

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

ICS 93.100

# National foreword

This British Standard is the UK implementation of EN 50129:2003, incorporating corrigendum May 2010. It supersedes DD ENV 50129:1999 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/9, Railway electrotechnical applications, to Subcommittee GEL/9/1, Signalling and communications.

A list of organizations represented on this subcommittee 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.

**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 7 May 2003

© BSI 2010

ISBN 978 0 580 71753 6

## Amendments/corrigenda issued since publication

| Date         | Comments                                                              |
|--------------|-----------------------------------------------------------------------|
| 31 July 2010 | Implementation of CENELEC corrigendum May 2010. Insertion of Annex ZZ |
|              |                                                                       |
|              |                                                                       |

EUROPEAN STANDARD

**EN 50129**

NORME EUROPÉENNE

EUROPÄISCHE NORM

February 2003

ICS 93.100

Supersedes ENV 50129:1998  
Incorporating corrigendum May 2010

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 2002-12-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.

**CENELEC**

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

**Central Secretariat: rue de Stassart 35, B - 1050 Brussels**

© 2003 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

## **Foreword**

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50129 on 2002-12-01.

This European Standard supersedes ENV 50129:1998.

This European Standard was prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and supports the essential requirements of Directive 96/48/EC.

The following dates were fixed:

- latest date by which the EN has to be implemented  
at national level by publication of an identical  
national standard or by endorsement (dop) 2003-12-01
- latest date by which the national standards conflicting  
with the EN have to be withdrawn (dow) 2005-12-01

Annexes designated "normative" are part of the body of the standard.

Annexes designated "informative" are given for information only.

In this standard, Annexes A, B and C are normative and Annexes D and E are informative.

---

## Contents

|                                                                                             | Page      |
|---------------------------------------------------------------------------------------------|-----------|
| <b>Introduction</b> .....                                                                   | <b>6</b>  |
| <b>1 Scope</b> .....                                                                        | <b>7</b>  |
| <b>2 Normative references</b> .....                                                         | <b>8</b>  |
| <b>3 Definitions and abbreviations</b> .....                                                | <b>9</b>  |
| 3.1 Definitions .....                                                                       | 9         |
| 3.2 Abbreviations .....                                                                     | 13        |
| <b>4 Overall framework of this standard</b> .....                                           | <b>14</b> |
| <b>5 Conditions for safety acceptance and approval</b> .....                                | <b>15</b> |
| 5.1 The Safety Case .....                                                                   | 15        |
| 5.2 Evidence of quality management .....                                                    | 17        |
| 5.3 Evidence of safety management .....                                                     | 20        |
| 5.4 Evidence of functional and technical safety.....                                        | 24        |
| 5.5 Safety acceptance and approval .....                                                    | 26        |
| <b>Annex A (normative) Safety Integrity Levels</b> .....                                    | <b>30</b> |
| A.1 Introduction.....                                                                       | 30        |
| A.2 Safety requirements .....                                                               | 30        |
| A.3 Safety integrity .....                                                                  | 31        |
| A.4 Allocation of safety integrity requirements.....                                        | 31        |
| A.5 Safety Integrity Levels .....                                                           | 39        |
| <b>Annex B (normative) Detailed technical requirements</b> .....                            | <b>42</b> |
| B.1 Introduction.....                                                                       | 42        |
| B.2 Assurance of correct functional operation .....                                         | 42        |
| B.3 Effects of faults .....                                                                 | 44        |
| B.4 Operation with external influences .....                                                | 50        |
| B.5 Safety-related application conditions.....                                              | 51        |
| B.6 Safety Qualification Tests.....                                                         | 53        |
| <b>Annex C (normative) Identification of hardware component failure modes</b> .....         | <b>55</b> |
| C.1 Introduction.....                                                                       | 55        |
| C.2 General procedure .....                                                                 | 55        |
| C.3 Procedure for integrated circuits (including microprocessors) .....                     | 55        |
| C.4 Procedure for components with inherent physical properties.....                         | 55        |
| C.5 General notes concerning component failure modes.....                                   | 56        |
| C.6 Additional general notes, concerning components with inherent physical properties ..... | 56        |
| C.7 Specific notes concerning components with inherent physical properties .....            | 57        |

|                                                                                                                                                                                                  |           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Annex D (informative) Supplementary technical information</b>                                                                                                                                 | <b>77</b> |
| D.1 Introduction                                                                                                                                                                                 | 77        |
| D.2 Achievement of physical internal independence                                                                                                                                                | 77        |
| D.3 Achievement of physical external independence                                                                                                                                                | 78        |
| D.4 Example of a method for single-fault analysis                                                                                                                                                | 79        |
| D.5 Example of a method for multiple-fault analysis                                                                                                                                              | 80        |
| <b>Annex E (informative) Techniques and measures for safety-related electronic systems for signalling for the avoidance of systematic faults and the control of random and systematic faults</b> | <b>85</b> |
| <b>Annex ZZ (informative) Coverage of Essential Requirements of EC Directives</b>                                                                                                                | <b>94</b> |
| <b>Bibliography</b>                                                                                                                                                                              | <b>95</b> |
| Figure 1 – Scope of the main CENELEC railway application standards                                                                                                                               | 8         |
| Figure 2 – Structure of EN 50129                                                                                                                                                                 | 15        |
| Figure 3 – Structure of Safety Case                                                                                                                                                              | 17        |
| Figure 4 – Example of system life-cycle                                                                                                                                                          | 19        |
| Figure 5 – Example of design and validation portion of system life-cycle                                                                                                                         | 21        |
| Figure 6 – Arrangements for independence                                                                                                                                                         | 22        |
| Figure 7 – Structure of Technical Safety Report                                                                                                                                                  | 26        |
| Figure 8 – Safety acceptance and approval process                                                                                                                                                | 28        |
| Figure 9 – Examples of dependencies between Safety Cases/Safety Approval                                                                                                                         | 29        |
| Figure A.1 – Safety requirements and safety integrity                                                                                                                                            | 30        |
| Figure A.2 – Global process overview                                                                                                                                                             | 32        |
| Figure A.3 – Example risk analysis process                                                                                                                                                       | 33        |
| Figure A.4 – Definition of hazards with respect to the system boundary                                                                                                                           | 34        |
| Figure A.5 – Example hazard control process                                                                                                                                                      | 36        |
| Figure A.6 – Interpretation of failure and repair times                                                                                                                                          | 37        |
| Figure A.7 – Treatment of functional independence by FTA                                                                                                                                         | 38        |
| Figure A.8 – Relationship between SILs and techniques                                                                                                                                            | 40        |
| Figure B.1 – Influences affecting the independence of items                                                                                                                                      | 46        |
| Figure B.2 – Detection and negation of single faults                                                                                                                                             | 49        |
| Figure D.1 – Example of a fault analysis method                                                                                                                                                  | 81        |
| Table A.1 – SIL-table                                                                                                                                                                            | 41        |
| Table C.1 – Resistors                                                                                                                                                                            | 61        |
| Table C.2 – Capacitors                                                                                                                                                                           | 62        |
| Table C.3 – Electromagnetic components                                                                                                                                                           | 63        |
| Table C.4 – Diodes                                                                                                                                                                               | 66        |
| Table C.5 – Transistors                                                                                                                                                                          | 67        |
| Table C.6 – Controlled rectifiers                                                                                                                                                                | 69        |
| Table C.7 – Surge Suppressors                                                                                                                                                                    | 71        |
| Table C.8 – Opto-electronic components                                                                                                                                                           | 72        |
| Table C.9 – Filters                                                                                                                                                                              | 73        |
| Table C.10 – Interconnection assemblies                                                                                                                                                          | 74        |

|                                                                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Table C.11 – Fuses .....                                                                                                                                                           | 75 |
| Table C.12 – Switches and push/pull buttons.....                                                                                                                                   | 75 |
| Table C.13 – Lamps .....                                                                                                                                                           | 75 |
| Table C.14 – Batteries .....                                                                                                                                                       | 75 |
| Table C.15–Transducers/sensors (not including those with internal electronic circuitry) .....                                                                                      | 76 |
| Table C.16 – Integrated circuits.....                                                                                                                                              | 76 |
| Table D.1 - Examples of measures to detect faults in large-scale integrated circuits by means of periodic on-line testing, with comparison (SW or HW), in a 2-out-of-n system..... | 82 |
| Table E.1 – Safety planning and quality assurance activities .....                                                                                                                 | 86 |
| Table E.2 – System requirements specification .....                                                                                                                                | 87 |
| Table E.3 – Safety organisation.....                                                                                                                                               | 87 |
| Table E.4 – Architecture of system/sub-system/equipment .....                                                                                                                      | 88 |
| Table E.5 – Design features .....                                                                                                                                                  | 89 |
| Table E.6 – Failure and hazard analysis methods.....                                                                                                                               | 90 |
| Table E.7 – Design and development of system/sub-system/equipment.....                                                                                                             | 91 |
| Table E.8 – Design phase documentation.....                                                                                                                                        | 91 |
| Table E.9 – Verification and validation of the system and product design .....                                                                                                     | 92 |
| Table E.10 – Application, operation and maintenance .....                                                                                                                          | 93 |

## **Introduction**

This document is the first European Standard defining requirements for the acceptance and approval of safety-related electronic systems in the railway signalling field. Until now only some differing national recommendations and general advice of the UIC (International Union of Railways) on this topic were in existence.

Safety-related electronic systems for signalling include hardware and software aspects. To install complete safety-related systems, both parts within the whole life-cycle of the system have to be taken into account. The requirements for safety-related hardware and for the overall system are defined in this standard. Other requirements are defined in associated CENELEC standards.

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

Cross-acceptance is aimed at generic approval, not specific applications. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will in future refer to this standard when it becomes an EN.

The standard consists of the main part (Clause 1 to Clause 5) and Annexes A, B, C, D and E. The requirements defined in the main part of the standard and in Annexes A, B and C are normative, whilst Annexes D and E are informative.

This standard is in line with, and uses relevant sections of EN 50126: "Railway applications: The Specification and Demonstration of Dependability - Reliability, Availability, Maintainability and Safety (RAMS)". This standard and EN 50126 are based on the system life-cycle and are in line with EN 61508-1, which is replaced by the set of EN 50126/EN 50128/EN 50129, as far as Railway Communication, Signalling and Processing Systems are involved. Meeting the requirements in these standards is sufficient to ensure that further compliance to EN 61508-1 need not be evaluated.

Because this standard is concerned with the evidence to be presented for the acceptance of safety-related systems, it specifies those life-cycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. Safety justification for the whole of the life-cycle is therefore required.

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

For safety-related systems which include programmable electronics, additional conditions for the software are defined in EN 50128.

Additional requirements for safety-related data communication are defined in EN 50159-1 and EN 50159-2.

## **1 Scope**

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

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

This standard is intended to apply to all safety-related railway signalling systems/sub-system/equipment. However, the hazard analysis and risk assessment processes defined in EN 50126 and this standard are necessary for all railway signalling systems/sub-systems/equipment, in order to identify any safety requirements. If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety-related), and provided the conclusion is not revised as a consequence of later changes, this safety standard ceases to be applicable.

This standard applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete signalling systems, and also to individual sub-systems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

This standard applies to generic sub-systems and equipment (both application-independent and those intended for a particular class of application), and also to systems/sub-systems/equipment for specific applications.

This standard is not applicable to existing systems/sub-systems/equipment (i.e. those which had already been accepted prior to the creation of this standard). However, as far as reasonably practicable, this standard should be applied to modifications and extensions to existing systems, sub-systems and equipment.

This standard is primarily applicable to systems/sub-systems/equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (e.g.: power supplies, modems, etc.), which is procured for use as part of a safety-related signalling system. As a minimum, evidence shall be provided in such cases to demonstrate

either that the equipment is not relied on for safety,

or that the equipment can be relied on for those functions which relate to safety.

This standard is applicable to the functional safety of railway signalling systems. It is not intended to deal with the occupational health and safety of personnel; this subject is covered by other standards.

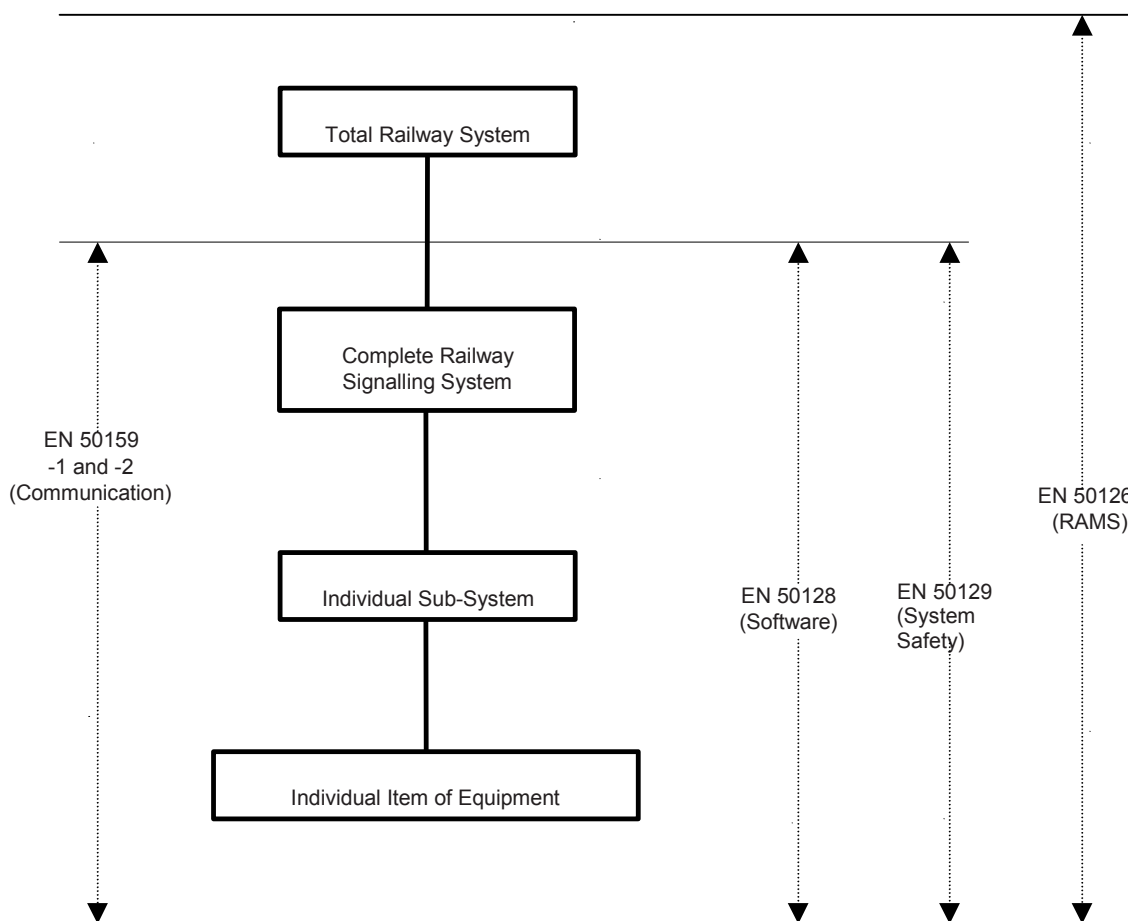


Figure 1 – Scope of the main CENELEC railway application standards

## 2 Normative references

This European Standard incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

NOTE Additional informative references are included in Bibliography.

|                 |                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EN 50121 Series | Railway applications – Electromagnetic compatibility                                                                                                        |
| EN 50124-1      | Railway applications – Insulation coordination – Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment |
| EN 50124-2      | Railway applications – Insulation coordination – Part 2: Overvoltages and related protection                                                                |
| EN 50125-1      | Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock                                                    |
| EN 50125-3      | Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and communications                                         |
| EN 50126        | Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)                                  |

|                  |                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| EN 50128         | Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems                  |
| EN 50155         | Railway applications – Electronic equipment used on rolling stock                                                                              |
| EN 50159-1       | Railway applications – Communication, signalling and processing systems<br>Part 1: Safety-related communication in closed transmission systems |
| EN 50159-2       | Railway applications – Communication, signalling and processing systems<br>Part 2: Safety related communication in open transmission systems   |
| EN 61508-1       | Functional safety of electrical/electronic/ programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1)        |
| IEC 60664 Series | Insulation coordination for equipment within low-voltage systems                                                                               |

### 3 Definitions and abbreviations

#### 3.1 Definitions

For the purposes of this standard, the following definitions apply:

##### 3.1.1

##### **accident**

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

##### 3.1.2

##### **assessment**

the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose

##### 3.1.3

##### **authorisation**

the formal permission to use a product within specified application constraints

##### 3.1.4

##### **availability**

the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided

##### 3.1.5

##### **can**

is possible

##### 3.1.6

##### **causal analysis**

analysis of the reasons how and why a particular hazard may come into existence

##### 3.1.7

##### **common-cause failure**

failure common to items which are intended to be independent

##### 3.1.8

##### **consequence analysis**

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

##### 3.1.9

##### **configuration**

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

##### 3.1.10

##### **cross-acceptance**

the status achieved by a product that has been accepted by one authority to the relevant European Standards and is acceptable to other authorities without the necessity for further assessment

**3.1.11**

**design**

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

**3.1.12**

**design authority**

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

**3.1.13**

**diversity**

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

**3.1.14**

**equipment**

a functional physical item

**3.1.15**

**error**

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

**3.1.16**

**fail-safe**

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

**3.1.17**

**failure**

a deviation from the specified performance of a system. A failure is the consequence of a fault or error in the system

**3.1.18**

**fault**

an abnormal condition that could lead to an error in a system. A fault can be random or systematic

**3.1.19**

**fault detection time**

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

**3.1.20**

**function**

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

**3.1.21**

**hazard**

a condition that could lead to an accident

**3.1.22**

**hazard analysis**

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

**3.1.23**

**hazard log**

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

**3.1.24**

**human error**

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

**3.1.25**

**implementation**

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

**3.1.26**

**independence (functional)**

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

**3.1.27**

**independence (human)**

freedom from involvement in the same intellectual, commercial and/or management entity

**3.1.28**

**independence (physical)**

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

**3.1.29**

**individual risk**

a risk which is related to a single individual only

**3.1.30**

**maintainability**

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

**3.1.31**

**maintenance**

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

**3.1.32**

**may**

is permissible

**3.1.33**

**negation**

enforcement of a safe state following detection of a hazardous fault

**3.1.34**

**negation time**

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

**3.1.35**

**product**

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

**3.1.36**

**quality**

a user perception of the attributes of a product

**3.1.37**

**railway authority**

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

**3.1.38**

**random failure integrity**

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

**3.1.39**

**random fault**

unpredictable occurrence of a fault

**3.1.40**

**redundancy**

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

**3.1.41**

**reliability**

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

**3.1.42**

**repair**

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

**3.1.43**

**risk**

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

**3.1.44**

**safe state**

a condition which continues to preserve safety

**3.1.45**

**safety**

freedom from unacceptable levels of risk of harm

**3.1.46**

**safety acceptance**

the safety status given to a product by the final user

**3.1.47**

**safety approval**

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

**3.1.48**

**safety authority**

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

**3.1.49**

**safety case**

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

**3.1.50**

**safety integrity**

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

**3.1.51**

**Safety Integrity Level**

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

**3.1.52**

**safety life-cycle**

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

**3.1.53**

**safety management**

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

**3.1.54**

**safety plan**

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

**3.1.55**

**safety process**

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

### 3.1.56

#### **safety-related**

carries responsibility for safety

### 3.1.57

#### **shall**

is mandatory

### 3.1.58

#### **should**

is recommended

### 3.1.59

#### **signalling system**

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

### 3.1.60

#### **stress profile**

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

### 3.1.61

#### **sub-system**

a portion of a system which fulfils a specialised function

### 3.1.62

#### **system**

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

### 3.1.63

#### **systematic failure integrity**

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

### 3.1.64

#### **systematic fault**

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

### 3.1.65

#### **system life-cycle**

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

### 3.1.66

#### **technical safety report**

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

### 3.1.67

#### **validation**

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

### 3.1.68

#### **verification**

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

## 3.2 Abbreviations

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

|       |                |                                                         |
|-------|----------------|---------------------------------------------------------|
| 3.2.1 | <b>AC</b>      | alternating current                                     |
| 3.2.2 | <b>ATP</b>     | Automatic Train Protection                              |
| 3.2.3 | <b>CENELEC</b> | European Committee for Electrotechnical Standardisation |

|        |      |                                                       |
|--------|------|-------------------------------------------------------|
| 3.2.4  | CCF  | common-cause failure                                  |
| 3.2.5  | DC   | direct current                                        |
| 3.2.6  | EMC  | electromagnetic compatibility                         |
| 3.2.7  | EMI  | electromagnetic interference                          |
| 3.2.8  | EN   | European Standard (Europäische Norm)                  |
| 3.2.9  | ESD  | electrostatic discharge                               |
| 3.2.10 | FET  | field effect transistor                               |
| 3.2.11 | FMEA | Failure Modes and Effects Analysis                    |
| 3.2.12 | FR   | Failure rate                                          |
| 3.2.12 | FTA  | Fault Tree Analysis                                   |
| 3.2.14 | H    | Hazard                                                |
| 3.2.15 | HW   | Hardware                                              |
| 3.2.16 | IEC  | International Electrotechnical Commission             |
| 3.2.17 | IRSE | Institution of Railway Signal Engineers               |
| 3.2.18 | ISO  | International Standards Organisation                  |
| 3.2.19 | RAMS | reliability, availability, maintainability and safety |
| 3.2.20 | SCR  | silicon controlled rectifier                          |
| 3.2.21 | SDR  | Safe down rate                                        |
| 3.2.22 | SDT  | Safe down time                                        |
| 3.2.23 | SIL  | Safety Integrity Level                                |
| 3.2.24 | SW   | software                                              |
| 3.2.25 | THR  | tolerable hazard rate                                 |
| 3.2.26 | UIC  | International Union of Railways                       |
| 3.2.27 | VDR  | voltage-dependent resistor                            |

## 4 Overall framework of this standard

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

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

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

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

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

**Annex D** (informative) contains supplementary technical information.

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

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

The structure of this standard is summarised in Figure 2.

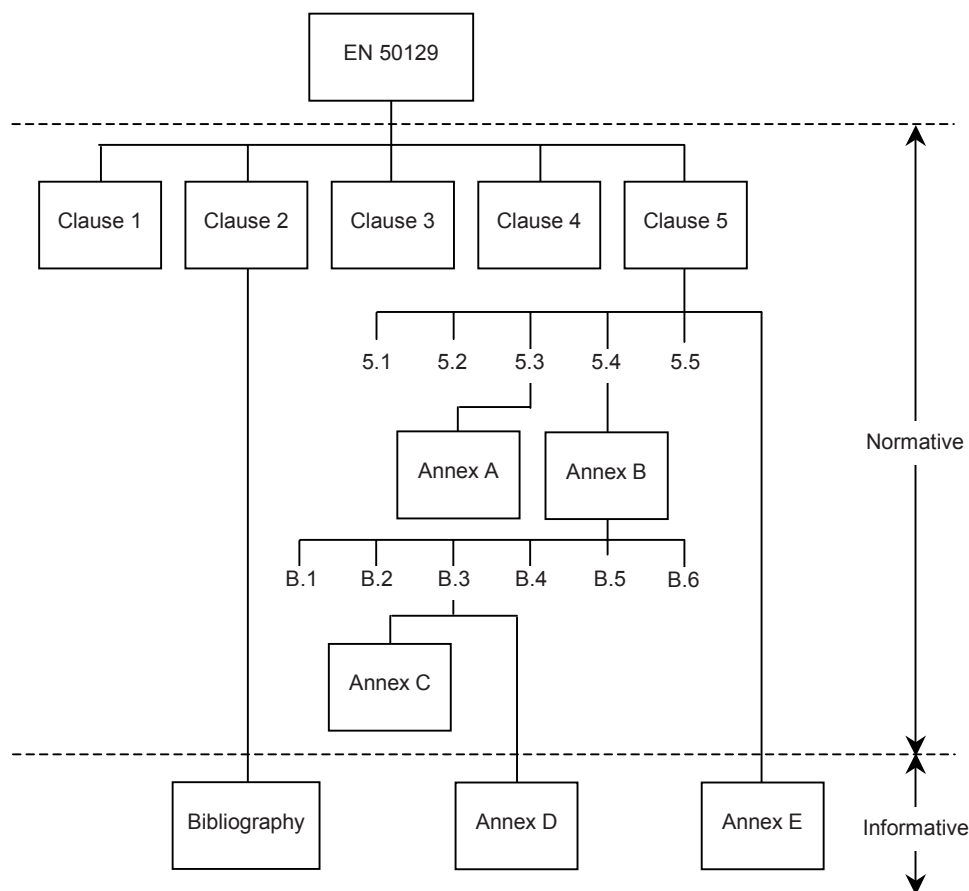


Figure 2 – Structure of EN 50129

## 5 Conditions for safety acceptance and approval

### 5.1 The Safety Case

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

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

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

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

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

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

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

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

**Part 2 Quality Management Report**

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

**Part 3 Safety Management Report**

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

**Part 4 Technical Safety Report**

This shall contain the evidence of functional and technical Safety, as specified in 5.4 of this standard.

**Part 5 Related Safety Cases**

This shall contain references to the Safety Cases of any sub-systems or equipment on which the main Safety Case depends.

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

either fulfilled in the main Safety Case,

or carried forward into the safety-related application conditions of the main Safety Case.

**Part 6 Conclusion**

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

The structure of the Safety Case is illustrated in Figure 3.

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

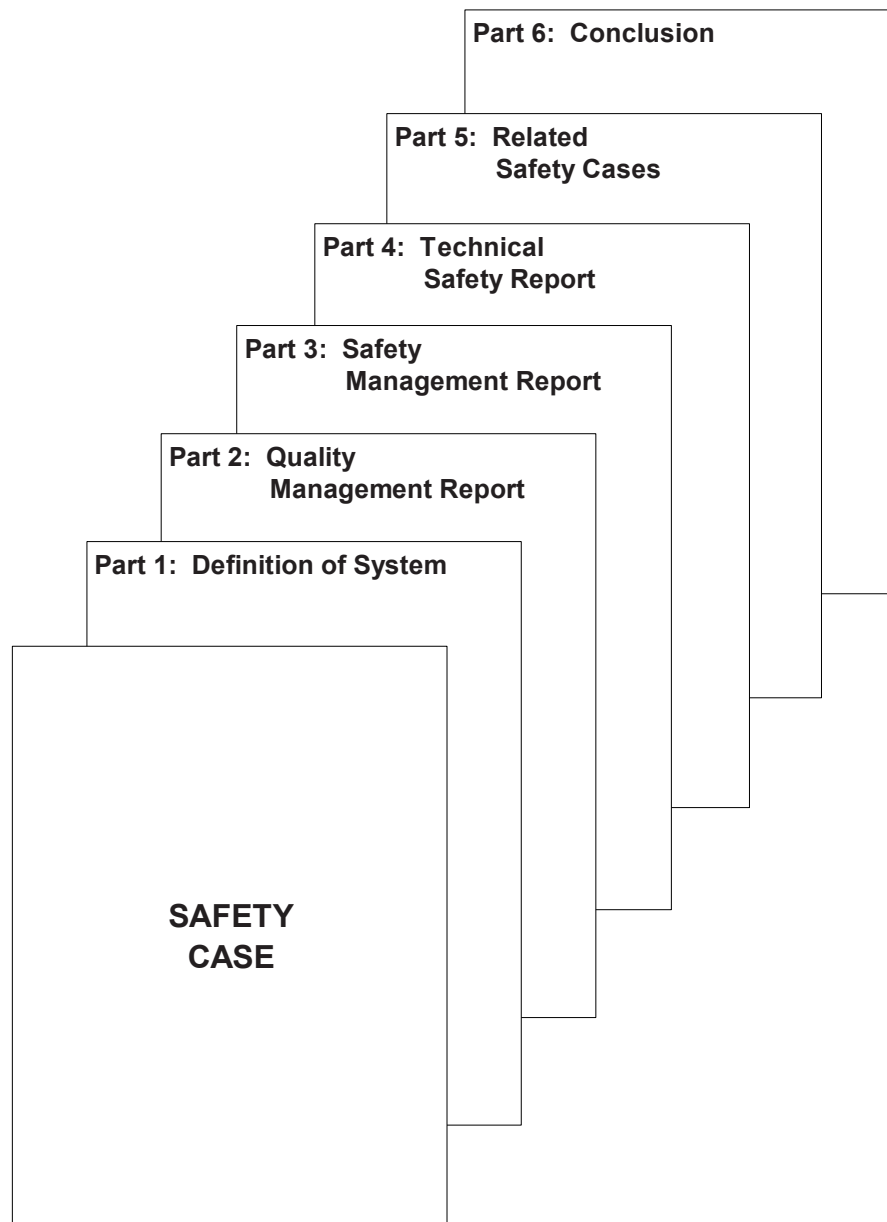


**Figure 3 – Structure of Safety Case**

## 5.2 Evidence of quality management

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

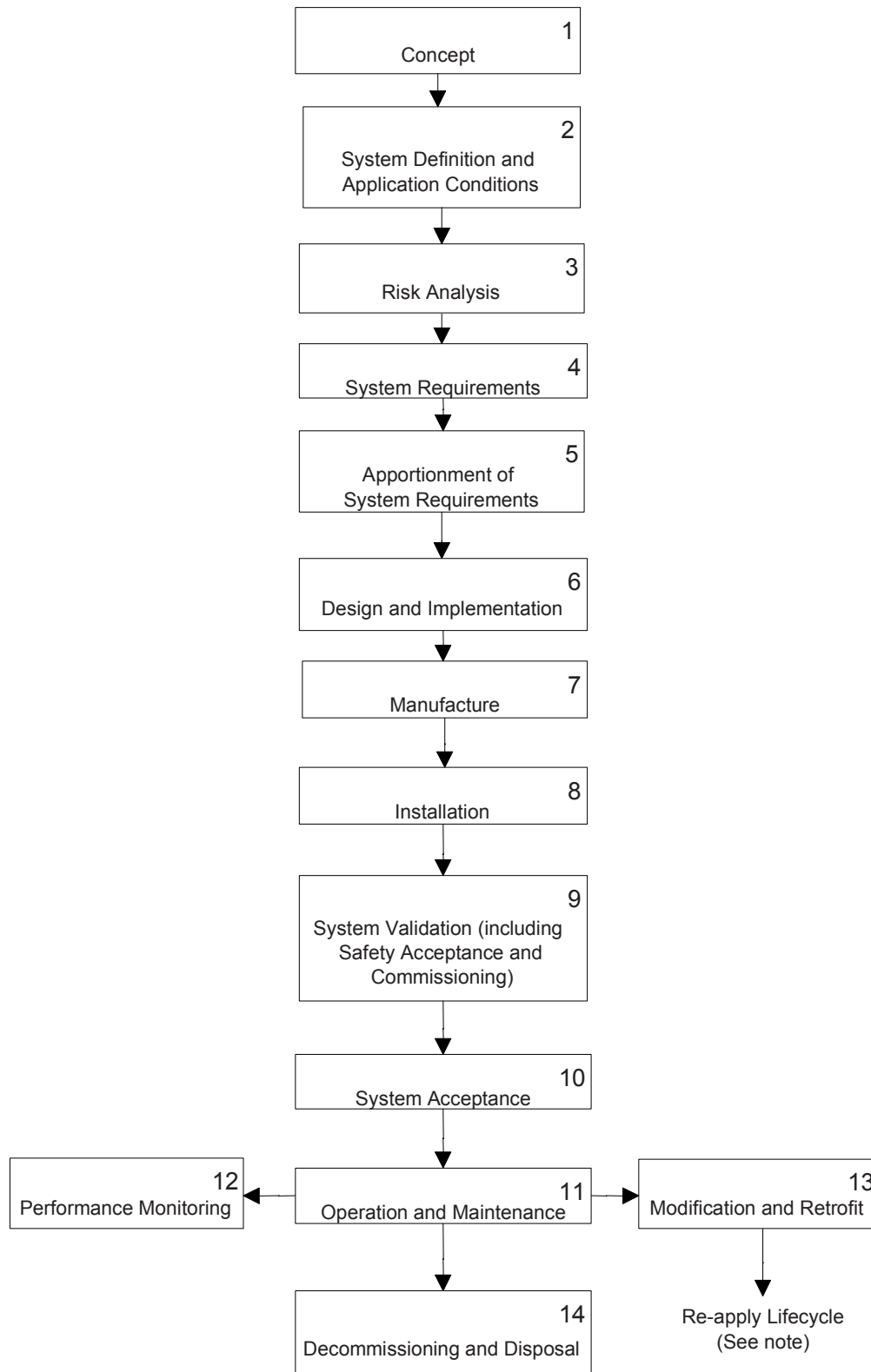
The purpose of the quality management system is to minimise the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system, sub-system or equipment.

The quality management system shall be applicable throughout the system/sub-system/equipment life-cycle, as defined in EN 50126. An example of a system life-cycle diagram (from EN 50126) is reproduced as Figure 4 of this standard.

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

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

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



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

**Figure 4 – Example of system life-cycle**  
(from EN 50126)

## **5.3 Evidence of safety management**

### **5.3.1 Introduction**

The second condition for safety acceptance which shall be satisfied is that the safety of the system, sub-system or equipment has been, and shall continue to be, managed by means of an effective safety management process, which should be consistent with the management process for RAMS described in EN 50126. The purpose of this process is to further reduce the incidence of safety-related human errors throughout the life-cycle, and thus minimise the residual risk of safety-related systematic faults. The elements of the safety management process are briefly summarised in 5.3.2 to 5.3.13 below.

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

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

In all cases the hazard analysis and risk assessment processes defined in EN 50126 are necessary, in order to identify the required level of safety integrity for each particular situation. This includes those cases where the analysis and assessment reveal that a Safety Integrity Level of zero may be assigned; however, once this conclusion has been reached (i.e. that the situation is non-safety-related), and provided it remains at level zero, this safety standard ceases to be applicable.

### **5.3.2 Safety life-cycle**

The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle; this should be consistent with the system life-cycle defined in EN 50126, which is reproduced as Figure 4 of this standard. The design and validation part of the system life-cycle can be viewed as a "top-down" phase followed by a "bottom-up" phase, (i.e. a "V"-diagram), an example of which is shown in Figure 5.

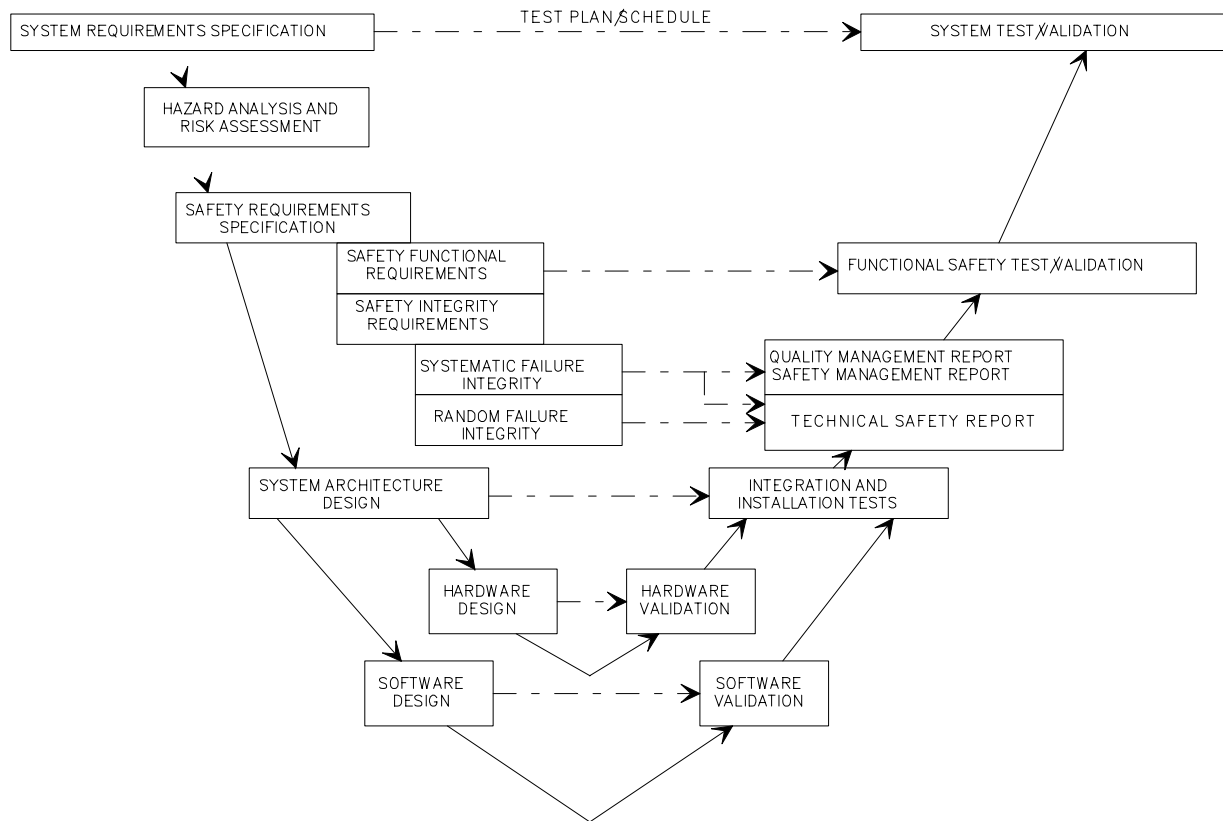
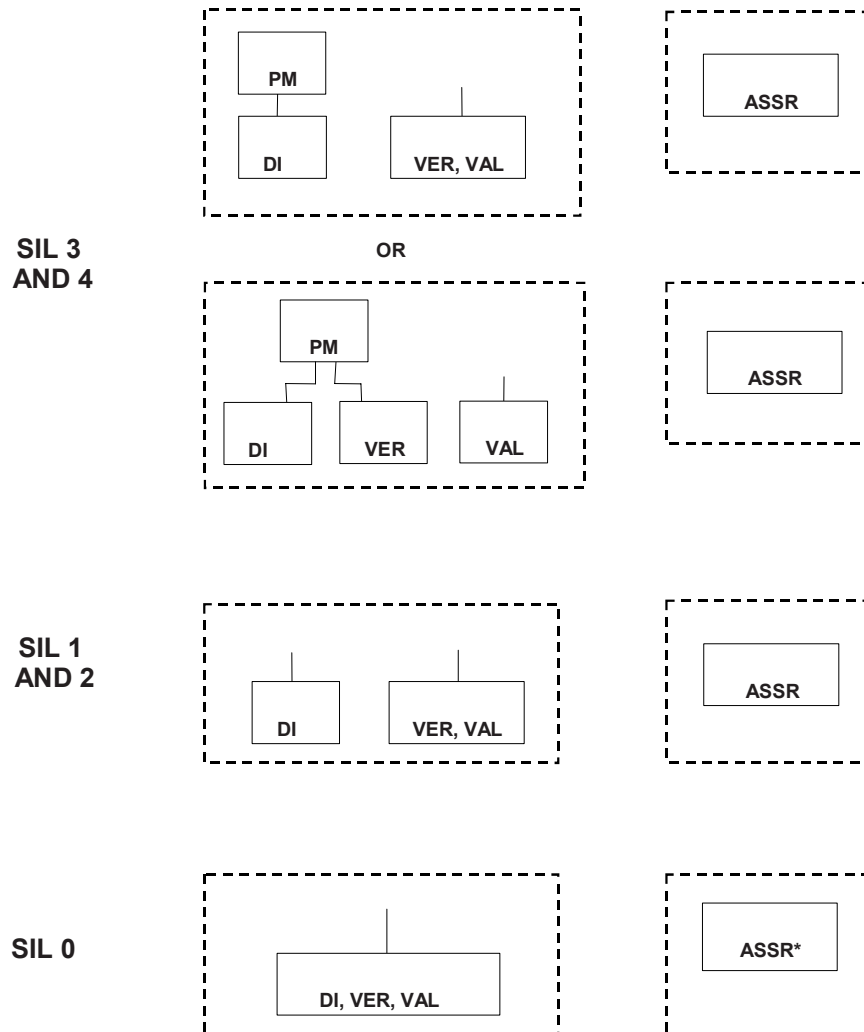


Figure 5 – Example of design and validation portion of system life-cycle

### 5.3.3 Safety organisation

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



Legend: PM = Project Manager  
DI = Designer/Implementer  
VER = Verifier  
VAL = Validator  
ASSR = Assessor

 = Can be the same person

 = Can be the same organisation

\* = For SIL 0, an assessor is necessary only if the safety of the overall system could be affected

Figure 6 – Arrangements for independence

#### **5.3.4 Safety plan**

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

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

The Safety Plan should include a Safety Case Plan, which identifies the intended structure and principal components of the final Safety Case.

#### **5.3.5 Hazard log**

A Hazard Log shall be created and maintained throughout the safety life-cycle, as explained in EN 50126. It shall include a list of identified hazards, together with associated risk classification and risk control information for each hazard. The Hazard Log shall be updated if any modification or alteration is made to the system, sub-system or equipment.

#### **5.3.6 Safety requirements specification**

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

- Hazard Identification and Analysis,
- Risk Assessment and Classification,
- allocation of Safety Integrity Levels,

as explained in EN 50126. Some information concerning Safety Integrity Levels for railway electronic systems is contained in Annex A.

NOTE The Safety Requirements Specification may be included in the system/sub-system/equipment Functional Requirements Specification or may be written as a separate document. See Table E.2, for guidance on System Requirements Specifications for each Safety Integrity Level.

#### **5.3.7 System/sub-system/equipment design**

This phase of the life-cycle shall create a design which fulfils the specified operational and safety requirements. A top-down, structured design methodology shall be used, with rigorously controlled and reviewed documentation. In particular, the relationship between hardware and software, as represented by the Software Requirements Specification and software/hardware integration, shall be strictly managed, and the standard EN 50128 shall be adhered to. Table E.7 gives guidance on design and development of system/sub-system/equipment for each Safety Integrity Level.

#### **5.3.8 Safety reviews**

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

#### **5.3.9 Safety verification and validation**

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

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

The degree of independence necessary for the verifier and the validator shall be in accordance with the Safety Integrity Level of the system/sub-system/equipment under scrutiny. This is shown in Figure 6. Table E.9 gives guidance on verification and validation techniques/measures for each Safety Integrity Level.

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

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

#### **5.3.10 Safety justification**

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

#### **5.3.11 System/sub-system/equipment handover**

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

#### **5.3.12 Operation and maintenance**

Following handover, the procedures, support systems and safety monitoring defined in the Safety Plan and in Section 5 of the Technical Safety Report (part of the Safety Case) shall be adhered to.

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

#### **5.3.13 Decommissioning and disposal**

At the end of the operational life of a system, its decommissioning and disposal shall be carried out in accordance with the measures defined in the Safety Plan and in Section 5 of the Technical Safety Report (part of the Safety Case).

### **5.4 Evidence of functional and technical safety**

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

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

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

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

#### **Section 1 Introduction**

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

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

## **Section 2 Assurance of correct functional operation**

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

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

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

## **Section 3 Effects of faults**

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

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

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

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

- 3.1 Effects of single faults (see B.3.1);
- 3.2 Independence of items (see B.3.2);
- 3.3 Detection of single faults (see B.3.3);
- 3.4 Action following detection (including retention of safe state) (see B.3.4);
- 3.5 Effects of multiple faults (see B.3.5);
- 3.6 Defence against systematic faults (see B.3.6).

## **Section 4 Operation with external influences**

This section shall demonstrate that when subjected to the external influences defined in the System Requirements Specification, the system/sub-system/equipment

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

The Safety Case is therefore valid only within the specified range of external influences, as defined in the System Requirements Specification. Safety is not assured outside these limits, unless additional special measures are provided.

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

More detailed requirements are contained in B.4.

## **Section 5 Safety-related application conditions**

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

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

## Section 6 Safety Qualification Tests

This section shall contain evidence to demonstrate successful completion, under operational conditions, of the Safety Qualification Tests. These are explained in B.6.

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

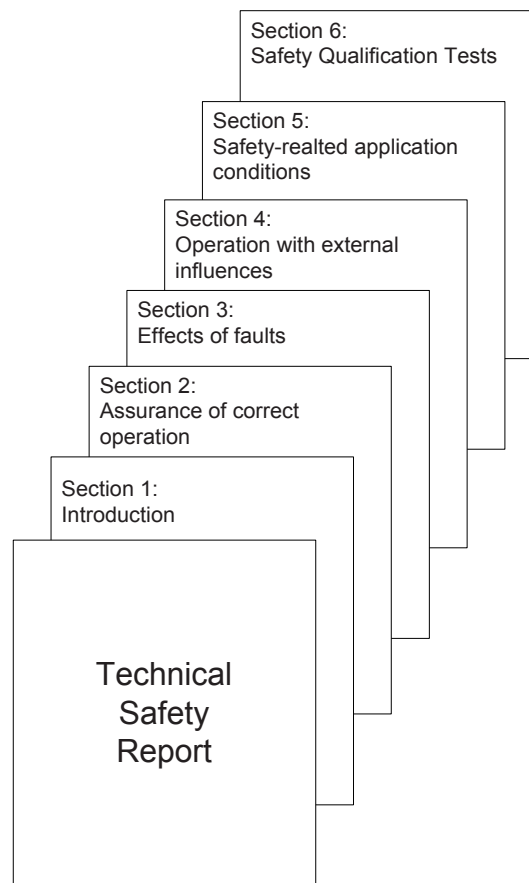


**Figure 7 – Structure of Technical Safety Report**

## 5.5 Safety acceptance and approval

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

### 5.5.1 Introduction

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

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

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

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

Three different categories of Safety Case can be considered:

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

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

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

- the Application Design Safety Case: this shall contain the safety evidence for the theoretical design of the specific application;
- the physical implementation Safety Case: this shall contain the safety evidence for the physical implementation of the specific application.

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

### 5.5.2 Safety approval process

Before an application for Safety approval can be considered, an independent safety assessment of the system/sub-system/equipment and its Safety Case shall be carried out, to provide additional assurance that the necessary level of safety has been achieved. Its results should be presented in a Safety Assessment Report. The report should explain the activities carried out by the safety assessor to determine how the system/sub-system/equipment, (hardware and software) has been designed to meet its specified requirements, and possibly specify some additional conditions for the operation of the system/sub-system/equipment. The depth of the safety assessment, and the degree of independence with which it is carried out, are based on the results of the risk classification, as explained in EN 50126. Specific tests may be required by the safety assessor in order to increase confidence.

The overall documentary evidence shall consist of

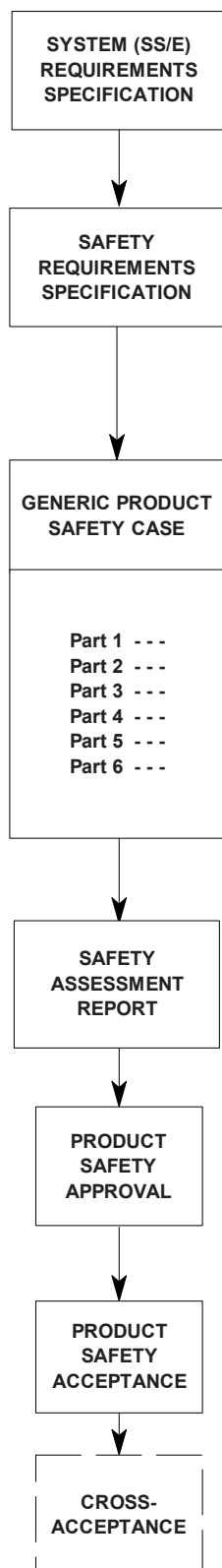
- **the System (or sub-system/equipment) Requirements Specification,**
- **the Safety Requirements Specification,**
- **the Safety Case, including**
  - Part 1: Definition of System/Sub-system/Equipment,
  - Part 2: Quality Management Report (evidence of Quality Management),
  - Part 3: Safety Management Report (evidence of Safety Management),
  - Part 4: Technical Safety Report (evidence of Functional/Technical Safety),
  - Part 5: Related Safety Cases (if applicable),
  - Part 6: Conclusion,
- **the Safety Assessment Report.**

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

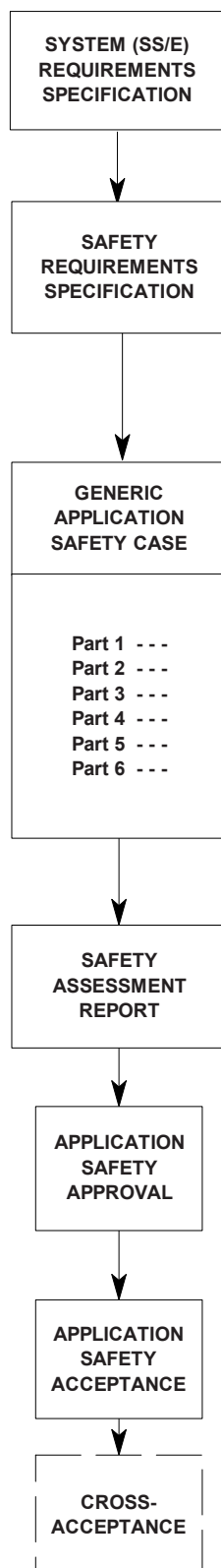
For a generic product (i.e. independent of application), and for a generic application (i.e. class of application), it should be possible for safety approval granted by one safety authority to be accepted by other safety authorities (i.e.: cross-acceptance). This is not considered possible for specific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

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

**GENERIC PRODUCT**  
(Independent of Application)



**GENERIC APPLICATION**  
(Class of Application)



**SPECIFIC APPLICATION**

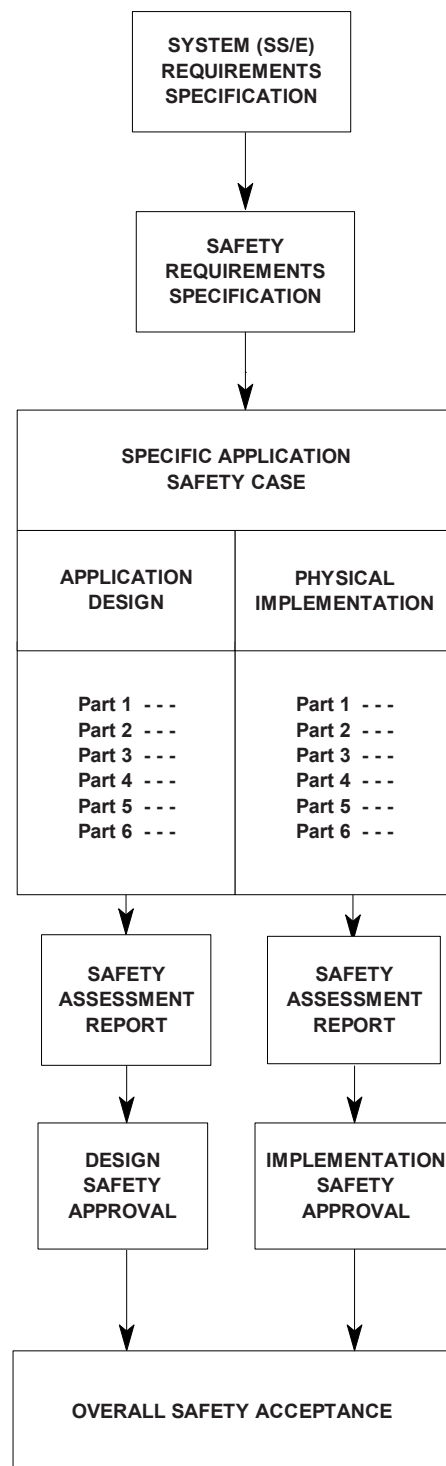


Figure 8 – Safety acceptance and approval process