# SLOVENSKI STANDARD
# SIST-TP CLC/TR 50126-2:2007

**01-september-2007**

**Železniške naprave – Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) – 2. del: Vodilo za uporabo EN 50126-1 za varnost**

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

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

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

**Ta slovenski standard je istoveten z:** **CLC/TR 50126-2:2007**

**ICS:**

| | | |
|---|---|---|
| 29.280 | Elektriļ na vleļ na oprema | Electric traction equipment |
| 45.020 | Železniška tehnika na splošno | Railway engineering in general |

**SIST-TP CLC/TR 50126-2:2007** **en**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

**CLC/TR 50126-2**

February 2007

ICS 45.020

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

**Figures**

**Tables**

## 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+Δt) 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.

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

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 (**Δt** →0) of time **λ(t)** * **Δt** 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 λ=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<br>railway undertaking |
| safety regulatory authority | safety authority |
| railway support industry | supplier<br>manufacturing industry |