SEVENTH FRAMEWORK PROGRAMME

MODSafe

European Commission
Seventh Framework Programme
MODSafe Modular Urban Transport Safety and Security Analysis

Analysis of On-Demand Functions

Deliverable No. D4.3

Contract No.	218606
Document type	DEL
Version	V1.3
Status	Final
Date	15 February 2012
WP	WP 4
Lead Author	Sven Scholz, Michal Matousek, Joerg Schuette
Contributors	WP4 members
Description	Analysis of On-Demand Functions
Document ID	DEL_D4 3_UITP_WP4_120220_V 1.3.docx
Dissemination level	PU
Distribution	MODSafe consortium

Document History:

Version	Date	Author(s)	Modification
V0.1	26 September 2011	Sven Scholz, Joerg Schuette	New document
V0.2	28 October 2011	Michal Matousek	comments from WP4
V1.0	16 November 2011	Michal Matousek, Sven Scholz	final comments from WP4; Berlin meeting 7 November 2011
V1.1	17 January 2012	Sven Scholz	comments from WP10; final consensus on 12 January 2012
V1.2	15 February 2012	Sven Scholz	editorial corrections
V1.3	20 February 2012	-	Coordinator Approval

Approval:

Authority	Name/Partner	Date
WP4 responsible	UITP (WP4 consensus of V1.0)	2011-11-16
WP10	RATP (WP10 consensus of V1.2a)	2012-02-15
Coordinator	TRIT	2012-02-20

Table of contents

List of figures

1 Summary

This deliverable concludes the result of an investigation how to handle safety functions which are not working in a Continuous Mode. Major normative reference is made to the IEC 61508 standard which describes the concept of Low Demand functions. The description in this standard is reviewed carefully to assess the applicability of the proposed concept to safety functions in the urban guided transport sector. Other material is also inspected for relevance.

The release of EN50126 [1] which is currently under revision does not cover the concept of safety functions operating in Low Demand mode. A conceptual guideline how to systematically allocate safety integrity requirements to this type of functions is not addressed. Only a more general statement requires that *“in the case that failure probabilities on demand are given, they have to be transformed in frequencies”.* This deliverable proposes such a transformation process based on the low demand concept of IEC 61508.

This deliverable will therefore briefly analyze first the most common normative reference (IEC 61508) and other materials and then return to the artifact of Low Demand functions thoroughly in its mathematical foundation based on Markov-Chain theory. Finally, a possible Safety Requirement Allocation Scheme to functions is applied and conclusions are drawn on its suitability.

Basically, the proposed allocation method takes into account three different rates, i.e., the hazard occurrence rate (demand rate), the wrong side failure rate of the safety function and the inspection rate to check the correct functionality (no undetected failure). This generic Safety Requirement Allocation Scheme for Low Demand functions shall give general guidance to the user but a case-by-case decision taking into account the specific application conditions, i.e. determining the three rates, is necessary.

Finally, the report presents some application examples for different Low Demand functions to demonstrate the proposed safety requirement allocation scheme.

Please note, this deliverable deals with safety requirements and is not applicable to security aspects. Security issues are solely covered in MODSafe WP8 and WP9 deliverables.

2 Bibliography

[1] COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: “EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)”, CENELEC 1999

[2] COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: “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

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-2 Ed. 2.0: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems“, IEC 04/2010

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-4 Ed. 2.0: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 4: Definitions and abbreviations“, IEC 04/2010

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION: “IEC 61508-5 Ed. 2.0: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 5: Examples of methods for the determination of safety integrity levels“, IEC 04/2010

[6] VOM HÖVEL, RÜDIGER; BRABAND, JENS ; 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 LNCS 5775, pp. 46-54, Springer-Verlag Berlin-Heidelberg 2009

3 Terms and abbreviations

3.1 Terms

Term	Definition	Reference
Accident	An accident is an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage.	EN 50129
Grade of automation	Automation level of train operation, in which Urban guided Transport (UGT) can be operated, resulting from sharing responsibility for given basic functions of train operation between operations staff and system	IEC 62290-1
Hazard	A condition that could lead to an accident.	EN 50129
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard or threat) and the degree of severity of that harm.	MODSafe
Safety	Freedom from unacceptable levels of risks resulting from unintentional acts or circumstances.	MODSafe
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
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.	Commission regulation (EC) No 352/2009
Tolerable hazard rate	Rate of occurrence of a hazard that would result in an acceptable level of risk for that hazard (normally judged acceptable by a recognized body e.g. railway authority or railway support industry by consultation with the safety regulatory authority or recognized by the safety regulatory authority itself)	CLC/TR 50126-2
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
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
D	Deliverable
E/E/PE	Electrical/electronic/programmable electronic
EN	European Standard
EUC	Equipment Under Control
GOA	Grade of Automation
IEC	International Electrotechnical Commission
MODSafe	Modular urban transport safety and security analysis
MODURBAN	Modular urban guided rail systems
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)
MTTH	Mean Time To Hazard (h)
MTTR	Mean Time To Restore (h)
PFD	Probability of Failure On Demand (average probability of dangerous failure on demand of the safety function)
PFH	Probability of Failure per Hour (average frequency of a dangerous failure of the safety function per hour, h^{-1})
PUI	Potentially Unsafe Incident
RA	Risk analysis
RAMS	Reliability, availability, maintainability, safety
SE	System Element / Safety Element
SIL	Safety integrity level
THR	Tolerable Hazard Rate
WP	Work package
λ_{SE}	Wrong side failure rate of the safety element (function) [$h^{-1]}$
λ_I	Occurrence rate of the potentially hazardous situation [h^{-1}]
μ_{SE}	Repair rate / inspection rate of the safety element (function) [h^{-1}]
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem
PFD_{avg}	Average Probability of dangerous Failure on Demand of the safety function, (PFD_{avg}), for a low demand mode of operation; it corresponds to its average unavailability (see IEC61508)
T_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (see above definition for *MooN*)

Abbreviation	Definition
μ_R	Repair rate of the safety function [h^{-1}] in case of undetected dangerous failures
μ_{SR}	Transition rate of the safety function [h^{-1}] in case of an occurred Potentially Unsafe Incident (hazardous situation) back into safe state
λ_{SYS}	Overall failure rate of the system (occupy the unsafe state) operating in low demand mode [h^{-1}]

4 Introduction

One of the substantial results of the MODSAFE project is the allocation of safety requirements to safety related functions which is intended to be performed by the work package WP4.

In deliverable D4.2 a general risk analysis (RA) and safety requirement allocation analysis approach had been introduced and applied to the majority of the safety related urban guided transport functions which had been defined in D4.2.

The mechanics of the risk analysis algorithms implied, however, the basic assumption that the safety function is required continuously to warrant its task. This means that the safety related functions deployed in high frequency Urban Guided Transport Systems shall permanently work without safety relevant (“wrong side”) failures to keep the system in a safe state, or, inversely, should the safety related function fail “wrong side” the risk group (passengers) is immediately in danger.

Examples for this artifact of the majority of the functions are “Supervise Safe Train Speed” (if overspeed is not safely detected due to a failure, the transport system becomes unsafe and immediate consequences are highly probable), “Authorize Train Movement by Wayside Signals” (if a signal shows a “Green” aspect instead of the intended “Red” aspect, the system is in an unsafe state and immediate consequences are highly probable), where immediate means at a scale of minutes or hours but not weeks, months or years. As an architectural consequence this means, that the function shall be built such that only very remote probabilities must be demonstrated which could lead to a wrong side failure in the continuously solicited function. For severe accidental consequences this means equivalently that the rate of occurrence of that system function failure event shall be at the lowest level of railway designs (SIL4 equivalent rates of 10^{-9}/h).

This is, however, not necessarily true for all safety related functions. Sometimes, a function is solicited only from time to time (not “continuously”, not a “High Demand” of the function, but rather at a “Low Demand”). Examples for this are “Detect Fire and Smoke”, where an undetected non-functioning fire detector that is repaired some weeks later during (frequent) inspection does not necessarily mean with high probability that a Fire Accident will occur until the next inspection (depending of course on the Fire Hazard rate). Another example may be “Detect Derailment”, where a wrong side failure of the function may be detected after a daily or weekly function check, but the likelihood that just in this relatively short inspection interval a derailment would occur is comparatively low.

In this deliverable low demand functions are considered as special type of functions which shall prevent from hazard with low or very low occurrence and which are not related to primary system hazards. For example: “derailment detection” covers the detection of a derailment, while a derailment can be assumed as a very rare event following assessed and approved measures in order to “ensure safe guidance of trains”, The function “collision detection” covers the detection of a collision with an object, while an obstacle in the guideway can be assumed as a very rare event following assessed and approved measures in order to avoid obstacles in the guideway. This is the precondition for train movements where the braking distance is longer than the sight distance and for GOA3 and GOA4. In this context the reader of D4.2 is advised to verify consistency of the low-demand character of the functions with this definition.

One architectural consequence of this brief analysis is that the “wrong side failure rate” itself does not need to be anymore necessarily at the highest level and becomes dependent on other features such as the estimated rate with which the hazard itself (that should be protected from) occurs, or the frequency of safe system diagnosis, checks, inspections etc. While the function in a broader context, including hazard reality and operational context, remains still at the highest safety level, the safety requirement (e.g. in the shape of a Safety Integrity Level equivalent rate) to the function in a narrower sense (i.e. the Derailment Detection Device function itself, or the Smoke Detector function itself) may change (read: “reduced”).

As intuitively clear the analysis may appear, as difficult it is to find commonly accepted or even understood definitions and formalisms that are adequate for the Urban Guided Transport Industry.

This deliverable will therefore briefly analyze first the most common normative reference (IEC 61508) and other materials, then return to the artifact of Low Demand functions thoroughly in its mathematical foundation, apply a possible Safety Requirement Allocation Scheme to functions and conclude on its suitability.

Please note, D4.3 is intended to give guidance how to control random failures for low demand functions to achieve a tolerable hazard rate. Systematic failures are not addressed in WP4. Different principles (design principles, quality checks, reviews, assessments etc.) are required in this case to protect from systematic failures. Here, the inspection pays attention to the discovery of random failures.

5 Low Demand Mode concept of IEC 61508

The European Standard EN50126 [1] which is currently under revision does not cover the concept of safety functions operating in Low Demand mode. A conceptual guideline how to systematically allocate safety integrity requirements to this type of functions is not addressed. Only a more general statement *“in the case that failure probabilities on demand are given, they have to be transformed in frequencies”* is made. Therefore, major reference is made to the generic safety standard IEC 61508 which clearly distinguishes between two modes of operation and outlines methods how to allocate safety requirements in either case.

5.1 IEC 61508-2, “Introduction”

The international standard IEC 61508 which specifies the Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems (E/E/PE), identifies already in the Introduction (IEC 61508-2, Introduction) two modes of operations/failures:

- “a low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its designed function on demand”
- “a high demand or continuous mode of operation, the lower limit is set at a probability of failure of 10^{-9}/h”

While in the CENELEC Standards EN50126, 50128, 50129 the (low) demand mode of operation has been withdrawn for the time being [1][2], the a priori high demand/continuous mode of operation safety target of the IEC 61508 matches the highest THR (SIL4 equivalent) of the CENELEC SIL table (see Figure 1).

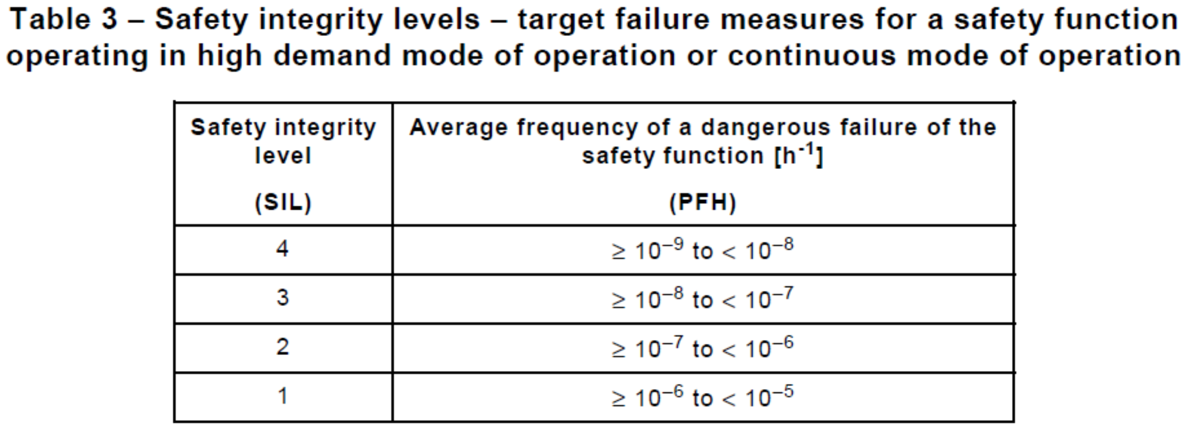

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 1 IEC 61508 SIL Table for High Demand or Continuous mode of operation

Since the SIL tables contain more than one value, the “lower limit” of the IEC 61508 definitions appears to coincide with the most conservative limit also. This is the case for the frequency of a dangerous failure of the safety function of 10^{-9} per hour which corresponds to a Safety Integrity Level 4.

Later chapters of the standard advise however for both modes of operation, to determine adequate safety integrity levels that do not in all cases reach the highest level, so the definitions in the Introduction of IEC 61508 is considered the most conservative limit if no further analysis is performed.

This interpretation is also supported by the SIL-Table vs. Averaged Probabilities of Failure on Demand as given by the below table of IEC 61508-1: According to this table, safety integrity levels are also defined for low demand mode of operation. However, frequencies (events per hour) of a dangerous failure of the safety function are not given in this context but a probability of a dangerous failure on demand is specified for the different Safety Integrity Levels.

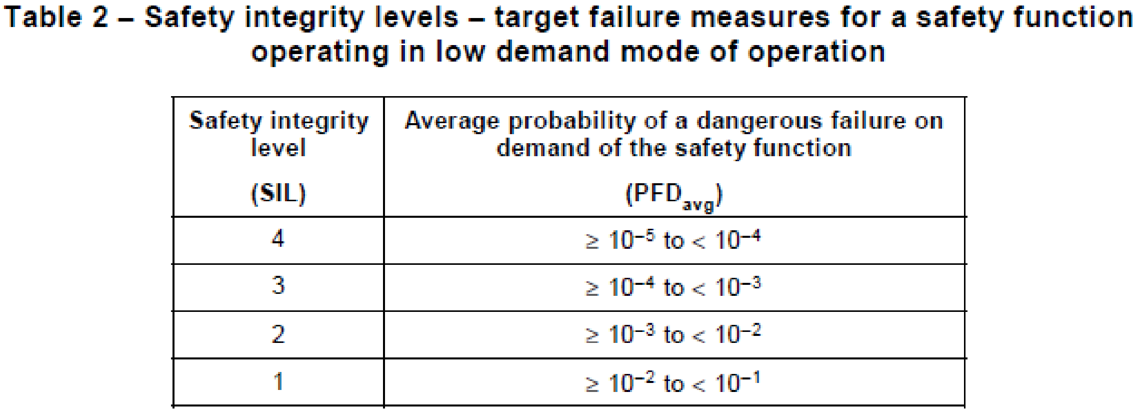

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Figure 2 IEC 61508 SIL Table for Low Demand mode of operation

In order to be in line with the relevant normative reference for railways, i.e. EN50126, this probability value which corresponds to a Safety Integrity Level (acc. Figure 2) needs to be transferred into a frequency. Achieving this requested transformation the safety integrity level for Low Demand mode of operation could then be expressed as a safety integrity level which is equivalent to those defined for Continuous mode of operation according to Figure 1. Therefore, this deliverable outlines an approach how to transfer failure probabilities into failure frequencies.

Regarding the Low Demand Concept, further precisions are found in paragraph 7.10.2.7 (Note 2 and Note 3) of the IEC 61508-1 [3], where the “target failure measures” to meet “required risk reduction” are compared to predefined SIL levels, where the targets shall be applied if the risk analysis requires it.

Paragraph 7.4.5.2 further details the previous definition by involving the concept of Diagnostics/Test Rates, where the application of the tests/diagnostics shall protect from leaving the system in undetected (dangerous) failure mode. Also probability calculation methods like Fault Tree Analysis, Reliability Block Diagrams or Markov Diagrams are introduced.

Paragraph 7.4.5.3 links the Diagnostics/Test Rates to the mode of operation by specifying:

“… credit shall only be taken for the diagnostics if … in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.”

Thus it may be treated like a function in low demand mode of operation.

If a system is demanded to control a hazardous situation for example once per year (10 000 h) and a “test” of system health is performed once per week then the system’s diagnostics can be taken into account as it would be for a “low demand” mode system.

Paragraph 7.4.8.2 defines consequently that – once the diagnostics/tests - have detected a dangerous fault (and the system is not fault tolerant), then the system shall go into a safe state or be repaired if this can be done faster than a Mean Time To Restore (MTTR).

By linking Safety to the diagnostics/test rate it is also a logical consequence, that chapter 7.6 (Operation and Maintenance) requires to take the "demand rate" of the system into account to determine the "frequency" of these detection tests as part of the maintenance.

Not consistent with the above specifications is the definition of IEC 61508-4, 3.5.16, where the low rate is defined as: "...where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; …".

The high demand mode is consequently defined as a system "…where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; …"

In paragraph 3.5.17 of IEC 61508-4 indicates the difference of target failure measure for

- Low demand mode: "the average probability of dangerous failure of the safety function on demand". This means, that in fact two limits reduce the numerical possibilities of achieving sufficient safety by dimensioning the safety target, the failure rate and the diagnostics/test rates. The first constraint is fixed on the combination of Failure Rate and Diagnostics/Tests and wrong side Failure Rate, which yield a "probability" that shall be below 10^{-5} that the system is in a failed state when "demanded" (necessary to maintain safety). The second constraint comes from the demand rate as such, which shall not occur more frequently than once per year (or with a rate less than 10^{-4}/h). The combination of both yields a rate of 10^{-9}/h for the situation, where a hazard or demand has occurred, the system has failed to protect against the hazard and this failure had not been diagnosed / revealed.
- High demand/continuous demand mode: "the average frequency of a dangerous failure [h^{-1}]"

These definitions are again in line with the specifications of part 2 of the standard, since involvement of a diagnostics/proof/test rate related to the failure rate defines a dimensionless "Probability" of not being able to perform the safety reaction when demanded, while in continuous mode the system is considered to be "always" solicited and the safety/risk level is therefore directly determined by the failure rate in hours.

Since for Urban Guided Transportation Systems the notion of demand "once per year" is hardly applicable ("continuous" would be a system that is required twice per year, which is not imaginable in our industry, where "continuous" means practically always, e.g. every minute) it is recommended to consider this numerical definition as inadequate but rather to observe the methodologies to be applied for the two different modes of operation.

It is therefore important, to consider the "Application Guide" IEC 61508-6 to see, what kind of methodologies are used to follow the intention of the standard, namely risk based calculations and estimation of Safety Targets.

5.2 IEC 61508- 6 "Application Guide"

The application guide resumes some definitions and an overview of standard relevant process elements.

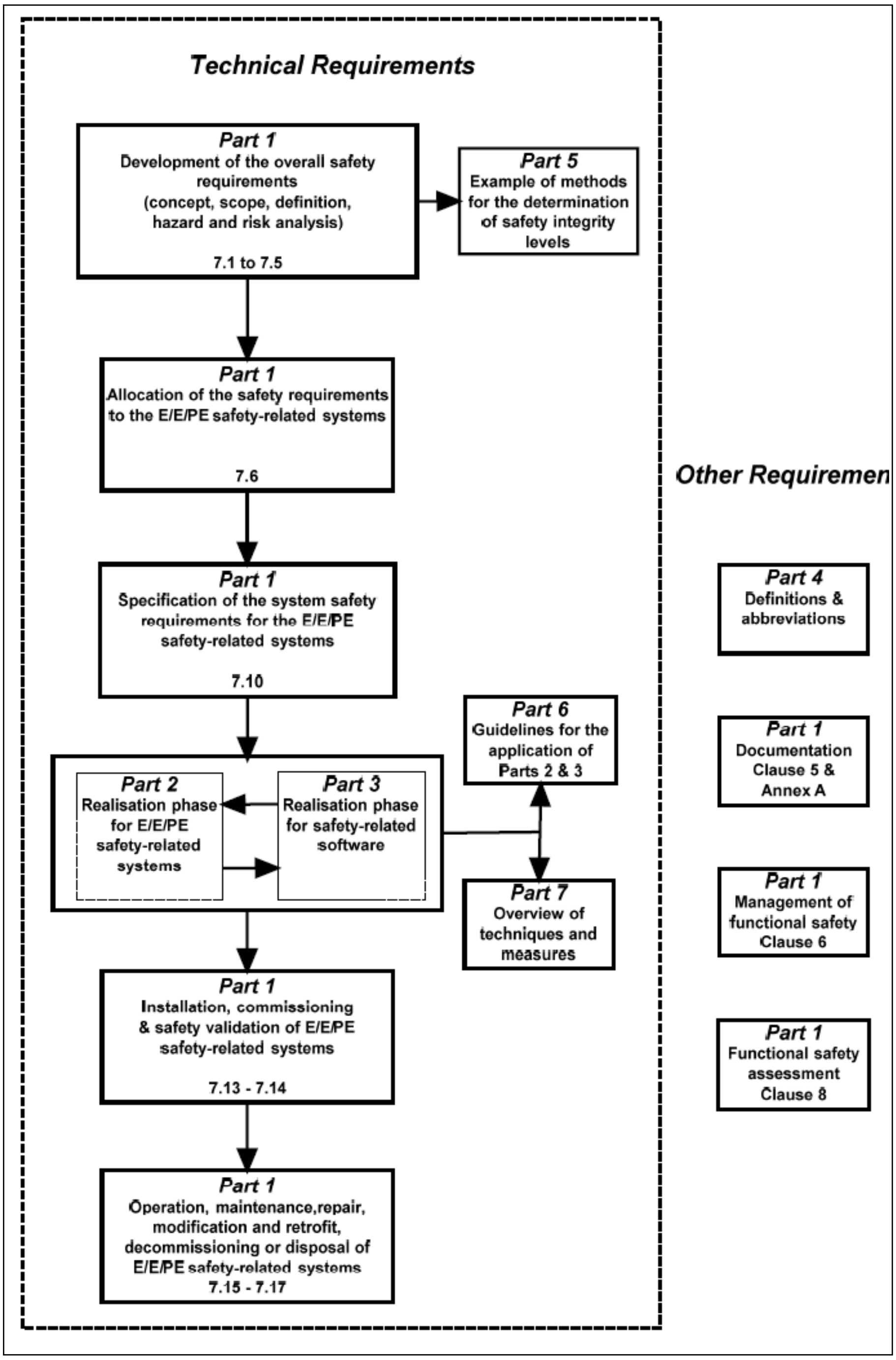
Technical Requirements
Part 1
Development of the overall safety requirements
(concept, scope, definition, hazard and risk analysis)
7.1 to 7.5
Part 5
Example of methods for the determination of safety integrity levels
Part 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
Part 1
Specification of the system safety requirements for the E/E/PE safety-related systems
7.10
Part 6
Guidelines for the application of Parts 2 & 3
Part 2
Realisation phase for E/E/PE safety-related systems
Part 3
Realisation phase for safety-related software
Part 7
Overview of techniques and measures
Part 1
Installation, commissioning & safety validation of E/E/PE safety-related systems
7.13 - 7.14
Part 1
Operation, maintenance,repair, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 - 7.17
Other Requiremen
Part 4
Definitions & abbreviations
Part 1
Documentation Clause 5 & Annex A
Part 1
Management of functional safety Clause 6
Part 1
Functional safety assessment Clause 8

Figure 3 Overall framework of the IEC 61508 series

In order to obtain, high safety levels, “supervised” systems like 1oo2, 2oo3 or other checked systems (inspections, tests, diagnostics) etc. are introduced, where for the “supervision” interval category values between a month and 10 years are given in table B.1. The requirement for such an interval or rate comes from the fact, that in particular with Low Demand systems a possible Failure Rate of the E/E/EP must be converted mathematically into a probability. The Application Guide recommends again Fault Tree Calculations, Markov Models or Reliability Block Diagrams as methods to perform these calculations.

Annex B, subclause B.3.2 “Average Probability of Failure on Demand” models the safety systems generally by a sensor subsystem, a logic subsystem (processors etc.), and a final element subsystem (outputs, etc.). Assuming individual failure rates, each of these subsystems may be calculated independently. As a model for the simplest architecture, Figures B.4 and B.5 in IEC 61508-6 show a 1oo1 system, where the safety channel is working without being permanently compared to other channels, but diagnosed. The Reliability Block Diagram of this simplest architecture shows the reasoning, according to which the system is out of order with a certain failure rate and restored for service after the MTTR = $1/\lambda_{DD}$, and in order to calculate a probability from these rates a time element T_{CE} is introduced, which is the equivalent mean down time (hour) of the system. A total (not strictly calculated) rate for the combination yields PFD=$(\lambda_{DU} + \lambda_{DD})*T_{CE}$.

The question of how useful this result is for concrete applications depends certainly on the capacity to detect safety relevant failures, it is in railways more this rate that determines the safety than the pure restoration time/rate.

The subsets and Figures B.6 to B.13 show the respective formulas for 1oo2, 2oo3 architectures and lists numeric estimations in Table B.2.

While for the transportation industry the different architectures are all deployed and used, there calculation results cannot be utilized to respond to the question of how a 1oo1 system’s overall safety level is calculated if the diagnostic is not functioning immediately and safely.

IEC 61508-7 resumes numerous particular concrete methods (like memory checks, path checks etc.) that may be used to supervise intrinsically the functioning of E/E/PE without addressing the above questions again.

5.3 Summary of Low Demand Rate Safety Calculations according IEC 61508

Compared to other standards the IEC 61508 has the clear merit of introducing analytic methods to calculating risk levels and various rates of possible safety architectures. Also, it introduces clearly the differentiation between “Continuous” High Demand Safety Systems where every single wrong side failure leads directly to hazardous situations, and Low Demand Safety Systems where the concept of safety systems is introduced that may fail, but not necessarily produce by this failure immanently a safety problem. To analytically better describe this situation, various notations and also limits are introduced that require, however, relatively complicated mathematical probability calculations. The methodologies are introduced in the standard and examples are given.

The disadvantage of employing directly the standard to the specific situation of railway/urban guided transport systems requires, however, to re-consider once again the basic problem of Low Demand safety systems utilizing the advised methodologies and then compare it to other listed examples in the standard.

5.4 Probability of Failure on Demand –The Why and the How

The article investigates similar to the analysis of this deliverable the concept and calculation of the Low Demand Mode operated systems and attempts to provide calculation prescriptions [6].

First the paper analyses the IEC 61508 concept of low demand mode systems (here concentrating on the “Probability of Failure on Demand”) and detects confusions in the definitions and the insufficiency of the fact that only one numerical example definition (“once per year”) is given in the norm. As previously noted in this deliverable, also the paper finds the “once per year” definition inadequate by the statement: *"…defining a system with low-demand mode of operation as a system with not more than one request per year is at least problematic*" [6].

Similar to this deliverable's analysis the basic differences between continuous mode (*"…dangerous failure …immediately lead to a dangerous failure of the system*" [6]), assumes for further considerations constant failure rates and restricts the analysis to the passenger's individual risk.

The analysis identifies the risk reduction principle in the Low Demand Mode of operation with checking or proof or supervision system by a definition: "*here, the safety-related system has a supervisory function*", which is also in line with this deliverable's conclusion.

After further analysis, the paper comes to a preliminary conclusion that "*The relation between the PFD and PFH as given in IEC 61508 lacks a sufficient logic*" (PFD = Probability of Failure on Demand, PFH = Probability of Failure per Hour) [6].

To obtain a clearer view of how the supervisory interval, failure rate and incident rates depend on each other in terms of ultimate safety, the paper follows a very similar approach then this WP4 deliverable by suggesting the calculation of the relevant Markov Diagram, which is given below:

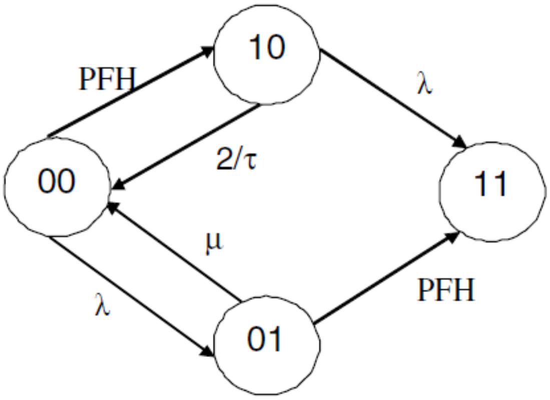

Fig. 2. Simple alternative Markov model

Figure 4 Example MARKOV model for state modeling

Since the paper uses different abbreviations and conventions a comparison shall identify the parameters. The PFH (average frequency of a dangerous failure of the safety function per hour) corresponds to the rate λ_{SE}, i.e., the wrong side failure rate of the safety element. The parameter λ describes the hazard occurrence rate (occurrence rate of the Potentially Unsafe Incident) and is equivalent to λ_I used in this report. The parameter μ is equivalent to a transition rate back into the safe state "00" in case the hazard has occurred with rate λ. This report uses the parameter μ_{SR} (Safe Reaction) instead. The repair rate/inspection rate of the safety function in case of failure PFH is expressed through 2/τ. It corresponds to the parameter μ_{SE} which is used in this report.

Different to our calculation is the fact, that the above Markov Diagram retains the state "01", which is a state where the safety system is required by the incident and reacts safely so that the system returns to the safe state "00". In the diagram presented in this report (see Figure 9 on page 23) this state is neglected for simplicity of calculation and for the observation that if the safety system is up and running the state "01" can also be considered a "safe state". The system shows either fail safe behavior or a dedicated safe reaction.

Also, the paper stops short of giving one final relationship, but concludes with an equation system for the ultimate hazard rate MTTH (Mean Time To Hazard). However, adequate approximations in the calculation would yield the same result:

$$MTTH = \frac{1}{\lambda + PFH} + \frac{\lambda}{\lambda + PFH} MTTH_{01} + \frac{PFH}{\lambda + PFH} MTTH_{10}$$

$$MTTH_{01} = \frac{1}{\mu + PFH} + \frac{\mu}{\mu + PFH} MTTH$$

$$MTTH_{10} = \frac{1}{\lambda + {}^{2}\!/_{\tau}} + \frac{{}^{2}\!/_{\tau}}{\lambda + {}^{2}\!/_{\tau}} MTTH$$

In conclusion, the above publication identifies the same deficiencies of the direct application of the IEC 61508 standard to railway applications, and takes a surprisingly parallel approach for a more neutral consideration of the basic relationships.

6 Fundamental Context Analysis

6.1 Introduction and Methodology

Since it was noted above that the IEC 61508 provides the correct and applicable methodologies but is in its examples and time scale definitions not specifically a railway standard, it is useful to consider again the fundamental relations between Hazards, Failures, Diagnostics/Tests/Checks etc., and safety function Demands.

On the Methodology, the standard introduces in IEC 61508-6 the details of the formalism of Markov Diagrams and their calculations, which appears well adjusted to the problem. Other methods, such as Fault Tree Analysis, are not explored in the rest of the document and would need to be checked for applicability. Since IEC 61508 directly proposes Markov Models for this kind of analysis, this approach had been taken to be compliant with IEC 61508.

As an example of a graphical representation of such a graph see Figure 5 representing possible failure states and state transitions of a system consisting of two components A and B.

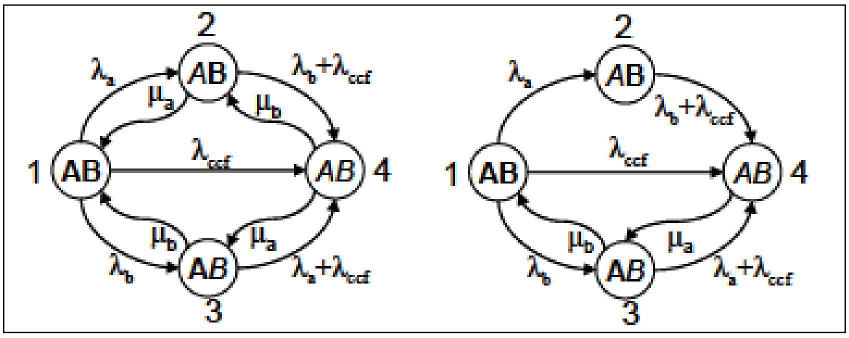

Figure 5 IEC 61508-6 Markov graph examples of a redundant system

This kind of graph represents the states that a system may adopt and also the transitions/transition rates between them. In Figure 5 a system consisting of two components A and B is assumed. Either of the components A or B may fail which is indicated by the failure rate λ_a and λ_b and transfer into states 2 or 3, respectively. Consequently, both components can also be repaired with repair rates μ_a and μ_b and return into state 1. In case of one failed either A or B the other component may fail too and the system goes into state 4. This state 4 can also be reached in case of common cause failures either from state 1 directly or from the states 2 or 3. The common cause failure rate is the parameter $\lambda_{ccf.}$

When arranging the possible states in a “state vector” and all transitions between every respective pair of states in a “Transition Matrix” M, then the probabilities $P_i(t)$ i = {1, …, 4} of the system being in any of the possible states can be calculated, either in the Time domain or Laplace space.

Taking the above example of a redundant system, neglecting common cause failures, then the vector equation in the time domain would have the shape

$$\begin{pmatrix} \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \\ \dot{P}_4(t) \end{pmatrix} = \begin{pmatrix} -(\lambda_a+\lambda_b) & \mu_a & \mu_b & 0 \\ \lambda_a & -(\lambda_b+\mu_a) & 0 & \mu_b \\ \lambda_b & 0 & -(\lambda_a+\mu_b) & \mu_a \\ 0 & \lambda_b & \lambda_a & -(\mu_a+\mu_b) \end{pmatrix} \begin{pmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{pmatrix}$$

or – in Laplace space -

$$\begin{pmatrix} s+\lambda_a+\lambda_b & -\mu_a & -\mu_b & 0 \\ -\lambda_a & s+\lambda_b+\mu_a & 0 & -\mu_b \\ -\lambda_b & 0 & s+\lambda_a+\mu_b & -\mu_a \\ 0 & -\lambda_b & -\lambda_a & s+\mu_a+\mu_b \end{pmatrix} \begin{pmatrix} F_1(s) \\ F_2(s) \\ F_3(s) \\ F_4(s) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Solving it (either in Time or Laplace Domain) yields for example for the State 4 (which is the state where neither component A nor component B work)

$$P_4(t\to\infty) = \frac{\lambda_a\lambda_b}{(\lambda_a+\mu_a)(\lambda_b+\mu_b)} = \frac{\lambda_a}{\lambda_a+\mu_a}\cdot\frac{\lambda_b}{\lambda_b+\mu_b} = U_a\cdot U_b = U_{1oo2}$$

which gives just the Unavailability of the simple redundant system as known from other sources and calculations. U_a is the unavailability of component A, U_b is the unavailability of component B and U_{1oo2} indicates the unavailability of the overall system in a 1-out-of-2 configuration.

On the non-redundant (single) system that is operated in the Low Demand mode, the IEC 61508-6 imagines a system, that knows a state of non-failed (intended) functionality, a state where it fails with a certain rate λ_{DD} into a non-functioning state but the failure is detected, and a state where it fails with another rate λ_{UD} into a non functioning state where the failure is, however, not detected. The system is tested with a certain rate (τ) if everything is still in order. Failed components can return to their nominal state with a “repair” rate μ (1/MTTR), provided however, the system is “known” to be in a failed state.

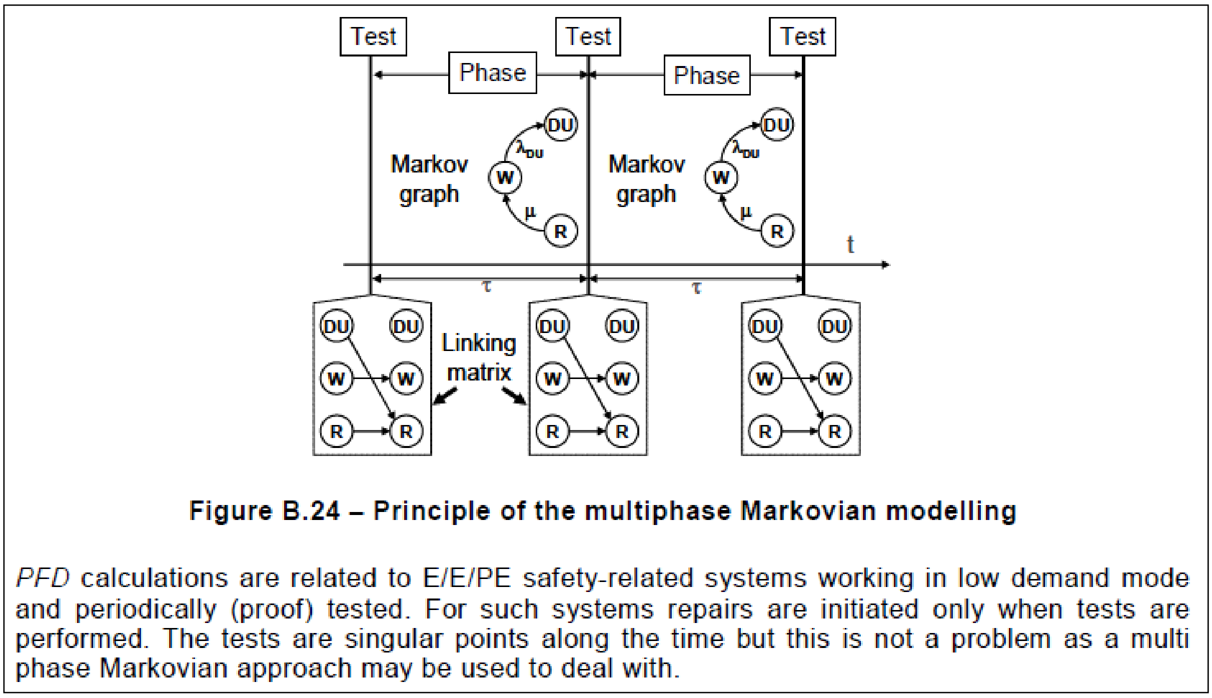

Figure B.24 – Principle of the multiphase Markovian modelling

PFD calculations are related to E/E/PE safety-related systems working in low demand mode and periodically (proof) tested. For such systems repairs are initiated only when tests are performed. The tests are singular points along the time but this is not a problem as a multi phase Markovian approach may be used to deal with.

Figure 6 Low Demand mode systems of IEC 61508 know several rates as explained in the text.

It shall be noted, that for the pure safety consideration of Urban Guided Transport Systems, the complication of including “detectable” failures may be neglected, since it simply means we stay in the safe state (which is the nominal state). Once we detect failures, the system turns into safe state, e.g.

through a failsafe mechanism. For the sake of simplification and to keep the approach applicable the test shall be considered complete.

Secondly, the problematic situation (but not necessarily an accident) arises, when the system is in a failed state (not performing its safety task) and a hazard – or better potentially unsafe event – arrives before a next test/proof/inspection/etc. reveals the failed state of the component.

To obtain a more complete situation, the (independent) potentially unsafe event should be included in the graph, and the complete system be analytically evaluated.

6.2 Low Demand Mode System Context and Fundamental Analysis

In order to model the context of a safety system in the Low Demand Mode, the elements and events need to be defined, as well as the states they may be in and the transitions between them.

The element of investigation in the analysis is called “System Element” or “Safety Element” SE and shall be the function or device that shall control a Potentially Unsafe Incident (PUI) which may arrive with a rate of λ_I not to develop into a Hazard. The System Element may fail from time to time (with a constant rate λ_{SE}) into a state where it may not be able to serve its safety purpose anymore. It may leave this failed state with a certain repair rate but in order to be repaired the failure must first be detected.

For Low Demand mode of operation it is assumed, that the health state of the system is not continuously checked (proof test, inspection, diagnostic etc.) but “only” with a rate μ_{SE} that is much larger than the failure rate and the PUI incident rate (e.g. 10, 100 or 1 000 times). In case of detected failures we assume the system to be transferred back into a safe state. Typically this may be achieved through a safety switch off of the system. For example, a train with a train door propulsion failure, e.g. door does not close anymore, will be removed from service, people have to get off the train, etc. The repair of this train of course takes some time but the system is in a safe state again. More general speaking, in case of equipment failure, may it be track circuits, signals or onboard obstacle detection devices, a degraded operation mode is initiated (controlled by personnel in a safe manner) and the system remains in this safe state until the failed component has been restored. However, for our calculation we can consider the system to be in a safe state again. Thus, the detected failures are assumed to not critical from a safety point of view. Consequently, for the safety analysis only the undetected failures are taken into account.

As an example of the rate relations, consider a Derailment Detector in an Unmanned Train Operation that signals whether a train had derailed or not, where the Derailment itself may occur with a rate of $\lambda_I \sim 10^{-4}$/h (once per year, in real systems a conservative assumption), the Detector Device/System Element may fail undetected to perform the detection task with a rate of $\lambda_{SE} \sim 10^{-6}$/h, and the device is checked for undetected failure once per day with $\mu_{SE} \sim 10^{-1}$/h.

For the nominal, intended behavior of the system, the System Element is properly functioning when the Potentially Unsafe Incident occurs. The system is then for a relatively very short time $1/\mu_{SR}$ in a state of Safety Reaction or Safety Reset. Since the system remains safe during this time and the rate is relatively very high this branch of the graph could also be neglected.

Remains one more state, where the System Element has failed, the system had not yet been checked/inspected/tested, and the Potentially Unsafe Event occurs. In this state, the system is not safe anymore, and all other rates must be designed such that the probability for this state is acceptably low. Formally the question emerges of how the system does ever leave again this unsafe state. Conservatively, an accident is likely to occur and after the accident the system is restored with a relatively low rate of μ_R.

Figure 7 gives a timeline example representation of the discussed situations.

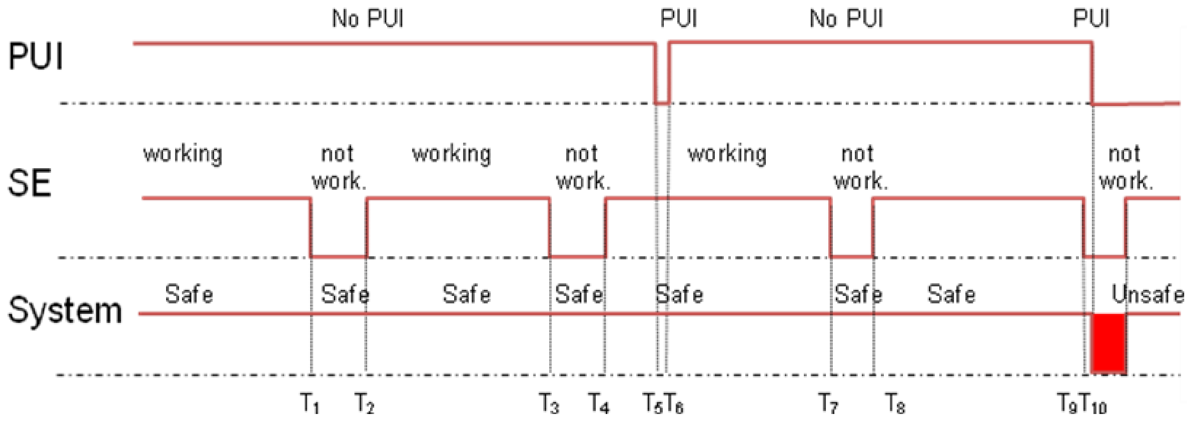

Figure 7 Illustration of events over time

From the above discussion, it becomes obvious that two independent variables namely the

1. state of the safety function / safety element and the
2. Potentially Unsafe Incident (hazardous situation)

exist which can have to different states each, i.e.,

1. working / failed
2. not occurred / occurred.

In total, this yields four different states which the system can be in.

State of the safety function / safety element

		Working	failed
Potentially Unsafe Incident (hazardous situation)	not occurred	S1	S2
	occurred	S4	S3

Figure 8: Combination of occurrence of the Potentially Unsafe Incident and failure of the Safety Function

Each of these states is characterized as:

S1: The Potentially Unsafe Incident has not occurred, the Safety Element works, the system is in a safe state

S2: The System Element has failed (undetected) to perform its safety function with a certain wrong side failure rate λ_{SE} until a test reveals the failure and the System Element is repaired with a repair/inspection rate μ_{SE}, all while the Potentially Unsafe Incident has not occurred; the system remains in a safe state

S3: The Safety Element failed (the system went through state S2 into S3) and the Potentially Unsafe Incident occurred with the hazard occurrence rate λ_I while the System Element is not yet fixed, System is in an unsafe state. In principle, the system could return into the safe state S1 with a certain repair rate μ_R.

S4: The Safety Element is working properly while the Potentially Unsafe Incident occurs with the hazard occurrence rate λ_I; the system is returning through safety reaction with rate μ_{SR} into the nominal state and is not in an unsafe state.

The central question of this analysis is how the probability to end in the unsafe state (S3) can be expressed as a function of the other rates that had been introduced. For this, a Markov Graph representation is shown in Figure 9.

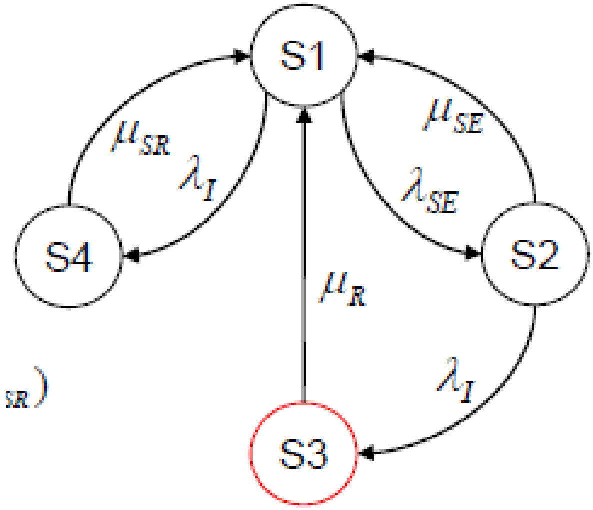

Figure 9 Markov Graph representation for a Low Demand mode operated System

A state transition matrix can be established for the above graph, yielding the following Equation System (already in Laplace space):

$$\begin{pmatrix} s+\lambda_I+\lambda_{SE} & -\mu_{SE} & -\mu_R & -\mu_{SR} \\ -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 & 0 \\ 0 & -\lambda_I & s+\mu_R & 0 \\ -\lambda_I & 0 & 0 & s+\mu_{SR} \end{pmatrix} \begin{pmatrix} F_1(s) \\ F_2(s) \\ F_3(s) \\ F_4(s) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

By utilizing the Cramer-Rule, a solution for $F_3(s)$ in the Laplace Space is found through the Quotient of the Sub-Determinant D_3 and the full Determinant D (the complete calculation is given in the annex) and the limit value in the time domain is calculated as indicated below:

$$\lim_{t\to\infty} P_3(t) = \lim_{s\to 0} s \cdot F_3(s) = \lim_{s\to 0} \frac{s \cdot D_3(s)}{D(s)} \approx \frac{\lambda_{SE}\lambda_I\mu_{SR}}{\mu_R\mu_{SE}\mu_{SR}} = \frac{\lambda_{SE}\lambda_I}{\mu_R\mu_{SE}} = \left.\frac{\lambda_{SE}\lambda_I}{\mu_{SE}}\right/\mu_R$$

For our purpose, this limit value means, that over longer times the system behaves like if there exists a “failure rate” λ_{sys} that determines the frequency with which the system develops into a state, where a Potentially Unsafe Incident arrives, but the protective System Element has failed before (with λ_{SE}) and the inspection has not discovered the failure or the restoration had not yet been completed due to the rate μ_{SE} (so the System Element is not in correct state); consequence would be as discussed above an unsafe situation.

$$\lambda_{sys} = \frac{\lambda_{SE}\lambda_I}{\mu_{SE}}$$

6.3 Discussion of the Result

Since the result of the previous chapter is obtained independently of minor variations of the Markov Graph, it appears to reflect the fundamental system behavior and deserves a discussion.

From the dimension, the λ_{sys} is a rate, i.e. in Failure/hours; from the basic graph it is clear that it is the rate with which the system may occupy the unsafe state. For the operator, it is this rate that determines the ultimate safety of the system and the residual risk, respectively, Should the consequence of the unsafe state be a catastrophic event, then it is clear that the rate should be equivalent to the THR of 10^{-9}/h.

Coming back to the requested transformation of failure probabilities into failure rates (see Section 5.1) by EN50126 it is this overall rate which is of interest from a safety point of view. This rate is formed from the failure probability (for low demand mode of operation) by taking into account the hazard occurrence rate.

On the right side, an expression of three rates forms a quotient that shows how the ultimate safety level is reached. It can be read like the rate with which a potentially unsafe event may appear (λ_I), but since a protection or safety System Element had been implemented, this rate is not directly developing into an accident. Instead, the rate must be suppressed by the likelihood that the System Element is not failed or the failure had been discovered. This likelihood is expressed by the relation of the diagnostic/check/test interval to the failure interval (or the inverse, i.e. the respective rates), giving

$$P = \frac{\lambda_{SE}}{\mu_{SE}}$$

Therefore, this relation expresses the failure probability in case of low demand mode of operation according to Figure 2 but can the transferred into a failure rate according to Figure 1 for continuous functions.

The System Element failure rate λ_{SE} is a rate similar to the safety integrity level concept for continuous systems, meaning that it determines the frequency that the system fails unsafely, except that in Low Demand operated systems this failure does not instantly lead to accidental consequences, since the potentially unsafe situation may not be present (as it is “low” in demand and not “continuously” present).

Compared to the IEC 61508, the norm sets a default value for λ_I by definition (less frequently than once per year, meaning $\lambda_I < 10^{-4}$/h), which explains why the highest safety level as Low Demand rate oriented SIL is set to a probability (not rate!) of 10^{-5} as 10^{-5} x 10^{-4}/h=10^{-9}/h.

In default variation of the IEC 61508 this means, that the probability $\frac{\lambda_{SE}}{\mu_{SE}}$ determines the SIL, leaving to the system designer the possibilities to select an adequate ratio of System Element failures λ_{SE} and supervisions μ_{SE}, inspections, tests etc. A value of for example 10^{-5} may be reached equally by $\lambda_{SE}=10^{-7}$/h and $\mu_{SE}=10^{-2}$/h or $\lambda_{SE}=10^{-5}$/h and $\mu_{SE}=1$/h.

While the fundamental relationship matches obviously with the IEC 61508 intentions, definitions and examples, it becomes again clear, that arbitrary example definitions of the IEC 61508 (like for λ_I) do not necessarily match the time scales and dynamics of a railway or Urban Guided Transport System. Since all three parameters characterizing the safety of a low demand system (λ_I, λ_{SE}, μ_{SE}) are varying parameters that may be different from application to application, it is recommended to utilize the fundamental relationship between them. Determining an equivalent safety integrity requirement for a system operated in Low Demand mode means therefore for an operator, to first determine approximately the appearance rate λ_I for the Potentially Unsafe Event and the consequences (determining the THR). In the next step the relation between the failure rate λ_{SE} of the Safety Element and the inspection rate $\mu_{SE\ must}$ be chosen accordingly to satisfy the overall failure rate λ_{sys} (system in unsafe state).

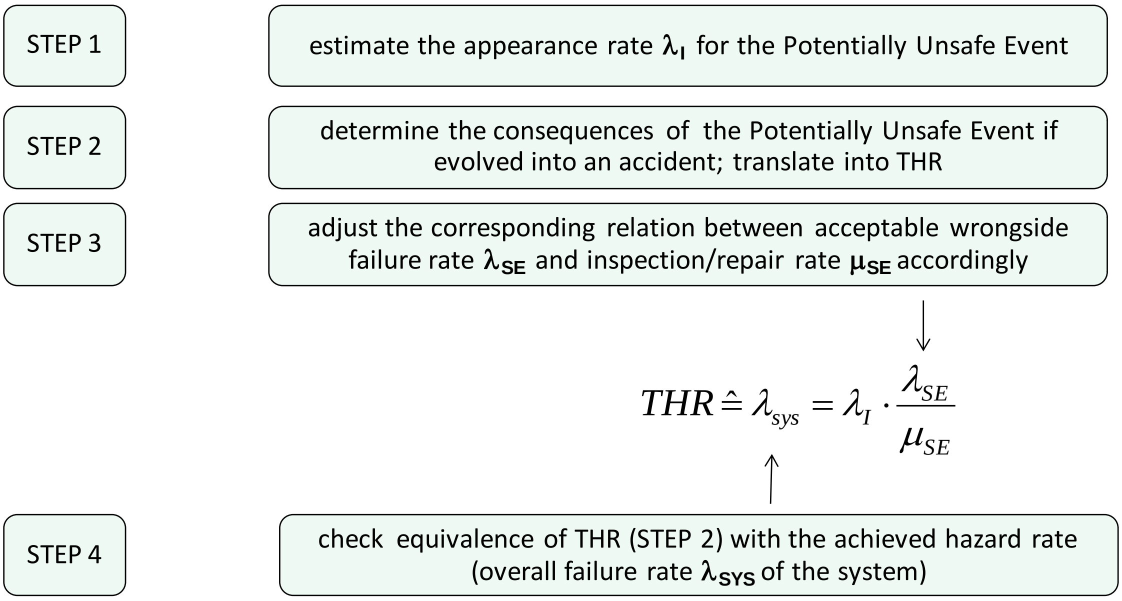
STEP 1
estimate the appearance rate λI for the Potentially Unsafe Event
STEP 2
determine the consequences of the Potentially Unsafe Event if evolved into an accident; translate into THR
STEP 3
adjust the corresponding relation between acceptable wrongside failure rate λSE and inspection/repair rate μSE accordingly
THR ≙ λsys = λI · λSE/μSE
STEP 4
check equivalence of THR (STEP 2) with the achieved hazard rate (overall failure rate λSYS of the system)

Figure 10: Determination of a safety integrity requirement for functions operating in Low Demand mode

If the process is applied to the example of the Derailment Detection Device, then first a $\lambda_I=10^{-4}$/h may be estimated conservatively by the operator. Secondly, the severity category of “Catastrophic” implies directly a THR=10^{-9}/h, leaving for the failure probability a value of P=10^{-5}. Furthermore, a relation of $\lambda_{SE}=10^{-6}$/h divided by $\mu_{SE}=10^{-1}$/h would satisfy this failure probability.

Note: The discussed fundamental relationships between SIL Allocations and Probability of Failure on Demand may be utilized for multiple purposes. Assume for example a GOA4 Urban Guided Transport System, where the track area in the station shall be monitored safely by a function “Supervise Platform Tracks” such, that if someone falls accidentally into the track (e.g. λ_I ~10^{-4}/h/platform track), and the monitoring itself can be demonstrated to achieve a wrong side failure rate of λ_{SE} ~ 10^{-5}/h and the question emerges of how often the correct performance of the monitoring system must be checked. Then, it can directly be derived:

$$\frac{THR}{\lambda_I} = \frac{10^{-8}/h - 10^{-7}/h}{10^{-4}/h} = 10^{-4} - 10^{-3}$$

$$\rightarrow \frac{\lambda_{SE}}{\mu_{SE}} = \frac{10^{-5}/h}{\mu_{SE}} = 10^{-4} - 10^{-3} \rightarrow \mu_{SE} = 10^{-2}/h - 10^{-1}/h$$

This calculation would determine consistently the monitoring/check interval to 10h-100h.

Vice versa, if the system would be checked with every train entrance (μ_{SE}~10^{1}/h), the still acceptable wrong side failure rate of the System Element would be λ_{SE}~10^{-3}/h-10^{-2}/h. Anyway, the ultimate rate λ_{sys} which describes the safety of the system from an operator point of view would equal a hazard rate of 10^{-7}/h to 10^{-8}/h as found acceptable by the determined THR.

In the context of Low Demand functions, IEC61508 proposed an arbitrary boundary between low demand and high demand functions of one year which was shown to be problematic for applications the railway domain. Although, an alternative boundary could have been proposed a more general approach had been taken in this deliverable with the direct calculation of the Markov graph. The developed formula clearly shows that the definition of such an arbitrary boundary is not necessary but can be substituted by the direct estimation of the three rates and the calculation of the ultimate hazard rate λ_{sys} of the system.

However, in order to distinguish between low demand and high demand functions the concept of very special functions has been proposed. In this context “very special” refers for example to functions which are used to protect against secondary hazards with low or very low occurrence. One example is the derailment detection device. Typically derailments are prevented by correct alignment of tracks and proper maintenance of tracks. For the residual risk we could use the Derailment Detection Device especially in case of unattended train operation such as GOA4. For example, an Onboard Obstacle Detection Device would also fall into this category, because typically no objects are expected to be on the guideway. Defined operational rules and measure exist to assure clearance of the track from obstacles or trains. This would include for example Safe Train Separation by the ATC or defined rules for trackside maintenance work to make sure no objects are left behind. However, because obstacles on the track might impose an additional risk in case of unattended operation, an Obstacle Detection Device might be installed. In this context the reader of D4.2 is advised to verify consistency of the low-demand character of the functions with this definition.

7 Conclusion

This deliverable is a proposal how to deal with low demand safety functions based on IEC 61508 concepts, because EN 50126 and EN 50129 do not cover the allocation process for low demand functions.

The deliverable reviews the concept of Low Demand safety functions described in IEC 61508 for generic purposes regardless of the urban guided transport domain. This concept is then adapted to the specific environment of urban guided transport taking into account the typical time scale for hazard and accident scenarios in the context of urban railways. Based on IEC 61508 a generic state model based on Markov-Chain theory is developed to describe Low Demand applications.

Based on this approach a Safety Integrity Requirement Allocation Scheme is described which can be used to determine a SIL equivalent safety requirement, in terms of an ultimate rate λ_{sys} which expresses the failure frequency of the system, i.e., the system is in an unsafe state. The requirement allocation scheme takes into account three different parameters, which characterize the safety of a Low Demand system. First, the hazard occurrence rate (demand rate) λ_I shall be considered. Secondly, the wrong side failure rate of the safety function λ_{SE} and finally the inspection rate μ_{SE} to check the correct functionality (no undetected failure) are required to determine a SIL equivalent overall safety integrity requirement.

Determining an equivalent safety integrity requirement for Low Demand Mode operated system means therefore for an operator, to first determine approximately the occurrence rate for the potentially unsafe event and the consequences (determining the THR) and from this determine the failure probability value for the protection/safety system. This failure probability then needs to be transferred into a failure rate (frequency) by taking into account the inspection rate and the acceptable wrong side failure rate of the system. Of course, the acceptable wrong side failure rate and the inspection rate need to be balanced and decisions have to be made whether to accept a solution which needs to be inspected very often but may have a higher failure rate (be less complex from a technical point). Vice versa a very reliable and more complex technical solution with a lower failure rate would need less inspection. This arbitration should be agreed upon between supplier (responsible for the technical system) and the operator (responsible for adequate maintenance).

Since the SIL equivalent safety integrity requirement for Low Demand functions depends on a construct of three different parameters which even depend strongly on the specific circumstances of each operator, e.g., maintenance and inspections schemes and requirements as well as occurrence rates of events outside the typical operational processes no generic safety requirements can be determined for different Low Demand safety functions.

This approach which takes into account specific circumstances such as maintenance and inspection strategies should be agreed upon among the Operator, the Independent Safety Assessor and the Safety Authority – where relevant – to explain and justify the specific assumptions for a certain low demand function.

For the sake of simplification and to simply demonstrate the issue of Low Demand safety functions in principle, only one failed equipment (Safety Element) has been taken into consideration. However, the Markov model might be extended to deal also with several equipment and thus several safety barriers. Additional states and state transitions would have to be introduced in this case and the corresponding wrong side failure rate as well as the inspection rate would have to be taken into account.

Examples are included in Annex 8.1 which shall illustrate the mechanism of the proposed method in principle but may of course vary from operator to operator.

8 Annex

8.1 Allocation of safety requirements to Low Demand safety functions

Since the SIL equivalent safety integrity requirement for Low Demand safety functions depends on a construct of three different parameters which even depend strongly on the specific circumstances of each operator, e.g. maintenance and inspections schemes and requirements as well as occurrence rates of events outside the typical operational processes no generic safety requirements can be determined for different Low Demand safety functions. Thus, only three examples are described hereafter which shall illustrate the nature of the proposed method in principle but may of course vary from operator to operator.

8.1.1 Detect fire and smoke

Item	Description	
Number of safety function	68	
Name of safety function	**Detect fire and smoke**	
Description	This function is intended to detect fire and smoke aboard trains.	
Reference of functions	New for MODSafe	
Reference for risk analysis	None	
Possible wrong side failure	Device does not detect fire onboard the train.	
Hazardous situation	Person exposed to smoke onboard the train. Suffocation of passengers from smoke.	
Possible hazard consequences – accidents	Due to failed fire detection the detection is delayed but still possible by passengers onboard the train. Immediate reaction to a small fire is not possible, thus passengers are exposed to more severe smoke. Severe person injuries or death may be the consequence.	
Severity of consequences due to failure of the Low Demand safety function	critical	
Required THR	10^{-8}/h	
Hazard occurrence rate λ_I	We assume a hazard occurrence rate for a burning train of one million hours, which corresponds to a $\lambda_I = 10^{-6}$/h	
Required failure probability on demand (THR / λ_I)	10^{-8}/h / 10^{-6}/h = 10^{-2}	
Wrong side failure rate λ_{SE} of the safety function	10^{-3}/h	10^{-3}/h / 10^{-1}/h = 10^{-2}
Inspection rate μ_{SE}	10^{-1}/h	
Achieved Hazard Rate and corresponding SIL	$\lambda_I \times \lambda_{SE} / \mu_{SE} = 10^{-6}$/h x 10^{-3}/h / 10^{-1}/h = 10^{-8}/h residual risk is equivalent to SIL 3 according to Figure 1	

Should we assume an inspection rate of 10^{-1}/h a wrong side failure rate of the detection function of 10^{-3}/h would be acceptable to achieve the overall SIL equivalent for the Low Demand mode of operation of the safety function.

The wrong side failure rate of the equipment (here smoke detector) is only 10-3/h, i.e., no SIL in the classical sense (for continuous functions). In total – taking into account – the hazard occurrence rate, the inspection rate and the wrong side failure rate, the risk is reduced to a level which corresponds to SIL3. However, this SIL in the context of Low Demand is not only for the wrong side failure rate of the safety function but of the unsafe event (formed by the hazard occurrence rate, the inspection rate and the wrong side failure rate)

8.1.2 Supervise platform tracks

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>Number of safety function</td><td colspan="2">37</td></tr>
<tr><td>Name of safety function</td><td colspan="2"><b>Supervise platform tracks</b></td></tr>
<tr><td>Description</td><td colspan="2">This function is intended to supervise the actions of an external platform track detection device to stop the train in case of intrusion of person.</td></tr>
<tr><td>Reference of functions</td><td colspan="2">IEC62290-2</td></tr>
<tr><td>Reference for risk analysis</td><td colspan="2">None</td></tr>
<tr><td>Possible wrong side failure</td><td colspan="2">Device does not detect person on platform tracks</td></tr>
<tr><td>Hazardous situation</td><td colspan="2">Train is approaching the station while person is on platform tracks</td></tr>
<tr><td>Possible hazard consequences – accidents</td><td colspan="2">Collision of train with person on track. Maximum one fatality</td></tr>
<tr><td>Severity of consequences due to failure of the Low Demand safety function</td><td colspan="2">critical</td></tr>
<tr><td>Required THR</td><td colspan="2">10^{-8}/h</td></tr>
<tr><td>Hazard occurrence rate λ_I</td><td colspan="2">We assume a hazard occurrence rate for a person on the track who need to be rescued, once a year, i.e.$\lambda_I = 10^{-4}$/h</td></tr>
<tr><td>Required failure probability on demand (THR / λ_I)</td><td colspan="2">10^{-8}/h / 10^{-4}/h = 10^{-4}</td></tr>
<tr><td>Wrong side failure rate λ_{SE} of the safety function</td><td>10^{-3}/h</td><td rowspan="2">10^{-3}/h / 10^{1}/h = 10^{-4}</td></tr>
<tr><td>Inspection rate μ_{SE}</td><td>10^{1}/h (i.e. 10 times per hour)</td></tr>
<tr><td>Achieved Hazard Rate and corresponding SIL</td><td colspan="2">$\lambda_I \times \lambda_{SE} / \mu_{SE} = 10^{-4}$/h x 10^{-3}/h / 10^{1}/h = 10^{-8}/h
residual risk is equivalent to SIL 3 according to Figure 1</td></tr>
</table>

Regarding the hazard occurrence rate λ_I only those persons on the track are considered who need to be rescued. There might be people on the track more often, depending heavily on the local metro system, but the either climb out again or run away. In principle they rescue themselves. Here, people who need assistance are in focus, e.g. accidentally fallen from the platform or drunken people.

Should we assume an inspection rate of 10^{+1}/h (which correspond to a check interval of 6 minutes) a wrong side failure rate of the detection function of 10^{-3}/h would be required. However, in case the inspection rate if 10^{-1}/h (once every ten hours), a wrong side failure rate of the detection function of 10^{-5}/h would be necessary.

8.1.3 Detect Derailment

Item	Description	
Number of safety function	76	
Name of safety function	**Detect derailment**	
Description	This function is intended to detect a derailment of the train in order to stop the derailed train and to warn trains running in opposite direction	
Reference of functions	New for MODSafe	
Reference for risk analysis	None	
Possible wrong side failure	Device does not detect the derailment	
Hazardous situation	Derailed train infringes clearance envelope of train on opposite track	
Possible hazard consequences – accidents	Collision of two trains with several fatalities	
Severity of consequences due to failure of the Low Demand safety function	catastrophic	
Required THR	10^{-9}/h	
Hazard occurrence rate λ_I	We assume a hazard occurrence rate for the derailment of a single train of $\lambda_I = 10^{-4}$/h, (10 000 h is a very conservative assumption for real operation)	
Required failure probability on demand (THR / λ_I)	10^{-9}/h / 10^{-4}/h = 10^{-5}	
Wrong side failure rate λ_{SE} of the safety function	10^{-6}/h	10^{-6}/h / 10^{-1}/h = 10^{-5}
Inspection rate μ_{SE}	10^{-1}/h	
Achieved Hazard Rate and corresponding SIL	$\lambda_I \times \lambda_{SE} / \mu_{SE} = 10^{-4}$/h x 10^{-6}/h / 10^{-1}/h = 10^{-9}/h residual risk is equivalent to SIL 4 according to Figure 1	

The given example values shall only illustrate the mechanism of the method. Different inspections rates, e.g. automatic inspection with e.g. 10 times per hour ($\mu_{SE} = 10^{+1}$/h) would require a wrong side failure rate of the derailment detection device of 10^{-4}/h (10^{-4}/h / 10^{+1}/h = 10^{-5}). This wrong side failure rate of $\lambda_{SE} = 10^{-4}$/h would then be outside the limit of SIL 1 – SIL 4 categories, i.e., SIL 0.

8.2 Calculation of the residually unsafe state of the full Markov Graph for Low Demand Operated System

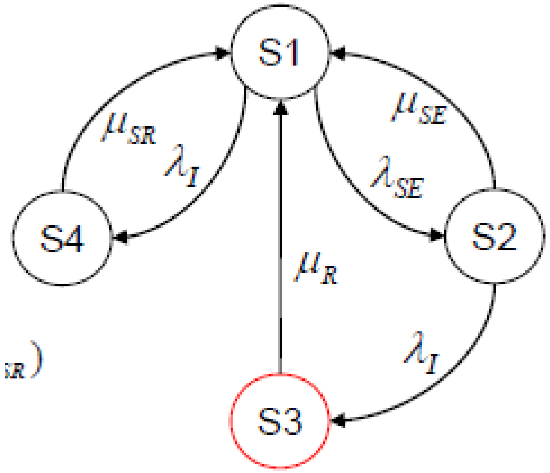

Figure 11: Complete Markov Graph for a Low Demand mode operated System

For completeness, the full Markov Graph for the Low Demand Mode Operated System is again depicted above.

Since for standard safety analyses, constant rates are assumed and in general the limit value in the long term time domain is required, the calculation formalisms advise to transfer the calculation into the Laplace domain with the respective transformations

$$L(f) = F(s) = \int_0^\infty e^{-st} f(t)dt \Rightarrow L(\dot{f}) \rightarrow s \cdot F(s) - f(0)$$

The solution of the Differential Equation System in the time domain can then often more easily determined in the Laplace Space and – if required - transformed back into the time domain.

In the Laplace domain, the Differential Equation System becomes a regular Linear Equation System characterized by the transformed Transition Matrix:

$$\begin{pmatrix} s+\lambda_I+\lambda_{SE} & -\mu_{SE} & -\mu_R & -\mu_{SR} \\ -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 & 0 \\ 0 & -\lambda_I & s+\mu_R & 0 \\ -\lambda_I & 0 & 0 & s+\mu_{SR} \end{pmatrix} \begin{pmatrix} F_1(s) \\ F_2(s) \\ F_3(s) \\ F_4(s) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

A solution for F_3 may be obtained by dividing the Subdeterminant D_3 by the main determinant D, where

$$F_3(s) = \frac{D_3}{D}$$

$$D_3 = \left| \begin{pmatrix} s+\lambda_I+\lambda_{SE} & -\mu_{SE} & 1 & -\mu_{SR} \\ -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 & 0 \\ 0 & -\lambda_I & 0 & 0 \\ -\lambda_I & 0 & 0 & s+\mu_{SR} \end{pmatrix} \right| =$$

$$= 1 \cdot \begin{vmatrix} -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 \\ 0 & -\lambda_I & 0 \\ -\lambda_I & 0 & s+\mu_{SR} \end{vmatrix} = (s+\mu_{SR}) \begin{vmatrix} -\lambda_{SE} & s+\mu_{SE}+\lambda_I \\ 0 & -\lambda_I \end{vmatrix} = \lambda_{SE}\lambda_I(s+\mu_{SR})$$

and

$$D = -\mu_R \begin{vmatrix} -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 \\ 0 & -\lambda_I & 0 \\ -\lambda_I & 0 & s+\mu_{SR} \end{vmatrix} + (s+\mu_R) \begin{vmatrix} s+\lambda_I+\lambda_{SE} & -\mu_{SE} & -\mu_{SR} \\ -\lambda_{SE} & s+\mu_{SE}+\lambda_I & 0 \\ -\lambda_I & 0 & s+\mu_{SR} \end{vmatrix} =$$

$$= -\mu_R(s+\mu_{SR}) \begin{vmatrix} -\lambda_{SE} & s+\mu_{SE}+\lambda_I \\ 0 & -\lambda_I \end{vmatrix} - \mu_{SR}(s+\mu_R) \begin{vmatrix} -\lambda_{SE} & s+\mu_{SE}+\lambda_I \\ -\lambda_I & 0 \end{vmatrix} + (s+\mu_R)(s+\mu_{SR}) \begin{vmatrix} s+\lambda_I+\lambda_{SE} & -\mu_{SE} \\ -\lambda_{SE} & s+\mu_{SE}+\lambda_I \end{vmatrix} =$$

$$= -\mu_R\lambda_{SE}\lambda_I(s+\mu_{SR}) - \mu_{SR}\lambda_I(s+\mu_R)(s+\mu_{SE}+\lambda_I) + (s+\mu_R)(s+\mu_{SR})(s+\lambda_I+\lambda_{SE})(s+\mu_{SE}+\lambda_I) - \mu_{SE}\lambda_{SE}(s+\mu_R)(s+\mu_{SR}) =$$
$$= s\cdot(s^3 + s^2\mu_{SR} + s^2\mu_R + s\mu_R\mu_{SR} + s^2\mu_{SE} + s\mu_{SE}\mu_{SR} + s\mu_R\mu_{SE} + \mu_R\mu_{SR}\mu_{SE} + 2s^2\lambda_I + s\mu_{SR}\lambda_I + 2s\mu_R\lambda_I + \mu_R\mu_{SR}\lambda_I + s\lambda_I\mu_{SE} +$$
$$+ \mu_R\lambda_I\mu_{SE} + s\lambda_I^2 + \mu_R\lambda_I^2 + s^2\lambda_{SE} + s\mu_{SR}\lambda_{SE} + s\mu_R\lambda_{SE} + \mu_R\mu_{SR}\lambda_{SE} + s\lambda_I\lambda_{SE} + \mu_{SR}\lambda_I\lambda_{SE})$$

Since we are more interested in the long term time value than in the explicit time function of P_3, we

$$\lim_{t\to\infty} P(t) = \lim_{s\to 0} s\cdot F(s), \qquad \lim_{t\to 0} P(t) = \lim_{s\to\infty} s\cdot F(s)$$

may determine the limit value for t -> ∞, which corresponds to the limit of F_3 for s->0:

We obtain

where we have used that the λ-values are in all practical cases negligibly small compared to the μ-

$$\lim_{t\to\infty} P_3(t) = \lim_{s\to 0} s\cdot F_3(s) = \lim_{s\to 0}\frac{s\cdot D_3(s)}{D(s)} = \frac{\left.D_3\right|_{s=0}}{\left.D\middle/s\right|_{s=0}} = \frac{\lambda_{SE}\lambda_I\mu_{SR}}{\mu_R\mu_{SE}(\mu_{SR}+\lambda_I) + \mu_R\lambda_I(\mu_{SE}+\lambda_I) + \mu_{SR}\lambda_{SE}(\mu_R+\lambda_I)} \approx$$

$$\approx \frac{\lambda_{SE}\lambda_I\mu_{SR}}{\mu_R(\mu_{SE}\mu_{SR} + \mu_{SE}\lambda_I + \mu_{SR}\lambda_{SE})} \approx \frac{\lambda_{SE}\lambda_I\mu_{SR}}{\mu_R\mu_{SE}\mu_{SR}} = \frac{\lambda_{SE}\lambda_I}{\mu_R\mu_{SE}} = \left.\frac{\lambda_{SE}\lambda_I}{\mu_{SE}}\middle/\mu_R\right.$$

values.

Since we formally write probabilities like P3 in the shape of a quotient of two values (a “failure rate” and a “downtime rate”) the above result had form wise been prepared for a similar shape.

$$U_{sys} = \frac{MTTR_{sys}}{MTTS_{sys} + MTTR_{sys}} = \frac{\frac{1}{\mu_{sys}}}{\frac{\lambda_{sys} + \mu_{sys}}{\lambda_{sys}\mu_{sys}}} \approx \lambda_{sys} / \mu_{sys}$$

This means, that the result may be interpreted as a safety relevant "failure" with the frequency $\lambda_{sys} = \frac{\lambda_{SE}\lambda_I}{\mu_{SE}}$ and a "downtime" of $\frac{1}{\mu_R}$.

Simplified Calculation with reduced state graph

Taking into account considerations which are typical for the safety related behavior of railway systems the complete state graph according to Figure 11 can be simplified. The following basic assumptions are made in this case:

- in all practical cases, the transition μ_R is in fact practically irrelevant for all calculations as we cannot speak of a repair process with a constant rate after a catastrophic accident and formally – after the damage was done – we are again in a safe state if the system does not operate any more,
- the branch with the Safety Reaction (μ_{SR}) also does not contribute to our analysis, since from a pure safety point of view the system is still safe once the safety response had been performed. In this context, we assume the safety response to be performed quickly enough to be effective, thus may neglect this branch of the state graph.
- remains the question how the above λ_{sys} may be found from a reduced graph if the μ_R and μ_{SR} are neglected.

By considering these specific circumstances and simplifications a reduced graph is represented by the diagram below.

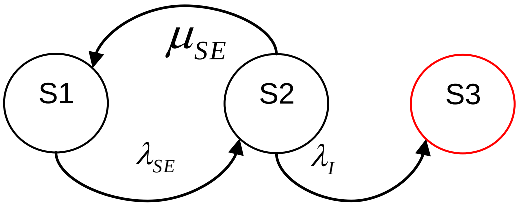

Figure 12: Reduced Markov Graph representation for a Low Demand mode operated System

For concrete calculation, we determine again Transition Matrix in the Laplace domain, the Subdeterminant D_3 and the Determinant D and form the quotient to obtain the function F_3:

$$\begin{pmatrix} s+\lambda_{SE} & -\mu_{SE} & 0 \\ -\lambda_{SE} & (s+\lambda_I+\mu_{SE}) & 0 \\ 0 & -\lambda_I & s \end{pmatrix} \cdot \begin{pmatrix} F_1(s) \\ F_2(s) \\ F_3(s) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$D_3 = \begin{vmatrix} s+\lambda_{SE} & -\mu_{SE} & 1 \\ -\lambda_{SE} & s+\lambda_I+\mu_{SE} & 0 \\ 0 & -\lambda_I & 0 \end{vmatrix} = (s+\lambda_{SE})\begin{vmatrix} s+\lambda_I+\mu_{SE} & 0 \\ -\lambda_I & 0 \end{vmatrix} + \mu_{SE}\begin{vmatrix} -\lambda_{SE} & 0 \\ 0 & 0 \end{vmatrix} + \begin{vmatrix} -\lambda_{SE} & s+\lambda_I+\mu_{SE} \\ 0 & -\lambda_I \end{vmatrix} = \lambda_{SE}\lambda_I$$

$$P_3(t\to\infty) = F_3(s\to 0) = \lim_{s\to 0}\frac{sD_3}{D} = \lim_{s\to 0}\frac{s\lambda_I\lambda_{SE}}{s\left[s^2+s(\lambda_I+\lambda_{SE}+\mu_{SE})+\lambda_I\lambda_{SE}\right]} = 1$$

As can be seen from the above calculation, the limit value in remote times may now not be used anymore, since it will always converge against 1 due to the absorbing state in the reduced Markov Graph. We need therefore to determine the concrete time function and determine at what time the probability to perform service had been sufficiently reduced (1/e) by the failure to serve as a characteristic time or frequency base.

The function F3 may be written in the form

$$F_3(s) = \frac{D_3}{D} = \frac{\lambda_I\lambda_{SE}}{s\left[s^2+s(\lambda_I+\lambda_{SE}+\mu_{SE})+\lambda_I\lambda_{SE}\right]};$$

And making use of the back-transformation rule below,

$$If \quad F(s) = \sum_{k=1}^{n}\frac{\alpha_k}{s-s_k} \to f(t) = \sum_{k=1}^{n}\alpha_k e^{s_k t}$$

We obtain for the time function

$$\to P_3(t) = 1 - \frac{1}{r_1-r_2}\left(r_1e^{r_2t} - r_2e^{r_1t}\right) where\ r_{1,2} = \frac{-(\lambda_{SE}+\lambda_I+\mu_{SE}) \pm \sqrt{(\lambda_{SE}+\lambda_I+\mu_{SE})^2 - 4\lambda_{SE}\lambda_I}}{2}$$

Probabilities P_i are normalized, so a typical time scale for the occurrence of P_3 is calculated by the approach

$$T = \int_0^\infty W(t)dt = \int_0^\infty P_1(t)+P_2(t)dt = \int_0^\infty 1-P_3(t)dt = \frac{1}{r_1-r_2}\int_0^\infty r_1e^{r_2t} - r_2e^{r_1t}dt$$

Inserting the concrete solution yields again

$$D=(s+\lambda_{SE})\begin{vmatrix} s+\lambda_I+\mu_{SE} & 0 \\ -\lambda_I & s \end{vmatrix}+\mu_{SE}\begin{vmatrix} -\lambda_{SE} & 0 \\ 0 & s \end{vmatrix}=(s+\lambda_{SE})(s+\lambda_I+\mu_{SE})s-\mu_{SE}\lambda_{SE}s=s\left[s^2+s(\lambda_I+\lambda_{SE}+\mu_{SE})+\lambda_I\lambda_{SE}\right]$$

$$T=-\frac{\left(\frac{-(\lambda_I+\lambda_{SE}+\mu_{SE})+\sqrt{(\lambda_{SE}+\lambda_I+\mu_{SE})^2-4\lambda_{SE}\lambda_I}-(\lambda_I+\lambda_{SE}+\mu_{SE})-\sqrt{(\lambda_{SE}+\lambda_I+\mu_{SE})^2-4\lambda_{SE}\lambda_I}}{2}\right)}{\left(\frac{-(\lambda_I+\lambda_{SE}+\mu_{SE})+\sqrt{(\lambda_{SE}+\lambda_I+\mu_{SE})^2-4\lambda_{SE}\lambda_I}}{2}\right)\left(\frac{-(\lambda_I+\lambda_{SE}+\mu_{SE})-\sqrt{(\lambda_{SE}+\lambda_I+\mu_{SE})^2-4\lambda_{SE}\lambda_I}}{2}\right)}=$$

$$=-\frac{(\lambda_I+\lambda_{SE}+\mu_{SE})}{\frac{1}{4}\left((\lambda_I+\lambda_{SE}+\mu_{SE})^2-\left((\lambda_I+\lambda_{SE}+\mu_{SE})^2-4\lambda_I\lambda_{SE}\right)\right)}=\frac{\lambda_I+\lambda_{SE}+\mu_{SE}}{\lambda_I\lambda_{SE}},$$

$$\lambda_I,\lambda_{SE}<<\mu_{SE}\rightarrow T\approx\frac{\mu_{SE}}{\lambda_I\lambda_{SE}},\quad \lambda_{Sys}=\frac{1}{T}\approx\frac{\lambda_{SE}\lambda_I}{\mu_{SE}}$$

By applying the detailed Markov calculation mechanism to a railway applicable context (with the respective approximations) yields therefore in different calculation paths always the same, easy to use and easy to understand result.