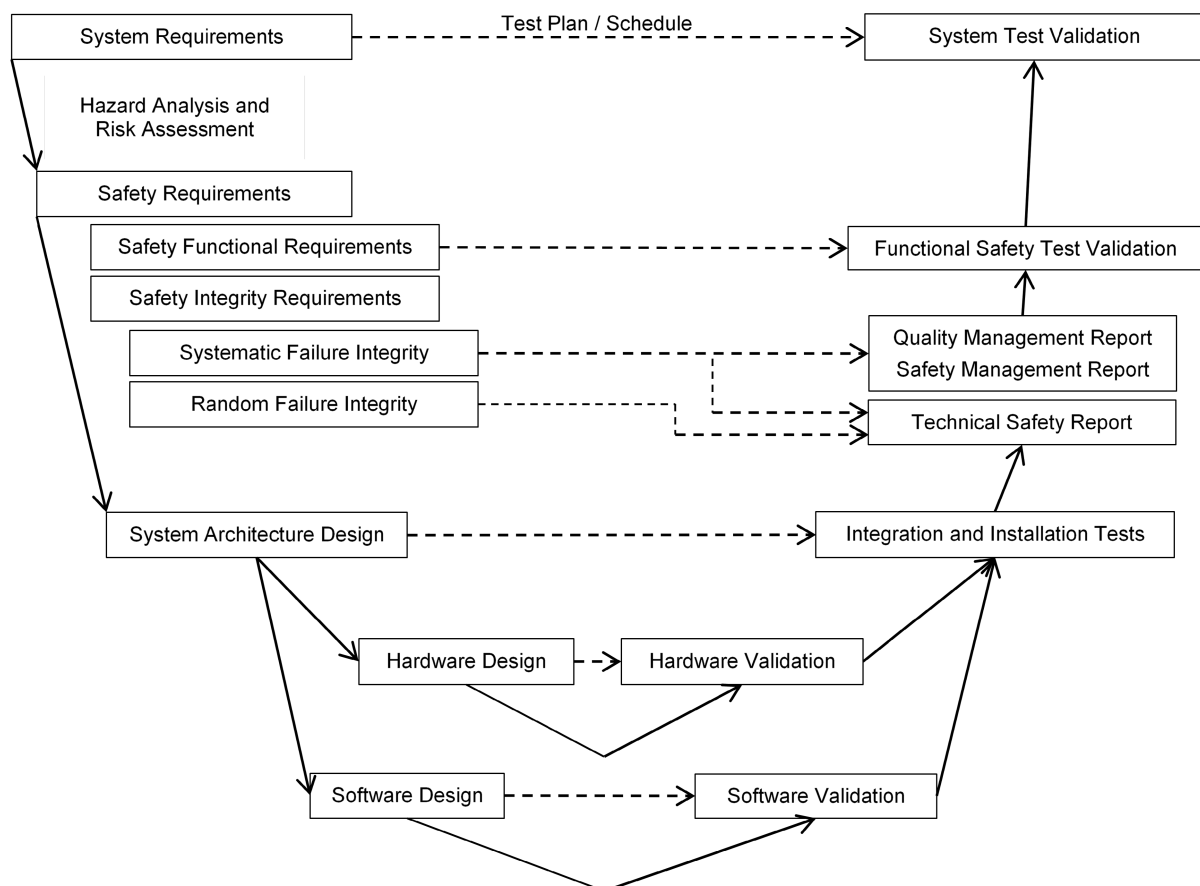


Figure 4 — Example of design and validation portion of system life cycle

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.

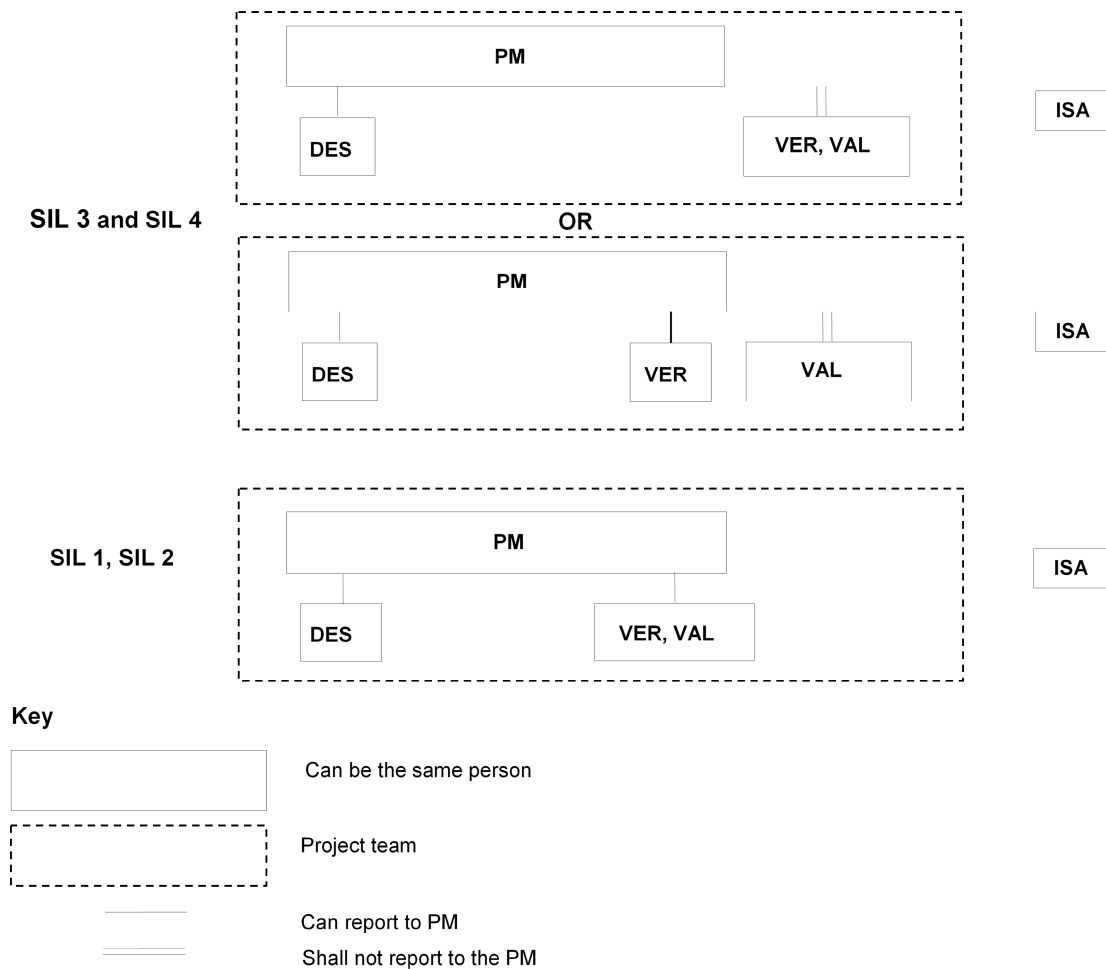


Figure 5 — Independence of Roles for different SILs

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.

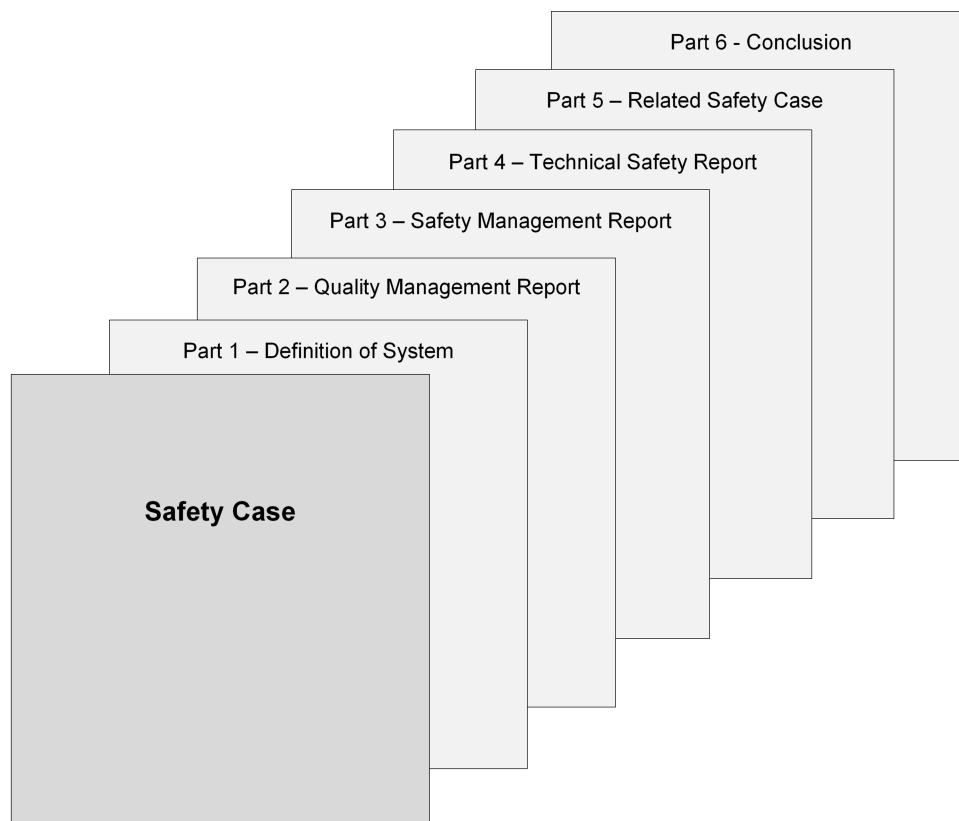


Figure 6 — Structure of Safety Case

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.

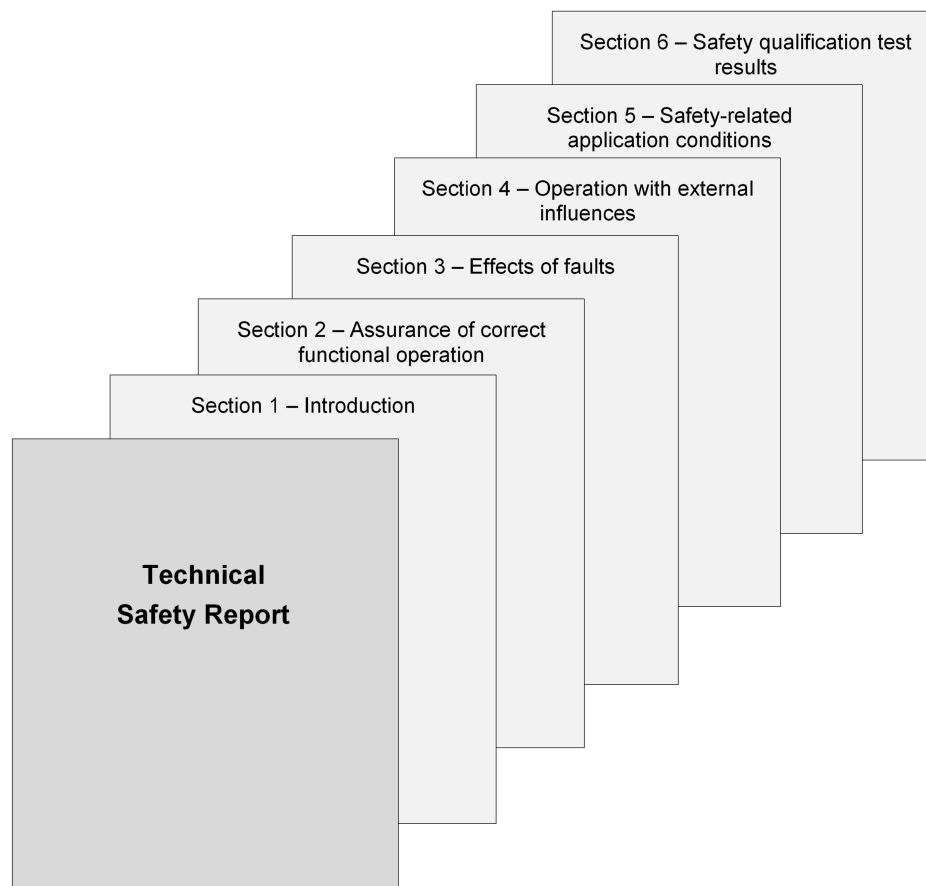


Figure 7 — Structure of Technical Safety Report

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;