MODSafe

European Commission

Seventh Framework programme

MODSafe Modular Urban Transport Safety and Security Analysis

WP 4 – D4.1

State of the art analysis and review of results from previous projects

Reviewed by:	WP4 and WP10
Authors:	WP4
Document ID:	DEL_D4.1_UITP_WP4_100318_V2.1
Date:	18. March 2010
Contract No:	218606

Contract No.	218606
Document type	*DEL*
Version	*V2.1*
Status	*Final*
Date	*18. March 2010*
WP	*WP 4*
Lead Author	*S. Scholz, H. Forchmann*
Contributors	*WP4 partners*
Reviewer	*WP 4, WP10*
Description	*State of the art analysis and review of results from previous projects*
Document ID	*DEL_D4.1_UITP_WP4_100318_V2.1*
Dissemination level	*PU*
Distribution	*WP4*

Document History:

Version	Date	Author	Modification
V1.0	27.11.2009	WP4	New document
V1.1	08.01.2010	WP4	Consideration of comments from WP4
V1.2	22.01.2010	WP4	Consideration of comments from WP4
V2.0	01.03.2010	WP4	Consideration of comments from WP10
V2.1	18.03.2010	WP4	Consideration of comments from WP10

Approval:

Authority	Name/Partner	Date	Visa
EB members			
WP responsible			
Coordinator			

Table of contents

List of figures

List of tables

1. Summary of this document

This deliverable aims at describing methods for the allocation of safety integrity requirements on hazard control or safety measures. It shall represent the state of the art of approaches described and outlined in standards and guidelines as well as actual methods used by railway operating companies.

These methods for safety requirement allocation are analysed and compared on the basis of example functions, its methodology and applicability.

The scope of this deliverable is the urban guided rail sector in Europe covering metros, trams and other light rail systems under regard of different grades of automation. These grades of automation are distinguished from “Driving on Sight” up to “Fully Automatic and Unattended Train Operation”.

The focus of this document is put on safety functions and measures from the signalling domain of urban guided transport systems, because most of the safety requirements put on overall systems traditionally can be found in this lot.

Nonetheless, the described safety requirement allocation schemes may also be applied to areas others than signalling, e.g. interfaces between signalling equipment and vehicle equipment or other safety functions in general. It is therefore not necessary to deal with other domains in detail. Signalling examples have only been chosen to illustrate the general approach. In some cases, standards or recommendations from other domains also dealing with safety requirements (e.g. for vehicle equipment) are mentioned in the deliverable, to inform the reader about their availability

This deliverable is written for MODSafe project partners and European railway authorities i.e. operators of urban guided transport systems.

Since this deliverable aims at comparing actual methods for safety requirement application, it uses original descriptions from these methods. Where appropriate, citations are made directly from the source documents. Citations are indicated in italic font.

The following figure compounds the idea of the deliverable.

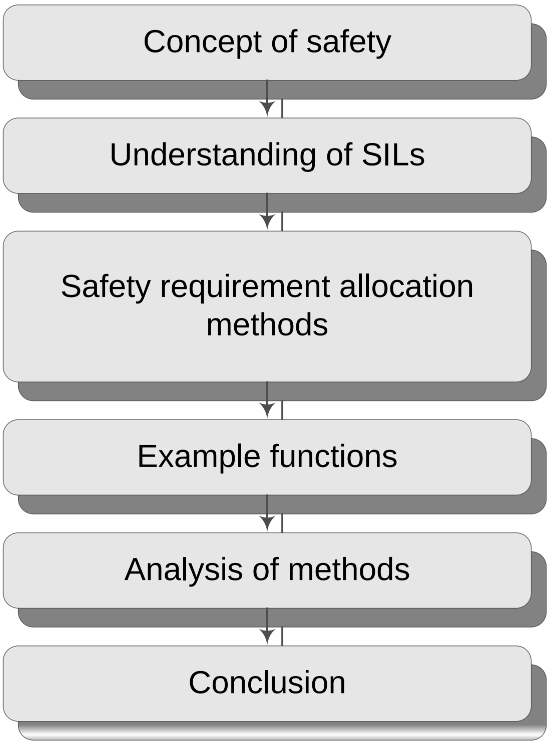


Figure 1 Structure of MODSafe deliverable 4.1

2. References

[1] – MODURBAN: “D126 – Preliminary safety plan“, MODURBAN – MODSYSTEM WP23 2009

[2] – SMITH, DAVID J; SIMPSON, KENNETH G L: “Functional Safety – a straight forward guide to applying IEC 61508 and related standards”, Elsevier Butterworth-Heinemann Second Edition 2004

[3] – CENELEC: “EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)”, CENELEC 1999

[4] – SHORT, ROGER: “The use and misuse of SIL”, Institution of Railway Signal Engineers - IRSE News Issue 142 February 2009

[5] – CENELEC: “CLC/TR 50506-2 Railway applications – Communication, signalling and processing systems – Application guide for EN 50129 – Part 2: safety assurance”, CENELEC 2009

[6] – REDMILL, FELIX: “Understanding the use, misuse and abuse of safety integrity levels”, Proceedings of the eighth safety-critical systems symposium, UK.Springer, 2000

[7] – CENELEC: “CLC/TR 50126-2 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Guide to the application of EN 50126 for safety”, CENELEC 2006

[8] – CENELEC: “CLC/TR 50451 Railway applications – Systematic allocation of safety integrity requirements (Technical Report)”, CENELEC 2007

(The CENELEC Technical Report CLC/TR 50451 is in fact a conversion of the old CENELEC report R009-004 “Railway applications - Systematic allocation of safety integrity requirements” published in 2001, without any other modification than the numbering. It shall be noted therefore that the content of CLC/TR 50451 was issued before EN 50129.)

[9] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-1 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General requirements“, IEC 1998

(It shall be noted that IEC 61508 series are under revision, that the new versions were approved at CDV (Committee Draft for Vote) stage in April 2009 and the FDIS (Final Draft International Standard) stage will be closed on 19 February 2010.)

[10] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-5 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 5: Examples of methods for the determination of safety integrity levels“, IEC 1998

[11] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-4 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 4: Definitions and abbreviations“, IEC 1998

[12] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-2 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 2: Requirements for E/E/PE safety-related systems“, IEC 2000

[13] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-6 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 6: Guideline on the application of IEC 61508-2 and IEC 61508-3“, IEC 2000

[14] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-7 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 7: Overview of techniques and measures“, IEC 2000

[15] – INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: “IEEE 1474.1 2004 - Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements“, IEEE Vehicular Technology Society - Rail Transit Vehicle Interface Standards Committee 2004

[16] – CENELEC: “EN 50129 Railway application – communication, signalling and processing systems – safety related electronic systems for signalling”, CENELEC 2003

[17] – EUROPEAN RAILWAY AGENCY: “Recommendation on the 1st set of Common Safety Methods (ERA-REC-02-2007-SAF)”, European Railway Agency 2007

[18] – RAIL SAFETY AND STANDARDS BOARD: “Engineering Safety Management (Yellow Book) – Issue 4”, RSSB 2007

[19] – VERBAND DEUTSCHER VERKEHRSUNTERNEHMEN: “Technische Regeln - TR SIG ZA: Zulassung und Abnahme von Signal- und Zugsicherungsanlagen gemäß BOStrab“, VDV 2007

[20] – VERBAND DEUTSCHER VERKEHRSUNTERNEHMEN: “VDV Schriften 331 – Sicherheitsintegritätsanforderungen für Signal- und Zugsicherungsanlagen gemäß BOStrab“, VDV 2007

[21] – MODURBAN: “D86 – Safety conceptual approach for functional and technical prescriptions“, MODURBAN – MODSYSTEM WP23 2006

[22] – MODURBAN: “D90 – Generic Model / Guidance for Risk Analysis“, MODURBAN – MODSYSTEM WP23 2008

[23] – KURZ, S.; MILIUS, B.: “Die Gefährdungseinstufung im ERA-Risikomanagementprozess”, Tetzlaff Verlag Hamburg, Signal und Draht (100) 09/2008

[24] –BRABAND, JENS: “Risikoanalysen in der Eisenbahn-Automatisierung”, Eurailpress Edition Signal und Draht, Herausgegeben von der Siemens AG, 2005

[25] – EUROPEAN UNION: “Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council”, Official Journal of the European Union L108/4 – 29.04.2009

[26] – VERBAND DEUTSCHER VERKEHRSUNTERNEHMEN: “VDV Schrift 161 – Sicherheitstechnische Anforderungen an die elektrische Ausrüstung von Stadt- und U-Bahn-Fahrzeugen. VDV 2005

[27] – Braband, Jens; vom Hövel, Rüdiger; Schäbe, Hendrik: “The probability of failure on demand – the why and the how“, Proceedings of the International Conference on Computer Safety, Reliability and Security SafeComp 2009

[28] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 62267 Railway Applications - Automated Urban Guided Transport (AUGT) - Safety Requirements”, IEC 2006

[29] – INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 62290-1 Railway applications - Urban guided transport management and command/control systems (UGTMS)- Part 1 System principles and fundamental concepts”, IEC 2009

3. Terms and abbreviations

3.1 Terms

Term	Definition	Reference
Assessment	The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product.	EN 50126
Hazard	A condition that could lead to an accident.	EN 50129
(Railway) Authority	The body with the overall accountability to a regulator for operating a (railway) system.	EN 50126
Railway operating company	Entity which is responsible for safe and orderly operation of a transport system and which is providing the transport service. NOTE: The term “railway operating company” shall stress the operational aspect (responsible for running and maintaining the system) of this entity but not indicate any regulatory or administrative power. Despite the different wording it is therefore by analogy with the definition for “railway authority” which is given in EN 50126.	Own definition for D4.1
(Railway support) Industry	Generic term denoting supplier(s) of complete (railway) systems, their sub-systems or component parts.	EN 50126
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.	CLC/TR 50126-2
Safety	Freedom from unacceptable level of risk of harm.	EN 50129
Safety acceptance	The safety status given to a product by the final user.	EN 50129
Safety approval	The safety status given to a product by the requisite authority when the product has fulfilled a set of predetermined conditions.	EN 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. Compare EN 50126: Safety regulatory authority – Often a national government body responsible for setting or agreeing the safety requirements for a railway and ensuring that the railway complies with the requirements.	EN 50129
Safety case	The documented demonstration that the product complies with the specified safety requirements.	EN 50129
Safety function	Function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event	IEC 61508-4
Safety integrity	The ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period of time.	EN 50129
Safety integrity level	A number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures.	EN 50129

Term	Definition	Reference
Safety measure	Means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.	ERA
Safety process	The series of procedures that are followed to enable all safety requirements of a product to be identified and met.	EN 50129
Urban guided transport	Urban Guided Transport (UGT) is defined as a public transportation system in an urban environment with self-propelled vehicles operated on a guideway.	MODURBAN

3.2 Abbreviations

Abbreviation	Definition
A	Exposure to danger
ATO	Automatic train operation
ATP	Automatic train protection
ALARP	As low as reasonably practicable
BOStrab	Verordnung über den Bau und Betrieb der Straßenbahnen (German Federal Regulations on the construction and operation of light rail transit systems)
C (as in **[10]**,**[20]**)	Consequences of hazardous events
C (as in **[21]**)	Consequence reduction probability
CBTC	Communication-based train control
CC	Car-borne controller
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardisation)
CSM	Common safety methods
D	Deliverable
E	Exposure probability of hazard
EN	European standard
E/E/PE	Electrical/electronic/programmable electronic
ERA	European railway agency
EUC	Equipment under control
F (as in **[10]**,**[20]**)	Frequency of, and exposure time in, the hazardous zone
F (as in **[21]**)	Hazard frequency
F_{np}	Frequency – no protection
F_p	Frequency – protected
F_t	Frequency – tolerable
G	Defence against danger/consequences
GAME (or GAMAB)	Globalement au moins équivalent (Globally at least equivalent)
H	Hazard
HR	Hazard rate
IEC	International electrotechnical commission
IEEE	Institute of electrical and electronics engineers
IRF	Individual risk of fatality
ISA	Independent safety assessor
MODURBAN	Modular urban guided rail systems
MODSafe	Modular urban transport safety and security analysis
MODTRAIN	Innovative modular vehicle concepts for an integrated European railway system
MTBHE	Mean time between hazardous events
P (as in **[21]**)	Accident probability reduction
P (as in **[10]**,**[20]**)	Possibility failing to avoid the hazardous event

Abbreviation	Definition
R	Risk
ΔR	Risk reduction
R_{np}	Risk – not protected
RAMS	Reliability, Availability, Maintainability, Safety
S (as in **[8]**)	Scaling factor
S (as in **[21]**)	Severity of hazard consequences
SI	Safety integrity
SIG RZA NE	Richtlinie für die Zulassung und Abnahme von Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (Guideline for approval and acceptance of railway signaling systems of non-federally owned railways)
SIL	Safety integrity level
SL	Severity level
SPTS	Spot transmission sub-system
SRS	Safety related system
TAR	Tolerable accident rate
TBD	To be discussed
TCMS	Train control and monitoring system
TFM	Target failure measure
THR	Tolerable hazard rate
TIR	Target individual risk
TR	Technical report
TR SIG ZA	Technische Regeln – Zulassung und Abnahme von Signal- und Zugsicherungsanlagen gemäß BOStrab (Approval and acceptance of signalling systems according to BOStrab)
UGTMS	Urban guided transport management system
UK	United Kingdom of Great Britain and Northern Ireland
VDV	Verband Deutscher Verkehrunternehmen (Association of German public transport undertakings)
W (as in **[10]**,**[20]**)	Probability of the unwanted occurrence
W (as in **[21]**)	Probability of danger occurrence
WP	Work package

4. Safety for urban guided rail systems

To establish safety for urban guided transport systems, structured and well-defined processes shall be used. The European standard EN 50126 outlines a framework for system safety for railway applications. The concepts introduced by this standard are well known throughout Europe and give guidance for a range of other European standards and guidelines.

In EN 50126 a system life cycle is presented which contains 14 steps, beginning with system concept until a final disposal of the system. Of interest for this deliverable are the first four life cycle phases and in particular the phase three, on the risk analysis and phase four, on the derivation of system requirements.

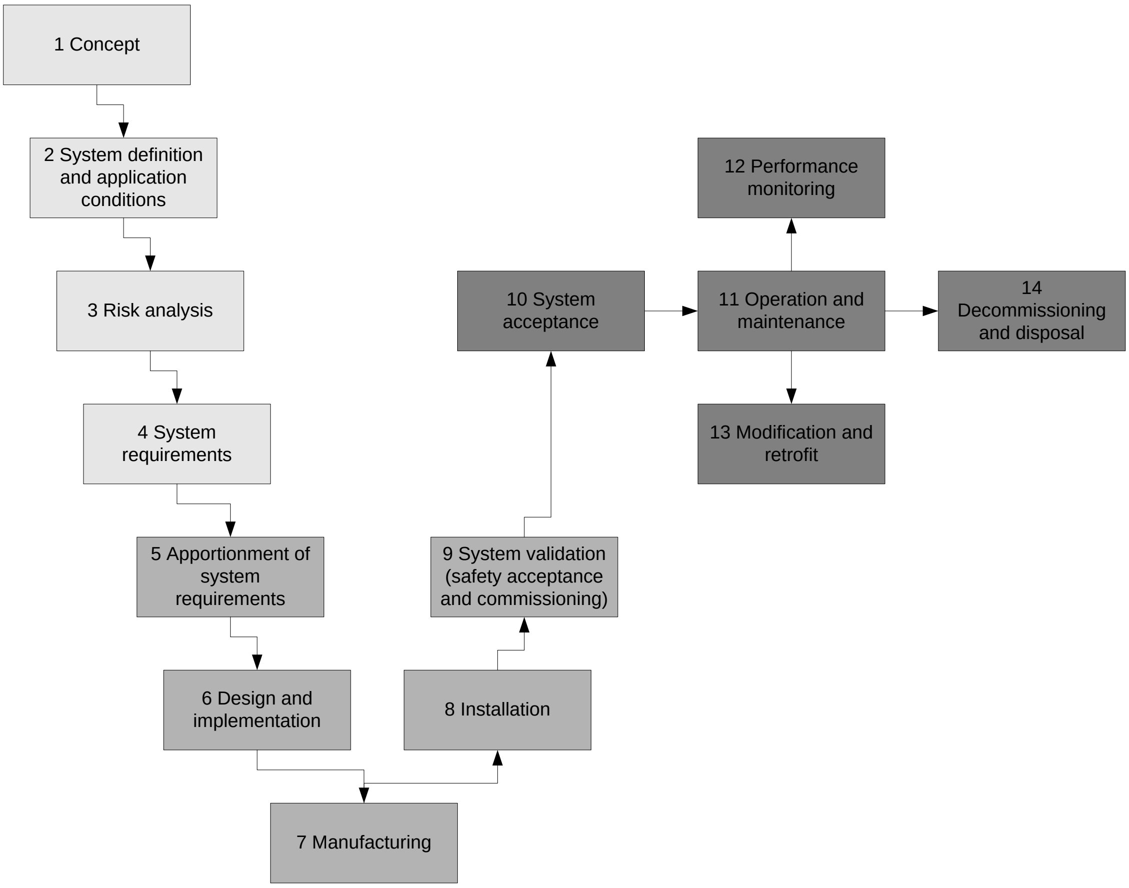

1 Concept
2 System definition and application conditions
3 Risk analysis
4 System requirements
5 Apportionment of system requirements
6 Design and implementation
7 Manufacturing
8 Installation
9 System validation (safety acceptance and commissioning)
10 System acceptance
11 Operation and maintenance
12 Performance monitoring
13 Modification and retrofit
14 Decommissioning and disposal

Figure 2 System lifecycle according to EN 50126

For an illustration of the participants and tasks in the safety process, an example is developed in MODURBAN D126 **[1]**. On a very general level, a distinction can be made between railway operating company, system supplier, independent safety assessor and safety authority as legal representatives of the state (as shown in the light grey rectangles). The operator may issue system requirements, which are realised by the system supplier by developing system design plans and an implementation of the actual system. Additionally, all plans and systems are subject to review, assessment and approval. The example is displayed in the figure below, see Figure 3.

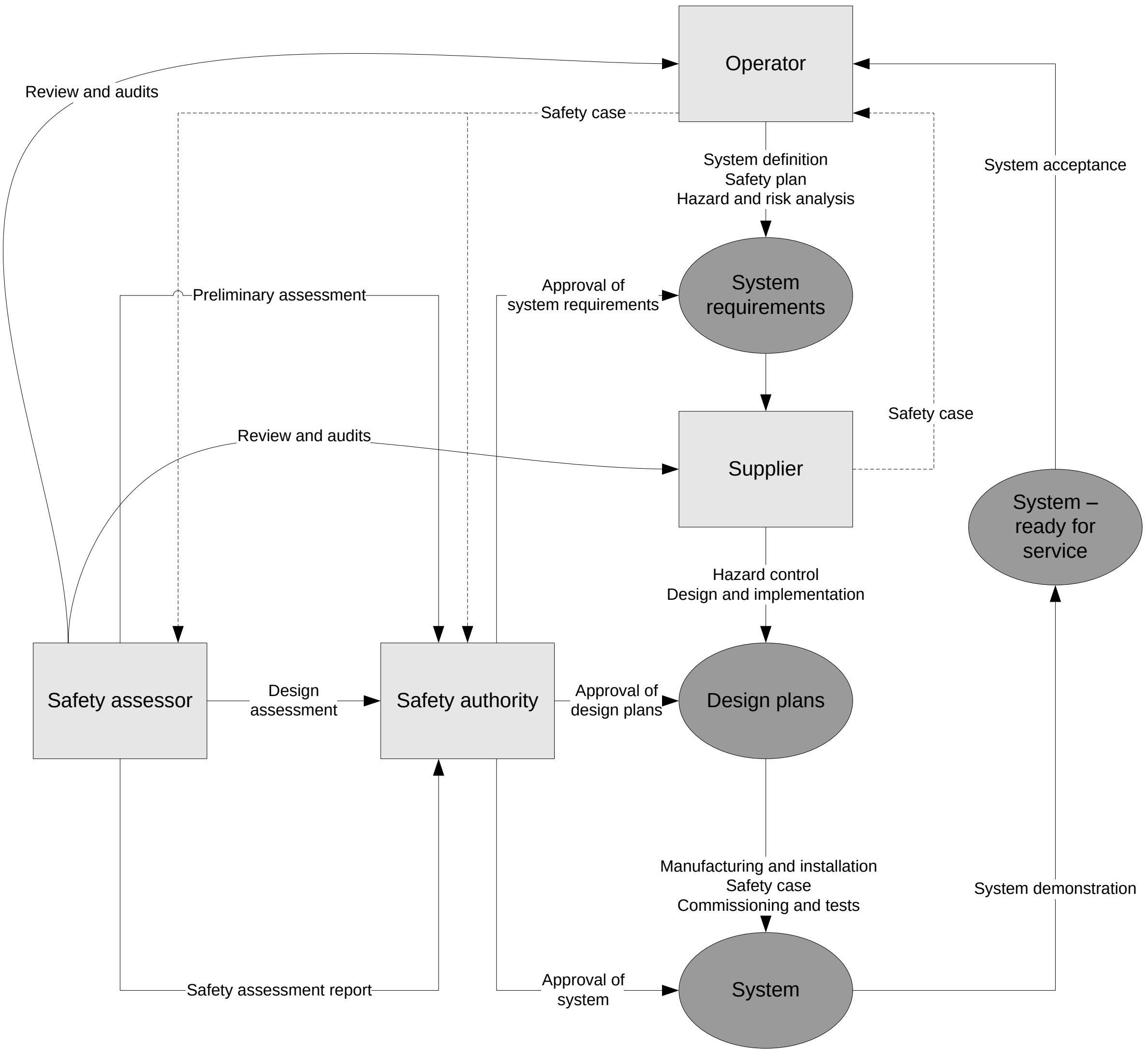


Figure 3 Example of safety process

For the purpose of MODSafe the following safety concept is presumed.

After a system definition, hazards which may arise from the system i.e. the urban guided transport system shall be identified. These hazards shall be subject to an analysis of the evolving risk. Subsequently, hazard control measures (i.e. safety measures, safety functions or risk reduction measures) shall be identified. Safety requirements shall be derived for the safety functions.

It shall be noted however, that depending on the grade of automation different safety functions with different safety requirements may be necessary. For example, IEC62290-1 provides a first brake down of basic functions, which is a precondition for risk analysis and SIL allocation on system level. Furthermore EN 62290-1 provides in Table 1 a rough determination which functions shall be provided as technical system functions under regard of different grades of automation **[29]**.

The procedures, on how to derive these requirements for safety functions, are the subject of this deliverable. Since this attempt may correlate with the allocation of safety integrity levels, abbreviated as SILs, the concept of SILs is outlined in the next clause.

5. Understanding of the SIL concept in the railway domain

According to **[2]** the concept of levels for safety integrity requirements was developed in the 1990s as discrete levels associated with a defined set of requirements for each level for safety integrity. To classify these levels, four (or five) discrete levels are used e.g. in EN 50126, which defines safety integrity level (SIL) in the following way:

One of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity. **[3]**

However, different understandings and application of SIL concepts exist, which may give rise to misunderstandings and misuse (compare **[4]**). For example, what does a SIL actually mean for operator or supplier, shall SILs be applied to functions or elements, do SILs correspond to a failure rate only, etc.

Basically, SILs are recommended to be applied to functions e.g. safety functions which are fulfilled by safety related systems. Functions are aimed to be free of specific technical solutions and therefore be assumed to be open for different suppliers. In this regard, the application guideline of EN 50129 states:

For each safety function carried out by the system, it is necessary to define the safety requirements for that function along with the safety integrity level with which the function has to be designed and developed. **[5]**

For the derivation of SILs **[6]** suggests that SILs may evolve from a risk assessment which are later used in the system development process, see figure below.

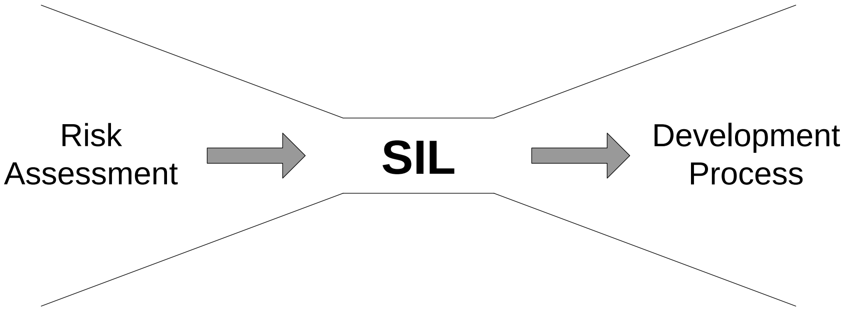


Figure 4 The 'Bowtie Diagram' showing the derivation and application of SIL [6]

It is possible to express the result of the risk assessment as a "desire" for a SIL, for example established by an operator, understanding SILs as intervals of THR values to which specific sets of measures, tools and techniques are assigned, which are believed to achieve the intended safety target. The development process might be understood as a "prediction" of the level of safety integrity, for instance claimed by a supplier. For an example, see figure below.

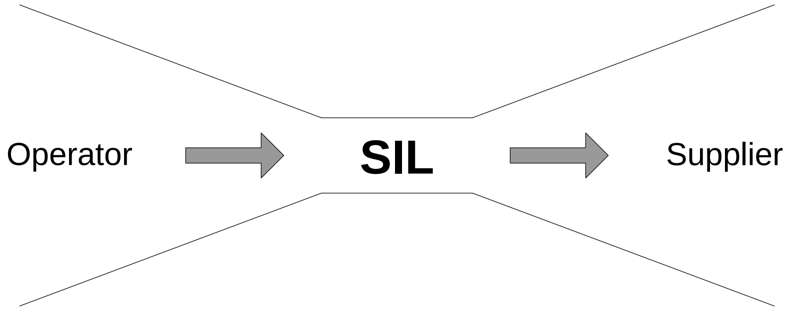


Figure 5 'Bowtie Diagram' – Example of main responsibilities considering [3]

At the 'knot' of the 'bowtie' diagram CENELEC standards recommend the use of tolerable hazard rates (THR) rather than SILs.

But following the example of a distinction between operators and suppliers, the following tasks may originate:

The operator may perform:

- Overall system functional requirements
- Overall system safety requirements (including safety targets and preliminary hazards identification)

The supplier may perform:

- Detailed functional and technical design
- Detailed hazard identification (coming from design)
- Risk assessment
- Derive SILs for safety functions
- Etc.

By postulating this approach of SILs, a core task arises on the correct and exhaustive definition of safety functions which are able to cover all identified hazards. This process may be assisted by the use of tools like a hazard log.

Matters like the decomposition of SILs from function to sub-systems, is often recommended to be within the responsibility of the system supplier.

But what are SILs; considering the required level of safety integrity for a particular system. In **[7]** a recommendation can be found:

Generally, safety relies on adequate measures to prevent or tolerate faults (as safeguards against systematic failure) as well as on adequate measures to control random failures. In this sense, safety integrity means that the qualitative measures (to avoid systematic failures) should be balanced with the quantitative targets (to control random failures) **[7]**.

This is summarised in the following figure, as safety integrity for a safety related function is influenced by three items, see figure below.

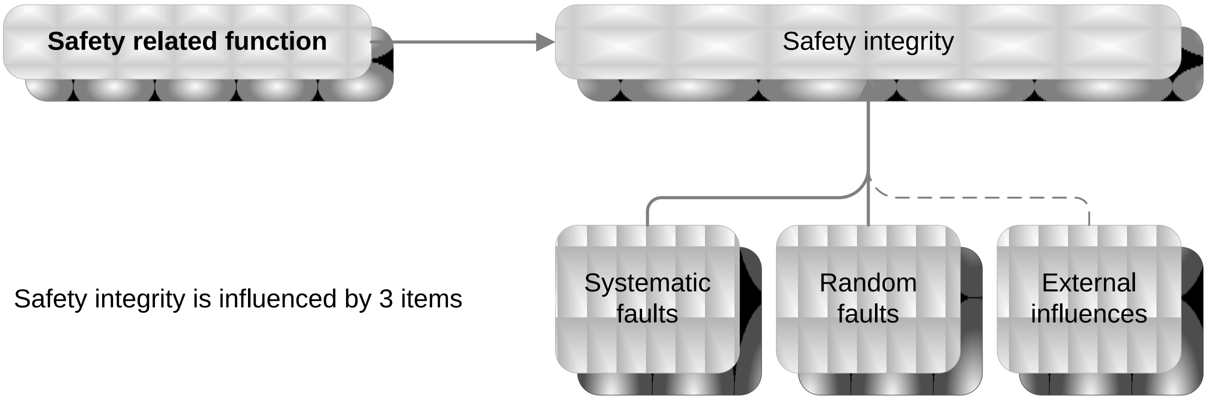


Figure 6 Factors influencing safety integrity according to [7]

Additionally, CLC/TR 50451 states: *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.* **[8]**

For an actual application EN 50129 gives the recommendation: *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.* Recommendations which tools and techniques can be used for a target SIL can be found in the annexes of EN 50129.

In his article about “Understanding the use, misuse and abuse of safety integrity levels” Felix Redmill concludes:

In essence, the SIL principle is this. If something is to do an important job, it needs to be reliable, and the more important the job, the more reliable it should be. Thus, there is an inverse relationship between the SIL and the tolerable rate of (dangerous) failures. In the case of a safety-related system, the job is to achieve safety, and the greater the importance to safety of the system whose SIL is under consideration, the lower the rate of unsafe failures should be. Then, the higher the SIL must be so as to indicate this requirement. **[6]**

The relations between safety functions and safety systems (performing these functions) are analysed in MODSafe WP5 in more detail.

6. Allocation of safety requirements in standards and guidelines

This clause aims at describing different standards and guidelines which can be applied for SIL allocation. International, European and national standards are delineated. Standards are selected which are dedicated to and used in the railway and urban guided railway domain.

6.1 International standards

6.1.1 IEC 61508

This standard is titled “Functional safety of electrical/electronic/programmable electronic safety-related systems”. It is a generic international standard on functional safety, applicable in all industry sectors.

IEC 61508 uses the life cycle concept as a project framework and introduces the concept of discrete levels of safety integrity i.e. SILs. Applying SILs to safety-related systems, a risk based approach is recommended using techniques for hazard and risk analysis.

To establish safety for systems, IEC 61508 uses a model which assumes that a system provides utility and risk by “equipment under control” (EUC) together with a “control system” for the EUC, see figure below.

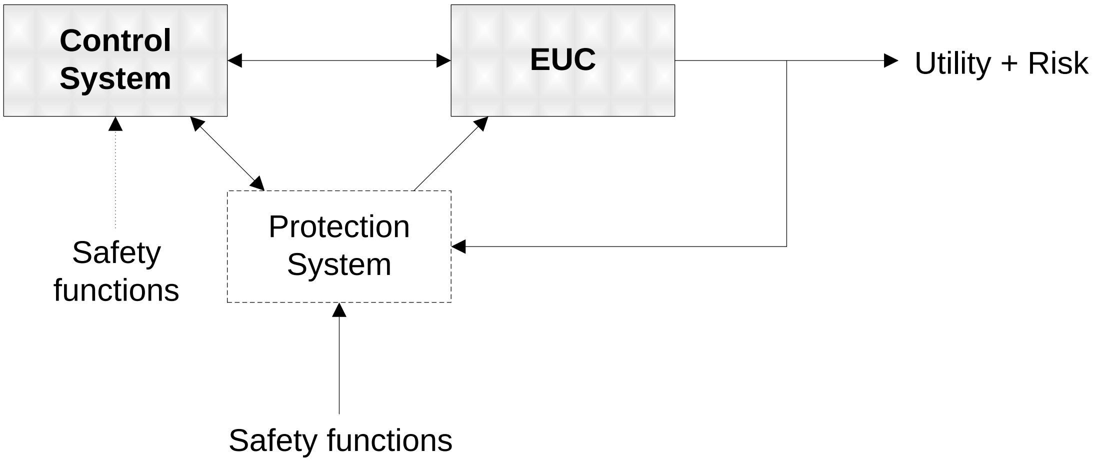


Figure 7 IEC 61508 system model according to [6]

To manage risks IEC 61508 recommends a risk assessment of EUC and control system. Hence, risk is posed by EUC and the control system, whereas the control system or protection systems may perform safety functions.

Regarding the safety function which may reduce the risk to an acceptable level, IEC 61508-1 states: *“Each safety function, with its associated safety integrity requirement developed according to 7.5, shall be allocated to the designated E/E/PE safety-related systems, taking* *into account the risk reductions achieved by the other technology safety-related systems and external risk reduction facilities, so the necessary risk reduction for that safety function is achieved*[1]*.* **[9]**

With respect to actual methods for a SIL allocation, IEC 61508 provides part 5 which is called “Examples of methods for the determination of safety integrity levels”. It comprises examples on qualitative and quantitative methods.

Qualitative approach for determination of SIL

One method is the risk graph to determine SILs for safety-related systems performing safety functions. Assuming that risk can be assessed with the knowledge of the risk posed by EUC and its control system, risk can be estimated with:

R = f x C

where:

***R** – is the risk with no safety-related systems in place*

***f** – is the frequency of the hazardous event with no safety-related systems in place;*

***C** – is the consequence of the hazardous event (the consequences could be related to harm associated with health and safety or harm from environmental damage).* **[10]**

Deduced from the above formula, the following four parameters may be used to describe risk qualitatively and can be found in the risk graph, see figure below.

C – consequences of the hazardous event

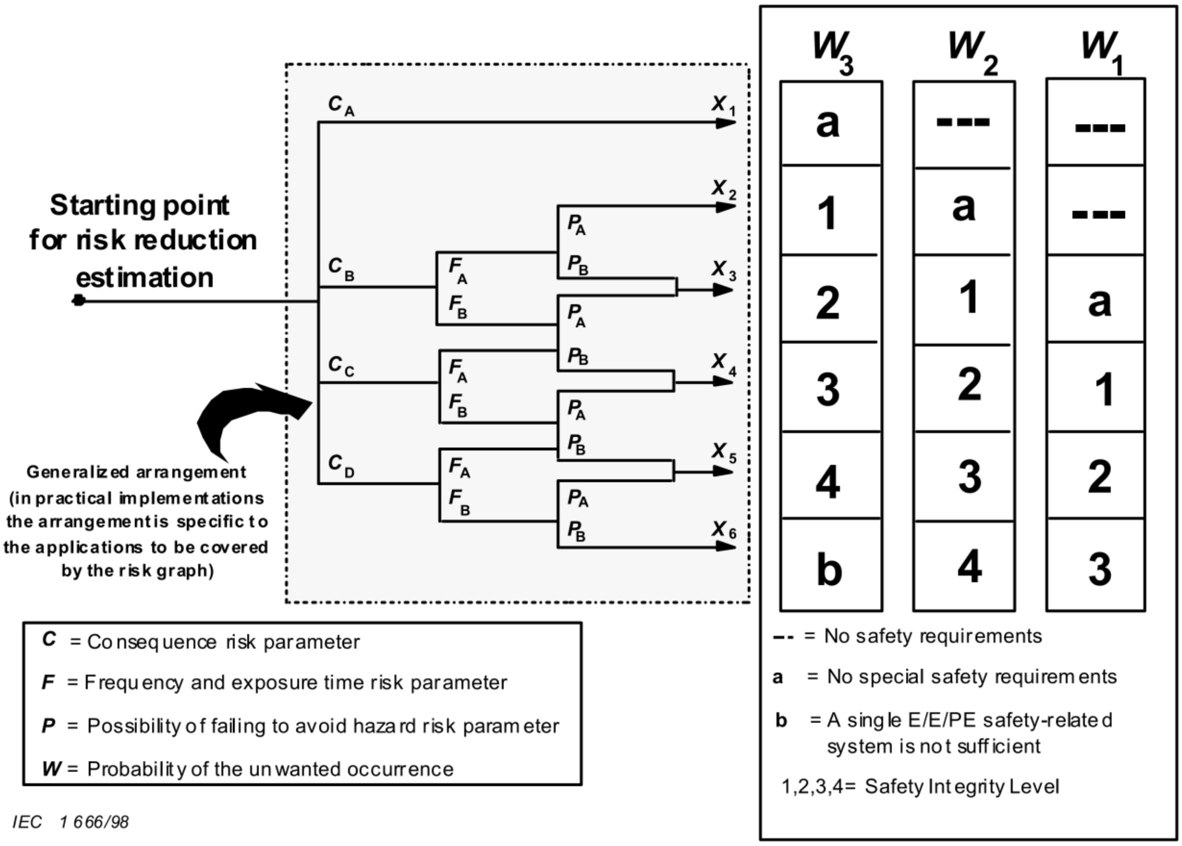
F – frequency of, and exposure time in, the hazardous zone

P – possibility of failing to avoid the hazardous event

W – probability of the unwanted occurrence

Regarding to Figure 8; beginning with the starting point, an evaluation of safety-related system may be performed by an estimation of the risk parameter and following the according line from the left to the right hand side. The required SIL for the safety related-system is indicated by one out of four levels.

[1] For more detailed information see the article by Braband, vom Hövel and Schäbe **[27]** which addresses the concept of probability of failures on demand, as used in IEC 61508.


Starting point for risk reduction estimation
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B
X_1
X_2
X_3
X_4
X_5
X_6
IEC 1 666/98

W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

C = Consequence risk parameter

F = Frequency and exposure time risk parameter

P = Possibility of failing to avoid hazard risk parameter

W = Probability of the unwanted occurrence

-- = No safety requirements

a = No special safety requirements

b = A single E/E/PE safety-related system is not sufficient

1,2,3,4= Safety Integrity Level

Figure 8 Risk graph: general scheme according to IEC 61508-5

Quantitative approach for determination of SIL:

A concept for performing a quantitative analysis which yields numerical values is outlined in the figure below.

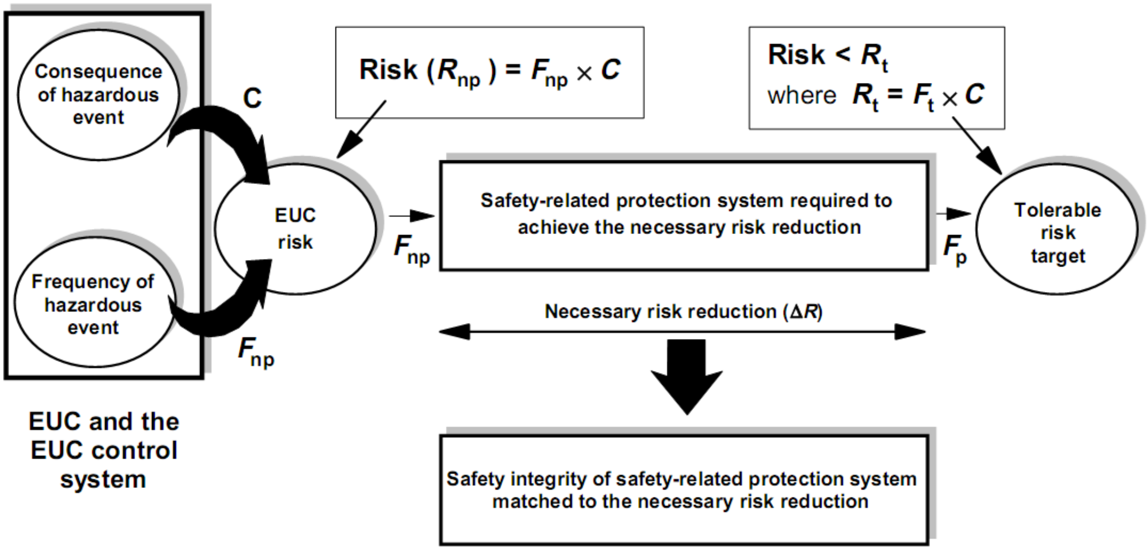

Consequence of hazardous event
Frequency of hazardous event
EUC and the EUC control system
C
F_{np}
EUC risk
Risk (R_{np}) = $F_{np} \times C$
Risk < R_t where $R_t = F_t \times C$
Safety-related protection system required to achieve the necessary risk reduction
F_{np}
F_p
Tolerable risk target
Necessary risk reduction (ΔR)
Safety integrity of safety-related protection system matched to the necessary risk reduction

Figure 9 Example for safety related protection system [10]

Consequences and frequencies of hazardous events may be calculated by applying quantitative methods to calculate the risk of EUC. (Even though, it is not explicitly mentioned, analysis techniques like fault or event trees may be applied.)

Comparing the frequency without any protection (F_{np}) to the target frequency contributing to the tolerable risk target (F_t), ΔR can be determined. ΔR can be understood as the necessary risk reduction, which, in turn, can be used to translate this numerical value into a SIL. This can be done by applying one or the two tables below; assuming ΔR is something like the target failure measure.

IEC 61508-4 differentiates between two concepts; on the one hand for “low demand mode of operation” (i.e. the safety-related system is required to perform its function less than once a year). On the other hand, a concept for “high demand or continuous mode of operation” may be used, if the safety function is used more than once a year e.g. continuously.[2]

While the concept of high demand or continuous functions is intuitively clear (solicited at all times, failure leads to immediate safety problems) the concept of low demand is more complex, since it involves besides a relatively rare rate of a potentially hazardous event also the probability that the system is in a noticed or unnoticed failure state at time of solicitation and it involves the concept of inspection or repair intervals to restore the failed component.[3]

IEC 61508-4 defines the low demand mode: *where the frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof-test frequency* **[11]**.

So, in fact it is not directly one single rate that interacts; but rather three rates. To account for this observation IEC 61508 offers a second definition of when low demand shall be assumed: whenever the rate of inspection or repair exceeds the rate of a potential solicitation of this function in a hazardous situation by a factor of 100 the low demand mode shall be assumed (cf. IEC 61508-2 **[12]**).

IEC 61508 quantification approaches are based largely on probabilistic considerations (cf. Annexes of part 5 and part 7). A number of methods are advocated also by the standard, in particular Markov models, (cf. part 6 **[13]** and part 7 **[14]**) to calculate specific probabilities and rates. For the low demand (or on demand) mode of safety functions, the MODSafe projects considers in a later deliverable appropriate calculations and examples.

[2] The second edition of IEC 61508 will distinguish between three different modes of operation, in comparison to edition one. More details are addressed in MODSafe deliverable 4.2 and 4.3.

[3] Specific aspects will be addressed in the MODSafe deliverable 4.3 and **[27]**.

Table 1 Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation [9]

Low demand mode of operation (Average probability of failure to perform its design function on demand)	**Safety integrity level (SIL)**
≥ 10^{-5} to < 10^{-4}	**4**
≥ 10^{-4} to < 10^{-3}	**3**
≥ 10^{-3} to < 10^{-2}	**2**
≥ 10^{-2} to < 10^{-1}	**1**

Table 2 Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation [9]

High demand or continuous mode of operation (Probability of a dangerous failure per hour)	**Safety integrity level (SIL)**
≥ 10^{-9} to < 10^{-8}	**4**
≥ 10^{-8} to < 10^{-7}	**3**
≥ 10^{-7} to < 10^{-6}	**2**
≥ 10^{-6} to < 10^{-5}	**1**

6.1.2 IEEE 1474

The title of this standard is “1474.1 IEEE Standard for Communications- Based Train Control (CBTC) Performance and Functional Requirements” and is recognised as an American national standard (see **[15]**). It describes general requirements on CBTC systems as well as performance and functional requirements.

For this deliverable the standard might be of particular interest since CBTC systems can be found more and more in the European urban rail sector.

The standard does not recommend a particular method for SIL allocation, though; it describes general requirements on safety for CBTC systems, which might be concluded as follows:

- Hazard identification
- Risk assessment to assess hazard likelihood and severity
- Design and implementation of vital functions to control hazards
- Vital function shall be implemented in accordance with fail safe principles
- Concept of Mean Time Between Hazardous Events (MTBHE) is used

- Documentation necessary to demonstrate that requirements and MTBHE have been met
- Total calculated aggregated mean time between hazardous event - MTBHE (total of all critical and catastrophic hazards) shall be at least 10^9 per hour.

6.2 European standards

6.2.1 EN 50126

The title of the European Standard EN 50126 (or IEC 62278) is “Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)”. The standard is a sector specific adaptation of IEC 61508. It defines the RAMS parameter and delineates a concept of a life cycle as project framework in the railway industry sector (see Figure 2).

Of particular interest is the concept of risk. Risk is described as a combination of two elements:

- *the probability of occurrence of an event or combination of events leading to a hazard, or frequency of such occurrences;*
- *the consequences of the hazard.* **[3]**

The risk parameter frequency of occurrence, severity of consequences and level of risk are described qualitatively and combined in a “Frequency – Consequence Matrix” also known as “Risk Matrix”, see table below.”

Table 3 Example of risk matrix according to EN 50126

Frequency of occurrence of a hazardous event	**Risk Levels**			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity Levels of Hazard Consequence			

In this example of the risk matrix, risk would be e.g. “Tolerable” if the “Severity Levels of Hazard Consequences” are “Critical” but the “Frequency of occurrence of a hazardous event” is “Improbable”.

Concerning SIL allocation methods, EN 50126 does not propose a particular method. However, it recommends a performance of a risk analysis before setting safety requirements, as explained in phase three of the system life cycle. Furthermore, it outlines a SIL concept and advises user on how to use the SIL concept.

Moreover, an application guide is provided, called CLC/TR 50126-2 “Railway Applications – The Specification and Demonstration of RAMS Part 2: Guide to the application of EN 50126 for safety”, which provides extended explanation on the SIL conception with respect to its use and misuse.

In clause six of the application guide, the SIL conception is described in more detail, containing a list of remarks for the usage of SILs. For example, it recommends a *Structured approach to allocation of SI* (safety integrity) **[7]**. This procedure is basically a quantitative approach to calculate THRs with techniques like the recommended cause-consequence diagrams and fault tree analyses. In particular the following steps may be followed:

- System definition
- Hazard identification at system level
- Consequence analysis
- Risk tolerability assessment at system level (which yields system hazards and associated THRs)
- System level safety requirements
- System design
- Causal analysis
- Sub system level safety requirements specification
- SI requirements Categorisation (which yield sub-system functional requirements with their associated SIL using the THR/SIL table)
- Optional: consolidation of SIL allocation

It has to be noted that risk analysis shall be repeated on each defined system level during life-cycle process and take into account hazards to be identified on each system level (e.g. top level: hazards arising from train operation; system level: hazards arising from a technical system or subsystem).

6.2.2 EN 50129

The EN 50129 is called “Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling”. It recommends conditions for safety acceptance and approval. The standard is in accordance with EN 50126, i.e. it applies the same understanding of the life cycle and risk.

EN 50129 does not recommend an explicit method for SIL derivation. However, it introduces the concept of tolerable hazard rates (THR) which are recommended to be applied to the identified hazards.

The THRs can be understood as a quantified safety target i.e. a target measure with respect to systematic and random failures. The calculation of THRs is recommended to be the responsibility of the operator.

For the derivation of THRs for hazards, the standard provides a general process. This process is divided into two parts. The upper part shall be in the responsibility of the railway authority (e.g. the railway operating company). It is called “Risk Analysis” and shall produce the THRs for hazards, according to its consequences. The system supplier shall be in charge of the second part of the process, “Hazard Control”, analyse hazard causes to finally allocate SILs. The overall process shall be subject to approval of the safety authority.

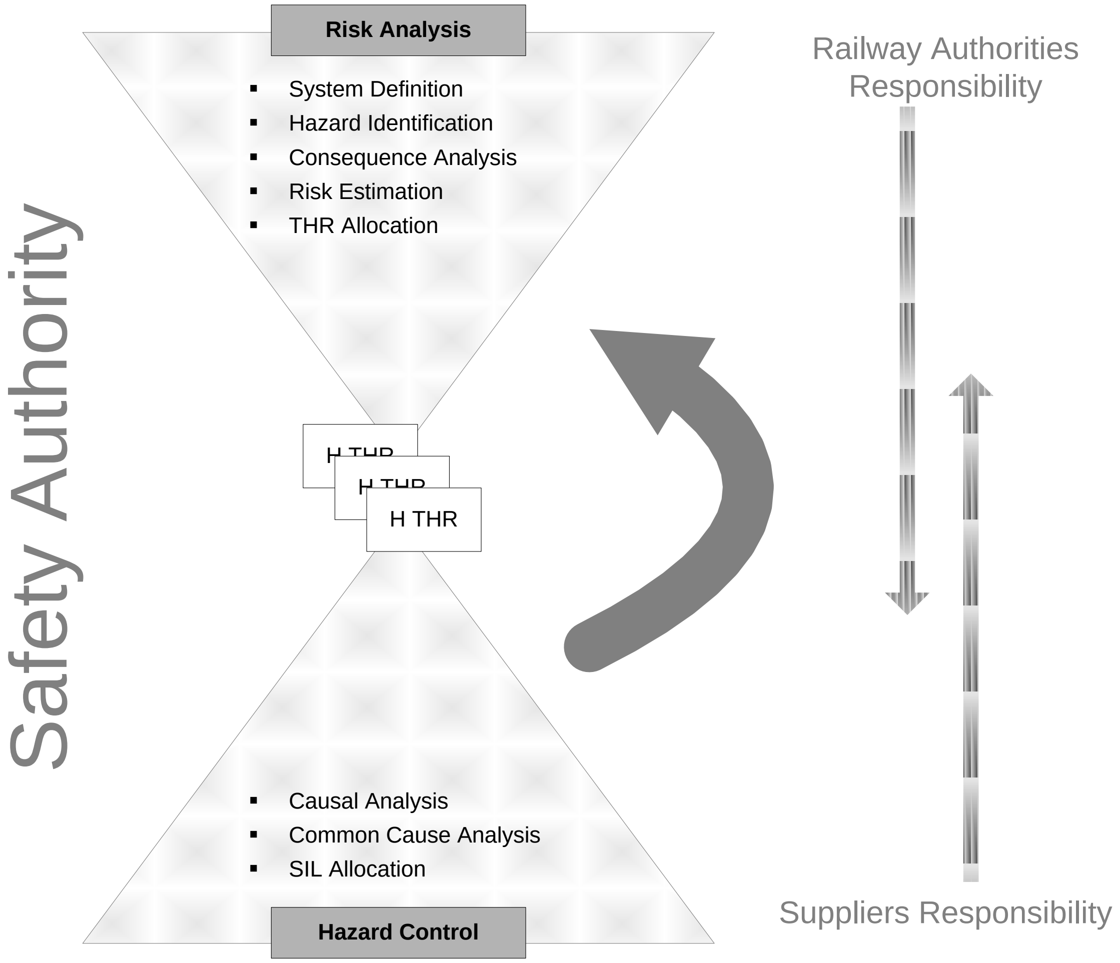


Figure 10 Global process overview according to EN 50129

For the actual allocation of tolerable hazard rates it is recommended:

- *To analyse the consequences, i.e. losses,*
- *To define the risk tolerability criteria,*

- *To derive the tolerable hazard rates, and*
- *To ensure that the residual risk is tolerable (with respect to the appropriate risk tolerability criteria)* **[16]**

Moreover, methods for an allocation THRs are recommended:

- To estimate risk explicitly
- To use statistical or analytical methods to derive THRs form reference systems or by relevant code of practices
- To apply alternative quantitative methods to derive THRs for hazards.

For a final allocation of safety integrity levels EN 50129 provides a table, suggesting a link between THRs and SILs. It is constructed according to IEC 61508, leaving out the on-demand mode of operation (see Table 4).

The standard states that *The SIL table is applicable to safety related functions or sub-systems implementing one or more of these functions.* **[16]**

Table 4 THR and SIL table according to EN 50129

Tolerable hazard rate (THR) per hour and per function	Safety integrity level (SIL)
$10^{-9} \leq$ THR $< 10^{-8}$	**4**
$10^{-8} \leq$ THR $< 10^{-7}$	**3**
$10^{-7} \leq$ THR $< 10^{-6}$	**2**
$10^{-6} \leq$ THR $< 10^{-5}$	**1**

Functions demanding a THR lower than 10^{-9} per hour and function shall be treated as follows:

- *If it is possible to divide the function into functionally independent sub-functions, the THR can be split between those sub-functions and a SIL assigned to each sub-function;*
- *If the function cannot be divided, the measures and methods required for SIL 4 shall, at least, be fulfilled and the function shall be used in combination with other technical or operational measures in order to achieve the necessary THR* **[16]**

6.2.3 CLC/TR 50451

This technical report is entitled “Railway applications – Systematic allocation of safety integrity requirements”. It describes a systematic methodology to determine safety integrity requirements and is in line with the European standards EN 50126 and EN 50129. Basis of this report is the “global process” (see Figure 10) defining an interface between task and responsibilities of operator, system supplier and safety authority.

For a derivation of safety requirements, CLC/TR 50451 uses the concept of tolerable hazard rates (THR). It suggests calculating THRs:

Derived from arguments like GAMAB by operational and performance statistics (instead of consequence analysis) or by system design analysis of equipment in use **[8]**.

In particular a THR calculation may be performed qualitatively or quantitatively.

Qualitative THR determination

Firstly, after a phase of hazard identification, the hazard likelihood and consequences shall be estimated. To rank the evolving risk a calibrated risk matrix may be used. (It is recommended to use decade scales for the risk matrix.) The calibration follows the assumptions that the term “Frequent” for the hazard frequency corresponds to one event in ten hours. For the severity of hazard consequences it is assumed that one fatality would correspond to ten major injuries which would be equal to 100 minor injuries. Additionally, the number of passenger exposed to the hazard might be considered. In this case e.g. 100 exposed passengers would be equal to a normalising factor of 0,01. However, this risk matrix does not propose any risk tolerability criteria. The following table summarises the assumptions in the frequency – consequence matrix.

The numerical values of the “Total Risk Level” can be interpreted as total risk per hazard i.e. the total hourly risk in fatality per hour. (Motivations for the numerical values of the risk parameter as well as an interpretation of the Total Risk Levels are not given in the technical report.)

Table 5 Example of a calibrated frequency – consequence matrix [8]

Frequency of occurrence of a hazardous event		**Total 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			

The actual estimation of a THR for particular hazards may be done using the individual risk of fatality (IRF) and a target individual risk (TIR) i.e. the tolerability limit.

For illustration an example can be given.

For a hazard which is estimated to occur with a remote frequency and hazard consequences which can be assumed to be marginal, the Total Risk Level would be 10^{-5}.

→ Total Risk Level = 10^{-5} (total risk of fatality per hour, considering the hazard occurs remote and is marginal)

Subsequently, this value shall be normalised according to the number of passenger exposed to the hazard in order to derive the individual risk of fatality (IRF). In this example 100 passenger are exposed to the hazard, which would correspond to a normalising factor of 10^{-2}. (1 000 passenger would be equal to 10^{-3}).[4]

→ IRF = 10^{-5} x 10^{-2} = 10^{-7} (IRF = Total Risk Level x Normalising Factor). If the numerical values for IRF and the target individual risk (TIR) differ, a scaling factor S shall be calculated by:

→ S= TIR / IRF

Finally, a THR for the particular hazard may be derived by:

→ THR = HR x S (HR = hazard rate of the particular hazard, S = scaling factor).

The approach can be summarised in the following figure:

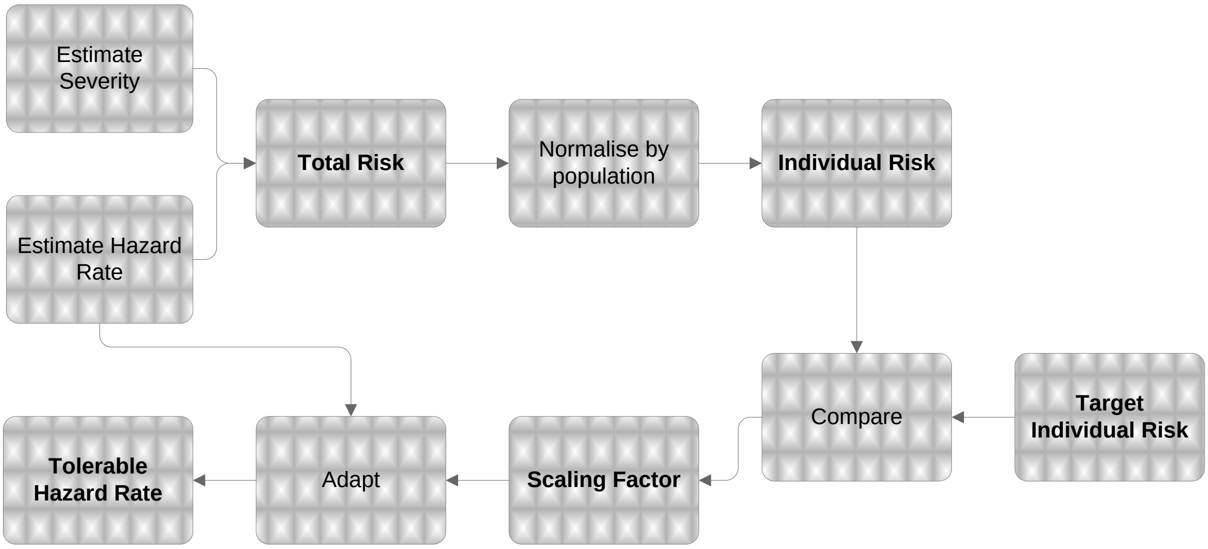


Figure 11 Overview of the qualitative hazard rate estimation [8]

[4] However, questions remain about the individual risk of fatality and its according normalising factor. It seems to be misleading that if more passengers are involved in a hazard this would lead to a declining individual risk of fatality. For example, if a train is entangled in a derailment or train collision; all passengers onboard of the train are exposed to the hazard consequences and the probability of a single fatality would not decline if more passengers are onboard.

Quantitative THR determination:

This approach uses a formula for the calculation of the individual risk of fatality (see formula (1)). One example of a formula uses parameters which are explained in the table below.[5]

$$(1) \qquad IRF_i = \sum_{H_j} \left(\left[N_i \times \left(HR_j \times D_j \right) + HR_j \times \left(N_i \times E_{ij} \right) \right] \sum_{A_k} C_j^k \times F_i^k \right)$$

Explanation on the example formula:

- Square brackets – first summand ($N_i \times \left(HR_j \times D_j \right)$): event rate with probability that a hazardous state already exists
- Square brackets – second summand ($HR_j \times \left(N_i \times E_{ij} \right)$): hazard rate under the individual exposure probability.
- Last summand can be understood as a kind of risk reduction factor

Table 6 Parameter for calculation of individual risk

Abbreviation	Definition
IRF_i	Individual risk of fatality of i
i	Individual using system
N_i	Number of uses (per year or per hour)
E_i	Exposure per use
H_j	Hazard j
HR_j	Rate of Hazard j
D_j	Duration of Hazard j
E_{ij}	Exposure time of individual i to hazard j
C_j^k	Consequence probability of hazard j and accident k
A_k	Accident type k
F_i^k	Probability of fatality for a single fatality in accident k

It can be assumed that the transformation of IRF to THR can be done in the same way as for the qualitative approach, see above.

As a framework an example of a risk analysis process is presented. With a system definition, according hazards, accidents and risks the individual risk can be calculated. Subsequently,

[5] This formula provides arguments to accept higher hazard rates for a system in an amusement park than for a commuter system. The higher hazard rate is compensated by the lower number of times the individual user is using the system.

the individual risks are compared to the tolerated individual risk. If the resulting risk is not acceptable, barriers have to be introduced to the system. These barriers are recommended to be of the particular strength in terms of the gap between TIR and IRF.

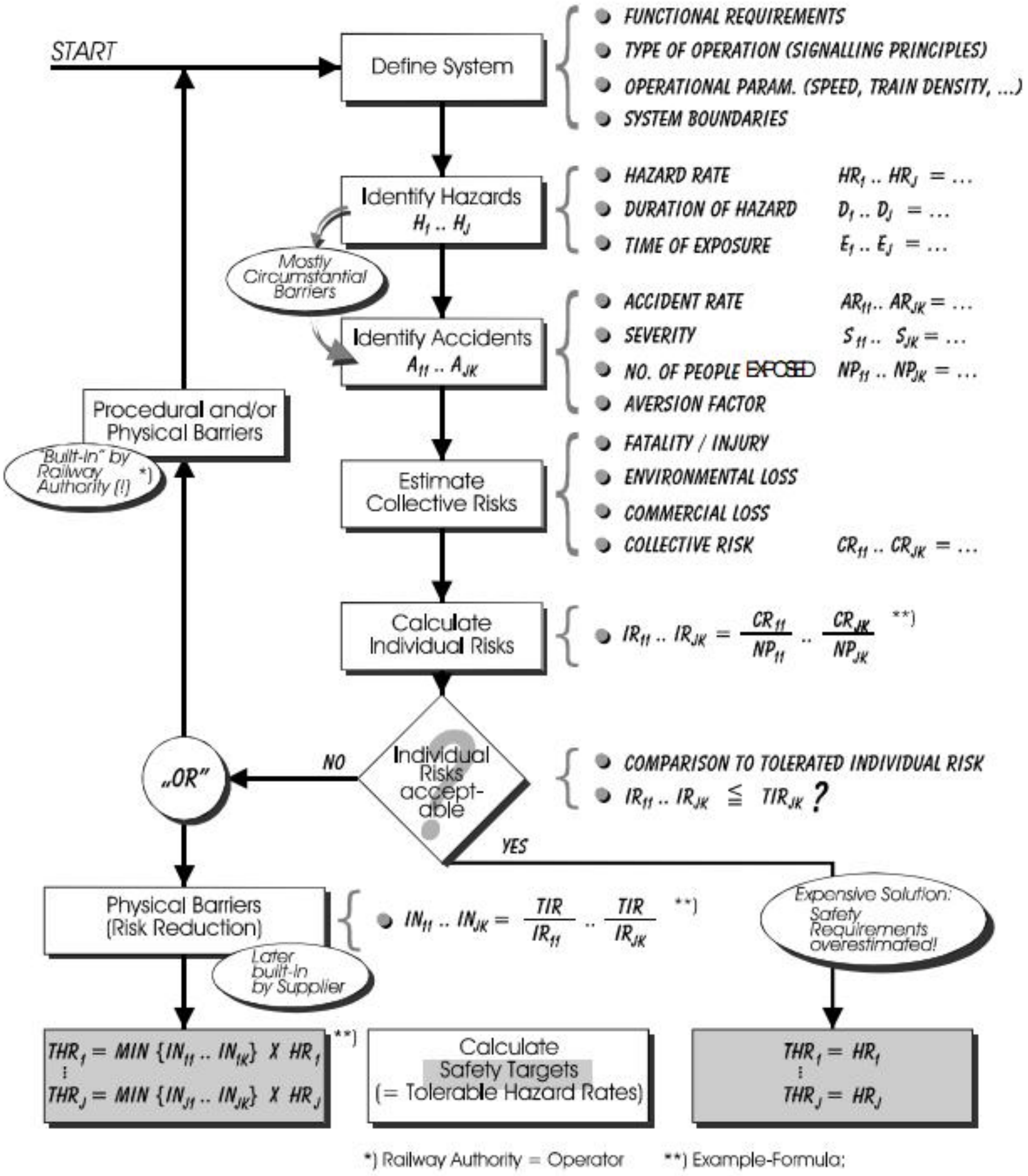

START
Define System
FUNCTIONAL REQUIREMENTS
TYPE OF OPERATION (SIGNALLING PRINCIPLES)
OPERATIONAL PARAM. (SPEED, TRAIN DENSITY, ...)
SYSTEM BOUNDARIES
Identify Hazards H_1 .. H_J
HAZARD RATE HR_1 .. HR_J = ...
DURATION OF HAZARD D_1 .. D_J = ...
TIME OF EXPOSURE E_1 .. E_J = ...
Mostly Circumstantial Barriers
Identify Accidents A_{11} .. A_{JK}
ACCIDENT RATE AR_{11}.. AR_{JK} = ...
SEVERITY S_{11} .. S_{JK} = ...
NO. OF PEOPLE EXPOSED NP_{11} .. NP_{JK} = ...
AVERSION FACTOR
Procedural and/or Physical Barriers
"Built-in" by Railway Authority (!) *)
Estimate Collective Risks
FATALITY / INJURY
ENVIRONMENTAL LOSS
COMMERCIAL LOSS
COLLECTIVE RISK CR_{11} .. CR_{JK} = ...
Calculate Individual Risks
IR_{11} .. IR_{JK} = $\frac{CR_{11}}{NP_{11}}$ .. $\frac{CR_{JK}}{NP_{JK}}$ **)
„OR"
NO
Individual Risks accept-able ?
YES
COMPARISON TO TOLERATED INDIVIDUAL RISK
IR_{11} .. IR_{JK} ≦ TIR_{JK} ?
Physical Barriers (Risk Reduction)
IN_{11} .. IN_{JK} = $\frac{TIR}{IR_{11}}$ .. $\frac{TIR}{IR_{JK}}$ **)
Later built-in by Supplier
Expensive Solution: Safety Requirements overestimated!
THR_1 = MIN {IN_{11} .. IN_{1K}} X HR_1 ⋮ THR_J = MIN {IN_{J1} .. IN_{JK}} X HR_J **)
Calculate Safety Targets (= Tolerable Hazard Rates)
THR_1 = HR_1 ⋮ THR_J = HR_J
*) Railway Authority = Operator
**) Example-Formula:

Figure 12 Example risk analysis process according to CLC/TR 50451

6.2.4 ERA – Common Safety Methods

In the ERA (European Railway Agency) recommendations called "Recommendation on the first set of Common Safety Methods (ERA-REC-02-2007-SAF)" **[17]** a framework is given on risk management. These recommendations were transformed into the EU Directive No. 352/2009 and therefore have been European compulsory legislation since 2009 **[25]**. The regulation shall be applied to railway systems of the European member states. *This Regulation shall not apply to: (a) metros, trams and other light rail systems* **[25]**. Further limitations on private, separated or heritage railway systems can be found in article 2(3) of **[25]**. But, since it applies to railway systems it is worth describing the risk management framework for MODSafe purposes. It does not recommend an explicit method for the allocation of safety requirements for safety measures. However, a framework is set on how safety measures fulfilling safety requirements can be derived.

After a phase of hazard identification, an expert judgement is performed on whether risk is broadly acceptable. Safety requirements shall be set for a particular hazard choosing one out of three approaches:

1. If the hazard can be treated according to a code of practice and the according risk would be acceptable, safety requirements for safety measures can be set.
2. Safety requirements can be taken over from a reference system to be applied to the new system under consideration.
3. Hazard shall be covered with safety function. Subsequently, risk shall be estimated either qualitatively of quantitatively (estimation of frequency and severity). If the resulting risk is acceptable safety requirements can be set. Furthermore, it is stated: *For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.* **[25]**

If risk is not acceptable, safety measures shall be implemented in order to cover hazards.

The following figure summarises the commission regulation No 352/2009, see **[25]**.

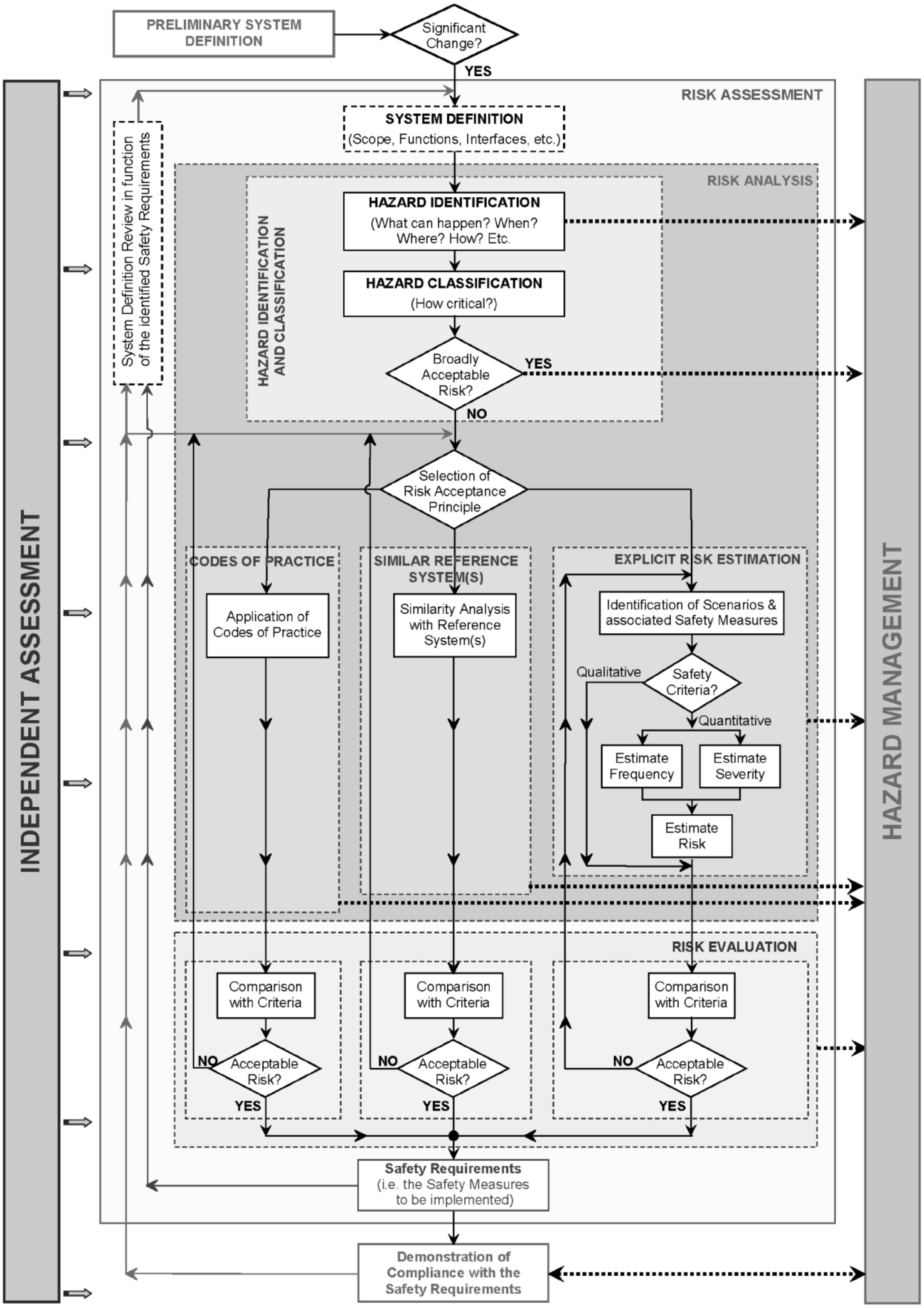

PRELIMINARY SYSTEM DEFINITION
Significant Change?
YES
RISK ASSESSMENT
SYSTEM DEFINITION (Scope, Functions, Interfaces, etc.)
System Definition Review in function of the identified Safety Requirements
RISK ANALYSIS
HAZARD IDENTIFICATION AND CLASSIFICATION
HAZARD IDENTIFICATION (What can happen? When? Where? How? Etc.
HAZARD CLASSIFICATION (How critical?)
Broadly Acceptable Risk?
YES
NO
Selection of Risk Acceptance Principle
CODES OF PRACTICE
SIMILAR REFERENCE SYSTEM(S)
EXPLICIT RISK ESTIMATION
Application of Codes of Practice
Similarity Analysis with Reference System(s)
Identification of Scenarios & associated Safety Measures
Qualitative
Safety Criteria?
Quantitative
Estimate Frequency
Estimate Severity
Estimate Risk
RISK EVALUATION
Comparison with Criteria
Acceptable Risk?
NO
YES
Safety Requirements (i.e. the Safety Measures to be implemented)
Demonstration of Compliance with the Safety Requirements
INDEPENDENT ASSESSMENT
HAZARD MANAGEMENT

Figure 13 Risk management process and independent assessment [25]

6.3 National standards

6.3.1 The Yellow Book – Engineering Safety Management (UK)

The so-called Yellow Book (according to the colour of the book cover) is a guideline for engineering safety management in the railway domain. It is published by the Rail Safety and Standards Board on behalf of the UK rail industry. It states that: *The Yellow Book is written to help you set up a process that protects you and others from mistakes and gives documented evidence (such as a safety case) that risk is at an acceptable level*. **[18]** In other words, it sets guidance on how to achieve, maintain and justify safety for railway projects. The Yellow Book can be assumed to be good practice and is used in Great Britain.

For the allocation of safety integrity requirements clause 17 gives guidance, which is about “Reducing risk; Safety requirements” It is recommended to set and meet safety requirements to control risk. In particular: *A project carrying out safety-related work should identify the hazards and accidents that may result from the work, assess the risk associated with these, control the risk to an acceptable level and set safety requirements to ensure this level of risk is met.* **[18]**

The Yellow Book recommends the use of safety integrity level (in the understanding of EN 50129) to meet safety integrity requirements i.e. safety targets. To set safety targets it is recommended:

If you set numerical safety targets, this is normally done by working from a fault tree (or similar representation of cause and effect logic) and the event probabilities to:

a) *Derive numerical accident target which conform to legal criteria for acceptable risk;*

b) *Derive hazard occurrence rate and/or unavailability targets which are consistent with (a);*

c) *If applicable, derive SILs for the system functions that are consistent with (b).* **[18]**

For an actual usage of the concept of SILs the Yellow Book states: *SILs are described in a number of widely-used standards, including EN50129:2003 and IEC 61508 and we recommend defining SILs for systems or parts of systems for which the guidance on SILs in such standards is applicable.* **[18]** However, no specific method is recommended for the allocation of SILs to functions.

But, in order to relate numerical values to actual SILs, these numerical safety targets for system functions may be expressed as “probability of failure on demand” or “dangerous failure rate per hour”. These safety targets (or tolerable hazard rates) may in turn be translated to safety integrity level, see table below.

Table 7 Safety Integrity Level according to Yellow Book [18]

Low Demand Mode of Operation (probability of failure on demand)	Continuous / High Demand mode of operation (Dangerous failure rate per hour)	Safety Integrity Level
≥ 10^{-5} to 10^{-4}	≥ 10^{-9} to 10^{-8}	**4**
≥ 10^{-4} to 10^{-3}	≥ 10^{-8} to 10^{-7}	**3**
≥ 10^{-3} to 10^{-2}	≥ 10^{-7} to 10^{-6}	**2**
≥ 10^{-2} to 10^{-1}	≥ 10^{-6} to 10^{-5}	**1**

After applying safety targets (or tolerable hazard rate) to functions, it is recommended to demonstrate that the tolerable hazard rate is within the Tolerability Region according to the ALARP principle. This demonstration may have an impact on the previously found safety target if no compliance can be demonstrated.

The following figure aims at summarising Yellow Book recommendations. After an identification of hazards and accidents the associated risk shall be assessed. Risks shall be controlled e.g. by safety functions. For the latter safety targets shall be set, which can be done by applying methods like event tree or fault tree analysis. Numerical values may be translated into SILs according to Table 7. Finally, it shall be checked whether the safety target complies with ALARP principles.

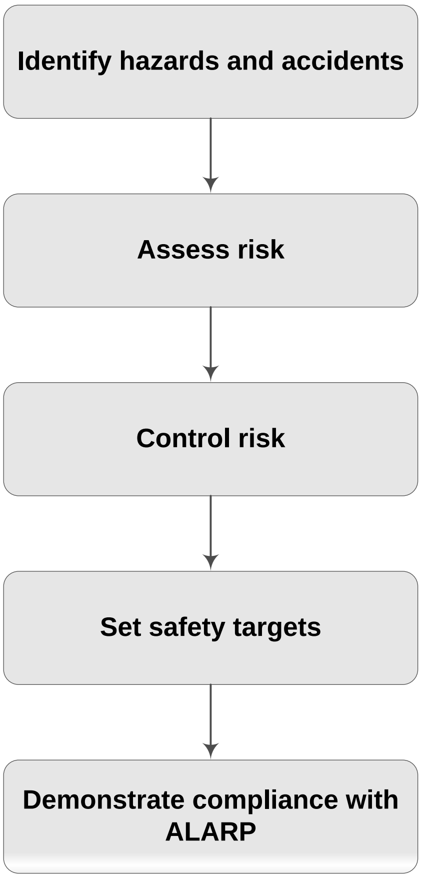

Identify hazards and accidents
Assess risk
Control risk
Set safety targets
Demonstrate compliance with ALARP

Figure 14 Possible interpretation of Yellow Book recommendation

Concerning responsibilities for performing the process for controlling risk and demonstrating compliance with legal obligations, the Yellow Book states that expertise is required on:

- *the system, its function and design; and*
- *the railway environment in which the system will run*. **[18]**

System knowledge can typically be found with the system suppliers. The railway environment is best known by the transport operator. Typically, it is the operator defining tolerable hazard rates.

6.3.2 TR SIG ZA and VDV 331 (Germany)

The TR SIG ZA (see **[19]**) are technical rules used in Germany. TR SIG ZA stands for „Zulassung und Abnahme von Signal- und Zugsicherungsanlagen gemäß BOStrab“, which can be translated as “Approval and acceptance of Signalling- and Train Control and Protection Systems according to BOStrab”. (The BOStrab are German Federal Regulations on the construction and operation of light rail transit systems). TR SIG ZA is developed in order to implement the use of the European standards EN 50126 and EN 50129, in reference to the German legislation (e.g. regarding the risk acceptance criteria and responsibilities of involved parties).

The legal status of the TR SIG ZA is that it is state of the art, accepted by safety regulatory authorities and therefore approved code of practice.

The TR SIG ZA applies to urban guided transit systems like metros, trams and light rail and shall be used for signalling and train control and protection systems. Therefore, it aims to be reliable and applicable rules for planning and predictability of legal decisions for operators[6], supplier and legal authorities.

For the field of railways, which are not owned by federal railway undertakings, there is an equivalent code of practice SIG RZA NE applicable to regional, suburban and industrial railways, regarding the specific railway laws of Germany.

For the description of how system approval and acceptance procedure shall be conducted TR SIG ZA follows strictly the system life-cycle concept mentioned in EN 50126. Furthermore, it uses the idea to differ between specific application, generic application or generic product, as described in EN 50129.

Therefore, TR SIG ZA is divided into a process to be conducted for specific applications and a process for type or product approvals which applies to generic applications and generic products. For a specific application the responsibilities are as follows:

According to TR SIG ZA (and EN 50126) the responsibility of the first four life cycle phases lies with the operator. This includes the concept, system definition, risk analysis and system requirements of the planed specific application. This shall be followed by an approval of plans by the legal authority (i.e. preliminary design) before construction and installation can be carried out by operator or the supplier.

Of particular interest is the phase for the risk analysis. TR SIG ZA provides guidance on how allocation of safety integrity requirements may be done.

Phase 3, which is about a risk analysis, requires:

- Identification of hazards
- Determination of requirement specification and safety functions
- Derivation of safety integrity requirements

The derivation of safety integrity requirements for safety functions shall be conducted as described in Figure 15 below.The allocation of SILs for a specific application shall be done in accordance with VDV 331 – "Sicherheitsintegritätsanforderungen für Signal- und Zugsicherungsanlagen gemäß BOStrab" (or VDV 332 „Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)" for use in railway

[6] Alternatively TR SIG ZA uses the term "Transport Authority" for operators.

environment according to SIG RZA NE). This is like “safety integrity requirements for signalling, train control and protection systems according to BOStrab” and can be understood as a generic base for the conduction of risk analyses and subsequent derivation of safety integrity requirements. VDV 331 is using the SIL concept with four discrete levels for safety integrity in reference to international standards IEC 61508, EN 50126, EN 50128 and EN 50129.

It has to be noted that there are additional VDV-Recommendations for other applications than signalling and train control and protection systems such as:

- VDV 399 “Requirements for Facilities Ensuring the Passengers’ Safety at Stations with Driverless Operation”
- VDV 161 Series “Sicherheitstechnische Anforderungen an die elektrische Ausrüstung von Stadt- und U-Bahn-Fahrzeugen” (Safety requirements for electrical equipment for metro and light-rail rolling stock) [26].

They all provide safety integrity requirements in a similar way.

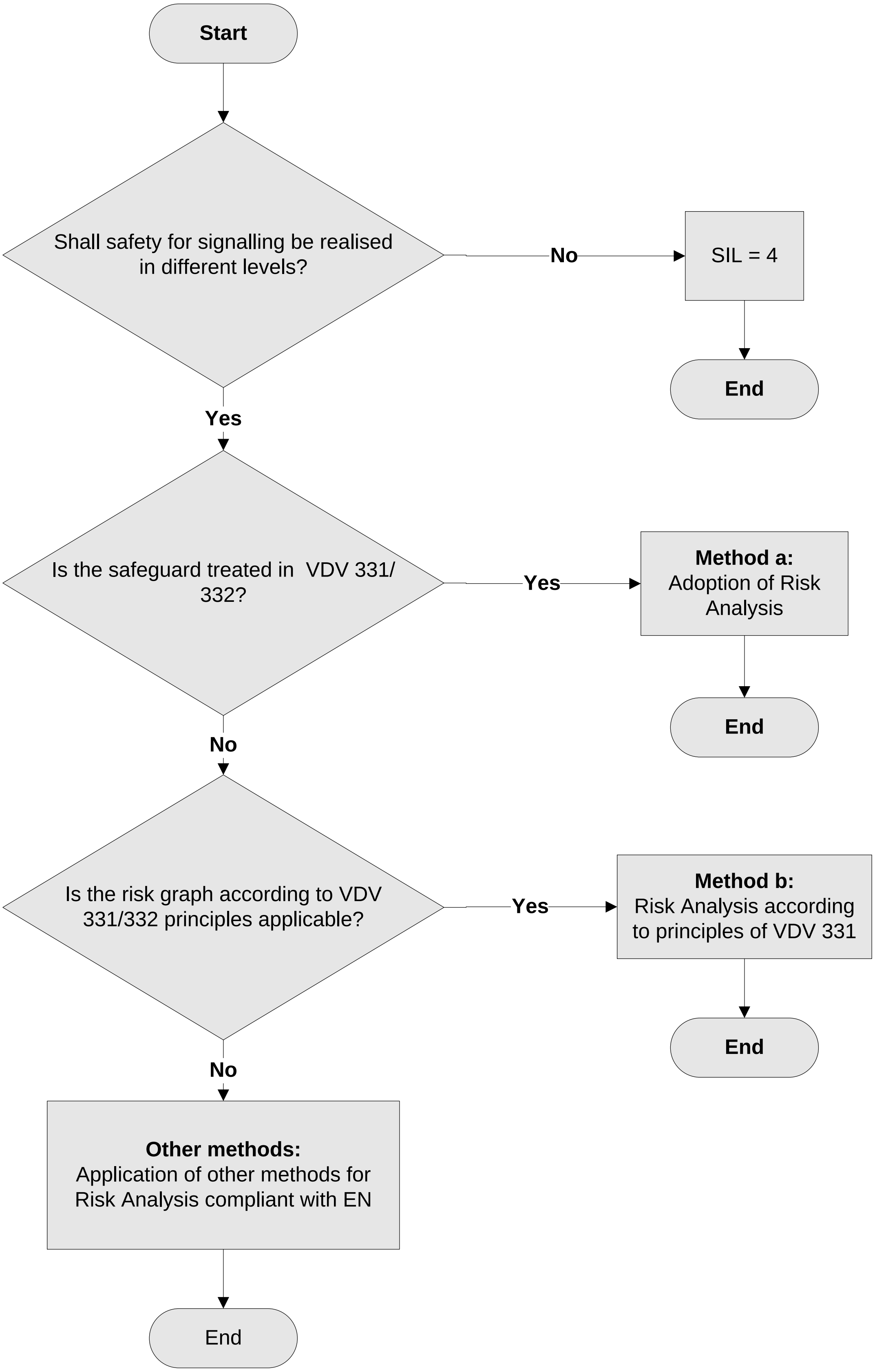

Start
Shall safety for signalling be realised in different levels?
No
SIL = 4
End
Yes
Is the safeguard treated in VDV 331/ 332?
Yes
Method a: Adoption of Risk Analysis
End
No
Is the risk graph according to VDV 331/332 principles applicable?
Yes
Method b: Risk Analysis according to principles of VDV 331
End
No
Other methods: Application of other methods for Risk Analysis compliant with EN
End

Figure 15 "Methods for allocation of safety integrity requirements" according to TR SIG ZA

According to TR SIG ZA and Figure 15; to assign SILs to safety function it shall be decided first whether to differentiate between different levels for safety integrity requirement. If all safety functions shall be built according to one level of safety integrity, SIL 4 shall be allocated to all safety functions of a determined system or sub-system.

If safety functions are to be analysed in more detail, it shall be checked whether the particular safeguard and its safety function is covered by VDV 331. If the function under analysis is mentioned in VDV 331 “Method A” shall be applied. This encompasses the use of previously performed risk analyses, already done in VDV 331 as state of the art for generic safety functions, with operational experience and for given conditions e.g. level crossings for trams.

If required safeguards and their safety functions are not sufficiently covered by VDV 331 a specific risk analysis is recommended according to the principles of VDV331 in order to derive SILs. This complies with “Method B”. The method shall be used e.g. for missing safety functions or safety functions to be used with differing operational contexts.

Alternatively, approaches derived from European standards which are divergent from “Method A” or “Method B” are permitted. However in this case, TR SIG ZA advises the use of the expected amount of data, needed for calculations and the justification of the risk acceptance criteria to legal authorities.

The SIL allocation shall be done according to the risk graph, depicted in Figure 16 below. (The risk graph is used for “Method a” and “Method b”, mentioned above.) The background of the risk graph is part 5 form IEC 61508.

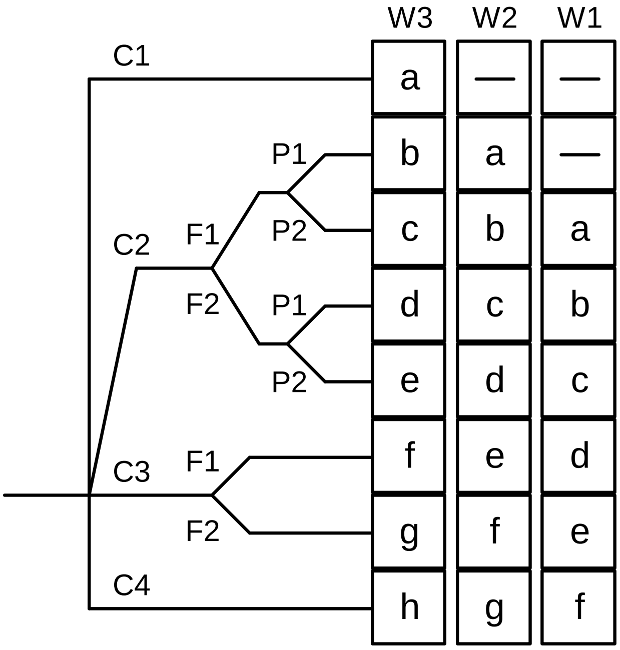


Figure 16 Risk graph – following VDV 331 [20]

The analysis follows the principles described in IEC 61508 (see sub-clause 6.1.1) calibrated within VDV331/332 to the process to be regarded. The safety function is analysed according to four attributes, which are:

- **C** – consequences of hazardous events
- **F** – frequency of, and exposure time in, the hazardous zone
- **P** – possibility of failing to avoid the hazardous event
- **W** – probability of the unwanted occurrence.

The result of the risk analysis provides a "Necessary minimum risk reduction" from which the safety integrity levels (SIL) can be derived directly. The connection between the results of the analysis for safety functions derived from the risk graph and safety integrity level are shown in Table 8.

Table 8 Risk reduction and SIL (example from IEC 61508 and used in VDV 331)

Tolerable Hazard Rate (THR)	Necessary minimum risk reduction	Safety integrity level
-	—	No safety requirements
-	A	No special safety requirements
$\geq 10^{-6}$ to $<10^{-5}$	b, c	1
$\geq 10^{-7}$ to $<10^{-6}$	D	2
$\geq 10^{-8}$ to $<10^{-7}$	e, f	3
$\geq 10^{-9}$ to $<10^{-8}$	G	4
-	H	An E/E/PE SRS is not sufficient

According to IEC 61508 the quantitative component ("Target Failure Measure (TFM)" which is equivalent to "Tolerable Hazard Rate (THR)") can be derived directly from the SIL.

TR SIG ZA stipulates furthermore the following steps necessary for approval and acceptance of a specific application for the live-cycle phases 5 to 9 (EN 50126) dealing with design and implementation according to legal environment of Germany. It takes into account the necessary documentation and the responsibilities of operator, safety regulatory authority as well as independent safety assessors for verification, validation and the overall approval process.

At last, TR SIG ZA stipulates the process and the responsibilities to maintain safety after acceptance of a specific application by safety regulatory authority while the system is operated by operator according to life-cycle phases 11 to 14 (EN 50126). Especially the responsibilities and necessary procedures for correct maintenance and modifications of the installed system are addressed.

On the other hand, TR SIG ZA stipulates also the process for so called “type approvals” or “product approvals” for generic applications or generic products, in order to allow a multiple use of such approvals in different specific applications as first step of cross acceptance. Even this process follows the life-cycle of EN 50126 without regarding phases 11 to 14 and with partly diverging responsibilities from the approval and acceptance process for specific applications.

7. Allocation of safety requirements in research and development projects

This clause describes methods and approaches which are developed and discussed in the European research projects MODURBAN and MODTRAIN.

7.1 MODURBAN

The following two sub-clauses are a citation from the MODURBAN D86 deliverable. The title of D86 is “Safety Conceptual approach for functional and technical prescription” **[21]** and delineates methods for SIL allocation. These methods are applied to a number of safety functions.

7.1.1 Method 1: risk graph

Risk Graphs are a method taken from IEC 61508 part 5 and adapted for determining safety requirements on safety critical functions in urban guided transport. The method evaluates qualitatively, through 4 risk parameters represented graphically, the risk that arises in the absence or failure of a particular function and assigns it a Safety Integrity Level accordingly.

A Risk Graph has the following structure:

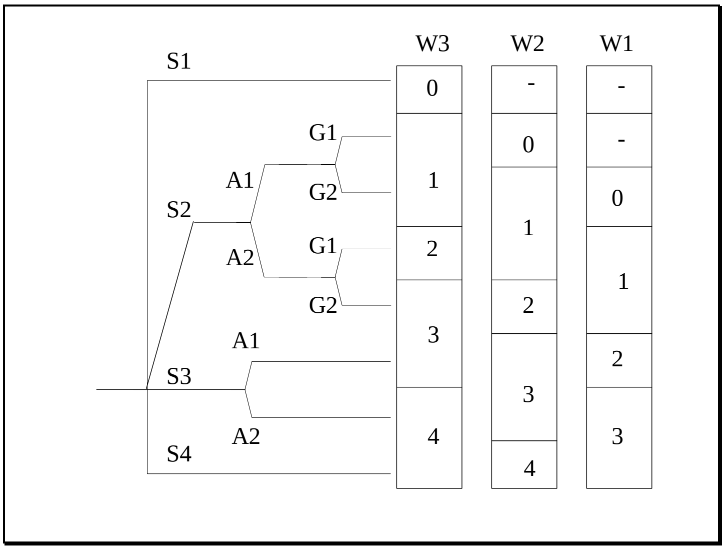


Figure 17 Risk Graph

The different branches and columns of the graph have the following meaning:

Severity of consequence (S)

S1: Minor injury

S2: One or several serious irreversible injuries, or one fatality

S3: Several fatalities

(S4: Catastrophic effects, very many fatalities - not use in transportation, normally in nuclear)

Exposure to danger (A)

A1: Rare or infrequent exposure to danger

A2: Frequent or constant exposure to danger

Defence against danger/consequences (G)

G1: Possible

G2: Hardly possible

Probability of danger occurrence (W)

W1: Very low (two barriers)

W2: Low (one barrier)

W3: Relatively high (no additional barrier)

These four parameters combined together make up the risk without/by failure of a particular protection function:

*Risk= Frequency of accident * Severity of accident = W*A*G*S*

This risk is not estimated explicitly and the risk tolerability criteria appear only implicitly through the assignment of the SIL in the graph, meaning that the function's SIL determined in this manner reduces the risk to a tolerable level.

The Severity Classes in this type of risk graphs are enumerated from one to four but this numbers do not match the numbers of the EN 50126 risk matrix. Since the risk graphs are referenced by IEC 61 508 for a broader context, the Severity Class S4 relates to large catastrophes where the application has typically nuclear core melt down as hazard in mind rather than a typical train collision. So, S2 and S3 correspond to "Critical" and "Catastrophic" of the Risk Matrix.

The Exposure of a passenger to a certain hazard is only divided into two classes. The involvement of the factor starts with an occurred hazard and asks than if passengers are more or less directly imposed, which is for the larger fraction of hazards the case. Only a few *processes (e.g. train turn back at terminal stations, end of station track door failure) are not directly impacting passengers.*

Risk Reduction Factors are typically those that may reduce the frequency of the occurrence of the accident in a hazardous situation or the damage. Damage reduction can be for example speed reduction when a train is on its course to collide. Frequency reduction can be for example the possibility of a passenger escaping from the consequence or prudence (e.g. not falling onto station tracks). It is interesting to note that in the graph above, some risk reduction factors are not taken into account for high severity consequences (G for S3, G and A for S4). This is to reflect a traditional conservative tendency when it comes to protect against collective accidents.

Concerning the likelihood of hazard occurrence, the word “probability” W can also be misleading. This parameter is used such, that whenever an occurred hazard cannot be controlled by another additional barrier (additional to the protection function that is subject of analysis) it is assumed to be “possible” and therefore W3. If another barrier or control element could prevent the hazard to evolve into an accident, the probability W2 can be assumed. Examples for these are protection function failures with still a driver on board that could safely react. If two independent additional barriers or probability limiting factors can prevent the accident, W1 may be used (e.g. train departure with undetected open doors only possible if a driver has not noticed and a door drive failure keeps door open and an interlock failure signals closed door).

7.1.2 Method 2: semi-quantitative analysis and risk matrix

The method uses as a basis a risk matrix (as described in EN 50126) in order to determine risk tolerability. The matrix from EN 50126 shown below includes only 2 risk parameters: hazard frequency (F) and severity of hazards consequences(S). Risk of a particular hazard is defined as the combination (implicitly multiplication) of these 2 parameters:

*Risk= Frequency of hazard * Severity of hazard consequence*

Table 9 Risk matrix

Frequency of occurrence of a hazard	**Risk Levels**			
frequent	undesirable	intolerable	intolerable	intolerable
probable	tolerable	undesirable	intolerable	intolerable
occasional	tolerable	undesirable	undesirable	intolerable
remote	negligible	tolerable	undesirable	undesirable
improbable	negligible	negligible	tolerable	tolerable
incredible	negligible	negligible	negligible	negligible
	insignificant	**marginal**	**critical**	**catastrophic**
	Severity Levels of Hazard Consequence			

The risk matrix shows a tolerability region roughly around a curve representing the tolerability limit (F = Tolerable Risk/S). It indicates that the tolerable frequency of hazard must decrease hyperbolically with increasing severity level, in conformity with the definition of risk above. This curve can be approximated by a stepwise tolerability boundary as shown in the EN 50126, where the steps determine what the hazard rate target (THR) must be for each severity category. In order to have an idea about the frequency scale one could use the SIL rates as given by EN 50129 to calibrate the matrix, which then yields 10^{-9}/h for hazards with catastrophic consequences and 10^{-7}-10^{-8}/h for the critical category.

The application of this methodology is a conservative use of the THR/SIL table:

Severity Category n of Hazard Consequence -> THRn=SILn

where n denominates the Severity Category (n=4 Catastrophic, n=3 Critical, n=2 Marginal, n=1 Insignificant).

Table 10 SIL-table, EN 50129 Annex A

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR 4: $10^{-9} \leq \text{THR} < 10^{-8}$	SIL 4
THR 3: $10^{-8} \leq \text{THR} < 10^{-7}$	SIL 3
THR 2: $10^{-7} \leq \text{THR} < 10^{-6}$	SIL 2
THR 1: $10^{-6} \leq \text{THR} < 10^{-5}$	SIL 1

This risk matrix gives however a conservative estimation of the risk compared to the Risk graph method, since it doesn't take into account such risk reduction factors as exposure and accident avoidance, meaning that a hazard occurring is assumed to lead directly to an accident causing harm. Also often in practice, the frequency of hazard without a protection function is not estimated, and the THRs from the matrix are used to give directly the SILs of the protection function. Thus, only one risk parameter actually needs to be evaluated for a hazard, namely the severity of its potential consequences, in order to determine the SIL. This was for instance the approach taken in UGTMS (D6), where the SILs were determined according to the consequences of the hazard (i.e. SIL4 for functions protecting against potentially catastrophic hazards, SIL3 for functions protecting against potentially critical hazards, etc.).

Such an approach has the advantage of being simple and likely to ensure reproducible results, but by neglecting other factors that influence risk, it may on the other hand produce excessive safety integrity requirements, especially for risks with less than catastrophic consequences.

Also, the demonstration of compatibility between the various practically used SIL allocation methods at a minimum level would require to take potentially risk impacting factors into account. Various standards and norms (like IEC61508) give the three groups of potentially risk impacting factors:

- *Exposure Probability to Hazard **E**: Is there good reason to conservatively assume that subjects of the risk group (e.g. passenger) are exposed to the hazard clearly less than permanently (by orders of magnitude in probability)?*
- *Accident Probability Reduction **P**: Is there good reason to conservatively assume that the evolvement of a certain hazard into an accident can be clearly controlled by additional barriers or circumstances (reduction of rate by orders of magnitude)?*
- *Consequence Reduction Probability **C**: Is there good reason to conservatively assume that the members of the risk group (e.g. passenger, workers or neighbours) can clearly avoid being subject to the hazard (by orders of magnitude) or reduce considerably the potential damage (by severity class)?*

Involving these conservative estimates of reducing factors provokes the question of numerical precision or values. Since all quoted steps/intervals in the standards and norms relating to risk are expressed by orders of magnitude in the decade system (SIL steps, risk matrix, risk graphs) it is clear that also risk reducing factors may only be incorporated by orders of magnitude in the decade system. Taking into account also the risk reducing factors definition of the IEC 61 508 the probability factors E, P and C lead only to plausible application by the numerical values:

E=1: Exposure of members of the risk group to hazard is conservatively to be assumed frequent or permanent

E=10^{-1}:Exposure of members of the risk group to hazard can conservatively assumed to be rare, only in exceptional cases (e.g. passengers in a turn back train, passengers walking into the tunnel etc.)

E=10^{-2}:Exposure of members of a risk group to hazard is only in very rare cases to be expected (e.g. passengers in depot etc.)

P=1 There can no additional barrier be conservatively assumed that would reduce the probability of the hazard evolving into an accident.

P=10^{-1}: There exists means or circumstances to clearly reduce the probability that a certain hazard evolves into an accident (e.g. additional barriers than the one being subject to analysis, driver that notices positioning failure and corrects manually, personnel onboard/in station that notice an otherwise undetected open door at train departure etc.)

P=10^{-2}:There exist two means or circumstances to clearly reduce independently the probability that a certain hazard evolves into an accident (e.g. a personnel onboard/in station notices an otherwise undetected open door at train departure and an independent door interlock senses the open door before train departs).

C=1 There is no reason to conservatively assume that a member of the risk group (e.g. passenger) may avoid being subject to the consequences of a certain hazard.

C=10^{-1} There is good reason to conservatively assume that a member of the risk group (e.g. passenger) can avoid being subject to the consequences of a certain hazard (e.g. in low headway train operation a passenger fallen into station tracks may climb out or move into emergency bay, driver notices overspeed protection system failure and reduces himself manually speed to avoid catastrophic accident and collide in Severity Level SL3 instead of SL4)

C=10^{-2} There are two independent good reasons to conservatively assume that a member of the risk group can avoid being subject to the consequences of a certain hazard (e.g.

passenger on track in Tramway operations can move away from track and driver can stop the train in time, Overspeed Protection Failure at End of Track (SL4-SL3) noticed by driver and manual speed reduction reduces further consequence to SL2)

If any of the factors can be plausibly and conservatively applied, the relation between a certain severity and the resulting SIL of the associated protection function will be:

Severity Category SL_n of Hazard Consequence -> $THR_m = THR_n/EPC = SIL_m$

with „m“ as a natural number between 1 and 4.

Certainly each operator has the freedom to set all factors 1. This could especially be the case if very crowded subway network are considered, where the Exposure Factors will be 1 in most cases. Nevertheless, to avoid extreme safety integrity requirements it should be considered to take the risk reduction factors into consideration.

If all factors need to be conservatively estimated to 1 then the relation expresses the conservative association of THR and SIL of the annex EN 50129. Graphically the analysis of the THR/SIL relation in the risk analysis process corresponds to varied rate distances in the risk matrix that reflect varied SIL requirement of the risk control measure.

Such a notion is actually in line with the definition of risk from EN 50126:

“The probable rate of occurrence of a hazard causing harm and the degree of severity of the harm”.

By employing in both methods, qualitative and quantitative, similar descriptions of the details between hazard emergence and possible accident consequences it is likely that the according SIL allocations yield similar (read same) minimum SIL requirements. On the other hand, the notation “minimum” relates to the fact that in some cases the minimum SIL requirements leave a non-zero potential to a Public Transport Authority to increase on their discretion to more conservative requirements.

7.2 MODTRAIN

The following approach is developed in the European research project MODTRAIN. Within MODURBAN the MODTRAIN approach is compared to the outcomes from D86. The following sub-clause cites from this comparison, see **[22]**.

This MODTRAIN method is a semi-quantitative risk analysis developed in a context for rolling stock of main railways.

The procedure of the safety analysis proposed by MODTRAIN is carried out in the following way:

Stage 1: System Definition: *The train system boundaries must be defined in regard to the train functions, and possibly the limits of responsibility.*

Stage 2: Hazard Identification: *The Accident Contexts are identified. An Accident Context is defined by association of an Operational Context*[7]*, a Boundary Hazard*[8] *at train system level and a potential Accident. Standard lists of Accidents and of Boundary Hazards should be used. It is necessary to always keep in mind that the expression of the Boundary Hazards may be incorrect until all aspects pertaining to the train system context have not been pushed out, especially the role of functions and subsystems at railway system level and external to the system boundary.*

Stage 3: Consequence Analysis: *The Consequence Barriers*[9] *that can prevent the Boundary Hazards from developing into Accidents under defined Operational Contexts are identified. A Consequence Barrier may reduce or eliminate the accident occurrence or reduce the accident severity. The sequence of Consequence Barriers from the Boundary Hazard to the Accident should be defined for each Accident Context. One or more safety requirements must be specified for each Consequence Barrier.*

Stage 4: Risk Estimation: *Hazard Tolerability is defined in terms of Tolerable Hazard Rate (THR) for each Accident, and subsequently for each Boundary Hazard considering the Consequence Barriers available under a defined Operational Context. Unless Hazard Risk objectives are provided by the Member States, a Risk Estimation must be performed on the*

[7] *The operational context is defined with an operational mode, an operational phase and an operational area and possibly with some specific circumstances.*

[8] *A boundary hazard is a state at the system boundary, which has potential either directly or in combination with other factors (external to the system), for giving rise to an accident at railway system level.*

[9] *A consequence barrier is a function or action that may help to reduce the likelihood of the development of a boundary hazard into an accident.*

Boundary Hazards when their tolerability is not well established. Main steps of the Risk Estimation are as follows:

- *For each Accident Context, determination of the Tolerable Accident Rate (TAR). A suggested way for its determination is the use of the Risk Tolerability Matrix that should be submitted to the Customer and/or to the National Safety Authority for approval. The Risk Tolerability Matrix qualitatively defines a set of Tolerability Categories of the Risk, as well as a set of Severity Categories and Frequency Categories. A Tolerable Risk Rate can be then determined for each Severity Category provided that each Frequency Category is also featured and ranged by an interval of hourly rates, continuous with the adjacent Categories. The Tolerable Accident Rate is equal to the Tolerable Risk Rate corresponding to the Severity Category of the Accident.*
- *For each Accident Context, determination of the probability of the Operational Context, and estimation of the efficiency of the Consequence Barriers identified during the Consequence Analysis*[10]*. Return of experience should be used for estimating these values.*
- *Finally, computation of the Tolerable Hazard Rate of the Boundary Hazard.*

Stage 5: Causal Analysis: *The Cause Barriers*[11] *that can prevent Hazard Causes*[12] *from developing into a Boundary Hazard under a defined Accident Context are identified. The sequence of Cause Barriers from a Hazard Cause to the Boundary Hazard under consideration should be defined. Then the sequences obtained for all the Hazard Causes are consolidated. One or more safety requirements must be specified for each Cause Barrier, as well as for the various Hazard Causes when meaningful.*

Stage 6: SIL Allocation: *THR and SIL allocation to the Train functions must be performed taking into account the identified Boundary Hazards, the Architecture Principles and Safety Principles at Train System level. When the THR of a Boundary Hazard is apportioned to several functions, a particular attention must be paid to the independence of the functions (Safety Principles). Main steps of the THR and SIL Allocation are as follows:*

For each Accident Context, estimation of the efficiency of the Cause Barriers, and allocation of Tolerable Rates to the Hazard Causes in order to meet the Tolerable Rate of the Boundary Hazard. Return of Experience should be used for estimating and allocating these values.

[10] *Analysis of events which are likely to happen after a hazard has occurred.*

[11] *A cause barrier is a function or action that may help to reduce the likelihood of the development of a hazard cause into a boundary hazard.*

[12] *Any event which contributes to the occurrence of a boundary hazard.*

THR apportionment and SIL allocation to concerned functions is the result of this analysis.

Note: The approach finally adopted by MODTRAIN is as follow (see "Guidance for safety analysis" version 2.0):

Safety-related functions and sub-functions that are supported by electrical, electronic or programmable subsystems are allocated with a SIL. The SIL Allocation must be performed taking account of the THR of the Boundary Hazards, the functional architecture, the distribution of the safety-related functions on the physical architecture and the safety role of each function.

Stage 7: Safety Demonstration and Justification: *Detailed safety analyses are carried out in order to allow the identification of detailed safety requirements that the elements of the Train Control and Monitoring (TCMS) system must fulfil in all the phases of their development. The final safety level that is achieved must be justified:*

- *by a defined and managed development process which prevents from systematic failures (quality assurance approach).*
- *in a quantitative way for scenarios resulting from random failures (probabilistic approach).*

The definition of these stages is supposed to be compliant with the approach developed in the EN 50129 standard.

The following figure gives an overall overview about the MODTRAIN process.

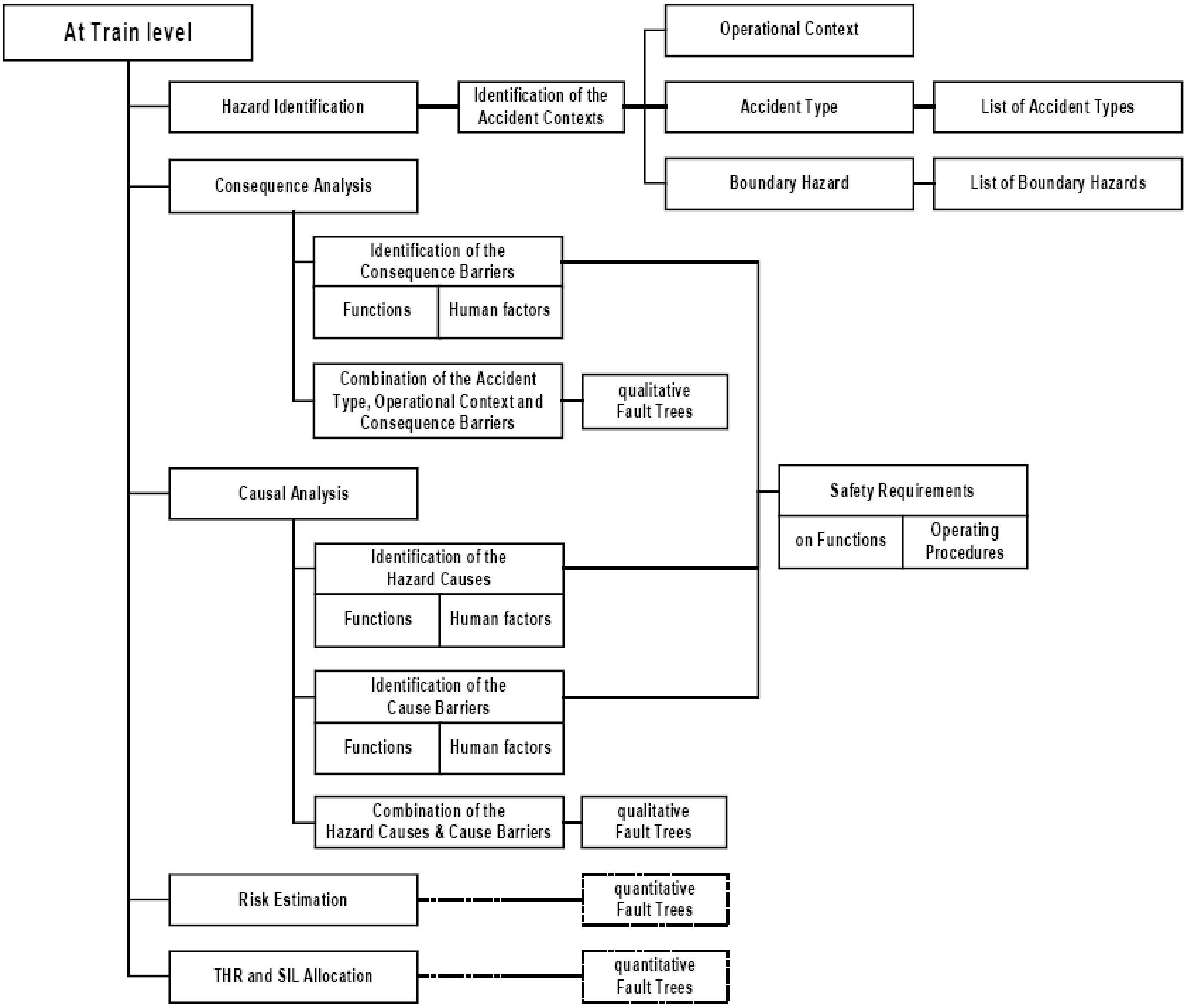


Figure 18 Procedure of MODTRAIN

8. Operator specific methods for the allocation of safety requirements

This clause describes methods and frameworks on how to allocate safety requirements used by operators. These approaches do not represent all methods applied in Europe. These approaches are additional and cover methods, not mentioned in clause 6 or 7.

8.1 Operator A

To derive safety targets a quantitative approach is used. These safety targets are expressed as tolerable hazard rates i.e. THRs, derived from a reference system. To transform these THRs into safety integrity levels a combination table is used, which is in accordance with EN 50129 (see Table 4).

In particular the method for safety requirement allocation is started with an analysis of possible hazards and functional failures. To analyse these failures and to estimate hazard consequences and frequencies tools like fault and event trees are used. Therefore, failure frequencies and probabilities are derived from an existing reference system. Assuming that the reference system is acceptably safe, safety targets are calculated for functions, according to the results analysed in event and fault trees. Finally, safety targets i.e. tolerable hazard rates are transformed into SILs according to EN 50129. However, safety targets may later be adjusted due to ALARP criteria or design changes.

8.2 Operator B

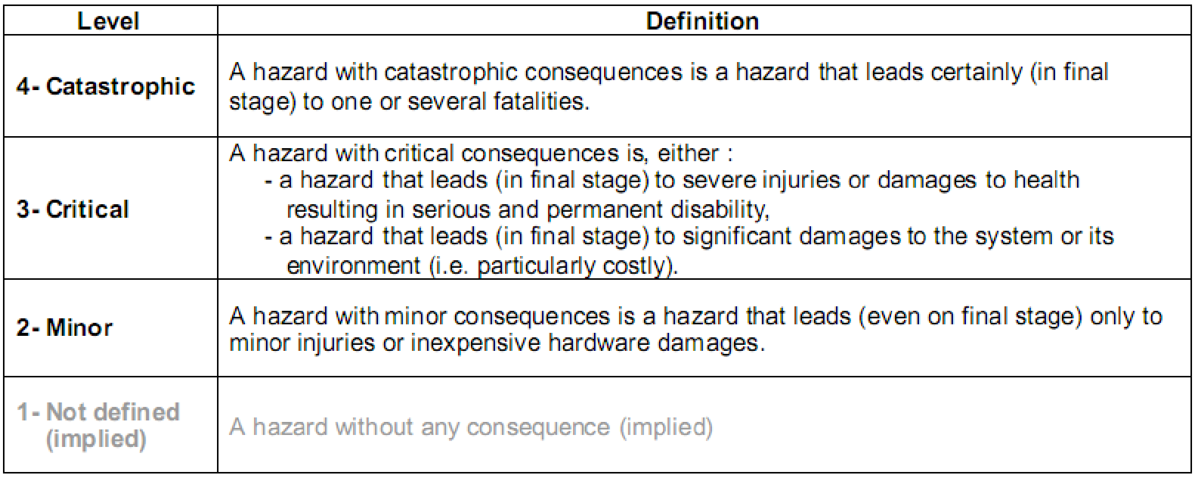
This description of the approach for safety requirement allocation is provided by the operator directly.

This example is a qualitative approach, which uses the idea of a consequence (i.e. severity) - frequency matrix.

Severity levels

The severity levels are the following (text in grey is not formally defined, but is implied):

Table 11 Description of hazard severity levels

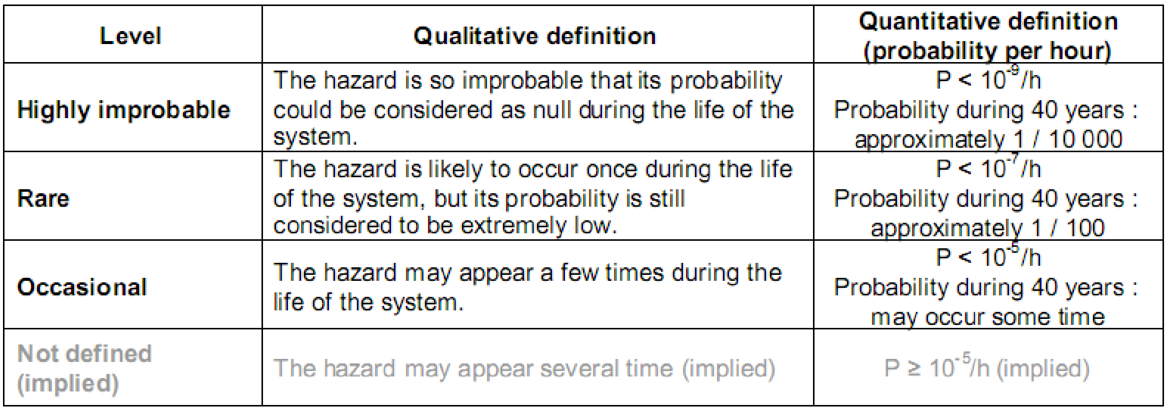


Level	Definition
4- Catastrophic	A hazard with catastrophic consequences is a hazard that leads certainly (in final stage) to one or several fatalities.
3- Critical	A hazard with critical consequences is, either : - a hazard that leads (in final stage) to severe injuries or damages to health resulting in serious and permanent disability, - a hazard that leads (in final stage) to significant damages to the system or its environment (i.e. particularly costly).
2- Minor	A hazard with minor consequences is a hazard that leads (even on final stage) only to minor injuries or inexpensive hardware damages.
1- Not defined (implied)	A hazard without any consequence (implied)

Frequency levels

The frequency levels are the following (text in grey is not formally defined, but is implied):

Table 12 Description of hazard frequency levels



Level	Qualitative definition	Quantitative definition (probability per hour)
Highly improbable	The hazard is so improbable that its probability could be considered as null during the life of the system.	$P < 10^{-9}$/h Probability during 40 years : approximately 1 / 10 000
Rare	The hazard is likely to occur once during the life of the system, but its probability is still considered to be extremely low.	$P < 10^{-7}$/h Probability during 40 years : approximately 1 / 100
Occasional	The hazard may appear a few times during the life of the system.	$P < 10^{-5}$/h Probability during 40 years : may occur some time
Not defined (implied)	The hazard may appear several time (implied)	$P \geq 10^{-5}$/h (implied)

Note that the frequency is relating to hazards (not accidents or failures).

Risk matrix

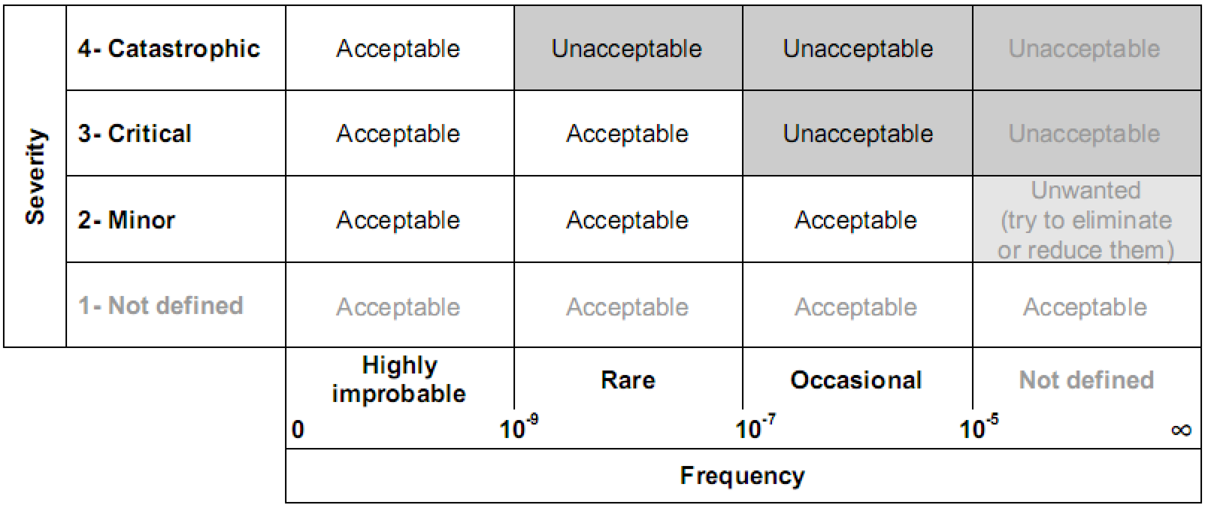
The risk acceptance is determined by the combination of severity and frequency of hazards. Formally, acceptance criteria of risks are the following:

- risks characterised by a catastrophic severity and a frequency other than highly improbable are unacceptable,
- risks characterised by a critical severity and a frequency other than highly improbable and rare are unacceptable,
- all other risks are acceptable.

Note that, formally, with these definitions, risks characterised by a minor severity are always acceptable but, in practice, one obviously seeks to eliminate or reduce them if possible (unwanted risk).

The risk matrix is then the following (text in grey is not formally defined, but is implied):

Table 13 Risk matrix



Severity	**4- Catastrophic**	Acceptable	Unacceptable	Unacceptable	Unacceptable
	3- Critical	Acceptable	Acceptable	Unacceptable	Unacceptable
	2- Minor	Acceptable	Acceptable	Acceptable	Unwanted (try to eliminate or reduce them)
	1- Not defined	Acceptable	Acceptable	Acceptable	Acceptable
		Highly improbable	**Rare**	**Occasional**	**Not defined**
		0 **10^{-9}**	**10^{-7}**	**10^{-5}**	**∞**
		Frequency			

SIL allocation rules

SIL are firstly allocated to functions. The process consists in relating the SIL of a function to the acceptance area of the risk matrix associated with the failure of that function. The functions are classified according to the risk associated with their failure in this way:

- A function whose failure leads to an unacceptable risk with catastrophic consequences has to be treated SIL4.
- A function whose failure leads to an unacceptable risk with critical consequences has to be treated SIL3.

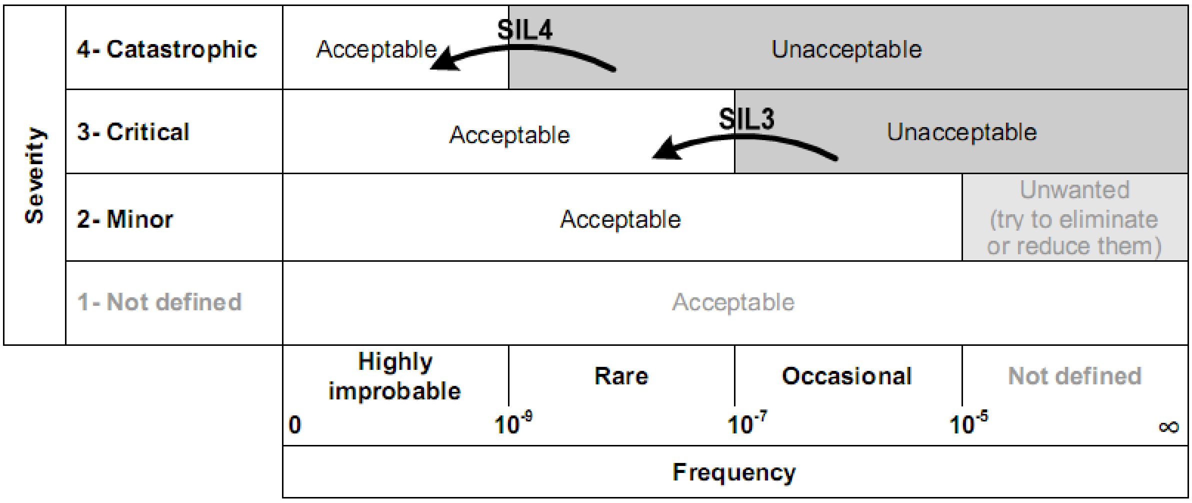
In fact, the basic principle of this process is to design functions with the SIL required to achieve the acceptable area of the risk matrix.

All other functions whose failure leads to acceptable risk have to be treated in the following manner:

- SIL2 when the functions participate to the global safety of the whole line by their very high availability,
- SIL0 in the other cases.

This process could be illustrated this way (text in grey is not formally defined, but is implied):

Table 14 Process of SIL allocation



Severity					
	4- Catastrophic	Acceptable	SIL4 Unacceptable		
	3- Critical	Acceptable		SIL3 Unacceptable	
	2- Minor	Acceptable			Unwanted (try to eliminate or reduce them)
	1- Not defined	Acceptable			
		Highly improbable	Rare	Occasional	Not defined
		0	10^{-9}	10^{-7}	10^{-5} ∞
		Frequency			

▨ Unacceptable risk
░ Unwanted risk (implied)
□ Acceptable risk

Note that, for SIL4, the corresponding upper limit required for THR is 10^{-9}/h and not 10^{-8}/h as it is mentioned in the SIL table of the EN 50129 standard.

Furthermore, in some marginal cases, the acceptable area could also be achieved by reducing the severity rather than reducing the frequency using the SIL concept.

SILs are then allocated to equipments. The SIL chosen for equipment is the maximum SIL among the functions (or parts of functions) it supports. Therefore, it is advisable to share out wisely the different functions in order to limit the number of equipments that must have a high level of SIL.

8.3 Operator C

This example of requirement allocation methods does not follow a formal approach. In this case no legal obligations exist on how to determine safety integrity level, except the fact that railway interlockings have to be constructed according to SIL 4, following EN 50128.

However, SILs have been stipulated for the following applications:

- For safety and protection equipment/functions
- For driving equipment/functions - ATO
- For maintenance and traffic control functions

8.4 Operator D

The following example uses as a consequence – frequency matrix (or risk matrix) as basis. For every hazard, identified and logged in the hazard log, frequency of occurrence and a severity level are estimated. Following the ideas of the risk matrix, for every hazard a risk level can be obtained.

To derive levels for safety integrity each level of risk, like “intolerable” or “undesirable” is associated with a SIL. Hence, for each function, covering a hazard, a SIL can be derived – including target frequency of the hazard. For illustration purposes an example can be given on how this risk matrix might look.

Table 15 Example of risk matrix

Frequency of occurrence of a hazard	**Risk Levels**			
frequent	Undesirable **SIL 2**	Intolerable **SIL 3**	Intolerable **SIL 3**	Intolerable **SIL 4**
probable	Tolerable **SIL 1**	Undesirable **SIL 2**	Intolerable **SIL 3**	Intolerable **SIL 4**
occasional	Tolerable **SIL 1**	Undesirable **SIL 2**	Undesirable **SIL 2**	Intolerable **SIL 4**
Remote	Negligible **SIL 0**	Tolerable **SIL 1**	Undesirable **SIL 2**	Undesirable **SIL 3**
improbable	Negligible **SIL 0**	Negligible **SIL 0**	Tolerable **SIL 1**	Tolerable **SIL 2**
incredible	Negligible **SIL 0**	Negligible **SIL 0**	Negligible **SIL 0**	Negligible **SIL 0**
	insignificant	**marginal**	**critical**	**catastrophic**
	Severity Levels of Hazard Consequence			

8.5 Operator E

In the following example safety requirements are derived in two ways[13]. Either applicable codes of practice are used or functions acting as hazard mitigation on hazard are evaluated. Therefore, a hazard log is applied using a defined set of top-hazards, each associated with hazard frequency, severity of consequences and a description of mitigation.

To evaluate risk, a consequence – frequency matrix is applied. To estimate the frequency of possible hazards techniques like Bayesian network are used. (Bayesian networks are probabilistic models, which can be represented graphically. These networks can be applied to model random variables and their conditional dependencies.) Possible hazard consequences and accidents are modelled with event tree tools. For consequences and accidents probability distributions are assumed. To assess the evolving risk, an acceptance curve is used representing the risk acceptance criteria.

This procedure yields safety integrity requirements for the defined top hazards.

[13] Due to a lack of information, this sub-clause provides only an overview of the process.

9. Example functions for application and comparison

This clause introduces example applications of some of the previously described methods to some sample safety functions.

9.1 Introduction

For the purpose of illustration on how to apply methods for safety requirement allocation and to support an analysis of the methods, examples of safety functions are given below. However, possible results in terms of levels of safety integrity can only be understood as examples and in the MODSafe context as generic results of a research project.

An application of some methods described above turned out as too many inputs are required that are normally not available at a generic level. Other more generic methods are however applicable also at a generic level.

Concerning the example functions, two different descriptions have been selected since other descriptions do not list functions. The example functions have been taken from the MODURBAN D86 **[21]** and as a comparison the German recommendations VDV 331 **[20]**.

Possible results for the safety functions are summarised in Table 16 to Table 19. The SILs shown in these tables originate from **[20]**, **[21]**, **[22]** and applications and information by operators.

Examples for levels of safety integrity are blank (“-”) if no SIL has been assigned, because no comparable function is found.

9.2 Overspeed detection

In D86 it is described as: *Speed is determined onboard by the subsystems CC, SPTS and odometer sensors. If speeds are above acceptable speed limits, the function detects the overspeed and initiates safety reaction.* **[21]**

In VDV 331 a similar function is described as continuous speed supervision and may be understood as: Supervision of defined maximum speed according to track topography, temporary speed restrictions, emergency stops or stopping points (cf. **[20]**).

Table 16 Example function: Overspeed detection

Methods for SIL allocation	Safety integrity level
MODURBAN method 1	**4**
MODURBAN method 2	**4**
VDV 331	**4**
MODTRAIN	**4**
Operator A	**-**
Operator B	**4**
Operator C	**4**
Operator D	**4**
Operator E	**-**

9.3 Safe switch command and status

The functional description in D86 is: *For switching under normal (undisturbed) and safe conditions* **[21]**.

As a comparison, VDV 331 defines one function for switches as: Protection against switching while switch is indicated as occupied (cf. **[20]**).

Table 17 Example function: Safe switch command and status

Methods for SIL allocation	Safety integrity level
MODURBAN method 1	**4**
MODURBAN method 2	**4**
VDV 331	**4**
MODTRAIN	**4**
Operator A	**4**
Operator B	**4**
Operator C	**4**
Operator D	**4**
Operator E	**-**

9.4 Safe manual (emergency) door opening

D86 describes it as: *In case of emergency situations (e.g. Failed Onboard ATP), manual emergency egress shall be authorized after TBD seconds (e.g. 15 s) onto the emergency walkway side only and shutdown of third rail* **[21]**.

This function is not described in VDV331 but considering the described procedures, the so called “method b” (see Figure 15) can be applied.

The result for MODTRAIN is taken from **[22]**.

It is guessed that for the procedure proposed by operator B SIL 4 should be applied, since the hazard consequences have to be assumed to be “catastrophic”.

Table 18 Example function: Safe manual (emergency) door opening

Methods for SIL allocation	Safety integrity level
MODURBAN method 1	**3**
MODURBAN method 2	**2**
VDV 331	**(3) “method b”**
MODTRAIN	**1**
Operator A	**-**
Operator B	**4**
Operator C	**-**
Operator D	**-**
Operator E	**-**

9.5 Door obstruction detection

D86 describes it as: *During passenger exchange, trains may not depart without authorization (see train departure), passengers need to be protected against being trapped in doors, obstruction needs to be detected* **[21]**.

This function is not described in VDV331 but considering the described procedures, the so called “method b” (see Figure 15) can be applied.

The MODTRAIN approach **[22]** does not cover this function. But considering the proposed procedure (compare sub-clause 7.2) it is assumed to lead to SIL 2.

Since hazard consequences can be “critical” the method of operator B is assumed to lead to SIL 3.

Table 19 Example function: Door obstruction detection

Methods for SIL allocation	**Safety integrity level**
MODUBRAN method 1	**2**
MODURBAN method 2	**2**
VDV 331	**(2) “method b”**
MODTRAIN	**(2)**
Operator A	**-**
Operator B	**3**
Operator C	**2**
Operator D	**-**
Operator E	**-**

10. Comparison of methods

This clause summarises and compares the methods for safety requirement allocation, introduced above. Its focus is mainly on a comparison and applicability of methodologies.

10.1 Introduction

For a comparison of methods, it is first of all necessary to distinguish between actual methods which can be applied in the sense of MODSafe, i.e. to derive safety requirements for hazard control measure. Furthermore, approaches or frameworks have to be differentiated, which describe an outline on how safety requirements shall be conducted in general, embedding methods in the project, rather than to follow a detailed procedure.

Methods to derive safety integrity requirements are described in:

- IEC 61508-5
- MODURBAN D86 (method 1 and 2)
- VDV 331
- MODTRAIN as described in MODURBAN D90 (see **[22]**)
- CLC/TR 50451
- Clause 8 of this deliverable (methods of operators)

Approaches outlining a framework to allocate safety requirements are described in:

- IEEE 1474
- EN 50126
- EN 50129
- Commission regulation No 352/2009
- Yellow Book

It is aimed to analyse both groups of methods, even though a comparison with the latter group is only possible on a rather generic level.

10.2 Comparison according to methodology

Basically, methods can be distinguished between the following characteristics. However, one characteristic is not necessarily represented by one method. Most methods combine a variety of characteristics.

Characteristics:

- Quantitative or qualitative derivation of safety requirements
- Is risk estimated with a risk based approach considering hazard frequency and the severity of consequences or is risk not explicitly expressed and safety targets derived from e.g. a reference system of a global safety target?
- Regarding risk based approaches; which parameters are considered, e.g. frequency, severity, exposure time, risk reduction measures, etc.?
- Regarding risk based approaches; is risk derived explicitly which enables the user to compare it to risk acceptance criteria or is risk derived implicitly to derive safety requirements directly?
- Concepts to express safety requirements as safety targets, tolerable hazard rates or safety integrity level which addresses the question; are these safety requirements applied to safety functions or hazards?

10.2.1 Quantitative and qualitative methods

Quantitative methods use exact (or ranges of) numerical values as an input for the calculation of safety targets. For example, the hazard frequency can be expressed in terms of events per hour, which may look like one event in ten hours, one event in hundred hours, and so on.

Qualitative approaches are using parameters to estimate risk, which are described in words, rather than exact numerical values. For example, for descriptions of the severity of consequences terms like “catastrophic” or “critical” may be applied.

However, orders of magnitude can be found to describe a parameter in more detail. For instance, it might be possible to associate the term “critical” with one fatality. This would turn a qualitative approach in something like a semi quantitative method.

A general comparison between qualitative and quantitative methods can be found in CLC/TR 50451. Advantages and disadvantages are summarised in the following table.

Table 20 Comparison of qualitative and quantitative methods [8]

	Qualitative methods	Quantitative methods
Benefits	▪ *Principally a judgement process* ▪ *No detailed quantification, data collection and analytical work* ▪ *Simple and can be carried out without assistance from process experts* ▪ *Auditable process with scope for review and improvement* ▪ *Does not require customisation or 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*	▪ *Generates a quantified measure of risk 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 risk* ▪ *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*
Drawbacks	▪ *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 risk leading to significant losses*	▪ *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*

Methods which perform a safety requirement allocation quantitatively are for example:

- The methods used by operator A, where THRs are calculated from a reference system.
- The quantitative procedure proposed by CLC/TR 50451. In this case a risk formula is used, requiring (exact) numerical values on each parameter.

Instances on how to derive safety requirements qualitatively are:

- The risk graph which is used in IEC 61508, VDV331, MODURBAN method 1

Additionally, it has to be mentioned that combinations of both quantitative and qualitative methods exist. MODURBAN method 2 can be assumed to a semi quantitative method since it used descriptions of risk parameter and numerical values for a calculation.

10.2.2 Risk based approaches

Methods using a risk based approach use parameters to describe risk. This can be done verbally or with numerical values. Finally, a level of risk can be derived, which might be used to derive safety requirements. The risk graph or the risk matrix describes risk according to certain parameters.

Alternatively, safety targets may be derived using reference systems which have an acceptable level of safety and transfer safety requirements to the design of the new system. Another method is to calculate or estimate a global safety target applicable to the overall system and to break down these safety targets to functions, defined for the system. As an example operator A can be mentioned.

The advantage of the latter method is that if operational data of an existing reference system are available and the system can be assumed to be acceptably safe, safety targets might be in an appropriate order of magnitude and not over estimated.

With risk based approaches risk can be estimated even without detailed operation data. Especially for new systems or generic analyses these approaches might have advantages.

10.2.3 Risk parameter

When deriving safety requirements according to the risk posed by a hazard or a failure of a safety function, parameters are considered to estimate risk. For example, the hazard occurrence frequency or severity of hazard consequences might be taken into account, see figure below.

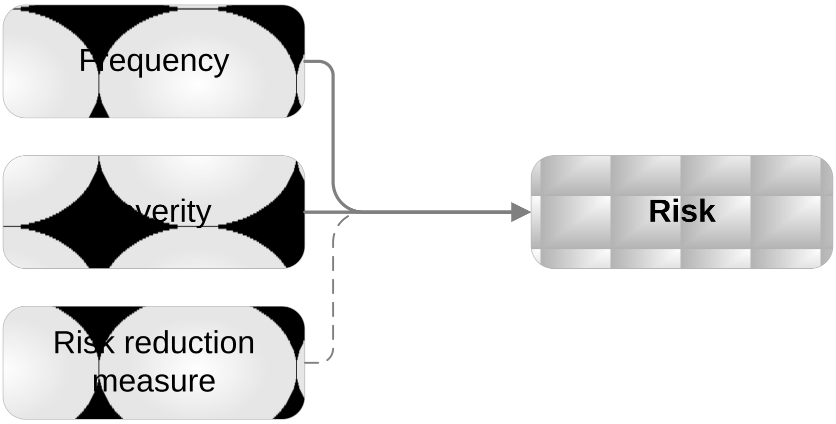


Figure 19 Conceivable parameter influencing risk

Additionally, risk parameters might be considered which might work as risk reduction. When it is possible to determine risk reduction measures appropriately, these may help to derive a more realistic level of risk and may prevent overestimation of risk and therefore too demanding safety requirements.

An example of a method is the consequence – frequency matrix (i.e. risk matrix) which considers two risk parameters.

A more detailed analysis can be found in risk formulas as described in CLC/TR 50451. Parameters like passenger exposure time, number of passenger or the probability of fatality in an accident are considered.

On the issue of risk reduction measures, operator B, for example, does not consider any measure for possible risk reduction; SILs are estimated on the severity only. This requires less effort in terms of operational data, knowledge and working time and leads to more conservative results - in comparison to methods using risk reduction measures. The probability to produce not enough demanding, i.e. not stringent enough, safety requirement is minimised. (This, however, may lead to too demanding requirements for the supplier and may increase costs for equipment. It may be considered for operators to invest in a more detailed hazard and risk analysis to set safety integrity requirements appropriate to its specific operation.)

10.2.4 Risk acceptance criteria

The criterion for risk acceptance may be expressed as a level of risk, which is acceptable to passenger, public and workers confronted with the system. Therefore, the level on which criteria are set should be determined, which parameter should be considered and what actual values should be applied. Hence, risk acceptance criteria are set by society or, as its representative, by the state i.e. the authority having jurisdiction. The difficulty to derive criteria for risk acceptance is explained in **[23]**.

Safety integrity requirements should be in accordance with the risk acceptance criteria. Hence, it may be of advantage for methods for a derivation of safety integrity requirements to state the risk acceptance criterion explicitly.

Methods, explicitly deriving risk are these which yield e.g. a verbal statement about the level of risk like “undesirable” or a THR. If criteria for risk acceptance would exist, associated with a numerical value and on the same level of analysis, it could be possible to compare their values. A comparison offers the user a clear judgement, if risk is acceptable or not, according to a criterion. (Comparison shall be conducted on the same level of analysis, e.g. on system level or sub-system level.)

A method not using an explicit risk acceptance criterion is the risk graph. This method yields safety requirements directly, without stating risk explicitly. But, according to **[24]** it seems not to be likely that the risk graph may be accepted in Europe overall due to the different criteria for risk acceptance (e.g. GAME or ALARP).

10.2.5 Level of analysis

When estimating risk, hazard analysis can be performed. After hazard identification a list of hazards should be available. Afterwards, risk can be estimated for all hazards, recorded i.e. in a hazard log, or an analysis can be applied to a set of top-hazards only, assuming a hierarchy of hazards. Performing hazard analyses may, for example, yield tolerable hazard rates.

Alternatively, an analysis can be conducted for failures of safety functions. Safety functions may be defined in advance to cover possible hazards. Safety requirements can be allocated directly to the safety function. An example of this might be the MODURBAN method 2.

The combination between hazard and THR and safety function and SIL, concerning European and international standards, is depicted in the following figure.

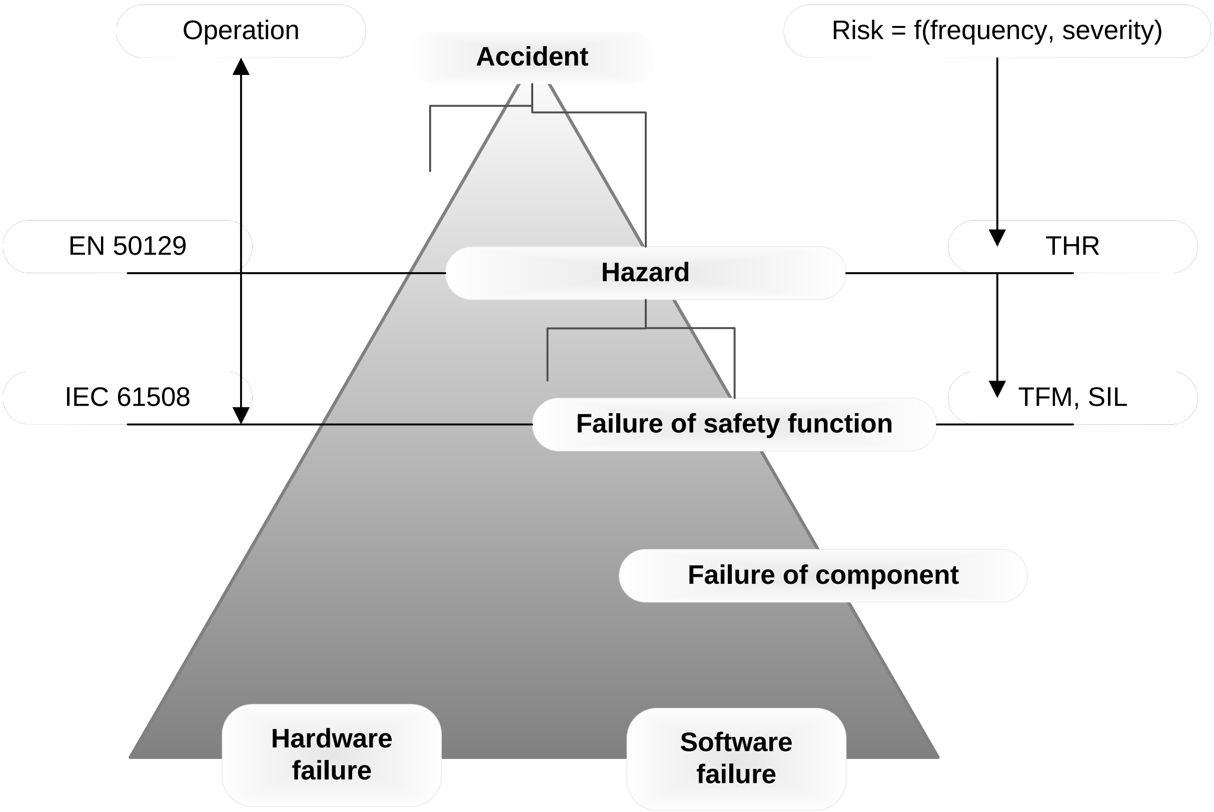


Figure 20 Connection between TFM and THR according to [24]

10.3 Comparison according to application

For an actual application the following might be considered.

- Repeatability of application
- Sensitivity of results
- Caution on the results
- Way of application in terms of e.g. straight forward or rather difficult

When speaking about repeatability of an application of methods, it is meant that different users shall be able to use the methods in the same way to obtain the same results for the same hazard or safety function. Given that the same operational circumstances are applied. This may primarily affect the way risk parameters are described and obtained and how the actual risk estimation or calculation is done.

Following Table 20; especially qualitative methods rely on user assumptions and judgements on how risk parameter may be chosen. Quantitative methods may however be prone to mistakes regarding the calculation of results. For example, this may be applied to complex systems where safety requirements are obtained from a reference system using tools like event or fault trees.

Another question may be, how sensitive they are once a risk parameter is chosen wrongly and subsequently what effects this might have on the final results. For qualitative approaches using ranges and verbal descriptions of risk parameter, a mistake in selecting the appropriate order of magnitude would immediately lead to different results, because every parameter is described coarsely. However, it is assumed that because of the general description of risk parameter it seems to be likely that the most appropriate category can be chosen. For quantitative methods; minor changes in the parameter are possible and might not necessarily lead to different results.

However, all methods should be geared towards obtaining results on the conservative side. In case a parameter cannot be estimated, used methods should produce increased safety and conservative results.

Finally, methods can be distinguished between their complexities in application. This may concern the used wording but also the calculation scheme of the method, itself. The use of qualitative concepts may produce ambiguous verbal descriptions, which need to be agreed upon by the different user of a method. For example the words “catastrophic” or “critical” which can be used to express the severity of the risk would need a definition of a metric. Furthermore, as seen above, too complex applications in terms of model parameters or methods of calculation would require more extended experience and know-how for successful application.

10.4 Comparison according to results

The application on the four safety functions, performed above, produces the same results for continuous mode functions, see first and second function.

The third and the fourth safety function can be assumed to work on demand rather than permanently. Differences in results have been shown already in **[21]**. A more detailed analysis for on demand functions is subject to future research in MODSafe.

11. Conclusion

This clause aims to summarise the approaches and explanations on safety requirements. This is done concerning actual methods for safety requirement allocation and its corresponding application.

The following criteria have been identified to have benefits for methods on safety requirement allocation:

- Conform with European standards
- Straight forward applicability possible, e.g. clear sequence of steps
- Well described risk parameter
- Not yield too optimistic results (prefer conservative estimates in case of uncertainty)
- Repeatable, i.e. yield same results by different users
- Possibility to compare results with a risk acceptance criterion, i.e. to express safety requirements as rates or probabilities
- Level of detail should be clear (single low-level hazard vs. high-level generic hazard)

Taking into account these criteria, the MODURBAN method 2 seems a plausible alternative regarding the upcoming tasks 4.2 in work package 4, which requires an allocation of safety requirements to safety measures and functions.

This method is first of all in accordance with CENELEC standards, cf. **[21]**. It is a semi-quantitative method, however, easy to use. (A purely quantitative method would not have been possible because it requires operational data. These are not available, even if so, the question remains, how to derive representative values.) Regarding its risk parameter, final results and repeatability the method has proven its applicability in the MODURBAN project. Furthermore, since it deals with numerical values, results are possible to be compared to risk acceptance criteria, if available. Besides it is clear on which level of analysis the methods has to be applied (i.e. failures of safety functions).

This recommendation primarily focuses on the activities in MODSafe.

Concerning the applicability of the presented safety requirement allocation methods to safety functions, two different findings can be stated:

1. For functions working in a continuous mode of operation, all methods yield the same results. This applies in particular to functions which have been applied to the risk graph (MODURBAN methods 1) and the MODURBAN method 2, which is shown in **[21]**.
2. For safety functions with an on demand character, as defined in IEC 61508, the results are not necessarily consistent. Therefore, special attention shall be paid to this

category of safety functions in task 4.3 of work package 4. An alternative method needs to be identified to allocate safety requirements in a comprehensible manner, considering all influencing factors which are typical for the “on demand” character, e.g. frequency of usage, diagnostics test intervals or safety relevant failure rate of the function.