

© Copyright SEK. Reproduction in any form without permission is prohibited.

**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**
(CENELEC Technical Report 50126-2: 2007)

ISSN 1651-1417

ICS 45.020

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. Telefax: 08 - 444 14 30
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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.