

Railway specifications — Systematic allocation of safety integrity requirements

The European Standard R009-004:2001 has the status of a
British Standard

ICS 45.020

National foreword

This Published Document is the official English language version of R009-004:2001.

The UK participation in its preparation was entrusted by Technical Committee GEL/9, Railway electrotechnical applications, to Subcommittee GEL/9/1, Signalling and Communication, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/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.

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

Cross-references

The British Standards which implement these international or European publications 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.

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 2001

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 111 and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 07-2001

ISBN 0 580 38174 9

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

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

Introduction	8
1 Scope	9
2 References	10
2.1 Supporting standards	10
2.2 Informative references	10
3 Definitions	10
4 Symbols and abbreviations	16
5 Safety Integrity Levels allocation framework	17
5.1 Prerequisites	17
5.2 Overview of the methodology	17
5.3 Definition of Safety Integrity Levels	21
5.4 Qualitative vs. quantitative methods	22
5.4.1 <i>Qualitative Assessment</i>	22
5.4.2 <i>Quantitative Assessment</i>	23
5.5 EN 50126 lifecycle context	24
6 System definition	26
7 Hazard identification	27
7.1 General principles	27
7.2 Empirical hazard identification methods	29
7.3 Creative hazard identification methods	29
7.4 Hazard ranking	30
7.5 Existing hazard lists	30
8 Risk analysis	30
8.1 Risk tolerability	30
8.2 Determination of Tolerable Hazard Rate	31
8.2.1 <i>Qualitative Risk Analysis</i>	31
8.2.2 <i>Quantitative risk analysis</i>	33
8.2.3 <i>GAMAB and similar approaches</i>	39
8.2.4 <i>The MEM approach</i>	40
8.2.4 <i>Other approaches</i>	41

9 System design analysis 41

9.1 Apportionment of safety integrity requirements to functions 42

9.1.1 *Physical independence* 43

9.1.2 *Functional Independence* 44

9.1.3 *Process independence*..... 45

9.2 Use of SIL tables 45

9.3 Identification and treatment of new hazards arising from design 46

9.4 Determination of function and subsystem SIL..... 48

9.5 Determination of safety integrity requirements for system elements 49

Annex A Single-line signalling system example 51

Annex B Level crossing example..... 71

Annex C Comparison of demand and continuous mode 83

Annex D Proposed changes for annex A of ENV 50129 97

Annex E Frequently asked questions 111

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).

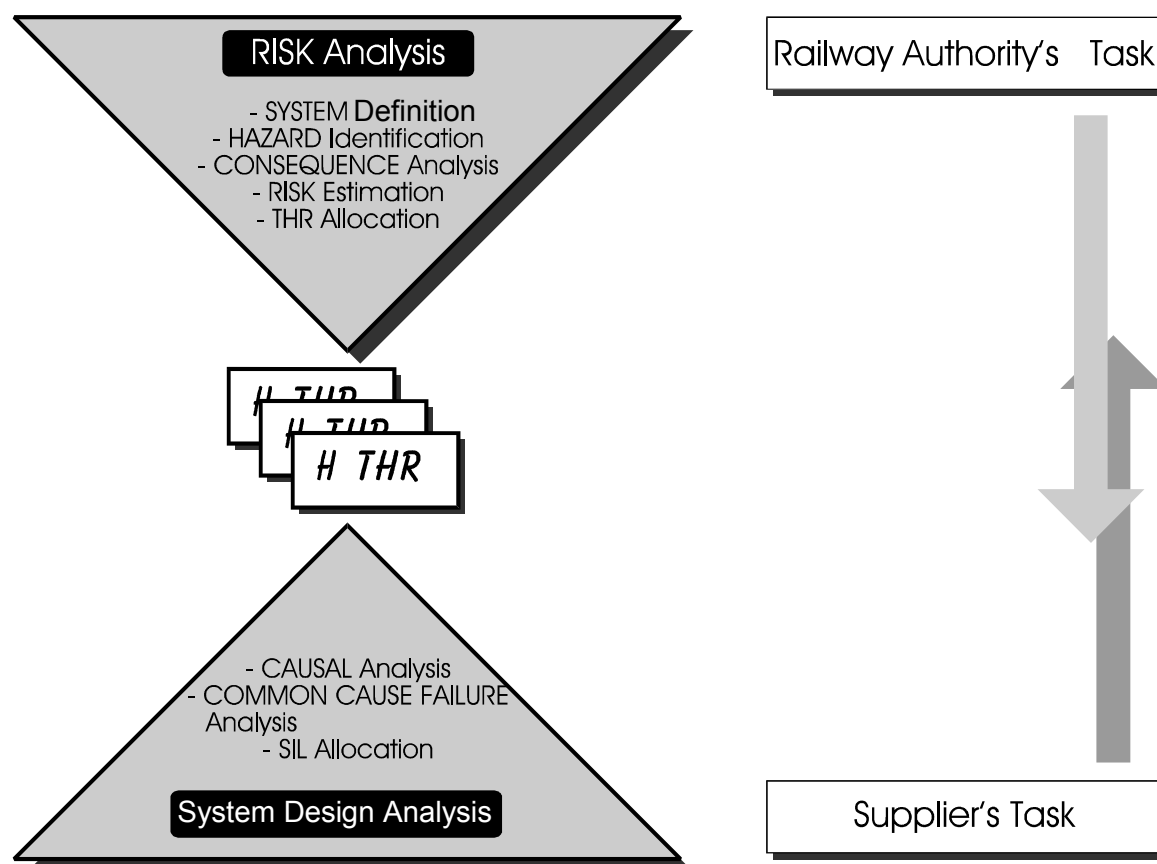


Figure 0.1 - Global process overview

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.

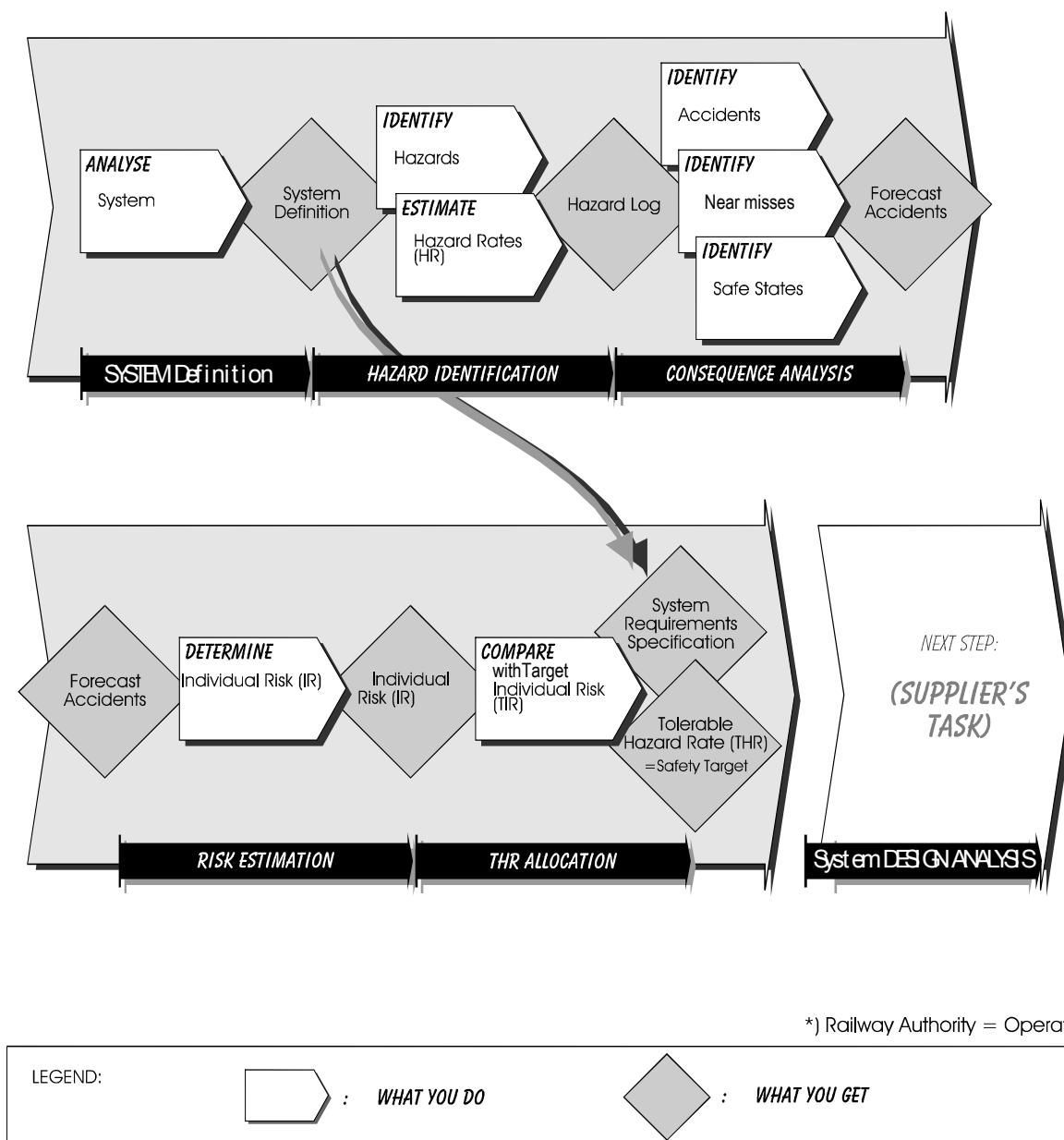


Figure 0.2 - Example Risk Analysis process

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.

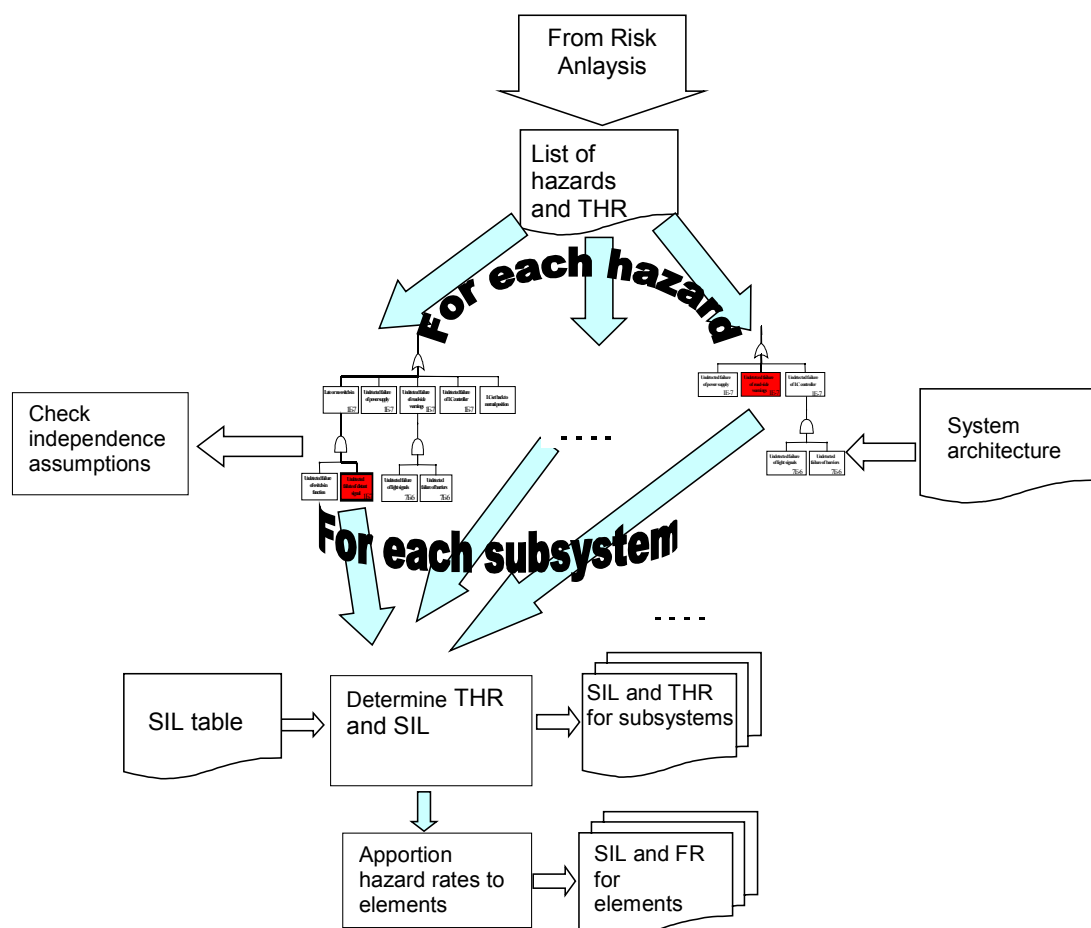


Figure 0.3 - Example System Design Analysis process

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:

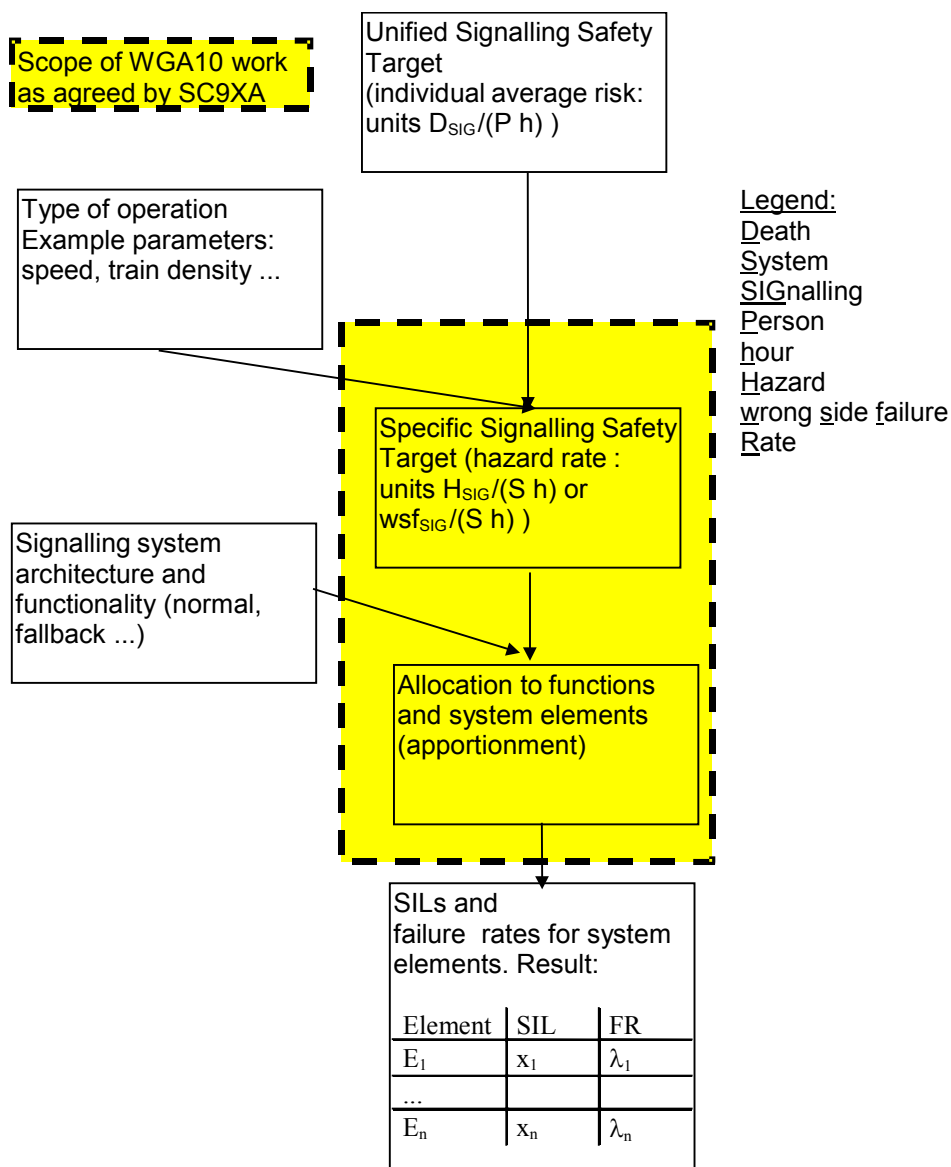


Figure 1.1 - Scope of WGA10

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 a 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)

random hardware failures

failures; occurring at random times; which result from a variety of degradation mechanisms in the hardware (EN 50126, IEC)

redundancy

the provision of one or more additional elements, usually identical, to achieve or maintain availability under the failure of one or more of those elements. (ENV 50129)

reliability

the probability that an item can perform a required function under given conditions for a given time interval (t_1 ; t_2) (EN 50126, IEC)

risk

likelihood of an event occurring and its consequences

Risk Analysis

systematic use of available information to estimate the likelihood and consequences of hazards

risk assessment

overall process of risk analysis and risk evaluation

risk aversion

the ambivalent attitude of society towards catastrophic outcomes. This may be taken into account by additional risk aversion factors, which give a weight to avoidance of catastrophic outcomes

risk reduction

a process of selection and implementation of options that is applied to reduce either the likelihood or consequences, or both, of a particular risk

safe state

a condition which continues to preserve safety (ENV 50129)

safety

freedom from unacceptable levels of risk (ENV 50129)

safety authority

the body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements (ENV 50129)

safety case

the documented demonstration that the product complies with the specified safety requirements (ENV 50129)

safety integrity

the likelihood of a safety-related system achieving its required safety features under all the stated conditions within a stated operational environment and within a stated period of time (ENV 50129)

(system) safety integrity level

a number which indicates the required degree of confidence that a system will meet its specified safety features (ENV 50129)

safety life-cycle

the additional series of activities carried out in conjunction with the system life-cycle for safety-related systems (ENV 50129)

safety loss

the measure of injury and fatality arising from an accident

safety process

the series of procedures that are followed to enable all safety requirements of a product to be identified and met (ENV 50129)

safety requirements

the requirements of the safety functions that have to be performed by the safety related systems; comprising safety functional requirements and safety integrity requirements . (EN 50126, IEC)

safety target

in the context of this report the safety target relates to a tolerable hazard rate derived by the Railway Authority by risk analysis

shall

is mandatory (ENV 50129)

should

is recommended (ENV 50129)

signalling system

particular kind of system used on a railway to control and protect the operation of trains (ENV 50129)

SIL table

a set of allocations between the values of safety integrity levels and the corresponding bands of tolerable hazard rates (= safety target)

Software Safety Integrity Level

a classification number which determines the techniques and measures that have to be applied in order to reduce residual software faults to an appropriate level (EN 50128)

system

a set of subsystems or elements which interact according to a design (ENV 50129)

NOTE The system is a matter of perspective. It is not a fixed term, but can be defined arbitrarily.

system design analysis

the process of analysing the causes of hazards and of identification of requirements to limit the likelihood of hazards to a tolerable level. "System Design Analysis" should better be called "System Hazard Analysis" or similar. But this definition would be contradictory to the EN 50126 definition of hazard analysis

system function

a system manifests a emergent property, which is not necessarily inherent in its constituent parts

system life-cycle

the activities occurring during a period of time that starts when a system is conceived and ends when the system is no longer available for use (EN 50126, IEC)

systematic failure

failure due to errors in any safety lifecycle activity; within any phase; which cause it to fail under some particular combination of inputs or under some particular environmental condition (EN 50126, IEC)

systematic failure integrity

the degree to which a system is free from unidentified hazardous errors and the causes thereof (ENV 50129)

systematic fault

an inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment (ENV 50129)

target individual risk

an individual risk which is tolerated by society

tolerable hazard rate

a hazard rate which guarantees that the resulting risk does not exceed a target individual risk

tolerable risk

the maximum level of risk of a product that is acceptable to the Railway Authority (EN 50126, IEC)

4 Symbols and abbreviations

A_k	accident type k
ALARP	as low as reasonably practicable
C_j^k	consequence probability (for hazard j leading to accident k)
CCA	cause consequence analysis
CCF	common cause failure
D_j	duration of hazard j
DR	detection rate
E_{ij}	exposure of individual i to hazard j
F_i^k	probability of fatality for individual i in accident type k
FR	failure rate
GAMAB	globalement au moins aussi bon
HR	hazard rate
IRF	individual risk of fatality
LC	level crossing
MEM	minimum endogenous mortality
MTBF	mean time between failure
N	number of uses
N_P	number of people in a population
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
S_k	severity of accident type k
T	periodic testing time
THR	tolerable hazard rate
TIR	target individual risk

5 Safety Integrity Levels allocation framework

5.1 Prerequisites

The report does not define any safety targets for signalling systems or system elements. It gives a generic methodology, therefore all numerical values shall be seen only as illustrative and may not be relied upon.

This methodology does not deal with safety acceptance or risk tolerability.

Note that the definition and usage of the SIL table is different from the current ENV 50129 [129]. The explanation is given in 9.2.

This report deals with system SILs as utilized by ENV 50129, not with software SILs as defined by EN 50128. Guidance on software SILs can be found in EN 50128 only.

Some definitions, mainly from ENV 50129, have been changed or extended. Refer to clause 3.

5.2 Overview of the methodology

This subclause is intended to give a bird's eye perspective of the methodology. It can not explain all details, which are worked out in the following sections. Major aspects of the methodology are highlighted.

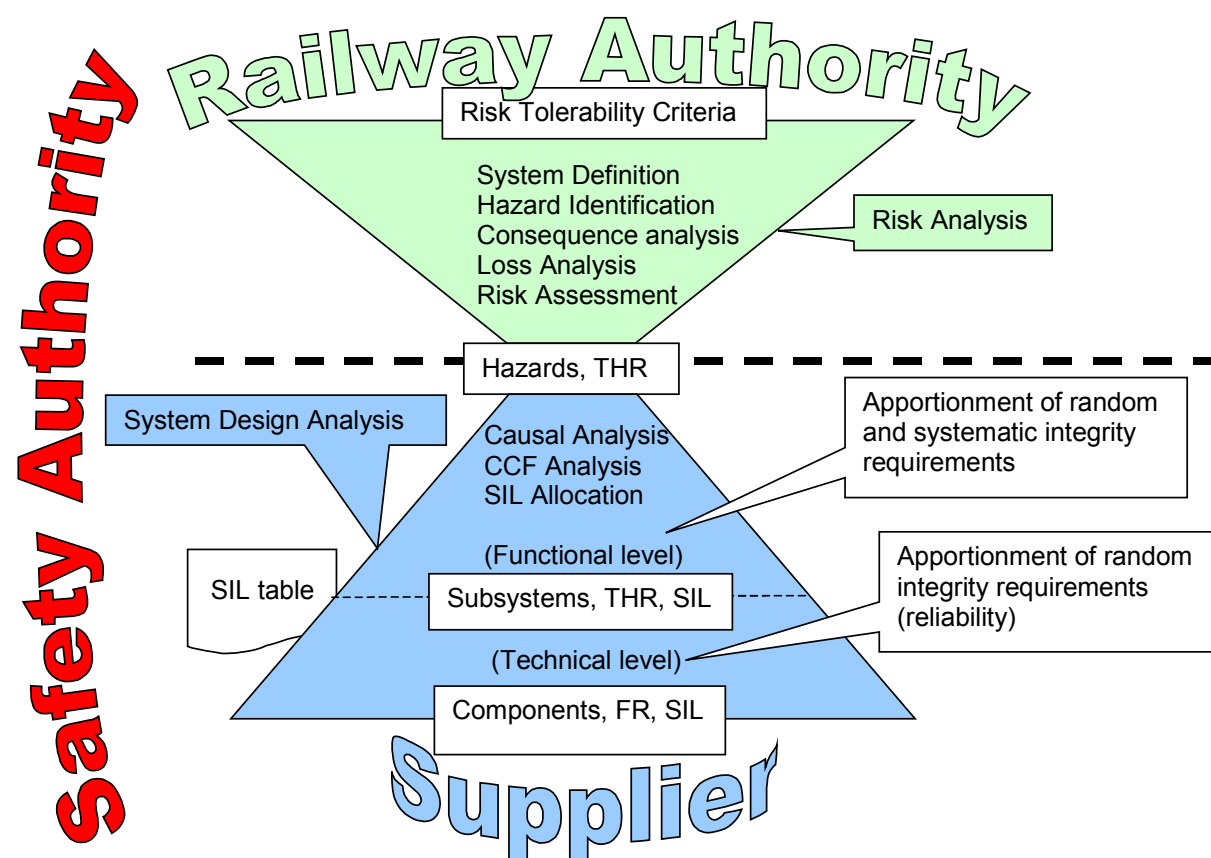


Figure 5.1 - Process overview

The general steps of the methodology can be summarized as follows (see Figure 5.1):

- 1) Define the system adequately.
- 2) Identify key operational hazards.
- 3) Determine the tolerable hazard rate THR_i for each hazard by analysing the consequences of the hazards (taking into account the operational parameters).
- 4) For each hazard: Analyse the causes down to a functional level taking into account system definition and architecture.
- 5) Decide which function(s) are implemented by which subsystem.
For each subsystem:
 - collect contributions of each function, which is realized by the subsystem, to all hazards;
 - calculate overall tolerable hazard rate THR_s for the subsystem;
 - translate THR_s into a safety integrity level SIL_s for the subsystem using a SIL table;
 - determine failure rates for the system elements to meet THR_s for the subsystem.

Note that this approach inherently divides the world into railway operation (the “real” world, for which the railway authority is responsible) and the technical solutions (the “technical” world, for which the supplier of signalling equipment is responsible). The natural border between these is defined by essential functions, the failure of which constitutes the hazards. These may have consequences (accidents in the worst case) and causes. Thus the approach defines a natural interface between railway authorities and suppliers. A different top-level perspective is given in Figure 5.2, which shows the flow of activities for a top-down application of the methodology and the relation to some major input and output documents.



© BSI 08-2001

In particular step 3 and steps 4/5 can be further subdivided to show more details. Here dotted lines depict optional steps.

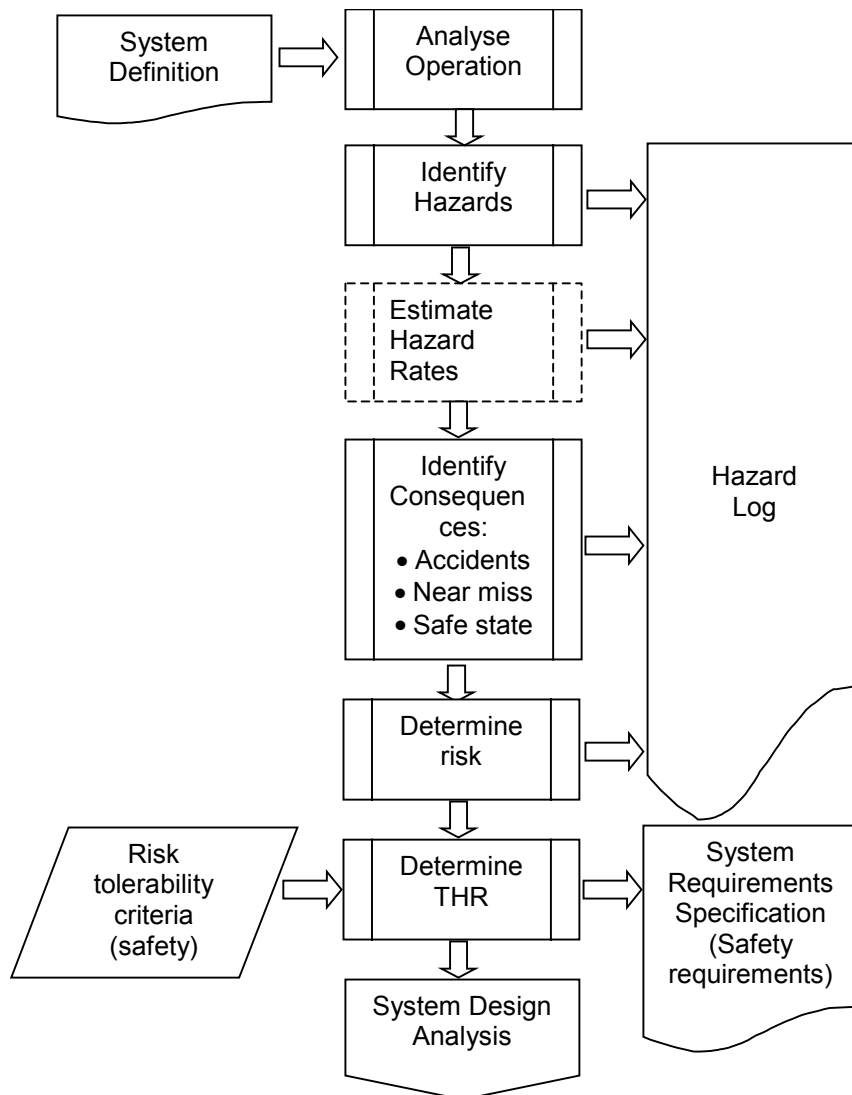


Figure 5.3 - Process details of Risk Analysis (steps 1-3) in flowchart notation

Note that the methodology is generic and may be tailored to the user's needs. For example if the railway authority or the supplier has ways to define the THR by other means then only a part of the methodology may be applied. In particular the THR may be derived from arguments like GAMAB by operational and performance statistics (instead of consequence analysis) or by system design analysis of equipment in use.

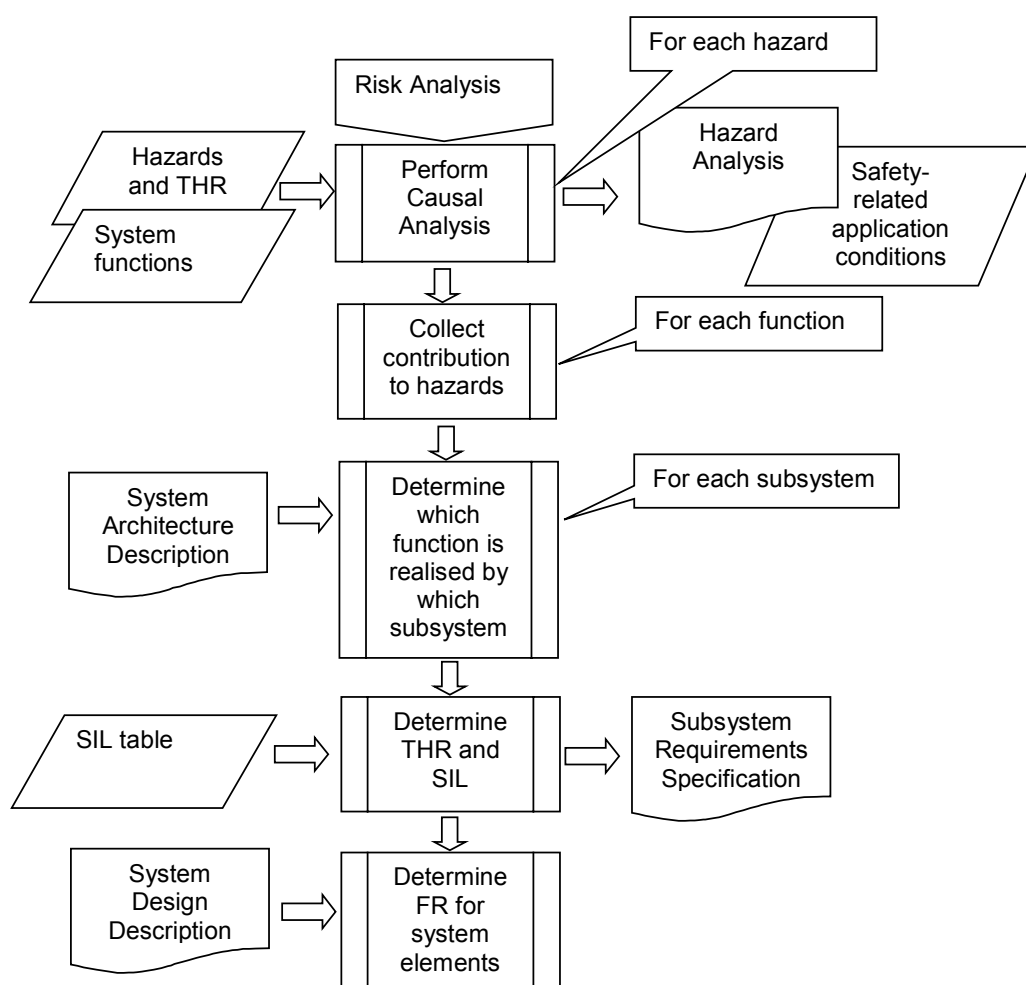


Figure 5.4 - Process details of System Design Analysis (steps 4-5) in flowchart notation

5.3 Definition of Safety Integrity Levels

The CENELEC standards for railway signalling 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.

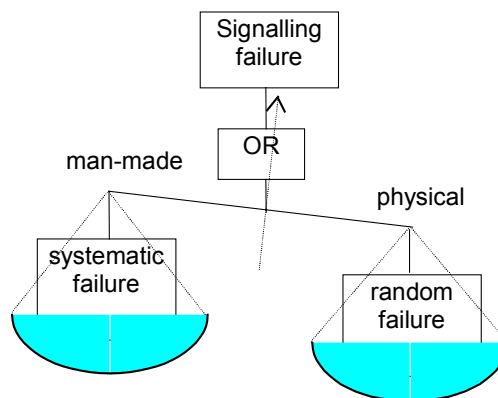


Figure 5.5 - SIL concept

This concept is clearly explained in annex A of ENV 50129:

Each of these Functions shall have a qualitative Safety Target and/or¹ a Quantitative Target attached to them. The Qualitative Target shall be in the form of a Safety Integrity Level, and shall cover Systematic Failure Integrity. The Quantitative Target shall be in the form of a numerical failure rate, and shall cover Random Failure Integrity.

It is important to recognize that achievement of a specified Safety Integrity Level requires compliance with all of the factors in Figure A.2, namely:

- **Quality Management conditions;**
- **Safety Management conditions;**
- **Technical Safety conditions;**
- **Quantified safety targets.**

In many standards like IEC [IEC] or ENV 50129 [129] this balance is expressed in a table, which consists of a list of integrity levels 0, 1, 2, 3, 4 and a list of corresponding intervals or bands for hazard rates $I_0, \dots, I_4$.

5.4 Qualitative vs quantitative methods

5.4.1 Qualitative assessment

The qualitative risk assessment process broadly relies on expert judgement and past experience primarily within a subjective and coarse quantitative process. It is worth noting that mere use of quantification and numbers does not necessarily qualify an assessment as quantitative. Such quantification is mainly a reflection of judgement and lacks the objectivity and accuracy to generate a detailed and reliable measure of risks.

The qualitative framework for assessment of risks arising from hazards of undertakings, products and processes, yields a number of benefits;

- principally a judgmental process;
- no detailed quantification, data collection and analytical work;
- simple and can be carried out without assistance from process experts;

¹ At first glance this formulation "and/or" may seem contradictory. But section A.4.2.2 (the one containing the SIL table) gives guidance what to do if only a qualitative Safety Target or a Quantitative Target is defined, namely to find the missing target by the SIL table.

- auditable process with scope for review and improvement;
- does not require customisation or a specific form of a ranking matrix;
- employs the same framework and principles as in the quantitative approach;
- ease of extension/migration to the quantitative assessment where necessary.

The constraints and disbenefits of the qualitative approach must be borne in mind however, these are;

- subjective and coarse nature of assumptions necessitating thorough documentation;
- simplistic hence unsuitable for complex systems and high-risk undertakings;
- inadequate for the assessment of major risks leading to significant losses.

5.4.2 Quantitative assessment

The quantitative risk assessment process generally satisfies the following requirements:

- extensive use of modelling;
- predominate application of objective and validated data;
- treatment of uncertainty associated with input data and results;
- treatment of dependency between significant factors;
- use of statistical simulation where appropriate.

Modelling predominately represents a simplification and generalisation of reality but, enhances our understanding of causal relationships, highlights important factors and provides a useful tool for anticipation and potentially prediction of future.

The quantitative framework for assessment of risks arising from hazards of undertakings, products and processes, yields a number of major advantages over its qualitative counterpart:

- generates a quantified measure of risks in complex situations;
- capable of addressing uncertainty and statistical variations in input data;
- capable of addressing dependencies in the input parameters/data;
- capable of generating confidence intervals for the quantified risks;
- capable of demonstrating compliance with legal duty and Industry Benchmarks;
- auditable objective process with scope for review and improvement;
- does not employ arbitrary tolerability criteria popularized by risk matrices;
- does not require customisation or a specific form of a ranking matrix;
- provides an auditable and traceable approach to decision support;
- employs the same framework and principles as in the qualitative approach.

The constraints and disbenefits of the quantitative approach must be borne in mind however, namely:

- complex hence unsuitable for low risk systems and undertakings;
- requires expert resource in knowledge elicitation and risk modelling;
- need for extensive range of objective data and the requisite pre-processing;
- need for formidable computing resource and know-how;
- resource intensive, costly hence inappropriate for applications where a qualitative approach may suffice;
- lack of readily available, robust and comprehensive computer based tools.

5.5 EN 50126 lifecycle context

The linking between the WG A10 tasks and the EN 50126 phases is described in this subclause.

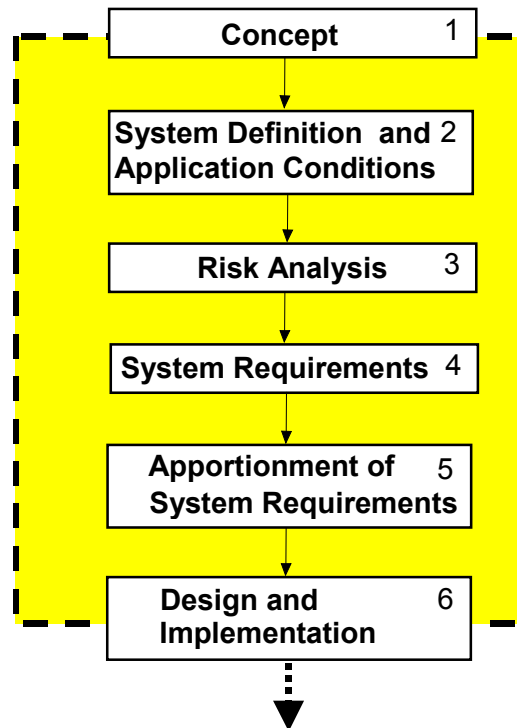


Figure 5.6 - Relevant phases of the generic EN 50126 lifecycle

The lifecycle process as described in EN 50126 is a top down approach. Therefore almost identical requirements appear in several successive phases. The output will of course be more detailed as the process proceeds through the phases. Even though the lifecycle could be seen as an advancing process, the results of a later phase could necessitate changes in a previous phases (recursion).

In Table 5.1 the corresponding tasks (requirements) from every lifecycle phase, as these are described in EN 50126 (or ENV 50129), are summarized and listed opposite the WGA10 tasks described in Figure 5.2.

Table 5.1 - Relation with EN 50126 lifecycle phases

WGA10-method task	Corresponding lifecycle phase and tasks from EN 50126
1 Define system (functions, boundary, interfaces, environment)	Close related to Lifecycle phase 2: System definition. The definition of the system starts in phase 1 and is refined in phase 2. It is very important that the final identification of hazards is not made before the scope, the boundaries and the application conditions of the system are well defined. Following the list of requirements for tasks to be performed in phase 1 and 2 will normally result in a sound system definition. The requirements of phase 1 and 2 from the EN 50126 are shown in clause 6 of this report.
2 Identify (system) hazards	Related to part of lifecycle phase 3: Risk analysis The identification of hazards starts in phase 1 with obtaining information about RAMS requirements, past RAMS performance, identified sources of hazards. It carries on in phase 2 with describing the scope of the system hazard analysis and making preliminary hazard identification. In phase 3 the hazard log for ongoing risk management is established and the identification of hazards is done. The hazard identification is a cardinal point in the whole process of allocation of SIL. Following the list of requirements for tasks to be performed in phase 1, 2 and 3 will not necessarily result in exhaustive hazard identification. To improve the understanding of the hazard analysis supplementary information can be found in clause 7 of this report.
3 Analyse consequences of hazards	Closely related to the main subject in lifecycle phase 3: Risk Analysis In phase 1 information about past RAMS performance, current Railway safety Authority policy and targets and safety legislation is collected In phase 2 types of accident initiating events is identified and initial risk tolerability criteria is defined. In phase 3 the consequence analysis is done. The frequency, the likely severity of the consequences, and the risk for each hazard is evaluated. The acceptability of the risk associated with each hazard is determined and classified. In phase 4 the results of the consequence analysis is transferred into the System requirement specification as safety function requirements, safety integrity requirements for each function and application environment. Many railway people are unfamiliar with the risk-concept and therefore the tasks listed in EN 50126 do not give enough guidance on consequence analysis. This is the reason why extra information is given in clause 8 of this report.
4 Analyse causes of hazards. Identify additional hazards	Related to lifecycle phase 5: Apportionment of system requirements and phase 6: Design and implementation. Phase 5 embraces requirements to allocate safety requirements to designated subsystems, components and external risk reduction facilities. Phase 6 includes requirements to design and realize the design of subsystems and components to meet the RAMS requirements and prepare a Generic safety case including a consideration of the SIL justifications for safety functions.
5 Allocate safety integrity requirements to subsystems/system elements	The requirements above are difficult to fulfil for the one who is going to design a real system. The causal analysis and the allocation of safety integrity to subsystems/ system elements is a part of the design process and must be documented in the Technical Safety Report which is part of the safety case. More guidance can be found in ENV 50129 in Annex A. However, a practicable method is not given in the annex. In order to close this gap a method is proposed in clause 9 of this report.

In conclusion the methodology presented here is in line with the EN 50126 lifecycle. In fact there is almost a one-to-one correspondence between the steps in the methodology and the EN 50126 lifecycle phases. However the exact location of tasks can depend on the system definition.

6 System definition

EN 50126 already lists sufficient requirements on the definition of railway systems in phase 1 and 2 of the RAMS lifecycle [126]. However in practice this information is not usually available or well documented. As a reminder, the essential requirements are repeated here.

Phase 1 (Concept):

6.1.3.1 Requirement 1 of this phase shall be to acquire, in the context of RAMS performance, an understanding of:

- a) the scope, context and purpose of the system.*
- b) the environment of the system, including:*
 - physical issues;*
 - potential system interface issues;*
 - social issues;*
 - political issues;*
 - legislative issues;*
 - economical issues.*
- c) the general RAMS implications of the system.*

6.1.4.1 The results from this phase shall be documented, along with any assumptions and justifications made during the phase.

Phase 2 (System Definition and Application Definitions):

6.2.3.1 Requirement 1 of this phase shall be to define:

- a) the system mission profile, including:*
 - performance requirements;*
 - RAMS targets;*
 - long term operating strategy and conditions;*
 - long term maintenance strategy and conditions;*
 - system life considerations, including lifecycle costing issues;*
 - logistic considerations.*
- b) the system boundary, including:*
 - interfaces with physical environment;*
 - interfaces with other technological systems;*
 - interfaces with humans;*
 - interfaces with other Railway Authorities.*
- c) the scope of application conditions influencing the system, including:*
 - constraints imposed by existing infrastructure;*
 - system operating conditions;*
 - system maintenance conditions;*
 - logistic support considerations;*
 - review of past experience data for similar systems.*
- d) the scope of the system hazard analysis, including the identification of:*
 - hazards inherent within the process to be controlled;*
 - environmental hazards;*
 - security hazards;*
 - the influence of external events;*
 - the boundaries of the system to be analysed;*
 - the influence on RAMS of existing infrastructure constraints.*

6.2.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

The system definition is therefore the key, without which the following steps may produce incorrect or invalid results.

Another important observation is that the definition of the term system depends on the perspective. The terms system, subsystem and system element are to a great extent arbitrary. There is no fixed definition as to what a system is and is not. Stated differently, the user of the process defines what the system is.

7 Hazard identification

7.1 General principles

Hazard Identification involves systematic analysis of a product, process, system or an undertaking to determine those adverse conditions (hazards) which may arise throughout the lifecycle. Such adverse conditions may have the potential for human injury, damage to the environment or economic loss.

With reference to the process overview in Figure 5.2 Hazard Identification applies in particular to steps 2 and 4.

Hazard Identification is fundamental to the risk assessment process. Absence of a systematic and comprehensive Hazard Identification phase can severely undermine the credibility of risk assessment process. This is particularly true where, due to inappropriate hazard identification, several significant hazards remain unidentified leading to inaccurate and misleading risk assessment. In the worst case this can create an illusion of safety and a false sense of confidence.

Systematic identification of hazards generally involves two phases (detailed further below):

- an empirical phase;
- a creative phase.

The empirical phase relies largely upon knowledge and experience of the past to identify potential hazards. This may be, for example, through application of an appropriate checklist.

Whilst empirical identification of hazards is sometimes sufficient for routine undertakings, novel or modified undertakings will additionally also require a more creative form of hazard identification. The second phase of hazard identification therefore applies systematic and creative techniques. Such techniques usually rely upon collective, imaginative thinking. The aim of such techniques is to identify previously unknown hazards which may arise from the undertaking.

The empirical and creative phases of Hazard Identification complement one another, increasing confidence that the potential hazard space has been covered and that all significant hazards have been identified. It should be noted that identification of a single significant hazard may outweigh identification of a large number of less significant hazards. That is, the quality and not the quantity is of the essence here.

Methodologies which generate an unrealistically large number of mostly trivial hazards are wasteful of resource and can lead to a misleading or unproductive risk assessment. With the exception of large undertakings, involving many personnel, activities and equipment, a large list of hazards extending into the hundreds is unreasonable and indicative of a poorly designed or conducted study.

The problem of large numbers of hazards is partially caused by the fuzzy definition of the term "hazard" itself. The definition of [129] is too general:

hazard: A condition that could lead to an accident

By this definition anything possibly contributing to an accident has to be called a hazard. So almost everything could be a hazard. This seems patently unhelpful (If everything is a hazard, the term has no meaningful use).

For practical purposes it seems more reasonable to follow the enhanced definition offered in clause 3 of this document or a standard textbook definition [Lev95]:

A hazard is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event). [...] A hazard is defined with respect to the environment of the system or component. [...] What constitutes a hazard depends upon where the boundaries of the system are drawn. [...].

This definition seems more useful because here the hazards depend on the system definition and in particular the system boundary, which allows a hierarchical structuring of hazards with respect to systems and subsystems. It also means that hazard identification and causal analysis can and must be performed repeatedly at several levels of detail during the system development. Figure 7.1 shows that the cause of a hazard on system level may be considered as a hazard on subsystem level (with respect to the subsystem boundary). Thus this definition enables a structured hierarchical approach to hazard analysis and hazard tracking.

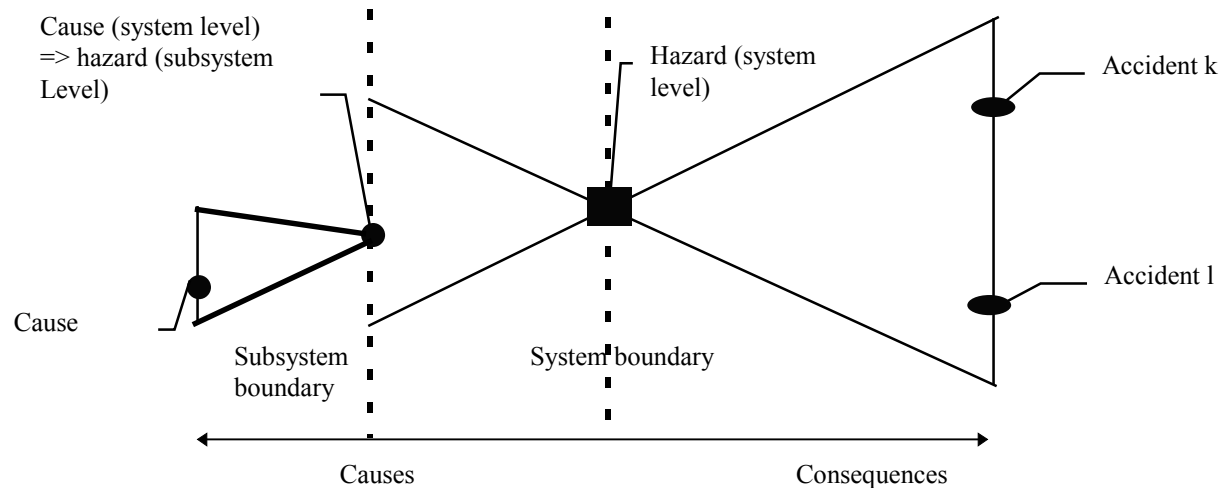


Figure 7.1 - Definition of hazards with respect to the system boundary

To further ensure that risk assessment effort is focused upon the most significant hazards, the hazards should, once identified, be ordered in terms of their perceived risk level. Hazard ranking should therefore take into account the rate as well as the severity of the adverse consequences which may arise from hazards. The subsequent stages of risk assessment should be applied on a prioritized basis, beginning with the highest ranking hazards. The relative rank of each hazard should be used to guide the breadth and depth of its further analysis.

A record must be kept of all identified hazards and other pertinent information. This is referred to as a Hazard Log.

7.2 Empirical hazard identification methods

Knowledge and experience of the past is a valuable means of determining potential hazards arising from a new or modified undertaking. The empirical phase of Hazard Identification exploits such knowledge and experience. It constitutes a simple, first-cut identification of potential hazards and ensures that, where possible, errors, failures and losses of the past are avoided.

Typical empirical hazard identification methods include:

- checklists of hazardous circumstances;
- structured walkthroughs.

Where an undertaking lends itself to more detailed scrutiny, the following methods may also be employed:

- Failure Mode and Effects Analysis (FMEA) for equipment and systems;
- Task Analysis for man-machine interfaces.

These latter techniques identify particular component failures or human errors which may lead to hazardous circumstances at the system level. Empirical hazard identification methods are not resource intensive and may be conducted by suitably informed individuals.

Where an undertaking involves no novel or modified aspects, empirical methods may prove adequate for identification of significant hazards. However, many undertakings include novel aspects or changes in functionality or technology. In such cases, empirical hazard identification will cover only a subset of the potential hazard space. The existence of additional, significant hazards should therefore be explored further through the use of complementary creative hazard identification techniques.

7.3 Creative hazard identification methods

Creative hazard identification comprises systematic techniques to encourage lateral and imaginative creative thought. Ideally a team-based approach is employed to exploit the diverse and complementary backgrounds of a range of individuals. Creative methods generally exhibit the following key characteristics:

- planning and process management procedures;
- guidelines for team selection and briefing;
- hierarchical decomposition and graphical representation of the problem domain;
- high level examination of the key elements of the system and determination of the critical subsystems and interfaces;
- comprehensive, step-by-step examination of subsystems and interfaces with a meticulous scrutiny of the critical areas;
- identification and recording of potential hazardous circumstances including causes, consequences and potential mitigation and control measures;
- judgmental ranking of the identified hazards, employing an appropriate frequency/consequence matrix.

Before conducting hazard identification, it is necessary to develop preliminary ideas concerning the scope or boundary of the undertaking concerned. However, rigid adherence to this boundary during the hazard identification process can prevent identification of interactions that have not previously been considered and which may lead to significant hazards (particularly where complex technological and/or human interfaces are involved). An important feature of creative hazard identification methods is their ability to fully explore the scope and boundary of an undertaking. In particular, they generally allow the full domain of influence of an undertaking to emerge during the hazard identification study.

Examples of creative hazard identification methods include:

- structured what-ifs;
- brainstorming;
- Hazard and Operability (HAZOP) studies.

7.4 Hazard ranking

A simple hazard ranking matrix should be employed to identify the relative significance of all identified hazards, and to enable further risk assessment effort to be focused upon the most significant hazards. For example a matrix of severity versus frequency (similar to the matrix used in EN 50126), generating a hazard index, or any other simple variant, will suffice for ranking and prioritisation purposes.

When determining the losses associated with each identified hazard, in subsequent stages of risk assessment, the relative rank of each hazard should be used to guide the breadth and depth of its further analysis. Hazards of low rank will require only limited further qualitative treatment. In contrast, the most significant hazards, which are likely to be small in number, may also warrant more detailed quantitative assessment.

All hazards must:

- be recorded in the Hazard Log generated as a result of Hazard Identification;
- continue to be reviewed in future, in order to ensure that their associated risks remain within the predicted bounds and continue to be appropriately managed.

The hazard ranking approach ensures that:

- subsequent risk assessment effort is focused on reducing those risks associated with the most significant hazards;
- the totality of risk associated with an undertaking is considered in determining the acceptability of risk mitigation measures, in compliance with the legal duty of care.

7.5 Existing hazard lists

Currently a number of industry level hazard lists are published and accessible in the public domain, for example [RSH]. These may prove helpful as a starting point for

- empirical hazard identification (as a checklist);
- creation of a comprehensive list of railway hazards;
- the determination of tolerability criteria.

8 Risk analysis

8.1 Risk tolerability

Risk acceptance is a societal and legal issue and should therefore be based on generally accepted principles or consensus. Currently there seems to be no such consensus in the CENELEC member states. However for interoperable systems such a consensus is explicitly necessary.

8.2 Determination of Tolerable Hazard Rate

8.2.1 Qualitative risk analysis

This qualitative assessment method essentially merges Consequence and Loss Analyses subjectively and generates estimates for the rate or the probability of the hazard and the consequent safety losses. A risk matrix, generally employed for ranking purposes can be calibrated to provide coarse measures of total risk per hazard. This subjective mode of analysis merges (or gives conservative estimates for)

- probability of timely detection and mitigation;
- the effect of various protection and mitigation barriers to escalation;
- probability that the hazard leads to an accident;
- the likely range of adverse consequences with varying degrees of intensity;
- probability that an accident leads to safety loss;
- various groups exposed to the hazards;
- the distribution of risk exposure per population;
- the contribution of various accidents to total safety loss.

This effectively amounts to over-estimation and sometime gross exaggeration of safety risks, potentially leading to excessive costs in over-engineering the product or process. The matrix in Table 8.1 represents a coarse calibrated safety assessment tool. The frequency scale in the matrix of Table 8.1 is calibrated on the basis of occurrence per hour rate, starting with a period of 10 hours. This is a declining decades scale culminating in a periodicity of 10^6 hours or roughly 100 years.

For the consequence scale, the following assumption is made (based on past UK figures):

- 1 fatality = 10 Major Injuries = 100 Minor Injuries;
- the frequency and severity classifications are contiguous overlapping bands as opposed to discrete values.

Therefore, the matrix elements contain the total hourly risk as follows:

Table 8.1 - A calibrated frequency - consequence matrix

Frequency of occurrence of a hazardous event		Total Safety Risk Levels			
10^{-1} per hour	Frequent	10^{-3}	10^{-2}	10^{-1}	1
10^{-2} per hour	Probable	10^{-4}	10^{-3}	10^{-2}	10^{-1}
10^{-3} per hour	Occasional	10^{-5}	10^{-4}	10^{-3}	10^{-2}
10^{-4} per hour	Remote	10^{-6}	10^{-5}	10^{-4}	10^{-3}
10^{-5} per hour	Improbable	10^{-7}	10^{-6}	10^{-5}	10^{-4}
10^{-6} per hour	Incredible	10^{-8}	10^{-7}	10^{-6}	10^{-5}
		Insignificant Minor Injuries	Marginal Major Injuries	Critical 1 Fatality	Catastrophic ≥10 fatalities
Severity Levels of Hazard Consequence					

Note that contrary to EN 50126 this matrix itself does not justify the tolerability of the risks which is a societal and legal matter and should preferably be stated by regulatory authorities at the industry level.

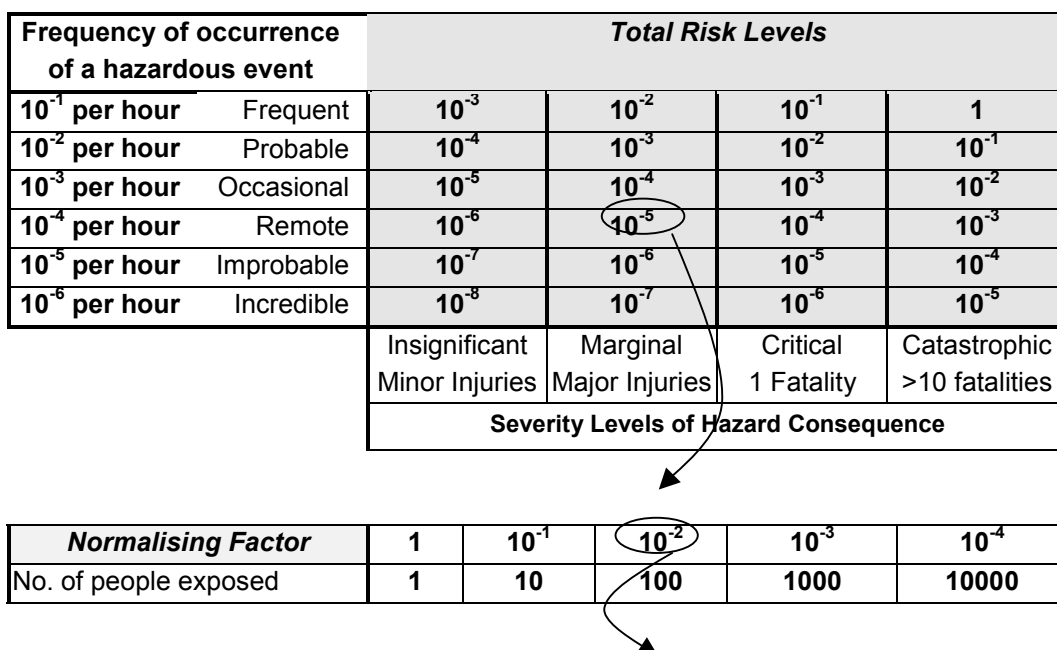
However, the total risk determined through the matrix must be normalized according to the number of people affected by the hazard (i. e. exposed to the risk) which amounts to a three dimensional matrix. A decade scale for simplicity and convenience is proposed in Table 8.2 as follows:

Table 8.2 - Normalising by population at risk

Normalising Factor	1	10⁻¹	10⁻²	10⁻³	10⁻⁴
No. of people exposed	1	10	100	1000	10000

The total risk figures in the matrix in Table 8.1 must be adjusted by the normalisation factor through adding the negative indexes. This would result in a very coarse measure for individual risk of fatality arising from a hazard caused by failure or mal-operation of a signalling system.

The overall process overview for subjective assessment so far is depicted in Figure 8.1 where as an example, a population of 100 is estimated to be exposed to a total risk of fatality of **10⁻⁵** per hour. It should be noted that the severity level and the number of people exposed are closely correlated. They are both to be determined as long-term averages in order to prevent misuse of a short-term view



$$\text{Individual Risk of Fatality per Hour (IRF}_{/h}) = 1\text{E-5} \times 1\text{E-2} = 10^{-5-2} = 10^{-7}$$

Figure 8.1 - Qualitative assessment process employing individual risk

For systems entailing a number of hazards, it is necessary to sum-up a number of contributions from each hazard and generate a total figure for IRF

$$IRF = \sum_{\text{all hazards } H_j} HR_j \times \frac{S_j}{N_P}$$

Subsequent comparison of IRF with the tolerability limit (Target Individual Risk, TIR) would show whether the risk is permissible or not. If the risk is permissible then the estimated hazard rates (HR_j) could be accepted as THR_j .

$$TIR = \sum_{\text{all hazards } H_j} THR_j \times \frac{S_j}{N_P}$$

If there is a gross disproportion between the IRF and the TIR, then the HR have to be adjusted until the TIR is matched by the IRF. As a simple mechanism an average scaling factor S can be used for the determination of Tolerable Hazard Rate (THR), where;

$$\begin{aligned} S &= (TIR) / (IRF) \\ THR_i &= HR_i \times S \end{aligned}$$

The assumptions implicit in the approach are that generally the rate and not the safety losses associated with a hazard can realistically be controlled and that the relationships are linear. The Tolerable Hazard Rate (THR) can now be employed in the determination of the system architecture and Safety Integrity requirements for systems and subsystems. Note that S is a dimensionless constant, but not necessarily a probability, because S may be greater than 1.

The qualitative process is diagrammatically shown in Figure 8.2.

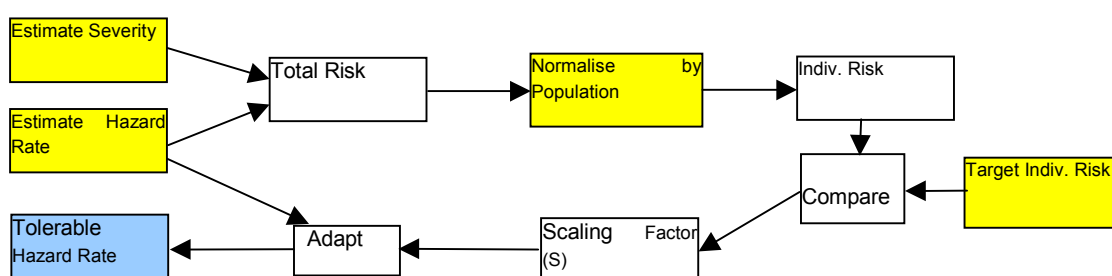


Figure 8.2 - Overview of the qualitative hazard rate estimation

In principle, the qualitative process employs a subjective approach to the estimation of the criticality. It is most suited to low risk situations or first attempt at evaluation before a more rigorous method is deemed appropriate. However, the proposed qualitative process does take into account the operational environment in order to arrive at a Tolerable Hazard Rate, which in turn, helps with the determination of a suitable system architecture to satisfy the criticality requirements.

8.2.2 Quantitative risk analysis

A more rigorous approach to determination of safety risks is pertinent to novel or potentially high-risk hazards. As for the qualitative approach, upon identification of the significant hazards, systematic and objective Consequence and Loss Analyses are required in order to forecast safety risks taking into account the operational environment. The aim is to systematically and objectively arrive at a quantitative Tolerable Hazard Rate (THR) in preference to subjective estimation employed in the Qualitative approach. This will in turn assist with a more credible determination of Safety Integrity Requirements.

8.2.2.1 Determination of individual risk

A mathematical treatment for the determination of individual risk is given, taking into account the causality leading from hazards to accidents.

- 1) The individual i uses a technical system (e.g. LC, train ...). The usage profile is described by the number of uses N_i (per year or per hour). For reference a total exposure per use E_i may be defined (i.e. the duration of a train journey or the time needed to pass a LC).