

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.

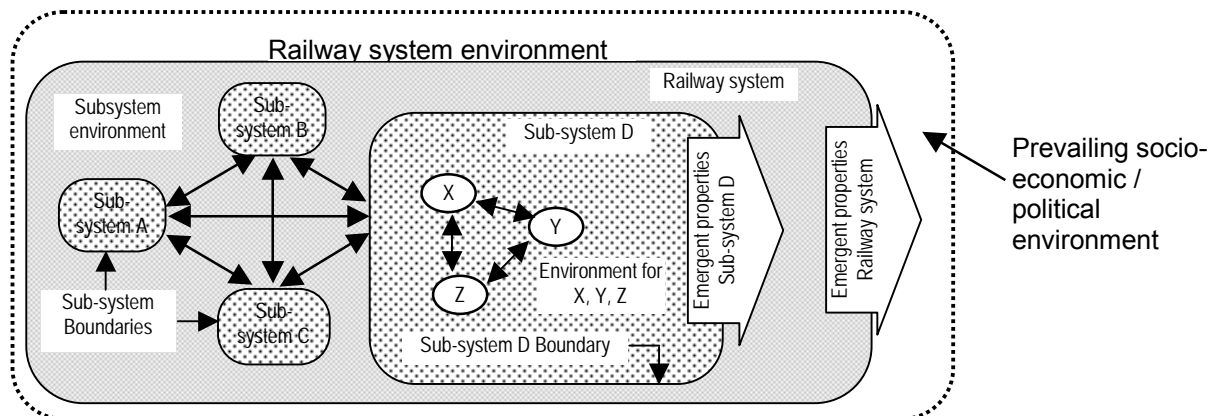


Figure 1 – Nested systems and hierarchy

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:

- a) 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.
- b) 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).

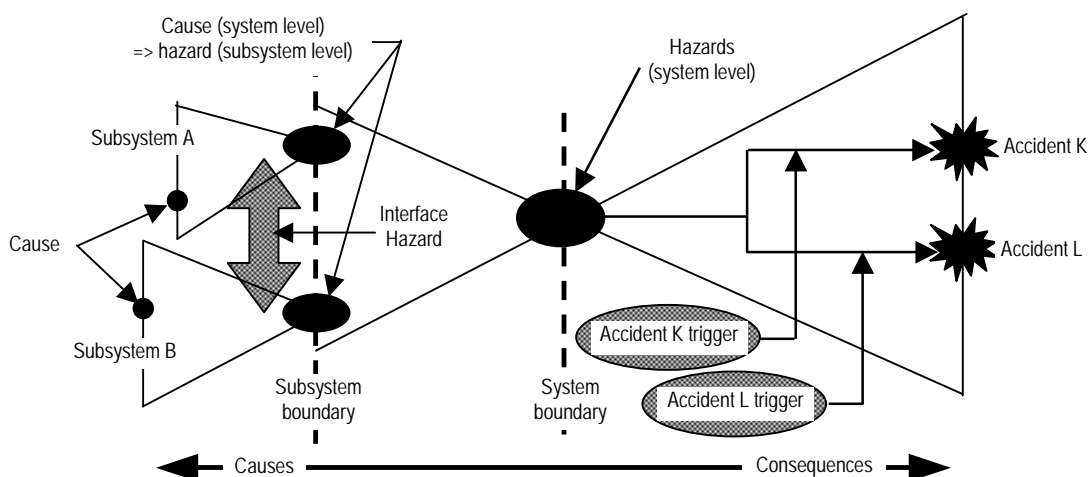


Figure 2 – Definition of hazards with respect to a system boundary and likely accident

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.

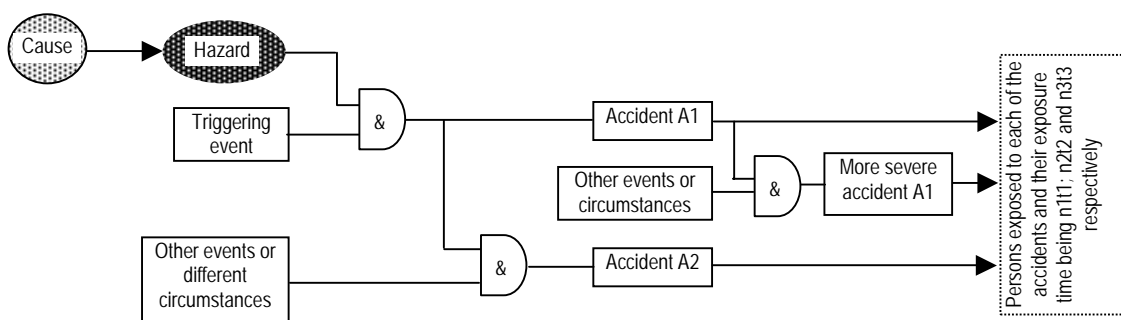


Figure 3 – Sequence of occurrence of accident, hazard and cause

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.

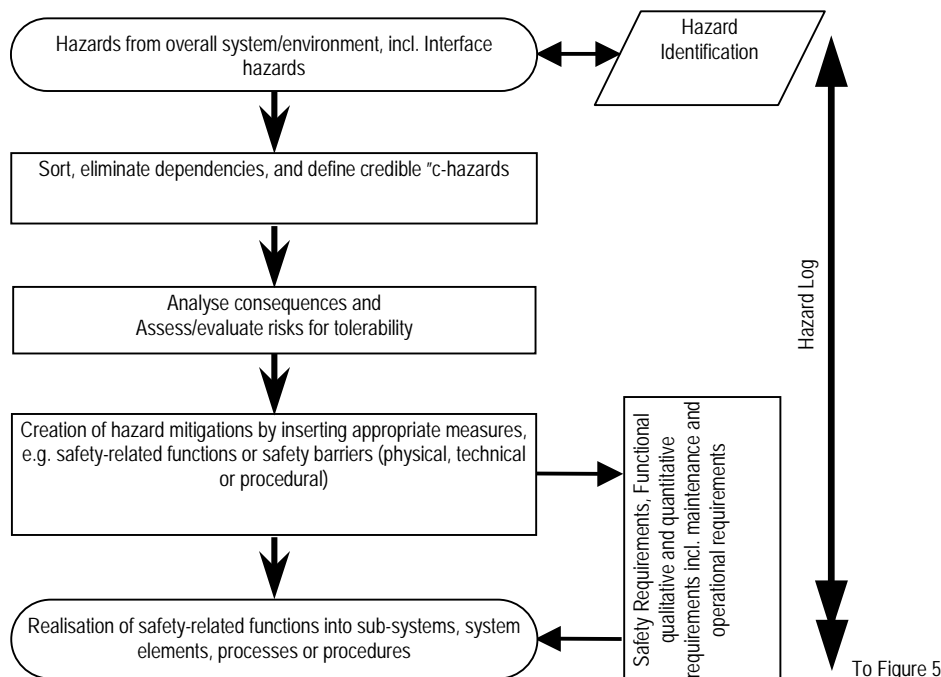


Figure 4 – Risk assessment flow chart

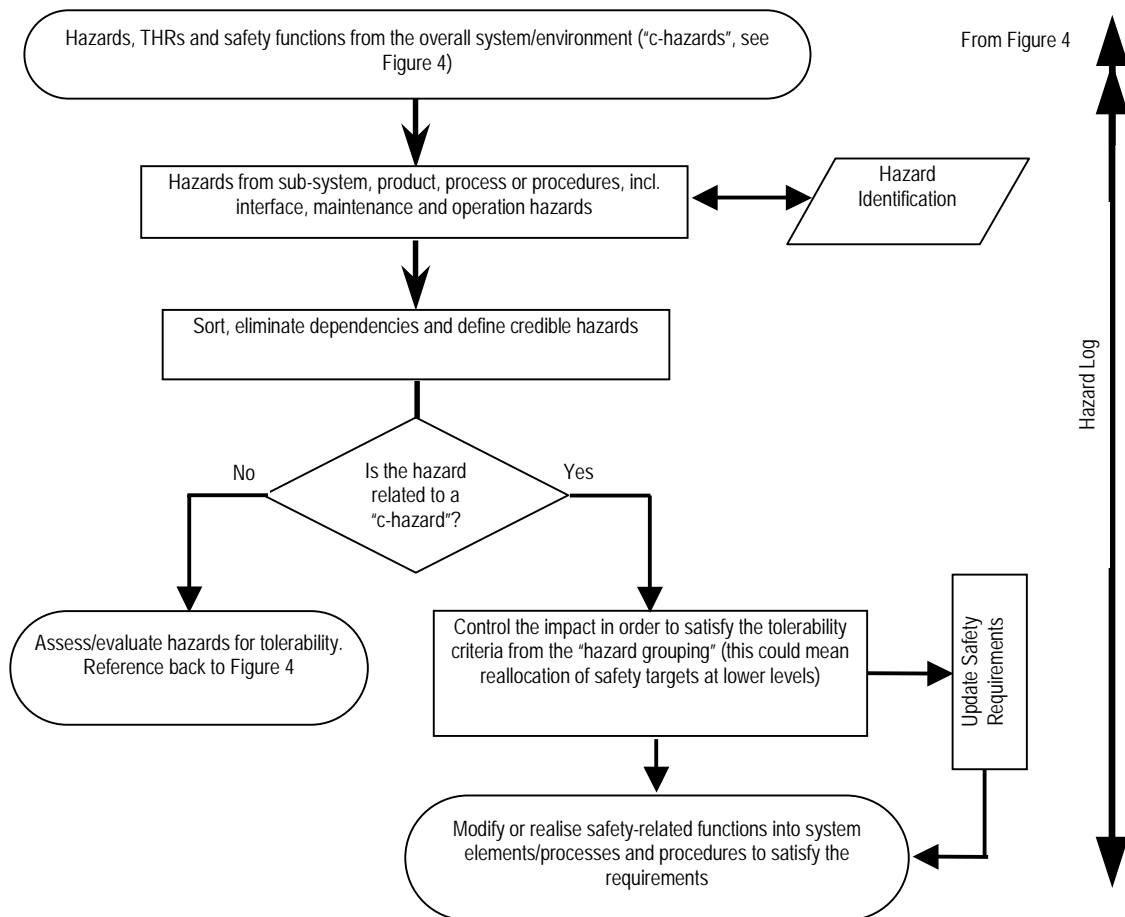


Figure 5 – Hazard control flow chart

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 THRs 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 THRs 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.

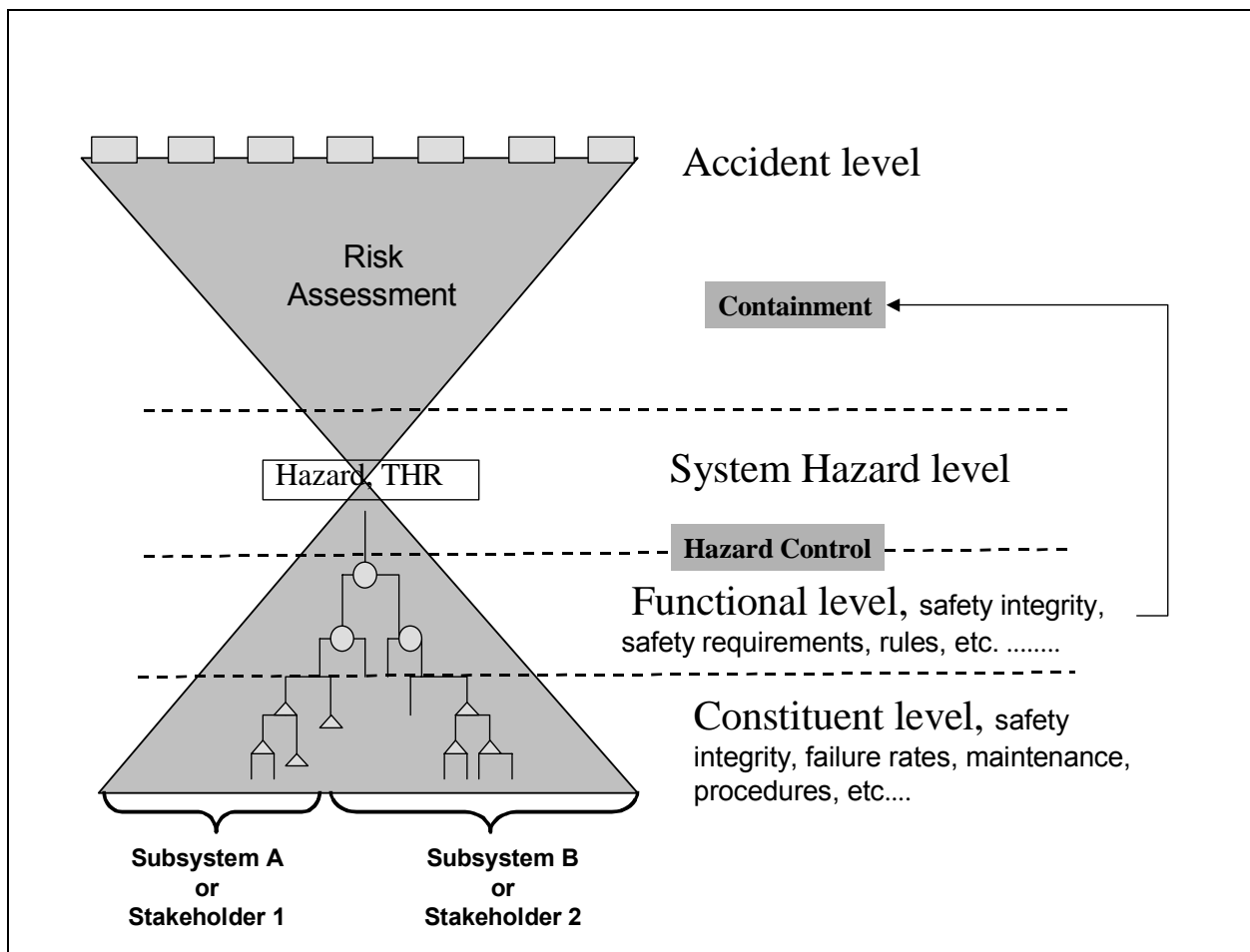


Figure 6 – Safety allocation process

The figure shows the relationship existing (as described in the risk assessment process in 5.3) between

- a hazard and the accidents it could lead to, investigated through risk assessment and,
- the functions/processes and the constituents (be it technical sub-systems, procedures or human operators), to operate a railway.

At the very bottom it indicates that, in theory, it would be possible to allocate at the end of the process the safety responsibilities between different bodies/entities i.e., sub-system A, sub-system B, etc., or stakeholder 1, stakeholder 2, etc., depending on the phase of the project.

The different risk classification approaches starting from the lowest level (constituents) up to the highest level (accidents) are further presented and their merits and demerits discussed in Annex C.

For any new railway application, a hazard analysis/risk assessment is indeed recommended by EN 50126-1 for allocating safety requirements to constituent parts. Nonetheless, doing it for the whole European railway system on a commonly accepted basis (for high speed, conventional and freight systems) would certainly be a considerable and difficult task and is considered impractical.

A common agreement concerning specific safety targets for parts of the railway also seems more difficult to achieve due to the variety of possible interpretations and approaches applicable. All the approaches mentioned above and further detailed in Annex C have advantages and disadvantages and none of them really stand out both on grounds of usefulness and of practicability.

6.3.3 Use of THRs

An alternative approach is to determine, for a specific system, THRs for each identified “c-hazard” independently from an overall quantitative risk target (see risk assessment in 5.3.2.5). This would require consideration of triggering events and accident scenarios together with the protective measures and safety barriers in place for reducing probabilities of accidents or their consequences.

Some hazards could lead to different accidents. Each accident could also escalate into outcomes with significantly different consequences. For example, a train derailment would typically only lead to minor injuries, due perhaps to passengers falling over inside the train, whereas in extreme cases, derailments can lead to multiple fatalities. In such cases, it would be necessary to consider and rank the risks associated with each of the accident and escalation scenarios to determine the hazard rate that should be assessed for tolerability (i.e. the rate associated with the highest ranked risk). For more guidance on risk ranking see Clause A.6 and Clause E.2.

Taking account of the appropriate risk tolerability criteria, THRs may be derived from comparison with the performance of existing systems or from acknowledged rules of technology, either by analytical or statistical methods, or from alternative qualitative approaches.

It should be noted that the RA is generally responsible for defining the hazards and corresponding THRs and have the freedom to define these at any system level, according to their particular needs. If no THRs are provided then either the RSI will propose these along with the system/sub-system proposal to the RA or they will work together to define them.

If all hazards of the system are assessed as “Tolerable” then it follows, using the explicit assumptions, that the total risk presented by the system is also tolerable and is consistent with overall risk targets set by the RA. This can be justified where the THRs are derived from the overall risk target. If not then the justification will require additional qualitative means.

6.4 Guidance on the concept of SI and the application of SILs

6.4.1 Safety integrity

Safety requirements are expressed as functional or technical requirements, and their contextual requirements, applied to a system (see 6.2). Note that safety functions may be dependant on entities on both sides of a boundary between two sub-systems. The level of confidence that can be placed in the achievement of such requirements is an essential part of the safety requirement specification and will contribute in determining the design solutions to be retained.

In essence, this level of confidence is related to the avoidance of sub-system related hazards at its boundary (i.e., states of the subsystem that could give rise to a railway system level “c-hazard”), and thus to the acceptability of the sub-system’s contribution in the occurrence of the relevant “c-hazards”.

Therefore, risk analyses should determine the list of hazards at the sub-system boundary, related to the sub-system, and their associated tolerable frequency of occurrence (THR).

SI is a measure of freedom of a system or function from undesirable states. It relates to how often the system/function could enter an undesirable state to ensure that the tolerable rate for the consequential c-hazards at the railway system level is not exceeded. SI may be expressed in a synthetic way using a conventional discrete index, called SIL.

SI is a generic concept, which should be applied to all kind of systems, regardless of the techniques used. In other words, SI is not specific to electronic systems, and the concept of SIL may be extended to other areas. However, before the concept of SIL is applied to non-electronic systems, it is necessary to calibrate the “levels” against specific safety integrity measures. In order to ensure comparability between similar systems, the related specific measures have to be commonly agreed. Some of these measures are likely to be different from those for electronic systems (also see 6.4.3).

Specifying SI for a subsystem without referring to the involved safety requirements or hazards at its boundary is simply meaningless. Therefore:

- SIL should not be allocated to a sub-system until the hazards at its boundary and the associated THRs are identified;
- Must not loose track of the hazards and their associated tolerable rates after the SIL has been allocated.

Once the SI requirement for a subsystem is defined, it should guide the implementation of associated risk control measures throughout the subsequent lifecycle phases, with the objective to contain the risk associated with the random and systematic failures of the subsystem within the tolerable range.

Figure 7 explains the factors influencing SI.

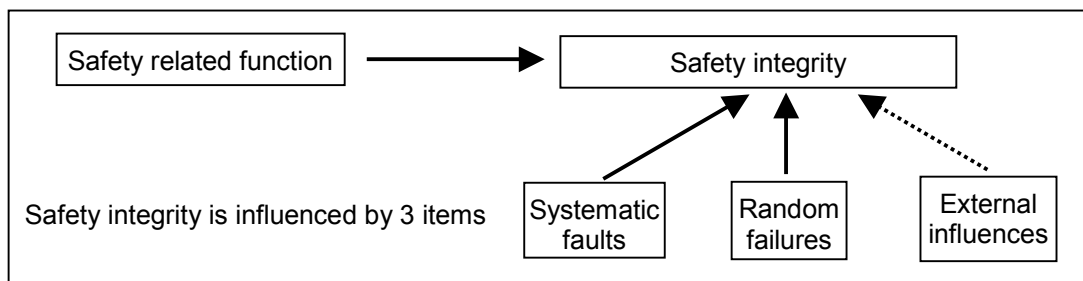


Figure 7 – Factors influencing SI

Measures against systematic faults and random failures need to be balanced with respect to each other.

Control of random failures is based on technical measures that are dependent on the techniques used. Random failures should be quantified where appropriate databases or calculation methods exist and when it is reasonable (see 5.4.3 for further explanation).

For other technical domains (e.g. mechanical or pneumatic systems), there is currently no standard specifying the technical measures associated to a SIL level. However:

- prediction information on mechanical products can be found in publications listed in the bibliography;
- control of reliability regarding wear-out problems are normally solved with the two shaping parameter Weibull-distribution;
- control of reliability should be carried out with simulation models and extend to real simulations and real application tests;
- Safety properties should be controlled maintained by dimensioning the component with adequate margins of safety, controlling statistical deviations in material properties, dimensional accuracies and tolerances to prevent undesired states, e.g. wearout, malfunction, etc., and implementing an effective maintenance programme.

Control of systematic faults relies on implementation of appropriate quality assurance and organisational measures.

NOTE A major distinguishing feature between random hardware failures and systematic failures is that the system failure rates (or the appropriate measures), arising from random hardware failures can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

Existing standards relating to electronic equipment also define such measures, which are now well accepted by the relevant community (EN 50128 and EN 50129). A number of these measures are generic, and should be implemented regardless of the technique used. The control of external influences is generally justified by a deterministic approach (based on correct specifications).

Regarding safety related electronic systems, it is recommended to consider the use of EN 50129 and EN 50128 standards (originally developed for signalling systems) also for electronic systems in other railway domains (e.g. rolling stock, power supply, etc.) as appropriate.

6.4.2 Using SI concept in the specification of safety requirements

6.4.2.1 Introduction

Subclause 6.4.2.2 presents the process for identifying, apportioning and specifying safety requirements down to subsystem level. This is a generic process where the use of SIL is an option.

The efficiency of this process is dependent on:

- a clear definition of system and subsystem boundaries, which governs the identification of the hazards at these boundaries.
- a clear and precise expression of the functional safety requirements, which are related to the hazards at these boundaries and should therefore be specific to the system/subsystem under consideration.

6.4.2.2 Example process for apportioning safety requirements within a system

Table 4 summarises the steps in a structured approach to allocation of SI within the risk assessment process described in 5.3. Apportionment of safety requirements from the railway “c-hazard” to a system and then to a subsystem is however, problematic and is discussed in 6.3. As already mentioned, more refinement levels may be necessary to specify the system elements.

As stated previously in 5.3.2, the activities pertaining to steps 1 to 4 of Table 4, and leading to the identification of system hazards and the assignment of associated THRs are generally referred to as risk assessment. This is mainly a top-down approach. These tasks require knowledge of the railway system, and imply a responsibility (regarding the assessment of the tolerability of a hazard) that rests with the RA. Therefore, it is commonly accepted that the RA should have the prime responsibility for the risk assessment at the railway system level.

Further steps of Table 4, as stated in 5.3.2, form hazard control. They are usually the prime responsibility of the RSI (system supplier).

There are iterations from the hazard control back to the risk assessment, for example, when new hazards are introduced by the design of the system. These iterations, together with the need to ensure a good understanding and coherence of the safety related information, requires co-operation between both parties concerned with risk assessment and hazard control.

Any functional or technical requirements on systems/equipment, at lower system levels, that are necessary to reduce risk to a tolerable level or other qualitative safety requirements such as conformance to standards should be incorporated as qualitative safety requirements for the relevant system/equipment (also see 7.1 for safety demonstration).

Table 4 – Structured approach to allocation of SI (refer to 6.4.2.2)


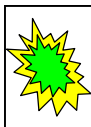
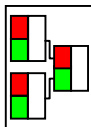


Stage	Input	Activity	Output
1 System Definition 	High level system description and requirements	Define system boundaries Perform functional analysis, along with the identification of functional safety requirements Identify safety related technical and operational requirements (system level)	System specification including definition of the system boundaries (physical as well as operational)
2 Hazard Identification at system level (1) 	List of railway system level c-hazards Field data on similar system (where available) System specification	Sort out the relevant c-hazards Identify hazards at system boundary (i.e. the system contribution in the hazard sequences) <i>These tasks can be efficiently dealt with through hazard identification sessions with the participation of the different stakeholders (installation teams, operators, maintainers, etc.). Dedicated hazard analyses may be performed in addition to further refine the understanding of hazards.</i>	List of the hazards at system boundary
3 Consequence Analysis 	List of system hazards Knowledge of the railway (incl. Mission profile, technical and operational aspects contributing as factors or mitigations in the hazard sequences) Railway Risk Model if available (2)	Analyse the possible consequences of each hazard, as identified in stage 1 (identify the sequences of events /conditions leading to an accident). The following methods may be used: <ul style="list-style-type: none"> • Cause-Consequence Diagrams (recommended) • Event Tree Analysis • Fault Tree Analysis <i>This analysis is useful to take into account the impact of a new or modified system on the pre-existing railway. It may be based on qualitative or quantitative analysis depending on the complexity and perceived risk.</i>	Cause Consequence model, including quantified estimates (3) for the probability of occurrence (4) of each accident sequence initiated by each hazard.
4 Risk Tolerability Assessment at system level. 	Cause Consequence model for each system hazard Risk Tolerability /Acceptability criteria (5), (6)	Using the Cause-Consequence Model and depending on the acceptability of each hazard consequence, identify the THR - (7) for each system hazard. NOTE THRs may also be derived from comparison with existing systems or from acknowledged rules of technology, either by analytical or statistical methods, or from alternative qualitative approaches	List of the system hazards (as identified in stage 1) and their associated THR.
5 System level safety requirements 	List of the system hazards and their associated THR.	Translate system hazards into functional safety requirements (8), (9). Refine / complement the identification of safety related technical and operational requirements.	List of system functional safety requirements (10). Quantified qualification of the tolerable frequency of system failure to meet each requirement (derived from the THR) List of system safety requirement (of technical or operational origin), which may not have been expressed as functional requirements.

Table 4 – Structured approach to allocation of SI (refer to 6.4.2.2) (continued)

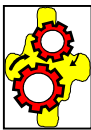
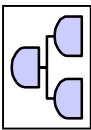



Stage	Input	Activity	Output
6 System design 	System specification System safety requirements	Breakdown the system into subsystems Develop a structured functional analysis down to subsystem level. Identify safety related technical and operational requirements related to subsystems.	Subsystem specifications traceable to the system specification.
7 Causal analysis 	System design (incl. Subsystem specifications) System hazards and associated THR	The purpose of this stage is to identify hazards at subsystem level and to allocate them a THR. It includes two major activities: <ul style="list-style-type: none"> • Fault tree Analysis (11), (12) • Common Cause Failure -CCF- analysis to justify independence of items where logical AND gates are used in the FTA. The causal analysis may reveal new system level hazards arising from interfaces between subsystems or from design choices (i.e. dependent on the techniques used). Such new hazards must be analysed as previously identified ones, and may require iteration from steps 2 or 3.	List of subsystem hazards. Description of the sequences of events linking subsystem hazards to system level hazards. Apportionment of THR to subsystem hazards
8 Sub system level safety requirements specification 	List of hazards at subsystem boundary and associated THR	Translate subsystem hazards into sub-system level functional safety requirements (8), (9). Refine / complement the identification of safety related technical and operational requirements.	List of subsystem functional safety requirements (10). Quantified qualification of the tolerable frequency of subsystem failure to meet each requirement (derived from the THR) List of subsystem safety requirement (of technical or operational origin), which may not have been expressed as functional requirements.
9 SI Requirements Categorisation 	List of hazards at subsystem boundary and associated THR	Using a definition of SILs (e.g. the SIL table), you can allocate a SIL, where appropriate, to each functional safety requirement. The results of the previous stage contain the information characterising the SI of the subsystem. However, it is generally valuable to simplify this information by using conventional categories of integrity that will be related to appropriate sets of techniques and methods to reach such integrity. This is the purpose of SILs.	List of subsystem functional safety requirements with their associated SIL <i>The results of steps 3 (Consequence Analysis), 5 (risk tolerability assessment) and 7 (causal analysis) should remain available, as they contain all the base information for thoroughly understanding the safety of the system in the subsequent lifecycle phases (e.g. assessment of changes, identification and monitoring of the key critical factors during the operational life). Best practise should ensure they are adequately recorded in a Hazard Log.</i>

Table 4 – Structured approach to allocation of SI (refer to 6.4.2.2) (continued)

Stage	Input	Activity	Output
<p>10 Optional: consolidation of SIL allocations</p> 	<p>List of subsystem functional safety requirements with their associated SIL</p>	<p>At this stage, SIL are often consolidated at:</p> <ul style="list-style-type: none"> • Function level (the SIL for a function will be the highest SIL for the functional safety requirements it implements) • Subsystem/equipment level (the SIL for a subsystem will be the highest SIL for the functional safety requirements it implements) 	<p>List of SIL for functions List of SIL for subsystems This SIL consolidation must be traceable to the results of the previous stages (8 and 9) – list of functional safety requirements and hazards. <u>SIL allocation to a subsystem or a function without reference to the relevant safety requirements / hazards would be in essence meaningless.</u></p>

NOTE 1 Subclause 5.3.2.2 provides further guidance on Hazard Identification.

NOTE 2 Subclause 5.2 provides guidance on risk modelling.

NOTE 3 The level of confidence in the estimate will depend on the accuracy and applicability of the available input data. If necessary, the most critical assumptions should be identified, so that they can be further refined or monitored in the subsequent lifecycle phases. Such assumptions could be referred to as "dependencies" i.e. external factors on which the system safety performance is dependent.

NOTE 4 This is a probability and not a hazard rate.

NOTE 5 The risk tolerability criteria should be applicable to each accident scenario (sequence leading from the hazard at system boundary to each consequence), as opposed to an overall target.

NOTE 6 Such criteria may be expressed by a risk acceptability matrix (refer to EN 50126-1, Sub4.6), but it must be recognised that risk acceptability may be a more complex issue with multi-dimensional inputs.

NOTE 7 THR can be an order of magnitude and can be estimated by different means including expert judgement. Extensive risk analyses are not systematically required.

NOTE 8 Functional safety requirements must be expressed by clear and precise statements that should be understandable without ambiguity by the system designers and from which validation tests can be derived.

NOTE 9 Functional hazards are "anti-functions": in other words, a functional hazard should be expressed as a behaviour of the system that doesn't meet one or more functional safety requirement(s).

NOTE 10 This list should be mapped onto the system structure specification.

NOTE 11 Other techniques, such as Cause-Consequence diagrams, Markov models can be used as an alternative or a complement to Fault Tree Analyses.

NOTE 12 Top events for the FTA analyses should be the system hazards, and most basic events should be subsystems hazards at its boundary.

6.4.3 Link between THR and SIL

Table 5 identifies the SIL required for a safety-related functional requirement from the THR requirement for the associated hazard. These are the most commonly accepted levels and are applied in some industry sectors.

Table 5 – THR/SIL relationship

THR (h^{-1})	SIL
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

NOTE 1 A SIL is not a synonym for THR. The quantitative requirement of a THR must be supplemented by the corresponding qualitative measures to arrive at the relevant SIL.

NOTE 2 This SIL table is the most commonly accepted for electronic systems and is provided for guidance. It is suggested that it may not be applicable to other systems. In particular, simple mechanical systems are far more reliable than electronic systems, i.e. the margin from 10^{-5} to 10^{-9} h^{-1} may not be adequate for mechanical/electromechanical systems or equipment. In such cases, the "proven in use" argument could be of special value. Safety of a mechanical, electro-mechanical, etc., systems or equipment may also be demonstrated by reference to current standards or best practice (see 5.4.1 and 5.4.4)

NOTE 3 This table sets a limit in the integrity that should be expected from a system: THR requirements more demanding than 10^{-9} h^{-1} are not handled, in recognition that in any system, there is a level below which the effect of systematic failures can not be reduced.

However, it is suggested that a function having quantitative requirements more demanding than 10^{-9} h^{-1} should be treated in one of the following ways:

- if it is possible to divide the function into functionally independent sub-functions, the THR can be split between these sub-functions and a SIL assigned to each sub-function;
- if the function cannot be divided, the measures and methods required for SIL 4 should, at least, be fulfilled and the function should be used in combination with other technical or operational measures in order to achieve the necessary THR.

6.4.4 Controlling random failures and systematic faults to achieve SI

SI is an expression of the failure rate and the corresponding qualitative measures required for achieving a THR, i.e. the tolerable frequency of undesirable events. Achieving the target requires control of all hazards related to the system or subsystem.

This is achieved through the application of

- technical measures, addressing the construction of the component to ensure that the rate of hazardous random failures is less than the specified THR,
- management and organisational measures, aiming at controlling the rate of hazardous systematic failures.

NOTE it may be useful to remind here that software should always be considered along with its supporting hardware (computer, sensors, actuators) in a holistic perspective. Therefore, EN 50128 should not be applied independently of EN 50129.

6.4.4.1 Technical measures for the control of random failures

Such measures are dependent on the technique used. For electronic systems, EN 50129 provides guidance on the technical measures to enable attainment of the SI requirements (for system and hardware aspects).

Whenever possible, the random failure rate of the component should be predicted to demonstrate that it is less than the target THR (this is the case for electronic hardware). For components whose failure behaviour is dominated by non-random causes (electromechanical, mechanical, software, etc.), it may be impossible to calculate failure rate or the mechanism for determining failure rate may be impractical.

In such cases, safety argument should be based on:

- the definition of adequate technical rules (addressing dimensioning, construction, testing, health monitoring and maintenance regime) that will support a qualitative argument. Use of the failsafe concept is one possible approach.
- the safety performance monitoring of the equipment (and/or of equipment designed and manufactured to the same technical rules and processes) through its service operation, with a view to improving the technical rules and/or processes, if necessary.

Sets of technical methods pertinent to each SIL are currently available for electronic systems (e.g. in EN 50129 and EN 50128). For other technologies (e.g.; electromechanical, mechanical, pneumatic, etc.) such methods are not described in generic standards. In these areas, suppliers should implement design standards or codes of practice and manufacturing processes in line with the different SI requirements (Note that specific standards for the major safety critical mechanical components exist. These should be used as an input, where appropriate).

Figure 8 summarises the process for justifying the random integrity of a system.

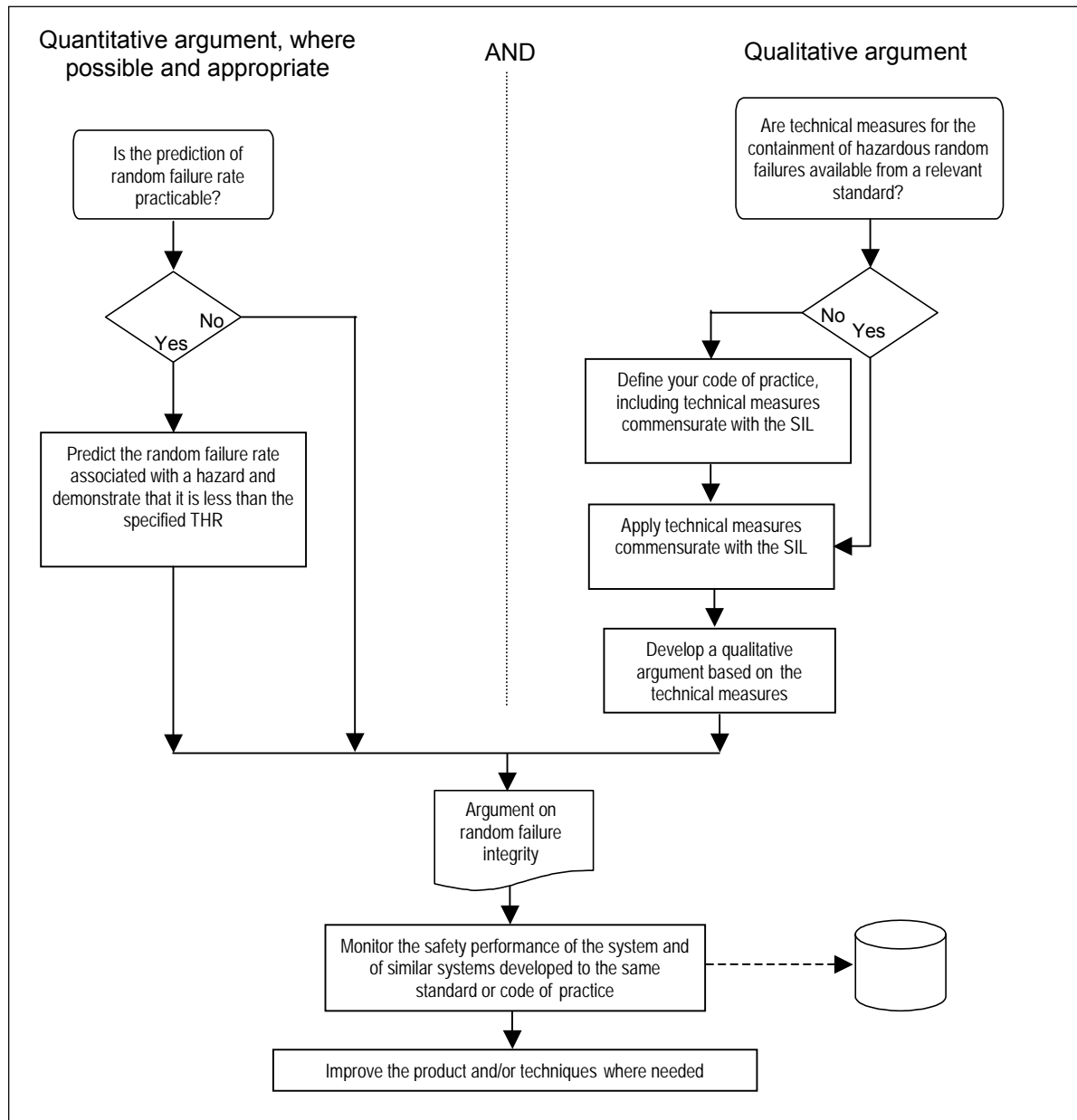


Figure 8 – Process for defining a code of practice for the control of random failures

6.4.4.2 Management measures for the control of systematic failures

Systematic failure integrity is a non-quantifiable part of the SI and relates to hazardous systematic faults (hardware or software). Systematic faults are 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.

Examples of systematic errors are specification errors, design errors, gaps in the verification process, manufacturing errors, installation errors, operation errors due to a deficiency in operational procedures, etc.

Systematic failure integrity is achieved by means of quality and safety management conditions. For electronic systems, EN 50129 and EN 50128 define such measures. For other technologies, a standardised approach to the control of systematic errors in consideration of the requirement for integrity may not be available in current standards.

In such cases, the RSI should develop their own codes of practice including adequate management measures, and continuously improve them when necessary (see Figure 9).

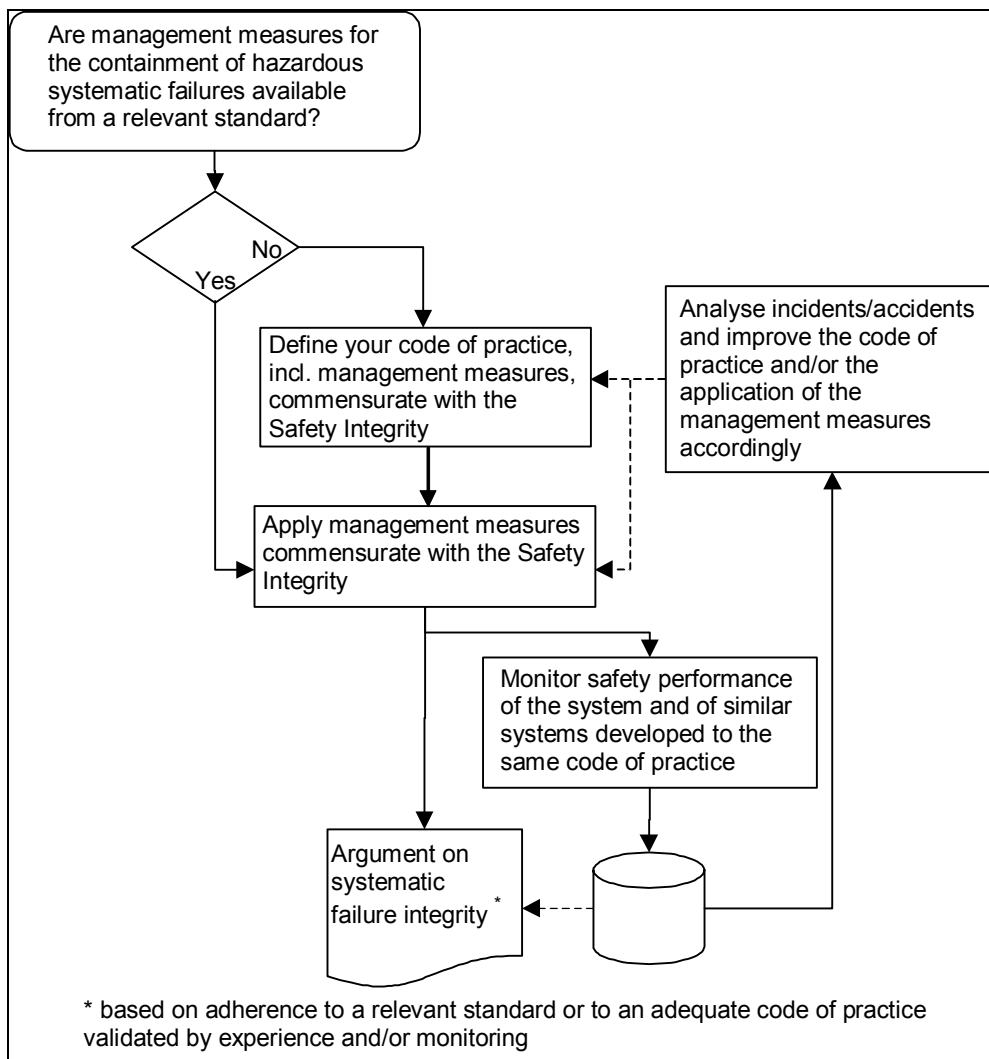


Figure 9 – Process for defining a code of practise for the control of systematic faults

Although most management measures may be technique-dependent to a certain extent and should, in any case, be considered in the light of the specific development process used, some of them are generic.

6.4.5 Use and misuse of SILs

This subclause provides some warnings about the use of SIL. Sometimes the SIL concept is misunderstood and used for non-intended applications.

For example, SIL should not be used as a marketing argument, e.g. this equipment is SIL = 4. A SIL 4 system is not necessarily safer than a SIL 1. Because, usually, the stringent requirements for SIL 4 are as a result of a much higher risk potential in comparison with a SIL 1. The intention of the risk based CENELEC approach is to bring the different risks under tolerable levels and many factors are necessary in order to do this. It is wholly improper to refer to SILs only.

6.4.5.1 Intention of the SIL concept

As described in 6.4.3 and 6.4.4, the SI of safety-related functions can be divided into parts that can be quantified and others that cannot be quantified. A SIL should address the qualitative appreciation of such factors as quality and safety management and technical safety conditions, which cannot be quantified. Usually SIL refers to techniques and measures in order to address the integrity against systematic faults.

The link between the quantifiable part and the non-quantifiable part of SI is the SIL table (see 6.4.3 and Table 5)

SIL should only be allocated to safety related functions. Each of these functions has a qualitative safety target and a quantitative target attached to them. The qualitative target should be in the form of a SIL, and

should cover integrity against systematic faults. The quantitative target should be in the form of a numerical failure rate, and should cover random failure integrity.

Safety-related functions within a system are implemented by sub-systems. SILs are allocated to safety-related functions and consequently the sub-systems implementing these functions, but no further. SIL for an equipment, which is part of a sub-system, is the same as for the sub-system, unless functional independence can be demonstrated between equipment within the sub-systems.

6.4.5.2 Misuse of SILs and warnings

The following non-comprehensive list gives advice on how SILs should not be used.

- i) SILs should not be used for marketing purposes, see above.
- ii) SILs should not be used for describing systems attributes, e.g. “this is a SIL 4 interlocking system” or “this is a SIL 3 sensor” because SILs may only be allocated to functions.
- iii) SILs should not be used for deriving THRs, e.g. do not determine a THR from a previously estimated SIL.
- iv) SILs should not be used for non-functional safety, e.g. applying SILs to safety against slips, trips and falls.
- v) SIL should not be used for specification purposes in contracts. Specification of SI requirements should be through the use of THR's, if they are available and of any significance.

Also, the following should be observed.

- i) SILs should be assigned only after a top-down analysis starting from the highest system level. It is meaningless to assign SILs prior to completing such an analysis. SIL assignment should be undertaken down to a level where functionally independent items can no longer be found.
- ii) Assigning SILs without having defined appropriate measures and techniques for each level is meaningless.
- iii) Concerning integrity against systematic faults, SILs should only be assigned to safety related functions.
- iv) Same SIL on different system levels does not necessarily mean that the random failure integrity is also the same. See explanation below.
- v) Fulfilling all SIL requirements does not necessarily mean that the related function is safe. In addition to SIL, all other safety related requirements must also be fulfilled to meet the required level of safety, e.g. quantitative safety targets.
- vi) Functions with $\text{THR} > 10^{-5} \text{ h}^{-1}$ exist and they may still make a significant contribution to safety. In such cases, no specific SI requirements are defined. Note that this does not mean that these functions are superfluous or that they need not be implemented. It only means that no SI requirements need to be specified.
- vii) Fulfilling all SIL requirements, for a specific function, means that the associated integrity against systematic faults is high enough. However, because integrity against systematic faults cannot be quantified, the hazard rate for the specific function is calculated from the random failure rates of the function components and the contribution from a systematic fault is considered to be negligible.

The following example clarifies point iv) above.

If a function for which a SIL 3 is required is implemented by two physically independent, but identical channels, so that the function can fail in an unsafe state only when both channels fail the same way, then

- the random failure rate for each channel doesn't need to meet the requirement for SIL 3, as failures of both physically independent channels are needed to cause failure of the function in to an unsafe state, and
- for the systematic fault, SIL 3 requirements should apply to both channels. This is because a systematic error would affect both channels, as a common mode.

6.5 Guidance on fail-safe systems

6.5.1 Fail-safe concept

6.5.1.1 Introduction

Fail-safe concept is described in 4.8 of EN 50126-1. A fail-safe system is a system that has design properties such that any single failure in the system renders it into a safe state. Also the probability that a subsequent failure event(s) in combination with the first event gives rise to a hazard, before a safe state has been reached or before the system is restored, should be tolerable with regards to the required level of safety.

This is generally achieved by combining components with well-established failure modes (components with inherent physical properties) so as to give priority to a failure mode that is safe.

This safe failure mode is a relative concept, and must be analysed from a safety standpoint. Some systems do not have one single status that is safe under all circumstances. For example, automatically stopping a train if an emergency is detected is usually safe but sometimes dangerous (e.g. burning train stopped in a tunnel).

Assumptions regarding the failure modes of the components are key to the failsafe concept. Based on specific properties and build of the component, the general assumption is that any failure or degradation of the component that exceeds performance limit will result in the component to enter a defined state (e.g. the absence of a signal, the opening of front contacts, or the close position of a valve, etc.), and that other failure modes that prevent the component entering the defined state are rendered incredible (depending on the specific properties of the component, incredible modes could be undue closure of the front contact of a relay, simultaneous make of a front and a back contact, open position of a valve, etc.).

6.5.1.2 Components with inherent physical properties

A set of credible assumptions regarding the failure modes of most electronic components is provided by the Annex C of EN 50129. This list should be regarded as best practice for any electric or electronic railway equipment.

Inherent fail-safe physical properties may also be claimed for other components, including mechanical, electromechanical and pneumatic components (e.g. clamping device, valves, pressure sensors, etc.). Full justification of the fail-safety properties should be provided. This should include, but not necessarily limited to, the following information:

- explanation of the claimed inherent properties, including the description of the safe failure mode(s), of how the failures are detected, and the hazards (unsafe states, also called wrong-side failures) of the component;
- exposé of the safety argument;
- theoretical explanation of inherent physical properties (including allocation of the inherent physical properties to the elementary parts by means of an FMEA);
- justification of how they are achieved (including list of the basic assumptions supporting the safety argument);
- explanation of how alterations of the component characteristics can be detected, and the related testing, monitoring and preventive maintenance prescriptions;
- explanation of special construction or assembly of parts;
- evidence of compliance with recognised quality standards;
- measures for ensure traceability during the manufacturing process;
- evidence that the failure mode will not occur as a result of component ratings being exceeded (for example, because of fault or overload conditions);
- results of tests to demonstrate fail-safe behaviour of component under adverse conditions (by means of physical tests, technical justifications, or simulation);
- where possible, evidence of previous experience of reliance on the component for inherent fail-safety;

- application conditions on which the safety is depending (safety-related application conditions), including, but not necessarily limited to
 - how to integrate and use the component within a system,
 - explanation of special mounting arrangements or other precautions for the component,
 - safety-related ratings,
 - testing, monitoring and maintenance prescriptions,
 - requirements for Failure Reporting and Analyses (failure of such components should be analysed, and specific attention be paid to a possibly systematic origin of defaults).

If satisfactory justification is provided, the relevant component failure modes may be excluded from the quantitative analysis.

6.5.2 Designing fail-safe systems

Failsafe technique satisfies the following requirements:

- a) no single failure leads to an unsafe condition.
- b) single failures are detected, negated (a safe state is enforced) and such safe state is retained (the system is locked in the safe state).

In addition,

- it must be verified that the probability that further occurrence of additional failures leads to an unsafe situation is acceptable with regards to the safety requirements of the system. The time to detection and negation, and the effectiveness of the retention are key parameters for a deterministic assessment,
- an argument must be developed to support that it can be credibly assumed that common causes with potential for precipitating multiple failures have a negligible probability with regards to the SI requirement or lead to detection and negation,
- the logic of the design must be submitted to a complete review (this could be done with formal methods).

The following Table 6 summarises the different states possible for a fail-safe system, and provides guidance accordingly.

More guidance for electronic safety related systems are available in EN 50129.

Table 6 – Possible states of a fail safe system

System State	Specified operating domain under normal conditions	Safety assured operating domain	Possible temporary unsafe state (case of reactive fail-safety) ^a	Safe (restrictive) state enforced ^b	System locked in a safe (restrictive) state ^{b,c}
Definition	Normal operating domain: there is no failure, or there are dormant failures, without impact on the functional characteristics.	Some safety-related characteristics may be degraded, but: the failure is not detected and the deviation from the nominal domain remains compatible with the safety requirements specification for the system.	Some safety-related characteristics are degraded such that the safety requirements are no longer satisfied.	Safety is ensured, but the operation of the railway is generally affected (because of the system restrictive state).	Safety is ensured, but the operation of the railway is generally affected (because of the system restrictive state).
Comments	This state may be permanent.	This state may be permanent.	Detection and negation of the failure must occur in a time, which does not exceed the duration of a potentially unsafe transient output.	This state must be followed by system lock-up, in a sufficiently short time to make the probability of cumulated failures less than the specified quantitative safety objective.	This state must be permanent until the system is repaired and re-commissioned. System lock-up may be inherent to the system (if an active and irreversible lock-up device exists), or procedural (the output of the system is by-passed by procedure) or a maintenance team disconnects the system.
Guidance	Analyse the impact of additional failures (FMEA and testing)	Check that the degradation in safety-related characteristics is in line with the safety requirements. Qualify the “safety margin” i.e. the area separating the safety assured operating domain from potentially unsafe states. For this purpose, a clear specification of the safety assured operating domain is necessary. Analyse the impact of additional failures (FMEA and testing)	Justify that the detection and negation will occur in a sufficiently short time not to create a hazard.	Analyse the impact of additional failures (FMEA and testing) that may occur until a lock-up takes place.	Verify the effectiveness of the system lock-up. Justify that additional failures will not cancel the safe state.
Recommendations	Eliminate as far as possible the causes of dormant failures. Consider means of detecting dormant failures in a time sufficiently short to make the probability of cumulated failures less than the specified quantitative safety objective.	Eliminate as far as possible the causes of dormant failures. Consider means of detecting dormant failures in a time sufficiently short to make the probability of cumulated failures less than the specified quantitative safety objective.			

^a In most fail-safe systems, such cases will not exist.

^b For justifying fail-safety at a system level, in addition to defining the system's safe state the overall railway system should also be analysed as the resultant degraded modes may give rise to other hazards (e.g. the recovery time from system lock-up in a restrictive state may be safety related).

^c In some cases, a restart of the system may be possible following integrity checks, by an authorised person, to confirm that it is safe to do so. However, the number and frequency of such restarts would need to be restricted/monitored from an availability perspective.

7 Guidance on methods for combining probabilistic and deterministic means for safety demonstration

The assurance of safety in the railways is often attained through adopting and implementing appropriate processes, procedures, tools, rules and methodologies throughout the life cycle of products, processes, systems and operations. However, complexity and novelty of most modern systems and undertakings challenge the degree of certainty that can be attained with most approaches.

Definition of deterministic is given in 3.2.4. Typically, where simplicity, past experience or quality of assurance processes generates a high degree of certainty, these are classed as deterministic approaches. Conversely, where novelty, complexity or nature of assurance processes yield a lower degree of confidence in the desired outcome, these approaches are referred to as probabilistic. Probabilistic is defined in 3.2.14. In principle, deterministic and probabilistic are merely labels determined by the degree of certainty and confidence and are not distinctly different matters.

7.1 Safety demonstration

7.1.1 Introduction

The processes given in EN 50126-1 cover all RAMS activities to be performed when a system is built from scratch. On acceptance all activities have to add up to provide sufficient evidence for the RAMS performance of the system to enable the appropriate parties to accept the system. The acceptance process often proves to be a difficult process, especially when it comes to the question of whether the safety of the system is sufficiently demonstrated. To avoid discussions at the system acceptance phase, all parties involved with the acceptance should agree, at the earliest project stage, the acceptance process to be applied and the risk acceptance principles to be used for the acceptance phase.

Roughly, three main strategies can be used for safety demonstration, which are often used in combination for a particular system. These are the following:

- safety demonstration by complete system analysis and risk calculation (generally applied for completely new systems or new parts of the system);
- safety demonstration by using an existing system as a reference;
- safety demonstration when using technical standards as a reference.

The use of the three generic risk acceptance principles MEM, GAME, and ALARP described in EN 50126-1 within the safety demonstration strategies will be explained. The principles themselves are explained in 8.1.

The main objective of this guidance is to provide a cost effective approach that provides the same level of confidence for acceptance for all classes of systems.

7.1.2 Detailed guidance on safety demonstration approaches

Demonstrating the level of safety of a system is not a matter of doing a single analysis at some point in the lifecycle of the system. Throughout the lifecycle of a system activities are performed that contribute to the final decision (typically in the system acceptance phase 10 of the lifecycle of EN 50126-1) whether or not the risk associated with the system is acceptable. This includes getting agreement with the parties involved in acceptance, at an early stage of the project, on the processes and methods to be used by the project/supplier to demonstrate safety. This clause indicates what the important issues to be addressed during the lifecycle of the system are, in order to facilitate a smooth acceptance of the system. Which issues are important in which phase of the generic EN 50126-1 RAMS lifecycle are described in Table 7.

Table 7 describes three distinct approaches. The reason for describing three different approaches is to allow for reuse of any available safety evidence without any concessions to the quality of the safety demonstration performed. It is important to use the most cost effective combination of the three methods depending on the properties of the system being developed.

a) Complete system analysis approach (Column A):

The safety demonstration approach that is explained in column A can be considered as the clean EN 50126-1 approach. All safety demonstration is started from scratch and the safety evidence needed for safety demonstration grows as the system develops. The purpose of the activities listed in column A is to clarify and detail the generic process requirements of EN 50126-1.

b) Existing system reference approach (Column B):

The approach described in column B of the matrix is suitable for systems that are very similar to an existing system with known safety features. For these types of systems it is usually more cost effective to re-use safety evidence either from analysis or from data gathered from field experience. By this approach extent of effort and resources for hazard identification and cause consequence analysis activities can be limited.

c) Proven design approach (Column C):

The approach described in column C is especially practicable when systems/subsystems/equipment) are used that have a proven design, which is well documented in technical standards or specifications. It is important that the safety delivered by these standards or specifications is based on sound analytical evidence or well documented field experience with systems built to the same standard or specification.

d) General remarks (Column D):

Column D gives general guidance for safety demonstration, which is applicable to all three approaches.

The activities described in the table add more detail/clarification to the activities described in Figure 9 of EN 50126-1. They relate only to the risk acceptance of the system. The table is not intended as a substitute or addendum to Figure 9 of EN 50126-1, and the objective is not to add additional requirements.

NOTE For the implementation of safety critical process, system or equipment where the proof of compliance is based on system requirement specification (mainly carried out by supplier RSI) may not be considered sufficient by a SRA. In such cases the SRA can demand additional proof of safety (usually from the operator RA or RSI) as provided in "Directive 2004/498/EC" (see also 7.1.3).

Table 7 – Approaches for system safety demonstration

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phase 1 concept	Select this approach for sub-systems or functions that are completely new or do not fulfil the prerequisites for using the other approaches, or this approach allows for technical solution with an acceptable level of safety at much lower costs (prevent over engineering).	<p>Select this approach for (parts of) systems that fulfil the following prerequisites:</p> <p>The sub system is to a large extent comparable, with respect to its safety related performance, to an approved existing system for a similar application, performing the same functionality</p> <p>The safety performance and application conditions of the existing system have to be well known and documented. Both analysis and experience data can be used as evidence</p>	<p>Select this approach for (parts of) systems that fulfil the following prerequisites:</p> <p>The system is built according to well-defined and accepted national or international technical standards or specifications.</p> <p>Sufficient evidence is available to demonstrate which safety aspects are covered by the standards or specifications.²⁾</p>	<p>Determine which of the three demonstration strategies is used for the different sub-systems of the system under development, and clearly define the sub-system boundaries. On system level you must also define the safety targets.</p> <p>The processes, tasks and responsibilities for approval will depend on the role (supplier, operator, authority, owner, etc.) of the organisation in the railway industry, and the country the system is intended for.</p>
Relevant deliverables Safety Case	Document approach in safety strategy.	Document approach in safety strategy.	Document approach in safety strategy.	The management established in this phase structure forms a basis for the quality management report and safety management report related to these phases.

2) For safety aspects not covered by the standards approach A will have to be followed.

Table 7 – Approaches for system safety demonstration *(continued)*

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phase 2 system definition	<p>Define top level safety targets using e.g.:</p> <ul style="list-style-type: none"> - determine ALARP boundaries, i.e. define the overall safety targets; - GAME; - MEM. 	<p>Gather experience data (qualitative and quantitative) from existing reference system.</p> <p>Identify potential differences between new and reference system.</p> <p>Identify differences between application conditions of reference and 'new' system.</p> <p>Identify hazards arising from the difference between the new and the existing system ALARP/ GAME.</p>	<p>Gather experience data and other safety evidence relevant to the standard.</p> <p>Seek approval for using specific standards and specifications as a basis for safety approval by relevant authorities.</p> <p>Assess applicability of standards and specifications against the current application conditions.</p> <p>Identify hazards arising from differences between scope/conditions of standard and scope/conditions of application or due to limitations of the coverage of relevant safety considerations in the standard.</p> <p>Identify safety issues not covered/supported by standards and specifications (especially on interfaces).</p>	<p>When defining application conditions maintenance and operating principles should be taken into account.</p> <p>It is strongly advised that safety targets are based on a sound and objective evidence using the principles described here.</p> <p>On system level you must define overall safety targets. For ALARP this means defining the upper and lower boundaries of ALARP region. An example of this is given in Clause G.2 (Copenhagen Metro example).</p>
Relevant deliverables Safety Case	<ul style="list-style-type: none"> - System definition/description - Results of above activities input for safety policy and safety requirements - Safety plan 	<ul style="list-style-type: none"> - System definition/description - Results of above activities input for safety policy and safety requirements - Safety plan 	<ul style="list-style-type: none"> - System definition/description - Results of above activities input for safety policy and safety requirements - Safety plan 	<p>The RAM policy should only be documented in the safety case as far as it concerns the RAM aspects of the safety functions.</p>

Table 7 – Approaches for system safety demonstration (continued)

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phase 3 risk assessment (referred to as risk analysis in EN 50126-1)	<p>Start at process level Go down to functional level Describe scenarios about the consequences of not mitigating the identified hazards, Describe causes of scenarios and assess the rate of occurrence of the hazard Give the first shot at how to mitigate each unacceptable/intolerable risk, by technical or procedural countermeasures. See also EN 50129 Figure A.3</p>	Analyse identified hazards in the same way as for approach A	Analyse identified hazards in the same way as for approach A	<p>Hazard log has to be maintained during the entire lifecycle Risk assessment should cover causes and consequences for all life cycle phases Special attention should be paid to maintenance and operation (especially for approach B&C). Start with high-level hazards and progress to detailed hazards as you "move" into each subsystem.</p>
Relevant deliverables Safety Case	Hazard Log and risk assessment	Hazard Log and risk assessment	Hazard Log and risk assessment	The hazard log is a key document, and should be included or referenced in the safety management report.

Table 7 – Approaches for system safety demonstration (continued)

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phase 4 System requirements	<p>Safety requirements may be derived from risk assessment or by other means, e.g., by contract or from authorities.</p> <p>THR's are specified by comparison with substantiated data from operating experiences of other railways and other industries (see 5.3.2.5).</p> <p>The process of specifying THR's is in practice done by traversing to and from phases 3, 4, and 5.</p> <p>Check that you are lying within the ALARP boundaries or below the lower boundary for each subsystem and system.</p>	<p>Safety requirements arise from differences between existing and new system which cause an increase in the overall risk associated with the system.</p> <p>Either THR's are based on substantiated data from an existing system or the new system is specified to be technically equivalent (with respect to SI) with the existing system.</p>	<p>Specify safety requirements for hazards that are not covered by the standard.</p> <p>Use THR's for these functions</p>	<p>Define a Certification Project Model with approval milestones. The Project Model is the roadmap to be followed by the supplier, assessor, owner and authority. Must be simple and the no. of milestones restricted.</p> <p>As part of defining the safety organisation, relations with parties involved in the acceptance (including rescue authorities) should be defined.</p> <p>Create Safety Case Structure. The Safety Case Structure defines all the safety cases (typical one for each subsystem + the overall safety case), and the relation to other project documentation. Be aware that this may have to be updated as you progress through the phases.</p>
Relevant deliverables Safety Case	<ul style="list-style-type: none"> - Safety Requirements Specification (+THR's) - Updated Safety Plan - Acceptance Plan with acceptance criteria 	<ul style="list-style-type: none"> - Safety Requirements Specification (+THR's) - Updated Safety Plan - Acceptance Plan with acceptance criteria 	<ul style="list-style-type: none"> - Safety Requirements Specification (+THR's) - Updated Safety Plan - Acceptance Plan with acceptance criteria 	<p>The acceptance plan for the safety functions should go into the safety management report as a basis for the validation program. The acceptance criteria's form basis for the assessment.</p>

Table 7 – Approaches for system safety demonstration (continued)

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phase 5 Apportionment of system requirements	Apportion safety requirements to the relevant sub-systems	Check the correctness and completeness of existing sub-system safety requirements	Check the correctness and completeness of the proven sub- system safety requirements	Writing a good safety specification for sub-systems is of paramount important including specification of acceptance criteria and methods. For apportionment of safety requirements to sub-systems, follow the guidance of Clauses 6 and 7. Finalise configuration management procedures (supplier)
Relevant deliverables Safety Case	- Updated safety plan - Sub system safety requirements	- Updated safety plan - Sub system safety requirements	- Updated safety plan - Sub system safety requirements	

Table 7 – Approaches for system safety demonstration *(continued)*

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phases 6, 7 Design and implementation, and manufacture	In addition to the guidance given in Clause 9, the following should be covered in the Generic Safety Cases: - If you have existing subsystems cooperating with new systems/subsystems it is important to define, describe and analyse the interfaces between systems and subsystems.	In addition to the guidance given in Clause 9, the following should be covered in the Generic Safety Case(s): - Demonstrate that the reference system is comparable and valid as a reference - As for Approach A if you substitute or change systems/subsystems be sure to define, describe and analyse the interfaces between them.	In addition to the guidance given in Clause 9, the following should be covered in the Generic Safety Case(s): - Demonstration of applicability and compliance to the standards and specifications - As for approach A if you substitute or change systems/subsystems be sure to define, describe and analyse the interfaces between them.	With respect to these phases the most important question to be answered is how to deal with existing parts of the system. For all approaches it is important to define and describe all subsystem and system tests before you accept the design milestone as completed. Guidance on the content of the safety case is given in Clause 9.
Relevant deliverables Safety Case	- A record of all (RAM)S validation tasks - Operation and maintenance procedures	- A record of all (RAM)S validation tasks, - Operation and maintenance procedures	- A record of all (RAM)S validation tasks, - Operation and maintenance procedures	The record of safety validation tasks goes into the safety management report, and the results are used in the technical safety report to demonstrate the fulfilment of the requirement being considered. The operation and maintenance procedures must be recorded in the safety case, under paragraph 5 in the technical safety report. A first version of the generic safety cases may be complete at this stage. The application safety case will usually not be ready until phases 9.

Table 7 – Approaches for system safety demonstration (continued)

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phases 8, 9, 10 Installation, system validation and system acceptance	<p>In addition to the guidance given in Clause 9, the following should be covered in the Specific Application Safety Case:</p> <ul style="list-style-type: none"> - A recalculation of the total risk for the complete system, and check against the risk acceptance criteria (MEM/ALARP) OR - Demonstrate that for the total system GAME is true. 	<p>In addition to the guidance given in Clause 9, the following should be covered in the Specific Application Safety Case:</p> <ul style="list-style-type: none"> - Recalculate or re-evaluate the risk for the total system, and check against the risk acceptance criteria (MEM/ALARP) OR - Demonstrate that for the total system GAME is true. 	<p>In addition to the guidance given in Clause 9, the following should be covered in the Specific Application Safety Case:</p> <ul style="list-style-type: none"> - Demonstration of applicability and compliance to the standards and specifications for the total system, - Demonstrate that there are no unintended failures introduced by integration, - Demonstrate that the design and installation is performed according to the requirements specified in the standards and specifications. 	<p>Prior to system acceptance the following activities should be completed:</p> <ul style="list-style-type: none"> All verification and validation activities. Hazard Log (hazards closed by system functions or procedural measures) Writing and validating of operating and maintenance procedures Complete Configuration Management procedures (for the operator/maintainer) Training should be completed and checked before going into operation

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Relevant deliverables Safety Case	<ul style="list-style-type: none"> - Updated safety plan, - Maintenance of record of (RAM)S validation tasks, - Record of acceptance tasks, - Hazard log with all hazards closed out. Those hazards that could not be closed out in these phases should be transferred and controlled in subsequent phases, - Concluding Safety Argument. 	<ul style="list-style-type: none"> - Updated safety plan, - Maintenance of record of (RAM)S validation tasks, - Record of acceptance tasks, - Hazard log with all hazards closed out. Those hazards that could not be closed out in these phases should be transferred and controlled in subsequent phases, - Concluding Safety Argument. 	<ul style="list-style-type: none"> - Updated safety plan, - Maintenance of record of (RAM)S validation tasks, - Record of acceptance tasks, - Hazard log with all hazards closed out. Those hazards that could not be closed out in these phases should be transferred and controlled in subsequent phases, - Concluding Safety Argument. 	<p>The specific application safety case should be issued in this phase. The safety validation tasks will be included in this document. Acceptance tasks can go into the safety case as an answer to the plan made in phases 4, but usually these will not be complete in this phase. Since the safety case is a key document in the assessment process, the assessment report will form an independent document and not go into the safety case.</p> <p>One version of the specific application safety case is a basis for the acceptance process. But the safety case should follow the system through the lifecycle. The deliverables from this phase must be recorded in the next version of the safety case</p>

Table 7 – Approaches for system safety demonstration (continued)

Acceptance approach Life Cycle Phase of EN 50126-1	A - Safety demonstration by complete system analysis and risk calculation	B - Safety demonstration by using safety evidence of an existing system as a reference	C - Safety demonstration when using proven designs	D - General remarks
Phases 11-13 Operation and maintenance, performance modelling, modification and retrofit, and decommissioning and disposal.				Update Configuration Management Procedures. Strict Configuration Control is THE most important issue in these phases. This MUST be in place. This phase requires continuous monitoring whether the claims, assumptions and prerequisites are and remain valid during operation.
Relevant deliverables Safety Case	<ul style="list-style-type: none"> - Updated system documentation - Update operation and maintenance manuals - Record of all verification, validation and acceptance tasks undertaken within this phase. - Updated hazard log/FRACAS 	<ul style="list-style-type: none"> - Updated system documentation - Update operation and maintenance manuals - Record of all verification, validation and acceptance tasks undertaken within this phase. - Updated hazard log/FRACAS 	<ul style="list-style-type: none"> - Updated system documentation - Update operation and maintenance manuals - Record of all verification, validation and acceptance tasks undertaken within this phase. - Updated hazard log/FRACAS 	<p>Update relevant references and analysis as appropriate</p> <p>The specific application safety case should be updated as appropriate</p>
Phase 14 Relevant deliverables Safety Case	<ul style="list-style-type: none"> - Record of decommissioning and disposal - Updated hazard log - Safety plan for decommissioning 	<ul style="list-style-type: none"> - Record of decommissioning and disposal - Updated hazard log - Safety plan for decommissioning 	<ul style="list-style-type: none"> - Record of decommissioning and disposal - Updated hazard log - Safety plan for decommissioning 	<p>Not relevant for operational safety acceptance</p> <p>The need for updating of the safety case is depending on the use of the system. The emphasis should be put on the influence the decommissioning will have on other systems close to this system or with an interface with the system. The hazard log must address any safety implications on these systems, and how they are handled.</p>

7.1.3 Safety qualification tests

Safety qualification tests may be justified for new or complex systems or may be called up by a SRA as an additional proof of safety.

Safety qualification tests are conducted under operational conditions and may be called 'field trials' or 'pilot operation'. The purpose of these tests is to gain increased confidence that the system has met its safety requirements. These tests can never be sufficient alone to demonstrate safety but can corroborate the analytical evidence presented in previous sections by showing that the results predicted by the analysis are actually achieved. They will typically check actual performance against predictions derived from this analysis.

The tests require the system to be put into operational service before final safety approval, therefore appropriate precautions and monitoring must be in place to ensure that safety is maintained during the testing period, including any necessary precautions against risk introduced by the monitoring. Provisional safety approval will normally be required before the tests can start. Safety qualification testing should never be used as a means for bringing a system into unrestricted operational service before its safety case is complete.

7.2 Deterministic methods

Traditionally, railway safety is based on deterministic means of safety demonstration. In the most critical systems there has been a practice to use components with very low failure rates or predictable failure modes. These components have been combined in simple ways so that analysing the effect of the known failure modes has been quite easy. A well known technique for this is FMEA or FMECA. By establishing safety barriers against single failures, by determining common mode and common cause failures and by eliminating these as far as possible, systems with a high degree of safety have been produced. An example of such a system is a relay-based interlocking system.

7.3 Probabilistic methods

With the introduction of more complex systems, such as computer-based systems or systems with unpredictable failure modes, the use of probabilistic methods becomes necessary. With these techniques numerical failure rates for each component are established and by applying FTA or similar analysis technique, the relationship between the failures of different components is established and their contribution to the overall risk is calculated.

However, there are some types of railway subsystem for which probabilistic methods are difficult or impossible to apply. Typical examples for such subsystems are mechanical components that are constructed to be fatigue endurable, i.e. random failures are reduced to almost zero and the failure behaviour is dominated by systematic failures.

In order to justify in a safety case that an overall risk target is fulfilled, it is therefore necessary to combine deterministic and probabilistic means of safety demonstration.

7.4 Combining deterministic and probabilistic methods

One way of combining these two approaches is to use deterministic methods down to a certain level of the system, and then analyse some parts in depth with probabilistic methods. For example, in a relay interlocking this could mean that the actual safety relays involved in changing the aspect of a signal could be established deterministically, while the probability for wrongly setting green aspect would be established probabilistically by using the probability for wrong side failure of each relay. This is a much less demanding task than calculation of the overall wrong side failure rate of the system, while a pure deterministic approach would not give the true value of the safety barriers.

For computerised systems there is also a need for utilising both deterministic and probabilistic methods. While hardware components may have well-established failure rates that allow extensive probabilistic calculation, the software only experiences systematic failures. Software can, on the other hand, at least to a certain extent be analysed deterministically. For example, using modular approaches and strongly typed languages, makes it possible to analyse software by determining its safety barriers and single failure modes. A recommendation on the use of methods for software development is given in EN 50128.

When performing an assessment on safety, a key element is the interpretation of the model (e.g. FTA) limitations. One of the pitfalls is parameter uncertainty and variability.

Variability refers to real and identifiable differences between individual items within a population addressed by the risk assessment (e.g., dimensional tolerances, process variability, material characteristics variability, etc.). True variability does not disappear with better measurement but could be improved with better processes and their controls.

Uncertainty differs significantly from variability. Uncertainty arises from our lack of perfect knowledge, and it may be related to the model used to characterise the risk, the parameters used to provide values for the model, or both (e.g. mechanical loads, earth leakage currents, electromagnetic and electrostatic interference, etc.). In some cases, obtaining better information can reduce uncertainty but this may not always be possible.

More information on deterministic and probabilistic methods, their applications and constraints is included in Clause E.12. Note that Petri Networks is one of the few methods that allows both deterministic and probabilistic modelling (E.11.3).

Nevertheless, combining deterministic and probabilistic methods is still an open issue and no further guidance can be offered at this stage.

7.5 Methods for mechanical and mixed (mechatronic) systems

For components with a failure behaviour that is largely dominated by non-random failures (e.g. fatigue endurable mechanics), the calculation of failure rates is difficult or even impossible, because random failures are almost non-existing for such components.

As a consequence, a large system (like a railway system) will always include components for which it is not practicable to determine a credible failure rate. For the consideration of such components in quantitative hazard analyses, it is recommended to assume a negligible failure rate (i.e., to consider them as being intrinsically safe), provided that the following conditions are met.

- The probability of random failures of the component must be very low, i.e. much lower than the THR of the function to which the respective component contributes. This might include the prescription of specific tests or preventative maintenance, e.g. in order to detect or prevent mechanical wear. Typically, arguments based on natural laws can be found for such components, proving that random failures are (almost) impossible.
- If internationally accepted railway standards or guidelines exist, which set requirements for the safe construction of the respective component (e.g., pressure vessels, wheel sets, axles, etc.) it is sufficient to fulfil these requirements. It has to be demonstrated that the respective component is not only designed, constructed and installed according to the standard but also maintained and operated within its stated environment and maintenance regime. Of course, detailed cause analyses followed by corrective actions have to be undertaken, if any component failures are experienced in order to prevent further failures.
- If there are no specific standards or guidelines, it has to be shown by qualitative arguments (e.g. based on long-term experience, natural laws, scientific publications, independent expert assessment), that sufficient, state-of-the-art quality assurance measures have been implemented which mitigate systematic failures during the construction of the respective component.

A specific challenge is the apportionment of quantitative safety requirements to components for which failure rates cannot be determined (also see 6.4.4). This is particularly relevant if a function is implemented by a combination of different technologies (e.g. a brake system consisting of electromechanical, electronic hardware and software, mechanical, pneumatic and hydraulic equipment).

As mentioned above, it is acceptable to set the (random) failure rate to zero, if certain conditions are met. However, in some cases systematic failures can represent a significant part of the overall failure rate. In these cases, it is recommended to reserve a certain percentage of the overall hazard rate for systematic failures. It is not possible for this report to recommend a specific figure, because this depends on the individual component and its functional integration in the system.

8 Guidance on the risk acceptance principles

8.1 Guidance on the application of the risk acceptance principles

Whilst there could be more acceptance principles, Clause 8 provides further guidance on the risk acceptance principles given in 4.6.3.3 of EN 50126-1 only.

8.1.1 Application of risk acceptance principles

The way to demonstrate that the level of risk achieved is acceptable has to be compliant with national law and application of any of these principles should take account of this. Within this context, use of such principles can provide a basis for establishing risk acceptance levels. However, in the absence of any legal or other such provisions or guidance, the choice of the principle will depend, to a large extent, on the prevailing social/political environment. The relevant parties including any RA and/or SRA should therefore agree the choice and use of these principles.

Table 8 – Criteria for each of the risk acceptance principles

Criteria	ALARP	GAMAB/GAME	MEM
General approach	based on frequency and severity classes; 3 regions of risks to distinguish: intolerable, tolerable and negligible risks. The boundaries between the regions are usually based on the national regulatory regime and/or set by the SRA.	comparison of two systems; the new system has to be globally equal or less risky than the existing one	calculation of THR directly derived from a common independent safety target
Reference of risk	collective or individual risk	reference system	normally to individual risk
Assumptions	additional considerations needed for derivation of THRs for each technical subsystem in the different severity classes	similar system like the new system has to be already existing; requires to analyse the existing (old) system; then GAMAB can be applied	further assumptions on apportionment of risks to subsystems and components to be made
Acceptance criteria	risk reduction needed as long as the system stays within the tolerable or the intolerable region; the reduction actions will be stopped if the system is in the broadly acceptable region or it is in the tolerable region and the needed effort of further risk reduction is grossly disproportionate to the improvement gained.	the new system is less risky or equal compared with the existing (old) system	the individual risk (fatalities per person and time) caused by the system is lower than the tolerable risk derived from MEM
Area of application	setting quantitative risk targets for systems and sub-systems; demonstrate an appropriate level of risk reduction	setting quantitative risk targets for systems; construct qualitative safety arguments; compare two or more equivalent systems (functional or technical equivalence)	setting quantitative risk targets for systems and sub-systems
Strengths	no reference system needed	Keeps, at least, the existing level of safety and tends to improve the level of safety.	no reference system needed; independent safety target is given
Weaknesses	more effort needed compared with GAME; arbitrary assumptions for risk level allocation to sub-systems (partitioning of ALARP region) monetary value of prevented fatality not acceptable in some countries	reference system with experience data needed; mutual compensation of more and less risky sub-systems not clarified.	not widely accepted; arbitrary assumptions for risk target allocation to sub-systems (share in system overall risk)

These approaches can be used for system level risk assessment as well as for the assessment of specific events (i.e. specific subsystem hazardous states or hazards) and can be used both for collective risk and individual risk.

The apportionment and calculation of tolerable risk limits to sub-systems and components is independent from the applied principle and is explained in more detail in 6.3.

8.1.2 The ALARP principle

8.1.2.1 ALARP definition

ALARP, acronym for As Low As Reasonable Practicable is one of the principles used when performing risk assessment. ALARP is based on dividing the risks in domains separated by boundaries of acceptance criteria. Three domains are used:

- 1) the upper risk domain where mitigation actions must be taken;
- 2) the middle risk domain where mitigation actions are evaluated using cost/benefit analyses;
- 3) the lower risk domain where the risks are accepted with no further action required.

The boundaries between the three risk domains are usually based on the national regulatory regime and/or set by the SRA. Normal way of illustrating the three risk domains is to use the F-n curves, i.e. a two dimensional table with frequencies (events/year) against consequences (number of fatalities arranged in groups of consequence classes).

The most important activity that must be performed using the ALARP principle is therefore to define the two boundaries or acceptance criteria, i.e. defining the upper and lower ALARP boundaries (frequencies) for each of the consequence classes, more precisely, the demarcation between the consequence classes and a reasonable assumptions about the number of events that are to be evaluated. Criterion for comparison of risk and effort (e.g. value of prevented fatality and of “grossly disproportionate”) must also be defined. This is generally defined by the RA, in collaboration with the SRA that has jurisdiction.

When defining the acceptance criteria care should be taken not to push the technological envelope, but to reflect the current General Accepted Rule of Technology (GART). There is no sense in specifying acceptance criteria that cannot be obtained by a known technique or is so expensive that it is not feasible. It might be said that this is the essence of the ALARP principle.

Example of ALARP calculation (safety against cost) and for deriving the acceptance criteria using ALARP is given in Annex G.

8.1.2.2 Calculation of Frequencies and Consequences

Assuming that the acceptance criteria have been defined, the next step is to perform Fault Tree Analysis (FTA) of the hazards, which have been identified during the Preliminary Hazard Identification and Analysis (PHIA).

A causal analysis using FTA, where appropriate, can then be performed for every hazard identified. FTA is explained in more detail in Clause E.9.

The task is completed when all the “basic” hazards for which a frequency can be established from either statistical data and/or by engineering judgement have been found. By AND/OR logic operation (i.e. multiplying/adding the frequencies depending on the logic of the fault tree, the analysis is progressed to the hazards at the top of the tree and the resulting frequencies obtained. Events contributing to FTA can be determined by use of the Failure Mode and Effect and Criticality Analysis (FMECA) method (see Clause E.7 for more details on FMECA).

Next the consequences of the hazards may be determined by performing an Event Tree Analysis (ETA) (see Clause E.8 for more details on ETA) or other suitable analysis (e.g. FTA, Markov, etc.) depending on whether the event is time dependant.

For each of the leaves (end states) the consequences of that leaf (damage/harm) must now be evaluated, i.e. if triggered, the number of fatalities this event/hazard may cause. In other words, determine which consequence class each leaf belongs to.

Lastly, the fault/event tree is ready for “harvest”. This is done by collecting all the leaves belonging to one of the consequence class and adding all those frequencies together.

When this is done, in which of the three ALARP domains the risk curve is placed can be seen. If it is in the middle risk domain the risk must be monitored and if reasonably practicable, efforts should be made to mitigate the situation and bring risk curve towards the lower ALARP limit, i.e. the lower acceptance criteria.

There have been some comments that ALARP only gives a collective risk. This is correct but it is rather easy to calculate an individual risk by integrating the computed risk curve and relating it to the total number of persons exposed to the risk.

8.1.3 The GAMAB (GAME) principle

This subclause gives guidance on the application of the GAMAB (Globalement Au Moins Aussi Bon) that is mentioned in Clause D.2 of EN 50126-1. The GAMAB principle is a risk acceptance principle introduced in France. The GAMAB principle states that a new system should be globally at least as good as the current system, including an element of continuous improvement. French authorities legally impose the GAME (Globalement Au Moins Equivalent) principle which is very similar to the GAMAB principle but with less emphasis on continuous improvement.

In the remainder of this report the acronym GAME is used.

GAME principle can be used in different ways for different purposes. This subclause explains the different ways in which GAME can be an effective and efficient approach to assess the acceptability of risk associated with a certain system.

8.1.3.1 Basic principles

There are a few important prerequisites for applying GAME:

- the system under consideration can be compared to an equivalent or similar (with respect to application) reference system;
- a clear system boundary can be defined for both new and reference systems;
- the properties relevant to the risks considered are known for both the new as well as the reference systems;
- any differences in properties need to be compensated for in the setting of risk targets or in demonstration of compliance.

8.1.3.2 Applying GAME for setting quantitative risk targets

First way of applying GAME is for use in setting quantitative risk targets. This can be done on any integration level in the railway system (both for a complete railway system or for a sub system). The reference will always be the contribution from the system to the risk of the complete railway system. In EN 50126-1 an example of such a calculation is given in D.2.2. When making such a calculation a few important issues should be taken into account.

8.1.3.3 Safety indicators used

A calculation can be performed for different safety performance indicators. The example uses casualties/passengers but other possibilities include: casualties per year, number of people injured per passenger-kilometre. It is also important to note that the example given in EN 50126-1 only gives the safety target for one accident (collision) by determining the target collision rate for the new system. For every relevant hazard a hazard rate should be determined. What the relevant hazards are is determined by the properties and the extent of the system under consideration.

8.1.3.4 Compensating for influencing factors

Various factors that influence the safety indicators chosen will have to be compensated for. Factors that can influence the level of risk in the reference system are, for example

- number of people using the system,
- number of operating hours of the system per year,
- number of systems in operation,
- operating speed of the railway the system is used for,
- the crashworthiness of the trains used in the railway system,
- any measures taken to reduce the number of casualties in case of a system induced hazard e.g. sprinklers, emergency exits etc.

These factors need to be compensated for in the calculation of the safety target for the new system. The example in Clause D.2 of EN 50126-1 uses the value of a number of these factors to derive a collision rate λ_C (= Accident rate for “collision”). The generic formula to compensate for relevant risk influencing conditions in the collision rate calculation would be

$$\lambda_{\text{new}} = \lambda_{\text{reference}} * C_1 * \dots * C_i.$$

In this calculation $C_i = F$ (condition parameter in reference system, value of condition parameter in new system). If the risk is proportional to the value of the condition parameter e.g. in the case of different number of people using the new system compared to the reference system, then the compensation formula will be

$$C_i = (\text{number of people using reference system}) / (\text{number of people using new system}).$$

For conditions that effect risks in the reference application in a different way, a different function will have to be defined.

8.1.3.5 Using GAME to construct a qualitative safety argument

In some cases a qualitative argument can be used to demonstrate compliance using the GAME principle. If GAME is used in this way it is very important to establish and demonstrate that the application conditions for both systems are identical. Any differences in application conditions need to be scrutinised for a potential to

- introduce new hazards,
- affect the probability of occurrence of known hazards,
- extend the consequences of known hazards.

Explanation for how such an argument can be constructed is given in Table 8.

8.1.4 **Minimum Endogenous Mortality (MEM) safety principle (EN 50126-1, Clause D.3)**

In 1997 the MEM principle was incorporated into prEN 50126 as an example of one of the Risk Acceptance Principles, together with ALARP and GAMAB. MEM is a scientific approach with predefined assumptions and is based on the work of A. Kuhlmann in Germany in 1981. It should be noted that whilst it has been recommended by the CASCADE research group for use as one of the common safety principles for railway applications, the method for apportioning the value to a railway system is still under discussion.

The MEM criterion allocates the same risk to an individual, independent of each technical system. This homogeneous allocation needs to be justified if the MEM criterion is used.

For more comprehensive explanation of the MEM principle see bibliography. Following paragraphs give a summary of that paper.

MEM incorporates the lowest natural death rate and uses this to assure that the total additional technical risk does not exceed a value equivalent to this natural risk. The natural death rate is focusing only on natural causes of death without any kind of accidents and native malformation influences.

In the range between 5 years and 15 years of age for humans, the natural death rate (R_m) in industrial developed states reaches a minimum for human individuals:

$$R_m = 2 * 10^{-4} \text{ fatalities / (person * year)}$$

The MEM requirement states that the additional overall hazard death rate caused by technical systems (R_t) shall not exceed this limit:

$$R_t \leq R_m$$

and each single system shall not contribute more than 5 % because each individual is endangered by n different technical systems in parallel; the assumption in the MEM principle is:

$$n \leq 20$$

It means that a single technical system shall not lead to a risk of fatality (R) of a single person with a rate of:

$$R \leq 10^{-5} \text{ fatality / (person * year)}$$

The principle does not state how a single system is defined and this should be agreed when applying the principle. However, a railway system may be considered as such a single technical system. Then for each railway subsystem (e.g. rolling stock, infrastructure, signalling) this figure has to be further apportioned in an appropriate manner.

Because society does not accept accidents with a high number of fatalities, MEM introduces a factor "differential risk aversion" (DRA), which results in the following curve (Figure 10) as given in EN 50126-1.

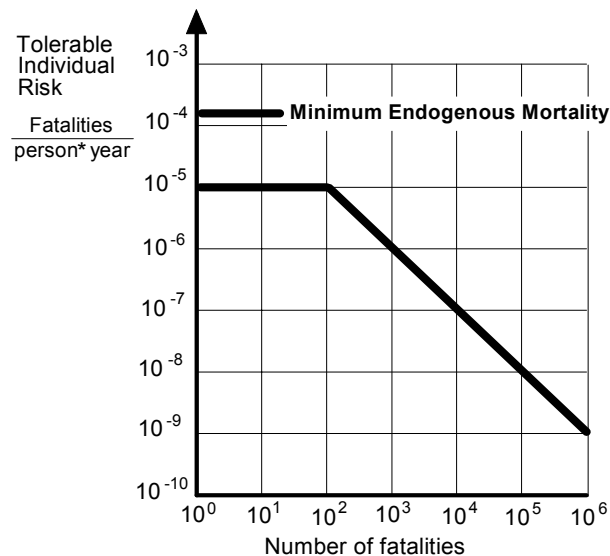


Figure 10 – Differential risk aversion

For MEM calculation the relationship between fatalities, major injuries and minor injuries is given by:

$$1 \text{ fatality} = 10 \text{ major injuries} = 100 \text{ minor injuries (major injuries} \Leftrightarrow \text{people disabled)}$$

EXAMPLE An accident with 2 major injuries and 40 minor injuries will correspond to 0,6 fatalities.

This calculation may also be used when other principles are applied.

9 Guidance on the essentials for documented evidence or proof of safety (Safety case)

9.1 Introduction

Safety cases are referenced in EN 50126-1 Figure 9, Project Phase related tasks. Safety cases are further detailed in Subclauses 6.6 and 6.9 of EN 50126-1. Clause 9 gives further guidance on the different types of safety cases and their contents.

In EN 50126-1 the safety case is defined as: "The documented demonstration that the product complies with the specified safety requirements" The keywords here are "demonstrate", "document" and "requirements". The railways have a long tradition of demonstrating compliance, usually by testing, but this has often been poorly documented. The aim of the safety case is to meet the need for documentation. It is important to be aware that it has to be demonstrated that the product complies with the requirements during its life cycle, not only at the time of approval. Therefore, the operability and maintainability of the safety functions has to be documented along with the reliability and availability of the same functions. So the whole concept of RAM, related to the safety functions, has to be taken into account when these functions are being approved and documented. When building a safety case its purpose should always be borne in mind, e.g., to demonstrate that the "product" (the system/sub-system/equipment) complies with the specified safety requirements. Since this is impossible to prove with absolute certainty, some predictions about the fulfilment of the requirements will need to be made, and the necessary evidence that these predictions are robust will have to be provided. A safety case can be compared with a legal case where the aim is to provide enough evidence to sentence or acquit someone.

EN 50129 provides a detailed account of how the safety case should be structured, and gives some guidance to the contents. Even though it is intended for use in signalling, the main body of the standard is generic, and can be used as a basis for a safety case in other parts of the railway industry. Using the safety case structure described in EN 50129 for all railway systems will provide the industry with a common basis for building the safety case and provide the system under consideration with a holistic safety case that can be a basis for safety operation through the life cycle.

Subclauses 9.6 and 9.4 summarise how the structure and levels of safety cases described in EN 50129 could be applied for all railway systems.

9.2 Safety case purpose

Proof of safety is needed for various purposes. The most important is the industries need to verify that their systems are safe. Approval by a SRA also usually requires a safety case.

One of the other purposes of the proof of safety is to avoid the consequences of product liability law. This law is mandatory in all countries of the European Union. Many other countries have similar laws.

The only possibility of limiting the consequences of this law is to demonstrate, that the system in question has been "failure-free" (in the legal sense) when being brought into operation. The burden of this demonstration is on the supplier. This can only be shown, if a well documented proof of safety exists. It will improve the value or significance of the proof of safety if a competent independent body confirms it.

The term "failure-free" implies also, that all documentation about operation and maintenance of the system in question is

- complete and
- unambiguous.

Otherwise it should be assumed that the system has not been "failure-free".

Hence, it may be necessary to carry out a proof of safety for internal protection of the supplier, even if an authority does not explicitly require it. The proof of safety is documented in the safety case.

9.3 Safety case scope

When starting work on a safety case its scope must first be established. This means defining the system under consideration, the safety functions of the systems, their integrity and the process needed to implement these functions. The project phases of EN 50126-1, which are applicable, and the deliverables from these phases should also be established.

EN 50126-1 lists a large number of deliverables. Usually all these deliverables will be necessary in one form or the other, but they do not need to be separate documents. In many cases it will be natural to integrate a number of them into one document or to just reference them from the safety case. The scope and extent of the safety case must reflect the scope and extent of the actual work that has been done. There is no sense in producing large documents for small and simple products only to satisfy the standard. This is in line with 5.3.4 of EN 50126-1.

9.4 Safety case levels

Whilst EN 50126-1 makes several references to levels of safety cases (particularly in Subclauses 6.6 and 6.9), EN 50129 gives a clearer description of the different levels of safety cases that could be developed. It is advisable to use the following categories:

- generic product safety case;
- generic application safety case;
- specific application safety case.

The philosophy behind these different categories is independent of the type of system. Therefore, it should be possible to use them for all kinds of railway related systems as appropriate. However, it may not be suitable for all classes of systems. The motivation to do this is to make a firm basis for approval by different authorities and consequently save effort by re-use of proven arguments. The safety case that is always needed is the specific application safety case, since that is the top document.

One difference between EN 50126-1 and EN 50129 lies in the use of the word “product”. EN 50129 defines the term “product” as “a collection of elements, interconnected to form a system/sub-system/equipment, in a manner which meets the specified requirements.” While the definition of the safety case uses the word product as a common term for anything you could write a safety case about, (and thereby include system/sub-system/equipment) this definition defines “product” as a building block for any system, sub-system or equipment. A “product” in this meaning of the term could have its own safety case that in the same manner is a “building block” for the generic application safety case and specific application safety case. There may be several levels of generic applications in a specific application, and this will also be reflected in the safety case. See Figure 11.

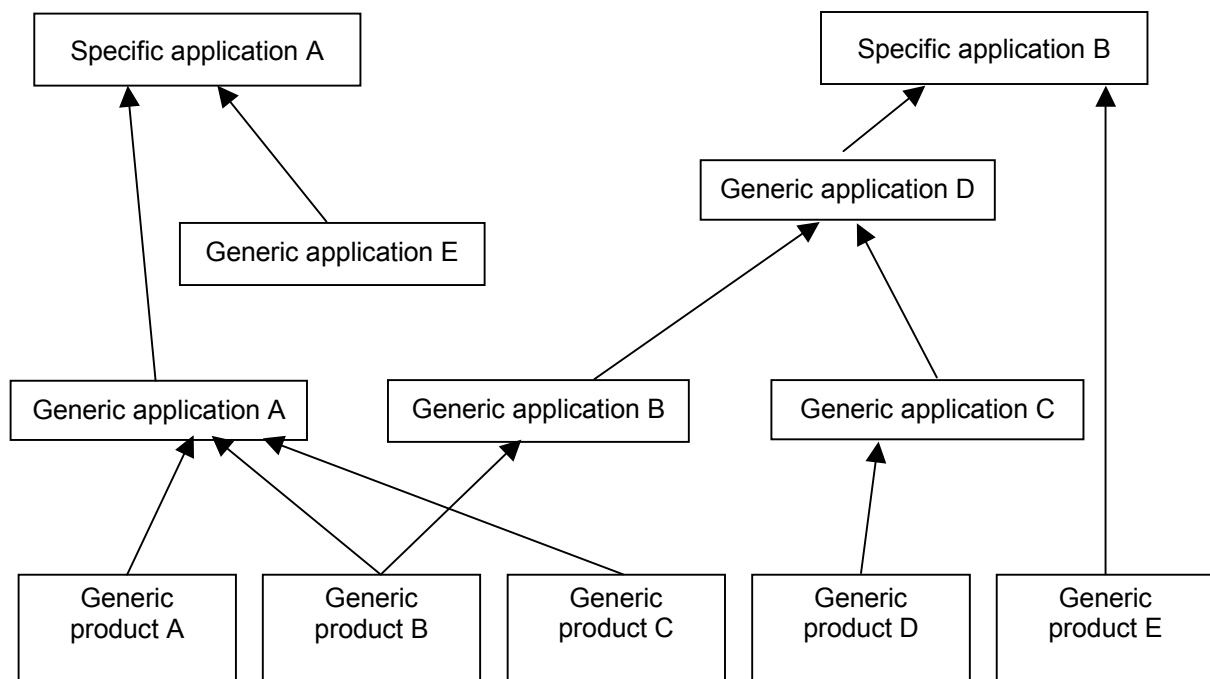


Figure 11 – Safety case levels

9.4.1.1 Generic product safety case (independent of application)

A generic product can be re-used for different independent applications. It is one of the building blocks for the applications.

The generic product safety case aims to prove that a re-usable product meets a specified safety target. Since the safety of a product is dependent on the context in which the product is used, the conditions under which the specified safety target is achieved have to be well defined. The product evidently has to have well defined interfaces to other products. An example of such a product is a safety relay for an interlocking system.

9.4.1.2 Generic application safety case (for a class of application)

A generic application can be re-used for a class/type of application with common functions. It is configurable, but is not ready configured.

The generic application safety case aims to prove that a collection of products in an application or a system meets a specified safety target. There must be evidence to show that the safe products, their interfaces and the context of the application meets the safety requirements placed on the system (application). An example is an interlocking system configurable for different locations or a platform development for rolling stock.

9.4.1.3 Specific application safety case (for a specific application)

A specific application is used for only one particular installation. It is ready configured. For some type of systems there are deliveries of many identical units, for example a series of locomotives. In this case it is sufficient to develop one specific application safety case and confirm conformity for every delivered unit.

This safety case is specified to be divided into two parts, one for the design and one for the physical implementation. For an interlocking system the specific application is one particular installation with all the geographic data (design) ready installed on one particular location (physical implementation). Dividing the safety case into these two parts may not be appropriate for other systems.

9.5 Safety case phases

EN 50126-1 states that the process for developing a safety case should be described in the safety plan, but that the preparation will take place in phase 6. This does not mean that there are no safety case related activities going on during the in between phases. Deliverables from all the phases make contributions to the safety case, and the work on the safety case must begin in phase 1. It is advisable that the safety plan provides timing and delivery of the safety case for a particular phase to be compatible with the progress for the approval of the project.

Safety argument should be presented by showing

- that the safety process is suitable and sufficient (quality management report and safety management report);
- that the product has the required level of safety (technical safety report);
- that the combination of process and product give the evidence necessary for safety approval (conclusion);
- where all the hazards are handled; they could be in the system itself, in a related system, in a technical safety barrier or by operational procedures. The last should be shown as safety related application conditions.

The compliance with the requirements must be valid throughout the life cycle of the product. To ascertain that this remains valid after commissioning, the safety case must also contain the information necessary for the operation and maintenance of the safety functions of the product. The hazard log should identify the hazards that could not be closed before commissioning and also how they are to be dealt with during operation. The control of these hazards will also appear as application conditions. A maintenance plan that states which maintenance activities are required for the safety functions to be valid and descriptions of the operational constraints of these functions are also a part of this documentation.

Finally it is important to note that when developing a new product you make some assumptions about the context of this product. These assumptions must hold true for the system to maintain the required level of safety. The safety case must therefore state these assumptions, and show why they are valid. If the validity of the assumptions depends on other assumptions, these dependencies must be documented as constraints on the use of the system.

In reality this means that the specific application safety case must be a living document through all lifecycle phases. According to EN 50126-1 typically the responsibility will lie with the RA for the first 4 phases and then with the manufacturer until the system is approved (phase 10). Then the responsibility will again be with the RA during the rest of the lifecycle.

A safety case can be handed over from organisation to organisation and updated, as appropriate by the relevant organisation that might be responsible for the update. A more common approach is to have a top safety case handled by the RA covering the phases within their responsibility and refer to the relevant RSI (manufacturers, suppliers, etc.) safety case and other safety cases as appropriate.

During operation the safety case must be updated to reflect the deliverables from phases 11-14. This includes updating the hazard log, the operation and maintenance procedures, and managing the system configuration.

The life cycle model of EN 50126-1 does not take into account the iterative process necessary to make it applicable in reality. Responsibility for the life-cycle phases may be shared by different entities/bodies, depending on their involvement in the activities of the phases. The safety case structure should take this into account.

9.6 Safety case structure

EN 50129 describes a common structure for documenting all safety cases. This overall structure can be used regardless of technology. The advantage of using this structure is that it provides a recognizable framework for any safety case. If there are paragraphs that do not apply to a given system, the actual paragraph can be used to explain why.

The safety case consists of the following 6 parts:

- 1) definition of system;
- 2) quality management report;
- 3) safety management report;
- 4) technical safety report;
- 5) related safety cases;
- 6) conclusion.

Clause 5 of EN 50129 gives guidance on the different parts. This report gives some comments to the guidance. Table 9 gives guidance to the applicability of the different clauses in EN 50129 and the contents of a safety case. Annex H gives three examples showing how this structure has been used in existing projects in real applications.

Table 9 – List of EN 50129 clauses and their applicability for documented evidence to systems other than signalling

Clause in EN 50129	Title	General applicability and brief overview of contents
1.	Scope	EN 50129 is intended for signalling purposes. The intention of this table is to provide some guidance on which clauses are recommended for application to other railway systems and what their contents should be.
2.	Normative references	This list of standards apply as given in the title of the standard.
3.	Definitions and abbreviations	These definitions apply. If they differ from the definitions of EN 50126-1, the latter should have precedence.
4.	Overall framework of this standard	All annexes should be considered informative for other systems than signalling.
5.	Conditions for safety acceptance and approval	
5.1	Safety case	The structure is generic and could be applied to all systems.
5.1	Part 1 Definition of system	This includes, for all systems: - purpose of the system, - operational conditions, - system boundaries, - interface between safety related and non safety related parts of sub-systems and the responsibility for demonstrating compliance for them.
5.2	Evidence of quality management	The need for a quality management report and its contents are independent of the system under consideration. The quality management report should cover all activities the organisation delivering the safety case is responsible for, related to the relevant lifecycle phases. The quality management report does not need to be a separate and self-contained document. In many cases it is sufficient to make reference to the quality management system, and the outputs from this. These outputs must be made available to assessors and approval authorities on request. The topics in the list of 5.2 of EN 50129 should be covered.

**Table 9 – List of EN 50129 clauses and their applicability
for documented evidence to systems other than signalling (continued)**

Clause in EN 50129	Title	General applicability and brief overview of contents
5.3	Evidence of safety management	The safety management report should document that safety management is undertaken according to EN 50126-1. The headlines of 5.3.3 to 5.3.13 in EN 50129 apply to all systems, but the extent and depth of each clause in the safety management report will depend on the system under consideration. As for the quality management report, the safety management report does not need to be a separate and self-contained document, but referenced documents must be open for inspection.
5.3.1	Introduction	Applicable to all systems
5.3.2	Safety lifecycle	This part should contain a description of the relevant phases for this safety case. One example is that the safety case handles only a limited number of phases, while a top level safety case refers to this one as a related safety case. Typically this is the case when a supplier handles phases 4-10, whilst the RA handles phases 1-4 and 11-14. The use of 14 phases may, sometimes, be inconvenient. If it is decided to operate with fewer phases, the motivation for this should be stated in 5.2, and the safety activities related to each of these phases described here.
5.3.3	Safety organisation	This part should address: - Description of the organisation undertaking the safety management, - Documentation of personnel competence, - The use of verifiers, validators, and assessors and their level of independence.
5.3.4	Safety plan	This part should address: - Safety related activities in all agreed lifecycle phases, - Safety case plan, The safety plan must be a living document that is updated and reviewed when alterations are made to the system under consideration.
5.3.5	Hazard log	Hazard log should be created and maintained during the life cycle. All identified hazards must be assessed, and if possible closed before moving to the next phase. If hazards remain when handing the system over to a different organisation, the remaining hazards must be clearly identified with all their application constraints and any implication this hazard will have on the operation and maintenance must be clearly stated.
5.3.6	Safety requirements specification	All systems with safety functions will need this specification. If it is included in the functional requirement specification, it must be clearly stated which functions are safety related or safety critical.
5.3.7	System/ sub-system/ equipment design	This clause is applicable to all systems, but is particularly relevant to electro-technical and programmable systems. It should be documented which design methodologies have been used. The use of recognized standards is highly recommended.
5.3.8	Safety reviews	A plan for safety reviews should be included in the safety plan, and their results should be documented in the safety report.
5.3.9	Safety verification and validation	The verification and validation plan could be part of the safety plan, but could also be a separate document. The results of the activities should be documented in the safety report.
5.3.10	Safety justification	The safety justification is the main purpose of the safety case, and must be built upon a solid chain of arguments that proves that the system under consideration meets the safety targets.
5.3.11	System/ sub-system/ equipment handover	The key documents at handover are: - Safety case including hazard log and application constraints and conditions, - Safety assessment report (if there is one), - Operation and maintenance plan.
5.3.12	Operation and maintenance	After handover the operating company must form the necessary procedures based on the documentation above. These procedures must take into account: - Remaining hazards, - Application conditions and constraints, - Operation and maintenance plan.
5.3.13	Decommissioning and disposal	If any particular actions are defined in the safety plan, the decommission and disposal must be in accordance with them.

**Table 9 – List of EN 50129 clauses and their applicability
for documented evidence to systems other than signalling (*continued*)**

Clause in EN 50129	Title	General applicability and brief overview of contents
5.4	Evidence of functional and technical safety	The technical safety report is an essential part of all safety cases. The structure given in EN 50129 is basically applicable, but the content of each section might need some alterations, particularly for non-electro technical systems.
	Section 1 Introduction	This section is applicable to all systems. In the introduction this should be included: - Overview description of the design, - Technical safety principles in use, - Identification of technical standards underlying the design.
	Section 2 Assurance of correct functional operation	This section is of fundamental importance. For electro technical systems there is some guidance in Clause B.2 of EN 50129. These are also partly applicable to mechanical and hydraulic systems. Regardless of the kind of system in question, the main issue is to go through the design, (a walk-through or a “what if” study) and determine if it is fit for its intended use. This is also part of validation and assessment, but must also be carried out at design level. When the design is deemed as correct and in line with the functional requirements, it must be shown that the system in question is built according to the design. These activities can be part of the verification process as the system passes through the life-cycles. It must be recognised that Clause 2 is applicable for fault free conditions only.
	Section 3 Effects of faults	While the section above deals with system in normal operations, this section addresses the behaviour of the system under faulty conditions. Again there is some guidance in Clause B.3 of EN 50129. There is also a basic principle that a single failure with cannot be reasonable excluded should never be allowed to cause an accident (for more details see 6.5. This is a simple principle to apply, but care must be taken that a single fault that is very unlikely to occur is seen as more critical than a combination of multiple faults with high probability when both situations could lead to an accident. An example is the value of a single high integrity safety barrier against two human safety barriers. Care must be taken here, and might need some calculation. For civil works it is usually more appropriate to demonstrate that the construction will not fail.
	Section 4 Operation with external influences	While the section above addresses faults coming from the system itself, this section handles the effect of the environment on the system. Clause B.4 of EN 50129 gives some guidance on this, which is mostly applicable to all systems.
	Section 5 Safety-related application conditions	This very important section should perhaps have been a heading on the same level as the technical safety report. Clause B.5 of EN 50129 gives some guidance on how to derive the application conditions. This should be documented here, but the resulting application conditions and constraints must go into the conclusion of the safety case.
	Section 6 Qualification tests	This section should contain evidence to demonstrate successful completion of the safety qualification tests under operational conditions. In many countries there are specific requirements for how these tests are carried out, and by whom. The procedures for these tests therefore need to be agreed with the RA or with the SRA.
5.5	Safety acceptance and approval	This clause addresses the safety acceptance and approval process for safety related electronic systems. It does not form part of the safety case structure. It is a safety management activity (included in safety plan) and might still be applicable to other systems, Whether or not to use this process must be agreed with the RA or the SRA as appropriate.
5.5.1	Introduction	In this clause it is described how the specific application safety case could be divided in two parts, the application design safety case and the physical implementation safety case. This may also apply to systems other than signalling, but care should be taken to avoid making the safety case structure more complex than necessary.
5.5.2	Safety approval process	Agree the safety approval process with the railway authority or the SRA.
5.5.3	After safety approval	This clause states that any modification to a system after approval should go through the same qualification procedures as the original system. This includes updating the safety case. It is of high importance that this is done. Otherwise the proof of safety is no longer valid. This must be done for all systems or sub-systems.
5.5.4	Dependency between safety approvals	This clause describes the hierarchy of safety cases. This is described in more detail in the clause below.

**Table 9 – List of EN 50129 clauses and their applicability
for documented evidence to systems other than signalling (continued)**

Clause in EN 50129	Title	General applicability and brief overview of contents
5.1	Part 5 Related safety cases	<p>Related safety cases are all those safety cases on which the proof of safety for the system under consideration depends. These include, but are not limited to, the safety cases for all sub-systems. Safety cases on all levels may have related safety cases. For a specific application safety case the generic safety cases for applied products must be referenced as well as the generic application safety case, if there is one for the system under consideration. Safety cases for older versions of a system or product may also be relevant, and can minimize unnecessary extra resources and paper work. All documents that are referenced must be made available to those who receive the safety case. If a referenced document cannot be made available in whole or in part, then the required information must be given otherwise. It is entirely up to the producer of the safety case to provide the necessary documentation. The structure of the safety case (e.g. how the different documents are related to each other) is demonstrated in the safety case plan.</p> <p>There may be other related safety cases, especially where the system being put into service interfaces with another. For example, the safety case for putting a new train onto existing infrastructure, in special cases, may require the safety case for the existing infrastructure to be amended. This is usually the case if the assumptions and specifications regarding the interface are changed.</p>
	Part 6 Conclusion	<p>Conclusion should state if there is sufficient evidence in support of the claims made to the safety of the system and if the risk acceptance criteria's have been met.</p> <p>Any application constraints, limitations or conditions which have to be met should be stated clearly, especially where they might affect the ability of the safety case to support a higher level safety case, which depends on it.</p>

9.7 Safety assessment

9.7.1 The scope of the safety assessor

A safety assessor is the person performing safety assessment. EN 50126-1 defines assessment as: “The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product.”. Safety assessment therefore applies to the judgement that all the conditions for safety acceptance have been satisfied. Subclause 9.7 suggests how to make this judgement.

EN 50126-1 says little about the different activities involved in a safety assessment. But to be able to make a judgement about the product (or system), it is necessary to consider both the system and its development process. The activities of a safety assessor should always include

- review of the adequacy of the safety requirement specification and the products ability to fulfill it,
- review of the safety and quality organisation,
- review of the safety process. Key elements here are the safety plan, the hazard log and the safety cases.

The activities for performing the safety assessment are

- safety audits,
- safety reviews,
- design analysis
- witnessing testing activities.

The results of these activities should be documented in the safety assessment report.

9.7.2 The independence of a safety assessor

The assessor must always be independent from the project organisation. Since the suitability of a product depends on all life-cycle phases, the independence from all involved parties is crucial. The level of this independence should depend on the criticality of the system. EN 50126-1 does not say anything about who performs this assessment and their level of independence from the project organisation. EN 50129 defines the level of independence for signalling systems. In principle this can also be used for other systems. Many

safety regulatory authorities require a certain level of independence of the safety assessor for all safety critical systems. This may also be a customer requirement.

EN 50129 states that a safety assessor should not belong to the same organisation as the project team, the verifier or the validator. In specific cases the assessor could be part of the same organisation as some of these parties, but other measures must then be taken to assure safety. One possible solution is a direct line of reporting between the assessor and the SRA.

This is well in line with the view that the safety assessor should look upon the product with the eyes of the SRA. Since the SRA is often a governmental body, the direct reporting may prove difficult, but some direct contact should be possible to maintain. In some countries independent safety assessors have to be approved by the national SRA. Because there are a lot of differences between countries, with respect to dealing with independent safety assessors, the level of independence and the means to achieve it must be agreed between the parties involved in the approval process at the start of a project.

It will increase the confidence in the safety case if it is approved by an independent safety assessor. On the other hand it must be noted that the use of an independent assessor does not change the responsibility for the product.

9.7.3 Competence of the safety assessor

Competency requirement for a safety assessor should be agreed with the SRA. Such requirements may differ between countries due to different educational and training environments and a common basis cannot be given in this report.

However, subject to approval by the SRA, a safety assessor may be required to be qualified to a university degree level standard or equivalent and be able to demonstrate sufficient (e.g., say a minimum of 5 years) experience in a responsible position, in safety engineering with thorough understanding of the relevant railway engineering domain.

NOTE In UK the Institution of Electrical Engineers / British Computing Society / Health and Safety Executive has specifically addressed the issue of competence of safety related practitioners and the results published as "Safety, Competency and Commitment" (IEE 1999, ISBN 0 85296 787 X).

9.8 Interfacing with existing systems

All systems interact with other systems. EN 50126-1 gives little guidance on how these interfaces should be handled. This report gives some hints on the precautions to be taken to avoid these systems interfering with the safety level of the system under consideration.

9.8.1 Systems developed according to the EN 50126-1 process

These systems have a safety case. This safety case should document the safety functions of the system and it is often easier to assess its interactions with the new system over the common interface. However, it's important that this is assessed, since the new systems may have functionality that the existing system was not intended to interface with. This assessment may be performed through document review and testing. This must be documented in the safety case of the system under consideration, and the safety case of the older system must be referenced under "related safety cases".

9.8.2 System proven in use

These are usually old systems developed long before EN 50126-1, but with many hours of operation behind them. The assessment here becomes complicated, since these systems are often badly documented. However the assessment can build upon experience data, review of drawings and existing technical documentation, and rigorous testing. The results from this assessment must be documented in the safety case of the system under consideration, usually in the specific application safety case. In some cases it might be more beneficial to replace them since interfacing them with new systems could cause unforeseen hazards and failures.

Another possibility is to make a retrospective safety case on the old product. This can be done, but is usually more complicated than the other methods. In retrospect you can never expect to be able to cover all aspects of a safety case.

9.8.3 Unproven systems

These are systems that fall under the label “Commercially off the shelf products” (COTS), “Systems of unknown pedigree” (SOUP) or undocumented software. These systems must always be regarded as hostile, and all kinds of inputs must be expected from them. This means that it must be proven that the system under consideration is able to control, in a safe manner, all inputs (intended as well as unintended) that originate from such systems. This demands a thorough testing of all possible inputs or sequences of inputs. That can sometimes prove impossible. Another method is to place a safety barrier between the systems that only let valid inputs through. This safety barrier must have its own safety assessment. It is important that this is documented in the safety case.

9.9 Criteria for cross acceptance of systems

Cross acceptance is an aspect of the technical and legal process principally aimed at establishing the fastest route to the deployment of products, systems or processes in a target (new) context or environment. Subclause 9.9 provides a brief introduction to the basic premise and framework for cross acceptance. More detailed information and guidance is within the scope of CLC/TR 50506 ‘Application Guide for EN 50129’.

One of the most important benefits a safety case regime, as described above, offers is the possibility for cross acceptance. A product, system or process considered for cross acceptance is generally assumed to satisfy the qualifications for reliability, tolerable safety and environmental performance in their native (original) context or environment. Cross acceptance is usually carried out on generic products or generic applications. Cross accepting a specific application requires the target environment and application to be identical with the native environment and application. This is very unlikely and as a consequence, certain basic premise and principles need to be observed.

9.9.1 The basic premise

The cross acceptance of a Product, System or Process (PSP) is implicitly founded on a number of key assumptions and conditions namely

- a) the PSP has been specified, designed and developed by a competent, capable and reputable organisation,
- b) the PSP has been scrutinised, analysed and assessed through a rigorous process to assure its relevant safety, environmental and technical performance and this process has been documented at an appropriate level of detail,
- c) the PSP has been assessed for its compliance with regulatory requirements and best practice standards and codes of practice,
- d) the assessment has been peer reviewed and the PSP approved or certified by a relevant competent body or authority in its native environment implying tolerability of its risks subject to specified constraints and controls,
- e) the PSP has preferably got a demonstrable record of adequate verification, validation and testing or trouble free operation in its native environment,
- f) the PSP has potential for wider scope of application beyond its initial native environment as is or through small-scale redesign and adaptation,
- g) there is a perceived or real commercial, safety or environmental benefit or need in adapting the PSP for use in new (target) environments,
- h) there is an implicit or explicit record of above which can be made available to relevant third parties as deemed appropriate.

The following aspects are important when assessing the native and target application:

- a) a record of technical, operational, commercial, environmental, quality and safety performance requirements;
- b) specification or description of relevant operational environment, scope, boundary and interfaces;
- c) description of the system architecture and composition including rules & procedures, people and competence issues and automation aspects;
- d) description of the operational, maintenance and retrofit processes;
- e) description of the operational scenarios under normal, degraded and failed modes of the system;
- f) description of emergency response arrangements and procedures.

Even though not always stated, these conditions and assumptions are required or perceived to hold true for the purpose of cross acceptance.

9.9.2 The framework

The framework developed and proposed here for cross acceptance of PSPs essentially comprises 7 key principles listed below.

1.1 Establish a credible case for the native (baseline) application:

The basis is the PSP and its performance in its native environment and application. The necessary documentation consists of all requirements the native environment and application imposes on the PSP, and records of the PSPs performance in this environment and in this particular application. The safety case(s) are basic documentation here, provided they cover all the life cycle. Other key documents are assessor reports, certificates and the final acceptance from the SRA.

1.2 Specify the target environment and application:

The requirements arising from the new environment and application, also on basis of the life cycle, must be documented.

1.3 Identify the key differences between the target and native cases:

This includes material changes in performance requirements, operational environment, interfaces and operational modes.

1.4 Specify the technical, operational and procedural adaptations required to cater for the differences:

The similarities and differences between the native and target application must be identified and assessed. On basis of this the necessary adaptations must be identified, and the feasibility of these adaptations established.

1.5 Assess the risks arising from the differences between the native and target application:

This includes risks arising from technical, operational and environmental differences. These risks might have to be mitigated by further adaptation of the PSP. All assumptions and evidence must be verified and validated, and risk reduction or risk mitigation should be identified.

1.6 Produce a credible case for the adaptations adequately controlling the risks arising from the differences:

On basis of the above a credible case for using the PSP in its target environment can be established.

1.7 Develop a generic or specific cross acceptance case:

A generic or specific cross acceptance case for the PSP in the target environment and application should be made.

Annex A

(informative)

Steps of risk assessment process

A.1 System definition

A system comprises not only of its technical components but also the interaction with humans developing, operating, and maintaining it. Therefore, these should be included in the definition and documentation of the considered system. Concept of system hierarchy is explained in 4.3.

Boundaries and functions of the system under consideration should be established before any hazards are identified. Therefore, the following aspects should be taken into account and clearly documented:

- System boundaries and interfaces, e.g.:
 - interfaces (with other systems or with the environment) that define the boundaries of the system to be analysed and the interactions between them.
- Intended function, e.g.:
 - system functions which are to be included in the analysis and system functions which are to be excluded, if any.
- Working environment, e.g.:
 - influence on neighbouring objects, systems, and environment including operational personnel, passengers, and public,
 - accurate definitions of physical and operational conditions and the environment under which the system works,
 - description of any necessary operator actions. Also identifying persons that are permitted to carry out these actions, indicating the skills and qualifications required and the basis for these actions, if any,
 - if no human activities have been included in the analysis, the reasons for this should be stated.
- Modes of operation, e.g.:
 - normal, abnormal/degraded mode of operation, disconnect/connect states and transitions, etc., and their interactions,
 - operational scenarios considered within the analysis, e.g., effects of maintenance operations (how, how often and by whom is the system maintained?),
- External Requirements:
 - external safety requirements resulting from the overall safety policy of the RA, from prevailing legal considerations, or from standards that could impose a pre-defined THR;
- Version of the system and related documents:
 - if assumptions are made about particular functions or subsystems that makes the system being considered deviate from an existing version, then the deviations should be explicitly stated and justified,
 - if the system is modified later during its life cycle, it may be necessary to revise the risk assessment or even to compile a completely new assessment,
 - the potential effects of new system versions on the safety of the railway system should always be checked by reviewing the risk assessment, in particular the hazard log.

NOTE For software related items it is clear that software cannot be studied alone. Only when software is loaded into a system operating within a certain environment and fulfilling a certain function is it viable to perform hazard identification.

A.2 Hazard identification

Boundary of the system under consideration and its interactions with its environment need to be understood before conducting hazard identification (also see 4.3 and 6.2.2).

To identify hazards in a specific system, the system states and functions are examined and any weaknesses together with their possible consequences, at the boundary of the system (e.g. its output), are determined. The objective of hazard identification is to stipulate clearly which of the system states are regarded as failure states. Hazard identification should be performed or monitored/controlled by the body/entity (see 4.2) responsible for the system/subsystem/product under consideration (also see 6.2.2) and be a subject of assessment by an appointed safety assessor. When performing hazard identification, one should always look out for interactions that have not been identified and that have the potential to be implicated in hazards.

Personnel with full range of knowledge and competencies to consider the whole system and its operation, particularly in relation to the occurrence of a hazard, should be involved.

Systematic identification of hazards may be performed empirically or creatively. These are described below:

A.2.1 Empirical hazard identification

Empirical hazard identification relies largely upon knowledge and experience of the past to identify potential hazards. Whilst it is sometimes sufficient for routine undertakings, novel or modified undertakings will generally also require a more creative form of hazard identification.

Empirical hazard identification methods include

- checklists (see Annex B), and
- structured walkthroughs.

The following more rigorous empirical methods may also be used:

- Failure Mode and Effects Analysis (FMEA) for equipment and systems (see Clause E.7), and
- Task Analysis for man-machine interfaces.

These latter techniques identify particular component failures or human errors, which may lead to occurrence of hazards. They do, however, require a detailed knowledge of the failure modes of components and sub-systems, including human actions and likely errors.

A.2.2 Creative hazard identification

Creative hazard identification methods provide systematic techniques to encourage lateral and imaginative creative thought. Ideally they should employ a team-based approach to exploit the diverse and complementary backgrounds of a range of individuals. They include:

- brainstorming,
- Hazard and Operability Studies (HAZOP) (see Clause E.4).

Empirical and creative hazard identifications complement one another, increasing confidence that all significant hazards have been identified.

A.2.3 Foreseeable accident identification

Since a hazard is an accident precursor, identification of foreseeable accidents is an important step in the risk assessment process. It is advisable to consider past records and data, previous studies, etc., as appropriate, and involve the widest range of competencies to ensure that all foreseeable accidents have been identified. Consideration should also be given to identifying the most exposed groups, which will be subject to the assessment of individual risk.

As a part of the accident identification process the routes that the trains operate over should be considered to determine if there are any potentially high risk locations (tunnels, long bridges, below ground stations, etc) for which additional controls may be required.

The accident types may be classified into the following categories.

A.2.3.1 Train accidents

This applies to accidents involving trains. For example:

- collisions,
- derailments,
- striking obstacles, such as obstructions on the track or at level crossings,
- fires,
- explosions,
- electrocution,
- pollution (e.g. toxic gas).

A.2.3.2 Inside train accidents

This applies to accidents causing injuries during or in connection with train operation (excluding injuries sustained in train accidents), for example accidents during boarding and alighting from trains and accidents on board trains, such as slips, trips, falls, electric shock, pollution, trapping of body parts, etc.

A.2.3.3 Station accidents

This applies to injuries resulting from, for example, pollution, slips, trips and falls on platform, on stairs, on escalators, etc.

A.2.4 Hazards

Hazards arise mainly from the physical conditions that are typical of the system under consideration and from inappropriate human behaviour.

They could arise during

- normal operation, failure conditions (malfunction), exceptional conditions (e.g. emergency, failure recovery, etc.).

They may result from

- a hazardous full or partial loss of operational functions, full or partial loss of protection functions, adverse effects on human health conditions.

The physical effects from which hazards could arise are typically

- mechanical power/energy,
- electrical current,
- thermal effects,
- sound/air pressure effects,
- electromagnetic fields,
- chemical effects,
- biological effects,
- radioactivity, etc.

A hazard can cause more than one type of accident. For example, a speedometer failure may cause derailment, collision, doors opening at wrong locations, etc.

Similarly, different types of hazards could cause same type of an accident (e.g. a collision).

For each type of operation or journey, the likelihood that additional hazards may occur as a result of the following should be considered:

- i) perturbed running e.g. train failure,
- ii) degraded or abnormal operations,
- iii) day or night operation,
- iv) extreme weather conditions,
- v) disabled people or other vulnerable groups,
- vi) overcrowding on stations or in trains,
- vii) criminal activity,
- viii) other conditions specific to the duty holder's operations.

For each of these procedures, any assumptions made during the structuring phase and later during the analysis phase should be documented.

Hazards identified from an identification session should be sorted in order to create a set of clear unambiguous hazard clusters with as few dependencies as possible (defined as "c-hazards").

Once the hazards are identified, the system should be subjected to a critical appraisal in order to introduce changes that either reduce these hazards or mitigate their effects.

To reduce the number of follow-up analyses, main hazards should be identified (e.g., by means of "what if" analysis) and, whenever possible, grouped (using an agreed hazard grouping structure) as "c-hazards". They should be further assessed to determine whether they are mutually independent, or whether they have common causes or identical effects. Dependencies should be visually represented in a failure tree analysis (causes) or in a consequence analysis (effects).

Guidance on the different hazard grouping structures is given in 5.5.2.

Where, in the course of risk assessment, certain hazards are not to be considered further the reasons for non-consideration should be stated (e.g., "probability of occurrence too low", "same cause or consequence as ...", etc.). The remaining hazards, i.e., those that are to receive further attention in the analysis, should be identified as such – i.e. "c-hazards".

More information about techniques and methods at different stages of development is given in Annex E.

Hazard identification and risk assessment process is applicable for all phases of system lifecycle (as given in EN 50126-1) and typically as follows:

- a) at system concept stage, by analysing its environment and application including the operational conditions and constraints;
- b) during development of new systems, subsystems, and products including manufacturing, installation, and commissioning with adequate processes and tools. This also concerns maintenance programme and operational instructions and integration of subsystems and systems, and subsequent operation and maintenance;
- c) at handover between a body/entity responsible for system design to the body/entity responsible for its operation and/or maintenance;
- d) in a system already in commercial operation, for example in order to insert auxiliary safety-related subsystems/products to further reduce inherent risks in the system;
- e) at integration of a system, subsystem, or to qualify products for acceptance of their use in an overall system;
- f) at modifications of systems, subsystems, products, or processes;
- g) failure reporting of suspicious deficiencies for a system in operation;
- h) at decommissioning of a system, subsystem or product.

NOTE Care should be taken to ensure that hazards arising at interfaces between sub-systems or between different bodies/entities have been considered involving both parties and also recognising that an action or system behaviour on one side of the interface could manifest in a hazard on the other side of the boundary.

A.3 Hazard log

An example of the contents of a hazard log is as follows.

i) Description of the hazard:

Brief description of the signs and effects that signal that an error or failure has occurred, and the manifestation time: ("Is the failure apparent immediately, only after some time, or not directly detectable?").

- brief description of the failure/condition;
- systems phase/operating state/transitional state when the event occurs complemented with any influencing environmental conditions;
- brief description of the consequences
 - for the system being analysed,
 - for the railway system.

ii) Computed risk level, from the risk assessment process, (before measures for risk reduction or elimination) from estimated frequency/likelihood of the hazard and the assumed consequent accident severity.

According to 4.6 of EN 50126-1 risk can be recorded as

- negligible,
- tolerable,
- undesirable,
- intolerable.

iii) Examples of measures taken to reduce the computed risk

To reduce the predicted risk the following types of risk reduction measures should be considered:

- introduction of a safety or monitoring system;
- introduction of design measures;
- computational evidence and/or representative testing;
- operational measures;
- maintenance measures.

Analyses made should take into account any limitations, accuracy of the information, and may also include confidence levels on data and sensitivity analysis.

iv) Agreements reached/Actions defined/Person responsible/Notes.

v) To document what action should or had to be done to manage the hazard.

vi) Risk level achieved, from the risk assessment process, (after introduction of measures for risk reduction or elimination).

vii) Documentation of what level of risk according to 4.6 of EN 50126-1 that will be expected after introducing risk reduction measures.

The log can be extended with Directory Data containing

- references;
- list of safety records- name-version-date;
- physical location;
- to be co-operated with project/product management documentation

and a Journal section containing

- day of notice;
- entry number;
- source of the information (person that announced the hazard);
- cause – description;

– referenced documents.

A.4 Consequence analysis

EN 50126-1 does not imply a worst-case scenario that a hazard would always lead to an accident. It is particularly important for railway operators to know what the consequences of the identified hazards are. Hazard identification phase is therefore followed by a so-called consequence analysis, which assesses the progression of the event after occurrence of a hazard. EN 50126-1 does not rely on the worst-case scenario of each hazard leading to an accident. As such, contrary to a worst-case assessment of a hazard, which may well end up with an incident or accident, a consequence analysis provides a clear, comprehensible and operationally relevant representation of the individual sequences, actions, and possible effects of the hazard by carefully identifying and quantifying the intermediate events (also see Figure 3).

Conducting a consequence analysis involves gathering and documenting the data that describes the effects of a hazard. The recommended approach is to use accident data, wherever available, and/or to interrogate individuals with expert knowledge of the current or future system or process environment (so-called “domain experts”).

A number of intermediate states or events can arise in the period between the occurrence of a hazard and the emergence of its possible consequences. The path taken by the system through to its end state depends on these intermediate states. The end state of the system can range from a random or controlled safe state, a safe state that can be reached with the help of a particular safety measure, or an accident.

One technique particularly well suited to representing the way in which a system develops, once a hazard has occurred, is an event tree analysis (ETA), (also see Clause E.8). ETA facilitates a structured understanding of the temporal and causal development of a system from the initiating event through to the final outcome or accident. ETAs also include those risk-reducing intermediate events and states that do not lead to an accident. It must be recognised however that ETA is based on pure probabilities and does not take into account the duration of an event.

It is important to recognise that such events are independent of the system under consideration, i.e., they are not control mechanisms inherent to the system itself, but are external events that can be of technical, operational, or environmental.

In contrast to qualitative consequence analysis, which focuses on the progression of events that are triggered by the occurrence of a hazard and that lead either to an accident or to the system entering a safe state, quantitative consequence analysis is concerned with quantifying the probability of occurrence of the various intermediate events.

In most cases, statistical records may only yield numerical data for end states (e.g., on the extent of damage caused by specific type of accident). To reduce, to a reasonable level, the effort required to establish numerical data for intermediate states in the event tree, it is often expedient to initially establish rough estimates of the intermediate events (risk reduction factors) on the basis of expert opinion and then to identify which branch of the event tree dominates the final end state.

Once the critical path has been identified, further surveys can be conducted to corroborate the probability values, i.e., find further mitigations or justifications that may lower the probabilities of the intermediate events that make up the critical path.

NOTE The effort spent on conducting a qualitative and a quantitative consequence analysis should be in the approximate ratio of 70:30. This ratio underlines the fact that it is more important to represent those post-hazard event sequences that correspond to actual or expected operational incidents rather than to spend excessive amounts of time establishing and documenting the probability of occurrence of individual intermediate events that have only a marginal effect on the final outcome of the system.

To reduce uncertainty associated with the estimated values, detailed analyses of events in the critical path may need to be conducted (including sensitivity analyses to determine how the probability or frequency of occurrence of particular intermediate events influences the likelihood of a particular outcome).

A.5 Hazard control

For hazard control, it is a pre-requisite that the overall implementation requirements, including safety requirements, resulting from the risk assessment are set at the level of information available at this stage. Hazard control activity is then to satisfy that the implementation meets the overall requirements.

If it is not possible to implement the overall requirements, it should be considered whether

- the requirements were set right,
- it is possible to make the requirements more precise,
- it is possible to reduce the hazard impact or risk by other means outside the suggested implementation.

Measures to be considered are

- elimination,
- substitution,
- engineering controls,
- administrative controls,
- providing protective systems/subsystems/products/equipment.

Example of elimination is to remove the causes of the hazard or eliminate the effects at the design phase.

Substitution means that a hazardous element is substituted with a non-hazardous element. An example is choosing fireproof cables when fire is a hazard.

Engineering controls means that safeguards/safety barriers are inserted to minimise the exposure or probability of hazard, i.e., isolating the hazard. The hazard remains and becomes active if the defence is for any reason removed or breached. Examples of measures are

- simplification;
- decoupling;
- redundancy.

Simplification uses the benefit that a simple system has a small number of unknowns, and is therefore better testable and more easily understood. Accidents tend to happen when systems become intellectually unmanageable, even without component failures.

Decoupling means that functions and equipment are not connected if they don't have to be. Decoupling also decreases the complexity of the system. However, accidents can still happen through unplanned interactions or unforeseen consequences of a failure. A type of analysis connected to the latter is Zonal Analysis that is in principle the same as a common cause analysis (CCF). For example, cables running in a structure that breaks can be destroyed and cause loss of safety even if safety implementations are strictly separated.

Redundancy means that a function is carried out by two or more physically independent elements, such that the function is maintained until all the elements fail. This can increase the reliability (availability) of the function and/or reduce the number of functional failures.

Administrative control may concern handling of people and procedures and is connected to reducing the probability of accident consequence.

In the last case the provision of protective equipment is governed by creating safety functions to be implemented as requirements to modify an existing system or to be the requirements for a new system/subsystem/product. This involves monitoring of the existing system. Many of the railway applications are of these categories.

A.6 Risk ranking

There are two main approaches to risk assessment, using risk-ranking methods, namely qualitative and semi-quantitative. The required method should be selected carefully to provide the degree of risk assessment required for the operations being considered.

It should be noted that risk-ranking methods only give approximate estimates of the level of risk. The results from such assessments should never be judged as absolute. If the risk ranking process identifies

- accidents which have a significant potential for an outcome which leads to multiple fatalities,
- that the individual risk to one or more groups may be in the intolerable region, or

- accidents which have a significant collective risk contribution and there is a significant degree of uncertainty in relation to the frequency and consequences rankings applied. It may, in such cases, be necessary to undertake more detailed analysis using techniques such as fault tree and event tree analysis.

A.6.1 Qualitative ranking

Qualitative ranking schemes for frequency and consequence may be appropriate as a first pass at assessing risk or for assessing risk in simple cases. Generally, a qualitative ranking approach would not be adequate in a risk assessment.

In a qualitative ranking scheme the magnitude of the ranking has no real meaning, it merely provides a label for the category. The gaps between rankings can vary significantly. Attempting to define a risk measure using the product of the frequency and consequence rankings is not meaningful because while, for example, it can be said that an AA is lower risk than a BB, the level of difference cannot be quantified. This method therefore gives a feel of the relative levels of risk for each hazard considered.

It is not possible to draw any conclusions about the tolerability of the risk from such a qualitative approach. It is, however, possible to provide guidance on how to judge the results of such qualitative assessments by drawing boundaries on the risk ranking matrix, as shown in Table 6 of EN 50126-1. This may be an appropriate approach for some task based risk assessments. It would then be possible to define actions for each category of risk, e.g., intolerable or undesirable contributors should be addressed before the task is undertaken.

It should be noted that this approach does not encompass risk aversion to catastrophic, multiple fatality events. Such qualitative risk assessments would not be deemed to be suitable and sufficient for events, which could lead to fatalities without the express acceptance by the SRA.

A.6.2 Semi-quantitative ranking approach

For the cases where data is available or a good degree of judgment can be applied to estimates of the frequency and consequences of each accident, a greater level of accuracy and consistency in the risk estimates can be obtained by using a semi-quantitative risk ranking approach. It should be noted that while traditionally risk ranking methodologies have been based on a 5 x 5 matrix approach with the frequency and consequence rankings broadly separated by a factor of 10, this does not have to be the case. The size of the matrix and the factor difference in frequency and consequence rankings can be altered to give the best ranges to suit a particular stakeholder's operation. Consider the examples of frequency and consequence rankings in Tables A.1 and A.2 below.

Table A.1 – Example of frequency ranking scheme

Description (as in Table 2 of EN 50126-1)	Frequency range, for example	Mid-point estimated frequency	Approximate numerical value events/year	Ranking
Frequent	1 in 20 days to 1 in 3 months	1 in 2 months	6,25	6
Probable	1 in 3 months to 1 in 1 ¹ / ₄ years	1 in 9 months	1,25	5
Occasional	1 in 1 ¹ / ₄ years to 1 in 7 years	1 in 4 years	0,25	4
Remote	1 in 7 years to 1 in 35 years	1 in 20 years	0,05	3
Improbable	1 in 35 years to 1 in 175 years	1 in 100 yrs	0,01	2
Incredible	< 1 in 175 years	1 in 500 yrs	0,002	1

Table A.2 – Example of consequence ranking scheme

Example of consequences Description	Approximate numerical value equivalent fatalities/event	Ranking
Minor injury	0,005	1
More serious injury/multiple minor injuries	0,025	2
Major injury	0,125	3
Multiple major injuries/single fatality	0,625	4
Multiple fatalities (2 to 5 equivalent fatalities)	3,125	5
Multiple fatalities (6 to 25 equivalent fatalities)	15,625	6

In this example each category is a factor of five different from its adjacent categories. The categories can be separated by any factor e.g., a factor of two, five, ten or one hundred providing both the frequency and consequence estimates (as represented by the changes in their corresponding ranking numbers) are separated by the same factor.

To use the above frequency and consequence ranking scheme as a risk ranking matrix it has become common practice in the railway industry to represent the risk by multiplying the frequency and consequence ranking numbers to give an overall risk ranking. However, the multiplication of the frequency and consequence rankings can lead to inaccuracies and inconsistencies within the final risk rankings and therefore it is proposed that when using such risk ranking methods the frequency and consequence rankings are added and not multiplied to give an overall risk ranking.

NOTE It is very important to note however, that adding the frequency and consequence rankings only works if the changes in both the frequency and consequence estimates (as represented by the changes in their corresponding ranking numbers) are separated by the same factor.

This solution works for any factor difference (two, five, ten, one hundred, etc) providing both the frequency and consequence ranking estimates are separated by the same factor.

The risk ranking matrix therefore becomes as shown in Table A.3 below.

Table A.3 – Risk ranking matrix

Frequency	Consequence					
	1	2	3	4	5	6
6	7	8	9	10	11	12
5	6	7	8	9	10	11
4	5	6	7	8	9	10
3	4	5	6	7	8	9
2	3	4	5	6	7	8
1	2	3	4	5	6	7

A.6.2.1 Events with the potential for significantly different outcomes

When assigning frequency and consequence rankings to hazardous events the rankings are based normally on the average frequency of occurrence and the average consequences for the event. For some hazardous events, however, different outcomes can lead to significantly different consequences. For example, a train derailment would typically only lead to minor injuries, due perhaps to passengers falling over inside the train, whereas in extreme cases, derailments can lead to multiple fatalities. It is recommended that in such cases, to get a better understanding of the risk profile, particularly in relation to potential multi-fatality outcomes, two separate rankings should be considered for the hazardous event as follows:

- the first ranking should relate to the frequency and consequences of the typical (most frequent outcome), and

- b) the second risk ranking should relate to the frequency and consequences of the realistic worst case outcome, if appropriate.

This is shown diagrammatically in Figure A.1 below based on the example frequency and consequence ranking scheme from Tables A.1 and A.2.

It should be noted that the risk ranking in (b) above should relate to a realistic worst case outcome rather than necessarily the absolute worst case outcome.

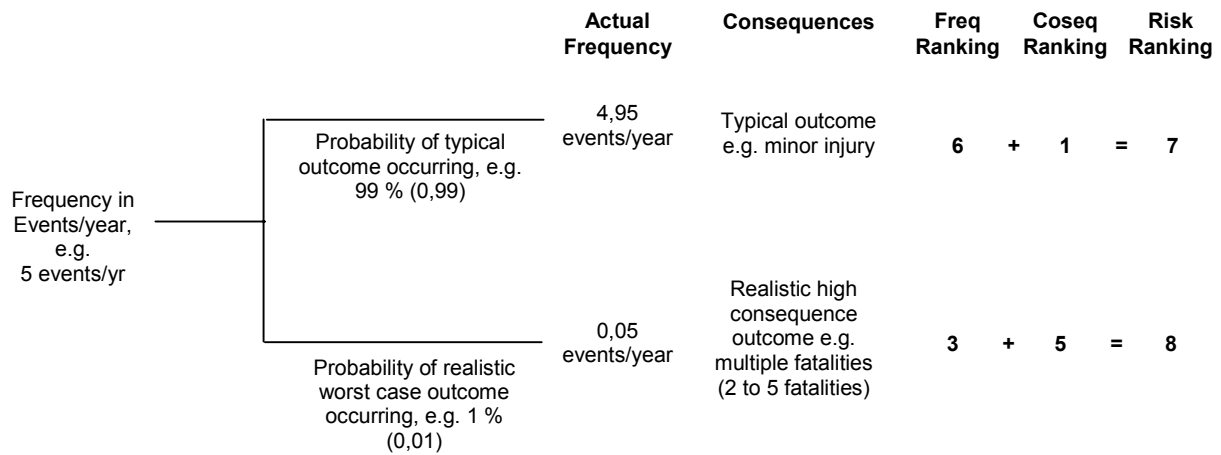


Figure A.1 – Risk ranking for events with potential for significantly different outcomes

Annex B (informative)

Railway system level HAZARDS - Check lists

B.1 General

Example checklists are supplied below which may be used if there are no existing, well-established checklists. They may be applied to the whole system or to a component of it. Each item should be interpreted as widely as circumstances permit in the endeavour to unearth possible hazards. No checklist can be exhaustive and the analyst should bring his or her full experience to bear in searching for hazards.

Functional Checklist should be applied to a functional specification of the item being considered in an attempt to unearth hazards arising from unspecified functionality or specified functionality in unforeseen circumstances:

- | | | |
|----------------------------------|--|----------------------------|
| a) Alarms and warnings, | b) Indication of failure, | c) Interlocks, |
| d) Maintenance and support, | e) Point setting, | f) Signal aspects, |
| g) Velocity control, | h) Software malfunction, | i) Software crash, |
| j) Vehicle structural integrity, | k) Deceleration control, | l) Train doors operation, |
| m) Gauge infringement, | n) Vehicle separation
(uncoupling), | o) Train separation, |
| p) Level crossing, | q) Train/track interaction, | r) Emergency controls, |
| s) Train/platform, | t) Obstacle on track, | u) Recovery from failure, |
| v) Slips and trips, | w) On train services and facilities | x) Environment influences. |

Mechanical Checklist should be applied to mechanical systems/equipment to unearth hazards involving physical interactions:

- | | | |
|---------------------------------------|-------------------------|-----------------------------|
| a) Corrosion, | b) Cryogenic fluids, | c) Derailment, |
| d) Exhaust gases, | e) Fire, | f) Foreign bodies and dust, |
| g) Insect, rodent or mould
damage, | h) Lasers, | i) Overheating, |
| j) Pressure systems, | k) Shock and vibration, | l) Vandalism, |
| m) Ventilation, | n) Humidity, | o) Flooding, |

Construction Checklist should be applied to civil engineering works, drawings and plans to unearth construction hazards:

- | | | |
|---|------------------------------|---|
| a) Access hazards at site, | b) Site preparation hazards, | c) Construction hazards, |
| d) Environmental effects | e) Vandalism, | f) Interference with normal railway operating procedures, |
| g) Training and control of contractors, | | |

Electrical Checklist should be applied to electrical systems/equipment to unearth hazards involving electrical interactions:

- | | | |
|---|-----------------------------------|---------------------------------------|
| a) Electromagnetic interference and compatibility, | b) Fire and explosion initiation, | c) Insulation failure, |
| d) Lightning strikes, | e) Loss of power, | f) Traction current, |
| g) Protection against earth faults, | h) Indirect and direct contact, | i) Emergency switching and isolation, |
| j) Overcurrent protection and effects of disconnection, | k) Current rating, | |

Operation and Support Checklist should be applied to operating and maintenance procedures and instructions to unearth hazards occurring during or triggered by operating and maintenance activities:

- | | | |
|-----------------------------------|----------------------------|-----------------------------------|
| a) Accessibility for maintenance, | b) Documentation, | c) Failure to activate on demand, |
| d) Human factors, | e) Inadvertent activation, | f) Lighting, |
| g) Manuals, | h) Spares, | i) Training, |
| j) Start-up, | k) Closedown, | l) Re-setting. |

Occupational Health Checklists should be applied to a general description to unearth hazards to passengers and personnel installing, operating, maintaining or disposing of an item:

- | | | |
|------------------------------|---------------------------|-------------------------|
| a) Asbestos, | b) Asphyxiates, | c) CFCs, |
| d) Corrosive materials, | e) Cryogenic fluids, | f) Electrocution, |
| g) Exhaust gases, | h) Fire, | i) High temperatures, |
| j) Injury from moving parts, | k) Lasers, | l) Noise and vibration, |
| m) Pressure systems, | n) Radioactive materials, | o) Toxicity, |
| p) Electrical overheating. | | |

Examples in Clauses B.2 and B.3 below are based on two separate hazard identification studies based on hazard groupings from the perspective of potential victims and from functional requirements respectively.

B.2 Example of hazard grouping according to affected persons

A human focused hazard identification from the perspective of various groups at risk from the operational railway system was conducted seven years ago at the level of the whole generic UK railway network.

- The first group of the industry level hazards identified relate to the people who live near the railway perimeter or come into contact with railways in the course of daily life referred to as railway Neighbours (B.2.1).
- The second group of the industry level hazards relate to the Passengers (B.2.2).
- The third group of the industry level hazards relate to the Workers in the industry (employees, contractors and suppliers) (B.2.3).

Note that hazards are generic and independent of the specific causes and sub-systems. The lists could be used as a check list of railway system level hazards based on a grouping according to potential victims.

B.2.1 “C-hazards” – Neighbours group

The system level hazards to railway neighbours are aggregated into ten groups referred to as Neighbour Group “c-hazards”. The key aim in this aggregation is rationalisation of the effort involved in further analysis and modelling. The secondary benefit arising from such clustering is the likely identification of additional hazards to railway neighbours, which belong to a specific “c-hazard” class.

Table B.1 – Railway neighbour “c-hazards”

“c-hazard” Reference	Description	Constituents
HN500	Abnormal or criminal behaviour	HN0416 Suicide attempt HN0417 Trespass HN0418 Abnormal behaviour at special events
HN501	Crossing Running Railway at Level Crossing	HN480 crossing running railway at a manual level crossing HN481 crossing running railway at an automatic level crossing HN482 crossing running railway at user worked level crossing HN484 crossing running railway at a level crossing
HN502	Contaminated Water and/or Land	HN0502 Contaminated Water and/or Land
HN503	Electro-Magnetic Interference (EMI) Caused to by Railway Operations	HN0503 EMI impact on neighbourhood
HN504	Impact from Railway Construction/Maintenance Works	HN0504 Impact from railway const/maintenance works
HN506	Loss of Balance	HN0403 Loss of balance on the ground HN0404 Loss of balance on stairs
HN509	Inappropriate Separation between Running Railway and Neighbourhood	HN509 Inappropriate separation between rail & neighbours
HN510	Inappropriate Separation between Un-insulated Live Conductors and the Public	HN0405 Occurrence of DC power arc HN0406 Existence of touch potential HN0407 Structure exposed to leakage current [DC] HN0408 Inappropriate separation from DC conductor rail HN0409 Structure in contact with live conductor rail HN0410 Inappropriate separation from OHL live conductor HN0411 Structure in contact with live OHL HN0412 Inappropriate separation from OHL induced voltage HN0413 Inappropriate separation from ground potential HN0414 Occurrence of AC power arc HN0415 Structure exposed to leakage current [AC]
	Flying Debris from Moving Train and Objects Falling from Trains	HN511 Flying debris / objects falling from trains
HN512	Unsecured Objects at Height	HN0512 Unsecured objects falling from height

B.2.2 “C-hazards” - Passengers group

The system level hazards to railway passengers are aggregated into twelve groups referred to as Passenger Group “c-hazards”. The key aim in this aggregation is rationalisation of the effort involved in further analysis and modelling. The secondary benefit arising from such clustering is the likely identification of additional hazards to passengers, which belong to a specific “c-hazard” class. A number of “c-hazards” were also identified which affected more than one specific group of people. These are numbered in the 600 range.

Table B.2 – List railway passenger “c-hazards”

“c-hazard” Reference	Description	Constituents	
HP500	Abnormal or Criminal Behaviour	HP0425 HP0426 HP0427	Irresponsible behaviour Destructive behaviour (all forms) Crossing line at station
HP502	Crowding	HP502	Crowding
HP503	Loss of Passenger Compartment Integrity during Movement	HP0503	
HP504	Passengers in Path of Closing Train Doors	HP0504	
HP506	Loss of Balance	HP0413 HP0414 HP0415 HP0416	Loss of balance on the ground Loss of balance on stairs & escalators Loss of balance getting on and off trains Loss of balance whilst in a train
HP509	Inappropriate Separation between Running Railways and Passengers	HP509	
HP510	Inappropriate Separation between Un-insulated Live Conductors and Passengers	HP0417 HP0418 HP0419 HP0420 HP0421 HP0422 HP0423 HP0424	Occurrence of DC power arc Existence of touch potential Inappropriate separation from DC conductor rail Structure in contact with live conductor rail Inappropriate separation from OHL Structure in contact with OHL Occurrence of AC power arc Inappropriate separation from OHL induced voltage
HP512	Passenger Protruding beyond Train Gauge during Movement	HP0512	
HP513	Unsecured Objects at Height	HP0513	
HP515	Inappropriate Separation between Passengers and Moving Vehicle (other than rail vehicle)	HP0515	
HP516	Handling Heavy Loads	HP0516	
HP517	Incompatibility of Train and Structure Gauge	HP0517	
HP600	Abnormal Deceleration	HP0518 & HW0516	
HP601	Uncontrolled Approach to Buffer	HP0501 & HW0501	
HP602	Loss of Train Guidance (Passenger Trains)	HP0412, HW0409 & HN0402	
HP603	Loss of Train Guidance (Freight Trains)	HP0411, HW0408 & HN0401	
HP604	Objects/Animals on the line	HP0511, HW0510 & HN0514	
HP605	Inappropriate Separation between Trains	HP0505, HW0504, HN0505	
HP606	Onset of Fire/Explosion	HN400 HP400 HP401 HP402 HP403 HW400 HW401	Fire at lineside Fire inside passenger carriage Fire outside passenger electric train Fire outside diesel passenger train Fire at station Fire on electric freight train Fire on diesel freight train
HP607	Unsound/Unsecured Structures	HP0404 HP0405 HP0406 HP0407 HP0408 HP0409 HP0410	Unsound / Unsecured Tree Unsound / Unsecured Tunnel Unsound / Unsecured Underbridge /Culvert Unsound / Unsecured Overbridge Unsound / Unsecured Station Unsound / Unsecured Signalling Structure Unsound / Unsecured Electrification Structure

B.2.3 “C-hazards” - Workers group

The system level hazards to railway workers are aggregated into seventeen groups referred to as Workers Group “c-hazards”. The key aim in this aggregation is rationalisation of the effort involved in further analysis and modelling. The secondary benefit arising from such clustering is the likely identification of additional hazards to workers, which belong to a specific “c-hazard” class.

Table B.3 – List of railway worker “c-hazards”

“c-hazard” Reference	Description	Constituents	
HW500	Abnormal or Criminal Behaviour	HW0426 HW0427 HW042	Irresponsible behaviour Destructive behaviour Crossing line at station
HW502	Loss of Passenger Compartment Integrity during Movement	HW0502	
HW503	Worker in Path of Closing Train Doors	HW0503	
HW505	Loss of Balance	HW0410 HW0411 HW0412 HW0413 HW0414	Loss of balance on the ground Loss of balance on stairs and escalators Loss of balance getting on and off trains Loss of balance whilst in a train Loss of balance when working at height
HW508	Inappropriate Separation between Running Railways and Workers	HW402 HW403	Red zone working Green zone working
HW509	Inappropriate Separation between Un-insulated Live Conductors and Workers	HW0415 HW0416 HW0417 HW0418 HW0419 HW0420 HW0421 HW0422 HW0423 HW0424 HW0425	Occurrence of DC power arc Existence of touch potential Structure exposed to leakage current [DC] Inappropriate separation from conductor rail Structure in contact with live conductor rail Inappropriate separation from OHL Structure in contact with live OHL Inappropriate separation from OHL induced voltage Inappropriate separation from ground potential Occurrence of AC power arc Structure exposed to current leakage [AC]
HW511	Worker Protruding beyond Train Gauge during Movement	HW0511	
HW512	Unsecured objects at height	HW512	
HW513	Inappropriate Separation between Workers and Moving Vehicle (other than rail vehicle)	HW0513	
HW514	Handling heavy loads	HW0514	
HW517	Unsound/Unsecured Machinery/Materials/Structures	HW0517	
HW518	Work in Confined Spaces	HW0518	
HW519	Contaminated Water and/or Land	HW0519	
HW520	Inappropriate Working Methods/Environment	HW0520	
HW521	Workers in Proximity to Harmful Substances	HW0521	
HW522	Road Vehicle Accidents	HW0522	
HW523	Objects Thrown or Falling from Train	HW0523	

B.3 Example of functional based hazard grouping

The system level hazards may be represented from a functional and discipline perspective as described in Clause C.1. An illustrative generic structure based on this philosophy is presented in Table B.4 below. This can be used as a check list for consideration of hazards on a functional basis.

Table B.4 – System level hazard list based on functional approach

	Infrastructure	Energy	Rolling Stock	Control & command
HAZARDS IDENTIFIED FROM FUNCTIONS PERSPECTIVE				
Access and egress hazards				
Hazards arising from reduced or lost operational functions/conditions				
Hazardous loss of door function	X		X	
.....				
Hazardous loss of escalator function	X			
.....				
Hazards arising from reduced or lost protection functions				
Loss of crush protection	X		X	
.....				
Safe stay impaired				
Hazards arising from reduced or lost operational functions/conditions				
Hazards while walking, standing or sitting	X		X	
Slippery ground	X		X	
Broken chair	X		X	
.....				
Safe functions of heating/air conditioning not given			X	
Heating fails at very low outside temperature			X	
Air conditioning fails at very high outside temperatures			X	
.....				
Safe provision of food not given	X		X	
Moulded water supply	X		X	
.....				
Safe luggage fixation not given			X	
.....				
Hazards arising from use of toilets	X	X	X	X
Door obstructed (person trapped)	X	X	X	X
.....				
Acceleration/deceleration limit values exceeded			X	
.....				
Hazards arising from reduced or lost protection functions				
Protective ground faults	X	X	X	X
Insufficient protection against allowable touch voltage	X	X	X	X
Fire extinguisher defective or missing	X	X	X	X
.....				
Loss of fire alarm function	X	X	X	X
.....				
Impaired train movement				
Hazards arising from reduced or lost operational functions/conditions				
Train on wrong route	X		X	X
Wrong route given				X
.....				
Non-compliance with structure clearance				
Straight line not cleared				
Track not clear				
Unallowed track access (incl counter train prevention)	X			X
Flank protection not given (incl cross level section)	X			X
Profile clearance not given				
Structure profile clearance not given	X	X		X
Vehicle profile clearance not given			X	

Table B.4 – System level hazard list based on functional approach (continued)

	Infrastructure	Energy	Rolling Stock	Control & command
Impaired train motion control			X	
Unintentional train movement			X	
.....				
Train braking ability impaired or lost			X	
.....				
Track gauging failure / derailment hazards	X		X	X
.....				
Loss of train integrity			X	X
.....				
Hazards arising from reduced or lost protection functions				
Interlocking malfunction				X
.....				
ATP malfunction			X	X
.....				
Loss of deadman switch function			X	
.....				
Train presence indication	X		X	X
Train detection when track occupied	X		X	X
Malfunction of vehicle lights			X	
Malfunction of warning horn			X	
Level crossing malfunction	X			X
Loss of high voltage power supply insulation		X	X	
.....				
Insufficient control of emergency situations				
Hazards arising from reduced or lost operational functions/conditions (during emergency				
Loss of traction (e.g. in case of fire in tunnels)			X	
Loss of braking function			X	
Loss of door opening function			X	
.....				
Hazards arising from reduced or lost protection functions				
Insufficient crash protection			X	
.....				
HAZARDS IDENTIFIED FROM THE PERSPECTIVE OF INHERENT PROPERTIES				
Overheating / smoke / fire	X	X	X	X
Inadequate EMI values	X	X	X	X
Shock wave (explosion, air pressure)	X	X	X	X
Inadmissible radioactivity				
Biological or chemical contamination	X	X	X	X
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="font-size: 3em; line-height: 1;">}</div> </div> <div> <p>These (and maybe more) have to be applied to components in the sense of a check list</p> </div> </div>				

Annex C (informative)

Approaches for classification of risk categories

The approaches for classification are summarised in 6.3.2. This annex provides more explanation of the different system breakdown approaches for allocating safety targets together with their merits and de-merits.

C.1 Functional breakdown approach (a)

The functional approach looks at all the phases, functions and processes taking place in the operation of a railway system and identifies the hazards that may occur in each of these before evaluating the potential resulting risks associated with each function, process and subsequently the phase of operation (bottom-up), or alternatively apportioning the global risk to each phase, functions and process (top-down).

An approach based on a functional decomposition has the main advantage that it offers, in theory, better potential for a generic description of a railway system that is neutral to specific system incarnation or specific operational issues. Such a top-down apportionment may thus not be so controversial when stopped at a level that remains sufficiently generic, with functions, processes and phases that are clearly distinguishable, easily comparable and also similar across different railway systems. Separating risks according to this functional scheme would also provide the added benefit of associating distinct risk exposure factors for each phase, process or function, which is critical in the determination of individual risks.

However, a difficulty with this approach is to find a generic functional description of a railway system that also goes into a sufficient level of functional breakdown to enable apportionment on a meaningfully accepted basis. The process could be continued further for lower level functions but it means that it would have to stop at a level where apportionment of risks between lower level functions becomes ambiguous and hard to decide on a commonly accepted basis.

It follows that below a fairly high level of abstraction, descriptions of functions and processes in a specific railway are likely to differ depending on the particular systems and their specific operational rules. Therefore, freezing the portion of risks to be attributed to each function/process, on a generic basis, may prove inappropriate. Also certain risks may arise at functional interfaces (e.g. speed control/train separation) that make unambiguous apportionment even more difficult (although presumably easier than by system breakdown).

If however it was felt necessary to apportion to a deeper level, an approach similar to (c), (see Clause C.3) based on a hazards breakdown within each general function or each subsystem would then be recommendable.

C.2 Installation (constituent) based breakdown approach (b)

This approach consists of decomposing the whole railway system into its major constituents (organisational and/or physical) parts and assigning a risk portion of the overall risk to each part, depending on the estimated or required contribution of each part to global risk.

For the System breakdown approach, one way to derive risk levels for constituent parts is to estimate through the use of statistics the contribution of each part to the total risk. Going through accident statistics, the average contribution of each part to each accident type is assessed, and summed up over all accident types to obtain an average percentage contribution to the total risk. The total risk is thus apportioned to the constituent parts according to these statistically derived percentages. In this sense it is a top-down apportionment.

Such an approach has, in principle, the obvious advantage that it would help provide a set of common safety requirements in the form of targets for various constituents of the railway system (although for this purpose, a target expressing the acceptable risk of a certain constituent would have eventually to be translated through some safety analysis into an acceptable dangerous failure rate). This would in turn make cross-acceptance of products/systems easier and also facilitate inter-operability.

There are however certain difficulties with this approach as far as common safety requirements are concerned.

- First, the European railway system is so heterogeneous that it might be difficult to agree on a systematic physical decomposition of the system which is valid everywhere, railway systems are better comparable through a functional decomposition.
- Second, even if the latter was possible (like in ERTMS for instance, which is one common system, albeit with 3 different levels), the hazards arising from interfaces between constituents and the complexity of the railway system makes it often difficult to apportion risks unambiguously between its constituents (transverse safety functions).
- The distribution of risks according to constituent parts should not be “frozen” and would thus require frequent updating in order to keep track with changes in the technology.
- Finally, this approach relies heavily on the use of statistics. Until there is harmonisation in the way accidents are recorded, databases organised and maintained, any statistical derivation of average risk percentage numbers at European level is likely to raise many suspicions, particularly since such accidents are rare events that make any meaningful statistical evaluation difficult.

C.3 Hazard based breakdown approach (c)

By this approach, the overall risk is apportioned between all possible hazards. By hazards it is meant here system level generic hazards (“c-hazards”) that can lead to accidents. As in the functional approach, these hazards ought to be defined at a sufficiently high level that they remain generic and independent of specific solutions or implementation issues of railway operation, yet also be detailed enough to provide a good focus point for safety control (e.g. incompatibility between train and structure gauge can be seen as a generic hazard of the highest level, but there isn’t one dedicated function, even at high level, that protects against it). Therefore the first step in this approach would be to identify hazards at the appropriate level (as low as possible, as high as necessary) covering the entire scope of railway operation and all groups of exposed persons, as required by the Safety Directive (passengers, employees, level crossing users, third parties, etc.). As an indication, the detail level of these hazards would be more or less corresponding to the incidents and near misses mentioned in Annex I of the safety Directive (e.g. broken rails, track buckles, wrong-side signalling failures, signals passed at dangers, etc.).

The derivation of specific safety target for each hazard can then be achieved by 2 different methods:

- top-down apportionment of global residual risk
- bottom-up determination of acceptable risk level per hazard

The first method is similar to that of the previous approaches, namely statistics is used to find the average portion of risks attributable to each hazard, and from there a Safety Target (ST) is set. This is straightforward but has the inconvenience of depending heavily on statistics that may, for the time being, lack sufficient reliable data, not to mention the problem of rare events, making evaluation of current risk levels for each hazard difficult.

The second method would determine what should be the maximum acceptable risk level per hazard based on the severity of consequence of a resulting accident and on its maximum tolerable frequency of occurrence. This could be done, for instance, by using a risk acceptance matrix similar to that of EN 50126-1 calibrated however, by help of statistics, to obtain numerical values for the frequency classes. Determining the typical consequence of a hazard might prove difficult (should it be the average, the worst case, or likely worst case?) but since severity categories would be used, high precision may not be so critical. Important in this scheme is a classification of hazards depending on their potential for causing harm in order to determine accordingly the tolerable accident frequency rate for the hazard.

Whichever method is used for ST determination, a hazard breakdown approach has the advantage of providing a focus on causes of accidents based on independent generic hazards. Contrary to the previous approaches mentioned above, well-defined generic hazards would not have interfaces or overlap between them, this would make the risk apportionment unambiguous. Considering generic hazards should also make the approach easily applicable for every railway. Therefore, the system hazard level seems to be a good level for setting specific ST, from which subsequent safety requirements could be derived, depending on the type of application. As with other approaches, this would nevertheless require a considerable effort, in particular for determining what should be the tolerable hazard rates (THR). In this approach the difference between a THR and a hazard ST (i.e. the difference between the occurrence of a hazard and the occurrence

of a resulting accident) lies in all sort of risk reduction and exposure factors, which are generally hard to investigate with any accuracy.

On the downside, the main inconvenience with this approach is first to find an agreement on a list of complete, independent and generic system level hazards, acceptable to all. This is believed to be possible and is similar to the problem of structuring an accident and incident database, but this is not so easy to achieve, as there are many ways of structuring such a list (see 5.5.2), on hazard grouping structures). Second, such a list could produce many different hazards, which would mean many specific STs. This could be awkward to handle and too constraining for railway operators.

C.4 Hazard causes based breakdown approach (d)

This approach does not classify risks either according to the part of the system they emanate from, or to the function or process they may appear through, but according to the nature of the cause creating the risk. For instance one can differentiate risks depending on whether they arise because of technical faults or human errors, and assign different targets to them according to statistics. An example for setting specific STs related to causes of hazardous situations, is based on the following classification:

- technical faults;
- human errors;
- organisational failures (e.g. wrong rules or procedures);
- external causes.

Occurring within the responsibility of each of the relevant duty holders (railway authority or railway support industry)

Such an approach follows the same principles for setting CST as in (a) (see Clause C.1), meaning it would also require a top-down apportionment based on statistical estimates of the risk carried by each category. The decomposition of risks into the 4 general groups of hazard causes may not be controversial in itself since it is meant to reflect broad categories of failing of a Safety Management System (SMS) and could in this sense help provide a useful safety focus for the duty holder while also serving as SMS criteria for delivering the safety certificate. Also, having only 4 specific targets to handle would be attractive. In spite of these advantages, this approach would however pose more or less the same inconveniences as in (a) (see Clause C.1).

- First, a look at the diversity of railway systems, their network characteristics and environment in Europe suggests that there could be great variations between them in the current portions of risks attributable to each hazard source category (e.g. various levels of automation). It does not make sense then to set common targets at this level. Although monitoring these 4 categories can provide useful indicators for a specific railway, it might be wiser to leave it up to the relevant railway authority or railway support industry organisations to decide in what areas they would want to concentrate their safety effort, taking their own specific characteristics into account. These hazard cause categories tend to reflect implementation issues of railway properties.
- Second, an accident will often be a combination of different types of causes, e.g., human error and/or technical faults. Also an organisational failure can often be found at the root of an accident that involved human errors and/or technical faults. This could make any apportionment between the 4 categories (with the exception, maybe, of external causes) difficult due to overlaps.
- Frequent update would also be required to avoid cementing the risk portions attributable to the different hazard cause categories.
- Finally the same problem with the statistics, as mentioned above for (a) (see Clause C.1), applies here also.

C.5 Breakdown by types of accidents (e)

This is the simplest approach of all. First a list of typical railway accidents, such as the one indicated in Annex I of the Safety Directive, has to be agreed. Then the global residual risk (per group categories) is apportioned to the different accident types, using statistics.

The main advantages of this approach are that

- it is relatively simple to implement (a classification by accident types is less likely to create much controversy),
- it would be quite easy to monitor with the corresponding indicators (it is in principle easy to determine the type of an accident when it has occurred) and
- there would be relatively few targets (one per accident type).

The downside of this approach is however that it concentrates more on the consequences of (lack of) safety than on the causes, which defeats somehow the purpose of specific STs, even though it provides more focus than the global STs.

Annex D (informative)

An illustrative railway system risk model developed for railways in UK

D.1 Building a risk model

To build a risk model, the following example of essential steps, consistent with the risk assessment process (5.3), should be taken:

- 1.1** Represent the system being analysed, its key elements, boundaries, internal and external interfaces, application environment and interactions diagrammatically.
- 1.2** Use the diagrammatic representation for a preliminary hazard identification ensuring people, processes and normal, degraded and emergency modes of operation are taken into account.
- 1.3** If necessary, detail and diagrammatically represent the key functions of the system and its interactions with the external world.
- 1.4** Use the functional representation to identify more detailed hazards.
- 1.5** For each hazard identified maintain a numbered unique record (hazard log) also capturing causes, consequences, likely estimated risk with the aid of a ranking table, people affected and likely actions.
- 1.6** Consolidate synergistic hazards i.e. those with a common cause or tangible relationship into clusters and classes with a label called “c-hazards”.
- 1.7** Develop a diagrammatic representation of the causation chain for each “c-hazard”, ensuring all the detailed hazards allocated to that group have been taken into account. The causation chain (Causal Model) should identify the logical combination of causes which may help realise the “c-hazard” including common causes, human and sub-system failures.
- 1.8** Develop a diagrammatic representation of the likely escalation of each “c-hazard” in an operational context and the defences that exist in detection, procedural and even chance mitigation. This (Consequence Model) would represent the likely end events i.e. incidents and accidents which may arise from a given “c-hazard”.
- 1.9** Consolidate the Causal and Consequence models for each “c-hazard” into one model module and represent the whole system by the number of “c-hazard” Modules.
- 1.10** If numerical analysis and forecasting of risks is required, ensure the causal and consequence aspects of each “c-hazard” Module are populated with numerical data. For the causal models, the required data are often related to failure rates and probabilities associated with each factor based on historical information or expert judgement. For Consequence models of each “c-hazard”, the required data often relate to the strength of defensive safety barriers in terms of conditional probabilities of success for each safety barrier in the escalation chain.
- 1.11** For each accident forecast in step 8, estimate or derive the severity of harm caused and using the computed probability or frequency for each accident, compute a risk figure. It is instructive to estimate financial and environmental damage alongside harm to humans and environment during this stage to support a broader decision making.
- 1.12** Sum up annualised risk estimates for each accident in a “c-hazard” Module.
- 1.13** Sum up the risk estimates for all “c-hazards” in the system. This presents a total risk profile for the product, process or system.
- 1.14** Verify and validate the model data and structures through expert and peer review as well as comparison of its forecasts against credible data sources and relevant historic performance.

- 1.15** Where possible, obtain an apportioned target for the system under analysis and contrast the total risk profile with the target to establish a measure of tolerability and need for further risk reduction.

The above would yield a qualitative or quantitative and often diagrammatic representation of the hazards, causes and likely consequences that provides a systematic basis for objective safety related decision making bearing in mind the limitations in complete and exact modelling of complex systems.

D.2 Illustrative example of a risk model for UK railways

The following subclauses of this annex describe only some of the key elements of the methodology applied to building the model representing the whole of UK railways and shows the results derived from the output of the model.

A Risk Profiling study aimed at developing a quantitative risk forecasting model for the whole UK railways infrastructure and operations, at the railway system level, was conducted during 1997. The so called risk profiling study was based on a number of industry level hazard identification exercises which had been carefully designed, planned and carried out with wide participation from across the rail industry (i.e., RSI and RA). These human focused studies scrutinised and identified the precursors to accidents from the perspective of the specific groups (Passenger, Worker and Neighbours) at risk from the operational railways. These were subsequently rationalised into a super set called c-hazards and subjected to the Causal, Consequence and Loss analysis with a view to develop a predictive risk based safety model giving a total forecast for the whole of the UK railway infrastructure and operations. When safety risks are involved, a human focused perspective may prove better aligned with railway metrics and targets than failure based norms often quoted as criteria for system safety.

D.2.1 Modelling technology

Most numerical models present reasonably rigid and rather inflexible structures and do not easily lend themselves to manipulation and what-if type analyses. The process of building the profiling component models is essentially modular. Each building block (C-hazard) comprises numerical logical structures which denote the causation chain (Causal Analysis) and the escalation scenarios (Consequence Analysis) culminating in the prediction of a range of accidents and incidents and their pertinent frequencies. The accidents and incident frequencies and risks from each building block are summed up with the aid of a tool to generate risk forecasts. To enhance the flexibility of the model structures and avoid the necessity for creating many variants of models for interim phases of a product or project, a new approach to modelling has been devised referred to as Parametric Modelling. This is mainly aimed at rationalising the enormous effort required in producing a bespoke model for varying designs and circumstances.

D.2.1.1 Parametric modelling

A forecasting model essentially comprises logical structures built around a set of hazards or c-hazards and the associated generic or case specific data. Once the logical structures are captured, reviewed and consolidated, it is desirable to ensure these are encapsulated and protected against alterations within a strict configuration control environment. The data however, are likely to be more changeable than the logical structure of a model and a new approach for data substitution into a model is called for. To this end, the basic failure probability/rates and barrier strength within a predictive numerical risk model can be declared as variables and mathematical expressions capable of being evaluated according to a supplied set of network data. The aim is to derive different forecasts without significant investment and diversity in model building effort and structures. A secondary benefit accrues due to a single reference environment for enhancements and continual improvement to the expensive modelling effort. The tertiary benefit is to decouple/separate data from internal model structures as far as possible thus enhancing the integrity, ownership and scrutiny of assumptions and data employed for forecasting. The model data are captured within a PArametric Dataset (PAD) that is illustrated in Table below.

Table D.1 – Sample parametric data for a risk forecasting model

Item	Parameter Reference	Parameter Description	Units
1	AC	Length of AC Line	Km
2	ALX	Number of automatic level crossings	-
3	ALXH	No. auto level crossings with auto half barrier	-
4	BULL	Percentage of bullhead rails	%
5	BULW	Percentage of bullhead rails, Current	%
6	CCTV	Number of manual level crossings with CCTV	-
7	CDL	Percentage of trains with CDL doors	%
8	CDLC	Current Percentage of trains with CDL doors	%
9	CDLJ	Number of CDL door journeys	-

D.2.1.2 Classification and apportionment

Apart from generating the much desired holistic forecasts for safety performance, it is highly beneficial to be able to identify and potentially quantify key contributions to a given risk forecast generated by a model. For example, apart from forecasting passenger fatalities, it is also desirable to know the main causes (hazards or failures) and their relative contribution to passenger risks. To achieve this goal, a series of coding were developed in order to be able to classify the elements and building blocks of the models during their incorporation into the model. These encodings also referred to as Classifications, facilitate systematic tracing and apportioning numerical risk values to basic causalities and lower level structures within the integrated models.

D.2.1.3 Statistical simulation of the model

The two principal areas of uncertainty in risk profiling are in the causal /consequence domain (reflected in the predicted consequence frequency) and in the loss estimation domain (reflected in the predicted losses associated with each consequence or accident). The causal and consequence domain can be analysed separately in terms of uncertainty. There is uncertainty in the model structure as well as in the data used to populate the models. In the loss estimation domain there is uncertainty in both the models used to calculate extents of damage and in the data employed which are often of historical nature.

By running the models deterministically, point values for frequencies and losses are obtained. If, however it proves desirable to determine the uncertainty of these values, it is necessary to apply probability distributions to the input parameters and run the numerical risk model stochastically using either Monte-Carlo or Latin-Hypercube sampling.

D.2.2 Usage and constraints

The risk profiling process presented in this guidance is illustrative and is intended to demonstrate one systematic approach to assessment and integration of risks within a project or product context. As for all models, the forecasts generated through risk profiling should be treated as an input in objective decision making within the social, legal and organisational constraints.

D.2.3 Model forecasts

The c-hazards customised from the national level safety analysis were modelled from Cause (how they come about) and Consequence (what effect they will have) point of view, leading to 123 building blocks for the whole UK railway network. Note that the model has been validated by comparison with data derived from analysis of accidents and near misses information collected by the UK's RA. The UK's RA maintains the computer based modelling tool.

D.2.3.1 Absolute risk forecasts

The risk modelling technology developed in realisation of the principled approach to forecasting essentially generates absolute forecasts in terms of harm to specific groups at risk from the totality of operational railway. In view of the perceptions about the tolerability and specific groups at risk, the railway system level risk forecasting models are designed to provide a very detailed safety forecast of Minor Injuries, Major Injuries and Fatalities for each of the groups (i.e., Passenger; Neighbour (Public); and Worker (Workforce)).

In addition, the holistic approach to loss estimation generates forecasts for the Commercial and Environmental risk aspects pertinent to each c-hazard. These present additional perspectives on the key hazards to enrich decision making, taking into account a more comprehensive portfolio of pertinent factors.

The absolute annualised safety forecasts derived from the model are depicted graphically in Figure D.1. They depict risk by showing the frequency of occurrence of accidents resulting in fatalities, major injuries and minor injuries to each group. These types of forecasts are essential outputs from any integrated numerical risk model.

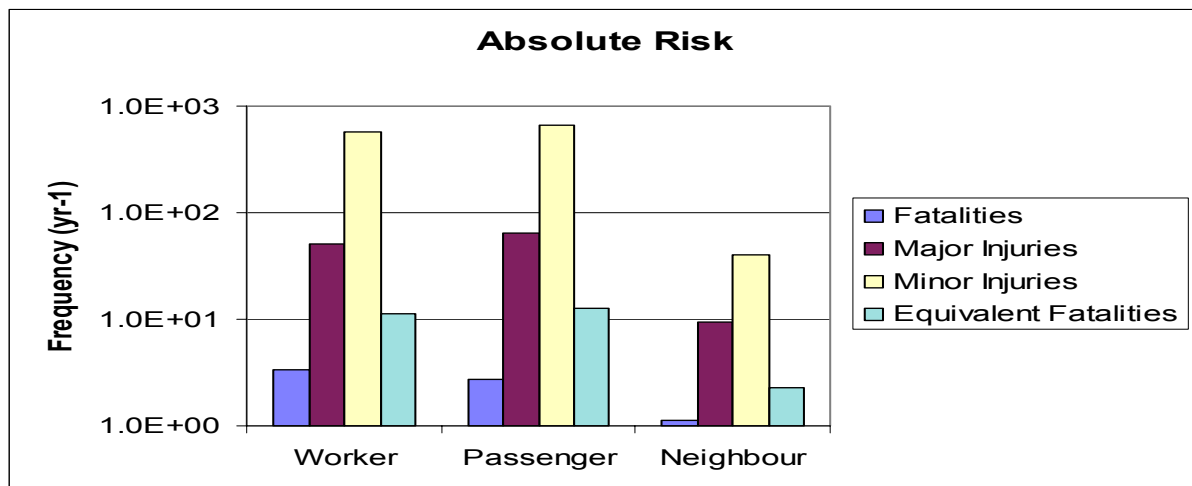


Figure D.1 – Illustrative annual safety forecasts generated by an integrated risk model

Figure D.1 also shows the “Equivalent Fatality” forecasts (a convention for integrating forecast injuries and fatalities in one unit). It indicates that in absolute terms and according to the model, the Passenger group is most at risk followed by Worker and the Public groups.

D.2.3.2 Normalised risk forecasts

The safety objectives detailed in the UK’s annual Railway Group Safety Plan, refer to Passenger, Public and Workforce safety in terms of individual risks of Accidental Fatality and Major Injuries. The absolute forecasts generated by a risk forecasting model are scaled according to an appropriate set of normalisation metrics in order to arrive at an estimate for the individual safety risks, arising from the railway’s infrastructure and operations. There are different sets of normalisation metrics for each group in view of the differences in the mechanism of usage and exposure within the operational railway network, as depicted in Figure D.2. Note that the baseline individual risks are computed for fatalities, injuries and equivalent fatalities, which is a combined measure for overall safety performance. The current convention employed in the UK for merging predicted injuries and fatalities into a single currency is based on treating 1 Fatality as = 10 Major Injuries = 200 Minor Injuries.

The illustrative individual risk figures, derived from the risk forecasting model, are depicted graphically in Figure D.2. They depict risk by showing the annualised probability of occurrence of accidents resulting in fatalities, major injuries and minor injuries to an individual in each group. The passenger individual risk has been derived from the risk per journey on the basis of 250 return journeys per year for a frequent passenger.

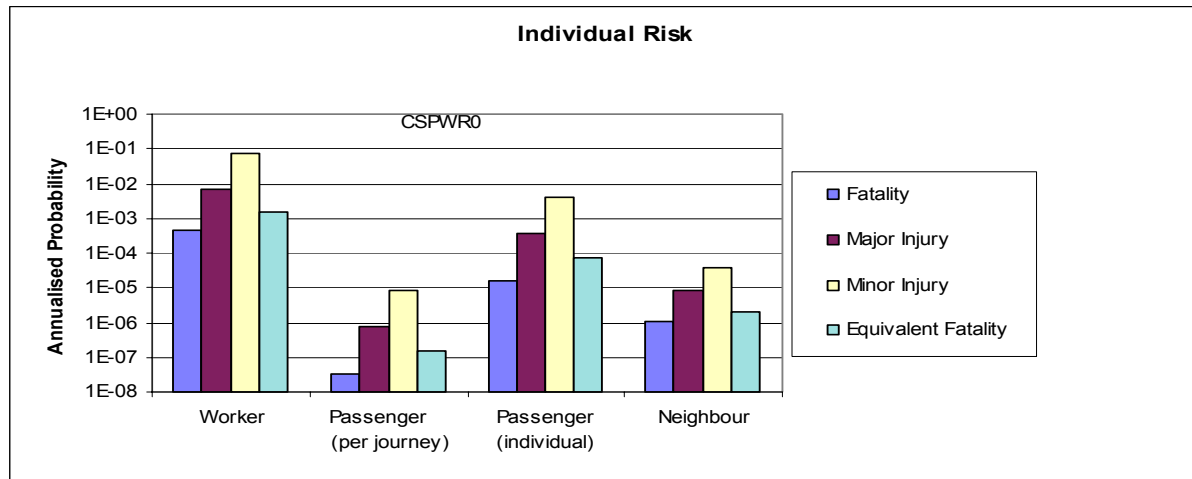


Figure D.2 – Illustrative individual risk forecasts generated by an integrated risk model

From the above, the worker group is most at risk on an individual basis, followed by passengers and then the neighbours.

Annex E (informative)

Techniques & methods

E.1 General

The following clauses describe some practical methods and tools suitable for the different stages of hazard analysis. Table E.1 gives some general guidelines but the selection of the method depends on the system and/or procedure for which a risk assessment is to be carried out and may be different from the one in the guideline. More information about techniques and methods is given in the subsequent clauses of this annex and referenced in the last column of the table. A separate column in the table references existing IEC standards on the method. Also Clause E.13 gives some guidance on the selection of tools and methods. Further guidance is given in Table E.6 of EN 50129 via recommendations applicable to safety-integrity level (SIL).

Table E.1 – Failure and hazard analysis methods

Technique/Method	Hazard Identification	Hazard Analysis/Risk Assessment	Hazard Control/Proof of fulfilment of safety targets	Ref to IEC standard	Reference to more information
RRA Rapid Ranking Analysis; Hazard Ranking	For preliminary purposes	Useful for preliminary hazard analysis and for identifying and ranking hazards for further detailed analysis.	Possible for recording rational for not performing further detailed analysis for low ranking hazards		E.2
Structured What If Analysis	For preliminary purposes				E.3
HAZOP Hazard and Operational Analysis	Useful		Partially useful as supporting element.	61882	E.4
STD State Transition Diagram	Useful in addition to e.g. HAZOP to visualise states and state transition events	Sometimes useful in addition to other methods to visualise states and state transition events	Sometimes useful in addition to e.g. HAZOP to visualise states and state transition events	-	E.5
FMECA Failure Mode, Effects and Criticality Analysis	Highly Recommended	Useful for parallel structures in addition to ETA	Useful for single and parallel structures in addition to FTA and for causal analysis	60812	E.7
ETA Event Tree Analysis		Highly recommended for consequence analysis	Sometimes useful to visualise consequences of a (sub-) system failure	-	E.8
FTA Fault Tree Analysis			Highly recommended for multiple structures, causal analysis	61025	E.9
CCF Common Cause Analysis			Complementary and often solved with a FMECA. Also needed to justify AND-gates in FTA	-	-
Formal methods			Useful for analysing logics	-	E.11.1
Markov		Useful especially for modelling states and fault sequences (in particular when FTA is not applicable)	Useful especially for modelling states and fault sequences (in particular when FTA is not applicable)	61165	E.11.2
RBD Reliability Block Diagram	Useful as a support to HAZOP	Sometimes useful	Useful for non-repairable systems	61078	-
Risk Graph		Apply with caution. See chapter			E.10

E.2 Rapid ranking analysis

Rapid ranking is a technique for capturing hazards in order of their risk significance. It is to ensure that risk assessment effort is focussed on the most significant hazards. Table E.2 gives an example of a matrix that may be used for the initial ranking of hazards. It is similar to the risk-ranking matrix shown in Clause A.3. The higher the ranking, the more priority should be assigned to the hazard.

Table E.2 – Example of a hazard-ranking matrix

	Severity of Potential Harm/Loss				
	5	4	3	2	1
Frequency	Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly	10	9	8	7	6
4= Monthly to yearly	9	8	7	6	5
3=1 to 10 yearly	8	7	6	5	4
2=10 to 100 yearly	7	6	5	4	3
1= Less than 100 yearly	6	5	4	3	2

Basic steps employed in the technique are

- a preliminary identification of hazards,
- a rapid ranking risk evaluation (ranked in order of risk level),
- record of measures that have been taken,
- need for additional or different measures.

The technique has the following properties:

- easy to use,
- focus on risks,
- identifies and documents known risks,
- unstructured,
- many low risks can be neglected.

However, the technique is not easy to apply to large systems and elements.

E.3 Structured What-if analysis

Structured What-if analysis is a predicted form of safety review and is used in analysing preferably previous non-conformities in logs etc to identify any hazardous behaviour. The analysis is managed in accordance to the following principles:

- analyse events and deviations from normal states
- make a preliminary first approximation of risks
- counter-measures possible?

and has the following properties

- easy to understand
- flexible (compared to HAZOP)
- easy to be unstructured

E.4 HAZOP

Hazop-studies is a structured method for identification risks invented in the chemistry industry using keywords to reveal the possible response of the system or process to changes or to deviations from the desired response. The method is described in IEC 61882.

Hazop contains the following paths:

- Intention: The expected functional behaviour
- Deviations: Starts from possible deviations from desired functional states
- Causes: For each deviation the reasons why the deviation should occur
- Consequences: The result of the deviation
- Hazard: The consequences, causing possible damage, injury or loss
- Measures: Possibility to reduce the hazardous condition/behaviour

Examples of guide words is given in Table E.3. The guide words should be tailored to the system/item concerned, before starting a Hazop study.

Table E.3 – Hazop guide words

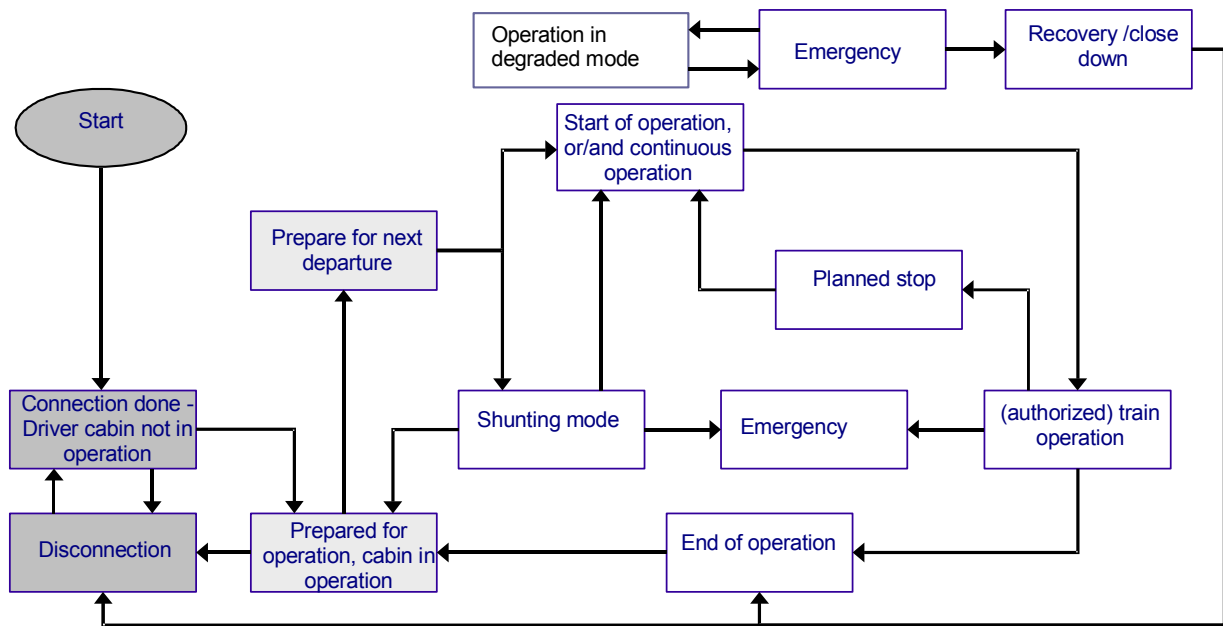
Guide words	Parameters	Deviations
1. No, not, none	Flow	No flow
2. More, higher	Temperature	Higher temperature
3. Less, lower	Current,	Less current
4. As well as	Voltage	Constant high voltage because of a failure
5. Part of	Pressure	Leakage due to loss of valve
6. Other than	Isolation/insulation	Break down of insulation causing possible fire
7. Reverse/Invert	etc.	
8. Late / Early		

NOTE 1, 2, and 3 represent quantifiable deviation parameter of the intended function or property; 4 and 5 represent addition or loss of a quality factor in the intended function or property. 6 represents something unexpected occurs.

The method needs an educated leader to manage the session, good input information, documents of the system and processes. It is effective in finding risks, if properly conducted. However, the method can be tedious and time consuming and is also only a qualitative method.

E.5 State transition diagrams

Visualising the system states in diagrammatic form is an effective means of rapidly achieving an overview of a system's characteristic states or of the states currently being studied. By analysing the transitions between the individual system states, one can obtain information on how events unfold if the conditions required for a transition from one system state to another are not met, are incompletely met, or are met too late. This type of graphical representation is also useful for addressing the question of whether further system states or system transitions need to be taken into account. An example is given in Figure E.1.



E.6 Message Sequence Diagrams

A message sequence diagram handles one single path in the event tree analysis. From a defined number of items and states the exchange of signalling messages after the occasion of an event can be found and analysed for any failure consequences. The diagrams indicates the chronological sequences of the characteristic communications and data interchange channels, as well as the actions, reactions and responses between process participants or system components. A message collaboration diagram (See Figure E.2) can better represent the relationship between the different actors.

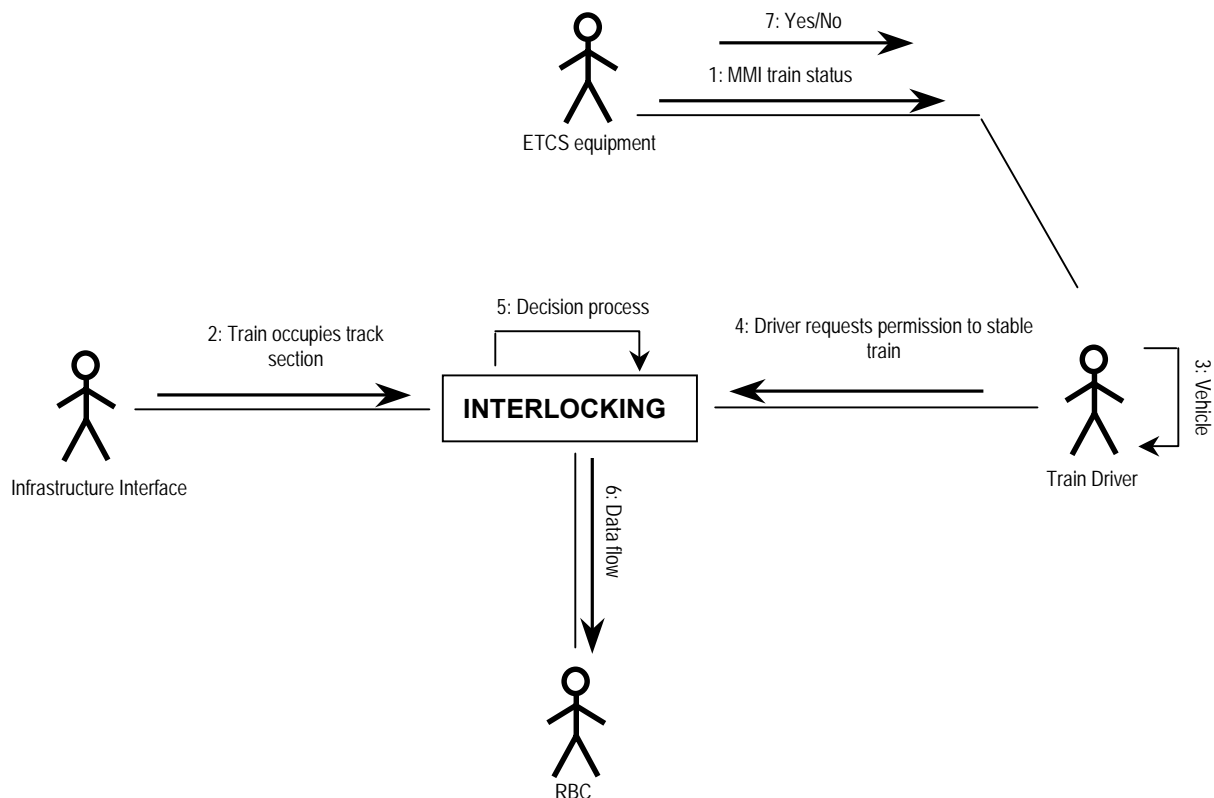


Figure E.2 – Example of message collaboration diagram

E.7 Failure Mode Effects and Criticality Analysis - FMECA

The method is used to study failures and their failure modes in any item under analysis. The item may be a large system or a single physical component and includes processes, functions, software, hardware and human errors. The analysis is of experimental type looking for effects from the failure modes of possible single faults, which can be inserted physically or be analysed more theoretically. Thus it is basically a bottom-up analysis. In software it can be replaced by error seeding and the effects from the error can be studied. Of special value is FMEA when making “intrinsic” safe hardware solutions to analyse the design robustness from a number of thinkable faults and environmental influences. This also makes the FMEA suitable for Common Cause Failure Analysis (CCF). For example it is of interest to assess the independence of the input events to the AND gates that reduce the failure probability or conditional or unconditional failure intensity in fault-tree analysis.

However, the method does not work well for multiple faults or errors where additional non-detected faults should be successively included in the analysis. The resultant number of analysed cases would then increase to impracticable levels. For such multiple-failure cases the fault-tree analysis works better.

FMEA can be extended with a criticality analysis, thereby analysing for critical and accidental effects/events. The method is then called Failure Mode Effects and Criticality Analysis, FMECA.

More information on FMEA and FMECA together with a suitable table for documenting FMECA is given in IEC 60812, which can also be used for a Preliminary Hazard Analysis (PHA). Important is the reference to whether failures are detected or not. If not detected, consecutive analysis should be performed. It is also recommended that the immediate failure and the possible final effect are stated and included. Tables should be suitable for data base handling where connections to fault tree analysis could also be inserted.

NOTE 1 If risk level estimation is part of the FMECA, a decision of risk tolerability includes acceptance from Railway Safety Authority and should be assessed with special care for special conditions and global environment related to tolerable individual and/or collective risk measures. This means that preliminary judgements may need to be reassessed,

NOTE 2 FMECA identifies single point failures only. It is of particular use for demonstrating that a function is fail safe,

NOTE 3 FMECAs have different level of investigations, e.g., system FMECA, design FMECA, etc.,

NOTE 4 FMECA is of particular use for identifying the basic events needed for conducting a FTA,

NOTE 5 FMECA should be limited to lower level sub-systems of a railway system or components. FMECA for a whole train system (although sometimes applied) are not appropriate.

E.8 Event tree analysis

Event tree analysis (ETA) is used mainly to analyse the consequences of failure events and especially in risk analysis. ETA analyses the occurrence of an event and the following sequences of triggering events and their probabilities to a possible end condition, e.g. a resulting accident. Thus, from the event frequency and the consequence probability the accident rate can be calculated. The tree is often graphically made by expanding the possible outcome along a horizontal or vertical axis (Figure E.3).

The structure of an event tree is suited to the visual representation of sequences of operational events and scenarios that can arise once a hazard has occurred and the possible system-inherent responses that can act to avert an accident. Event tree analyses can be used to quantify safety objectives by (a) specifying for each event in a sequence the probability that the event will promote or mitigate the unwanted outcome and (b) by quantifying the possible end states (final outcome) of the system (e.g. the magnitude or severity of an accident). The probability that a particular end state occurs can then be calculated using the rules of probability calculus by multiplying the probabilities of the events along the branch of the event tree from the “trunk” (hazard) to the “leaf” (end state).

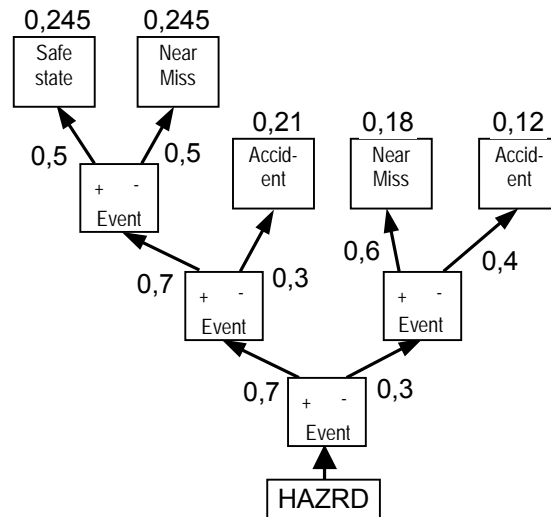


Figure E.3 – Example of consequence analysis using event tree

As the probabilities of the intermediate events will be less than one, these events are known as (risk) reduction factors (multiplication with a probability factor less than one will obviously reduce the likelihood that an accident occurs – not every hazard leads automatically to an accident.)

Multiple operational scenarios can be incorporated within the event tree by introducing events with more than two (yes/no) possible outcomes. Here too, the sum of the probabilities (split fractions) must be equal to one. To handle sequences message sequence diagrams (see Clause E.6) are used in conjunction with Event Tree Analysis.

The power of this method relies on clear model of subsystem's failures, modelled using a Fault Tree. Nevertheless in the railway field, the method should be used with care.

E.9 Fault tree analysis

The fault tree analysis is a widely accepted method of presenting the interaction of system, subsystem and component failures and described in IEC 61025. Fault tree analysis can be used qualitatively, for both systematic and random failures, and quantitatively, where the failure can be quantified, in order to find new fault events to be analysed by Fault event analysis and Failure mode effect and criticality analysis (FMECA).

Fault tree analysis derives the causes for a system failure by examining the logical relationships between the failures of other (sub) systems, components and, in some cases, operating procedures. Logical operations are represented in the diagram by the symbols of Boolean algebra. As OR gates and, in the case of independent events that must occur together to cause failure, AND gates are both used within a fault tree, it is necessary (particularly in the latter case of AND gates) to carry out a so-called common-cause failure analysis to establish that the events being considered are indeed independent of one another. In addition to the physical, technical and functional characteristics of the components, particular attention must also be paid to the operational processes used (such as maintenance, operating methods etc.) to ensure that a failure of the otherwise independent components or subsystems does not have a common cause. Joint maintenance specifications are an example of operational processes that can act as a common cause of failure; inadequate maintenance can result in the failure of otherwise independent components. Other examples are precautions against unauthorised access to railway facilities, or atmospheric effects such as lightning.

The figure below shows a simple failure tree. As error trees rapidly grow in complexity, it is sometimes useful to deal with an element of one tree by constructing another separate tree.

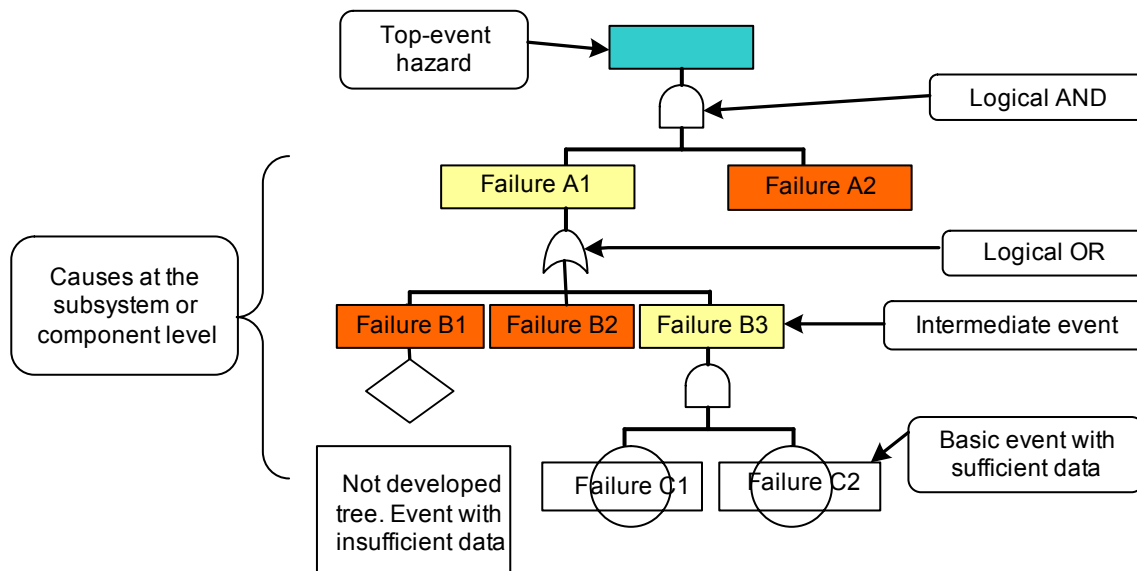


Figure E.4 – Fault tree analysis – Example

Starting from the “system failure” hazard, all possible causes of this (top) event are examined systematically. In the example shown in Figure E.4, the hazard occurs if A1 and A2 fail. The subsystem A1, in turn, will fail if B1 or B2 or B3 fails etc. Important conclusions can be drawn even from qualitative failure trees. For example, if A2 fails, and if B1 or B2 or the combination of C1 and C2 fails then the top event will occur. Whatever the sequence of events, the top event will only occur if A2 fails; the reliability of this subsystem must therefore be particularly high.

E.10 Risk graph method

This is a semi-graphical qualitative method, which estimates the level of required risk reduction in a tree structure. It is an intuitive method, which is described in Annex D of EN 61508-5. Typically, the following 4 risk parameters are graphically depicted, in a tree structure, to enable the safety integrity level for a safety-related system to be determined:

- W - probability of occurrence of an accident (without any safety-related systems but including external risk reduction).
- P - possibility of avoiding the accident.
- F - frequency of, and exposure time in, the hazardous zone.
- C - consequence (severity of the potential accident).

Each of the parameters is divided into a number of classes. The estimation of risk reduction to be provided by the safety-related system, against an accident, is then determined by selecting the most likely class for each parameter and following the decision path in the given tree structure to arrive at the risk reduction level. From this risk reduction level a safety integrity level can be derived, provided that the graph has been appropriately calibrated before hand.

Example data relating to the risk parameters and to their classes is given in Table D.1 of EN 61508-5.

It should be noted that the application of the method for railways relies on the acceptance of the parameters and classes by the bodies/entities involved and by the SRA. It must be understood that these parameters and classes have not been agreed internationally or in Europe for the railway domain:

The method has been developed for the assessment of safety integrity level for electro-mechanical, electrical, or pneumatically controlled protection systems and simple systems (e.g. machine tools) for which the accident scenarios and consequences are easily foreseeable. Its use for the assessment of complex system (like the railways) is questionable.

E.11 Other analysis techniques

E.11.1 Formal methods analysis

Formal methods provide a means of developing a description of a system at some stage in its development specification, design or code. The resulting description takes a mathematical form and can be subjected to mathematical analysis [often by computerised tools] to detect various classes of inconsistency or incorrectness.

One difficulty of formal methods is to understand and properly apply the abilities of the method. Another is to know what the method does not cover. Anything not covered by the method and/or not included in the application specific model at hand will naturally be out of scope of the results from the formal method. (Quote from EN 50128):

Formal methods are used on carefully evaluated “as needs” bases, since incorrect use can give the false impression of producing 100% coverage of all possible combinations.

E.11.2 Markov analysis

Markov analysis can be considered as a special kind of formal method that is a widely used for reliability analysis. Markov analysis uses state diagrams and state transfer rates on the basis that a transition could always occur independently of the state conditions (memory-less transitions). Such behaviour is normal in electronic systems.

With a Markov model it is possible to model time and sequence dependent events, which a fault-tree analysis is not intended to do. For more details about the theory of Markov models see special literature about Markov models (e.g. IEC 61165). Many computer tools that solve Markov models are also available in the market.

E.11.3 Petri networks

Petri networks are a variant of Markov methods. They enable processing of more complex systems where transitions between states do not necessarily obey an exponential distribution (e.g. Weibull distribution). “Stochastic Petri Network” is a class of Petri network that is frequently used for quantitative analysis in RAMS engineering. Furthermore, there is a class of stochastic Petri networks (Deterministic and Stochastic Petri Nets (DSPN)) that includes both exponentially distributed and deterministic delays.

The most important advantage of a Petri network approach to RAMS engineering is its ability to combine qualitative analysis, monitoring and testing, as well as quantitative analysis (in terms of performance/reliability prediction and worst-case analysis).

E.11.4 Cause consequence diagrams

A cause consequence diagrams (CCD) is a combination of event-tree and fault-tree analysis. Since both techniques have already been described (Clause E.8 and Clause E.9), CCD needs no further explanation.

E.12 Guidance on deterministic and probabilistic methods

E.12.1 Deterministic methods and approach

Deterministic methods are in an abstract view a “set of implications”, e.g. “if the system detects a failure the system will shut down”.

These sets of implications may be simple and written down in text form or may be complex and supported by tools or methods. A general way to handle more complex systems is the FMEA or FMECA method. These methods are explained in more detail in Clause E.7.

In general, the problem with a deterministic approach is the reliance on assumptions or a set of boundary conditions. If these definitions are weak then the results of the deterministic analysis will likewise be weak.

However, deterministic methods work particularly well in cases of “fail-safe” principles. In such cases all the known effects (may not be known really exactly) can be put in one class and covered by one fail-safe reaction or one fail-safe mechanism.

Deterministic approach tends to be conservative in establishing acceptance values for new systems, as reliability is treated as point values only associated with a range based on uncertainty (i.e. lack of knowledge, as little or no proven track record exists). This interpretation of probability is referred to as frequentist, as values are assigned on a basis of prior repeated observations. When few observations are available the uncertainty will be high, and a safety assessment will have to be based on a worst case interpretation of the values.

E.12.2 Probabilistic methods and approach

Probabilistic Risk Assessment (PRA) has emerged as an increasingly popular analytical method especially during the last decade. PRA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity (e.g., facility, spacecraft, or railway system) from concept definition, through design, construction and operation, and up to removal from service.

Probabilistic Risk Assessment is based on knowledge of subsystem or component reliability distributions. The system safety behaviour is simulated using the reliability distributions in combination with a system safety model e.g. a fault tree. The interpretation of probability is referred to as Bayesian or logical probability and uncertainty is described as system variability.

Probabilistic methods have been developed to convert deterministic problem formulations into probabilistic formulations to model and assess the effects of known uncertainties.

This approach requires more component data and documentation than the rule based deterministic methods, and is usually supported by computer-aided simulation. Even though the acceptance process tends to be more costly, the developed systems tend to be “leaner” as the approach gives a more detailed description of the system hazards, and offers guidance on which parts of the system has the biggest impact on system safety.

The dynamic simulation of the fault tree (e.g. Monte Carlo simulation) allows using the laws of appearance or disappearance basic event.

E.12.2.1 Monte Carlo Simulation

Monte Carlo Simulation is an example of a probabilistic quantitative method for evaluating exposure and risk. Quantitative methods to assess uncertainty, such as sensitivity analysis and probabilistic analysis using Monte Carlo Simulations (MCS), have been increasingly used to identify factors that have the greatest effect on the risk estimation and to provide a frequency distribution for potential risks.

Probabilistic analyses represent one means of characterising uncertainties in risk assessment. MCS is one method used to generate probabilistic risk estimates and is a computer-assisted propagation of risk based on various combinations of exposure parameters to simulate the entire spectrum or distribution of risk and hazard for a potentially exposed individual. Using MCS techniques, it is possible to represent the uncertainty in the risk characterisation model by generating sample values (in the form of frequency distributions) for the model input and running the model repetitively. Instead of obtaining a single risk estimate to represent the model output as in a deterministic risk assessment, a set of sample results are obtained that can present the output as a frequency distribution or a cumulative density function. These results can then be summarised using, typically, to identify central tendencies (expected risks) and associated high-end exposure with probability of occurrence.

There are several commercially available MCS software packages, which can be used in conjunction with standard spreadsheet software to perform probabilistic risk computations. Most commercial MCS software packages include Latin Hypercube sampling capability as a means to reduce the number of computer runs by selectively sampling more at the tails (i.e., upper and lower ends) of the distribution.

Advantages and disadvantages of performing MCS are as follows.

Advantages:

- 1.1 More complete characterisation of uncertainty in a form that is less likely to include a bias.
- 1.2 The probability distribution enables the risk manager to associate the high-end risk with the likelihood or probability of occurrence.
- 1.3 When combined with sensitivity analyses, MCS allows a more informative and quick “what-if” assessment of the impact on the risk estimate of a change in an individual parameter or a group of parameters, thus providing a cost-effective tool for making risk management decisions.
- 1.4 The probabilistic analysis permits more constructive comparisons of remedial alternatives when diverse attributes must be compared to systematically reduce the baseline risk. This includes comparing alternatives or intervening measures that could also cause remediation risks.

Disadvantages:

- 1.1 MCS requires time and effort to set up the database and document the rationale for the cumulative density function (distribution of possible values) for individual parameters in the risk algorithm.
- 1.2 The distribution patterns for some parameters are not definitively known, requiring the use of credible professional judgment or costly subsystem or component-specific studies or data collection efforts. (Despite the cognisance of a risk assessor of parameters that could be dependent variables, the impact of such interdependencies between or among variables may be difficult to quantify if their co-relations are not well known.)
- 1.3 MCS is resource intensive. Additional costs could be higher than that of a standard deterministic risk assessment.

E.13 Selection of tools & methods

Selecting methods is a highly individualized process so that a general suggestion for a selection of one or more of the specific methods cannot be made. Selection should be done early in the development of safety programme and should be reviewed for applicability.

Often there is a temptation to try and apply a particular method or tool, that one is very familiar with or an expensive tool that has been purchased for a specific technique, to all problems. However, this does not always produce the desired results.

For example, FTA is very powerful when applied to complex problems of the combinatorial type (Boolean logic), but has drawbacks in particular for systems with state-dependant or sequence-dependent events. On the other hand, Markov models handle the latter well, but work on the constant failure rate assumption. Hence it cannot be said that FTA is better than Markov (or vice versa) and use one technique only. The decision needs to be taken on a case-by-case basis and in some cases other methods (e.g. numerical integration, Monte Carlo simulation, etc.) or a combination of them may be most appropriate.

EN 60300-3-1 provides an overview and selection criteria for tools and methods. However, selecting methods and tools could also be made easier by considering the following:

- *System complexity*: Complex systems, e.g. involving redundancy or diversity features, usually demand a deeper level of analysis than simpler systems.
- *System novelty*: A completely new system design may require a more thorough level of analysis than a well-proven design.
- *Qualitative vs. quantitative analysis*: Is a quantitative analysis necessary?
- *Single vs. multiple faults*: Are there relevant effects arising from combination of faults or can they be neglected?
- *Time-dependent or sequence-dependent behaviour*: Does the sequence of events play a role in the analysis (e.g. the system fails only if event A is preceded by B, not vice versa) or does the system exhibit time dependent behaviour (e.g. degraded modes of operation after failure, phased missions)?
- *Bottom-up vs. top-down analysis*: Usually, bottom-up methods can be applied in a more straightforward manner while top-down methods need more thought and may therefore be more error-prone.

- *Allocation of safety requirements*: Should the method be capable of quantitative allocation?
- *High safety requirements*: The demonstration of high safety requirements usually demands a more thorough level of analysis.
- *Domain expertise*: What level of education or experience is required in order to meaningfully and correctly apply the method and is it easily explainable to non-specialists so that they can be involved?
- *Acceptance and commonality*: Is the method commonly accepted, e.g. by a regulatory authority or a customer?
- *Standardisation*: Is there an industry wide recognized standard, which describes the features of the method and the presentation of results (e.g. symbols, etc.)?
- *Need for tool support*: Does the method need tool support or can it also be performed manually?
- *Plausibility checks*: Is it easy to inspect the plausibility of the results manually? If not, are the available tools validated?
- *Availability of tools*: Are tools available commercially? Do these tools have a common interface with other analysis tools so that results may be re-used or exported?

Annex F (informative)

Diagrammatic illustration of availability concept

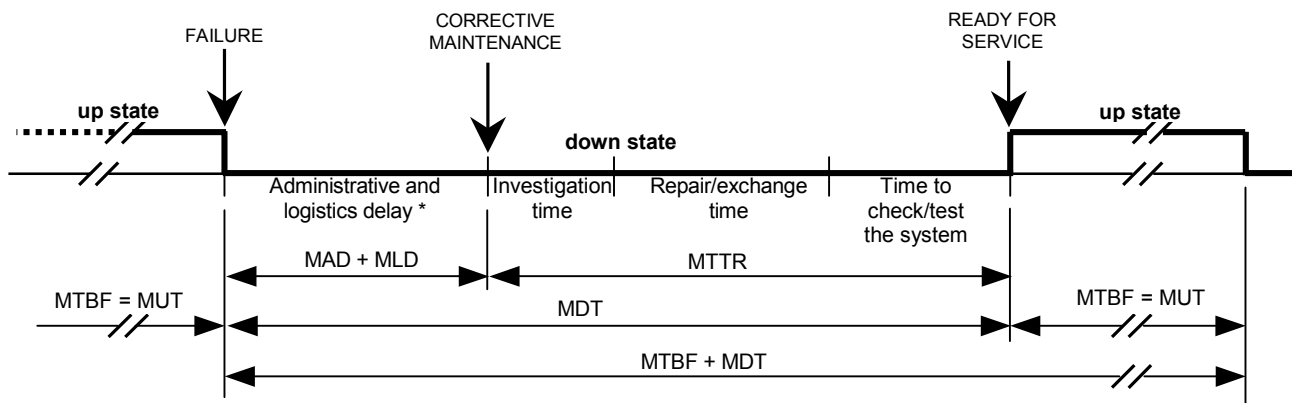
The *availability* A of a system is defined by the fraction of time the system is running properly hence

$$A = \frac{MUT}{MUT + MDT} = \frac{MTBF}{MTBF + MDT} \leq 1,$$

and generally has a value close to 1. As a consequence its complement, called the *unavailability*

$$1 - A = \frac{MDT}{MTBF + MDT} \geq 0$$

tends to zero.



MTBF mean (operating) time between failures
 MUT mean up time
 MDT mean down time
 MAD mean administrative delay
 MLD mean logistics delay

MTTR mean time to restoration (for corrective maintenance)

This period of time describes the active maintenance time.
 In case of preventive maintenance there is no detection time.

* represents all relevant fractions within MDT

Figure F.1 – Availability concept and related terms

Annex G (informative)

Examples of setting risk acceptance criteria

G.1 Example of ALARP application

The following examples indicate how the ALARP principle can be applied, independently from national requirements and other risk assessment requirements.

The basic idea is already given in EN 50126-1 itself. Table 6 of EN 50126-1 shows a risk matrix with four areas of risk:

- intolerable;
- undesirable;
- tolerable;
- negligible.

For the ALARP principle only three areas apply, because "intolerable" and "undesirable" is classed the same, i.e., it is an area of unacceptable risk.

Hence the three remaining areas are

- unacceptable, which equates to the unacceptable region,
- tolerable, which equates to the ALARP region,
- negligible, which equates to the broadly acceptable region.

The basic idea of risk assessment is as follows.

- **Unacceptable risk** has to be **reduced**, (approval is unlikely).
- Negligible risk needs no further risk reduction.
- **Risk** assessed or calculated to be in the **"tolerable" region**, needs to be further investigated to see if **additional risk reducing measures** can transfer the risk into the "negligible" region **and** that this safety improvement **really pays**.

Referring to [Bibliography 8], engineering safety management systems (Yellow Book) in UK, risk assessment is described as a seven-stage process, with the following stages (also see 5.3.2, which is the same in principle but lumps some of the stages together):

- i) *Hazard identification*: identification of a specific hazard;
- ii) *Causal Analysis*: cause of the hazard;
- iii) *Consequence Analysis*: intermediate and final consequences of the hazard;
- iv) *Loss Analysis*: magnitude of safety losses (before a mitigation measure);
- v) *Options Analysis*: determination and assessment of mitigation measures;
- vi) *Impact Analysis*: assessment of the benefit of each measure;
- vii) *Demonstration of ALARP and compliance*: justification of the remaining risk.

In order not to repeat the Yellow Book, it is assumed that the first six stages have already been done. So, there is demonstration of ALARP.

Consequently, the first task is to establish the upper and lower boundaries for the tolerable risk region.

A customer or an authority may provide the boundary levels, or they may be generated by yourself and agreed the relevant customer or authority (for deriving the boundary levels also see "The Yellow Book". Volume 2 Part D, Examples).

Remember, that risk has two parameters:

- the severity of harm from an accident;
- the frequency of occurrence of the accident.

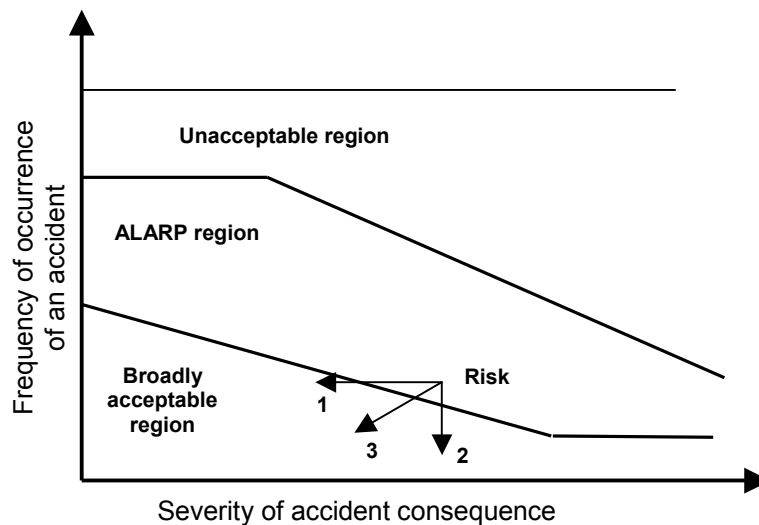


Figure G.1 – Risk areas and risk reducing measures

Hence, there are 3 options for reducing the risk:

- mitigate the consequences of an accident (e.g., a safety belt in a motorcar) (Arrow 1 in Figure G.1);
- reduce the probability of occurrence of the accident by implementing additional safety barriers or by using more reliable components (Arrow 2 in Figure G.1);
- do both (Arrow 3 in Figure G.1).

The following examples are neutral and do not focus on a specific application or technology. They are based on a TUEV seminar (see bibliography).

Assume that analysis of a system shows, for one specific hazard, the following properties.

- The average loss of harm in case of an accident is estimated to 1 Million € (e. g. light or medium heavy injury to a person or damage to equipment or goods).
- The rate of occurrence for an accident is estimated at $4 \cdot 10^{-3}$ per year.
- Operational time is 10 years.

Which of the following options are the most effective ones according to ALARP?

Option 1: The risk reduction is performed by a supervision device, which controls the safety of the process. It is assumed, that this will reduce the rate of accidents to $2 \cdot 10^{-4}$ per year. The device will cost 30 000 €.

Option 2: A protective coverage will be implemented. This will reduce the loss of harm from 1 Mio € to 500 000 €. The coverage will cost 6 000 €.

Option 3: Improved operational instructions and warning tags will reduce the time under risk and will improve safety awareness. It is estimated, that the accident rate is reduced to 50 %. The cost will be 1 000 €.

Option 4: An additional control person will supervise the process continuously. It is estimated, that this will reduce the accident rate to $1 \cdot 10^{-5}$ per year. The cost for this person will be 25 000 € per year.

Solutions:

The actual total risk (over 10 years) will be calculated according to:

$$\text{Risk} = \text{Rate of occurrence per year} * \text{Loss of harm} * \text{Number of years}$$

$$\text{Risk 0} = 4 \cdot 10^{-3} \text{ per year} * 1 \text{ Mio €} * 10 \text{ years} = 40\,000 \text{ €}$$

For Option 1:

The supervision device reduces the accident rate to $2 \cdot 10^{-4}$ per year

$$\text{Risk 1} = 2 \cdot 10^{-4} \text{ per year} * 1 \text{ Mio €} * 10 \text{ years} = 2\,000 \text{ €}.$$

The risk will be reduced from 40 000 € to 2 000 €, with a cost of 30 000 €

Hence benefit: $40\,000 \text{ €} - 2\,000 \text{ €} = 38\,000 \text{ €}$, cost: 30.000 €, consequently cost benefit = $38\,000 \text{ €} - 30\,000 \text{ €} = 8\,000 \text{ €}$

For Option 2:

$$\text{Risk 2} = 4 \cdot 10^{-3} \text{ per year} * 500\,000 \text{ €} * 10 \text{ years} = 20\,000 \text{ €}$$

The risk will be reduced from 40 000 € to 20 000 €.

Hence benefit: 20 000 €, cost: 6 000 €, consequently cost benefit = 14 000 €.

For Option 3:

$$\text{Risk 3} = 2 \cdot 10^{-3} \text{ per year} * 1 \text{ Mio €} * 10 \text{ years} = 20\,000 \text{ €}$$

The risk will be reduced from 40 000 € to 20 000 €.

Hence benefit: 20 000 €, cost 1 000 €, consequently cost benefit = 19 000 €.

For Option 4:

$$\text{Risk 4} = 1 \cdot 10^{-5} \text{ per year} * 1 \text{ Mio €} * 10 \text{ years} = 100 \text{ €}$$

The risk will be reduced from 40 000 € to 100 €.

Hence benefit 39 900 €, cost 250 000 €, consequently cost benefit = $(- 210\,100) \text{ €}$.

Consequences of the solutions are:

Options 2 and 3 are rather cheap and efficient and could be implemented. Option 1, the supervision device, is more expensive, but according to ALARP, is more cost effective. Option 4 provides the best risk reduction, but the cost is too high. So, this option should only be implemented, if specifically required by e.g. an Approval body.

The following picture (Figure G.2) shows the impact of the options in the risk graph:

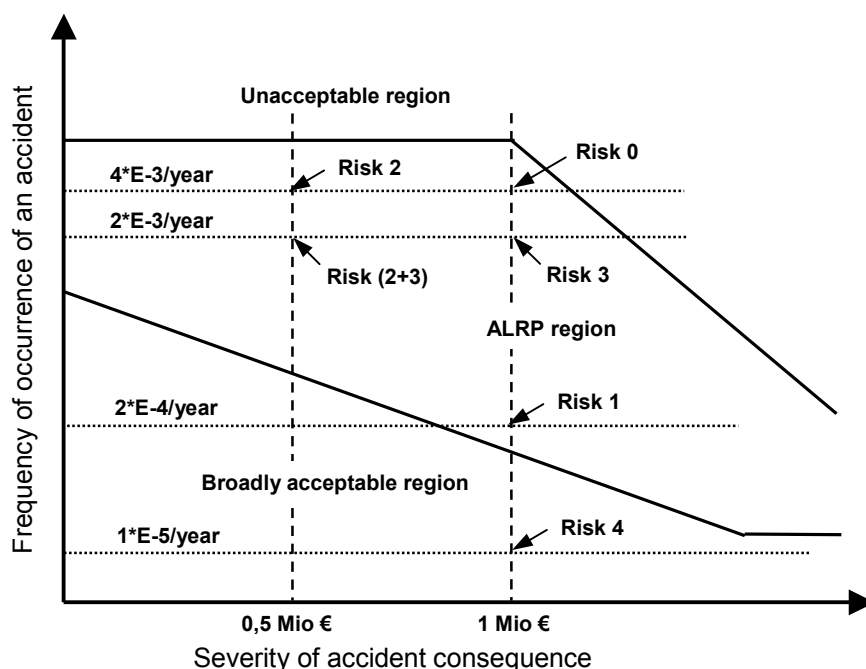


Figure G.2 – ALARP results of options 1 to 4

Discussion of the results: If Options 2 and 3 are combined then even though the risk remains in the ALARP area, the safety has improved significantly. Both the frequency of occurrence and loss of harm are reduced to 50 %.

A "Genuine ALARP" option would be Option 1, because the risk gets into the broadly accepted area. Option 4 would consequently not be a good ALARP option, because the term "as reasonably practicable" is not valid.

G.2 Copenhagen Metro

The example in Table G.1 is from the Copenhagen Metro where a comparison and scaling of the Skytrain system in Vancouver, Canada and the VAL system in Lille, France was performed.

The figures in Table G.1 were chosen by starting with defining the upper and lower limits of the first consequence class (1 - 2 fatalities) based on data from Lille and Vancouver. Then the slope of 1½ decade by decade on a double logarithmic scale was used to define the ALARP band. This slope was determined based on an evaluation of acceptance criteria from the Øresund Link to Sweden and from British Rail (the Channel Tunnel Safety Case).

Table G.1 – Upper and lower ALARP limits

Consequence class (fatalities)	Characteristic no. of fatalities	Max acceptable frequency pr. year	Lower delimitation of ALARP domain (pr. year)
1 – 2	1	4,0 E-2	4,0 E-5
3 – 30	10	1,3 E-3	1,3 E-6
31 – 300	100	4,0 E-5	4,0 E-8
> 300	1 000	1,3 E-6	1,3 E-9

NOTE The example and figures are specific to Copenhagen Metro. These figures are not directly transferable to other systems. Care must be taken when applying the method to other projects. Whilst the method could be applicable, the figures to be used must be derived from the risk assessment of the particular system.

Annex H

(informative)

Examples of safety case outlines

These are indicative examples and should not be treated as exhaustive.

H.1 Rolling stock

1 Introduction

- 1.1 Background and objective
- 1.2 Scope and limitations
- 1.3 Definitions and abbreviations
 - 1.3.1 General
 - 1.3.2 Assemblies

2 Definition of system

- 2.1 System structure/numbering
 - 2.1.1 Locomotive
 - 2.1.2 Bogie
 - 2.1.3 Brakes
 - 2.1.4 Control & Communication
 - 2.1.5 Auxiliary system
 - 2.1.6 ATC/ATP
 - 2.1.7 Main Technical Data
- 2.2 Description of new technology
 - 2.2.1 Wheel Slide Protection, (WSP)
 - 2.2.2 Line Interference Monitor, (LIM)

3 Quality management report

- 3.1 Quality management control
- 3.2 Suppliers quality control system
 - 3.2.1 Change control procedure
 - 3.2.2 Document control
 - 3.2.3 Sub-supplier Quality assurance
 - 3.2.4 Type- and Routine test program

4 Safety management report

- 4.1 Safety management control system
- 4.2 Safety work group Operator/Supplier

5 Technical safety report

5.1 Definition of safety aspects covered by the report - Hazards

5.2 Safety requirements

5.2.1 Overall risk criteria

5.2.2 Norms and standards incl. Deviations

5.2.3 Contract safety requirements

5.2.3.1 Safety activities

5.2.3.2 Content of the Safety Report

5.2.3.3 Risk evaluation

5.2.3.4 Risk criterion

5.2.3.5 Safety critical functions

5.2.4 Safety functional requirement of sub-systems

5.3 Risk evaluation

5.3.1 Preliminary Hazard Analysis-Event Statistics Review

5.3.2 Critical Condition- Cause Analysis

5.3.3 Fault Tree Analysis

5.3.4 Risk Evaluation

5.4 Summary of performed safety activities

5.4.1 Operator activities

5.4.2 Overview of activities

5.4.3 List of activities

5.5 Verification of Safety Critical Functions

5.5.1 General

5.5.2 Verification of SCF:s in the Type-/Routine test program

5.5.3 Verification of SCF:s in Driver's Manual and Maintenance plan

6 Related safety cases

7 Conclusion: Concluding safety judgment

7.1 "Worst Case Scenarios"

7.2 Scenario 1, "Components falling down on track"

7.3 Scenario 2, "Acute wheel breakdown"

7.4 Scenario 3, "Broken wheel axle"

7.5 Scenario 4, "Motor, gear box or transformer/protection coming in contact with track"

7.6 Scenario 5, "Emergency heater/tank fire"

7.7 Scenario 6, "No pressure reduction in main brake pipe"

7.8 Scenario 7, "Failure in loco brakes –Section travelling alone"

7.9 Scenario 8 "ATC does not apply brakes and traction cut off"

7.10 Comparison with existing material

- 8 Document list
- 9 Appendices
- 10 References

H.2 Signalling

- 1 Introduction
 - 1.1 Aim of the document
 - 1.2 Fields of application
 - 1.3 Structure of the document
 - 1.4 Regulations applicable to the system
- 2 Definition of system
 - 2.1 Part 1 a: definition of the system
 - 2.1.1 Structure and functions of the pai-pl system
 - 2.1.2 System performance
 - 2.1.2.1 "Vital" Obstacles Detection Mode
 - 2.1.3 Records traceability
 - 2.1.4 Definition of hierarchic levels
 - 2.1.5 Document revisions traceability
 - 2.2 Part 1b: definition of the control logic system
 - 2.2.1 Structure and functions of the control logic system
 - 2.2.1.1 CPU board description
 - 2.2.1.2 Description of the WD board
 - 2.2.1.3 I/O board description
 - 2.2.1.4 BARR board description .
 - 2.2.1.5 ALIM board description
 - 2.2.1.6 SOS board description
 - 2.2.1.7 ALF board description
 - 2.2.2 Records traceability
 - 2.2.3 Definition of hierarchic levels
 - 2.2.4 Document revisions traceability
 - 2.3 Part 1c - definition of the sensors system
 - 2.3.1 Structure and functions of the sensors system
 - 2.3.1.1 TRX board description
 - 2.3.1.2 PRF board description
 - 2.3.1.3 MDR/MMDT board description
 - 2.3.1.4 ITR board description
 - 2.4 Records traceability
 - 2.5 Definition of hierarchic levels
 - 2.6 Document revisions traceability

3 Quality management reports – Part 2

- 3.1 Quality plan
- 3.2 Technical inspection report
- 3.3 Quality testing report

4 Safety management report – Part 3

- 4.1 Introduction
- 4.2 Safety life cycle
- 4.3 Safety organization
- 4.4 Safety plan
- 4.5 Hazard log
- 4.6 Safety requirements specification
- 4.7 System design
- 4.8 Safety reviews
- 4.9 Verification and validation plan
- 4.10 Safety assurance
- 4.11 Approval of the system by the railway authority
- 4.12 Operation and maintenance
- 4.13 Decommissioning and disposal
- 4.14 RAM plan (and activity)
- 4.15 Software development plan
- 4.16 Configuration management plan

5 Technical safety report – Part 4a

- 5.1 Introduction
- 5.2 Assurance of correct functional operation
 - 5.2.1 System Architecture Description
 - 5.2.2 Definition of Interfaces
 - 5.2.3 Fulfilment of System Functional requirements Specification
 - 5.2.4 Fulfilment of System safety requirements Specification
 - 5.2.5 Assurance of correct hardware Functionality
 - 5.2.6 Assurance of correct software Functionality
- 5.3 Effects Of Faults
 - 5.3.1 Single Faults
 - 5.3.2 Independence of Items
 - 5.3.3 Detection of Single fault
 - 5.3.4 Actions Following Detection
 - 5.3.5 Multiple faults
 - 5.3.6 Defence against systematic faults

5.4 Operation With External Influences

- 5.4.1 Climatic conditions
- 5.4.2 Mechanical conditions
- 5.4.3 Altitude
- 5.4.4 Electrical conditions
- 5.4.5 Electrical conditions (on the vehicle)
- 5.4.6 Protection against unauthorized access
- 5.4.7 More Severe Conditions

5.5 Application Conditions Affecting Safety

- 5.5.1 System configuration and manufacturing
- 5.5.2 Operation and Maintenance
- 5.5.3 Operational safety monitoring
- 5.5.4 Decommissioning and Disposal

5.6 System Qualification Test

- 5.6.1 Test definition and planning
- 5.6.2 Tests Report

5.7 Part 4b - control logic safety technical report

5.8 Part4c - microwave sensors safety technical report

6 Related Safety Case

7 Conclusions

- 7.1 Summary of system operation and characteristics

8 Documents and applicable regulations

- 8.1 Applicable regulations
- 8.2 Customer (rfi) input documents
- 8.3 Supplier (gets) documents required for this plan
- 8.4 Definitions, acronyms, abbreviations

9 Appendices

10 References

H.3 Infrastructure

"Safety Case Structural Design of Segmental Lined Bored Tunnels and Tunnel Internal Elements"

1 Introduction

- 1.1 Abbreviations and Acronyms
- 1.2 General

2 System Definition

2.1 General System

- 2.1.1 General
- 2.1.2 Contract Responsibilities
- 2.1.3 Subsystem Definition
- 2.1.4 General
- 2.1.5 Tunnel Linings and Internal Structures
- 2.1.6 Construction
- 2.1.7 Interface with Station and Shaft Construction
- 2.1.8 Interface with the TS (Transportation System) Contract

3 Quality Management Report

- 3.1 Quality Assurance
- 3.2 Organisational Structure
- 3.3 Quality Planning and Procedure
- 3.4 Specification of Requirements
- 3.5 Design Control
- 3.6 Design Verification and Validation
- 3.7 Documentation and Records
- 3.8 Quality Monitoring and Feedback
- 3.9 Change Control
- 3.10 Personnel Competency and Training
- 3.11 Quality Audits and Follow-up

4 Safety Management Report

- 4.1 Safety Related Documents
- 4.2 Safety Management Organisation
- 4.3 Safety Verification and Validation
- 4.4 Safety Reviews and Hazards Logs
- 4.5 Safety Meetings
- 4.6 Safety Assessor Process

5 Technical Safety Report

- 5.1 General
- 5.2 Design Codes and Standards
- 5.3 Technical Notes Prepared by the Designer
- 5.4 Reliability Requirements
- 5.5 Safety Related Design Aspects

6 Related Safety Cases

7 Conclusions.

8 Document list

9 Appendices

10 References

10.1 Quality and Safety Management Documents

10.2 Safety Related Standards

10.3 Design Documentation Produced by Faber Maunsell

10.4 Design Documentation Produced by Taylor Woodrow Construction Ltd

10.5 Documentation Produced for the Safety Assessment of the Design of the Segmental Lined Bored Tunnels and Tunnel Internal Elements

Bibliography

In addition to the references to standards listed in Clause 2, the following documents were consulted during the preparation of this report:

- 1 Deterministic and Probabilistic approaches in Risk Analysis. The Walloon Region's hybrid approach. G. Van Malder.
- 2 Monte Carlo Simulation in Environmental Risk Assessment Science, Policy and Legal Issues. Susan R. Poulter, University of Utah College of Law.
- 3 Information theory, Inference, and learning Algorithms. On-line textbook by David MacKay.
<http://www.inference.phy.cam.ac.uk/mackay/itila/book.html>
- 4 Probabilistic Risk Assessment: What Is It and Why Is It worth Performing It?
Dr. Michael Stamatelatos, NASA Office of Safety and Mission Assurance
- 5 NPRD-95- Non-electronic Parts Reliability Data (published by Reliability Analysis Centre) and NSWC-94/L07- Handbook of reliability prediction procedures for Mechanical Equipment.
- 6 Krebs, H: Minimale Endogene Mortalität – ein universelles Sicherheitskriterium, ETR 49 Dezember 2000
- 7 Schäbe, H: Different Principles Used for Determination of Tolerable Hazard Rates, Contribution to the WCRR 2001
- 8 Engineering Safety Management Systems, Yellow book; Published by Railtrack on behalf of the UK rail industry (RSI and RA)
- 9 Procedures for formal design reviews: with emphasis on RAMS, using some general and application specific check lists as appropriate. e.g.

IEC 61160 Formal design review; (amendment 1)
- 10 Procedures for performing hazard & safety/risk analysis. Some of these are described in:

US MIL HDBK 882D System safety programme requirements

US MIL HDBK 764 (MI) System safety engineering, design guide for army materiel

UK Def Stan 00-56 Safety Management Requirements for Defence Systems, UK Ministry of Defence
- 11 TUEV Seminar: given by the German "RW TUEV Informationstechnik, Dept. Safety Approval Services" (example included with their kind permission).
- 12 Leveson, N. G.: Safeware – System safety and computers, Addison-Wesley, 1995 (hazard concept)
- 13 Kumamotu, H and Henley, E.: Probabalistic risk assessment and management for engineers and scientists, IEEE press, 1996 (general risk concept)
- 14 Schneider, J.: Sicherheit und Zuverlässigkeit im Bauwesen, Teubner, Stuttgart, 1996 (risk assessment of other technologies)
- 15 Abernathy: The Weibull Handbook, 2002 (general failure rates)
- 16 System Safety Analysis Handbook, 2nd edition, System Safety Society, 1998
- 17 Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment, Vol 1: Methods and Techniques, Wiley 1992

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at <http://www.bsi-global.com>.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.
Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.
Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001.
Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at <http://www.bsi-global.com/bsonline>.

Further information about BSI is available on the BSI website at <http://www.bsi-global.com>.

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained.

Details and advice can be obtained from the Copyright & Licensing Manager.
Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553.
Email: copyright@bsi-global.com.