

Railway applications — Communication, signalling and processing systems — Hazardous failure rates and Safety Integrity Levels (SIL)

ICS 29.280

National foreword

This Published Document reproduces verbatim CENELEC Report R009-001:1997
The UK participation in its preparation was entrusted by Technical Committee GEL/9, Railway electrotechnical applications, to Subcommittee GEL/9/1, Signalling and communications, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the CENELEC Report title page, pages 2 to 15 and a back cover.

The BSI copyright notice displayed throughout this document indicates when the document was last issued.

This Published Document, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 August 1999

© BSI 08-1999

ISBN 0 580 32859 7

Amendments issued since publication

Amd. No.	Date	Comments

English version

Railway applications
Communication, signalling and processing systems
Hazardous failure rates and Safety Integrity Levels (SIL)

This CENELEC Report has been prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways. It was approved by CENELEC on 1997-03-11.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and 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

© 1997 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. R009-001:1997 E



Documents
Document Sharing Hub

Foreword

This report has been prepared by SC 9XA, Communication, signalling and processing systems, of the Technical Committee TC 9X, Electrical and electronic applications for railways.

It was approved for publication by the CENELEC Technical Board on 1997-03-11.

1 Introduction

This report defines the interpretation and use of Safety Integrity Levels in safety-related electronic systems for railway applications.

The aim is to clarify the concept of Safety Integrity Levels (SIL) through the provision of:

- a methodology for the derivation of the safety process which is described in prEN 50126 standard and based on SIL down to the elementary level in a structured and coherent manner;
- a proposal for the correspondence between SIL and hazardous failure rates.

Figure 1 shows the limits of the ad-hoc group work.

The actual safety requirements (particular safety targets) and the system SIL for each railway application are considered to be the responsibility of the relevant Railway Authority, and are not defined by this document.

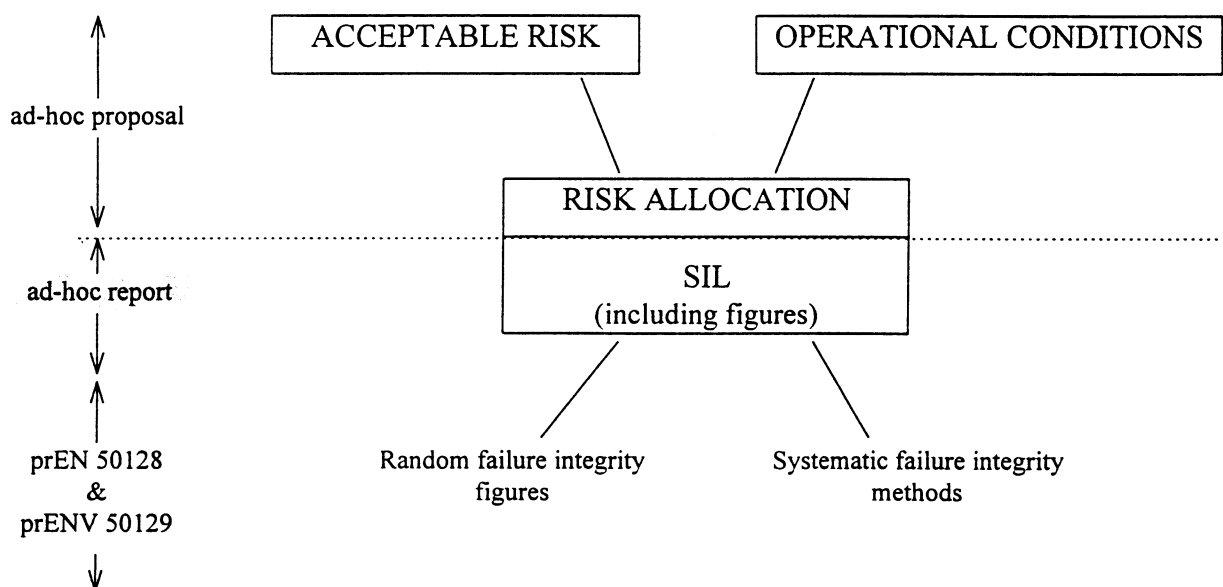


Figure 1: Scope of the ad-hoc group work

2 Safety requirements

The system requirements specification (or sub-system/equipment as appropriate) may be considered in two parts:

- requirements which are not related to safety (including operational functional requirements);
- requirements which are related to safety.

Requirements which are related to safety are usually called safety requirements. These may be contained in a separate safety requirements specification.

Safety requirements may be considered in two parts:

- safety functional requirements;
- safety integrity requirements.

Safety functional requirements are the actual safety-related functions which the system, sub-system or item of equipment is required to carry out.

Safety integrity requirements define the level of safety integrity required for the safety-related functions.

3 Safety integrity

Safety integrity relates to the probability of a safety-related system, sub-system or item of equipment achieving its required safety features. The higher the safety integrity of an item, the lower the probability that it will fail to carry out the required safety functions. An overall quantitative safety integrity requirement may be specified.

Safety integrity is comprised of two components:

- systematic failure integrity;
- random failure integrity.

It is necessary to satisfy both the systematic and the random failure integrity requirements if adequate safety integrity is to be achieved.

In the case of signalling electronic systems, systematic failure integrity is the non quantitative part of the safety integrity and relates to hazardous systematic faults (hardware and software). Systematic faults are caused by human errors in the various stages of the system/sub-system/equipment lifecycle.

EXAMPLE:

- specification errors;
- design errors;
- component deficiencies;
- manufacturing errors;
- installation errors;
- operation errors;
- maintenance errors;
- modification errors.

Systematic failure integrity is achieved by means of the quality management and safety management conditions specified in prENV 50129.

Technical defences against systematic faults are included in the technical safety conditions specified in prENV 50129.

Because it is not possible to assess systematic failure integrity by quantitative methods, Safety Integrity Levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realisation of a system to a stated integrity level.

Random failure integrity is that part of the safety integrity which relates to hazardous random hardware faults. Random hardware faults are the results of the finite reliability of hardware components.

The achievement of random failure integrity is included within the technical safety conditions specified in prENV 50129.

A quantified assessment of random failure integrity should be carried out, by means of probabilistic calculations. These are based on known data for hardware component failure rates and failure modes, and disclosure times of random hardware failures. In the case of components with inherent physical properties (see annex C of prENV 50129) a hazardous failure rate of zero is generally assumed, although a residual risk of hazardous failure may exist and should be defended against as specified in prENV 50129.

4 Safety Integrity Levels

Safety Integrity Level is one of 4 possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.

A SIL should address both quantitative measures of failure rates (random failures) and qualitative appreciation of factors such as quality and safety management (systematic failures). Levels of safety integrity may be described qualitatively as follows:

Safety Integrity Level		Descriptive words (alternatives)	
4	Very high	Vital	Fail-safe
3	High		High integrity
2	Medium	Semi-vital	Medium integrity
1	Low		Low integrity
0	Not specified	Non-vital	Non-safety

The required level of safety integrity for any given application shall be based on the results of hazard analyses and risk assessment, as explained in prEN 50126.

The relationship between Safety Integrity Levels and the quality management, safety management and technical safety conditions, is shown in figure 2. The methodology that will be described is highly recommended as an enabling mechanism for cross-acceptance in Europe.