

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

**Railway applications –
Communication, signalling and processing systems –
Application Guide for EN 50129 –
Part 2: Safety assurance**
(CENELEC Technical Report 50506-2:2009)

Denna tekniska rapport ska användas tillsammans med SS-EN 50129.

ISSN 1651-1417

ICS 93.100

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 -
Communication, signalling and processing systems -
Application Guide for EN 50129 -
Part 2: Safety assurance**

This Technical Report was approved by CENELEC on 2009-07-17.

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: Avenue Marnix 17, B - 1000 Brussels

Foreword

This Technical Report was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to vote in accordance with the Internal Regulations, Part 2, Subclause 11.4.3.3 (simple majority) and was approved by CENELEC as CLC/TR 50506-2 on 2009-07-17.

Contents

Page

Introduction	5
1 Scope	6
2 References	6
3 Terms, definitions, symbols and abbreviated terms	7
3.1 Terms and definitions	7
3.2 Symbols and abbreviated terms	8
4 Safety design for signalling subsystems	10
4.1 Safety principles	10
4.2 Components development guideline	19
4.3 Specific implementation examples	25
5 Safety case structure in relation with associated documents and activities	28
5.1 Introduction	28
5.2 Safety Case for Signalling Systems	28
5.3 Recommendations regarding the fulfilment of the requirements of tables in EN 50129:2003, Annex E	62
6 Safety assessment and approval	68
6.1 Guidance on the concept of Safety assessment	68
6.2 Migration strategy from other Standards to CENELEC	73
6.3 Approval for modification and internal adaptation	75
Annex A (informative) EN/IEC standards for safety analysis	77
Annex B (informative) Documentation for approval	78
B.1 Introduction	78
B.2 Documentation table structure	79
B.3 Liaison to EN 50129:2003, 5.5.2	79
Annex C (informative) Structure of the System Requirements Specification	87
C.1 Part one – General information	87
C.2 Part two – Requirements	87
Bibliography	89

Figures

Figure 1 – Example for hierarchical composition of Functional units	11
Figure 2 – Example for creation and manifestation mechanisms of faults, errors, and failures.....	11
Figure 3 – Example for the mechanisms of ‘fundamental chain’	12
Figure 4 – Relationships of faults, errors and failures	12
Figure 5 – Representation for failures of single and multiple natures	14
Figure 6 – Inherent fail safe devices structure and associated threats	15
Figure 7 – Composite fail safe devices structure and associated threats	17
Figure 8 – Reactive fail safe devices structure and associated threats	18
Figure 9 – Example of composite fail-safety with identical VLSI components	21
Figure 10 – Example of reactive fail-safety with different VLSI components	23
Figure 11 – Example of development process for VLSI components (FPGA, EPLD, etc.).....	25
Figure 12 – Example of overall Safety Cases structure	30
Figure 13 – Structure of the Technical Safety Report	46
Figure 14 – Example of inherent fail-safety	50
Figure 15 – Example for Relation between Design Functional Breakdown	55
Figure 16 – Example of Relation breakdown from FMEA to FTA	56
Figure 17 – SRAC classification	58
Figure 18 – Exported constraints and SRAC management	59

Tables

Table 1 – Examples for single and coupled failures types	14
Table 2 – Guidance for threats mitigation in inherent fail-safe devices.....	16
Table 3 – Guidance for threats mitigation in composite fail-safe devices	17
Table 4 – Guidance for threats mitigation in reactive fail-safe devices	18
Table 5 – Example of documentation linked to Quality Management	32
Table 6 – Typical Example of some Safety Activities in the Lifecycle	36
Table 7 – Methods for Safety Analysis	37
Table 8 – List of safety methods and reference Standards.....	37
Table 9 – Safety planning and quality assurance activities.....	63
Table 10 – System requirements specification.....	64
Table 11 – Design phase documentation	66
Table 12 – Operation and maintenance	67
Table 13 – Typical assessor activity during the life cycle.....	69
Table 14 – Possible Work split Approval for modification	76
Table B.1 – Documentation for Approval.....	80

Introduction

EN 50129 was developed in CENELEC and is now regularly called up in specifications. In essence, it lists factors that influence RAMS (see EN 50126-1) and adopts a broad risk-management approach to safety. EN 50129 is the basic standard for safety related electronic systems for signalling.

Use of EN 50129 has enhanced the general understanding of the issues, but also showed, that items like Safe Design, Safety Documents and Reports, Safety Assessment and Approval, and Cross-Acceptance need further explanation and clarification. Therefore CENELEC decided to address those items in this Application Guideline. The Cross Acceptance is included in CLC/TR 50506-1.

1 Scope

This document is a Technical Report about the basic standard. It is applicable to the same systems and addresses the same audience as the standard itself. It enhances information on specific items on the application of EN 50129. The following items are covered, within the scope of this Application Guideline of EN 50129, as follows:

- Clause 4 deals with identification and mitigation of failures in the concept, specification and design phases. It is mainly dedicated to designers and verifiers and product safety engineers;
- Clause 5 deals with the preparation of a safety case, enhancing points providing the required evidence for safety assessment and approval. It is mainly dedicated to verifiers, validators, safety managers, quality managers and safety engineers;
- Clause 6 deals with the activities an Independent Safety Assessor has to carry out. It is mainly dedicated to safety assessors, safety authorities, safety managers and safety approvals.

In drafting this guidance, it is assumed that the reader is familiar with the basic structure of the standard.

This document does not claim to be exhaustive. It is not a complete compilation of best practices, but only the translation of the knowledge of all the experts of the Working Group in charge of composition of this Application Guideline.

2 References

This Application Guideline uses as basis for specific topics the following reference standards, already mentioned in the main EN 50129.

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CLC/TR 50506-1, *Railway applications – Communication, signalling and processing systems – Application Guide for EN 50129 – Part 1: Cross-acceptance*

EN 45004 ¹⁾, *General criteria for the operation of various types of bodies performing inspection*

EN 50121 series, *Railway applications – Electromagnetic compatibility*

EN 50121-4, *Railway applications – Electromagnetic compatibility – Part 4: Emission and immunity of the signalling and telecommunications apparatus*

EN 50124-1, *Railway applications – Insulation coordination – Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment*

EN 50125-1, *Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock*

EN 50125-2, *Railway applications – Environmental conditions for equipment – Part 2: Fixed electrical installations*

EN 50125-3, *Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications*

¹⁾ Superseded by EN ISO/IEC 17020:2004, *General criteria for the operation of various types of bodies performing inspection* (ISO/IEC 17020:1998).

EN 50126-1:1999 + corr. May 2006, *Railway Applications – The specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process*

EN 50128, *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*

EN 50155, *Railway applications – Electronic equipment used on rolling stock*

EN 50159-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety related communication in closed transmission systems*

EN 50159-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety related communication in open transmission systems*

EN 61508 series, *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC 61508 series)

EN ISO 9001:2000²⁾, *Quality Management Systems – Requirements* (ISO 9001:2000)

ESA PSS 01-403, *Hazard Analysis and Safety Risk Assessment*

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

The following standard is mentioned as complementary source of information:

EN ISO/IEC 17020 (former EN 45004), *General criteria for the operation of various types of bodies performing inspection* (ISO/IEC 17020)

[REDACTED]

²⁾ Superseded by EN ISO 9001:2008, *Quality management systems – Requirements* (ISO 9001:2008).