SLOVENSKI STANDARD
SIST R009-001:1998

01-november-1998

Železniške naprave – Komunikacijski, signalni in procesni sistemi – Nevarne stopnje odpovedi in ravni varnostne integritete (SIL)

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

Ta slovenski standard je istoveten z: R009-001:1997

ICS:

35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST R009-001:1998 en

CENELEC

R009-001

REPORT

July 1997

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

Ref. No. R009-001:1997 E

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.

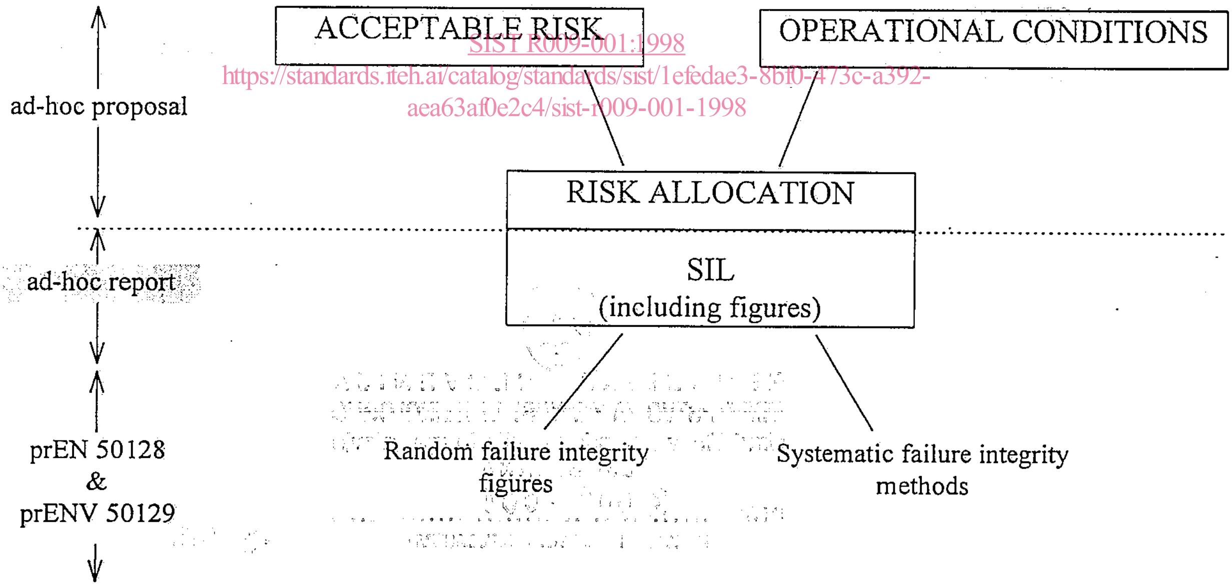


Figure 1: Scope of the ad-hoc group work

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.

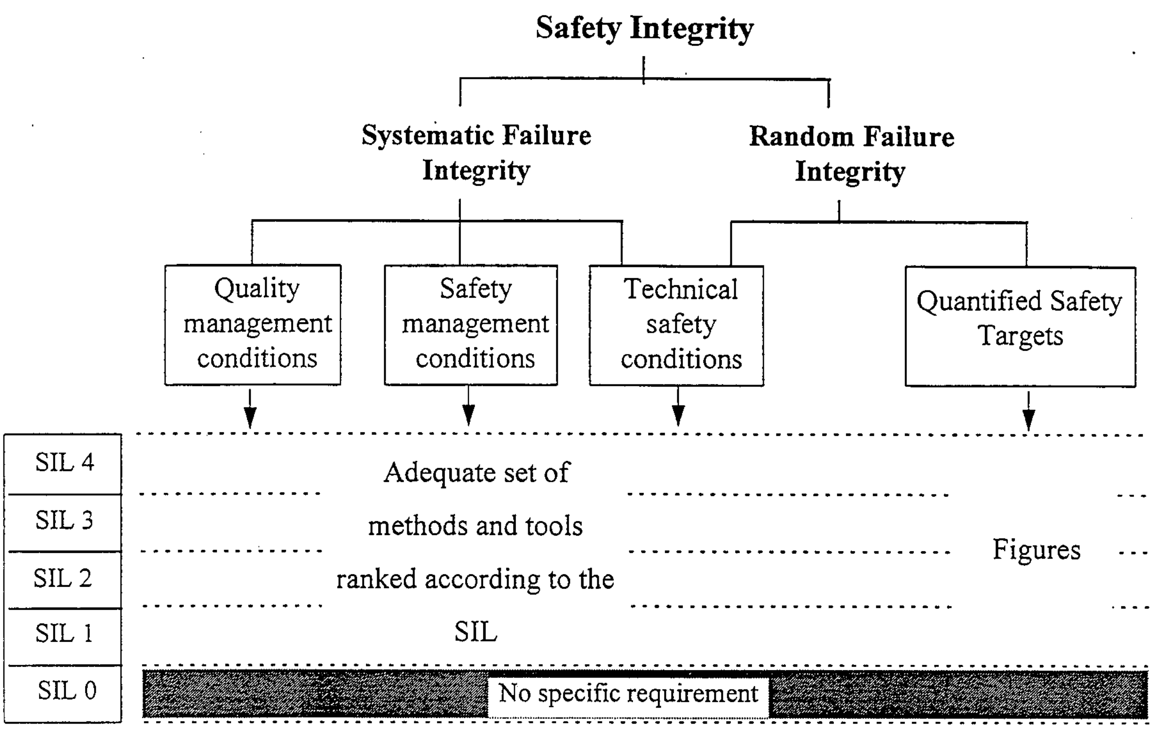

Safety Integrity
Systematic Failure Integrity
Random Failure Integrity
Quality management conditions
Safety management conditions
Technical safety conditions
Quantified Safety Targets
SIL 4
SIL 3
SIL 2
SIL 1
SIL 0
Adequate set of methods and tools ranked according to the SIL
Figures
No specific requirement

Figure 2: Relationship between SILs, figures and techniques

It is important to recognise that achievement of a specified Safety Integrity Level requires compliance with all factors in figure 2, namely:

- quality management conditions;
- safety management conditions;
- technical safety conditions;
- quantified safety target.

Fulfilment of a particular quantified safety target does not mean, by itself, that the corresponding Safety Integrity Level has been achieved. Similarly, fulfilment of the quality management and technical safety conditions associated with a particular Safety Integrity Level does not mean that the corresponding quantified safety target, or the overall safety integrity, have been achieved. All of the factors in figure 2 need to be fulfilled in order to achieve the specified overall safety integrity.

It is also important to understand that, whilst the quantified safety targets in figure 2 are those required in order to achieve the railway safety performance as described in the next paragraphs, it is assumed that the target for a particular safety function can be achieved by a single sub-system or item of equipment. As explained in 5.3 of this document, the claim limits for a quantified safety target shall be achieved by combination of functions, sub-system or items of equipment.

5 Methodology for determining the SIL

5.1 Safety management process

Standard prEN 50126 defines a safety management process for a system. This is based on a lifecycle and a top-down approach to safety requirements derivation and allocation.

Such an allocation leads to a specific design, based on a particular architecture and specific system elements. A risk analysis on this design is aimed at allocating finally to each system element a safety target and/or a SIL compliant with the safety integrity requirements of the safety functions that it is supposed to perform.

Risk reduction process is used in order to reduce the intrinsic risk of dangerous events caused by a system element to an acceptable level of safety. This iterative process leads to the modification (or the confirmation) of the previous SIL in order to enable a final SIL to be demonstrated for the system element. This demonstration should be based on prEN 50128 and prENV 50129.

The description of this safety management process is summed up in figure 3.

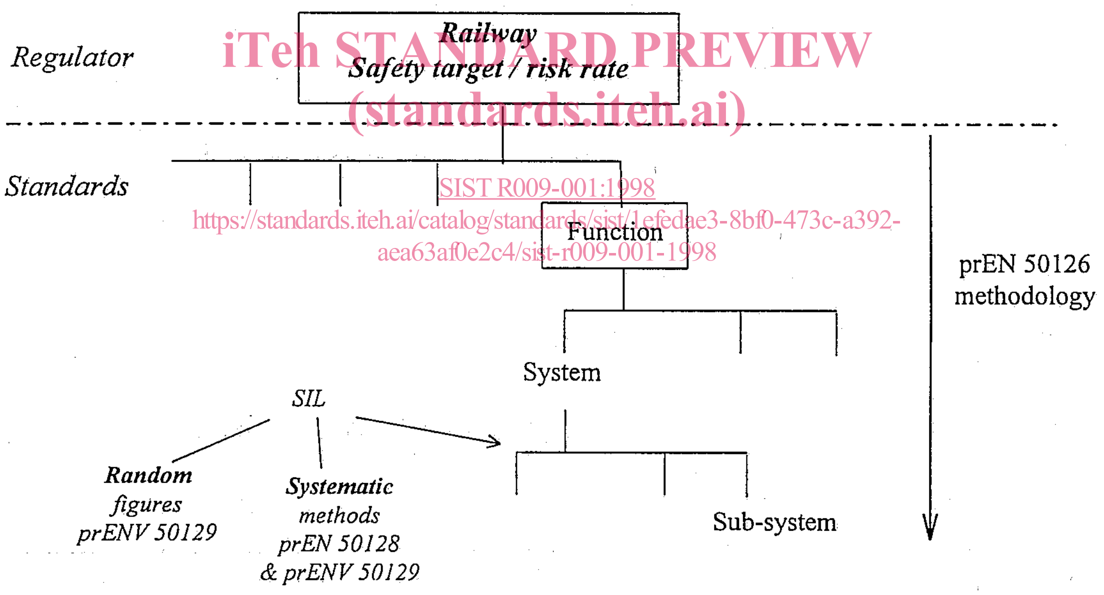


Figure 3: Safety management (as described in standards)

Thus, the SIL represents the bridge between a top-down methodology for the apportionment of the system safety requirements (design phases) and a bottom-up methodology for the realisation of an equipment (realisation phases) as shown in figure 4. Once a SIL has been demonstrated and an equipment certified, it is no more necessary to demonstrate this SIL for an other system, unless the safety requirements (functional and/or integrity) are different for the new application.

This boundary is not clear and distinct: it is better instead to speak of a zone which would be common to both methodologies; in fact, it is up to specialists to establish the adequate level of SIL applicability.

As the process of allocation of SIL is intended to enable cross-acceptance of equipment, the basic unit, that we shall call "element" in this paper, is *de facto* generic: the element is necessarily a stand-alone equipment which performs one or more simple functions and which can be replaced by an other one performing the same function(s).

Generally speaking, such an element is often the lowest level equipment that can be replaced during a first level corrective maintenance operation.

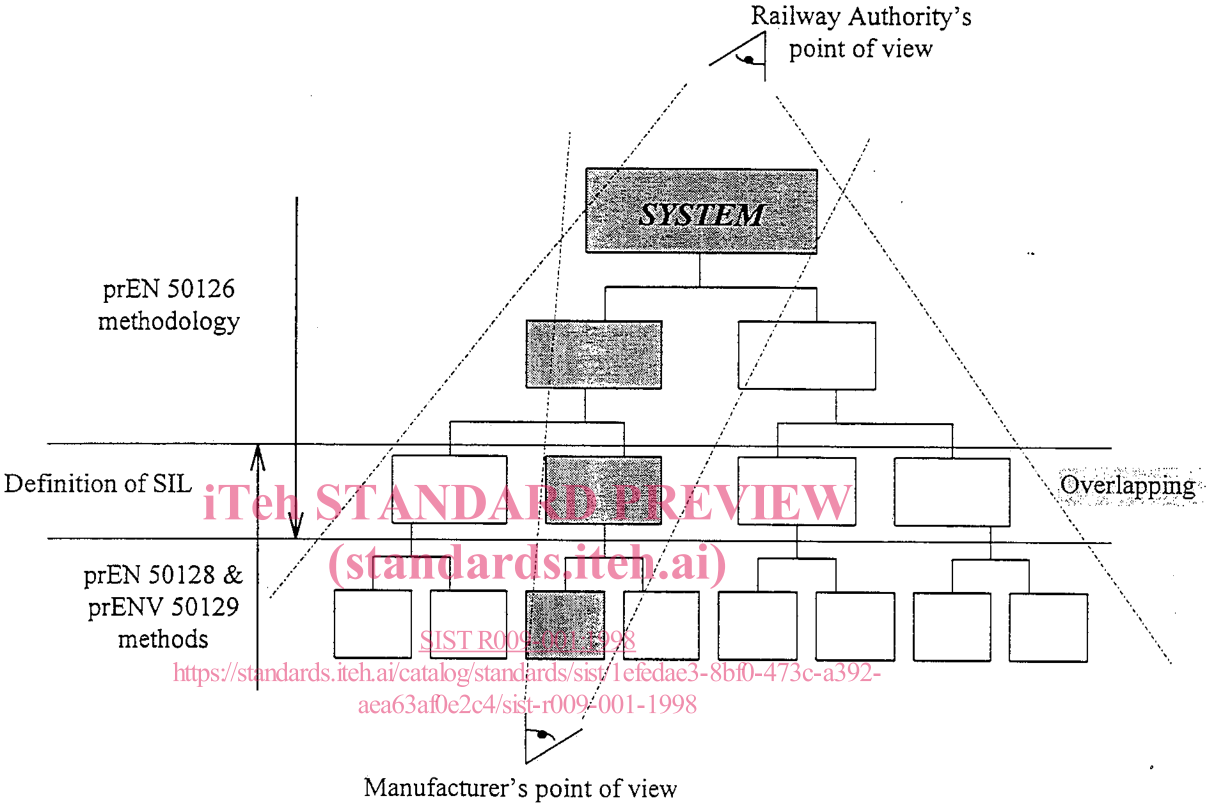
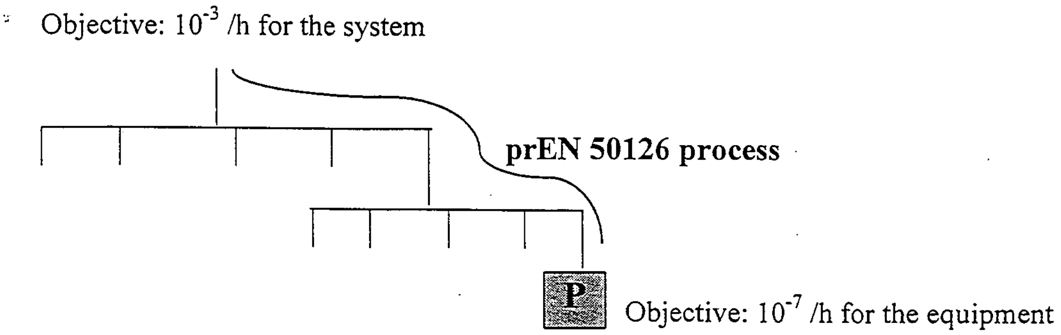

Railway Authority's point of view
SYSTEM
prEN 50126 methodology
Definition of SIL
Overlapping
prEN 50128 & prENV 50129 methods
Manufacturer's point of view

Figure 4: Sil viewpoints

5.2 Examples

One seeks to develop a railway system. The safety target for the overall system is, for example, 10^{-3} hazardous failures per hour.

Using the prEN 50126 process, a risk analysis is carried on, first risk reductions are performed and, at the end, an objective of 10^{-7} per hour is apportioned to the safety function F performed by the particular electronic equipment P.


Objective: 10^{-3} /h for the system
prEN 50126 process
P
Objective: 10^{-7} /h for the equipment