



DPC: 24 / 30465361 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 29 January 2024

Origin: International

Latest date for receipt of comments: 20 March 2024

Project No. 2022/02624

Responsible committee: GEL/9 Railway Electrotechnical Applications

Interested committees:

Title: BS IEC 62278-2 Railway applications - Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Part 2: Systems approach to safety

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 20 March 2024**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Ms Bash Berry (BSI)**Direct tel: **0203 142 5620**E-mail: **bash.berry@rssb.co.uk**

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:

IEC 62278-2 ED1

DATE OF CIRCULATION:

2024-01-26

CLOSING DATE FOR VOTING:

2024-04-19

SUPERSEDES DOCUMENTS:

9/2904/CD, 9/2931A/CC

IEC TC 9 : ELECTRICAL EQUIPMENT AND SYSTEMS FOR RAILWAYS

SECRETARIAT:

France

SECRETARY:

Mr Denis MIGLIANICO

OF INTEREST TO THE FOLLOWING COMMITTEES:

PROPOSED HORIZONTAL STANDARD:



Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC☐ ENVIRONMENT☐ QUALITY ASSURANCE☒ SAFETY☐ SUBMITTED FOR CENELEC PARALLEL VOTING☒ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (See [AC/22/2007](#) or [NEW GUIDANCE DOC](#)).

TITLE:

Railway Applications – Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems approach to safety

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

Copyright © 2024 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

Contents

Page

FOREWORD	6
INTRODUCTION	8
1 Scope	9
2 Normative references	10
3 Terms and definitions	10
4 Abbreviations	10
5 Safety process	11
5.1 Hourglass model for risk assessment and hazard control	11
Figure 1 — The Hourglass Model	12
5.2 A. Risk assessment	12
5.2.1 General	12
5.2.2 Conducting risk assessment	13
5.3 B. Outcome of the risk assessment	13
5.4 C. Hazard control	13
Figure 2 — Illustration of hazards with respect to the system boundary	14
5.5 D. Revision of risk assessment	14
5.6 Responsibilities	15
6 Safety demonstration and acceptance	15
6.1 Introduction	15
6.2 Safety demonstration and safety acceptance process	15
Figure 3 — Example of safety acceptance processes	18
6.3 Responsibility in managing the Safety Case	19
6.4 Modifications after safety acceptance	19
6.5 Dependencies between Safety Cases	19
Figure 4 — Examples of dependencies between safety cases	20
6.6 Relationship between safety cases and system architecture	20
7 Organisation and Independence of Roles	21
7.1 General	21
7.2 Early phases of the lifecycle (phases 1 to 4)	21
Figure 5 — Independence of Roles in the early phases (phases 1 to 4) of the lifecycle	22
7.3 Later phases of the lifecycle (starting from phase 5)	22
Figure 6 — Independence of Roles in later phases of the lifecycle (starting from phase 5)	23
7.4 Personnel Competence	23
8 Risk assessment	24
8.1 Introduction	24
8.2 Risk Analysis	24
8.2.1 General	24
8.2.2 The risk model	24
Figure 7 — An example of risk model	25
Table 1 — Examples of hazards	26
8.2.3 Techniques for the consequence analysis	27
8.2.4 Expert Judgement	27

8.3	Risk acceptance principles and risk evaluation	28
8.3.1	Use of Code of Practice.....	28
8.3.2	Use of a reference system.....	28
8.3.3	Use of Explicit Risk Estimation	29
8.4	Application of explicit risk estimation	30
8.4.1	Quantitative approach	30
Figure 8	— Tolerable rates in an example of risk model	31
8.4.2	Variability using quantitative risk estimates	33
8.4.3	Qualitative and semi-quantitative approaches	34
9	Specification of System Safety Requirements	34
9.1	General	34
9.2	Safety requirements	35
9.3	Categorization of Safety Requirements.....	35
9.3.1	General.....	35
Figure 9	— requirements classification	36
9.3.2	Functional safety requirements	36
9.3.3	Technical safety requirements	37
9.3.4	Contextual safety requirements	37
10	Apportionment of functional Safety Integrity requirements.....	38
10.1	Introduction	38
10.2	Functional safety integrity for electronic systems	38
10.2.1	General.....	38
10.2.2	Apportioning safety requirements.....	38
Figure 10	— Apportionment of functional safety requirements	39
10.2.3	Safety Integrity Factors	41
10.2.4	Functional safety integrity and random failures	41
10.2.5	Systematic aspect of functional safety integrity	41
10.2.6	Balanced requirements controlling random and systematic failures.....	41
Figure 11	— Categorisation of Safety Integrity measures	42
10.2.7	The SIL table	42
Table 2	— SIL quantitative and qualitative measures	43
10.2.8	SIL allocation	43
10.2.9	Apportionment of TFFR after SIL allocation.....	43
10.2.10	Demonstration of quantified targets	43
10.2.11	Requirements for Basic Integrity	44
10.2.12	Prevention of misuse of SILs	45
10.3	Safety Integrity for non-electronic systems – Application of CoP	45
11	Design and implementation	46
11.1	Introduction	46
11.2	Causal analysis	46
11.3	Hazard identification (refinement).....	47
11.4	Common cause analysis	47
Figure 12	— Common Cause Failures (CCF)	48
Figure 13	— Impact of functional dependence in a fault-tree analysis.....	48
Annex A (informative)	ALARP, GAME, MEM	49
A.1	ALARP, GAME, MEM as methods to define risk acceptance criteria	49
Table A.1	— Overview of ALARP, GAME, MEM	49

A.2 ALARP (As Low As Reasonably Practicable)	50
A.2.1 General	50
A.2.2 Tolerability and ALARP	51
A.3 Globalement Au Moins Equivalent (GAME) principle	51
A.3.1 Principle	51
A.3.2 Using GAME	52
A.3.2.1 General	52
A.3.2.2 Basic principles	52
A.3.2.3 Using GAME to construct a qualitative safety argument	52
A.3.2.4 GAME using quantitative risk targets	52
A.4 Minimum Endogenous Mortality MEM	53
Figure A.1 — Differential risk aversion.....	53
Annex B (informative) Using failure and accident statistics to derive a THR.....	55
Annex C (informative) Guidance on SIL Allocation	56
Annex D (informative) Safety target apportionment methods	58
D.1 Analysis of the system and methods.....	58
D.2 Example of qualitative apportionment method.....	58
D.2.1 General	58
Figure D.1 — Example of qualitative apportionment method.....	59
D.2.2 Example of qualitative/semi-quantitative method for barrier efficiency	59
Table D.1 — Efficiency based on the component's failures.....	60
Table D.2 — Efficiency based on the component's knowledge.....	60
Table D.3 — Efficiency based on the use of the component	60
Table D.4 — Efficiency based on the maintenance of the component	61
D.3 Example of quantitative apportionment method.....	61
D.3.1 Introduction	61
Figure D.2 — Interpretation of failure and repair times	62
D.3.2 Functions with independent failure detection and negation mechanisms.....	62
Figure D.3 — Combination of two functions with independent failure detection and negation mechanism	63
Figure D.4 — Allocation of Safety Integrity requirements.....	64
D.3.3 Function and independent barrier acting as failure detection and negation mechanism	64
Figure D.5 — Combination of Function and independent barrier acting as failure detection and negation mechanism	65
D.3.4 Apportionment of a probability safety target.....	65
D.3.5 Apportionment of a “per hour” safety target	66
Figure D.6 — Example of quantified apportionment.....	66
Annex E (informative) Common mistakes in quantification.....	67
E.1 General	67
E.2 Mixing failure rates with probabilities	67
Figure E.1	67
E.3 Using formulas out of their range of applicability	68
Annex F (informative) Techniques / methods for safety analysis.....	69

Table F.1 — Techniques / Methods for safety analysis.....	69
Table F.2 — Techniques / Methods for BI and SILs.....	70
Annex G (informative) Key system safety roles and responsibilities	71
Table G.1 — Role specification for Designer.....	71
Table G.2 — Role specification for Verifier	72
Table G.3 — Role specification for Validator.....	72
Table G.4 — Role specification for Independent Safety Assessor.....	73
Table G.5 — Role specification for Project Manager	74
Bibliography.....	75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY AND SAFETY (RAMS) PART 2: Systems Approach to Safety

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62278-2 has been prepared by IEC technical committee 9: Electric railway equipment.

It was submitted to the National Committees for voting under the Fast Track Procedure as the following documents:

FDIS	Report on voting
9/xxx/FDIS	9/xxx/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This document is based on EN 50126-2:2017.

The revision work improved the coherency and consistency of the standard, the concept of safety management and the practical usage of IEC 62278. IEC 62278 series is derived from the European Standard series EN 50126:2017, consisting of EN 50126-1:2017 and EN 50126-2:2017.

The IEC 62278 series forms part of the railway sector specific application of IEC 61508. IEC 62278, IEC 62279 and IEC 62425 comprise the railway sector equivalent of the IEC 61508 series so far as railway communication, signalling and processing systems are concerned. When compliance with these documents has been demonstrated, further evaluation of compliance with the IEC 61508 series is not required.

With regard to safety, IEC 62278-1 provides a Safety Management Process which is supported by guidance and methods described in IEC 62278-2.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under “<http://webstore.iec.ch>” in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

IEC 62278:2002 was aimed at introducing the application of a systematic RAMS management process in the railway sector. Through the application of this document 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 (Signalling), Rolling Stock and Electric power supply for Railways (Fixed Installations).

This document provides railway duty holders and the railway suppliers 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 document. This international Standard promotes a common understanding and approach to the management of RAMS.

IEC 62278-1 and IEC 62278-2 are independent from the technology used. As far as safety is concerned, IEC 62278 takes the perspective of safety with a functional approach.

The application of this document can be adapted to the specific requirements for the system under consideration.

This document 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 system level approach developed by this document facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This document promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAMS and cost for railway applications.

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

1 Scope

This part 2 of IEC 62278

- 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 document with:
 - the understanding of the system approach to safety which is a key concept of IEC 62278;
 - 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 document 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 document 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 document;
 - an approval process by the safety authority.

This part 2 of IEC 62278 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 combined subsystems and components within these major systems, including those containing software, in particular:

- 63 – to new systems;
- 64 – to new systems integrated into existing systems already accepted, but only to the extent and
65 insofar as the new system with the new functionality is being integrated. It is otherwise not
66 applicable to any unmodified aspects of the existing system;
- 67 – as far as reasonably practicable, to modifications and extensions of existing systems accepted
68 prior to the creation of this document, but only to the extent and insofar as existing systems are
69 being modified. It is otherwise not applicable to any unmodified aspect of the existing system;
- 70 • at all relevant phases of the life cycle of an application;
- 71 • for use by railway duty holders and the railway suppliers.

72 It is not required to apply this document to existing systems which remain unmodified, including those
73 systems already compliant with any former version of IEC 62278.

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

78 2 Normative references

79 The following documents are referred to in the text in such a way that some or all of their content
80 constitutes requirements of this document. For dated references, only the edition cited applies. For
81 undated references, the latest edition of the referenced document (including any amendments) applies.

82
83 IEC 62278-1:202x, *Railway Applications — The Specification and Demonstration of Reliability,*
84 *Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process*
85
86

87 3 Terms and definitions

88 For the purposes of this document, the terms and definitions given in IEC 62278-1 apply.

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

- 90 • IEC Electropedia: available at <http://www.electropedia.org/>
- 91 • ISO Online browsing platform: available at <http://www.iso.org/obp>

92

93 4 Abbreviations

ALARP	As Low As Reasonable Practicable
CBA	Cost Benefit Analysis
CCF	Common Cause Failures (Analysis)
CoP	Code of Practice
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
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
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 (unsafe) Failure Rate
THR	Tolerable Hazard Rate

94 **5 Safety process**

95 **5.1 Hourglass model for risk assessment and hazard control**

96 In this subclause, the Hourglass Model in Figure 1 is introduced: it offers a simplified approach that,
97 although not containing all aspects implied in the life cycle model, helps to clarify some issues.

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

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

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

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

112 The Hourglass Model describes two main aspects:

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

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

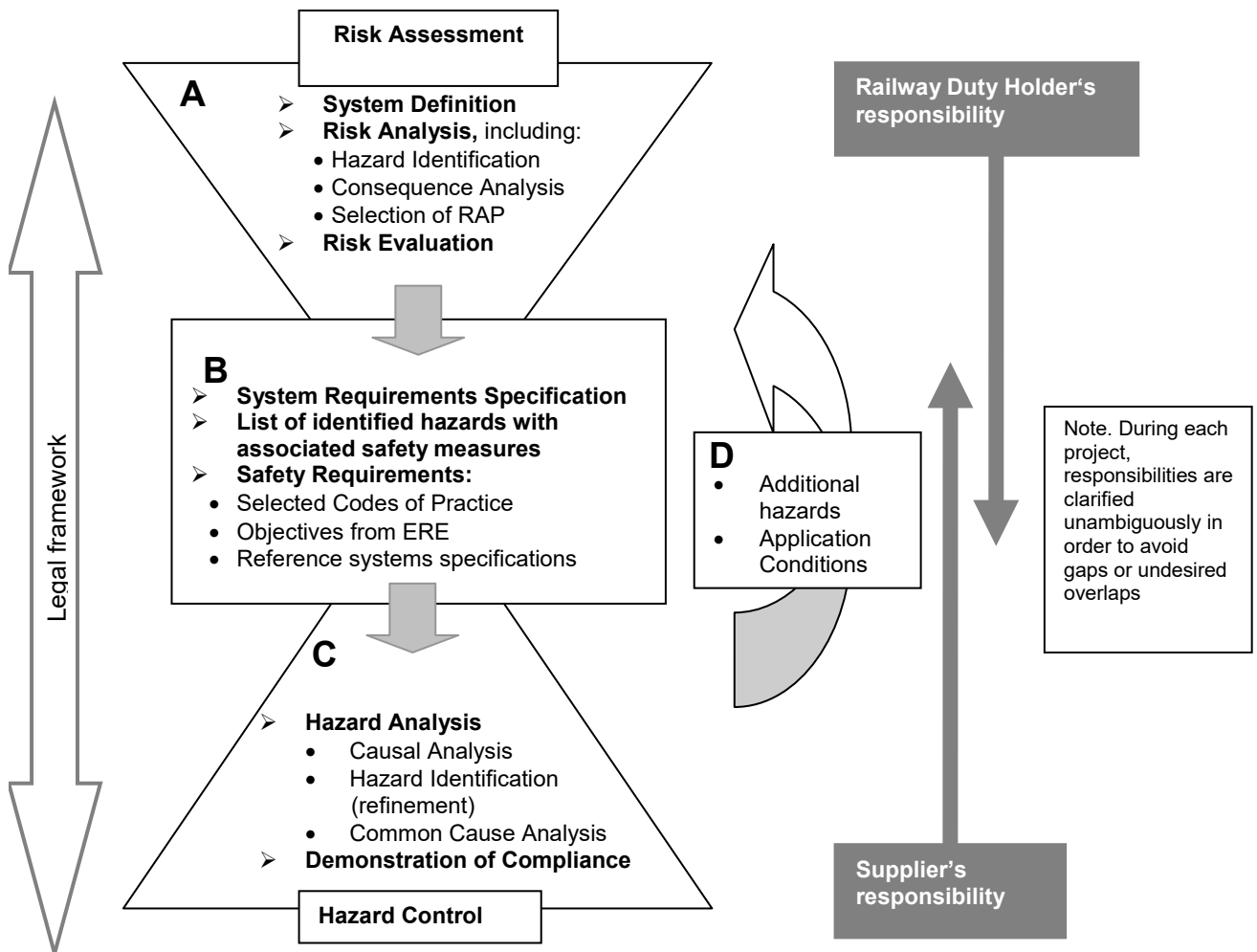


Figure 1 — The Hourglass Model

NOTE Part A (Risk Assessment) is associated with phases 1 to 3 in the life cycle as depicted in Figure 7 in IEC 62278-1. 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 7 in IEC 62278-1).

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).

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 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).

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).

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.

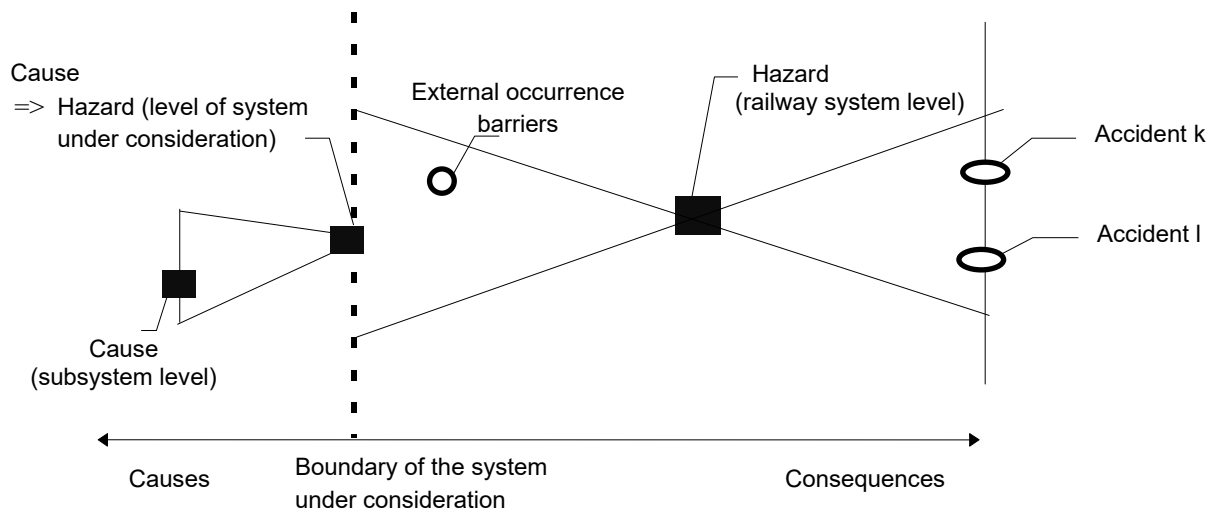


Figure 2 — Illustration of hazards with respect to the system boundary

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 subsystem 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.

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

213 **5.6 Responsibilities**

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

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

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

225 **6 Safety demonstration and acceptance**

226 **6.1 Introduction**

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

230 Safety demonstration evidence is based on the safety case. The purpose and content of the safety case
231 are defined in IEC 62278-1, Clause 8.

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

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

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

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

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

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

241 **6.2 Safety demonstration and safety acceptance process**

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

- 244 • Generic Product;
- 245 • Generic Application;
- 246 • Specific Application.

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

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

- 249 • the Application Design;

- 250 • the Physical implementation, including manufacturing, installation, and the facilities for operation and
251 maintenance.
- 252 If separate safety acceptance is needed for the application design and for its physical implementation, it
253 might be possible to divide the safety case for specific applications into two portions:
- 254 • the Application Design safety case;
- 255 • the Physical implementation safety case.
- 256 The safety case, as defined in IEC 62278-1, Clause 8, includes:
- 257 – Part 1: Definition of the system;
- 258 – Part 2: Quality Management Report;
- 259 – Part 3: Safety Management Report;
- 260 – Part 4: Technical Safety Report;
- 261 – Part 5: Related safety cases (if applicable);
- 262 – Part 6: Conclusion.
- 263 Whenever independent safety assessment is required for the system under consideration, this is performed
264 before system acceptance, in order to provide additional assurance that the necessary level of safety has
265 been achieved.
- 266 In this case, independent safety assessment shall take into consideration the safety case related to the
267 system under consideration and shall be performed in accordance with requirements defined in IEC 62278-
268 1, 6.8 and in accordance with the independence of role defined in subclause 7.3 of this document.
- 269 System acceptance of the system under consideration as adequately safe for its intended application, shall
270 be based on the following conditions:
- 271 • it has been developed, verified and validated in accordance with IEC 62278 series;
- 272 • the specified safety requirements have been fulfilled in accordance with IEC 62278 series.
- 273 The overall documentary evidence for system acceptance should consist of:
- 274 • the system definition and operational context;
- 275 • the system requirements and characteristics, including the safety requirements (and related risk
276 analysis whenever applicable);
- 277 • the safety case;
- 278 • the Independent Safety Assessment Report, when required. This report explains the activities carried
279 out to determine whether the system under consideration has been designed to meet its specified
280 safety requirements, and if necessary specify some additional conditions for its operation.
- 281 Provided all the conditions for safety acceptance have been satisfied, as demonstrated by the safety case,
282 and subject to the results of the independent safety assessment when required, the system under
283 consideration may be granted safety acceptance by the stakeholders responsible for its incorporation into
284 another system or final use.
- 285 When using a Generic Product (i.e. independent of application), or a Generic Application (i.e. class of
286 application) in the context of a Specific Application, it should be possible for safety acceptance to be based
287 on existing related independent safety assessment. This is not considered possible for Specific
288 Applications.

289 When a safety case for Generic Product (i.e. independent of application), or a Generic Application (i.e.
290 class of application) is developed, a validation activity for the system under consideration usually performed
291 in phase 9 “system validation” of the system life cycle, shall be also performed at the end of life cycle phase
292 6 “design and implementation” considering also the manufacturing of the first item.

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

296 According to tailoring requirements defined in IEC 62278-1, the stakeholder responsible for a given safety
297 process shall provide evidence and justification of the coverage and limits of the covered life cycle phases.

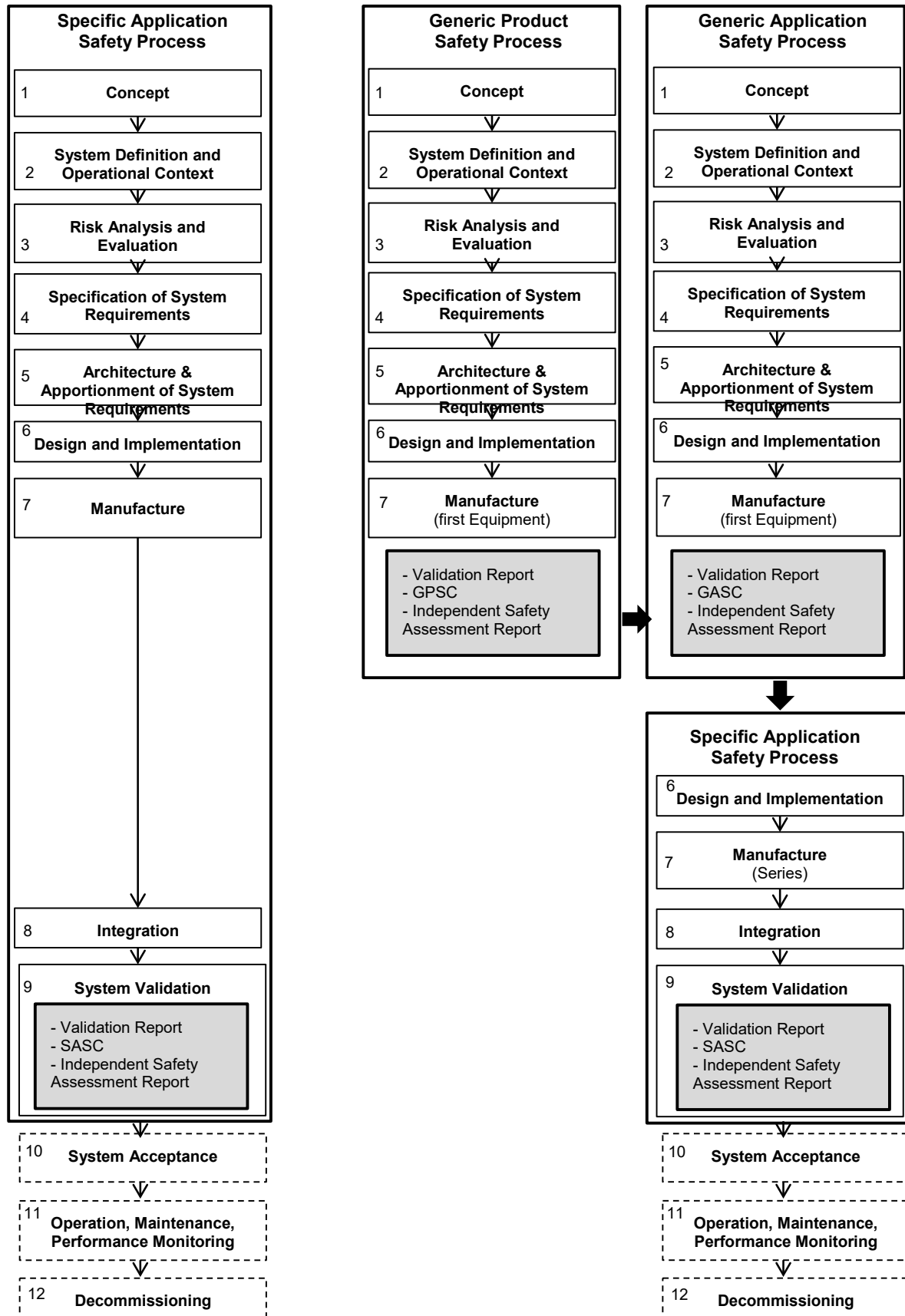


Figure 3 — Example of safety acceptance processes

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/subsystem/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/subsystem/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 subsystems or equipment. In such circumstances, safety acceptance of the main system is not possible without previous safety acceptance of the related subsystems/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.

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.

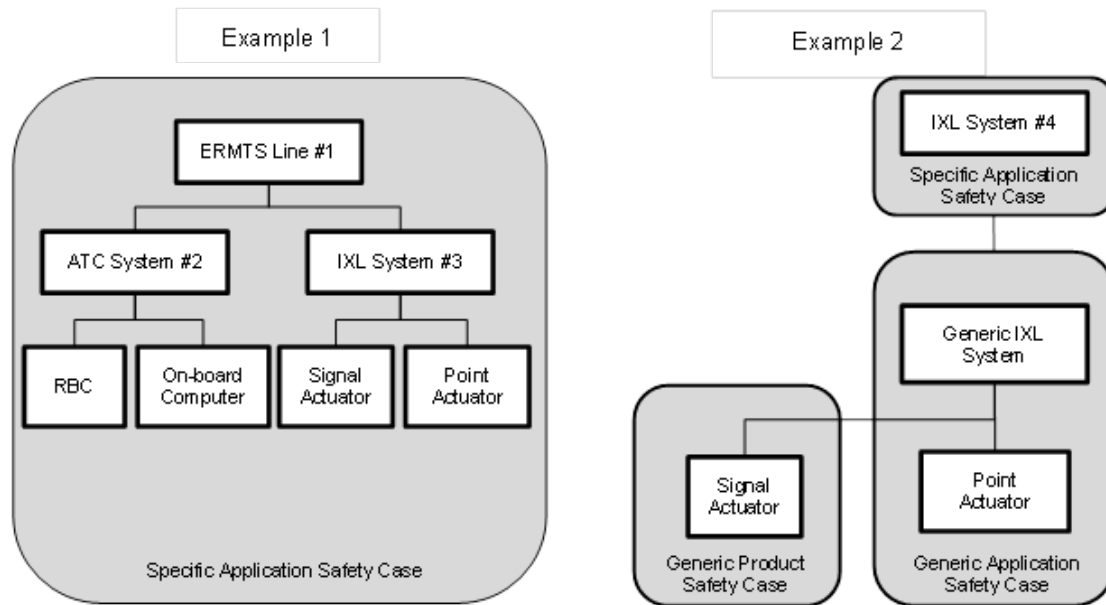


Figure 4 — Examples of dependencies between safety cases

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”, “subsystem” 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:

- It can be considered as a GP, and validated / approved with reference to IEC 62280, 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);
- 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;
- 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 completely 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.

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 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. In this case, 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.

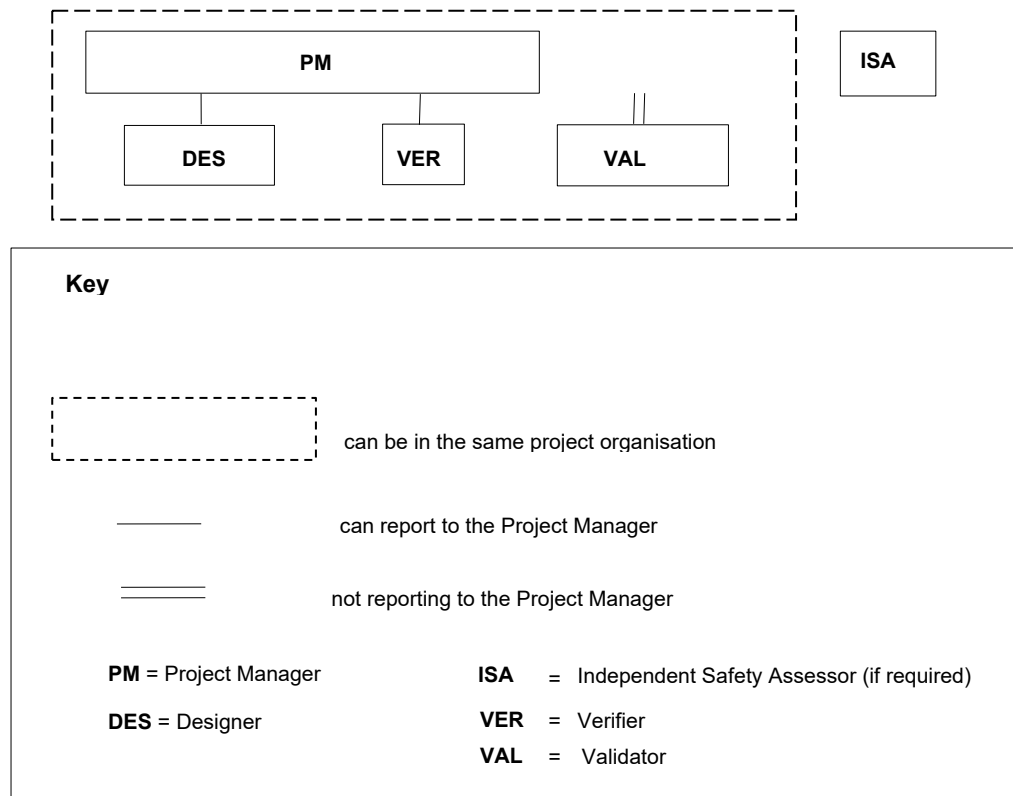


Figure 5 — Independence of Roles in the early phases (phases 1 to 4) of the lifecycle

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 6). 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