BS EN 50126-2:2017+A1:2024

BSI Standards Publication

Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Part 2: Systems approach to safety

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

National foreword

This British Standard is the UK implementation of EN 50126-2:2017+A1:2024. It supersedes BS EN 50126-2:2017, which will be withdrawn on 30 November 2027.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to CENELEC text carry the number of the CENELEC amendment. For example, text altered by CENELEC amendment A1 is indicated by ▌A1⟩ ⟨A1▌.

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

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 25780 9

ICS 45.020

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2017.

Amendments/corrigenda issued since publication

Date	Text affected
30 November 2024	Implementation of CENELEC amendment A1:2024

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50126-2:2017+A1

November 2024

ICS 45.020

Supersedes CLC/TR 50126-2:2007

English Version

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

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

This European Standard was approved by CENELEC on 2017-07-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2017 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50126-2:2017 E

AVA Documents Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

Contents

Page

European foreword ... 5
European foreword to Amendment 1 ... 5
Introduction ... 6
1 Scope ... 7
2 Normative references ... 8
3 Terms and definitions ... 8
4 Abbreviations ... 8
5 Safety process ... 9
5.1 Risk assessment and hazard control ... 9
5.2 A. Risk assessment ... 10
5.2.1 General ... 10
5.2.2 Conducting risk assessment ... 11
5.3 B. Outcome of the risk assessment ... 11
5.4 C. Hazard control ... 11
5.5 D. Revision of risk assessment ... 12
5.6 Responsibilities ... 13
6 Safety demonstration and acceptance ... 13
6.1 Introduction ... 13
6.2 Safety demonstration and safety acceptance process ... 13
6.3 Responsibility in managing the Safety Case ... 17
6.4 Modifications after safety acceptance ... 17
6.5 Dependencies between Safety Cases ... 17
6.6 Relationship between safety cases and system architecture ... 18
7 Organisation and Independence of Roles ... 19
7.1 General ... 19
7.2 Early phases of the lifecycle (phases 1 to 4) ... 19
7.3 Later phases of the lifecycle (starting from phase 5) ... 20
7.4 Personnel Competence ... 21
8 Risk assessment ... 22
8.1 Introduction ... 22
8.2 Risk Analysis ... 22
8.2.1 General ... 22
8.2.2 The risk model ... 22
8.2.3 Techniques for the consequence analysis ... 24
8.2.4 Expert Judgement ... 25
8.3 Risk acceptance principles and risk evaluation ... 25
8.3.1 Use of Code of Practice ... 25
8.3.2 Use of a reference system ... 26
8.3.3 Use of Explicit Risk Estimation ... 27
8.4 Application of explicit risk estimation ... 28
8.4.1 Quantitative approach ... 28
8.4.2 Variability using quantitative risk estimates ... 30
8.4.3 Qualitative and semi-quantitative approaches ... 31

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

9 Specification of System Safety Requirements ... 32
9.1 General ... 32
9.2 Safety requirements ... 32
9.3 Categorization of Safety Requirements ... 32
9.3.1 General ... 32
9.3.2 Functional safety requirements ... 33
9.3.3 Technical safety requirements ... 34
9.3.4 Contextual safety requirements ... 34
10 Apportionment of functional Safety Integrity requirements ... 35
10.1 Deriving and apportioning system safety requirements ... 35
10.2 Functional safety integrity for electronic systems ... 35
10.2.1 Deriving functional safety requirements for electronic systems ... 35
10.2.2 Apportioning safety requirements ... 35
10.2.3 Safety Integrity Factors ... 38
10.2.4 Functional safety integrity and random failures ... 38
10.2.5 Systematic aspect of functional safety integrity ... 38
10.2.6 Balanced requirements controlling random and systematic failures ... 38
10.2.7 The SIL table ... 39
10.2.8 SIL allocation ... 40
10.2.9 Apportionment of TFFR after SIL allocation ... 40
10.2.10 Demonstration of quantified targets ... 40
10.2.11 Requirements for Basic Integrity ... 41
10.2.12 Prevention of misuse of SILs ... 42
10.3 Safety Integrity for non-electronic systems – Application of CoP ... 42
11 Design and implementation ... 43
11.1 Introduction ... 43
11.2 Causal analysis ... 43
11.3 Hazard identification (refinement) ... 44
11.4 Common cause analysis ... 44
Annex A (informative) ALARP, GAME, MEM ... 46
A.1 ALARP, GAME, MEM as methods to define risk acceptance criteria ... 46
A.2 ALARP (As Low As Reasonably Practicable) ... 47
A.2.1 General ... 47
A.2.2 Tolerability and ALARP ... 48
A.3 Globalement Au Moins Equivalent (GAME) principle ... 48
A.3.1 Principle ... 48
A.3.2 Using GAME ... 49
A.3.2.1 General ... 49
A.3.2.2 Basic principles ... 49
A.3.2.3 Using GAME to construct a qualitative safety argument ... 49
A.3.2.4 GAME using quantitative risk targets ... 49
A.4 Minimum Endogenous Mortality MEM ... 50
Annex B (informative) Using failure and accident statistics to derive a THR ... 52
Annex C (informative) Guidance on SIL Allocation ... 53
Annex D (informative) Safety target apportionment methods ... 55
D.1 Analysis of the system and methods ... 55

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

D.2 Example of qualitative apportionment method 55
D.2.1 General 55
D.2.2 Example of qualitative method for barrier efficiency 56
D.3 Example of quantitative apportionment method 58
D.3.1 Introduction 58
D.3.2 Functions with independent failure detection and negation mechanisms 59
D.3.3 Function and independent barrier acting as failure detection and negation mechanism 61
D.3.4 Apportionment of a probability safety target 62
D.3.5 Apportionment of a “per hour” safety target 62
Annex E (informative) Common mistakes in quantification 64
E.1 Common misuses 64
E.2 Mixing failure rates with probabilities 64
E.3 Using formulas out of their range of applicability 65
Annex F (informative) Techniques / methods for safety analysis 66
Annex G (informative) Key system safety roles and responsibilities 69
Annex ZZ (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC 73
Bibliography 76

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

European foreword

This document (EN 50126-2:2017) has been prepared by CLC/TC 9X "Electrical and electronic applications for railways".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2018-07-03
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2020-07-03

This document supersedes CLC/TR 50126-2:2007.

The former edition of CLC/TR 50126-2:2007 is made obsolete by ⟨A1⟩ the new editions of the EN 50126 series ⟨A1⟩; the reason is that the scope of the present part was modified compared to the superseded edition.

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

EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*" consists of the following parts:

– Part 1: Generic RAMS process;

– Part 2: System approach to safety.

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

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

European foreword to Amendment 1

This document (EN 50126-2:2017/A1:2024) has been prepared by Technical Committee CLC/TC 9X “Electrical and electronic applications for railways”.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2025-11-30
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2027-11-30

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

This document has been prepared under a standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

AVA Documents
Document Sharing Hub

Introduction

EN 50126-1:1999 was aiming at introducing the application of a systematic RAMS management process in the railway sector. Through the application of this standard and the experiences gained over the last years, the need for revision and restructuring became apparent with a need to deliver a systematic and coherent approach to RAMS applicable to all the railway application fields Command, Control and Signalling, Rolling Stock and Fixed Installations.

The revision work improved the coherency and consistency of the standards, the concept of safety management and the practical usage of [A1⟩ the EN 50126 series ⟨A1] and took into consideration the existing and related Technical Reports as well.

This European Standard provides railway duty holders and the railway suppliers, throughout the European Union, with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS.

Processes for the specification and demonstration of RAMS requirements are cornerstones of this standard. This European Standard promotes a common understanding and approach to the management of RAMS.

[A1⟩ The EN 50126 series forms part of ⟨A1] the railway sector specific application of IEC 61508. Meeting the requirements in this European Standard together with the requirements of other suitable standards is sufficient to ensure that additional compliance to IEC 61508 does not need to be demonstrated.

With regard to safety, EN 50126-1 provides a Safety Management Process which is supported by guidance and methods described in EN 50126-2.

[A1⟩ The EN 50126 series is ⟨A1] independent from the technology used. As far as safety is concerned, EN 50126 takes the perspective of safety with a functional approach.

The application of this standard should be adapted to the specific requirements for the system under consideration.

This European Standard can be applied systematically by the railway duty holders and railway suppliers, throughout all phases of the life-cycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The systems-level approach developed by this European Standard facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This European Standard promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAMS and cost for railway applications. Adoption of this European Standard will support the principles of the European Single Market and facilitate European railway inter-operability.

In accordance with CENELEC editing rules [1)], mandatory requirements in this standard are indicated with the modal verb “shall”. Where justifiable, the standard permits process tailoring.

Specific guidance on the application of this standard for Safety aspects is provided in EN 50126-2. EN 50126-2 provides various methods for use in the safety management process. Where a particular method is selected for the system under consideration, the mandatory requirements of this method are by consequence mandatory for the safety management of the system under consideration.

This European Standard consists of the main part (Clause 1 to Clause 11) and Annexes A, B, C, D, E, F, G and ZZ. The requirements defined in the main part of the standard are normative, whilst Annexes are informative.

---

1) CEN/CENELEC Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2017-02), Annex H.

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

1 Scope

[A1] This document [A1]

- considers the safety-related generic aspects of the RAMS life-cycle;
- defines methods and tools which are independent of the actual technology of the systems and subsystems;
- provides:
  - the user of the standard with the understanding of the system approach to safety which is [A1] a key concept of the EN 50126 series [A1];
  - methods to derive the safety requirements and their safety integrity requirements for the system and to apportion them to the subsystems;
  - methods to derive the safety integrity levels (SIL) for the safety-related electronic functions.

  NOTE This standard does not allow the allocation of safety integrity levels to non-electronic functions.
- provides guidance and methods for the following areas:
  - safety process;
  - safety demonstration and acceptance;
  - organisation and independence of roles;
  - risk assessment;
  - specification of safety requirements;
  - apportionment of functional safety requirements;
  - design and implementation.
- provides the user of this standard with the methods to assure safety with respect to the system under consideration and its interactions;
- provides guidance about the definition of the system under consideration, including identification of the interfaces and the interactions of this system with its subsystems or other systems, in order to conduct the risk analysis;
- does not define:
  - RAMS targets, quantities, requirements or solutions for specific railway applications;
  - rules or processes pertaining to the certification of railway products against the requirements of this standard;
  - an approval process by the safety authority.

[A1] This document [A1] is applicable to railway applications fields, namely Command, Control and Signalling, Rolling Stock and Fixed Installations, and specifically:

- to the specification and demonstration of safety for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

combined sub-systems and components within these major systems, including those containing software, in particular:

– to new systems;

– to new systems integrated into existing systems already accepted, but only to the extent and insofar as the new system with the new functionality is being integrated. It is otherwise not applicable to any unmodified aspects of the existing system;

– as far as reasonably practicable, to modifications and extensions of existing systems accepted prior to the creation of this standard, but only to the extent and insofar as existing systems are being modified. It is otherwise not applicable to any unmodified aspect of the existing system;

- at all relevant phases of the life-cycle of an application;
- for use by railway duty holders and the railway suppliers.

It is not required to apply this standard to existing systems which remain unmodified, including those systems already compliant with any former version of EN 50126.

The process defined by this European Standard assumes that railway duty holders and railway suppliers have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within EN ISO 9001.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[A1] EN 50126-1:2017,[1] *Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process* [A1]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in [A1] EN 50126-1:2017 [A1] apply.

4 Abbreviations

ALARP	As Low As Reasonable Practicable
CBA	Cost Benefit Analysis
CCF	Common Cause Failure (Analysis)
CoP	Code of Practice
COTS	Commercial Off-The-Shelf
DRA	Differential Risk Aversion
ERE	Explicit Risk Estimation
EMC	Electromagnetic compatibility
ETA	Event Tree Analysis
FMECA	Failure Mode Effect & Criticality Analysis
FTA	Fault Tree Analysis
GA	Generic Application
GASC	Generic Application Safety Case

[A1] [1] As impacted by EN 50126-1:2017/A1:2024. [A1]

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

GP	Generic Product
GPSC	Generic Product Safety Case
GAME	Globalement Au Moins Equivalent
HAZOP	Hazard and Operability study
IM	Infrastructure Manager
LRU	Line Replaceable Unit
MEM	Minimum Endogenous Mortality
RAC	Risk Acceptance Criterion
RAMS	Reliability, Availability, Maintainability, Safety
RAP	Risk Acceptance Principle
RBD	Reliability Block Diagram
RRA	Rapid Ranking Analysis
RU	Railway Undertaking
SA	Specific Application
SASC	Specific Application Safety Case
SDR	Safe Down Rate
SDT	Safe Down Time
SIL	Safety Integrity Level
SRAC	Safety-Related Application Conditions
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate

5 Safety process

5.1 Risk assessment and hazard control

In this sub-clause, the Hourglass Model is introduced: it offers a simplified approach that, although not containing all aspects implied in the life-cycle model, helps to clarify some issues.

The Hourglass Model provides an overview of the major safety-related activities that are needed to ensure an acceptable safety level for a technical system, including the corresponding responsibility areas.

Technical system means a product or an assembly of products including the design, implementation and support documentation. The development of a technical system starts with its requirements specification and ends with its acceptance. The design of relevant interfaces considering interactions with human operators and their behaviour is considered, while human operators themselves and their actions are not included in a technical system. Both the maintenance process (described in the maintenance manuals) and the operation are specified but are not considered parts of the technical system itself. They can be restricted by “application conditions”.

The purpose of this model is to highlight the separation between risk analysis as part of risk assessment (at the railway system level) from hazard analysis as part of hazard control (at the level of the system under consideration).

This enhances co-operation between the relevant stakeholders, clarifying responsibilities and interfaces and has the advantages of reducing complexity and facilitating modularization.

The Hourglass Model describes two main aspects:

- risk assessment, deriving safety requirements for operational and technical issues (including maintenance), and

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

- hazard control, satisfying given functional safety requirements coming from upper levels by determining and analysing causes and designing and implementing control measures.

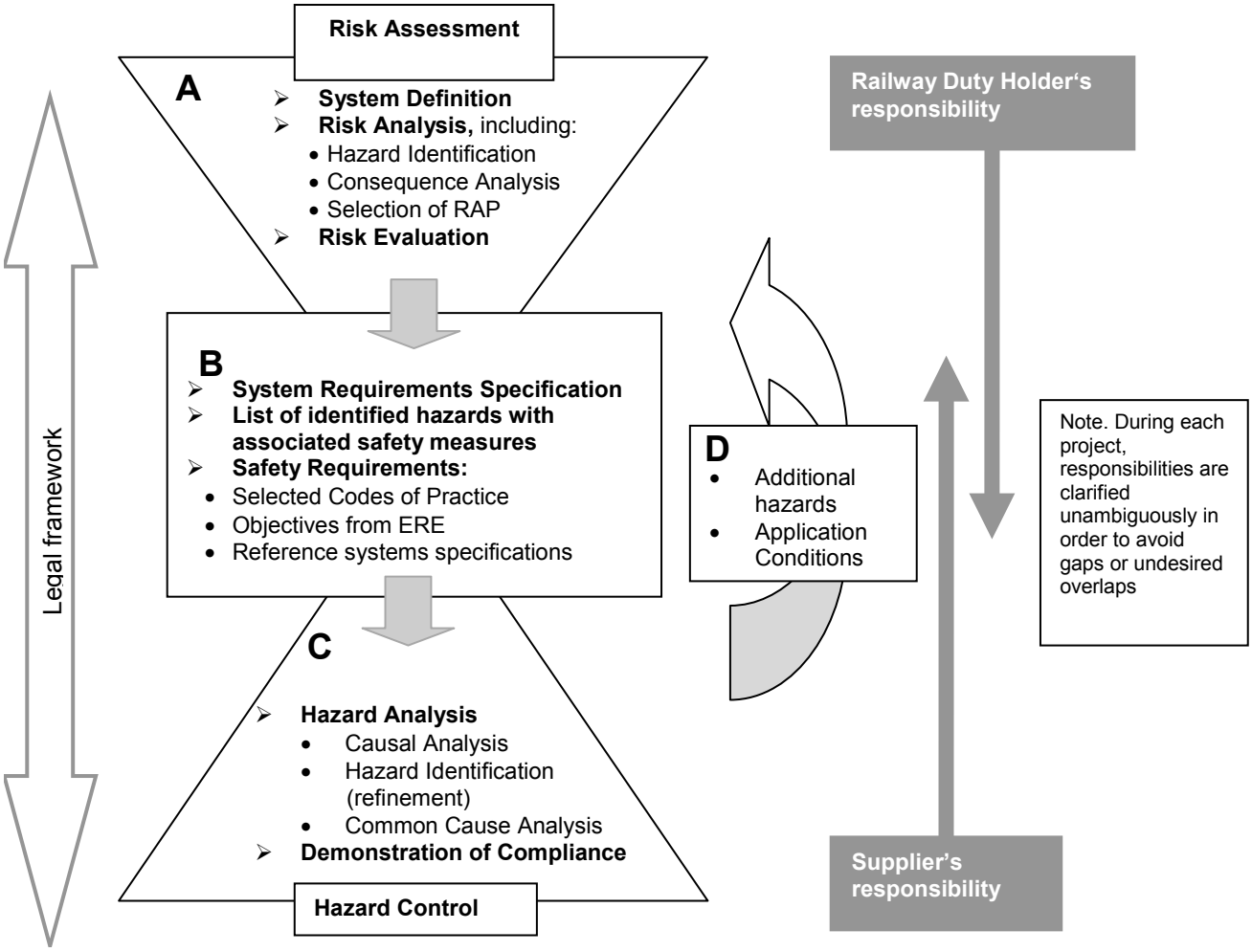

Figure 1 — The Hourglass Model

NOTE Part A (Risk Assessment) is associated with phases 1 to 3 in the life-cycle as depicted in Figure 4 in EN 50126-1:2017. Part B corresponds to phase 4 and part C to phases 5 to 9. Part D shows the "feedback of subsequent hazard identification into risk analysis" (see Figure 4 in EN 50126-1:2017).

5.2 A. Risk assessment

5.2.1 General

Risk assessment is performed at the railway system level.

It relies on a System Definition and includes Risk analysis and Risk evaluation.

It defines the high level system safety requirements, in particular safety requirements for the system under consideration from the perspective of the railway duty holder and the operator. It takes into account safety-related operational aspects, previous experience and the regulatory requirements for the railway application.

The main task for this activity is the risk analysis, which is derived from the system definition. The risk analysis includes hazard identification, consequence analysis, and selection of Risk Acceptance Principle (RAP).

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

The specification of safety requirements is the final result of risk assessment; in Figure 1 it is allocated to box B, because it constitutes an interface (together with system requirement specifications and the list of identified hazards) between different responsibilities.

5.2.2 Conducting risk assessment

The level of detail in a risk assessment should be adequate to enable the risk to be properly considered. The purpose is not to catalogue every trivial hazard, nor is it expected that hazards beyond the limits of current knowledge will always be identified. A risk assessment should reflect a reasonable analysis of hazards and their associated risks within the railway operation and within the applied technology itself. Where considered to be worthwhile, risk assessments should be correlated with historical records of accidents and the records of causes.

When possible, consideration of technical implementation/architecture should be avoided in this first stage, i.e. the system to be developed should be considered as a black box, of which functions and hazards are evaluated only at the boundaries. These boundaries are well defined interfaces between the operational environment and the system under consideration.

As an example, an “unintentional train motion” is a hazard for a train. It can be observed as an abstraction at the boundary of the “system train” and it could lead to different accidents depending on the operational context (e.g. collision in context with over-speeding while running or fall of persons in connection with a train moving in a station while expected to stand still, etc.).

Assumptions defined during the risk assessment shall be checked and updated throughout the life-cycle phases.

5.3 B. Outcome of the risk assessment

The results of the risk assessment are a set of safety requirements associated to clearly-identified functions, systems or operating rules. They are part of the System Requirement Specification which establishes the technical interface between the stakeholders.

NOTE The project organisational structure and responsibilities are other factors to consider in understanding and controlling risk. For organisational aspects and requirements it is advised to refer to Clause 7.

On the basis of the selected risk acceptance principles, safety requirements can refer to Codes of Practice, to Reference Systems, or give explicit targets derived from an Explicit Risk Estimation (ERE).

Safety requirements include required safety functions, which could be assessed quantitatively (e.g. maximum rates of hazards), semi-quantitatively or qualitatively (e.g. use of trained drivers for controlling human errors).

Safety requirements should be assessed with an holistic approach to the system under consideration, i.e. the residual risk of the whole system after introducing safety requirements should be assessed taking into consideration all identified hazards.

5.4 C. Hazard control

The hazard control stage in the hourglass model ensures that the system under consideration is compliant with the safety requirements. Hazard control is performed for a specific system architecture.

The major impacts of human factors, operational and general maintenance rules as well as procedures are part of the preceding risk analysis and should have already been taken into account in the safety requirements. Therefore, during hazard control, the designer of the system under consideration can focus on the internal causes of the identified hazards.

The main task is the “hazard analysis” comprising:

– a dedicated hazard identification focusing on the system under consideration (refinement);

– causal analysis;

– a Common Cause Analysis (see 11.4 for details).

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

Hazard identification is a recurring task, iterating on several levels during development of the system under consideration. In order to distinguish between different tasks (and related documents) the hazard identification has been quoted twice in Figure 1:

1. during risk assessment, hazard identification focuses on high level hazards derived from the system functions (black box) and related operation of the system as well as its environment;

2. within the hazard control, a refined/iterated hazard identification focuses on hazards and their causes derived from the technical solutions, i.e. from defined architecture and internal interfaces of the system under consideration, and potential new hazards introduced by the system itself.

Both kinds of identified hazards shall be addressed during hazard control. Figure 2 shows the general case where the cause of a hazard at the railway system level consists of a hazard on the level of the system under consideration, with respect to its boundary. The boundary for a hazard identification is always given in the system definition that limits the scope of the task. This implies that the hazards are structured hierarchically. Hence a hierarchical approach to hazard analysis and hazard logging should be used.

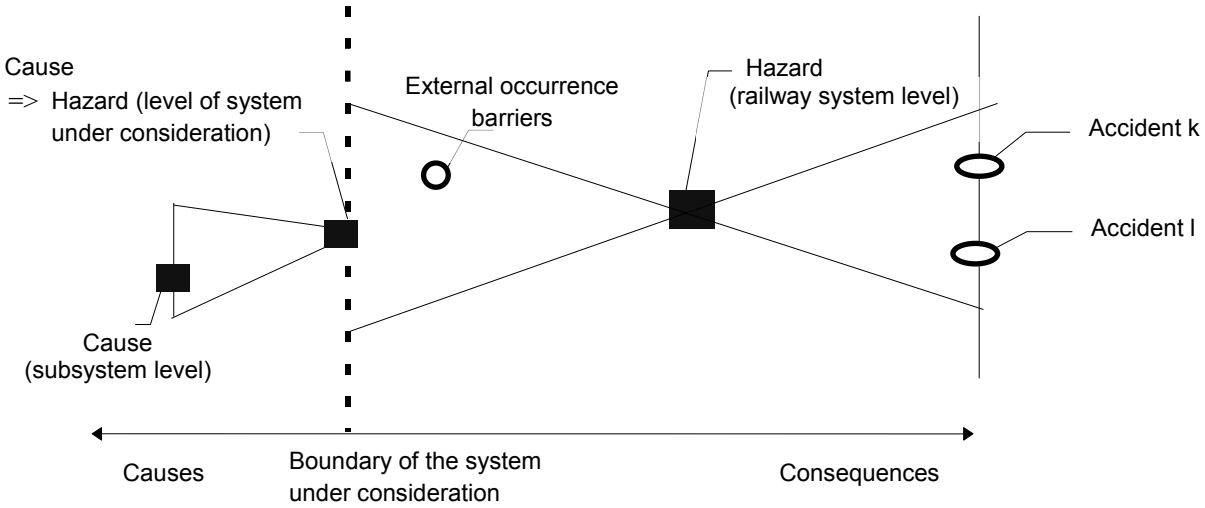

Figure 2 — Illustration of hazards with respect to the system boundary

The picture is hazard-oriented and shows a “bow-tie” shape, suggesting that several causes could lead to the same hazard and one hazard could lead to several different accidents.

Example The hazard at railway system level is a train passing a signal at danger and entering another train’s route, potentially leading to a collision (the accident). The cause at railway system level (the hazard at the level of system under consideration) is a too long braking distance. The cause at the sub-system level is that the brakes were not applied by the Driver (or applied too late). The external occurrence barrier is provided by safety equipment ordering an emergency brake.

The demonstration of compliance with the safety requirements for the system under consideration can be performed in various forms of verification. These forms depend on the nature of the underlying requirements set at the beginning of the hazard control.

5.5 D. Revision of risk assessment

During the hazard control stage, fulfilment of safety requirements might not be reached in the first iteration. Three potential causes are:

– additional hazards are identified at the level of the system under consideration;

– a need for new operational rules arises;

– additional external safety measures are required to fulfil the safety targets.

In all these cases, a revision of the risk assessment is necessary.

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

This revision should also take into account the application conditions that could arise at the level of the system under consideration.

5.6 Responsibilities

Risk assessment is mainly within the responsibility of the railway duty holders and operators. If no risk assessment is provided by the railway duty holder or operator, the roles and responsibilities may be contracted to other parties (manufacturers and suppliers), provided that they have a documented and suitable range of competencies to consider the whole operational context in detail. They shall assess the risk resulting from introducing changes to the operational context, taking into account safety-related operational aspects, previous experience and regulatory requirements. In any case the railway duty holders should accept the results of the risk assessment.

The supplier of the technical system is responsible for the hazard control. In the case that several suppliers are in charge for different systems under consideration, the railway duty holder shall be responsible for organising an overall hazard control.

Railway duty holder and supplier shall conform to the prevailing legal requirements.

6 Safety demonstration and acceptance

6.1 Introduction

This clause provides additional details on safety demonstration and safety acceptance processes for the system under consideration. Except where considered appropriate, it does not specify who should carry out the work at each stage, since this may vary in different circumstances.

Safety demonstration evidence is based on the safety case. The purpose and content of the safety case are defined in EN 50126-1:2017, Clause 8.

In terms of safety processes, the development of a system can be categorised in three types:

- Generic Product: The system is considered from a generic point of view, applicable to different classes of applications;

  Analyses are carried out within an operational context which is application-independent.

- Generic Application: The system is considered suitable for multiple applications of the same class;

  Analyses are carried out within an operational context which is application-dependent. The safety process includes the definition of the application design process.

- Specific application: The system is considered for a specific application (including its physical implementation).

6.2 Safety demonstration and safety acceptance process

Three different categories of safety case can be defined according to the involved type of development as previously defined:

- Generic Product;
- Generic Application;
- Specific Application.

In all three categories the structure of the safety case is basically the same.

The Specific Application Safety Case shall address the following two aspects:

- the Application Design;

Documents
Document Sharing Hub

- the Physical implementation, including manufacturing, installation, and the facilities for operation and maintenance.

If separate safety acceptance is needed for the application design and for its physical implementation, it might be possible to divide the safety case for specific applications into two portions:

- the Application Design safety case;
- the Physical implementation safety case.

The safety case, as defined in EN 50126-1:2017, Clause 8, includes:

– Part 1: Definition of the system;

– Part 2: Quality Management Report;

– Part 3: Safety Management Report;

– Part 4: Technical Safety Report;

– Part 5: Related safety cases (if applicable);

– Part 6: Conclusion.

Whenever independent safety assessment is required for the system under consideration, this is performed before system acceptance, in order to provide additional assurance that the necessary level of safety has been achieved.

In this case, independent safety assessment shall take into consideration the safety case related to the system under consideration and shall be performed in accordance with requirements defined in EN 50126-1:2017, 6.8 and in accordance with the independence of role defined in EN 50126-2:2017, 7.3.

System acceptance of the system under consideration as adequately safe for its intended application, shall be based on the following conditions:

- it has been developed, verified and validated in accordance with EN 50126 series;
- the specified safety requirements have been fulfilled in accordance with EN 50126 series.

The overall documentary evidence for system acceptance should consist of:

- the system definition and operational context;
- the system requirements and characteristics, including the safety requirements (and related risk analysis whenever applicable);
- the safety case;
- the Independent Safety Assessment Report, when required. This report explains the activities carried out to determine whether the system under consideration has been designed to meet its specified safety requirements, and if necessary specify some additional conditions for its operation.

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 when required, the system under consideration may be granted safety acceptance by the stakeholders responsible for its incorporation into another system or final use.

When using a Generic Product (i.e. independent of application), or a Generic Application (i.e. class of application) in the context of a Specific Application, it should be possible for safety acceptance to be based on existing related independent safety assessment. This is not considered possible for Specific Applications.

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024

When a safety case for Generic Product (i.e. independent of application), or a Generic Application (i.e. class of application) is developed, a validation activity for the system under consideration usually performed in phase 9 “system validation” of the system life-cycle, shall be also performed at the end of life-cycle phase 6 “design and implementation” considering also the manufacturing of the first item.

An example of safety acceptance process, for all three categories of Safety Case, is illustrated in Figure 3, where for the Specific Application it is considered the case of reference to Generic Products / Generic Application and Specific Application stand-alone.

According to tailoring requirements defined in ▌A1⟩ EN 50126-1:2017 ⟨A1▌, the stakeholder responsible for a given safety process shall provide evidence and justification of the coverage and limits of the covered life-cycle phases.

AVA Documents
Document Sharing Hub

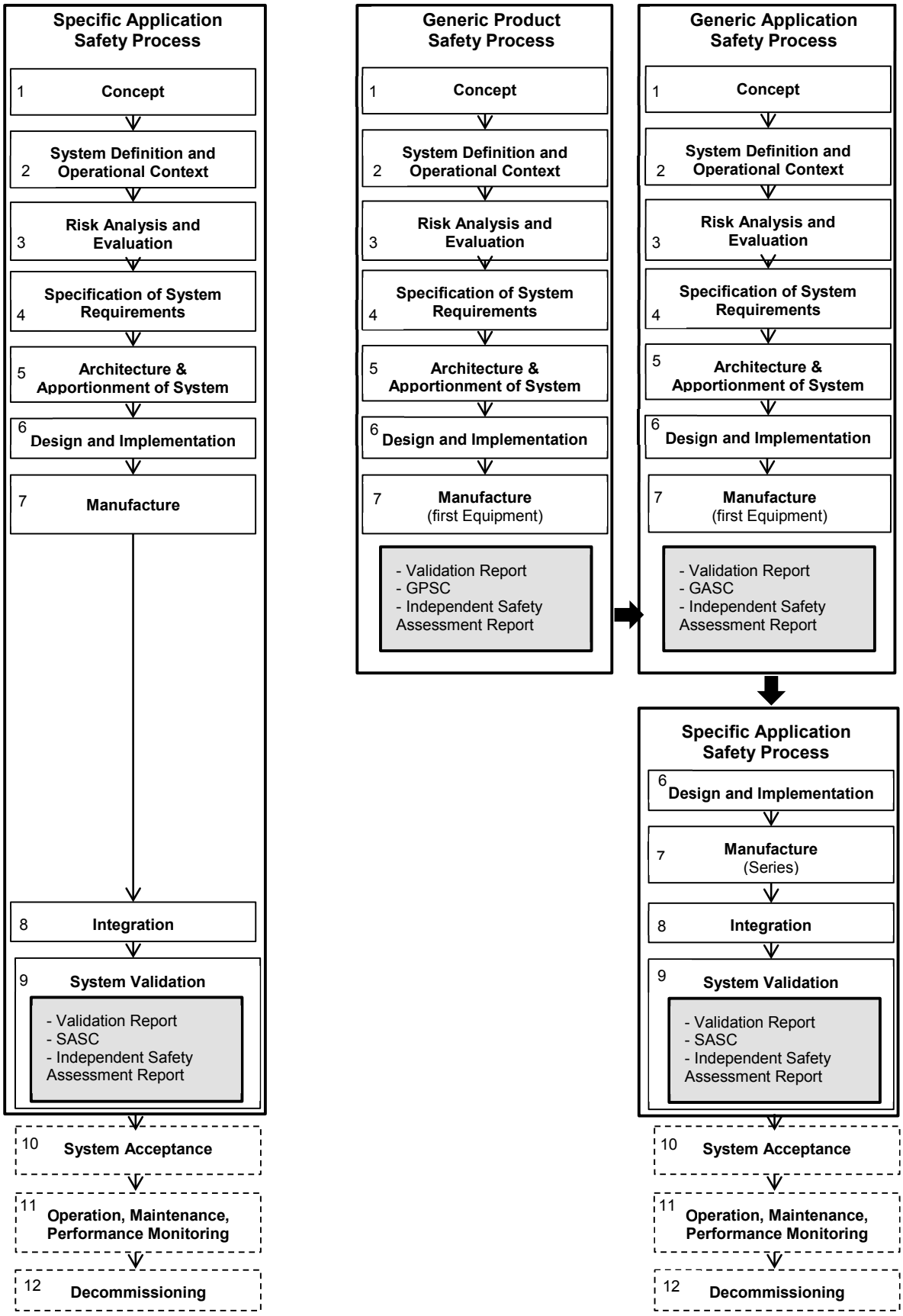

Figure 3 — Example of safety acceptance processes

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

6.3 Responsibility in managing the Safety Case

Responsibility for managing the safety case depends on the defined relationship between stakeholders and it is subjected to contractual agreements. Typically:

- The Generic Product Safety Case is the evidence written by the supplier for the party responsible for configuring it for use (e.g. a supplier or contracting entity).
- The Generic Application Safety Case is the evidence written by the party responsible for generic configuration of the product (e.g. the product supplier) for the party responsible for specific configuration (e.g. the supplier, a contracting entity, or RU/IM project delivery organisation).
- The Specific Application Safety Case is the evidence written by the party configuring the system for specific use (e.g. the supplier or a contracting entity or RU/IM project delivery organisation) for the party responsible for the operational railway (e.g. the RU or IM).

As the work progresses from generic to specific arrangements, the safety argument evolves and builds upon each previous safety case, and the ultimate specific application safety case therefore comprises evidence from all related safety cases. Safety-Related Application Conditions are developed at each stage and taken forward by the next actor. By definition, the safety case for a specific application, and the safety-related application conditions it defines, once accepted by the RU or IM, become an extension of the safety management system of the RU or IM. At that level, all the SRACs are evaluated to have been met.

6.4 Modifications after safety acceptance

After a system/sub-system/component has received safety acceptance, 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 should be subject to the acceptance processes in the duty holder's safety management system and the approval processes required by the particular legal framework.

Once an installed system/sub-system/component has been validated and accepted, appropriate procedures, support systems and safety monitoring, as defined in the Safety Plan, are used to ensure continued safe operation throughout its working life, including operation, maintenance, alteration, extension and eventual decommissioning. These activities are controlled using quality management, safety management and technical safety criteria at least as safe as for the original design. The on-going safety of the system is managed by the duty holder and this should require the relevant documentation, including the Safety Case, to be kept up-to-date.

6.5 Dependencies between Safety Cases

The safety case for a system could depend on the safety cases of other sub-systems or equipment. In such circumstances, safety acceptance of the main system is not possible without previous safety acceptance of the related sub-systems/equipment.

Relationship among safety cases shall be associated to a corresponding system decomposition established during life-cycle phase 2 “system definition and operational context”.

The different types of Safety Case may be defined according to reuse needs.

If independent safety assessment report has been obtained for a generic product, or for a generic application, a reference may be made to this for safety acceptance of a specific application; it is not needed to repeat the generic independent safety assessment process for each specific application. This dependency between Safety Cases is illustrated with examples in Figure 4.

A safety case may be based on demonstration that the proposed specific application is technically equivalent to an existing application with specific safety acceptance. A new safety acceptance for this specific application is necessary.

It is essential to ensure that the Safety-Related Application Conditions (SRACs) 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 SRACs of the higher-level Safety Case.

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

EXAMPLE 1 Left-side of Figure 4 shows an example, where a whole ERTMS system for specific line #1 is addressed in a Specific Application Safety Case, embracing also a railway interlocking system (IXL system #3) and an ATC System #2. No other Safety Cases are reused or referenced. This means that the two subsystems (interlocking and ATC) are being developed within this application and do not rely on previous acceptance.

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

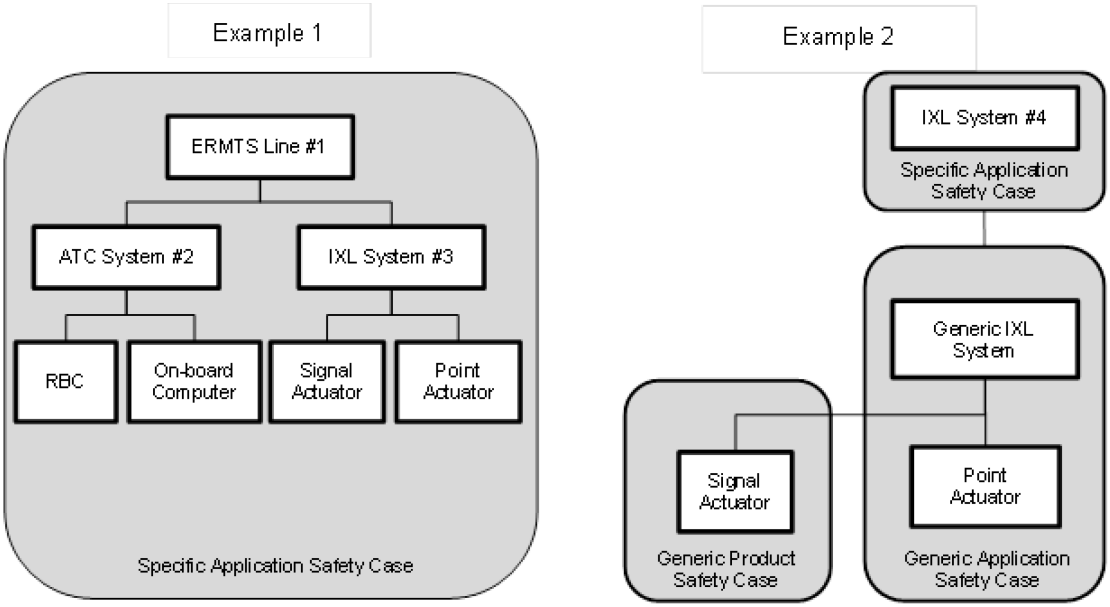

Figure 4 — Examples of dependencies between safety cases

6.6 Relationship between safety cases and system architecture

It is not necessary for the number, scope and hierarchy of the various safety cases (GPSC, GASC, SASC) to reflect the architectural view of the system under development, i.e. “generic product” (GP), “generic application” (GA) and “specific application” (SA). The safety case architecture should not be confused with “system”, “sub-system” and “component” architectural view.

Although a GP is often a component in a GA or SA, those terms could even refer to the same item, just with different perspectives.

EXAMPLE A component implementing a safety-related communication over a transmission system, to exchange the status of a field equipment:

a) It can be considered as a GP, and validated / approved with reference to EN 50159, if its scope is the mitigation of generic threats to messages (deletion, corruption, re-sequencing, etc.), regardless of their content. A number of safety-related parameters will be defined as configurable (e.g., transmission cycle, length of time-outs, number of replies);

b) It can be considered as a GA, and validated / approved with reference to a set of applications requirements. Type of field equipment, its dynamics and how the status information is used will define all the safety-related parameters configurable at the GP level;

c) It can be considered as a SA for a specific site, and validated for its specific use, within the parameters’ ranges defined as application conditions in the GA.

These steps might be grouped according to the needs of re-use, e.g. step a) might be useful if the system is intended to be used for completly different applications, otherwise the related safety analyses could be integrated in b). Similarly, step b) is advisable if the system will be replicated on different physical installations.

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

7 Organisation and Independence of Roles

7.1 General

Organisation and related roles and responsibilities are key factors for reduction of systematic failures to be considered over the entire life-cycle of the system under consideration. Clause 7, with related information in Annex F for the different phases of the lifecycle, provides specific requirements to be adopted in the different phases of the life-cycle.

Persons responsible for a project may cover other roles in other projects; provided this is compliant with defined independence requirements (e.g. the same person allocated as designer in project A may be allocated as verifier in project B).

Since “Early phases” of the lifecycle (from Concept phase to Specification of System Requirements phase) can be contractually under responsibility of stakeholders different from those of the later phases of the lifecycle, Clause 7 differentiates the related requirements.

This means that in 7.2 and 7.3, the roles defined for the design and development of “later phases” may be different from the roles defined for the “early phases” (e.g. when the project is transferred from the railway duty holder to the railway supplier or from the railway supplier to a different railway supplier).

Also the Independent safety assessor involved in “early phases” may be different from the one involved in the ”later phases”.

As a minimum, each organisation shall implement a process, for the organisation and management of personnel and responsibilities, equivalent to those set out in EN ISO 9001. This clause gives additional requirements as far as safety is concerned.

If an Independent safety assessor is required, they shall be appointed and be given authority to perform the independent safety assessment of the system under consideration.

The Independent safety assessor shall always be independent from the Project manager and shall be a different entity to those undertaking other roles in the project.

Other regulatory requirements could also call for safety assessment to be performed independently. Although such a role could be defined with a different purpose, the work should be combined in a way to serve both purposes and to avoid duplication of work.

7.2 Early phases of the lifecycle (phases 1 to 4)

In the early phases of the life-cycle (from the “concept” life-cycle phase to the “Specification of System Requirements” life-cycle phase), the emphasis is on the prevention of the systematic failures only. This can be met by detecting such failures using control measures and subsequent correction. One of the main instruments is the verification of the results at the end of each life-cycle phase. The verification shall be performed by an entity which has not been involved with other roles in the elaboration of those results.

The system requirements, including the safety requirements, shall be validated by a competent entity who has not been involved in the development of the requirements. The Validator shall state whether the requirements are adequately analysed and specified in order to allow the system under consideration to serve the intended use or application.

The Validator shall be independent from the Project Manager.

The Validator may be selected from the same entity as the Verifier, but still maintaining independence from the Project manager (this option is not shown in Figure 5). If the Verifier and the Validator are the same person, the verification and validation outputs shall be reviewed by another competent person with the same level of independence as the Validator.

NOTE The Validator needs sufficient autonomy and responsibility to reach an independent judgement of the completeness and adequacy of the safety requirements.

Independence requirements for early phases are illustrated in Figure 5.

Documents
Document Sharing Hub

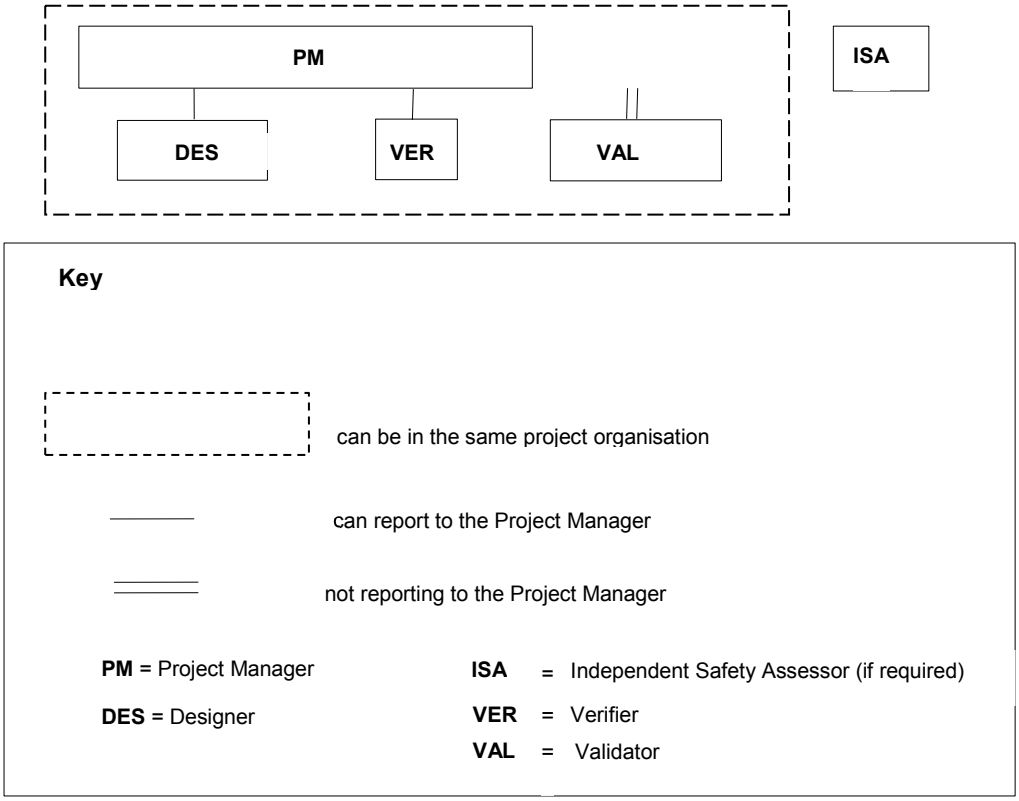

Figure 5 — Independence of Roles in the early phases (phases 1 to 4) of the lifecycle

7.3 Later phases of the lifecycle (starting from phase 5)

For these phases of the lifecycle, Verifier shall be competent for this role and shall not be involved in other activities in the same life-cycle phase, and Validator shall be qualified for this role and shall not have been involved in the design, in any earlier phases of the project, including specification of system requirements, system architecture and system design implementation.

Nevertheless, Verifier and/or Validator might identify missing safety requirements, and in that respect contribute to the requirements specification. In this case, these requirements shall be reviewed by a peer.

Two alternative arrangements apply, depending on the results of the Risk Assessment performed in phase 3 of the lifecycle (they depend on the higher/lower severity of the consequences or alternatively higher/lower Safety Integrity Levels as defined in Clause 10):

- Case (A): same independence structure as per “Early phases”. This arrangement is the most constraining and is always allowed;

- Case (B): reduced independence structure. This arrangement is allowed under the condition that results of the risk analysis have shown no credible direct potential for at least one fatality, or when applicable, that the apportioned Safety Integrity Level is lower or equal to SIL 2.”

In Case (A): the Validator may be selected from the same entity as the Verifier, but shall maintain independence from the Project manager (this option is not shown in Figure 5). If the Verifier and the Validator are the same person, the verification and validation outputs shall be reviewed by another competent person with the same level of independence as the Validator.

In Case (B): the Validator and the Verifier may be selected from the same entity and they may both be under the direct control of the Project manager.

The Independent Safety Assessor may be part of any stakeholder organisation (e.g. supplier, infrastructure manager, railway undertaking). The Independent Safety Assessor shall always be independent from the

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

Project Manager and shall be a different entity to those undertaking other roles in the project. The legal framework can ask for additional independence requirements.

The Safety Plan shall define how the roles defined in this standard are covered by the project organisation, and who is assigned to the roles. These roles and the assigned personel should ideally remain unchanged throughout the development project.

Independence requirements for later phases are illustrated in Figure 6.

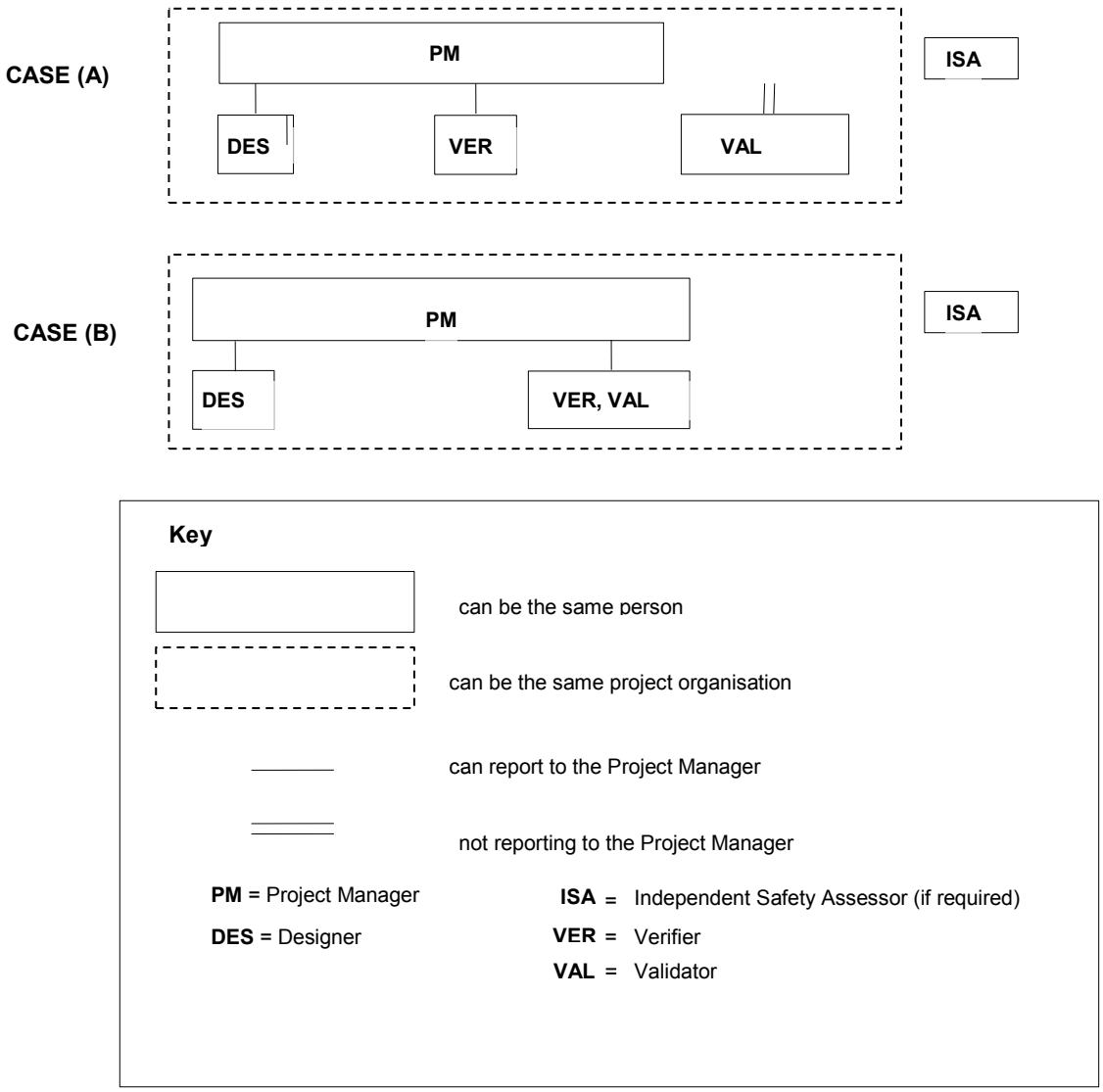

Figure 6 — Independence of Roles in later phases of the lifecycle (starting from phase 5)

7.4 Personnel Competence

For all the phases of the life-cycle, the key competencies required for each role in the development of the system under consideration should be compliant with the indications given in Annex G. The experience, capabilities and qualifications required for a role in specific phases of the life cycle, should be defined in the quality management system.

Documented evidence of personnel competence, including technical knowledge, qualifications, relevant experience and appropriate training, should be maintained by the responsible organisation in order to demonstrate appropriate safety organisation.

Documents
Document Sharing Hub
Full document details: BS EN 50126-2:2017+A1:2024

The organisation should maintain procedures to manage the competence of personnel to suit appropriate roles in accordance with existing quality standards.

Once the competence has been demonstrated for all personnel responsible for the roles described in 7.2 and 7.3, those individuals should show continuous maintenance and development of competence. This could be demonstrated by a logbook documenting the activity and the additional training (as an example see provisions on competence, training and awareness in EN ISO 9001).

8 Risk assessment

8.1 Introduction

The core part of the Risk assessment (i.e. analysis and evaluation) is performed at phase 3 of the life-cycle and continued as appropriate through the system life-cycle. This clause describes:

- Sub-clause 8.2: Risk analysis with identification of the hazards and their consequences;
- Sub-clause 8.3: Selection of risk acceptance principles, related acceptance criteria and risk evaluation. Risk acceptance principles are;
  - o Use of Code of Practice;
  - o Use of a reference system;
  - o Use of Explicit Risk Estimation.
- Sub-clause 8.4: Application of explicit risk estimation

The risk assessment process can be described as several tasks such as Risk Analysis, Hazard Identification, Consequence Analysis, Risk Evaluation, Selection of Risk Acceptance Principles.

8.2 Risk Analysis

8.2.1 General

Initially, the analysis is performed qualitatively, identifying all contributing factors and their combination without quantification.

The risk analysis process is an iterative process. It shall start with the definition of the system under consideration. Then the hazards, the risks, the associated safety measures, and the resulting safety requirements for the system under consideration shall be identified.

Consequence analysis, see 8.2.3, involves gathering and documenting data that describe the effects of a hazard. The recommended approach is to use accident data, wherever available, and/or to consult experts on the environment related to the system or process under consideration (i.e. “domain experts”).

8.2.2 The risk model

Where needed to support hazard identification, hazard classification and the selected risk acceptance principles a risk model should be defined. Causes, hazards and accidents stand in a many-to-many relationship, such as:

- a single cause can trigger (or contribute to) several different hazards;
- a hazard can be triggered by several different causes;
- a hazard can result in different types of accidents under different operational and environmental contexts;
- an accident can have different consequences under different operational and environmental contexts.

An example of risk model is provided in Figure 7 and shows:

Documents
Document Sharing Hub

Full document details: BS EN 50126-2:2017+A1:2024