

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

**Part 2: Guide to the application of
EN 50126-1 for safety**

ICS 45.020

National foreword

This Published Document was published by BSI. It is the UK implementation of CLC/TR 50126-2:2007.

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

A list of organizations represented on GEL/9 can be obtained on request to its secretary.

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2007

© BSI 2007

ISBN 978 0 580 50488 4

Amendments issued since publication

Amd. No.	Date	Comments

English version

**Railway applications -
The specification and demonstration of Reliability, Availability,
Maintainability and Safety (RAMS) -
Part 2: Guide to the application of EN 50126-1 for safety**

Applications ferroviaires -
Spécification et démonstration
de la fiabilité, de la disponibilité,
de la maintenabilité
et de la sécurité (FDMS) -
Partie 2: Guide pour l'application
de l'EN 50126-1 à la sécurité

Bahnanwendungen -
Spezifikation und Nachweis
der Zuverlässigkeit, Verfügbarkeit,
Instandhaltbarkeit, Sicherheit (RAMS) -
Teil 2: Leitfaden zur Anwendung
der EN 50126-1 für Sicherheit

This Technical Report was approved by CENELEC on 2007-01-22.

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

CENELEC

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

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

Foreword

The European Standard EN 50126-1:1999, which was prepared jointly by the Technical Committees CENELEC TC 9X, Electric and electronic applications for railways, and CEN TC 256, Railway applications, under mode 4 co-operation, deals with the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) for railway applications.

A guide to the application of EN 50126-1 for safety of railway systems (this CLC/TR 50126-2) and a guide for the application to EN 50126-1 for rolling stock RAM (CLC/TR 50126-3:2006) have been produced to form informative parts of EN 50126-1:1999. Whilst this CLC/TR 50126-2 is applicable to all railway systems, including rolling stock, CLC/TR 50126-3:2006 is applicable to rolling stock RAM only.

This Technical Report, which was prepared by WG 8 of the Technical Committee CENELEC TC 9X, forms an informative part of EN 50126-1:1999 and contains guidelines for the application of EN 50126-1 for the safety of railway systems.

The text of the draft was submitted to the vote and was approved by CENELEC as CLC/TR 50126-2 on 2007-01-22.

Contents

Introduction.....	8
1 Scope.....	9
2 References.....	11
3 Definitions and abbreviations.....	12
3.1 Guidance on the interpretation of terms and definitions used in EN 50126-1	12
3.2 Additional safety terms	15
3.3 Abbreviations	17
4 Guidance on bodies/entities involved and concepts of system hierarchy and safety.....	17
4.1 Introduction.....	17
4.2 Bodies/entities involved in a system.....	18
4.3 Concepts of system hierarchy	18
4.3.1 Rail transport system environment and system hierarchy	19
4.4 Safety concepts	19
4.4.1 Hazard perspective	19
4.4.2 Risk.....	21
4.4.3 Risk normalising	22
5 Generic risk model for a typical railway system and check list of common functional hazards	23
5.1 Introduction	23
5.2 Generic risk model	23
5.3 Risk assessment process.....	24
5.3.1 Introduction.....	24
5.3.2 Generic process	24
5.4 Application of the risk assessment process	28
5.4.1 Depth of analysis.....	29
5.4.2 Preliminary hazard analysis	29
5.4.3 Qualitative and Quantitative assessment.....	30
5.4.4 Use of historical data.....	31
5.4.5 Sensitivity analysis	32
5.4.6 Risk assessment during life cycle phases.....	32
5.5 Check-list of common functional hazards and hazard identification	33
5.5.1 Introduction.....	33
5.5.2 Hazard grouping structures	34
5.5.3 Check-list of “Hazards”	35
6 Guidance on application of functional safety, functional safety requirements and SI targets, risk apportionment and application of SILs	36
6.1 Introduction.....	36
6.2 Functional and technical safety	36
6.2.1 System characteristics	36
6.2.2 Railway system structure and safety requirements	37
6.2.3 Safety related functional and technical characteristics and overall system safety	37

6.3	General considerations for risk apportionment	38
6.3.1	Introduction	38
6.3.2	Approaches to apportionment of safety targets	38
6.3.3	Use of THRs	40
6.4	Guidance on the concept of SI and the application of SILs	40
6.4.1	Safety integrity	40
6.4.2	Using SI concept in the specification of safety requirements	42
6.4.3	Link between THR and SIL	46
6.4.4	Controlling random failures and systematic faults to achieve SI	46
6.4.5	Use and misuse of SILs	49
6.5	Guidance on fail-safe systems	51
6.5.1	Fail-safe concept	51
6.5.2	Designing fail-safe systems	52
7	Guidance on methods for combining probabilistic and deterministic means for safety demonstration	54
7.1	Safety demonstration	54
7.1.1	Introduction	54
7.1.2	Detailed guidance on safety demonstration approaches	54
7.1.3	Safety qualification tests	65
7.2	Deterministic methods	65
7.3	Probabilistic methods	65
7.4	Combining deterministic and probabilistic methods	65
7.5	Methods for mechanical and mixed (mechatronic) systems	66
8	Guidance on the risk acceptance principles	67
8.1	Guidance on the application of the risk acceptance principles	67
8.1.1	Application of risk acceptance principles	67
8.1.2	The ALARP principle	68
8.1.3	The GAMAB (GAME) principle	69
8.1.4	Minimum Endogenous Mortality (MEM) safety principle (EN 50126-1, Clause D.3)	70
9	Guidance on the essentials for documented evidence or proof of safety (Safety case)	71
9.1	Introduction	71
9.2	Safety case purpose	72
9.3	Safety case scope	72
9.4	Safety case levels	72
9.5	Safety case phases	74
9.6	Safety case structure	75
9.7	Safety assessment	78
9.7.1	The scope of the safety assessor	78
9.7.2	The independence of a safety assessor	78
9.7.3	Competence of the safety assessor	79
9.8	Interfacing with existing systems	79
9.8.1	Systems developed according to the EN 50126-1 process	79
9.8.2	System proven in use	79
9.8.3	Unproven systems	80

9.9	Criteria for cross acceptance of systems	80
9.9.1	The basic premise	80
9.9.2	The framework	81
Annex A	(informative) Steps of risk assessment process	82
A.1	System definition	82
A.2	Hazard identification	83
A.2.1	Empirical hazard identification	83
A.2.2	Creative hazard identification	83
A.2.3	Foreseeable accident identification	83
A.2.4	Hazards	84
A.3	Hazard log	86
A.4	Consequence analysis	87
A.5	Hazard control	87
A.6	Risk ranking	88
A.6.1	Qualitative ranking	89
A.6.2	Semi-quantitative ranking approach	89
Annex B	(informative) Railway system level HAZARDS - Check lists	92
B.1	General	92
B.2	Example of hazard grouping according to affected persons	94
B.2.1	“C-hazards” – Neighbours group	94
B.2.2	“C-hazards” - Passengers group	95
B.2.3	“C-hazards” - Workers group	96
B.3	Example of functional based hazard grouping	96
Annex C	(informative) Approaches for classification of risk categories	99
C.1	Functional breakdown approach (a)	99
C.2	Installation (constituent) based breakdown approach (b)	99
C.3	Hazard based breakdown approach (c)	100
C.4	Hazard causes based breakdown approach (d)	101
C.5	Breakdown by types of accidents (e)	102
Annex D	(informative) An illustrative railway system risk model developed for railways in UK	103
D.1	Building a risk model	103
D.2	Illustrative example of a risk model for UK railways	104
D.2.1	Modelling technology	104
D.2.2	Usage and constraints	105
D.2.3	Model forecasts	105
Annex E	(informative) Techniques & methods	108
E.1	General	108
E.2	Rapid ranking analysis	109
E.3	Structured What-if analysis	109
E.4	HAZOP	110
E.5	State transition diagrams	110
E.6	Message Sequence Diagrams	111
E.7	Failure Mode Effects and Criticality Analysis - FMECA	112
E.8	Event tree analysis	112

E.9	Fault tree analysis	113
E.10	Risk graph method	114
E.11	Other analysis techniques	115
E.11.1	Formal methods analysis	115
E.11.2	Markov analysis	115
E.11.3	Petri networks	115
E.11.4	Cause consequence diagrams	115
E.12	Guidance on deterministic and probabilistic methods	115
E.12.1	Deterministic methods and approach	115
E.12.2	Probabilistic methods and approach	116
E.13	Selection of tools & methods	117
Annex F	(informative) Diagrammatic illustration of availability concept	119
Annex G	(informative) Examples of setting risk acceptance criteria	120
G.1	Example of ALARP application	120
G.2	Copenhagen Metro	123
Annex H	(informative) Examples of safety case outlines	124
H.1	Rolling stock	124
H.2	Signalling	126
H.3	Infrastructure	128
Bibliography		131

Figures

Figure 1	– Nested systems and hierarchy	18
Figure 2	– Definition of hazards with respect to a system boundary and likely accident	20
Figure 3	– Sequence of occurrence of accident, hazard and cause	21
Figure 4	– Risk assessment flow chart	25
Figure 5	– Hazard control flow chart	26
Figure 6	– Safety allocation process	39
Figure 7	– Factors influencing SI	41
Figure 8	– Process for defining a code of practice for the control of random failures	48
Figure 9	– Process for defining a code of practise for the control of systematic faults	49
Figure 10	– Differential risk aversion	71
Figure 11	– Safety case levels	73
Figure A.1	– Risk ranking for events with potential for significantly different outcomes	91
Figure D.1	– Illustrative annual safety forecasts generated by an integrated risk model	106
Figure D.2	– Illustrative individual risk forecasts generated by an integrated risk model	107
Figure E.1	– State transition diagram – Example	111
Figure E.2	– Example of message collaboration diagram	111
Figure E.3	– Example of consequence analysis using event tree	113
Figure E.4	– Fault tree analysis – Example	114
Figure F.1	– Availability concept and related terms	119
Figure G.1	– Risk areas and risk reducing measures	121
Figure G.2	– ALARP results of options 1 to 4	123

Tables

Table 1 – Cross-reference between certain life cycle phase activities and clauses of the report.....	10
Table 2 – Clauses of the report covering scope issues	10
Table 3 – Comparison of terms (duty holders).....	13
Table 4 – Structured approach to allocation of SI (refer to 6.4.2.2)	43
Table 5 – THR/SIL relationship	46
Table 6 – Possible states of a fail safe system	53
Table 7 – Approaches for system safety demonstration	56
Table 8 – Criteria for each of the risk acceptance principles	67
Table 9 – List of EN 50129 clauses and their applicability for documented evidence to systems other than signalling	75
Table A.1 – Example of frequency ranking scheme.....	89
Table A.2 – Example of consequence ranking scheme	90
Table A.3 – Risk ranking matrix.....	90
Table B.1 – Railway neighbour “c-hazards”	94
Table B.2 – List railway passenger “c-hazards”	95
Table B.3 – List of railway worker “c-hazards”	96
Table B.4 – System level hazard list based on functional approach.....	97
Table D.1 – Sample parametric data for a risk forecasting model	105
Table E.1 – Failure and hazard analysis methods	108
Table E.2 – Example of a hazard-ranking matrix	109
Table E.3 – Hazop guide words	110
Table G.1 – Upper and lower ALARP limits	123

Introduction

EN 50126-1 was developed in CENELEC under a mode 4 co-operation with CEN and is now regularly called up in specifications. In essence, it lists factors that influence RAMS and adopts a broad risk-management approach to safety. The standard also gives examples of some risk acceptance principles and defines a comprehensive set of tasks for the different phases of a generic life cycle for a total rail system.

Use of EN 50126-1 has enhanced the general understanding of the issues involved in dealing with safety and in achieving RAMS characteristics within the railway field. However, a number of issues have arisen that suggest that there are differences in the way that safety principles and/or requirements of this standard are being interpreted and/or applied to a railway system and its sub-systems.

Therefore, the guidelines included are to remove such differences and to enable a coherent and pragmatic approach, within Europe, for setting safety targets, assessing risks and generally dealing with safety issues. The report is not intended to set any specific safety targets (which will remain the responsibility of the relevant regulatory authorities) but only to provide guidance on different methods that can be used for setting targets, assessing risks, deriving safety requirements, demonstrating satisfactory safety levels, etc., with examples, where appropriate. The responsibility for accepting the methods to be used and for setting targets remains with the Railway Authority (RA) in conjunction with the Safety Regulatory Authority (SRA).

Furthermore the introduction of the proposed safety directive (European Directive on the development of safety on the Community's railways through development of common safety targets and common safety methods) should lead to a common safety regulatory regime within Europe. Such a regime will require that there is a common European approach to the methods for setting safety targets and for assessing risks.

The Technical Report is intended to cover the full spectrum of railway systems and for use by all the different user groups of the standard EN 50126-1. User groups may be part of any of the different players (bodies/entities) involved during the life cycle phases of a system, from its conception to disposal.

However, this Technical Report deals with only those items covered by the standard EN 50126-1 that are identified by the scope of work and with clarification of areas where EN 50126-1 could be misinterpreted. Clauses in the report are structured to cover clarifications of definitions and concepts and then to reflect the items in the scope and in order of the risk assessment process. But the contents are limited to include guidance and explanations for only those items that were remitted by resolution 26/5 of TC 9X and any related issues.

1 Scope

1.1 This Technical Report provides guidance on specific issues, listed under 1.3 below, for applying the safety process requirements in EN 50126-1 to a railway system and for dealing with the safety activities during the different system life cycle phases. The guidance is applicable to all systems covered within the scope of EN 50126-1. It assumes that the users of the report are familiar with safety matters but need guidance on the application of EN 50126-1 for safety issues that are not or could not be addressed in the standard in detail.

1.2 EN 50126-1 is the top-level basic RAMS standard. This application guide, CLC/TR 50126-2 forms an informative part of EN 50126-1 dealing explicitly with safety aspects as limited by the scope defined in 1.3 below.

1.3 Limitation of scope

The scope is limited to providing guidance only for the following issues related to EN 50126-1.

- i) Production of a top-level generic risk model for the railway system down to its major constituents (e.g., signalling, rolling stock, infrastructure, etc.) with definition of the constituents of the model and their interactions.
- ii) Development of a checklist of common functional hazards within a conventional railway system (including high speed lines, Light Rail Train's, metro's, etc.).
- iii) Guidance on the application of the risk acceptance principles in EN 50126-1.
- iv) Guidance on the application of functional safety in railway systems and qualitative assessment of tolerable risk with examples.
- v) Guidance for specifying relevant functional safety requirements and apportionment of safety targets to the requirements for sub-systems (e.g. for rolling stock: door systems, brake systems, etc.).
- vi) Guidance on the application of safety integrity level concept, through all the life cycle phases of the system.
- vii) Guidance on methods for combining probabilistic and deterministic means for safety demonstration.
- viii) Guidance on the essentials (incl. maintenance, operation, etc.) for documented evidence or proof of safety (safety case) with proposals for a common structure for such documentation.

1.4 A diagrammatic representation of the scope and limitations of the scope cross linking with the safety activities within the life cycle phases of EN 50126-1 and the roles/responsibilities of the principal players is given in Table 1 below. However, for full comprehension it is suggested that these clauses are considered only after the whole document has been read:

Table 1 – Cross-reference between certain life cycle phase activities and clauses of the report

Lifecycle phase of EN 50126-1	Bodies/Entities involved	Relevant clause
1. CONCEPT		Not in the scope
2. SYSTEM DEFINITION AND APPLICATION CONDITIONS	Generally, Railway Authority (RA) for railway system level, Railway Support Industry (RSI) for lower system levels.	4.3, 5.3.2.1
3. RISK ANALYSIS	RA or RSI, depending on the life cycle phase.	4.4, 5.3, 5.4
4. SYSTEM REQUIREMENTS	Generally, RA for railway system level. RSI for lower system levels.	5.3.2.1, 6.2
5. APPORTIONMENT OF SYSTEM REQUIREMENTS	Body/entity responsible for the design of the system under consideration.	5.4.6, 6.2, 6.3, 8
6. DESIGN AND IMPLEMENTATION	RSI	4.3, 5.4, 6
7. MANUFACTURING		Not in the scope
8. INSTALLATION		Not in the scope
9. SYSTEM VALIDATION (INCLUDING SAFETY ACCEPTANCE AND COMMISSIONING)	SRA and RSI	7.1, 9
10. SYSTEM ACCEPTANCE	RA and SRA	7.1, 9
11. OPERATION AND MAINTENANCE	RA	5.4.6, 9.5
12. PERFORMANCE MONITORING		Not in the scope
13. MODIFICATION AND RETROFIT	RA, SRA and RSI as relevant	Part of 9.8
14. DECOMMISSIONING AND DISPOSAL		Not in the scope

1.5 This Technical Report is structured generally to reflect the order of the safety process. However, the issues within the scope of the report, as listed under 1.3 above, are covered in the clauses as tabulated below.

Table 2 – Clauses of the report covering scope issues

Clause 1	Scope.
Clause 2	References.
Clause 3	Interpretations and explanations of the definitions in EN 50126-1 and definition of additional terms and abbreviations used in the report.
Clause 4	Provides guidance on system hierarchy, on bodies/entities involved and their responsibilities and on safety concepts implicit in the safety process as covered by the scope.
Clause 5	Items i) and ii) of the scope.
Clause 6	Items iv), v) and vi) of the scope.
Clause 7	Item vii) of the scope.
Clause 8	Item iii) of the scope.
Clause 9	Item viii) of the scope.

2 References

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

EN 50126-1:1999	Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process
CLC/TR 50126-3:2006	Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the application of EN 50126-1 for rolling stock RAM
EN 50128:2001	Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems
EN 50129:2003	Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling
CLC/TR 50506 series ¹⁾	Railway applications – Communication, signalling and processing systems – Application Guide for EN 50129
EN 60300-3-1:2004	Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology (IEC 60300-3-1:2003)
EN 61508:2001 (series)	Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508 series)
EN 61078:1993	Analysis techniques for dependability – Reliability block diagram method (IEC 61078:1991)
EN 61160	Design review (IEC 61160)
EN 61703	Mathematical expressions for reliability, availability, maintainability and maintenance support terms (IEC 61703)
IEC 60050-191	International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service
IEC 60300-3-9:1995	Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems
IEC 60812:1985	Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
IEC 61025:1990	Fault tree analysis (FTA)
IEC 61165:1995	Application of Markov techniques
IEC 61882:2001	Hazard and operability studies (HAZOP studies) – Application guide
ISO/IEC Guide 51:1999	Safety aspects – Guidelines for their inclusion in standards

¹ At draft stage.

3 Definitions and abbreviations

The definitions in EN 50126-1 are a necessary prerequisite for the correct understanding and application of the standard. User experience has shown however, that in some cases definitions in the standard can be interpreted in more than one way. In other cases, the definitions differ from those used in other safety related standards, e.g. EN 50128, EN 50129 or EN 61508.

Furthermore, user feedback suggests that some translated definitions of EN 50126-1 (in a language other than English), are not sufficiently accurate with the consequence that misinterpretations have occurred.

Consequently some clarification of the terms and definitions used in EN 50126-1 is included in this report to ensure a coherent interpretation of these terms.

Some additional safety terms used in the report have also been defined. Use of these terms in the report is to further ensure a coherent interpretation of certain safety management concepts of EN 50126-1 and to enhance their understanding.

3.1 Guidance on the interpretation of terms and definitions used in EN 50126-1

The following paragraphs provide clarifications to the definitions in EN 50126-1. The respective clause numbers of EN 50126-1 are shown in brackets.

3.1.1

apportionment (3.1)

EN 50126-1 defines apportionment as:

a process whereby the RAMS elements for a system are sub-divided between the various items which comprise the system to provide individual targets.

In this definition the term “RAMS elements” can usually be interpreted as “targets” or “requirements” for Reliability, Availability, Maintainability and Safety. The overall RAMS targets (e.g. risk acceptance criteria) has to be apportioned to the individual system elements in order to enable these elements to be constructed in a way that allows the overall target to be achieved

3.1.2

availability (3.4)

In EN 50126-1 this term is defined as:

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

Availability is related to *failed states/failure-modes* (see Figure 3 of EN 50126-1) of functions that the system is supposed to provide. Considering only the subset of *safety-related failure modes* the direct influence of *safety* on *availability* becomes obvious.

NOTE Terms contributing to the definition of availability are sometimes used incorrectly. Figure F.1 (Annex F) illustrates the concept of availability and clarifies the correct use of contributory terms.

Prior to the determination of the availability the system boundaries have to be defined to be able to decide whether external resources (e.g. the supplied power) are part of the system

3.1.3

failure rate (3.14)

The definition used in EN 50126-1 is abstract, formulated in mathematical language as:

the limit, if this exists, of the ratio of the conditional probability that the instant of time, T , of a failure of a product falls within a given time interval $(t, t+\Delta t)$ and the length of this interval, Δt , when Δt tends towards zero, given that the item is in an up state at the start of the time interval.

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{R(t) - R(t + \Delta t)}{\Delta t \cdot R(t)} = -\frac{\dot{R}(t)}{R(t)}$$

$R(t)$ means the reliability function

For better understanding of this definition, the following might be useful:

The product of the failure rate (at a certain time t in the components live) and the following very small interval ($\Delta t \rightarrow 0$) of time $\lambda(t) \cdot \Delta t$ describes the conditional probability that an item which has survived until time t will fail in the following period of time Δt .

NOTE Due to lack of data very often a constant failure rate is assumed although failure rates in reality are rarely constant. For electronic equipment $\lambda = \text{const.}$ is commonly used. For components subject to wear out (mechanical, pneumatic, electromechanical, etc.) the so-called bath tub curve often replaces the reliability behaviour if not known in detail. This curve is represented by the areas “early failure”, “constant failure” and “wear-out failure” and can be described by the *Weibull* function.

The ratio of the number of counted failures divided by the related interval of time (or distance) gives an approximation of the failure rate in this specific interval.

More information can be found in EN 61703.

3.1.4

hazard (3.17)

The definition used in EN 50126-1 only refers to situations that may lead to personal injury as:
a physical situation with a potential for human injury.

Definitions in other standards are broader in the sense that damage to the environment and significant loss of material values is also a harm to be considered in safety analyses. Additionally, the limitation of hazards to physical situations might be rather restrictive in some cases. Therefore, the following definition, as given in EN 50129, is considered more appropriate:

“a condition that could lead to an accident”

3.1.5

maintainability (3.20)

In EN 50126-1 this term is defined as:

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

Maintainability has to be designed into the system and is then an intrinsic property of the system. EN 50126-1 classifies it as a system condition (see Figure 5 of EN 50126-1)

3.1.6

maintenance (3.21)

In EN 50126-1 this term is defined as:

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

Maintenance of a system is a matter of logistics and is planned by the supplier and/or railway-company. It is classified as maintenance condition in EN 50126-1 (see Figure 5 of EN 50126-1)

3.1.7

railway authority (3.26)

In EN 50126-1 this term is defined as:

The body with the overall accountability to a Regulator for operating a railway system.

NOTE Railway authority accountabilities for the overall system or its parts and lifecycle activities are sometimes split between one or more bodies or entities. For example:

- the owner(s) of one or more parts of the system assets and their purchasing agents;
- the operator of the system;
- the maintainer(s) of one or more parts of the system;
- etc.

Such splits are based on either statutory instruments or contractual agreements. Such responsibilities should therefore be clearly stated at the earliest stages of a system lifecycle.

Sometimes the users of EN 50126-1 have misinterpreted the term “authority”. To clarify the term, it is emphasised that a “railway authority” in the sense of EN 50126-1 is NOT the regulator or the government.

See Table 3 for equivalent terms for duty holders used in EN 50126-1 and the EU Safety Directive:

Table 3 – Comparison of terms (duty holders)

EN 50126-1	EU Safety Directive
railway authority	infrastructure manager railway undertaking
safety regulatory authority	safety authority
railway support industry	supplier manufacturing industry

3.1.8

risk (3.34)

EN 50126-1 defines this term as:

the probable rate of occurrence of a hazard causing harm and the degree of severity of that harm.

This is often misinterpreted to mean:

“The probable rate of occurrence of a hazard **that may cause harm** and the degree of severity of that harm.”

The problem is that the occurrence of a hazard is not equivalent to an occurrence of harm. In order to make risks comparable with each other it is important to consider the probability that a hazard actually leads to harm. For example, if the barriers at a level crossing do not close when commanded (hazard) this does not automatically lead to a crash between a train and a car (i.e. accident or occurrence of harm).

Correct interpretation:

“the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.”

Mathematically this is represented as:

$$\text{Risk} = \text{Rate (of accidents)} \times \text{Degree of Severity (of harm)}$$

Consequently, in Table 4 of EN 50126-1 (frequency-consequence-matrix) the title in the left column “*frequency of occurrence of a hazardous event*” has to be read as “*frequency of occurrence of an accident (caused by a hazard)*” Also see 3.2.9

3.1.9

safety (3.35)

EN 50126-1 defines safety as:

freedom from unacceptable risk of harm.

This could be misleading, because the aspect “harm” is already included in the term “risk” as defined in 3.1.8 above. To avoid misunderstandings the shortened definition “*freedom from unacceptable risk*” is more appropriate

3.1.10

safety integrity (3.37)

EN 50126-1 defines the term as:

the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Generally, safety relies on adequate measures to prevent or tolerate faults (as safeguards against systematic failure) as well as on adequate measures to control random failures. In this sense, safety integrity means that the qualitative measures (to avoid systematic failures) should be balanced with the quantitative targets (to control random failures).

3.1.11

systematic failures (3.42)

EN 50126-1 defines this term as:

failures due to errors in any safety lifecycle activity, within any phase, which cause it to fail under some particular combination of inputs or under some particular environment condition

Wording used in the definition of this term in EN 61508 gives an alternative explanation, even though there is no actual difference in the meaning between the two. EN 61508 defines it as:

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

NOTE 3 Examples of causes of systematic failures include human error in

- the safety requirements specification;
- the design, manufacture, installation, operation of the hardware;
- the design, implementation, etc. of the software.

NOTE 4 Failures in a safety-related system are categorised as random failures or systematic failures.

3.1.12

tolerable risk (3.43)

EN 50126-1 defines this term as:

the maximum level of risk of a product that is acceptable to the Railway Authority (RA).

The RA is responsible for agreeing the risk acceptance criteria and the risk acceptance levels with the Safety Regulatory Authority (SRA) and for providing these to the Railway Support Industry (RSI) (see 5.3.2). Usually, it is the SRA or the RA by agreement with the SRA that defines risk acceptance levels. Risk acceptance levels currently depend on the prevailing national legislation or national/other regulations. In many countries risk acceptance levels have not yet been established and are still in progress and/or under consideration

3.2 Additional safety terms

This clause lists useful additional safety terms that are not defined in EN 50126-1 but are used in the report and provide better understanding of the principles and concepts in EN 50126-1.

3.2.1

accident

an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage [EN 50129]

3.2.2

collective risk

the risk from a product, process or system to which a population or group of people (or the society as a whole) is exposed

3.2.3

commercial risk

the rate of occurrence and the severity of financial loss, which may be associated with an accident or undesirable event

3.2.4

deterministic

a characteristic of a system whose behaviour can be exactly predicted because all its causes are either known or are the same as for a proven equivalent system

3.2.5

environmental risk

the rate of occurrence and the severity of the extent of contamination and/or destruction of the natural habitat which may arise from an accident

3.2.6

equivalent fatality

a convention for combining injuries and fatalities into one figure for ease of processing and comparison

3.2.7

fault, error, failure

These terms are closely related with each other although they have different meanings. In order to avoid misunderstandings, it is recommended to consider the differences between these terms.

- A failure is the termination of the ability of an item to perform a required function. [IEC 60050 (191)].

NOTE 1 After a failure the item has a fault.

NOTE 2 “Failure” is an event, as distinguished from “Fault”, which is a state.

- A fault is an item state, characterised by its inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [IEC 60050 (191)].

NOTE 3 A fault is often the result of a failure of the item itself, but may exist without prior failure.

- An error is a discrepancy between a computed, observed or measured value or condition and the true specified or theoretically correct value or condition [IEC 60050 (191)].

NOTE 4 An error can be caused by a faulty item, e.g., a computer error made by faulty computer equipment.

NOTE 5 The French term “erreur” may also designate a mistake.

– A Human Error or Mistake is a human action that produces an unintended result [IEC 60050 (191)].

A fault can be an incorrect signal value or an incorrect decision within a system. If a fault is actually exercised, it may contaminate the system by causing an error, i.e. erroneous information or system states.

A failure has occurred if a functional unit is no longer able to perform its required function, i.e. a failure is an observable effect outside the system boundary arising from an internal error or fault. An error or fault does not always lead to a failure. For example, internal error checking may correct the error. Consequently, failure is a matter of function only and is thus related to purpose, not to whether an item is physically intact

3.2.8

functional safety

that part of safety that is dependent upon the functions of a system in the normal operation, in response to external stimuli, and under failure modes (also see 6.2)

3.2.9

hazardous event

the term “hazardous event” is used but not defined in EN 50126-1. It should be noted that the term, as used in the standard, is not consistently related to a *hazard* only. In most cases, the term has been used in the standard to mean an “**accident**” and should be interpreted as such

3.2.10

independent safety assessor

a person or an entity (appointed to carry out safety assessment of a system) with a degree of independence from the system design/project organisation. The degree of independence must be appropriate to the required safety integrity for the system

3.2.11

individual risk

the risk from a product, process or system to which an individual person is exposed

3.2.12

loss

harm to people, damage to the natural environment or financial detriment to an enterprise or a combination of these which may arise from accidents

NOTE The terms harm and loss have a very similar meaning. In the context of safety they can be regarded as being synonymous.

3.2.13

loss analysis

estimation of the severity of loss associated with an accident

3.2.14

probabilistic

relating to, or governed by, probability.

The behaviour of a probabilistic system cannot be predicted exactly but the probability of certain behaviours is known. A probabilistic analysis represents predictive calculation of system behaviour. The calculation is based on underlying models. Input data typically involves expert judgement as well as known subsystem or component reliability data and distributions

NOTE Probabilistic functions have an expectancy value and a distribution.

3.2.15

procedural safety

that part of safety that is dependent on procedures (e.g. operational and maintenance procedures)

NOTE Whilst operational procedures are a part of safety, maintenance procedures only maintain a degree of safety but do not create safety.

3.2.16

risk based approach

related to safety, the risk based approach is a process for ensuring the safety of products, processes and systems through consideration of the hazards and their consequent risks

3.2.17

technical safety

that part of safety that is dependent on the technical characteristics of a product derived from the system requirements and/or from the system design

3.2.18

safety barrier

a system or action, intended to reduce the rate of a hazard or a likely accident arising from the hazard and/or mitigate the severity of the likely accident. The effectiveness of the barrier will depend on the extent of their independence

3.3 Abbreviations

For the purposes of this report and unless otherwise explained elsewhere in the report, the abbreviations given below apply:

Abbreviation	Full expression	Definition and/or explanation of term
PSP	Product, System or Process	Used as an acronym
RA	Railway Authority	Definition 3.1.7
RSI	Railway Support Industry	Defined in EN 50126-1 (3.27); Generic term denoting supplier(s) of complete railway systems, subsystems or component parts
SI	Safety Integrity	Definition 3.1.11
SIL	Safety Integrity Level	Defined in EN 50126-1 (3.38); One of a number of defined discrete levels for specifying safety integrity requirements of the safety functions to be allocated to safety related systems.
SRA	Safety Regulatory Authority	Definition 3.1.7
THR	Tolerable Hazard Rate	Rate of occurrence of a hazard that would result in an acceptable level of risk for that hazard (normally judged acceptable by a recognised body e.g. RA or RSI by consultation with the SRA or recognised by the SRA itself).

4 Guidance on bodies/entities involved and concepts of system hierarchy and safety

4.1 Introduction

EN 50126-1 defines safety as the “freedom from unacceptable risk of harm”, taking into account all the interactions between a system and its environment. This definition addresses safety in all aspects, incorporating functional and technical safety, health and safety issues and impact of human factors.

Clause 4 gives a perspective of the bodies/entities involved in a railway system and aims at providing guidance on some of the underlying concepts implicit in system hierarchy and in safety and risk assessment, e.g., risk, hazards, harm and safety itself. In this regard, it complements the analysis of railway RAMS and of the influencing factors provided in Subclauses 4.3 and 4.4 of EN 50126-1.

4.2 Bodies/entities involved in a system

Depending on the social/political environment and the organisational/management structure of the railway system concerned, a number of bodies/entities, performing different functions, may be involved within the life cycle phases of the system. For the purpose of guidance the bodies/entities are divided into 3 main categories (as defined in EN 50126-1) and are as below (also see 3.1.7). These are also referred to as “duty holders” in the EU safety directive and the equivalent term used in the safety directive for these categories is shown in brackets:

- RA (Infrastructure manager and/or railway undertaking),
- SRA (safety authority),
- RSI (system supplier/installer/manufacturer)

The roles and responsibilities of these bodies may vary or be contracted out to several other players or sub-contractors, depending on:

- Social, political or legal considerations,
- Size and complexity of the system or subsystem concerned,
- Economic, organisational or managerial considerations.

It is therefore advisable to identify all the players that can be a part of this relationship and to examine and document how the roles and responsibilities of dealing with safety, during the life cycle of the system/sub-system concerned, are shared between them.

4.3 Concepts of system hierarchy

Basic concept of nested systems in a system hierarchy can be shown diagrammatically by Figure 1.

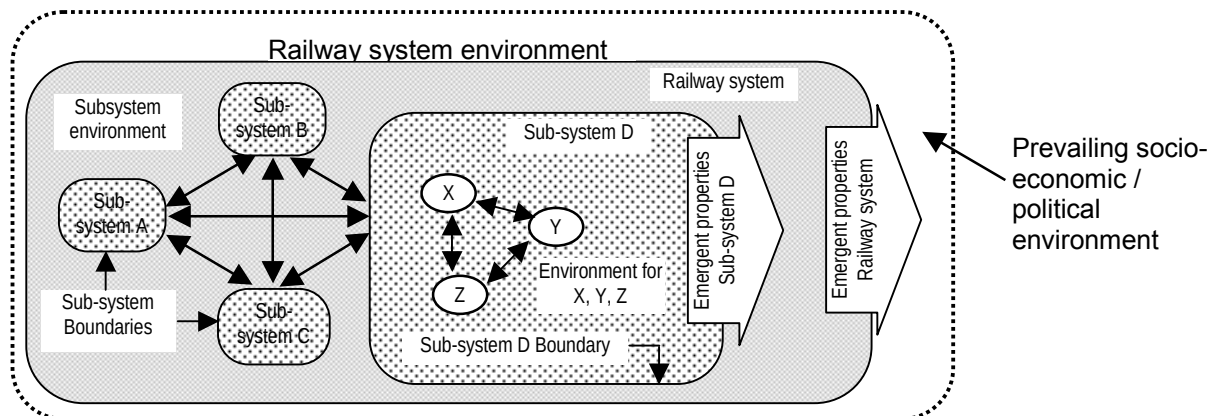


Figure 1 – Nested systems and hierarchy

The external view of a system under consideration represents its emergent properties that are the ones that the user or the customer expects. The properties are meaningful only when attributed to the whole system and not ascribable to any one part of the system on its own. According to the nested systems concept, systems are themselves built up of smaller systems that themselves are built up of even smaller systems and so on.

For convenience, multi level nested systems are usually handled on the basis of successive groupings of systems at 3 levels of hierarchy. The 3 level hierarchies would consist of a “system under consideration” (e.g. sub-system D) containing its intra-related subsystems (X, Y and Z) and itself being contained, together with its inter-related sub-systems (A, B and C) in a containing or parent system (e.g. Railway system). This provides visibility of the 3 levels and enables consideration of:

- the interactions and interfaces between the “system under consideration” and its “siblings” i.e. the inter-related sub-systems and,
- the influences and interactions between the “system under consideration” and its environment (i.e. the “parent” or “containing system”).

Functions of a system are the activities performed by the system as a whole. Functions and structure provide the “internal” view of the system properties that produce the emergent properties and are the concern of the body/entity responsible for the design of the system. The environment consists of anything that could influence, or be influenced by, the system. This will include anything to which the system connects mechanically, electrically or by other means, including EMI, thermal, etc. The environment will also include people and procedures that can effect, or be affected by, the operation of the system.

Understanding the boundary between the system under consideration and its environment and the interactions with its inter-related sub-systems is a pre-requisite to understanding how the system might contribute to an accident and what its hazards are. (See 6.2.2).

4.3.1 Rail transport system environment and system hierarchy

A rail transport system would normally operate within a prevailing socio-economic/political environment. The affordability of the rail transport system, both in terms of its design, construction and implementation and in terms of its subsequent use, also depends on this environment. Therefore any safety considerations for the railway system must be taken within the context of affordability of the railway system and of the existing safety levels within the prevailing environment or safety levels that are socially/politically tolerable within this environment. A railway system that is unaffordable to the users reduces safety within the social environment, irrespective of how safe the railway system is.

The relevant authority within the prevailing socio-economic/political system that has jurisdiction over the rail transport system would have the responsibility for ensuring a balance between affordability and safety and therefore for providing/specifying safety requirements and targets for tolerable levels of safety risk for the railway system as a whole. Often such targets may not be available at the start of a project and the body/entity responsible for the railway system (e.g. for its design/configuration) may propose targets that are endorsed or revised by the relevant authority with jurisdiction.

Similarly, considering a hierarchical system structure, when the system under consideration is a subsystem of the railway system then it would be the body/entity responsible for the railway system (e.g. the RA) that should set or specify the safety requirements and targets for tolerable levels of risk for the subsystem. In general, therefore, it is the body/entity responsible for the design/configuration at each system level that would also be responsible for setting or specifying safety requirements and targets for its subsystems. In some instances, the RA itself may set or specify safety requirements and safety targets for lower level subsystems or for specific hazards.

4.4 Safety concepts

Guidance on the underlying concepts implicit in some of the safety terms is given in the following subclauses.

4.4.1 Hazard perspective

Hazard is defined in 3.1.4. However, the following concepts are beneficial for a structured approach to identifying hazards, in particular enabling exposure of hazards such as those arising from interaction of sub-systems and for the rationalisation of the effort involved in further analysis:

4.4.1.1 Hazard clusters

A hazard cluster is a unique set of independent number of hazards, which share common characteristics such as same causation or same consequence. The aim of aggregating hazards into such clusters is to rationalise the effort involved in further analysis and to facilitate mapping them to key safety functions. Clause B.2 shows examples of aggregation of hazards into clusters. To distinguish the cluster of hazards from the raw information of hazards (i.e. the detailed hazards), in this document, the hazard clusters are referred to as “c-hazards”.

The concept of “c-hazard” can be extended to apply at more than one level of system definition. Hazard identification (initially at the top system level, i.e. the railway system level) may yield many hazards. The hazards are then reviewed to remove repetitions and dependencies and to identify synergistic hazards i.e. those with a common cause or tangible relationship, which are then aggregated into clusters to form c-hazards (see Clause B.2 for examples).

4.4.1.2 Top-level hazard

The term top hazard or top-level hazard refers to hazards at the highest system level, e.g., the railway system level. The term should not be used in any other sense.

4.4.1.3 Interface Hazards

These are hazards arising due to interaction of subsystems at system interfaces. System interfaces, in this context, refers to any of the following:

- subsystem interfaces as part of system hierarchy during the system development,
- interfaces between organisations or entities involved in different activities during development, operation, maintenance, etc. of the system. These may be different for different life cycle phases.

Identification of interface hazards requires cooperation between the two “sibling” systems or “neighbour” entities to ensure that all significant hazards have been identified and the responsibilities and measures for their management clearly defined and understood by the parties/entities involved.

The concept of “Interface Hazard” is important as they may not be evident by either system on its own but result from interaction between the systems during different system states.

4.4.1.4 Hazards at system boundaries

Figure 2 illustrates the relationship between a system boundary, hazards, hazard causes and accidents (derived from Figure A.4 of EN 50129). It shows that the cause of a hazard at system level (internal view of the system), resulting from a subsystem failure or error is considered as a hazard at the sub-system level with respect to its boundary (external view of the subsystem). This concept enables a structured hierarchical approach to hazard analysis and hazard tracking within “nested” systems and allows hazard identification and causal analysis to be performed at several system levels, particularly during system development.

It is necessary to understand that the hazard at a system boundary relates solely to the functions of the system under consideration. Therefore, the expression of the hazard should take into account all aspects pertaining to its interaction with other inter-related systems, which may provide mitigating factors. Two examples are given below:

- if a hazard associated with a subsystem is monitored by another subsystem, then the safety requirement for the hazard should take into account the mitigation provided by the monitoring equipment and the consequent time at risk.
- at a subsystem level, axlebox seizure on a high speed train might be regarded as a hazard. If the vehicle is running on infrastructure with a network of monitoring devices (e.g. hot axlebox detectors), then the safety requirement for the hazard should take into account the presence of the monitoring equipment and the consequent time at risk.

Hence, the apportionment of safety requirements within a system is a refinement process. It may require several iterations to ensure that the safety requirements are understandable by the concerned stakeholders (e.g. the development team responsible for the subsystem).

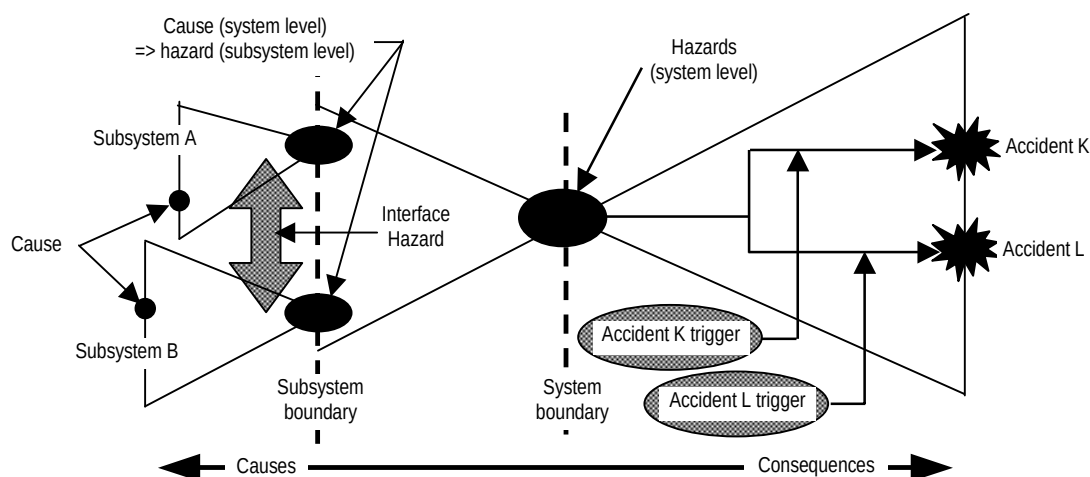


Figure 2 – Definition of hazards with respect to a system boundary and likely accident

NOTE Care should be taken to avoid applying the term “hazard” down to a system level/component, (creating several layers of hazards and THRs), to such an extent that eventually, for example, a broken resistor becomes a hazard. This should be avoided by considering system functions, and stopping the breakdown at level where functionally independent items can no longer be found.

4.4.2 Risk

Risk is defined in 3.1.8 and is concerned with occurrence of harm and the degree of its severity. In this context harm may imply

- Human harm (causing injuries, fatalities);
- Environmental harm (damage to property, spread of toxic substances, other environmental impact, etc.);
- Commercial harm (loss of trust and/or loss of assets).

Tolerability of risk depends on how a risk is perceived which, differs greatly between people. The reasons being, prevailing social and cultural conditions, psychological and physical factors and also factors such as whether the risk is voluntary (e.g. self imposed) or involuntary (e.g. imposed by others) and whether it has fearfully large consequences. Voluntary risk is generally more acceptable than involuntary risk or where the person exposed to the risk does not have control over the risk. Such factors need to be taken into account for establishing risk tolerability criteria.

For railway systems, the relevant authority may choose to classify persons exposed in different ways. As an example, they may be classed into 3 groups, i.e. passengers, railway workers (i.e. those employed by or contracted by the RA or the RSI for working on the railway or authorised by the RA for carrying out a specific task on the railway) and general public. The groups, with different level of involvement in the system and having a range of abilities, may perceive risks differently. Hence, the risk acceptability criteria for the three groups may be different. It is therefore recommended that the appropriate criteria to be applied be agreed with the relevant authorities at the start of the project.

Level of risk faced by the groups may also be influenced by a number of factors. Such influencing factors are

- exposure of the persons;
i.e. how long will the person be exposed to a hazard, the frequency of such exposures and the opportunity for the person exposed recognising the hazard and taking voluntary avoidance action, in time to prevent an accident,
- duration of the hazard occurrence;
i.e. the window of time that a hazard would last and the probability of the person being exposed to the hazard,
- triggering events and/or conditions that are a prerequisite for the hazard to lead to an accident and the likelihood or frequency of their occurrence that will be transferred to likelihood or frequency in a global perspective,
- different triggering events or a sequence of events or circumstances following a triggering event that could lead to accident scenarios or escalation of an accident with more severe consequences but in a global perspective, may be less likely to occur.

Figure 3 shows a diagrammatic representation of the above factors and accident escalation scenarios. It should be noted that safety barriers or protection measures might be introduced at the level of the hazard or at the level of the triggering event or the accident to mitigate risk. In such cases, in addition to the occurrence of an event, a breach of the safety barrier would also need to occur for the sequence to progress.

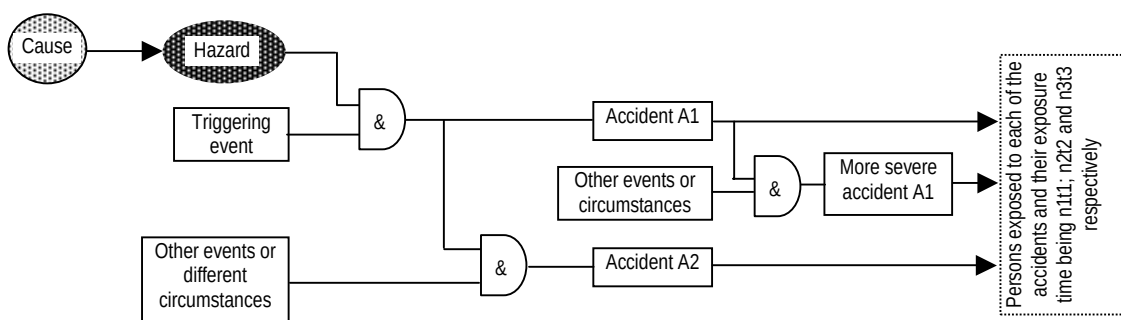


Figure 3 – Sequence of occurrence of accident, hazard and cause

Also, society in general has an aversion to single accidents that lead to catastrophic multiple fatality outcomes. It is therefore important to consider the potential for such accidents within a risk assessment.

4.4.2.1 Human harm

Human harm is a casualty resulting in fatalities, major/serious injuries or minor injuries to passengers, employees or other members of the public. What constitutes a fatality, a major injury or a minor injury is usually defined by statutory/legal regulations of a country. It is therefore recommended that the RA, by agreement with the relevant SRA, establishes a common measure for the project. An example (from EUROSTAT) of what may be covered by the terms is as follows.

- **Fatality:** Death within 30 days after the accident. The accident being established as the main cause of death.
- **Major injuries:** Injuries to passengers, staff or members of the public such that the person injured requires more than 24 hours of clinical treatment. The accident being established as the main cause.
- **Minor injuries:** Injuries to passengers, staff or members of the public, which are not major injuries. Shock or trauma due to witnessing an accident or a near miss may also be classified as a minor injury in some countries.

4.4.2.2 Environmental harm

This refers to damage to neighbouring property, spread of toxic or other harmful agents into the environment, fire, etc., damage being caused as a direct result of the incident. Presently there are no established measures for the level of damage that constitutes environmental harm. Most railway safety studies tend to concentrate on human harm. However, it is recommended that its exclusion be agreed between the RA and the SRA. If it is to be included, then a measure should also be defined.

4.4.2.3 Commercial harm

This refers to damage to property/assets belonging to the stake holders or damage to the reputation/ridership of the operation. It is a commercial issue and although included here for completeness of safety concepts, it is not usually included in safety studies.

4.4.3 Risk normalising

The concept of normalising is useful for ensuring that the units and the base measure for the safety data are consistent for the communication and comparison of risk. For example, rate of occurrence of harm would depend on the population effected (e.g. number of employees involved in maintenance, no of hours worked, etc.), traffic density, train-km, passenger-km, train or passenger-hours, number of journeys, number of trains run, topography (e.g. number of tunnels, bridges, level crossings, etc.). Following subclauses summarize normalization base.

4.4.3.1 Rate of events (reference base for probability of occurrence)

It is recommended that the basis for the rate of injuries/fatalities to the different groups affected by the railway, for the purpose of processing and comparison only, is agreed between the RA and the relevant SRA or follows generally accepted basis. For example a single figure of collective risk, for the passenger and general public, may be based on cumulative harm per annum for each group. This may also be converted to individual risk.

4.4.3.2 Equivalent fatalities (reference base for harm)

An equivalent fatality is defined in 3.2.6. It is recommended that the relationship between injuries and fatalities, for the purpose of processing and comparison only, be agreed between the RA and the relevant SRA. For example a single figure may be based on treating:

1 Equivalent fatality = 1 fatality = 10 major injuries = 100 minor injuries.

5 Generic risk model for a typical railway system and check list of common functional hazards

Clause 5 introduces the concept of a generic risk model with emphasis on the risk assessment process and guidance on its application and provides hazard checklists.

5.1 Introduction

A railway system exhibits many properties in the course of delivering a transportation service. Amongst the many facets of performance, relating to a railway system or undertaking, safety is generally a more demanding aspect to forecast, manage and deliver. The statutory framework poses further constraints on performance where the potential for harm to people or the environment arising from a product or system is regulated. Whilst traditionally, safety performance has been improved through the expensive lessons learnt from accidents, nowadays, a more systematic approach emphasises focus on root causes and escalation scenarios with a view to developing a deeper understanding of the inter-related issues and tackling the problem more successfully in a proactive manner. In this paradigm, learning from accidents remains a possible but generally undesirable approach to safety.

A systematic approach to safety performance requires an understanding of the risk assessment process together with an understanding of the railway system structure and its interactions with its environment. Description of the risk assessment process is given in 5.3 and the principles of railway system structure and other relevant factors are described in 6.2.2.

Subclause 5.4 gives some guidance for deciding on the depth and type of risk assessment necessary.

5.2 Generic risk model

Modelling predominantly represents a simplification and generalisation of reality but, enhances our understanding of causal relationships, highlights important factors and provides a useful tool for anticipation and potentially prediction of future.

A risk model may be created for a specific task (e.g., occurrence of a hazard, a combination of hazards, an operation, a sub-system, etc.) for a particular application or for a whole railway system by applying the risk assessment process to the relevant task or to the railway system.

Developing a risk forecasting/profiling model for a product, process or system constitutes a major step towards a systematic understanding and proactive safety management. Models naturally represent an abstract perspective of a system and irrespective of its qualitative or quantitative nature, could support safety processes in

- a consistent representation of the system for consultation and endorsement by all stakeholders,
- explicit and often graphical representation of the system elements, its boundary and key external and internal interfaces,
- a structured environment to support safety related decision making whilst delivering a readily comprehensible record for the life of a system.

Most risk assessments tend to consider risk to passengers only. Given that safety risk is about impact on people, it is important that all groups affected are identified and their risks assessed for tolerability. To develop an estimation of safety risks to all groups exposed to an operational railway network, risks to each group should be estimated on a consistent basis i.e. per annum or per journey/train kilometre.

Developing a risk model for a whole railway system is a demanding task and due to the diversity of railway systems with respect to their environments, operations, interfaces with other systems, diversity and quality of data available, complexity of such a model, general availability of integrated modelling tools and the difficulties in validating a large and complex model, the report does not recommend a single generic risk model for a whole railway system. Consequently, the rest of this clause addresses a generic risk assessment process and its application and provides hazard checklists.

Nevertheless, a risk model, using qualitative, quantitative or hybrid basis for assessment, could be applied at different system levels depending on the purpose of the analysis. It may be applied at the very high functional level, for instance, to assess the basic functionality or applied at a lower level to assess the technical solution implemented.

Annex D lists essential steps for building such a model and presents only an illustrative example of a railway system risk-forecasting model.

5.3 Risk assessment process

5.3.1 Introduction

Risk assessment mainly addresses the identification of hazards, evaluation of risks and a judgement on the tolerability of the risks where as risk management involves identification and implementation of cost effective risk control measures and assurance that resources are diligently applied to control and maintain risk at acceptable levels.

Risk analysis is an intrinsic part of the overall system life cycle shown in Figure 8 of EN 50126-1 and should be performed during the different life cycle phases. Subclause 4.6 of EN 50126-1 gives an outline of basic risk concept together with risk analysis, evaluation and acceptance. The term “risk assessment”, as described in the above paragraph, therefore encompasses the terms “risk analysis” and “risk evaluation and acceptance” as used in 4.6.2 and 4.6.3 of EN 50126-1. Therefore, the “risk analysis” during system lifecycle, as shown in Figure 8 of EN 50126-1, should strictly be read as “risk assessment”. Further description of a generic risk assessment process is given in 5.3.2. Guidance for the application of the process and the depth and breadth of analysis is given in 5.4.

Risk assessment, using qualitative, quantitative or hybrid approaches, is a systematic and structured process for

- i) identifying the accidents that may cause injury or death to individuals who are directly or indirectly exposed to the operation and maintenance of a system. In the context of a railway operation this could mean passengers, workers and members of the public,
- ii) identifying the hazards, i.e. the component, sub-system or system failures, physical effects, human errors or operational conditions, which can result in the occurrence of accidents,
- iii) identifying the control measures that are in place to control or limit the occurrence of each hazard that cannot be eliminated,
- iv) estimating the frequencies at which hazards and accidents can occur, where appropriate
- v) estimating the consequences in terms of injuries and fatalities that could occur for the different outcomes that may follow the occurrence of an accident. This would include identifying, where risk reduction is necessary, the control measures that are in place to control or limit
 - the occurrence of each hazard that cannot be eliminated through identification of causes and accident triggers, and
 - the consequences of the related accidents.
- vi) estimating the overall risk associated with major accidents,
- vii) estimating the individual risk associated with exposed group(s), as appropriate
- viii) identifying, where necessary, the additional measures required to ensure that risk is mitigated to levels acceptable by the SRA (e.g. it satisfies the defined risk acceptance criteria)
- ix) providing clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgments and interpretations used in carrying out the risk assessment.

5.3.2 Generic process

The generic process consists, essentially, of two distinct groups of steps as follows:

- a) risk assessment steps comprising:
 - system definition,
 - hazard identification (preliminary and detailed) including hazard log,
 - consequence analysis,
 - risk assessment and allocation of THRs, where appropriate;
- b) hazard control steps comprising:
 - hazard control, including causal and common cause analysis.

Performing the entire process requires expertise of the system, its function, design, operation and maintenance, and the railway environment in which the system will run. The responsibility for the steps within the two groups is primarily determined by the domain of influence of the body/entity over the system or its environment and is generally as follows:

- Risk assessment steps, particularly at the top system level (i.e. railway system level), falls within the responsibility of the RA, as it is under their domain of influence. They would normally have the overall detailed knowledge and understanding of the railway network and its operation. However, the roles and responsibilities may be contracted to other entities (see 4.2) in relation to their accountabilities,
- Hazard control steps, on the other hand, falls within the responsibility of not only the system suppliers within the RSI, who would normally have the system design expertise, but also with the owners, operators and maintainers (may be RA or RSI) – in relation to their respective accountabilities.

NOTE The term “Hazard Control” has been chosen instead of “Risk Control” because it contains, in principle, no assessment and statement of risk levels whilst the term risk control does. This distinction between hazard control and risk assessment then also mirrors the organisational responsibilities for the respective steps.

Assuming that a system has been defined and the system boundary established, an illustrative example of the risk assessment and hazard control steps is given in the flow chart shown in Figure 4 and Figure 5. Activities involved in each of the process step are described in 5.3.2.1 to 5.3.2.6 below.

The risk assessment and hazard control steps are inter-related and part of the overall risk assessment process. However, they address different aspects of the life cycle and of the domains of influence.

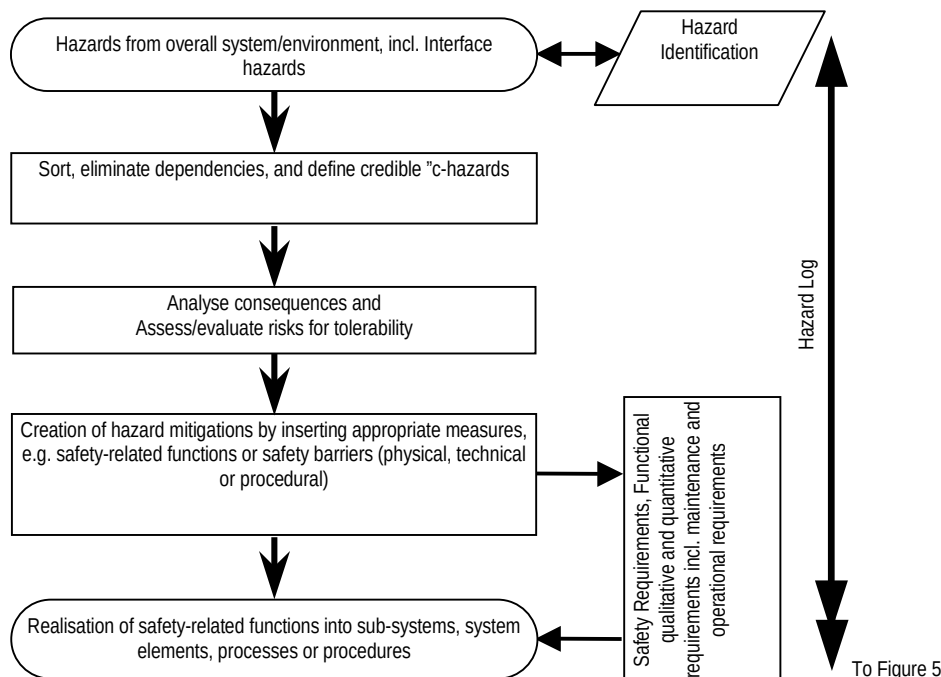


Figure 4 – Risk assessment flow chart

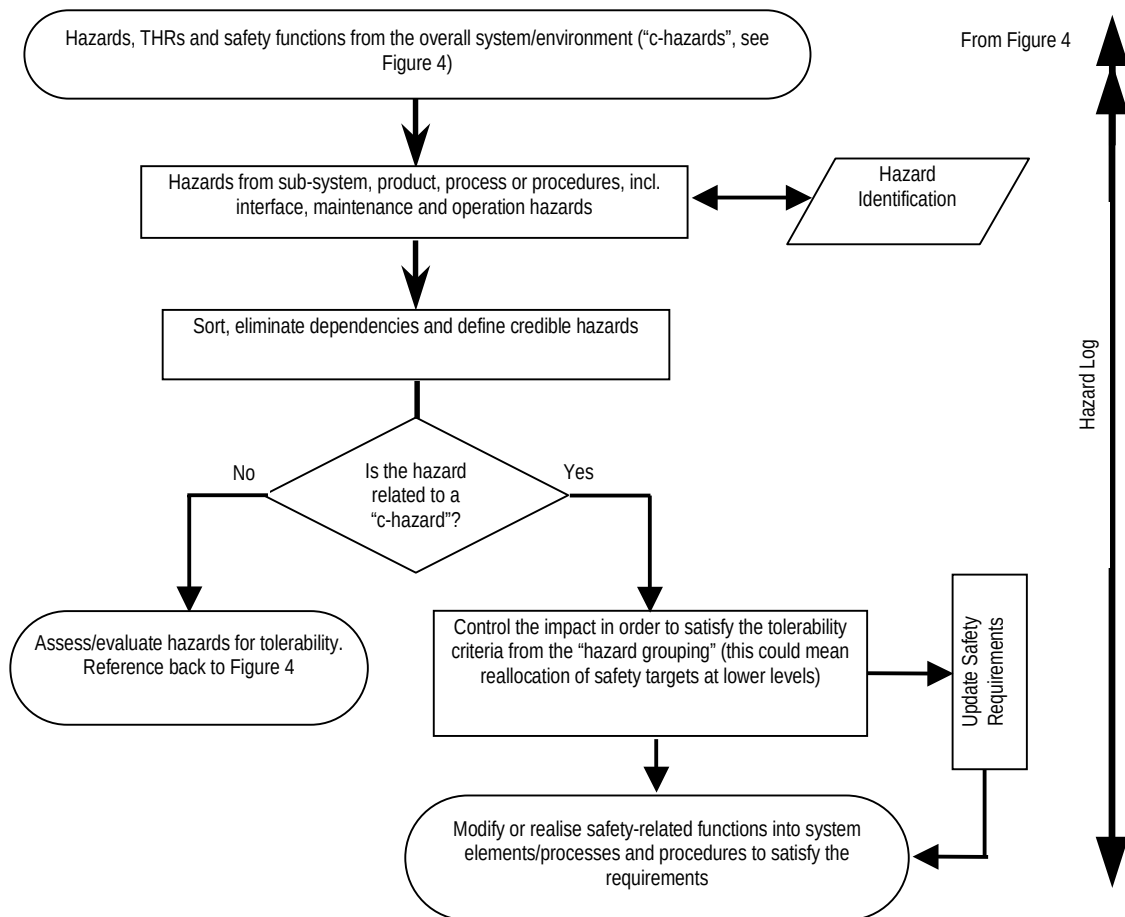


Figure 5 – Hazard control flow chart

5.3.2.1 System definition

Clearly define the system and its physical and logical boundaries (i.e., interfaces with other systems and with its environment). Understanding the boundary between a system and its environment is a pre-requisite to understanding how the system might contribute to an accident. Environment consists of anything that could influence, or be influenced by, the system. This includes anything to which the system connects (mechanically, pneumatically, electrically, etc.) or interacts with through electromagnetic interference, pressure pulses, thermal interchange, etc. Environment also includes people and procedures that can affect, or be affected by the system and its operation.

Further explanatory information for system definition is given in Clause A.1.

5.3.2.2 Hazard identification and preliminary hazard analysis

Hazard Identification is fundamental to the risk assessment process. All best practice models for safety engineering and management emphasise hazard identification as a key step in the overall safety assurance. Absence of a systematic and comprehensive hazard identification phase can severely undermine the risk assessment process. In the worst case this can create an illusion of safety and a false sense of confidence.

Hazards are systematically identified, ensuring that people, processes and system operating modes (normal, degraded and emergency) are taken into account and the results collated and documented. These are subsequently analysed to eliminate dependencies and to assess their ranking in terms of the impact of each hazard. The results, at railway system level, define a set of credible “c-hazards” of different severity levels. Note that the systematic process enhances confidence in the completeness of the hazard identification but does not guarantee it.

All involved parties should agree the actual scope of a hazard identification exercise. As in some cases, it may be appropriate to limit the analysis to those hazards leading to personal injury while in other cases (e.g. transport of dangerous goods) it might be more reasonable to also include other types of harm.

Once identified the hazards should be listed. The record of hazards is usually maintained in a Hazard Log (see 5.3.2.3)

Each hazard is usually associated with several causes. If a large number of hazards have been identified, it should be checked to see that multiple causes of a single hazard have not been separately identified.

To focus risk assessment effort upon the most significant hazards, a preliminary hazard analysis should be performed to rank the hazards in order of their risk. Subsequent stages of risk assessment, as detailed in this report, should be applied on a prioritised basis, beginning with the highest-ranking hazards. The relative rank of each hazard should be used to guide the breadth and depth of its further analysis. A simple frequency of occurrence and hazard severity level matrix, for example, as shown by Tables 2 and 3 of EN 50126-1, could be employed. Note that such matrices are more appropriate for risk ranking than for assessment. For assessment purposes it would be necessary that the risk matrix is calibrated for the specific application.

Further guidance on hazard identification is given in Clause A.2. Guidance on hazard structures and checklist of common functional hazards is given in 5.5.

5.3.2.3 Hazard Log

Hazard log is a tool to document identified hazards together with measures and actions taken or to be taken for their mitigation to tolerable levels. It includes measures that will form a source for establishing safety requirements for implementation at other system or subsystem levels. A hazard log may be contained in any suitable database (electronic or paper based) as long as an appropriate process exists, such that the hazards get a classification and a list could be extracted. It is also appropriate that the log covers a “class” of systems/subsystems/products of similar assembly in order to cover events that need corrective action in several technical related applications.

From an initial status of the log containing preliminary hazards identified at the start of a project, the hazard log is amended or extended to include any further hazards identified during the system's life cycle. In addition the log should also document the processing of the hazards, i.e. their evaluation (directly or by reference) and the measures selected for removal, reduction, containment of the hazard or mitigation of its effects to achieve safe operation of the system.

It is recommended that as part of top level safety management a process is established for the management of the hazard log e.g. duty holders responsible for its maintenance, upkeep, data dissemination, etc., during the different life cycle phases and the transference of such responsibilities as the project moves through its life cycle phases. The log should also reflect the status of the hazards as to whether these are managed, transferred or eliminated.

Overall, a hazard log is a live document/database and is central to the risk management process and therefore its design, operation, upkeep and maintenance together with the responsibilities require careful attention. However, the extent and detail to be covered will depend on the size and complexity of the project and a common sense approach, supported by the SRA, should be considered.

An example of the contents to be recorded in a hazard log is given in Clause A.3.

5.3.2.4 Consequence analysis

Consequence analysis involves establishing intermediate conditions or events and assessing the hazard development scenarios to estimate the probability of a “c-hazard” resulting in an accident (taking into account any accident triggers and/or likely events that could escalate the associated losses) and the extent of the likely losses arising from the accident. For instance, following a train derailment there could be a bridge collapse onto a train, a fire or a toxic goods release.

Further explanatory information for consequence analysis is given in Clause A.4.

5.3.2.5 Risk assessment and allocation of THRs

Risk is evaluated and assessed against risk acceptance criteria either derived from or based on legal or other requirements (such as, e.g., prevailing legal requirements, existing technical standards, existing safe systems or processes, etc.), agreed by the SRA. Further information on the use of technical standards or reference systems as approval criteria for safety demonstration is given in 7.1. Measures are then implemented to safeguard against unacceptably high risks by introducing risk reduction and/or risk

avoidance measures to mitigate the risk to an acceptable or tolerable level based on the risk acceptance criteria. Note that risk acceptance criteria can also be expressed qualitatively.

From an estimate of the accident rates and the tolerability of the losses associated with that accident, numerical value of the rates for the identified hazards are recalculated to give the tolerability criteria for each of the hazards. These are regarded as THR (Also see 6.3.3). THR then form the input for hazard control.

However, there are areas where it is difficult to establish THR values, e.g.,

- for mechanical parts that rely on material endurance and design tolerance properties over a stated product lifetime,
- for hazards arising from electricity that rely on technical measures in the design to avoid electrocution, induced voltages, etc. The measures may depend on insulation and earthing design, in which case, they could have a failure frequency and a measurable hazard rate.
- in the area of operational rules (including operating staff, maintenance workers, etc.), where it may be almost impossible to establish a THR.

In conclusion, a justification should be provided, both for when applying THR and for when applying THR is not appropriate.

The RA, as the body responsible, would perform the risk assessment at railway system level and from the results of the assessment would also define THR for common applications of common systems, i.e., the maximum acceptable rates for the occurrence of the hazards that are consistent with their legal and regulatory constraints and corporate safety objectives.

5.3.2.6 Hazard Control

The system chosen together with its implementation and safety measures should satisfy all the safety requirements (including THR requirements), e.g., by inserting specific safety functions, protective measures, safety barriers, etc. The system is then analysed using causal analysis for possible contributors to the hazards at system boundaries and for identifying any other hazards or interface hazards. Further risk assessment may be needed to take account of any new hazards identified. It should be noted that a causal analysis might reveal many causes that could lead to a hazard. Similarly, a single hazard may lead to many accidents. Common-cause effect analysis (CCF) also plays an important part in claiming independence of the inserted safety measures (further information is given in Clause A.5). SI requirements can then be derived and allocated to a function. The process can then be cascaded down to lower level systems (for further guidance see 6.4).

Further guidance on the public domain tools and techniques available and applicable to the process are given in Annex E.

5.4 Application of the risk assessment process

The generic process presents a uniform framework for assessment of the full range of risks associated with any given undertaking. Within this framework, the assessment may be performed to different depths using qualitative, quantitative or hybrid approaches. Some risks cannot adequately be evaluated without a structured approach to risk assessment, whilst many might be suitable for assessing using a ranking matrix.

All risk assessments contain uncertainties and therefore their results can only be used as a guide to the level of risk within the bounds of the uncertainty. The results of such assessments should therefore only be used as an input into decision-making and should not be the sole basis for making a decision. A sensitivity analysis could also be used to support the decision.

Personnel with a full range of competencies required to consider the whole operation in detail (e.g. the necessary system and domain knowledge and experience) should be involved within the risk assessment process, particularly in relation to the hazard, accident triggers, escalation scenarios, and accident identification and in relation to tolerability assessment stages.

The following subclauses summarise some of the advantages and disadvantages of the different assessment approaches and provides guidance for determining the extent of analysis that may be appropriate for demonstrating safety during the different life-cycle phases. However, these must be included in the relevant, phase related, safety plan and be subject to acceptance by the SRA.

5.4.1 Depth of analysis

Although EN 50126-1 is applicable to a complete railway system or to its subsystems, the extent of analysis necessary to demonstrate safety will depend on subsystem under consideration, the level of its proven record in use, novelty of its design or application, environmental differences, system boundary condition differences, interface differences and the level of risk posed. Work necessary to demonstrate safety should therefore be suitable and sufficient to these levels. The safety plan should specify the required depth of analysis to be conducted or a method for determining it.

The level of detail in a risk assessment should be broadly proportionate to the risk. 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 suitable and sufficient risk assessment should reflect what is reasonably practicable to expect to be known about hazards on the railways and those associated with the technology applied (e.g., functional and technical safety). When it is practical to do so, risk assessments should be correlated with historical records of accidents and the records of causes.

The definition of what constitutes “suitable and sufficient” is difficult to establish owing to the wide range and scales of operation such risk assessments have been applied to. Care should be taken not to exaggerate the level of sophistication needed. Also see 7.1 for guidance on safety demonstration approaches.

The risk assessment process adopted should be capable of addressing both qualitative and quantitative methods, ideally based on a framework, which inherently supports both approaches.

Qualitative risk assessment is likely to suffice for most hazards. Risk ranking (see Clause A.6) can be used to determine which risks need to be subjected to further, more detailed, assessment. A sensitivity analysis (see 5.4.5) may also be undertaken to gain an appreciation of the extent to which detailed assessments may be necessary. However, hazards, with the potential to lead to major or catastrophic consequences, may require full or partial quantitative risk assessment in order to establish the extent of the risks and assist with systematic risk reduction. Where quantitative safety requirements are necessary (e.g. for signaling as per EN 50129), a quantitative risk assessment would be needed. A quantitative approach may also be justified for novel systems where there is insufficient experience to support an empirical, qualitative approach.

Use of quantified risk assessment should be considered for the more substantial cases. It can be particularly difficult to assess risks, where the types of accidents with severe consequences occur rarely, e.g., catastrophic railway accidents. The frequency and severity of some accidents can be particularly sensitive to aspects for which little is known. For such cases it is important to give due recognition to uncertainty.

However, it should be emphasised that it is the qualitative aspects of the risk assessment, and the dissemination of this information throughout the stakeholders (bodies/entities) involved in the system that provides significant potential benefit from the risk assessment, in terms of

- improved awareness of such events,
- the ways in which failures can be prevented, controlled or managed, and
- the consideration of additional control measures.

If the risk is low and completely covered by a standard or authoritative good practice, then showing that this has been followed may be enough to show that the risk is acceptable. For example, certifying it against pressure vessel standards normally shows the safety of a pressure vessel for use in brake air reservoirs. However, before deciding that just referring to standards is enough, it must be ensured that

- the equipment is being used as intended;
- all of the risk is covered by the standards; and

the standards cover the particular application. This applies only to the relevant equipment covered by the standard and does not imply that the risks in the system in which the equipment is used are also covered.

5.4.2 Preliminary hazard analysis

Preliminary hazard analysis is a first-pass hazard identification and risk analysis. Carried out at the start of a project, it consists of annotating identified hazards with an initial appraisal of their probability and consequence severity and is intended to determine:

- a) the scope and extent of risk represented by the project, so that the risk assessment process may be applied to an appropriate depth;
- b) a list of potential hazards that may be eliminated or controlled during initial design activity.

At the start of a project, design detail will almost always be limited, so the results of preliminary hazard analysis (in particular the depth of analysis) should be backed up and re-assessed by carrying out a full risk analysis and assessment as soon as detail is available.

Preliminary hazard analysis should be carried out before any significant design activity begins. It requires a full high-level description of the system's function and construction and its interfaces to people and other systems.

The risk analysis activity carried out during preliminary hazard analysis should consist of annotating identified hazards with an initial appraisal of their severity and likelihood. Ideally, the preliminary hazard analysis should support the process of initial safety requirements setting and, therefore, should provide targets for the likelihood of each of the identified hazards.

The results of a preliminary hazard analysis would enable a risk-ranking matrix to be created (see Clause A.6 and Table E.2). It should be used to decide where further detailed analysis (qualitative or quantitative) is required.

As decisions on the scope, functionality and design of the system are taken it is possible to improve the identification of hazards, to analyse their causes and consequences and, eventually, to assess the risks.

In each phase of the project, the analysis should be taken as far as the available information permits, in order to provide the best support for decisions taken during that phase. For example, during implementation, maintenance and operation of the system new hazards may arise. It would then be necessary to reassess the risks associated with these hazards.

5.4.3 Qualitative and Quantitative assessment

The risk assessment process, described in 5.3.2, is based on a framework, which inherently supports both qualitative and quantitative approaches for assessment and capable of addressing both methods.

Qualitative risk assessment is appropriate for systematic failures and as a first pass subjective judgment. Quantitative risk assessment can only be used for random failures. It is also possible to adopt hybrid approaches, e.g. semi-quantitative.

It is acceptable, in the above approaches, to adopt approximations provided that they are sensibly conservative, that is that they do not under-estimate risk.

Besides the above approaches that may be used to determine safety requirements, assessment of risk can also be performed, in a qualitative manner, by applying safety requirements based on, for example, existing technical standards, similar approved safe systems, credible past experience, domain expert judgement, etc.

5.4.3.1 Qualitative assessment

Qualitative risk assessment relies mainly upon domain expert judgment and credible past experience. It addresses the risks of an undertaking in a subjective and coarse manner. It should be done, by applying the risk assessment process, to a depth sufficient to enable a realistic subjective estimate to be made of the likelihood of the hazard. There is not a complete lack of quantification but estimates in orders of magnitude are generally used. Its advantages are that

- it does not require detailed quantification, data collection or analytical work,
- it is relatively simple, and
- it is less expensive than quantitative risk assessment.

Its disadvantages are that

- the assumptions require thorough documentation, and
- it may be inadequate as the sole basis for assessment of major risks, including those arising from low loss incidents of high frequency, as well as from low frequency incidents associated with high losses.

Risk graph

Risk graph method, as described in Clause E.10 is another qualitative approach used for determining safety requirements for safety critical functions. However, the method requires that the parameters indicated in Clause E.10 and their weightings are accurately defined for each specific situation in the railway sector. Since no such European or International consensus exists in the railway sector, this report is unable to recommend the method. Therefore, its use in railways should be considered with caution and only by agreement with the SRA and the project stakeholders.

5.4.3.2 Quantitative assessment

Quantitative risk assessment should aim to minimize the significance of uncertainties. It employs rigorous analytical processes. Whilst based upon the same fundamental principles as qualitative risk assessment, quantitative risk assessment will typically employ modelling (e.g. Fault Tree Analysis, Cause Consequence Analysis, etc.) using

- objective and validated data,
- explicit treatment of the uncertainty associated with input data, and
- explicit treatment of the dependencies between significant factors contributing to risk.

Its advantages are that

- it is more accurate than qualitative risk assessment, provided that sufficiently accurate data is available for the assessment,
- helps with identifying flaws in the design or shortcomings of the safety concepts,
- assists with integration of all risk contributions towards a total profile,
- it helps identify hidden assumptions due to more detailed scrutiny, and
- it provides a better understanding of the significance of potential causes and consequences of a hazard.

Its disadvantages are that

- it is complex,
- it requires a lot of objective data,
- it is not suitable for assessment of systematic failures,
- it is more expensive than qualitative risk assessment, and
- it may require significant resource.

Qualitative risk assessment is likely to suffice for most hazards. However, hazards, with the potential to lead to major or catastrophic consequences, may require quantitative risk assessment in order to establish the extent of the risks and assist with systematic risk reduction. Also where quantitative safety requirements are required (e.g. for signalling as per EN 50129), then a quantitative risk assessment is necessary. A quantitative approach may also be justified for novel systems where there is insufficient experience to support an empirical, qualitative approach.

Quantitative risk assessment is more time and resource consuming than its qualitative counterpart and should only be applied if it is justified by the increased confidence achieved.

5.4.4 Use of historical data

Risk assessment always relies on some form of extrapolation from the past to the future. Historical data is used at many stages. It may also be used to check the validity of a “risk model” when built. But it should be used with care. The reasons for this include the following.

- Insufficient information may be available to determine whether historical figures are relevant to the circumstances of concern, particularly regarding rare major or catastrophic accidents and the circumstances surrounding previous incidents.
- Secondary effects arising from an incident are likely to be difficult to reliably determine (for example fires, derailment or exposure to harmful substances).

Inappropriate use of historical data can undermine the analysis, and significantly reduce the accuracy of risk assessment.

Where historical data is employed in an assessment, a clear argument should be presented that its use provides an accurate forecast of the losses associated with the particular circumstances under study.

5.4.5 Sensitivity analysis

In carrying out any risk analysis and subsequently its tolerability it is often necessary to make assumptions and, due to lack of data, use judgments when quantifying hazard frequencies and probabilities and accident consequences. The results of the overall risk and tolerability assessment may therefore be very dependent on the way in which the assumptions and judgments are made and it is therefore necessary to be aware of the relative importance of these assumptions and judgments within the overall results. A guide to the influence of these assumptions and judgments can be made using sensitivity analysis.

Having completed a risk analysis it cannot be assumed that the results are necessarily correct. It is therefore essential to review the results to make sure that they make sense, e.g.:

- Do the results look believable in terms of overall collective risk, the accidents ranked by risk and the individual risk estimates?
- Are they what you expected?
- How do they compare with the national averages, etc?
- Are the major risk contributors what you expected? If not, is there a rational explanation for the difference.

Whether the results make sense or not, it is important that the specific assumptions and judgments made and recorded within the risk assessment process are examined to determine if there are any for which there is a high level of uncertainty. If there are, then the sensitivity of the results to changes in the assumptions should be checked by asking the question, "if there were a factor of 2 to 5 difference (higher or lower) in the numbers affected by the assumption or judgment, would it make a material difference to the conclusions of the risk and/or its tolerability?" If it would make a material difference, consideration should be given to

- a more detailed examination of the assumptions and judgments to see if more accurate assessments can be made, and if this is not possible
- confirm that the existing or potential additional control measures are sufficiently robust to cater for the potential level of uncertainty.

5.4.6 Risk assessment during life cycle phases

As stated in EN 50126-1, risk analysis, which should be read as risk assessment (phase 3) may have to be repeated at several stages of the lifecycle (also see last paragraph of A.2.4). The following summarises the application of risk assessment process for the different design phases, and for the maintenance and operation phase.

5.4.6.1 Risk assessments during design phase

Design phase is generally covered by phases 1, 2, 4, 5 and part of 6 of EN 50126-1 (phase 3 is risk assessment itself):

Bodies/entities involved:

For system design at the railway system level, it is usually the RA. It is also responsible for setting safety policy, safety targets and safety requirements for its subsystems. At subsystem levels it would be the RSI that is responsible for the design/supply of the system under consideration and for setting safety targets and safety requirements for lower subsystems/equipment (See 4.2 and 4.3). Such safety requirements would also include maintenance and operational safety requirements.

Risk assessment:

At the beginning of a project life cycle there is usually insufficient information to perform a detailed risk assessment and the analysis is usually limited to a preliminary identification of hazards. This is sufficient to support early discussions on the approach to controlling each hazard. Preliminary hazard analysis (see 5.4.2) should be carried out before any significant design activity begins. However, it requires a full high-level description of the system's function and construction and its interfaces to people and other systems.

Risk assessment is iterative. As design progresses, the assessment should be repeated at appropriate stages of design progress, and to an appropriate depth (see 5.4.1), to take account of change and extended to cover the extra detail. The design can then be modified to avoid hazards or reduce risks as soon as they are identified.

Safety plan should record the design progress stages that will be linked to further iteration of risk assessment. The hazard log should also be updated at each stage, to include any new hazards identified and to reflect the status of all the hazards (see 5.3.2.3). Also see 9.5 and phases 1 to 10 in Table 7.

Hazard log:

A hazard log should be established from the earliest stage and maintained throughout the project life cycle phases (see 5.3.2.3).

5.4.6.2 Risk assessment during maintenance and operation

This is generally covered by phase 11 of EN 50126-1. Safety responsibility for these phases would be transferred to the relevant bodies/entities involved (see 6.11 of EN 50126-1)

Bodies/entities involved:

It is usually the RA or its appointed agent. However, depending on the contractual arrangements, a relevant RSI may be required to undertake the task (see 3.1.7 and 4.2), e.g., design, build and operate type of contracts.

Risk assessment:

Hazard log and the safety requirements from earlier project phases form the starting point for controlling risk during maintenance and operation. Safety requirements should include all operation and maintenance information and documentation including information for any specific training and competency requirements and for any specific equipment and facilities where they do not already exist. The bodies/entities responsible for the design and implementation of the project are generally responsible for the provision of such information.

The level and depth of information, documentation and guidance provided would, once again, depend on the levels of complexity and risk presented by the system or the equipment.

The information provided should be supplemented by a maintenance and operation risk assessment and any other prevailing statutory or legal requirements, as part of the maintenance and operation safety case (see 9.5 and phases 11 to 13 in Table 7). This would be carried out by the relevant body/entity responsible for the maintenance and operation. It should be conducted before start of the operation and again as the situation demands it or as dictated by the safety case.

Such information should also include instructions to be followed in the event of a failure, instructions to bring a system in to a safe state while a failure is resolved, maintaining essential functions during a failure, recovery from a failure, other system related tasks for protection and recovery of passengers and assets from an emergency situation, etc.

Operation and maintenance is a very important stage in the safety lifecycle and the potential exists during this stage to have a positive influence on safety. All stakeholders involved in the maintenance and operation activities should fully understand the implications of their tasks on the safety of the system. Safety is every body's responsibility. Any change to the system configuration, maintenance or operation should be fully reviewed and assessed as in some cases the change may effect operation or maintenance activity performed by a different stakeholder (different body/entity or even a different person within the same organisation).

5.5 Check-list of common functional hazards and hazard identification

5.5.1 Introduction

Whilst traditionally, safety performance has been improved through the expensive lessons learnt from accidents, nowadays, a proactive and more systematic approach emphasises focus on root causes and escalation scenarios. In this respect, hazard identification is a key step in the overall safety assurance. Whilst many techniques are employed at individual project level, generic approaches at the system/industry level are rather rare.

Guidance on hazard identification is given in 5.3.2.2 and Clause A.2. Subclause 5.5 provides insight into the different possibilities for building a generic hazard structure. A suitable structure helps to enable systematically addressing the whole spectrum of functions, interfaces, operating scenarios, hazards and events during the hazard identification process.

5.5.2 Hazard grouping structures

Identification of hazards and their potential elimination or consequential risk reduction is one of the most important aspects of the risk-based approach to safety. To ensure an efficient process as well as supporting cross acceptance of safety systems, a commonly used grouping structure of hazards should be agreed.

This structure ideally has to

- cover/address the entire railway system,
- ensure, that the hazard is described at a level to allow the underlying causes to be identified and assigned for subsequent consideration,
- be unambiguous to a high degree,
- support proof of coverage,
- allow the allocation of responsibilities for each hazard and its causes,
- enable the apportionment of quantified safety targets.

The structure

- could be used by RA or RSI.
- supports the allocation of risk targets to system hazards and the further apportionment of THRs down to lower functional levels,
- increases the efficiency of the hazard identification and hazard close out process,
- establishes a standard to allow better comparison of safety analysis results.

Unfortunately, defining a structure under consideration of all the needs of all parties involved is an almost impossible task. Currently, safety practitioners are faced with either unstructured lists or many types of structures from different points of view. A commonly acceptable grouping structure may not be achievable.

However, there are several different approaches for hazard grouping structures at railway system level, each having its specific advantages and disadvantages. Also the grouping structure has to be detailed further down to lower functional levels to accommodate the requirements of the stakeholders involved.

Some examples of grouping structures are given below.

- i) Hazards grouped according to the main constituent parts of a railway system (logical breakdown of a railway system). Similar to the EU safety directive e.g., Infrastructure; Energy; Rolling Stock; Control & command and signalling; etc.
- ii) Hazards grouped according to responsibilities, e.g., RSI; Operators; Maintainers; Other duty holders; etc.
- iii) Hazards grouped according to operation modes in which they occur, e.g., Normal; Degraded; Exceptional; etc.
- iv) Hazards grouped according to their effects on the system, e.g., Hazardous full or partial loss of operational functions; Full or partial loss of potential functions; Adverse effect on human health conditions; Inherent effects of the technology used (mechanical power/energy; electrical energy/effects; thermal energy/effects; sound/air pressure effects; electromagnetic/electrostatic effects; chemical effects; biological effects; radioactivity); etc.
- v) Hazards grouped according to the potential groups affected, e.g., Passengers; Railway workers; Railway neighbours; Environment; etc.
- vi) Hazards grouped according to the accident types to which they may contribute, e.g., Collision; Derailment; Striking obstacles on the track or at level crossings; Fires; Explosions; Electrocution; Other impacts/accidents inside a sub-system (rolling stock, station, etc.); etc.

When using any of the above, at least some of the groupings may have to be combined, typically in a hierarchical structure. This could lead to a multitude of possible hazard structures. All structures, assuming that they are not unstructured lists, suffer from the difficulty that hazards can be placed into more than one group, e.g. a brake system failure could lead to a collision or a derailment and it may affect passengers, workers, railway neighbours and the environment.

Consequently, duplications occur and difficulties may arise when making an apportionment of requirements for these hazards or when the overall risk associated with a hazard has to be calculated. This is a deficiency of all hazard structures that have been reviewed for this report (including the examples listed in Annex B).

Since hazard identification is a key step in the overall safety assurance, it is important that the grouping is not restricted to any one structure. Grouping structure or combinations chosen may depend on the users perspective (e.g. system level, system designer, operator, etc.) or on the availability and viability of past data.

For avoiding duplications the ideal solution would be to develop an n-dimensional hazard structure. Such a structure would be too complicated to handle and a suitable trade-off has to be made. In order to satisfy as many hazard structure requirements as possible, examples of two different generic hazard structures is given below.

- One potential hazard structure at railway system level was derived through a holistic study of a full railway infrastructure and operations and is shown in Clause B.2. This study led to the identification of key hazards to the safe operation of the railways from Passengers, Workers and Neighbours perspective. In view of the large numbers of hazards identified, these were aggregated into higher-level groupings referred to as “c-hazard” in order to simplify and rationalise hazard analysis without losing coverage.
- Another potential hazard structure at railway system level, shown in Clause B.3, combines the following two groupings:
 - Hazards identified from a functional perspective, and
 - Hazards identified from the perspective of inherent properties, e.g. overheating/smoke/fire, electromagnetic interference, etc.

Functional hazards are defined in a generic way, which allows their application to the different railway system constituents. For example, the functional hazard “safe stay impaired” relates to passengers in a train as well as to the operating personnel in signal towers.

Inherent properties perspective becomes necessary for hazards, which are not related to a specific function but to the inherent properties of the technology used (i.e. technical safety and not functional safety, see 6.2). For example, a door control unit may cause electromagnetic interference but this is not due to the door control function but due to the nature of the equipment used (electronic microprocessor unit).

5.5.3 Check-list of “Hazards”

General check lists for hazard identification are provided in Clause B.1. Clause B.2 provides, as an example, a checklist of “c-hazards” derived from a strategic study conducted for a specific railway. The hazards have been identified as a generic exercise at the whole railway system level and are generally independent of the specific causes i.e. functional and technical failures. Furthermore, the hazard identification carried out at railway system level has been output focused i.e. based on the specific groups of people exposed to risks from the operational railway.

Clause B.3 provides, as an example, a logical approach for identifying hazards, structured on a functional basis and augmented by hazards from the inherent environmental properties. It also provides a link between the functions and the main subsystems of a railway system. However, it is an example only and should not be treated as a comprehensive list.

Checklists of hazards at railway system level are intended as a complementary support tool for a project or product specific hazard identification and not a replacement for this essential safety activity. Once the system constituents, boundary and interfaces are defined and preliminary or detailed hazard identification at functional or implementation level is carried out, it is advisable to identify the particular groups at risk from the system and verify the completeness of the identified hazards against the checklists. Any potential gaps recognised through this exercise should be addressed so that a complete portfolio of hazards for a particular product, process or system is generated. This exercise would result in a comprehensive identification of the likely mechanisms for harm to people that is fundamental to engineering and deployment of safe systems.

6 Guidance on application of functional safety, functional safety requirements and SI targets, risk apportionment and application of SILs

6.1 Introduction

The activity of establishing safety requirements follows and builds on the work carried out during hazard identification and analysis and risk assessment (see 5.3 and 5.4). Estimating safety requirements is an iterative activity to reflect the iterative nature of risk assessment. Therefore, some overlap and duplication in the description of activities between the different clauses of this report is inevitable.

The depth and extent of establishing safety requirements, as for the risk assessment, also depends on the nature, complexity, and level of the risk presented by the system under consideration.

Subclause 5.4 provides guidance on the application of the generic risk assessment process. Clause 6 provides information on the derivation of functional safety requirements and SI for a system under consideration and on the application of SILs.

6.2 Functional and technical safety

Functional safety is defined in 3.2.8. The key to understanding the difference between functional and technical safety is the concept of system characteristics that satisfy the functional and technical requirements. This is explained as follows:

6.2.1 System characteristics

Firstly, a system is implemented to fulfil certain functions that are fundamental to the system and the prime reason for its creation. Depending on the system design, additional requirements may also be needed to ensure proper functioning of the system.

The fundamental requirements and the additional requirements together are referred to as “Functional requirements”. They express the behaviour of the system and may also need to be complemented by properties qualifying its level of performance (e.g. reliability, safety, accuracy, timing, etc.). Furthermore, the relation between the system and its environment may need to be further qualified by means of contextual requirements (i.e. the operating and maintenance conditions as given in Figure 4 of EN 50126-1). They would address issues like the system mission profile, maintenance and logistics, human factors (e.g. personal qualification), procedural environment, costs, etc.

Secondly, the technical implementation of the system may generate further requirements that do not derive from the system functions but from its technical implementation. Such requirements are referred to as “Technical requirements” in this report. They impact the system build. Technical requirements may address issues such as maintainability, environmental conditions, potential threats created by the technology/equipment regardless of their intended functions (e.g. presence of sharp edges, presence of electric voltage, presence of combustible material, etc.).

Finally, detailed design involves engineering the sub-systems and equipment that implement the functional requirements of the system under consideration. It leads to refining the functional requirements to ensure compatibility between the different sub-systems / equipment, and to implement the refined functional requirements whilst enforcing the technical and contextual requirements. See 6.2.2 below for a railway system structure for implementing the functional requirements.

Characteristics of the system and its constituents (user-related characteristics, derived from the functional, technical and contextual requirements) ensure compliance with the requirements. Implementation of the system (i.e. the technical solution) is then likely to give rise to additional characteristics (referred to as implementation characteristics) introduced by the design.

6.2.2 Railway system structure and safety requirements

A typical hierarchical system structure for a Guided Transport System (railway system) is given below. It is essentially a hierarchical breakdown into physical subsystems. The subsystems proposed at each level are typically those that are often independently procured in the traditional rail market and are also based on tradition. The European safety directive also breaks the railway system into similar subsystems e.g.:

- Infrastructure (e.g., track, stations, points, level crossings, civil works, etc.),
- Energy (e.g., power supply, overhead catenaries supply, sub stations, etc.)
- Rolling Stock,
- Control, Command and Signalling.

There is some merit therefore, in mapping the safety requirements and SI, derived from the decomposition of the functional requirements of the railway system, to these subsystems. However, this may not always be practicable (see 6.3.2) and requires that their boundaries, boundary conditions and contents are clearly defined.

Based on the concept of system hierarchy (4.3.1), it would then be the task of the body/entity responsible for each of the subsystems (Infrastructure, Rolling Stock, Energy, Control, Command and Signalling, etc.) to map the safety requirements to their subsystems/components. Once again the boundaries and boundary conditions of each of the subsystems/components must be clearly defined. It is often helpful for this task to be carried out with the cooperation of the responsible body/entity of the subsystems/components to ensure that the requirements and targets are practicable. This process may require several iterations to ensure that the overall system is optimised.

6.2.3 Safety related functional and technical characteristics and overall system safety

At the railway system level, the basic functions, i.e. those that are fundamental to the system and the prime reason for its creation, are typically as follows (this is indicative only and for a passenger operation):

- movement of persons on a station (for various activities) and to a platform;
- transfer of passengers between station platform and train;
- services and facilities for passengers, whilst on the train;
- train movement.

There are other basic functions associated with energy flow, fare collection, etc., that are not basic, in the strict sense, but needed for the proper or safe functioning of the system.

The architecture and the technical choices for the implementation of the railway system will determine the functional and technical requirements for the subsystems. These choices, when cascaded further down, will determine the functional and technical requirements for the lower level subsystems and equipment.

Safety of a system is dependent on its characteristics (user-related as well as technical), and of their potential for creating hazards. Characteristics may be safety-related (if they have potential for creating or contributing to a hazard) or non safety-related. See A.2.3 and A.2.4 for identifying hazards and determining safety related characteristics, Clause B.3 for an example of functional and technical hazards and 6.3.2 for different approaches to apportionment of safety targets.

Hence the objective of functional and technical safety is to satisfy

- that the functions of the system, as designed and constructed, generate an acceptable level of safety (referred to as functional safety), and
- that its implementation does not give rise to undesirable/unacceptable characteristics (referred to as technical safety).

Safety related characteristics could also be categorised according to the modes of activation of a hazard as follows.

- Characteristics that are inherently hazardous: they are generally related to the system mission. For example, at a level crossing, the interaction between rail and road traffic creates an inherent risk of collision between rail and road traffic.

- Characteristics that become hazardous because of internal system degradation (e.g. failure of one of the components, excessive wear, etc.)
For example, the existence of a failure mode such that the train detection device used to control the level crossing does not detect passing trains.
- Characteristics that reveal hazardous traits because of an inappropriate response to external threats or stimuli
For example, a traction transformer may fulfil its mission, but have a combustible load (quantity of heat energy released in case of fire) that will threaten the lives of the passengers if the train is on fire in a tunnel.

Any functional and technical requirements for the system under consideration or its subsystems and equipment that are necessary to reduce risk to an acceptable level should be incorporated as qualitative safety requirements. These may contain SI requirements, which may be defined as quantitative or qualitative requirements.

They may also include other qualitative safety requirements such as conformance to external standards, relevant regulations, codes of practice, etc., which should be included whenever:

- a) such conformance is assumed in the calculation of safety targets; or
- b) such conformance is otherwise required to reduce risks to an acceptable or tolerable level.

Safety requirements are therefore qualities that should be inherent in the implementation of the system (functional, technical and contextual). Their fulfilment is implicit in achieving safety and should be proven before in service operation.

NOTE Overall system safety implies taking a holistic view of the performance of the system under consideration. In this respect, safety cannot be separated. The different aspects of safety, i.e., functional, technical, procedural and human factors are interrelated and therefore should be addressed as a whole and should also form part of the safety case, as appropriate.

6.3 General considerations for risk apportionment

6.3.1 Introduction

The overall degree of harm, which is considered tolerable by the society, is often regarded as the system's target safety performance. This arises from many factors including infrastructure and rolling stock sub-systems, operations, human factors, etc. If the contributions to the total safety performance is known or estimated, it may be possible to apportion the required system safety performance to the contributory sub-systems hence setting a target safety performance for each sub-system. Target safety performance, in this context includes the safety requirements as described in 6.2 above but also quantified "safety targets". It is necessary that where required, safety targets are Specific, Measurable-using accident/incident databases via defined indicators, Achievable, Realistic, and attained within a required period of Time (SMART).

Although theoretically possible, it is a daunting task and currently there is no adequate method for undertaking a reasonable, undisputable apportionment of safety requirements and safety targets for a complex system like a railway. However, some of the approaches that could be applied to different system breakdown levels are briefly described in this clause.

6.3.2 Approaches to apportionment of safety targets

Before safety targets can be apportioned, the overall safety target valid for the whole system must be defined. As a good practical starting point, also confirmed by risk acceptance principles like GAME (GAMAB in EN 50126-1), is the current "state of the art" expressed by a statistically achieved safety, e.g., the number of accidents within a defined period of time (normally one year of operation) and its relating volume of operation (train kilometres, passenger hours, etc.). For guidance on GAME and other risk acceptance principles see Clause 8.

The overall safety target may be for the overall risk profile or individual risk requirements resulting from all likely accidents and accident scenarios or for specific accident situations.

Allocation of target or an acceptable risk level for the various parts of the railway system requires first a breakdown of the railway system into various risk classification categories, and then the assignment of a target or acceptable risk level to each category. Such a process is also called risk apportionment.

Safety requirements and safety targets, at any system level, may be based on data from existing systems or may have to be derived from other studies. Where a similar system exists, then it is often pragmatic to derive safety requirements and targets from this system. However any differences, functional, technical, operational or in the application environment (e.g., system boundaries and boundary conditions, maintenance and operational competence levels, functional and technical interfaces with other systems and with its environment, etc.), and the effect of the differences on the safety performance should be evaluated for acceptability.

There are several ways of classifying risks depending on their various characteristics. Considering the state of the art in this subject one can identify roughly 5 distinct approaches for the classification of risks and derivation of acceptable risk levels for parts of the railway system. These are listed below and are similar to the hazard grouping structures (see 5.5.2).

- a) Functional breakdown approach (see Clause C.1)
- b) Installation (Constituent) based breakdown approach (see Clause C.2)
- c) Hazard based breakdown approach (see Clause C.3)
- d) Hazard causes based breakdown approach (see Clause C.4)
- e) Breakdown by types of accidents (see Clause C.5)

However, there is no commonly agreed approach and each has its merits and demerits.

These 5 approaches depend on stakeholder perspective and correspond to different levels of detail that can be focused on when analysing safety of a railway system. The approaches are not exclusive and may be applied in combination. This can be illustrated by Figure 6 showing the hierarchy in a typical safety requirement allocation process.

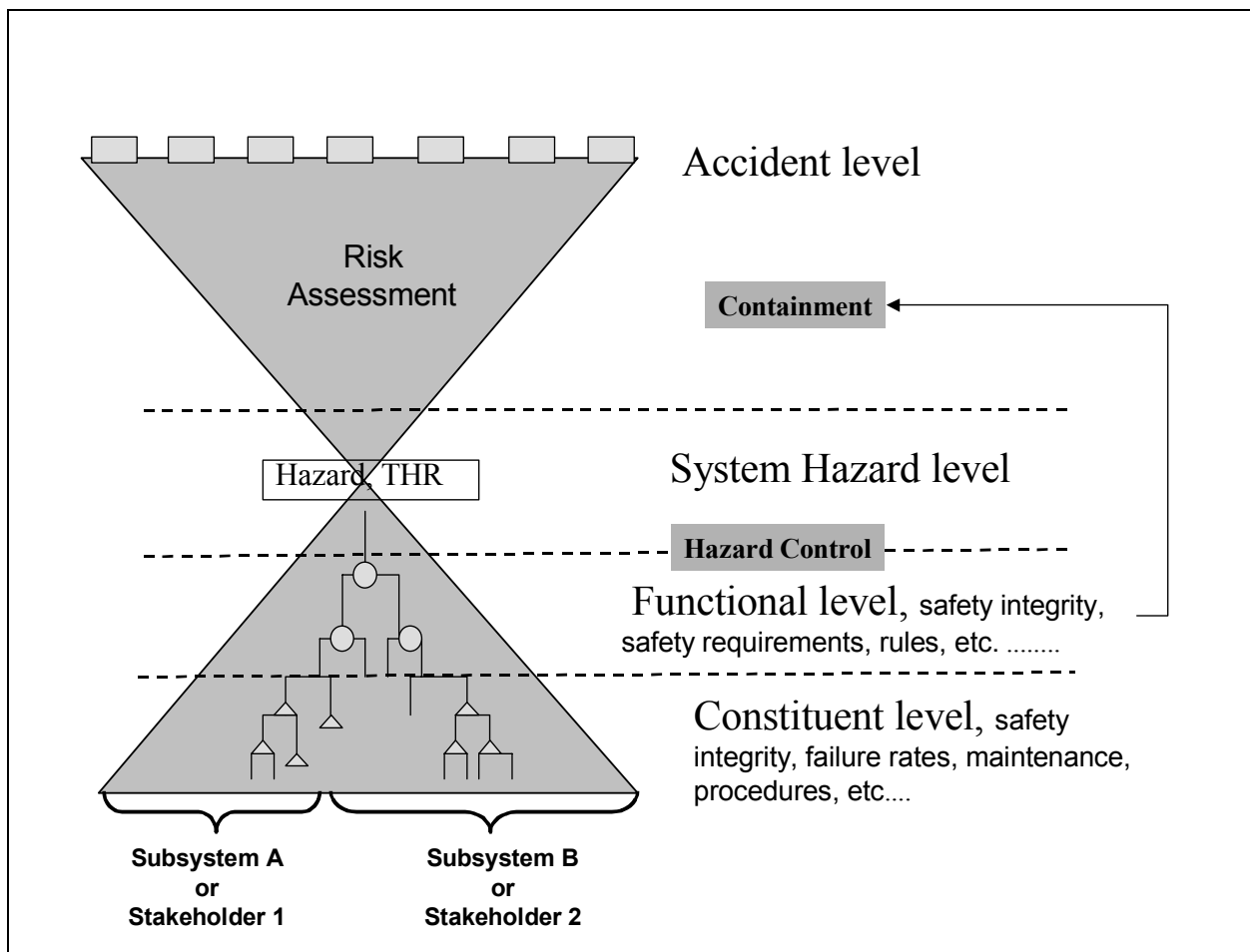


Figure 6 – Safety allocation process