

Railway applications — Safety related electronic systems for signalling

ICS 45.020 ; 93.100

National foreword

This Draft for Development is the English language version of ENV 50129:1998.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because the ENV is a prospective standard for provisional application for an initial period of three years. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use of this Draft for Development are requested so that the UK experience can be reported to the European organization responsible for its conversion into a European Standard. A review of this publication will be initiated 2 years after its publication by the European organization so that a decision can be taken on its status at the end of its three-year life. The commencement of the review period will be notified by an announcement in *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European Standard, to extend the life of the prestandard or to withdraw it. Comments should be sent in writing to secretary of BSI Subcommittee GEL/9/1, Signalling and communications, at 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled "International Standards Correspondence Index", or by using the "Find" facility of the BSI Standards Electronic Catalogue.

Summary of pages

This document comprises a front cover, an inside front cover, the ENV title page, pages 2 to 138, an inside back cover and a back cover.

The BSI copyright notice displayed throughout this document indicates when the document was last issued.

This Draft for Development, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 August 1999

© BSI 08-1999

ISBN 0 580 32697 7

Amendments issued since publication

Amd. No.	Date	Comments

Descriptors: Railway equipment, safety related systems, electronic components, safety integrity levels, safety requirements, safety acceptance, safety case

English version

Railway applications
Safety related electronic systems for signalling

Applications ferroviaires
Systèmes électroniques de sécurité pour
la signalisation

Bahnanwendungen
Sicherheitsrelevante elektronische
Systeme für Signaltechnik

This European Prestandard (ENV) was approved by CENELEC on 1997-06-17 as a prospective standard for provisional application. The period of validity of this ENV is limited initially to three years. After two years the members of CENELEC will be requested to submit their comments, particularly on the question whether the ENV can be converted into a European Standard (EN).

CENELEC members are required to announce the existence of this ENV in the same way as for an EN and to make the ENV available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the ENV) until the final decision about the possible conversion of the ENV into an EN is reached.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, 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

© 1998 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Foreword

This European Prestandard was prepared by Subcommittee 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 CENELEC members for comments and approved as ENV 50129 during the voting meeting of CENELEC/SC 9XA on 1997-06-17.

The following date was fixed:

- latest date by which the existence of the ENV
has to be announced at national level (doa) 1998-02-01
-

Contents

	Page
Introduction	5
1 Scope	7
2 Normative references	9
3 Definitions and abbreviations	10
3.1 Definitions	10
3.2 Abbreviations	16
4 Overall framework of this standard	17
5 Conditions for safety acceptance and approval	19
5.1 The Safety Case	19
5.2 Evidence of quality management	22
5.3 Evidence of safety management	25
5.4 Evidence of functional and technical safety	31
5.5 Safety acceptance and approval	35
Figures	
1 Scope of CENELEC railway standards	8
2 Structure of this standard (ENV 50129)	18
3 Structure of Safety Case	21
4 Example of system life-cycle	24
5 Example of design and validation portion of system life-cycle	26
6 Arrangements for independence	30
7 Structure of Technical Safety Report	34
8 Safety acceptance and approval process	38
9 Examples of dependencies between Safety Cases/Safety Approvals	39

Annexes

A (normative)	Safety Integrity Levels	41
B (normative)	Additional technical requirements	53
C (normative)	Identification of hardware component failure modes	77
D (informative)	Supplementary technical information	107
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	121
F (informative)	Bibliography	138

Introduction

This document is the first European standardization document 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 subsystems 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 European Standard (EN).

The standard consists of the main part (clauses 1 to 6) and annexes A, B, C, D, E and F. The requirements defined in the main part of the standard and in annexes A, B and C are normative, whilst annexes D, E and F are informative.

This European Prestandard standard is consistent with, and uses relevant sections of EN 50126: "Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)". In particular, both standards are based on the system life-cycle.

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 "Railway applications - Software for railway control and protection systems".

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

1 Scope

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

The scope of this European Prestandard, and its relationship with other CENELEC standards, are shown in figure 1.

This European Prestandard is primarily intended to apply to "fail-safe" and "high-integrity" systems (e.g.: main-line signalling and ATP systems), rather than medium or low-integrity systems (e.g.: running "on-sight", or in marshalling yards where points are moved as vehicles approach). However, in all cases the hazard analysis and risk assessment processes defined in EN 50126 are necessary, in order to identify the safety requirements for each particular situation. This includes those cases where the analysis and assessment reveal that no safety requirements exist; however, once this conclusion has been reached (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 European Prestandard applies to the acceptance of the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension of complete systems, and also to individual subsystems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

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

This European Prestandard is not applicable to existing systems/subsystems/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, subsystems and equipment.

This European Prestandard is primarily applicable to systems/subsystems/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 European Prestandard 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.

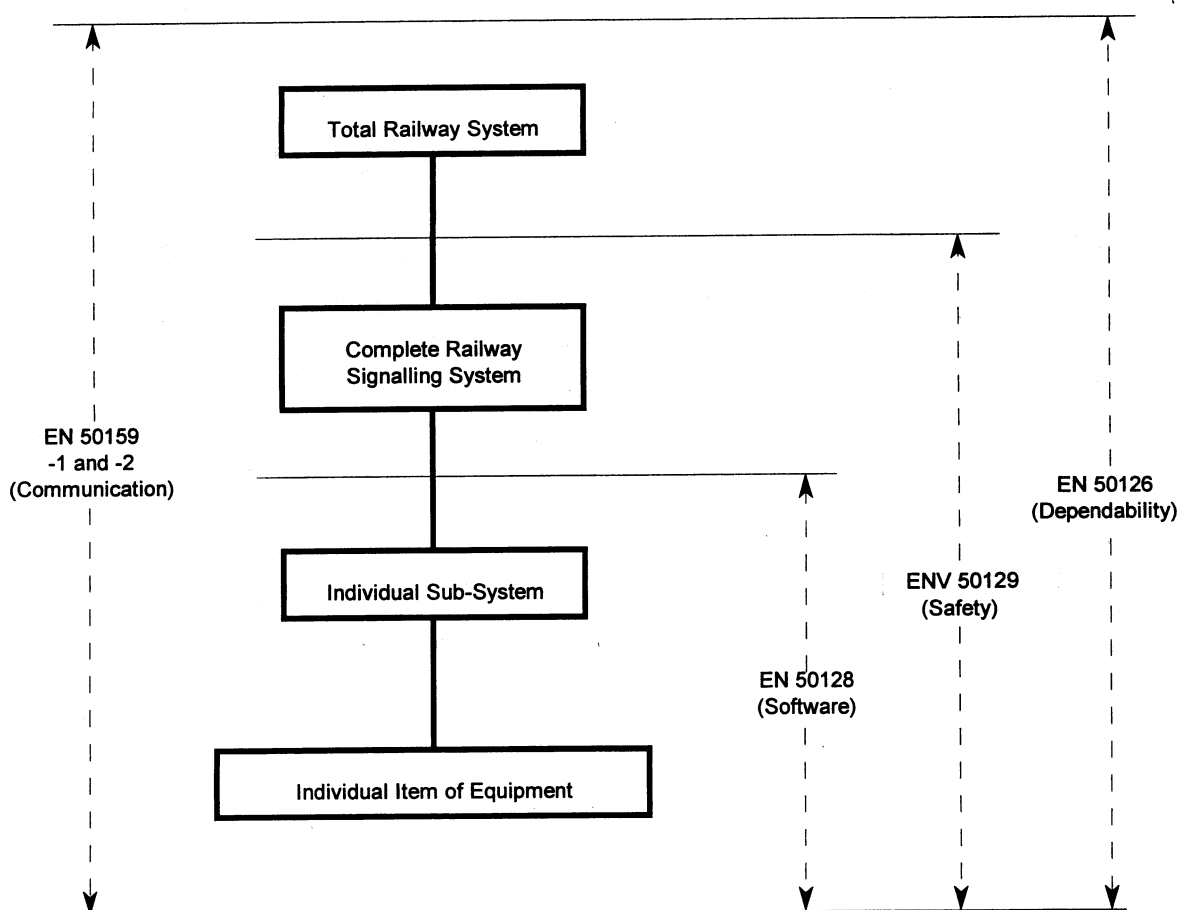


Figure 1: Scope of CENELEC railway standards

2 Normative references

This European Prestandard 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 Prestandard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

NOTE: Additional informative references are included in annex F: Bibliography.

EN 50121-2	Railway applications - Electromagnetic compatibility (EMC) - Interaction of the whole railway system with the outside world
EN 50121-3	Railway applications - Electromagnetic compatibility (EMC) - Rolling stock
EN 50121-4	Railway applications - Electromagnetic compatibility (EMC) - Signalling and communications
EN 50124-1	Railway applications - Insulation co-ordination - Basic requirements, clearances and creepage distances
EN 50124-3	Railway applications - Insulation co-ordination - Solid and liquid insulations
EN 50125-1	Railway applications - Environmental conditions for equipment - Equipment on board rolling stock
EN 50125-3	Railway applications - Environmental conditions for equipment - Signalling and communications
EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
EN 50128	Railway applications - Software for railway control and protection systems
EN 50155	Railway applications - Electronic equipment used on rail vehicles
EN 50159-1	Railway applications - Signalling and communications - Safety-related communication in closed transmission systems
EN 50159-2	Railway applications - Signalling and communications - Safety-related communication in open transmission 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 assessor: The person or agent appointed to carry out the assessment.

3.1.4 authorisation: The formal permission to use a product within specified application constraints.

3.1.5 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.

3.1.6 can: Is possible.

3.1.7 common-mode fault: Fault common to items which are intended to be independent.

3.1.8 component: See **element**

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 pre-build exercise of defining elements and their interconnection such that the product will meet its specified requirements.

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 designer: One or more persons assigned by the Design Authority to analyse and transform specified requirements into acceptable design solutions which have the required safety integrity.

3.1.14 diversity: A means of achieving all or part of the specified requirements in more than one independent and dissimilar manner.

3.1.15 element: A part of a product that has been determined to be a basic unit or building block. An element may be simple or complex.

3.1.16 equipment: A functional physical item.

3.1.17 error: A deviation from the intended design which could result in unintended system behaviour or failure.

3.1.18 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.

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

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

3.1.21 fault detection time: Time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected.

3.1.22 hazard: A condition that could lead to an accident.

3.1.23 hazard analysis: The process of identifying the hazards which a product or its use can cause.

3.1.24 hazard log: The document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced.

3.1.25 human error: A human action (mistake), which can result in unintended system behaviour/failure.

3.1.26 independence (human): Freedom from intellectual, commercial and/or management involvement.

3.1.27 independence (technical): Freedom from any mechanism which can affect the correct operation of more than one item.

3.1.28 item: Element under consideration.

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

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

3.1.31 may: Is permissible.

3.1.32 negation: Enforcement of a safe state following detection of a hazardous fault.

3.1.33 negation time: Time span which begins when the existence of a fault is detected and ends when a safe state is enforced.

3.1.34 product: A collection of elements, interconnected to form a system, subsystem or item of equipment, in a manner which meets the specified requirements.

3.1.35 quality: A user perception of the attributes of a product.

3.1.36 railway authority: The body with the overall accountability to a safety authority for operating a safe railway system.

3.1.37 random failure integrity: The degree to which a system is free from hazardous random faults.

3.1.38 random fault: The occurrence of a fault based on probability theory and previous performance.

3.1.39 redundancy: The provision of one or more additional elements, usually identical, to achieve or maintain availability under the failure of one or more of those elements.

3.1.40 reliability: The ability of an item to perform a required function under given conditions for a given period of time.

3.1.41 repair: Measures for re-establishing the required state of a system, subsystem or item of equipment.

3.1.42 risk: The combination of the frequency, or probability, and the consequence of a specified hazardous event.

3.1.43 safe state: A condition which continues to preserve safety.

3.1.44 safety: Freedom from unacceptable levels of risk.

3.1.45 safety acceptance: The safety status given to a product by the final user.

3.1.46 safety acceptance process: The series of procedures that are followed to achieve safety acceptance.

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 Approval process: The series of procedures that are followed to achieve Safety Approval.

3.1.49 safety assessment: The process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified safety requirements and to form a judgement as to whether the product is safe for its intended purpose.

3.1.50 safety assessor: The person or agent appointed to carry out the safety assessment.

3.1.51 safety authority: The body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements.

3.1.52 Safety Case: The documented demonstration that the product complies with the specified safety requirements.

3.1.53 safety-critical: Carries direct responsibility for safety.

3.1.54 safety-critical system: A system that is intended to achieve, on its own, the necessary level of safety integrity for the implementation of the required safety functions.

3.1.55 safety integrity: The likelihood of a safety-related system achieving its required safety features under all the stated conditions within a stated operational environment and within a stated period of time.

3.1.56 Safety Integrity Level: A number which indicates the required degree of confidence that a system will meet its specified safety features.

3.1.57 safety-involved: Carries indirect responsibility for safety.

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

3.1.59 safety management: The management structure which ensures that the safety process is properly implemented.

3.1.60 safety plan: The implementation details of how the safety requirements of the project will be achieved.

3.1.61 safety process: The series of procedures that are followed to enable all safety requirements of a product to be identified and met.

3.1.62 safety-related: Carries responsibility for safety.

3.1.63 shall: Is mandatory.

3.1.64 should: Is recommended.

3.1.65 signalling system: Particular kind of system used on a railway to control and protect the operation of trains.

3.1.66 stress profile: The degree and number of external influences which a product can withstand whilst performing its required functionality.

3.1.67 subsystem: A portion of a system which fulfils a specialised function.

3.1.68 system: A set of subsystems or elements which interact according to a design.

3.1.69 systematic failure integrity: The degree to which a system is free from non-identified hazardous errors and the causes thereof.

3.1.70 systematic fault: An inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment.

3.1.71 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.

3.1.72 Technical Safety Report: Documented technical evidence for the safety of the design of a system, subsystem or item of equipment.

3.1.73 validation: The activity of demonstration, by test and analysis, that the product meets in all respects its specified requirements.

3.1.74 validator: The person or agent appointed to carry out validation.

3.1.75 verification: The activity of determination, by analysis and test, that the output of each phase of the life-cycle fulfils the requirements of the previous phase.

3.1.76 verifier: The person or agent appointed to carry out verification.

3.2 Abbreviations

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

3.2.1	a.c.	alternating current
3.2.2	ATP	automatic train protection
3.2.3	CENELEC	European Committee for Electrotechnical Standardisation
3.2.4	CMF	common-mode failure
3.2.5	d.c.	direct current
3.2.6	EMC	electromagnetic compatibility
3.2.7	EMI	electromagnetic interference
3.2.8	EN	European Standard
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	FTA	fault tree analysis
3.2.13	HW	hardware
3.2.14	IEC	International Electrotechnical Commission
3.2.15	IRSE	Institution of Railway Signal Engineers
3.2.16	ISO	International Standards Organisation
3.2.17	RAMS	reliability, availability, maintainability and safety
3.2.18	SCR	silicon controlled rectifier

3.2.19	SIL	Safety Integrity Level
3.2.20	SW	software
3.2.21	UIC	International Union of Railways
3.2.22	VDR	voltage-dependent resistor

4 Overall framework of this European Prestandard

Clause 5 of this European Prestandard 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 additional technical requirements for safety-related systems/subsystems/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.

Annex F (informative) contains references to documents which have been consulted during the preparation of this Prestandard.

The structure of this European Prestandard is summarised in figure 2.

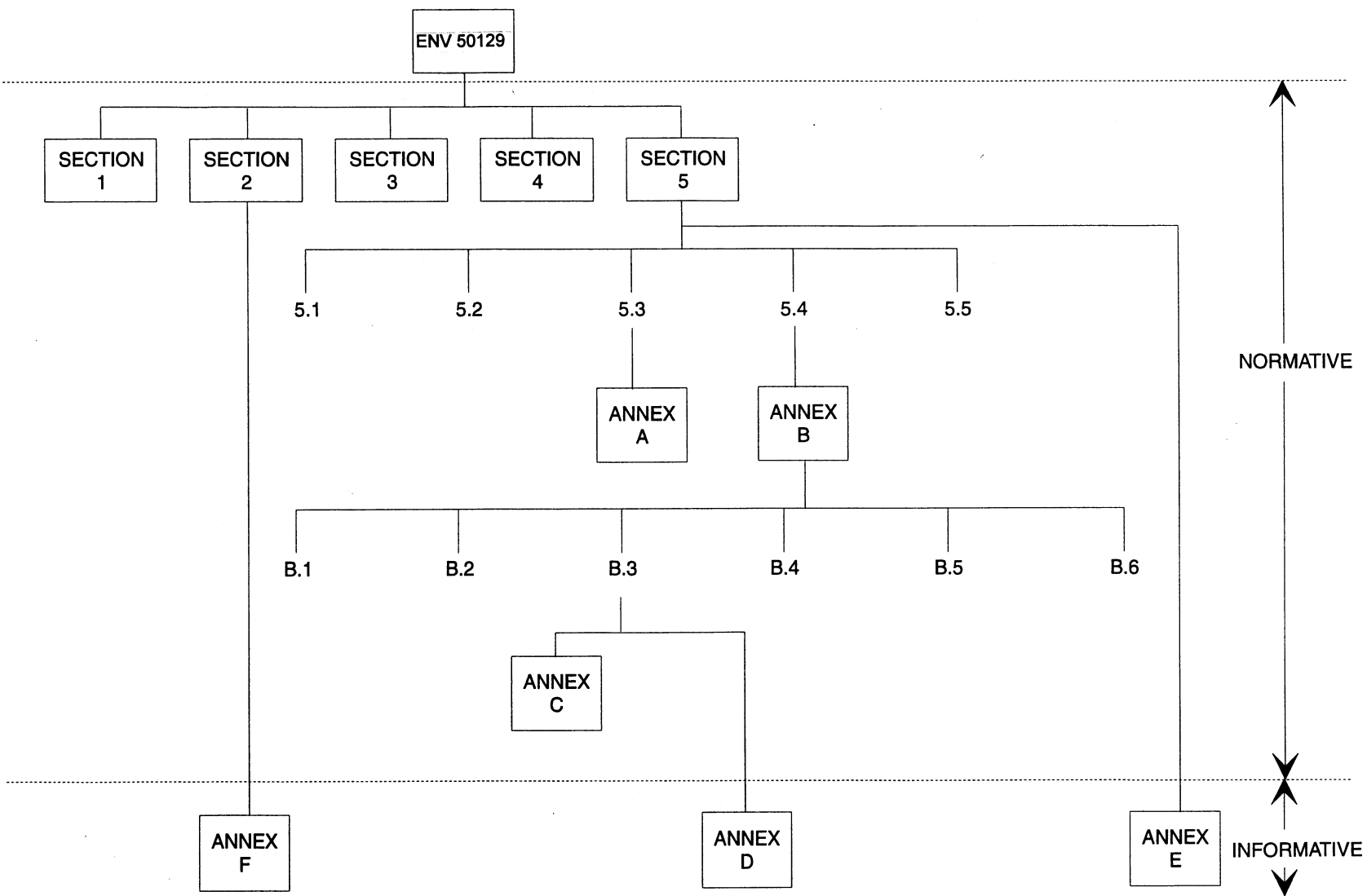


Figure 2: Structure of ENV 50129

5 Conditions for safety acceptance and approval

5.1 The Safety Case

This European Prestandard defines the conditions which shall be satisfied in order that a safety-related electronic railway system, subsystem or item of 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, subsystem and system levels, before the safety-related system can be accepted as adequately safe.

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

The Safety Case contains the documented safety evidence for the system, subsystem or item of equipment, and shall be structured as follows:

Part 1 Definition of System (or subsystem/equipment)

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

Part 2 Quality Management Report

This shall contain the evidence of Quality Management, as specified in 5.2.

Part 3 Safety Management Report

This shall contain the evidence of Safety Management, as specified in 5.3.

Part 4 Technical Safety Report

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

Part 5 Related Safety Cases

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

This part shall also demonstrate that all the safety-related application conditions specified in each of the related subsystem/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/subsystem/equipment is adequately safe, subject to compliance with the specified application conditions.

The structure of the Safety Case is illustrated in figure 3 of this standard.

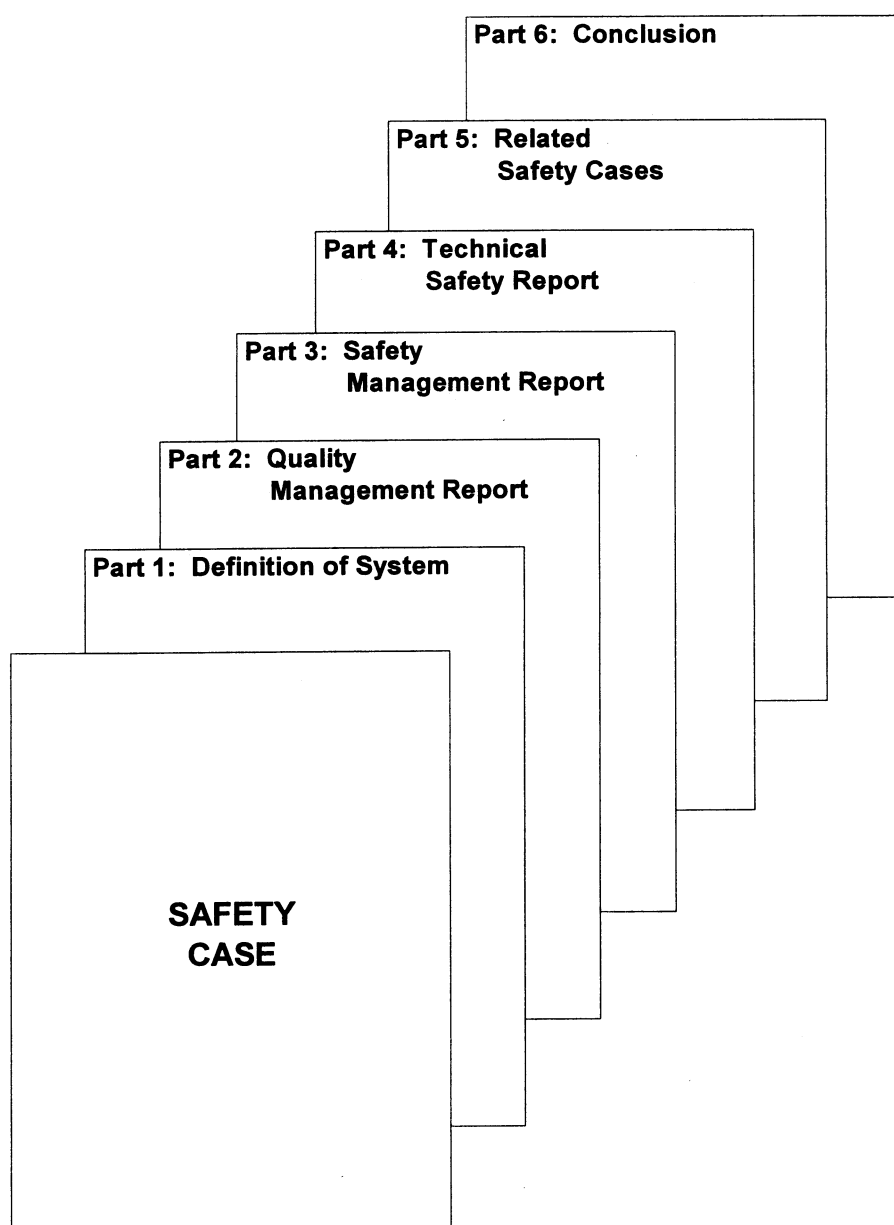


Figure 3: Structure of Safety Case

5.2 Evidence of quality management

The first condition for safety acceptance which shall be satisfied is that the quality of the system, subsystem 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, subsystem or equipment.

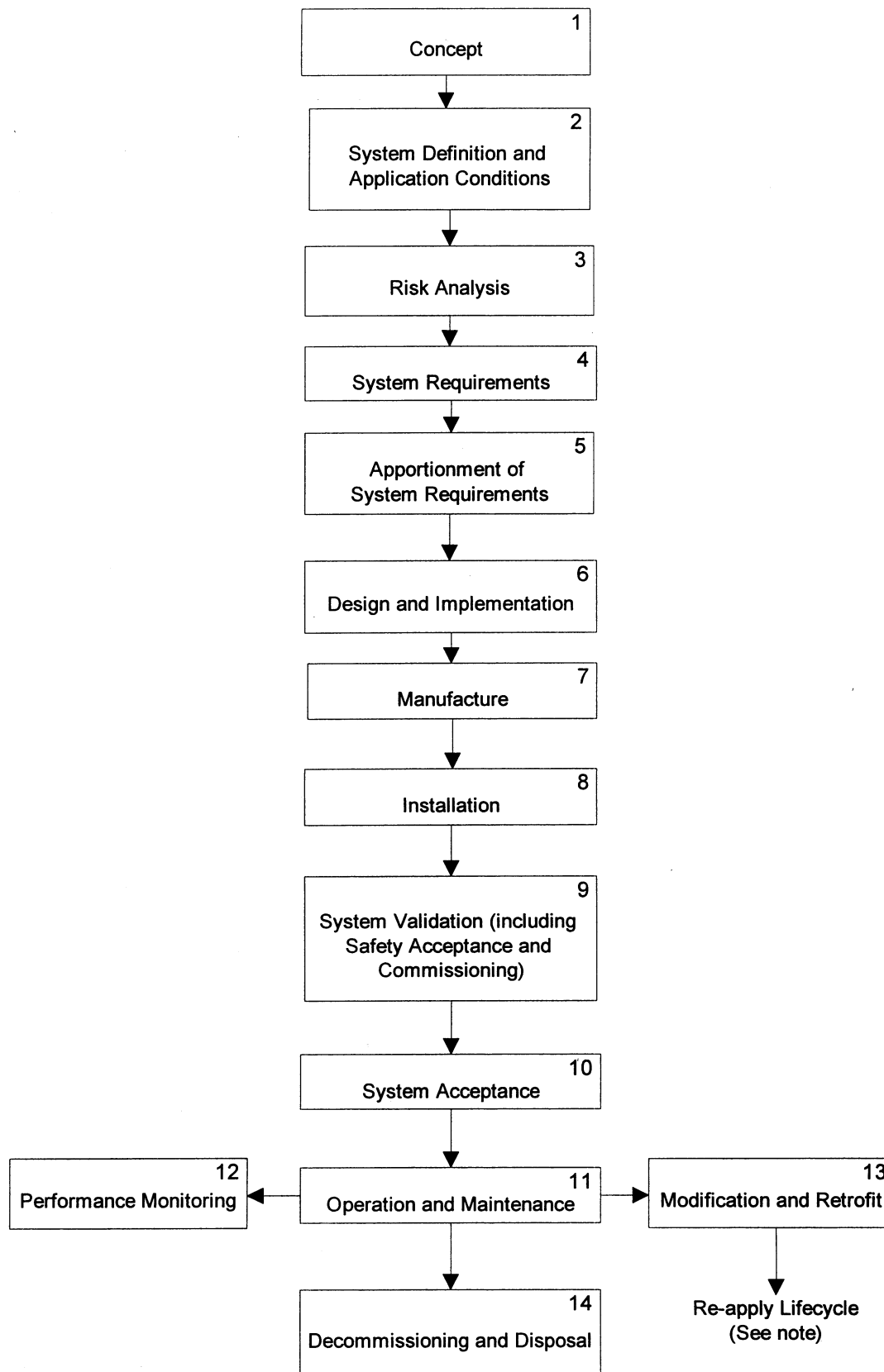
The quality management system shall be applicable throughout the system/subsystem/equipment life-cycle, as defined in EN 50126. An example of a system life-cycle diagram (from EN 50126) is reproduced as figure 4 of this standard.

NOTE: Examples of aspects (based on ISO 9001) 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.

Large volumes of detailed evidence and supporting documentation need not be included in the Quality Management Report, provided precise references are given to such documents.

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/subsystem/equipment under scrutiny (see tables E.1 and 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, subsystem 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 Dependability (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/subsystem/equipment under scrutiny. The requirements for Safety Integrity Level 0 (non-safety-related) are outside the scope of this safety standard.

NOTE: 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 of this standard.

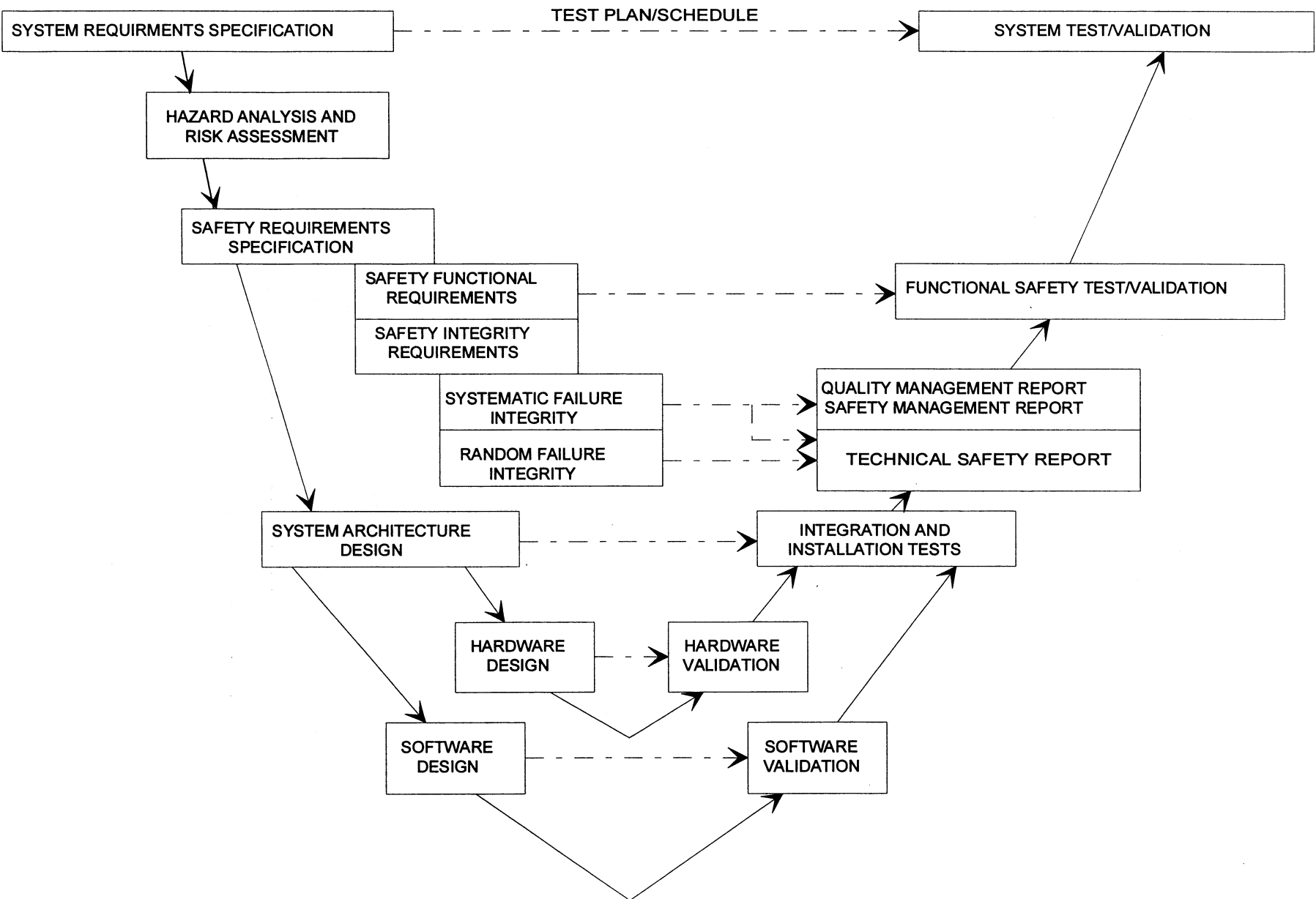


Figure 5: Example of design and validation portion of system life-cycle

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 of this standard. See also table E.3, for guidance on the safety organisation required for each Safety Integrity Level.

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/subsystem/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/subsystem/equipment, including both hardware and software. A software safety plan, in accordance with EN 50128, shall be included or referenced.

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, subsystem or equipment.

5.3.6 Safety requirements specification

The specific safety requirements for each system/subsystem/item of 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/subsystem/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/subsystem/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/subsystem/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, subsystem or equipment shall also be subject to review.

5.3.9 Safety verification and validation

The safety plan shall include 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/subsystem/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/subsystem/equipment.

The degree of independence necessary for the verifier and the validator shall be in accordance with the Safety Integrity Level of the system/subsystem/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/subsystem/equipment meets the defined conditions for safety acceptance shall be presented in a structured safety justification document known as the Safety Case, as explained in 5.1.

5.3.11 System/subsystem/equipment handover

Prior to handover of the system, subsystem or item of 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.

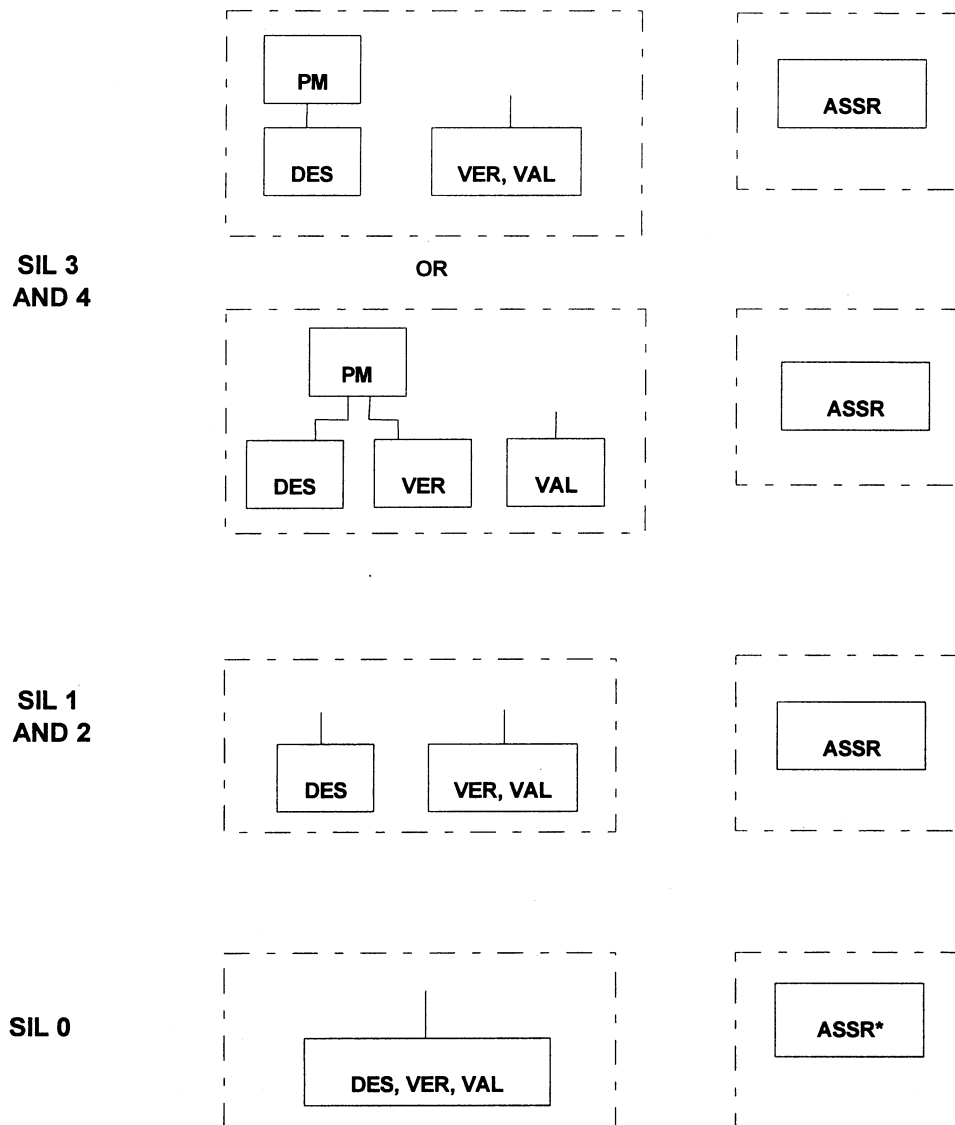
5.3.12 Operation and maintenance

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.

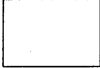
During the operational life of a system, change requests may be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation. Where a change request results in 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).



Legend: PM = Project Manager
DES = Designer
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 an overall system could be affected

Figure 6: Arrangements for independence

5.4 Evidence of functional and technical safety

In addition to the evidence of quality and safety management, described in 6.2 and 6.3 of this standard, a third condition shall be satisfied before a system, subsystem or item of 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/subsystem/equipment, as explained in 5.1.

The Technical Safety Report is mandatory for Safety Integrity Levels 1 to 4 inclusive (see annex A for explanation of Safety Integrity Levels). However, the depth of the information and the extent of the supporting documentation should be appropriate to the Safety Integrity Level of the system/subsystem/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). Large volumes of detailed evidence and supporting documentation need not be included, provided precise references are given to such documents.

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 which are relied on for safety and the extent to which the system/subsystem/equipment is claimed to be fail-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/subsystem/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 Fulfilment of the specified environmental conditions (see B.2.6);
- 2.7 Assurance of correct software functionality (see B.2.7).

Section 3 Effects of faults

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

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

This section shall also include demonstration that faults in any system/subsystem/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 tables E.5 and E.6.

- 3.1 Results 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/subsystem/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/subsystem/equipment. This shall include the application conditions contained in the Safety Case of any related subsystem or item of 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 of this standard.

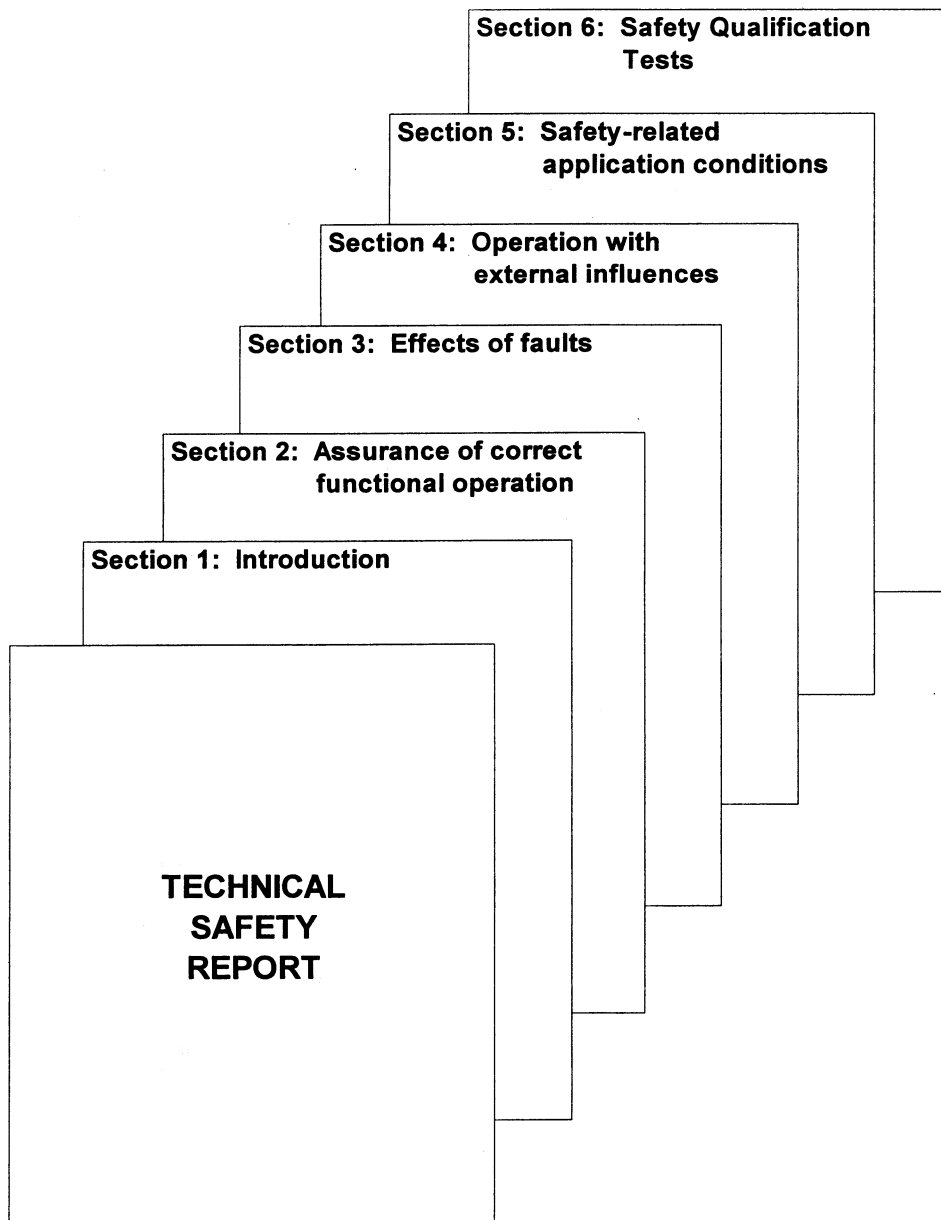


Figure 7: Structure of Technical Safety Report

5.5 Safety acceptance and approval

This subclause defines the safety acceptance and approval process for safety-related electronic systems, subsystems or items of 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, subsystem or item of equipment can be accepted as adequately safe for its intended application:

- **Evidence of quality management;**
- **Evidence of safety management;**
- **Evidence of functional and technical safety.**

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

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

Three different categories of Safety Case can be considered:

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

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

In all three categories, the structure of the Safety Case and the procedure for obtaining Safety Approval are basically the same.

However, there is an additional factor for specific applications : in this category, separate Safety Approval is needed for the application design of the system and for its physical implementation (e.g., manufacture, installation, test, and facilities for operation and maintenance). For this reason, the Safety Case for specific applications shall be divided into two portions:

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

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

5.5.2 Safety Approval process

Before an application for Safety Approval can be considered, an independent safety assessment of the system/subsystem/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, subsystem or item of equipment, (hardware and software) has been designed to meet its specified requirements, and possibly specify some additional conditions for the operation of the system/subsystem/item of 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 subsystem/equipment) requirements specification;**
- **The safety requirements specification;**
- **The Safety Case, including:**
 - Part 1 - Definition of system/subsystem/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, subsystem or item of 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.

5.5.3 After Safety Approval

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

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

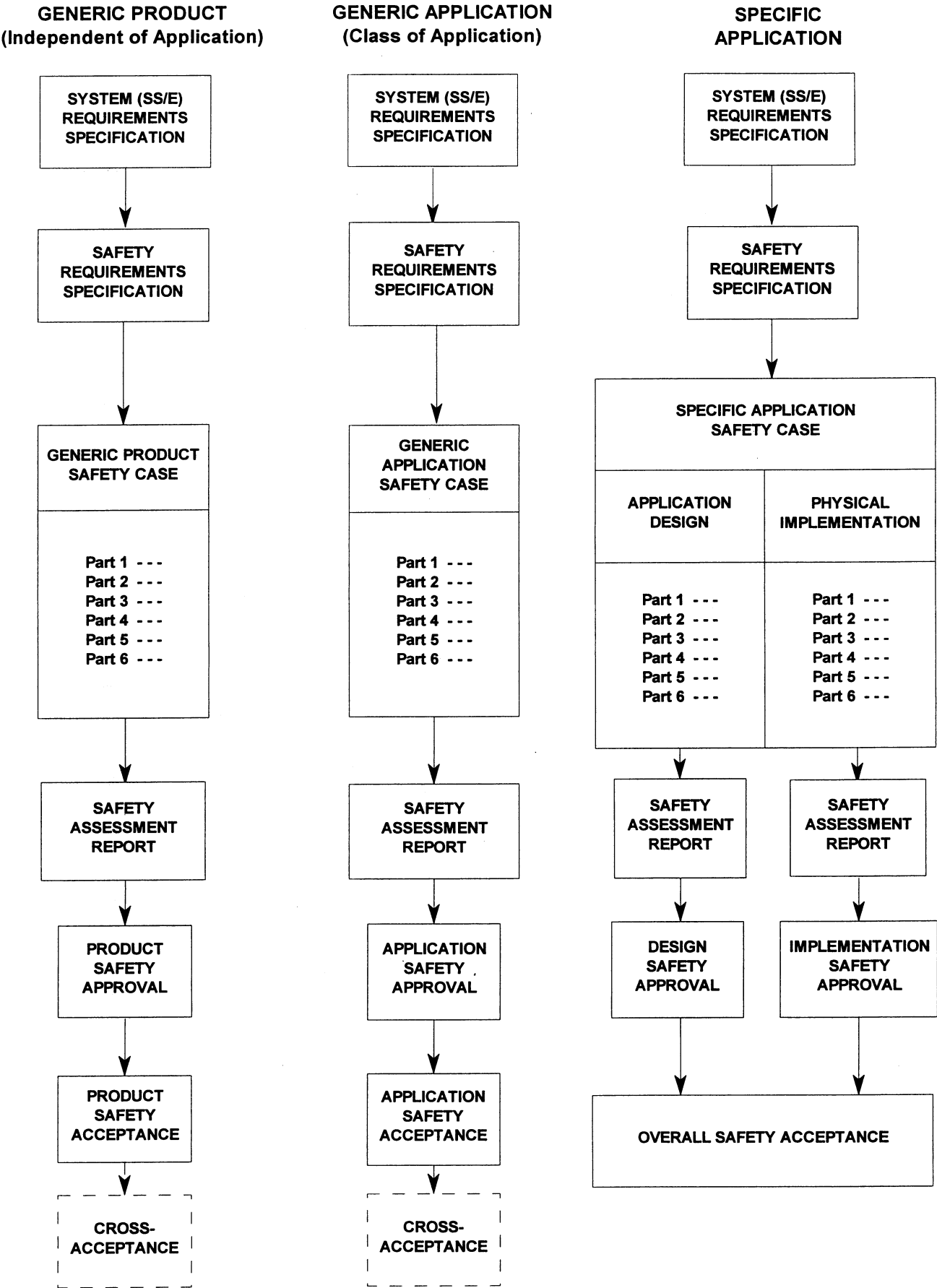


Figure 8: Safety acceptance and approval process

5.5.4 Dependency between Safety Approvals

As mentioned in 5.1, the Safety Case for a system may depend on the Safety Cases of other subsystems or equipment. In such circumstances, Safety Approval of the main system is not possible without previous Safety Approval of the related subsystems/equipment.

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

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

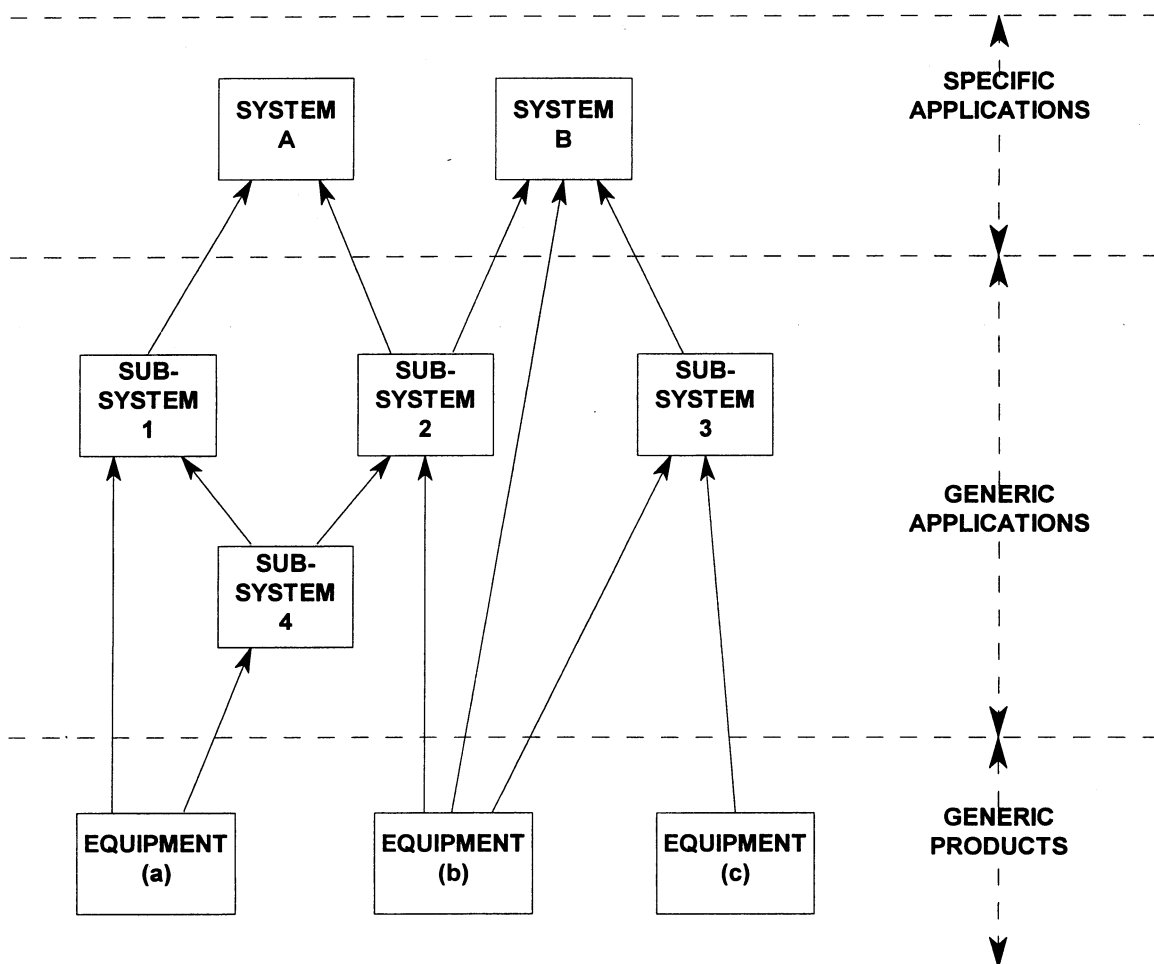


Figure 9: Examples of dependencies between Safety Cases/Safety Approval

Blank page

Annex A (normative)

Safety Integrity Levels

	Page
A.1 Introduction	42
A.2 Safety requirements	42
A.3 Safety integrity	43
A.4 Safety Integrity Levels (SIL)	45
A.4.1 General Aspects	45
A.4.2 Methodology for determining the SIL	47
A.5 Allocation of Safety Integrity Levels	51
A.6 Link between risk reduction and allocation of SIL	51
 Figures	
A.1 Safety requirements and safety integrity	43
A.2 Relationship between SILs, techniques and figures	47
A.3 Safety management process	48
A.4 SIL Viewpoints	49
A.5 Generic explanation of the risk reduction process	52
A.6 Risk reduction and allocation of the SIL at the level of element	52