SLOVENSKI STANDARD

SIST R009-004:2002

01-marec-2002

Železniške naprave – Sistemska razporeditev zahtev varnostne integritete

Railway applications - Systematic allocation of safety integrity requirements

Ta slovenski standard je istoveten z: R009-004:2001

ICS:

45.020	Železniška tehnika na splošno	Railway engineering in general

SIST R009-004:2002 **en**

CENELEC **R009-004**

REPORT June 2001

English version

Railway applications
Systematic allocation of safety integrity requirements

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 SC9XA on 1999-10-05 and endorsed by the CENELEC Technical Board on 2000-04-01.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, 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. R009-004:2001 E

Foreword

This CENELEC Report was 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 SC9XA on 1999-10-05 and endorsed by the CENELEC Technical Board on 2000-04-01.

Annexes designated "informative" are given for information only.

Content

Executive summary

This report presents a systematic methodology to determine safety integrity requirements for railway signalling equipment, taking into account the operational environment and the architectural design of the signalling system.

At the heart of this approach is a well defined interface between the operational environment and the signalling system. From the safety point of view this interface is defined by a list of hazards and tolerable hazard rates associated with the system. It should be noted that the purpose of this approach is not to limit co-operation between suppliers and railway authorities but to clarify responsibilities and interfaces.

It is the task (summarized by the term Risk Analysis) of the Railway Authority

- to define the requirements of the railway system (independent of the technical realisation);
- to identify the hazards relevant to the system;
- to derive the tolerable hazard rates, and
- to ensure that the resulting risk is tolerable (with respect to the appropriate risk tolerability criteria).

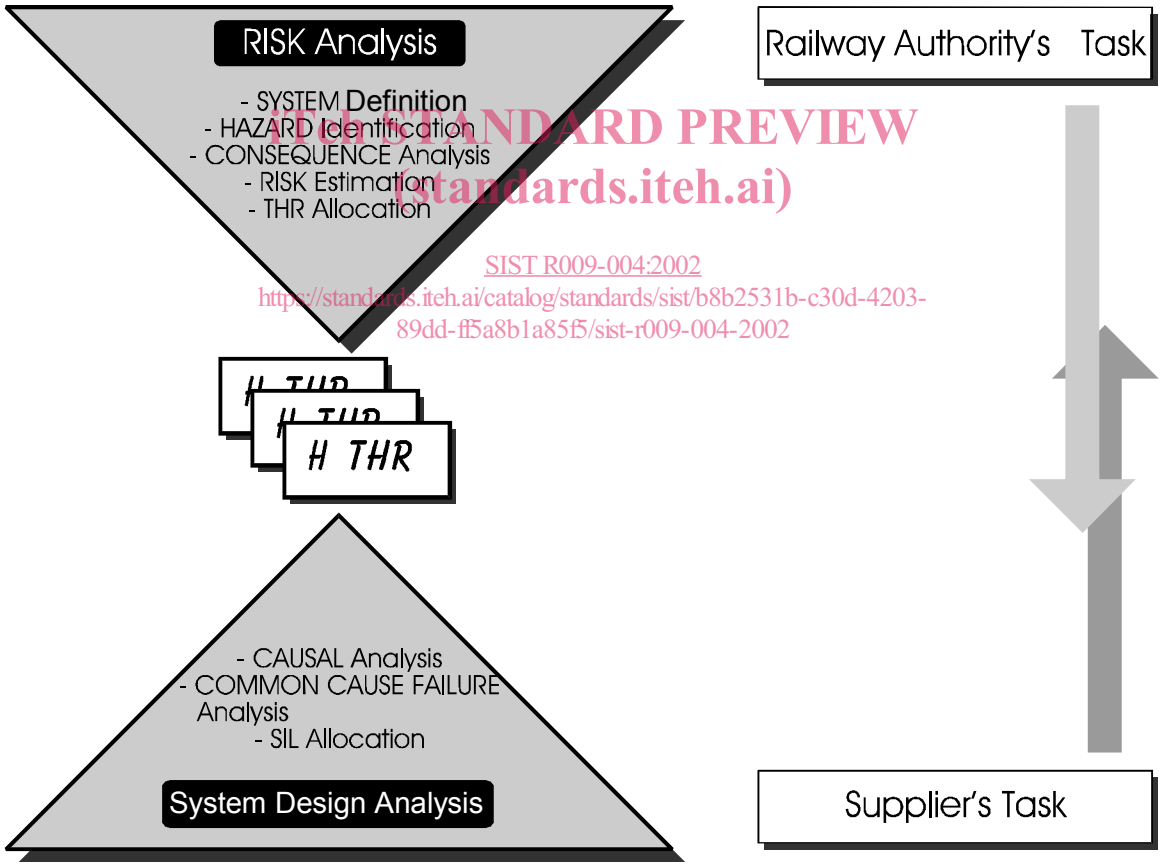

Figure 0.1 - Global process overview

The only requirement is that the tolerable hazard rates must be derived taking into account the risk tolerability criteria. Risk tolerability criteria are not defined by this report, but depend on national or European legislative requirements.

Among the risk analysis methods two are proposed in order to estimate the individual risk explicitly, one more qualitative, the other more quantitative. Other methods, similar to the GAMAB principle, do not explicitly determine the resulting risks, but derive the tolerable hazard rates from comparison with the performance of existing systems, either by statistical or analytical methods. Alternative qualitative approaches are acceptable, if as a result they define a list of hazards and corresponding THR. The specification of the system requirements comprising performance and safety (THR) terminates the Railway Authority's task.

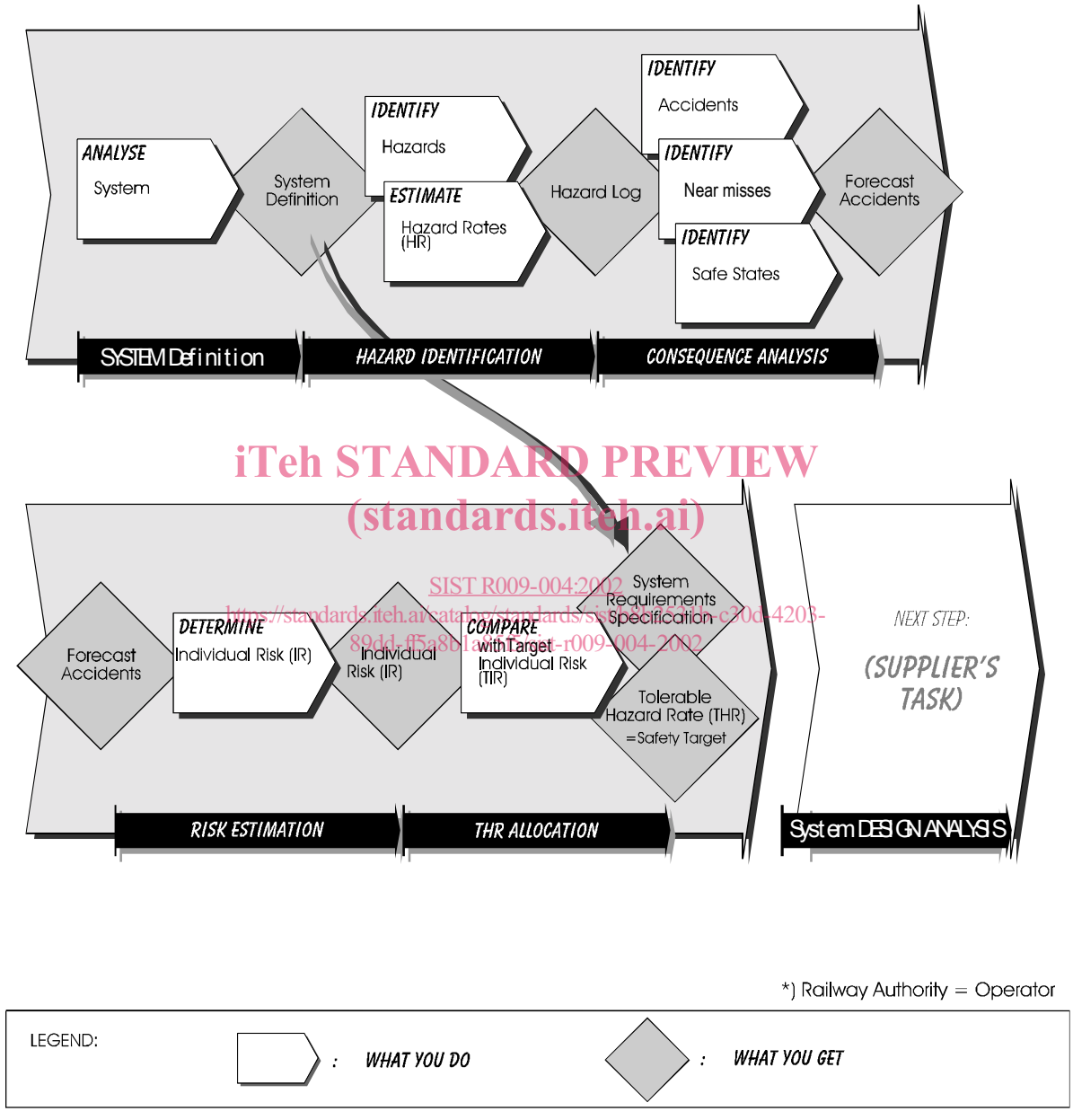

Figure 0.2 - Example Risk Analysis process

The supplier's task (summarized by the term System Design Analysis) comprises

- definition of the system architecture;
- analysis of the causes leading to each hazard;
- determination of the safety integrity requirements (SIL and hazard rates) for the subsystems;
- determination of the reliability requirements for the equipment.

Causal analysis constitutes two key stages. In the first phase the tolerable hazard rate for each hazard is apportioned to a functional level. Safety Integrity Levels (SIL) are defined at this functional level for the subsystems implementing the functionality. The hazard rate for a subsystem is then translated to a SIL using the SIL table.

During the second phase the hazard rates for subsystems are further apportioned leading to failure rates for the equipment, but at this physical implementation level the SIL remains unchanged. Consequently also the software SIL defined by EN 50128 would be the same as the subsystem SIL but for the exceptions described in EN 50128.

The apportionment process may be performed by any method which allows a suitable representation of the combination logic, e.g. reliability block diagrams, fault trees, binary decision diagrams, Markov models etc. In any case particular care must be taken when independence of items is required. While in the first phase of the causal analysis functional independence is required, physical independence is sufficient in the second phase. Assumptions made in the causal analysis must be checked and may lead to safety-relevant application rules for the implementation.

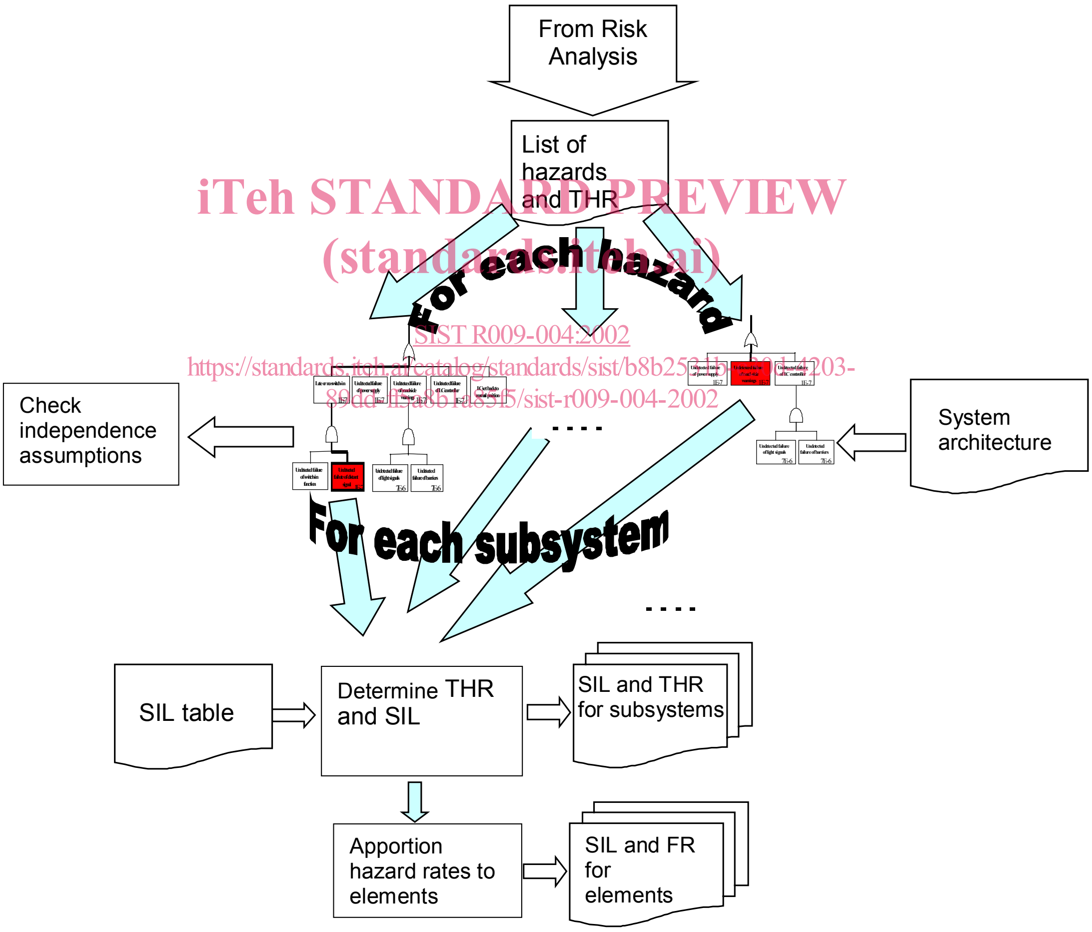

Figure 0.3 - Example System Design Analysis process

Both, the risk analysis and the system design analysis, have to be approved by the Railway Safety Authority.

However whilst the risk analysis may be carried out once at the railway level, the system design analysis must be performed for every new architecture. It is prudent to review the risk analysis and system design analysis when safety related changes are introduced.

Introduction

Historically the interoperability of European railways was not only hindered by incompatible technology but also by different approaches towards safety. The common European market is the main driving force behind the harmonisation of the different safety cultures. In a joint pan-European effort comprehensive safety standards have been established for railway signalling by the European electrotechnical standardisation committee CENELEC:

- EN 50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

- EN 50128: Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

- ENV 50129: Railway applications - Safety related electronic systems for signalling

These CENELEC standards assume that safety relies both on adequate measures to prevent or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failure should be balanced in order to achieve the optimum safety performance of a system. To achieve this the concept of Safety Integrity Levels (SIL) is used. SILs are used as a means of creating balance between measures to prevent systematic and random failures, as it is agreed within CENELEC that it is not feasible to quantify systematic integrity.

A shortcoming of the CENELEC standards as of today is (similar as in other related standards like IEC 61508 [IEC] or ISA S84.01 [ISA]) that while the guidance on how to fulfil a particular SIL is quite comprehensive the process and rules to derive SILs for system elements from system safety targets or the tolerable system risk are not adequately covered. A general convincing solution to this problem is still an open research problem, see [LM][ZD][YB2][GAM] for some divergent examples. However in order to achieve cross-acceptance of safety cases and products for railway signalling applications it is necessary to fill the gap.

This has been realized by SC9XA in 1997 and consequently a working group has been set up in March 1998 in order to find a joint harmonized approach at least for railway signalling applications.

Although the major driving forces behind this work were novel signalling applications which are required to be interoperable throughout Europe, the scope and applicability of the approach presented in this report should not be limited to signalling or interoperable applications.

1 Scope

The scope of this report is to define a method to determine the required Safety Integrity Level of railway signalling equipment taking in consideration

- the operational conditions of the railway and
- the architecture of the signalling system.

The following picture may be used in order to detail more precisely the scope of this report:

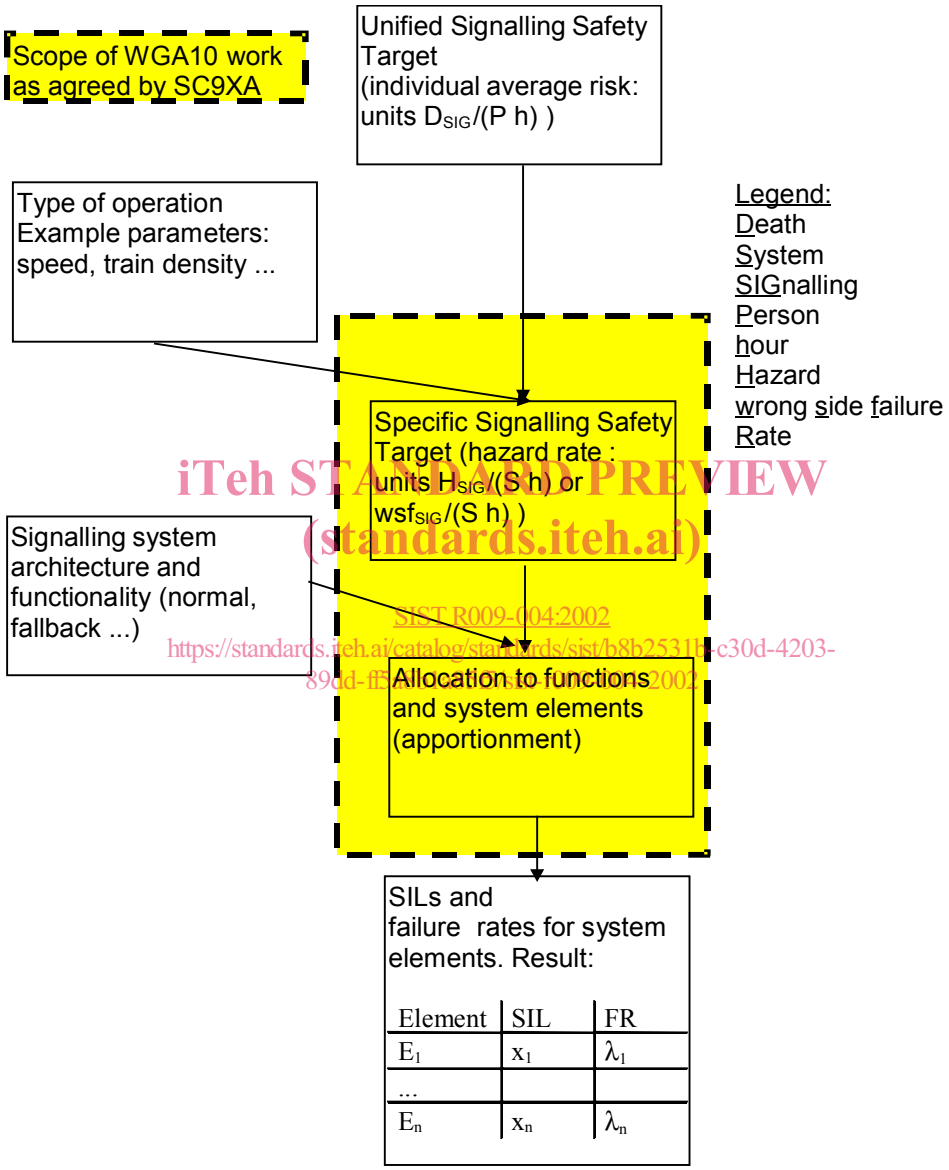

Figure 1.1 - Scope of WGA10

From a mechanistic point of view the task of this report is to define a method of calculation, which determines the integrity requirements (qualitatively and quantitatively) from the inputs stated above.

2 References

This CENELEC Report incorporates by dated or undated references, provisions from other publications. These references are cited at the appropriate place in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Report only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

2.1 Supporting standards

[126] Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), EN 50126:1999

[128] Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems, EN 50128:2001

[129] Railway applications - Safety related electronic systems for signalling, ENV 50129:1998

2.2 Informative references

[0056] UK Ministry of Defence, Safety Management Requirements for Defence Systems, Def Stan 00-56

[GAM] CASCADE: Generalised Assessment Method <GAM>, Part II: Guidelines, ESPRIT 9032 report, ref. CAS/IC/MK/D2.3.2/V3, 1996

[HK] Kumamotu, H. and Henley, E.: Probabilistic risk assessment and management for engineers and scientists, IEEE Press, 1996

[IEC] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508 series

[ISA] ISA: Application of Safety Instrumented Systems for the Process Industries, ISA S84.01, February 1996

[ISO] ISO/IEC: Information technology - System and software integrity levels, ISO/IEC 15026

[Lev95] Leveson, N. G.: Safeware - System safety and computers, Addison-Wesley, 1995

[LM] Lindsay, P. A. and McDermid, J. A.: A systematic approach to software safety integrity levels, in: Peter Daniel (Ed.): SAFECOMP'97 , Springer Verlag, 1997, 70-82

[R01] Railway applications - Communication, signalling and processing systems - Hazardous failure rates and Safety Integrity Levels (SIL), R009-001:1997

[RSH] Railway Signalling Hazards, Swedish National Rail Administration, Technical Report 1999:1

[SAH] System Safety Analysis Handbook, 2nd edition, System Safety Society, 1998

[VIL] Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment, Volume 1: Methods and Techniques, Wiley, 1992

[YB2] Engineering Safety Management System, Issue 2.0, "Yellow Book", Railtrack, 1997

[ZD] Zerkani, H. and Dumolo, D.: System Safety Lifecycle Based on IEC 61508 and its Use for Railway Applications, Proc. 16th International System Safety Conference, Sept. 14-19, 1998, Seattle

3 Definitions

For the purpose of this report, the following definitions apply. For terms not defined here, the following references should be consulted in order of priority:

- IEC 60050(191): International Electrotechnical Vocabulary (Chapter 191, dependability and quality of service);
- ISO 8402: Quality Vocabulary;
- ISO/IEC 2382: Information Technology Vocabulary.

accident
an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage (ENV 50129)

apportionment
a process whereby the RAMS elements for a system are sub-divided between the various items which comprise the system to provide individual targets (EN 50126)

can
is possible (ENV50129)

causal analysis
analysis of the reasons how and why a particular hazard may come into existence

collective risk
a risk which is related to a group of people

common cause failure
a failure which is the result of an event(s) which causes a coincidence of failure states of two or more components leading to a system failing to perform its required function (EN 50126)

common-mode fault
fault common to items which are intended to be independent (ENV 50129)

consequence analysis
analysis of events which are likely to happen after a hazard has occurred

cross-acceptance
the status achieved by a product that has been accepted by one Authority to the relevant European Standards and is acceptable to other Authorities without the necessity for further assessment (ENV 50129)

dependent failure
the failure of a set of events; the probability of which cannot be expressed as the simple product of the unconditional probabilities of the individual events (EN 50126)

diversity
a means of achieving all or part of the specified requirements in more than one independent and dissimilar manner (ENV 50129)

element
a part of a product that has been determined to be a basic unit or building block. An element may be simple or complex (ENV 50129)

environment
the surrounding objects or region or circumstances which may influence the behaviour of the system and or may be influenced by the system (ENV 50121-5)

equipment
a functional physical item (ENV 50129)

error
a deviation from the intended design which could result in unintended system behaviour or failure (ENV 50129)

failure
a deviation from the specified performance of a system. A failure is the consequence of an fault or error in a system (ENV 50129)

failure cause
the circumstances during design; manufacture or use which have led to a failure (EN 50126, IEC)

failure mode
the predicted or observed results of a failure cause on a stated item in relation to the operating conditions at the time of the failure (EN 50126, IEC)

failure rate
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) and the length of this interval; (t; when (t tends towards zero; given that the item is in an up state at the start of the time interval (EN 50126, IEC)

fault
an abnormal condition that could lead to an error in a system. A fault can be random or systematic (EN 50126, IEC)

fault detection time
time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected (ENV 50129)

fault mode
one of the possible states of a faulty product for a given required function (EN 50126, IEC)

fault tree analysis
an analysis to determine which fault modes of the product; sub-products or external events; or combinations thereof; may result in a stated fault mode of the product; presented in the form of a fault tree (EN 50126, IEC)

FMEA
an acronym meaning Failure Modes and Effects Analysis. A qualitative method of reliability analysis which involves the study of the fault modes which can exist in every sub-product of the product and the determination of the effects of each fault mode on other sub-products of the product and on the required functions of the product (EN 50126, IEC)

function
a mode of action or activity by which a product fulfils its purpose (EN 50126, IEC)

hazard
an object, condition or state that could lead to an accident [YB2].In the context of a system safety, a hazard is an unprotected state of the system, which under certain external conditions leads to an accident

hazard identification
the process used to define potential hazards related to a system

hazard log
the document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced (EN 50126, IEC)

human error
a human action (mistake), which can result in unintended system behaviour/failure (ENV 50129)

independence (functional)
two items are functionally independent, if they do not have any common cause failures, neither systematic nor random

independence (physical)
two items are physically independent, if they do not have any random common cause failures

independence (technical)
freedom from any mechanism which can affect the correct operation of more than one item (ENV 50129)

individual risk
a risk which is related to a single individual only

item
element under consideration (ENV 50129)

loss analysis
analysis of safety, environmental or economical harm or damage

may
is permissible (ENV 50129)

negation
enforcement of a safe state following detection of a hazardous fault (ENV 50129)

negation time
time span which begins when the existence of a fault is detected and ends when a safe state is enforced (ENV 50129)

product
a collection of elements, interconnected to form a system, subsystem or item of equipment, in a manner which meets the specified requirements (ENV 50129)

railway authority
the body with the overall accountability to a Regulator for operating a railway system (EN 50126, IEC)

RAMS
an acronym meaning a combination of Reliability; Availability; Maintainability and Safety (EN 50126, IEC)

random failure integrity
the degree to which a system is free from hazardous random faults (ENV 50129)

random fault
the occurrence of a fault based on probability theory and previous performance (ENV 50129)