



MODURBAN

FP6 Project: IP 516380

EC Contract n°: TIP4-CT-2005-516380

MODSYSTEM SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D 90
Deliverable Title:	Generic Model / Guidelines for Risk Analysis
Responsible Partner:	TU DRESDEN
Contributors:	WP 23 Partners

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the MODURBAN Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the MODURBAN consortium.

Document Information

Document Name: Generic Model / Guideline for Risk Analysis
Document ID: D 90
Revision: Final Draft
Revision Date: March 2008
Author: TUD – Eckel, Forchmann, Schütte
Security: Consortium only

Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERTSORFF P. TEILLET / G. P-RIVIÈRE D.DIMMER G. LEGOFF L. LINDQVIST A. PRICE / U. HENNING M. NOCK JP RICHARD/D. COINEAU Y. AMSLER C. GOUTORBE	UNIFE ALSTOM THALES ANSALDO STS BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA	17/07/2008	OK
<i>Coordinator</i>	Bernard VON WULLERSTORFF	UNIFE	17/07/2008	OK
<i>Quality Manager</i>	Bernard VON WULLERSTORFF C. GOUTORBE	UNIFE ALMA	17/07/2008	OK

Document history

Revision	Date	Modification	Author
Draft 1	07/10/27	First Version for comments	TUD
Draft 2	07/12/12	Consideration of comments received during review of Draft 1	TUD
Draft 3	08/01/31	Consideration of comments received during review of Draft 2	TUD
Final Draft	08/03/31	Consideration of comments received during review of Draft 3	TUD



The scope of the document applies to:

Metro systems only	Metro and Light Rail		Light Rail only
	<i>With no differentiation</i>	<i>With specific adaptation(s)/recommendation(s) (1)</i>	
		<i>For metro</i>	

(1) – Put a [D] if these adaptations/recommendations are present in the document and a [L] if they will have to be detailed later.





SECTION I: DELIVERABLE SUMMARY

Deliverable Title	
Deliverable ID , associated WP & Subproject	D 90 MODSYSTEM / WP 23
Type of Deliverable	Report
Input / Starting stage	D86
Output / Final stage	

Lead partner(s)	
Achievement to date (%)	100%
Expected date of achievement	
Type of exploitation	
Exploitation potential	
Protection	
Protection date	

IP's	Partners, (type, identification, date)
Pre-existing Know-How	UGTMS
Exploitation Rights	

Associated Risk analysis	Type, solution envisaged, action, actors	Actual Reduction
Before start	not relevant	
During task implementation	not relevant	

Deliverable Title

Deliverable Abstract

In this deliverable, the algorithms and processes of the MODURBAN SIL allocation processes of D 86 are analysed and compared in detail with other methodological aspects (MODTRAIN). While the MODURBAN approaches turn out much more straightforward than the MODTRAIN approach, all three involve similar groups of parameters like hazard frequencies, severity classes, risk exposure or barriers. The MODTRAIN prescriptions require additional parameter inputs and numerical assumptions before being applied because the underlying model of the safety entities is more developed than those used by MODURBAN. The results obtained for Continuous Safety Functions are similar or identical using the different approaches described in this document. The Deliverable confirms, however, the Cenelec Working Group on EN 50129, that the SIL concepts cannot be reasonably applied for On Demand Functions in the same sense as for continuous functions by any of the processes.

The Guidelines and Application Recommendations are summarized in clause 7.

Associated Milestone (if relevant):

SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

Contents

Contents	6
1 Introduction.....	7
2 Terms, definitions and abbreviations	9
2.1 Terms and definition.....	9
2.2 Abbreviations	10
3 Risk Analysis within MODTRAIN and MODURBAN	11
3.1 MODTRAIN	11
3.1.1 Overall Safety Process.....	11
3.1.2 Procedure for the Application of MODTRAIN	14
3.1.3 Proposed Values and lists of MODTRAIN.....	18
3.1.4 Final Calculation.....	22
3.2 MODURBAN	23
3.2.1 Method 1: Risk Graph – Qualitative Method.....	23
3.2.2 Method 2: Semi-Quantitative Analysis and Risk Matrix.....	25
4 Comparison and Analysis of Methodologies.....	29
4.1 Fundamental Approach	29
4.2 Identification of Boundary Hazard and Accident Types	30
4.3 Comparison of Parameters	30
4.3.1 Severity of consequences	30
4.3.2 Operational context	31
4.3.3 Consequence barrier/reduction	32
4.3.4 Cause barrier	34
5 Application of MODURBAN/MODTRAIN methods	35
5.1 Adjustments for the application of MODTRAIN to MODURBAN	35
5.1.1 Changes to the parameters.....	35
5.1.2 Final calculation	36
5.1.3 Changes to the procedure.....	37
5.1.4 Suggestion or the procedure of an adjusted MODTRAIN version	38
5.2 Selection of Safety Functions.....	39
5.3 Application of safety functions.....	40
5.3.1 Safety function MU 1.1 Train Integrity Supervision	41
6 Comparison and evaluation of applications	45
6.1 Introduction	45
6.2 Transferability.....	45
6.3 Simplicity	45
6.4 Unambiguity	46
6.5 Reason for different Results.....	46
7 Findings and Recommendations	49
References	50

1 Introduction

Safety of urban guided transportation has traditionally had a very good record, inheriting many of the safe features of mainline railways gained over the years (e.g. fail-safe principles), and even adding in to some extent extra protection to deal with the increased dangers associated with high frequency traffic typical of most metro operation. This explains for instance why many metro systems have long been equipped with ATP systems, before this was the case for mainline trains.

The sector is currently undergoing rapid changes brought about by increasing demands for lower costs and higher performances from operators on the one hand and the technology innovations that must help fulfil these demands on the other hand. MODURBAN's objectives are essentially aimed at supporting solutions meeting such demands. However the usually good safety performance of urban guided transportation must not be jeopardized in this process and this requires a thorough approach in the way safety is treated. The notion of a risk-based approach for ensuring safety has thus been relatively recently introduced and adopted in the railway (and urban rail) industry in order to provide some objective measure of the safety that must be achieved by the systems or parts thereof, independently of the solutions chosen for realizing safety functions. As a corollary to this risk-based approach, the concept of graded/differentiated safety levels (Safety Integrity Levels) was also adopted and is meant to allow more room for cost optimisation in the specification of safety requirements while maintaining a high level of global safety. The main difficulty for the use of these concepts (risk and SIL) is to specify consistently the level of safety of new systems that must be achieved with respect to a risk criteria whereas traditionally safety of railway systems was appraised solely through the compliance with well established standards (often at national level only) and according to well known safety principles (e.g. fail-safe) which may not be applicable any more for new complex solutions (cf. D 86). Although relatively new international standards (from CENELEC and IEC) have addressed this issue so that risk and SIL have become familiar concepts in the railways and are now widely used, there remain however various interpretations in their definitions and implementations; this makes it necessary to agree on common approach within an harmonization project such as MODURBAN.

The deliverable D 86 "Safety Conceptual Approach for functional and technical prescription" dealt with all the aspects mentioned above. Starting with proposing some clarification on the issue of risk and safety integrity requirements and a description of the state of the art (work carried out within the UGTMS project, current practice, national regulations etc.) the deliverable proposed a safety conceptual approach for MODURBAN and applied it on a number of MODURBAN functions to test its feasibility and practicality to determining SILs.

This deliverable D 90 bases on the work done within D 86 and proposes a guideline for risk analysis. Therefore the approach of D 86 is compared with the preliminary results of another European project called MODTRAIN which deals with the similar task of risk analysis, but for rolling stock of the mainline railways only (and not the



whole system). Differences of the two approaches are shown and advantages and disadvantages are taken into account when proposing the guideline for risk analysis.

Furthermore, D 128 deals with the influence of human factors on risk assessment.

2 Terms, definitions and abbreviations

2.1 Terms and definition

It is a rather complex task to find a general definition for the terms of “Continuous functions” and “On-Demand functions”. This is mainly due to the fact that a general base for a definition is not found. For the application to the MODURBAN project a preliminary definition is therefore applied which is based on the failure effects of the respective function.

If a function fails and this failure leads to a hazardous situation, with a high probability, then the function is considered a “**continuous function**”. An example is a signalling failure in a heavy frequented train operation. In the most cases, this failure of the signal leads more or less immediately to a highly hazardous situation.

If a function fails and this failure leads to a hazardous situation, with a low probability, then the function is considered an “**on-demand function**”. An example may be that a failed means of fire protection e.g. fire extinguisher does not necessarily and immediately lead to a hazardous situation. Reason for this risk behaviour is the circumstance that on-demand or semi-continuous functions are those that protect against hazardous situations that occur non-continuously (e.g. rarely) so that the resulting effective hazard rate requires first the primary hazard (fire) and then secondly the failure of the on-demand safety system.

2.2 Abbreviations

A	Exposure to Danger (in context of method 1)
AC	Accident Case
AT	Accident Type
ATP	Automatic Train Protection
BE	Barrier Efficiency
BH	Boundary Hazard
C	Consequence Reduction Probability (in context of method 2)
CAB	Cause Barrier
CC	Car Borne Controller
COB	Consequence Barrier
E	Exposure Probability to Hazard (in context of method 2)
EB	Emergency Braking
EC	Efficiency Category
EMI	Electro-Magnetic Interface
F	Frequency of Occurrence of Hazard
FBS	Functional Breakdown Structure
FRS	Functional Requirements Specification
FT	Fault Tree
G	Defence against Danger/Consequence (in context of method 1)
GIPS	Guideway Intrusion Protection System
GOA	Grade of Automation
HAB	Hazard Barrier
HC	Hazard Cause
HF	Human Factor
MP	(Operational) Mode Probability
MT	MODTRAIN
MU	MODURBAN
OC	Operational Context
OCC	Operations Control Centre
P	Accident Probability Reduction (in context of method 2)
PC	Probability Category
PBS	Product Breakdown Structure
RTM	Risk Tolerability Matrix
S	Severity of Consequences (in context of method 1)
SC	Severity Category
SIL	Safety Integrity Level
SL	Severity Category (Level)
TAR	Tolerable Accident Rate
TBHR	Tolerable Boundary Hazard Rate
TCMS	Train Control & Monitoring System
THCR	Tolerable Hazard Cause Rate
THR	Tolerable Hazard Rate
TSI	Technical Specification for Interoperability
UGTMS	Urban Guided Transport Management System
W	Probability of Danger Occurrence (in context of method 1)

3 Risk Analysis within MODTRAIN and MODURBAN

The approach for the European project MODTRAIN is considered to elaborate a guideline for risk analysis. Therefore, this clause presents the MODTRAIN approach for risk analysis as presented in the document “Guidance for Safety Analysis” and summarize the findings of the MODURBAN deliverable D 86.

3.1 MODTRAIN

3.1.1 Overall Safety Process

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 Context¹, a Boundary Hazard² at train system level and a potential Accident. Standard lists of Accidents and of Boundary Hazards should be used (see sub-clause 3.1.3.2). 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 Barriers³ 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.

¹ The operational context is defined with an operational mode, an operational phase and an operational area and possibly with some specific circumstances.

² 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.

³ 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.



Unless Hazard Risk objectives are provided by the Member States, a Risk Estimation must be performed on the 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 Analysis⁴. 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 Barriers⁵ that can prevent Hazard Causes⁶ 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.

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

⁴ Analysis of events which are likely to happen after a *hazard* has occurred.

⁵ 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.

⁶ Any event which contributes to the occurrence of a boundary hazard.

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.

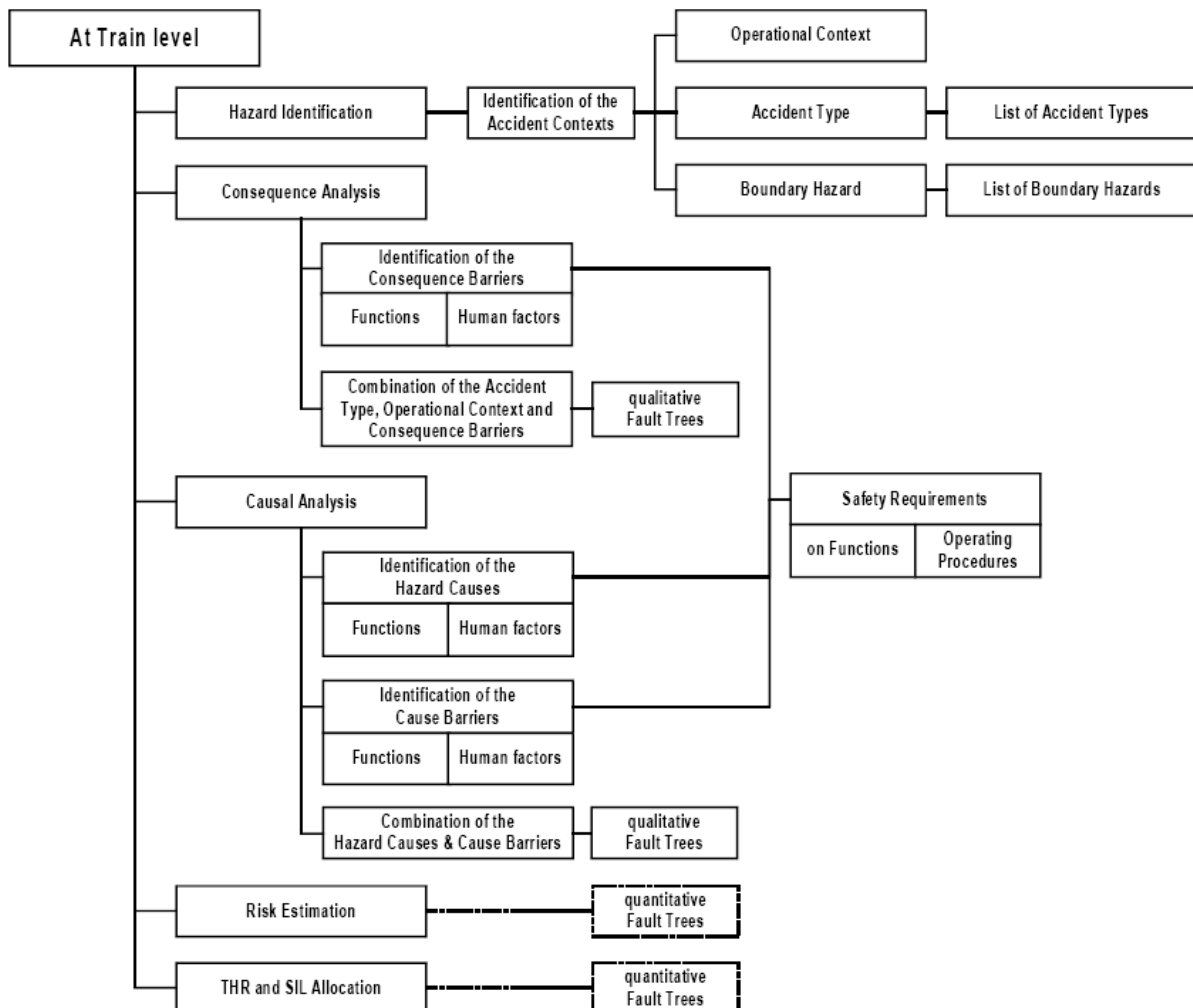


Figure 1 - Procedure of MODTRAIN



3.1.2 Procedure for the Application of MODTRAIN

The following table (table 1) describes the procedure of MODTRAIN to identify the demanded parameters. The content of this table is extracted from the MODTRAIN guidelines although the table itself is not part of the MODTRAIN guidelines itself. The tabulation has been chosen due to readability reasons.

Table 1 - Procedure of MODTRAIN (* further details can be found in sub-clause 3.1.3.1 and 3.1.3.2)

Step	Stage	Description	Comments	
0	Input	System Definition – identified function	FBS level 3 (4)	
1	Hazard Identification	Define Accident Case		
1a		Identify Operational Context	List of OC*, PC*	
1b		Identify Boundary Hazards	List of BHs*	
1c		Identify Accident Type	List of AT*	
2		Determine Safety Impact		
3		Consolidate Accident Case		
3a		Recap different Accident Cases		
3b		Recap the functions concerned by AC		
4		Consequence Analysis	Identify Consequence Barriers	
4a			Identify Functional Barriers	Add purpose
4b	Identify Human Factors		Operation or HF	
4c	Efficiency of each Consequence Barrier		EC*	
4d	Define Safety Requirements			
5	Cause Analysis	Identify Hazard Causes	Which lead to BH*	
5a		Identify Failures of Sub-Functions	FBS Level 4	
5b		Identify specific Failures	e.g. mechanical	
5c		Identify Human Factors		
5d		Identify Safety Impact		
6		Identify Cause Barriers		
6a		Identify Sub-Functions	FBS Level 4	
6b		Identify Human Factors	Operation or HF	
6c		Determine Efficiency of each CAB	EC*	
6d		Safety Requirements		
7		Fault Tree (Hazard Cause, Cause Barrier)		
8		Fault Tree (Accident Context)		
9		Risk Estimation, SIL and THR Allocation	Determine Tolerable Accident Rate	SC*, RTM
10			Determine Tolerable Boundary Hazard Rate	
10a	Justify the efficiency of each COB			
10b	Compute the efficiency of each COB		In combination	
10c	Compute TBHR of BH		TAR, OC*, COB	
11	Determine Tolerable Hazard Cause Rate			
11a	Justify the efficiency of each CAB		EC*	
11b	Allocate THCR to HC		CAB, TBHR	
11c	Justify TBHR by Fault Tree			
12	Select the lowest THCR of each HC among all ACs			

Table 1 - Procedure of MODTRAIN (continued)

Step	Stage	Description	Comments
13	Risk Estimation, SIL and THR Allocation	Allocate SIL to each function involved in HC according to its THCR	
14		Allocate a SIL to each function involved in CAB and COB according to the average probability of failure	
15	Safety	Critical Analysis	
16	Demonstration and	Provide Evidence of correct implementation	
17	Justification	Overall Safety Report	

Note: MODTRAIN has finally adopted another approach for the steps 11 to 14 about SIL allocation (see "Guidance for safety analysis" version 2.0):

- Distribute functions on subsystems
- Allocate SIL to functions directly contributing to BH for each AC
- Allocate SIL to functions indirectly contributing to BH for each AC
- Consolidate SIL of functions for all AC.

The following figure provides a graphical chart of the MODTRAIN risk-based approach. Based on an operational context a certain function might fail, which correlates with the hazard cause. Consequences are the boundary hazard and subsequently the accident. An emergence of the boundary hazard is possibly interrupted by a cause barrier. An accident could be prevented by a consequence barrier. The accident features a tolerable accident rate (TAR), the operational mode of an operational context a probability category (MP), cause and consequence barriers an efficiency category (BE). Suggested values of MODTRAIN can be found in sub-clause 3.1.3.1.

3.1.3 Proposed Values and lists of MODTRAIN

3.1.3.1 Proposed Values

MODTRAIN has suggested and initialised several definitions for probability, efficiency and frequency categories. These categories are defined for the efficiency of consequence barrier and cause barrier, the probability of the operational context and the frequency for risk categories are given in EN 50126.

MODTRAIN indicates “that figures are given for illustration only.

The following tables show the values that have been adopted by MODTRAIN. These tables can be found in the guidelines of MODTRAIN in the same way.

Table 2 - Efficiency Categories for Safety Barriers

Attribute	Value	Interval of Probability
Efficiency Category	Low	Example: [0% - 60%]
	Medium	Example: [60% - 90%]
	High	Example: [90% - 99%]
	Very High	Example: [99% - 99.9%]
	Exceptional	Example: [99.9% - 99.99%]

Table 3 - Operational State and Frequency Categories for the Operational Context

Attribute	Value	Description
Operational State	Normal Operation	
	Degraded Operation	
	Maintenance	
	Emergency Situation	
Probability Category	Frequent	[100% - 10%]
	Probable	[10% - 1%]
	Occasional	[1% - 0.1%]
	Remote	[0.1% - 0.01%]

Table 4 - Risk categories given in EN 50126

Attribute	Value	Description
Frequency Category	Frequent	Example: $> 10^{-1}/h$
	Probable	Example: $[10^{-3}/h - 10^{-1}/h]$
	Occasional	Example: $[10^{-5}/h - 10^{-3}/h]$
	Remote	Example: $[10^{-7}/h - 10^{-5}/h]$
	Improbable	Example: $[10^{-9}/h - 10^{-7}/h]$
	Incredible	Example: $< 10^{-9}/h$
Severity Category	Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment
	Critical	Single fatality and/or severe injuries and/or significant damage to the environment
	Marginal	Minor injury and/or significant threat to the environment
	Insignificant	Possible minor injury
Tolerability Category	Intolerable	Shall be eliminated
	Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
	Tolerable	Acceptable with adequate control and with the agreement of the Railway Authority
	Negligible	Acceptable with/without the agreement of the Railway Authority

3.1.3.2 Hazards, Accidents and Operational Context

MODTRAIN provides lists to aid the identification of boundary hazards, accident types and operational contexts. Due to the fact that MODTRAIN describes a safety analysis only for rolling stock the lists are not generally transferable to MODURBAN as such, but can be seen as a starting basis to support risk analyses.

List of Accident Types

- Collision
- Derailment
- Explosion
- Contamination (gases, fluid, fibres outside the train)
- Asphyxia, Suffocation (gas emission, fumes, no air change)
- Burns (flames, gases, hot surfaces)
- Electrocution
- Fall of persons:
 - from train onto tracks or within platform-train gap
 - from train onto platform
 - inside a vehicle
- Trapping of persons
 - by external doors

- by internal doors (gangways)
- Impact on persons (object striking persons)
- Cuts

List of Boundary Hazards

1. Train motion control impaired or lost
 - Unintentional train motion (failure of parking or holding brakes, propulsion fault, etc.)
 - Incapacitated driver not detected (driver vigilance)
 - Wrong travel direction
 - Excessive speed
2. Train braking impaired or lost
 - paired (or lost) braking capability (stop distance not respected)
 - Unintentional braking
3. Train running stability impaired or lost
 - Excessive lateral movements
 - Train/track guidance impaired or lost
4. Train gauge infringed
 - Train parts or equipment extended beyond dynamic envelopes
 - Excessive lateral movements
5. Loss of Train integrity
 - Break of coupling or un-demanded decoupling under gangways
 - Undetected decoupling of Multiple Units
6. Train presence not detected
 - Train position not detected by signalling system (vehicle defects)
 - Train not perceived (optical/acoustic devices)
7. Hazards related to Train Door Management
 - Unintentional door opening / footstep deployment / ramp deployment
 - Untimely door closing (during transfer of passengers)
 - An external door remains open (after train departure)
 - No deployment of steps / ramps (during transfer of passengers)
 - Steps / Ramps not withdrawn (prior to train departure)
 - Untimely steps / ramps withdrawal (during transfer of passengers)
 - Incompatible steps / ramps deployment (train is stopped)
8. Hazards to train/maintenance staff, public, passengers
 - Excessive EM fields
 - Insufficient ventilation or air conditioning
 - Contaminated food or drinking water [not TCMS]
 - Excessive sound/noise level
 - Excessive jerk
 - Accessible hazardous voltage
 - Accessible sharp edges
 - Accessible hot surfaces
 - Slipping surfaces [not TCMS]
 - Train parts detached
 - Objects not fastened (luggage, loads)
 - Aerodynamic suction [not TCMS]
 - Projection of ballast or ice [not TCMS]

- Excessive release of stored energy (air pressure blast, spring load etc.)
- Accessible moving parts [not TCMS]
- 9. Hazards during emergency situations
 - Insufficient emergency equipment or information
 - Train unintentionally immobilized in emergency situation
 - Impaired movements of persons
 - 9.3.1 Door does not open (detrainment)
 - 9.3.2 External doors do not open (detrainment)
 - 9.3.3 Bad visibility (detrainment at night, in tunnels)
 - 9.3.4 inappropriate to disabled people (detrainment)
 - Internal door does not close on demand (fire)
- 10. Ignition/fire source and smokes
 - Excessive heating source near flammable train parts
 - Sparking near flammable train parts
 - Spread of smokes/fumes or fire
- 11. Hazardous reactions of materials/fluids/germs
 - Excessive fluid pressure (liquids or gases)
 - Fluid Leakage (toxic fluids or high pressure) [not TCMS]
 - Chemical reaction (fluids, gases, materials) [not TCMS]
 - Spread of fibres [not TCMS]
 - Spread of germs [not TCMS]
- 12. Interference with signalling or other safety systems
 - Train causes interference with trackside equipment or other trains
 - Malfunction of safety-related train function due to EMI

List of Operational Contexts

An operational context is defined by three parameters; operational mode, operational phase and operational area. In MODTRAIN an explicit list can be found for the operational mode only (this is probably due the fact that an operational mode i.e. state can be quantified in terms of probability of occurrence). Therefore, a proposal for a list for operational phase and area has been seen as useful. These lists aim to support the identification and determination of the Operational Context. These lists are not comprehensive, and a specific determination of the Operational Context has to be made for each project. The information is taken from the FBS/PBS table for the safety analysis of the MODTRAIN system (the data are extracted from an actual application of the MODTRAIN approach). In other words; these operational contexts are a selection of examples from an actual application of the MODTRAIN approach. These points are meant as supporting examples to clarify and to give an idea about the approach of MODTRAIN. The different examples are not used for further application.

- Operational Mode:
 - Normal Operation
 - Degraded Mode
 - Maintenance
 - Emergency Case
- Operational Phase:
 - Train is running
 - Transfer of passengers/train at standstill

- Passenger in gangway
- Train is departing
- Train is berthing
- Train is standstill
- Train is stopped
- Train is stopped. Smoke outside train or car
- Train is stopped. Fire on train
- Train is standstill at station
- Passenger movement onboard train
- All operational scenarios when train not at platform
- Train at night or in tunnel
- Train passing near trackside staff and at level crossing
- On-sight driving
- Other trains should not pass or meet a train affected by flashing lights
- Train standing. No driver in cab
- Train is stopped at a place where evacuation is difficult
- Train is moving slowly or stops
- Train is running. Cold Weather
- Train is stopped at track gradient. Doors closed and locked
- Loss of power supply to batteries
- Loss of emergency energy
- Operational Area:
 - Station
 - Main line
 - Tunnel
 - Bridge

3.1.4 Final Calculation

A Tolerable Accident Rate (TAR) can be determined for each Accident Case with the Risk Tolerability Matrix and the Severity category of the Accident. A Tolerable Hazard Rate (THR) can be determined for each Boundary Hazard, in the context of an Accident Case, knowing the Tolerable Accident Rate (TAR) of the Accident, the efficiency of the Consequence Barriers, and the probability of the operational context. Thus the MODTRAIN approach of the risk estimation (TAR and THR) is semi-quantitative. (A modified version for an actual application of the MODTRAIN approach is proposed in clause 5.)

Note: MODTRAIN has finally adopted another approach about SIL allocation (see "Guidance for safety analysis" version 2.0). MODTRAIN recommends a propped-up reasoning for the SIL allocation to functions that directly or indirectly contribute to the hazards. The SIL allocation is guided by:

- the FMEA results consolidated by qualitative fault trees,
- the mapping of functions on the subsystems
- return of experience and reference to existing solutions
- some tables giving qualitative links between categories of parameters (THR to SIL, EC to SIL, SIL combination)

As a conclusion, the MODTRAIN approach of the SIL Allocation is mainly qualitative.

3.2 MODURBAN

This clause gives an overview about the methods as presented in the deliverable D 86 – it is for recapitulation only and in D 86 further details and examples can be found.

3.2.1 Method 1: Risk Graph – Qualitative Method

Risk Graphs are a method taken from IEC 61508 part 5 (described in the informative part of this norm) 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:

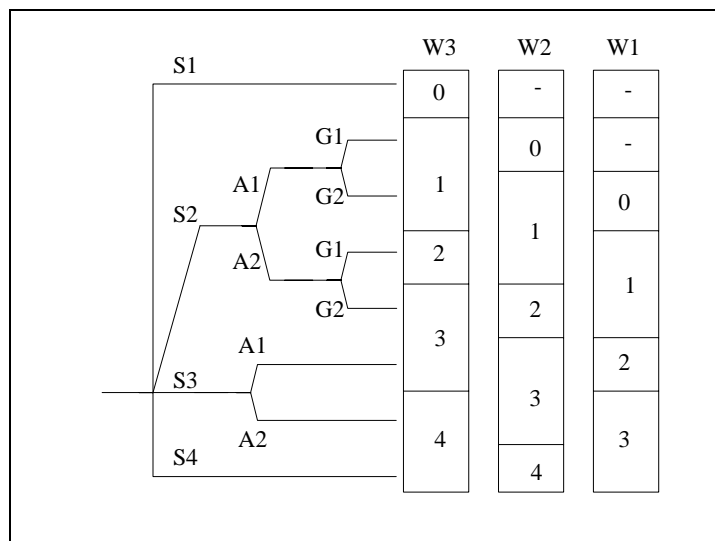


Figure 3 - Risk Graph

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:

$$\text{Risk} = \text{Frequency of accident} * \text{Severity of accident} = W * A * G * S$$

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).



3.2.2 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:

$$\text{Risk} = \text{Frequency of hazard} * \text{Severity of hazard consequence}$$

Table 5 - Risk Matrix with THR/SIL-Relationship

Frequency of occurrence of a hazard	Risk Levels			
	frequent	undesirable	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 ($F = \text{Tolerable Risk}/S$). 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:

$$\text{Severity Category } n \text{ of Hazard Consequence} \rightarrow \text{THR}_n = \text{SIL}_n$$

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

Table 6 - Relationship between THRs and SILs

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Compared to the Risk Graph method, estimations given by the Risk Matrix one are made without considering risk reduction factors such as exposure or accident avoidance: when a hazard occurs, it is assumed that it lead to an accident. 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 is for instance the approach taken in UGTMS (D6), where the SILs are 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, workers or neighbours) are exposed to the hazard clearly less than permanently – this includes the consideration of the operational phase and period (by orders of magnitude in probability)?
- Accident Probability Reduction **P**: Is there good reason to conservatively assume that the evolvment 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:

$$\text{Severity Category } SL_n \text{ of Hazard Consequence} \rightarrow \text{THR}_m = \text{THR}_n / \text{EPC} = \text{SIL}_m$$

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, relevant safety integrity levels shall be determined taking into account ad hoc risk reduction factors.

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 applying both methods, qualitative and quantitative, it is likely that similar descriptions of the details between hazard emergence and possible accident consequences yield same minimum SIL requirements using the corresponding SIL allocation process. 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.

4 Comparison and Analysis of Methodologies

The content of the following clause is the discussion of the three described methods, the two of MODURBAN against the method of MODTRAIN. The comparison includes the approaches for risk analysis and the corresponding identification of the hazards, accidents and parameters to evaluate the risk analysis. It starts off with a description of the fundamental approaches of MODURBAN and MODTRAIN. Afterwards the identification of hazards and accidents is discussed, followed by a comparison of the parameters which are used in the three methods.

Different aspects are stressed in this clause to outline the main differences between the approaches of MODTRAIN and MODURBAN.

4.1 Fundamental Approach

While MODTRAIN requires the development of a structured model of the safety entities, including the hazard causes and the related barriers as well as the barriers to prevent a hazard developing into an accident, the MODURBAN approach is much more straightforward orientated.

The author of this deliverable considers that the structured model adopted by MODTRAIN is more complex than the two MODURBAN methods.

MODURBAN starts with the safety function itself and has a look on the related hazards which may occur without. MODURBAN does not include all possible aspects related to causal analysis which could identify all reasons and circumstances (hazard causes, cause barriers etc.) that may lead to a failure but starts directly with the failure (e.g. of the safety function itself). All following considerations (possible consequence/accident, exposition, barriers reducing the occurrence of the accident, other consequence reduction measures) are related to the already failed or absent safety function. Nevertheless such aspects as operation mode or other operational contexts are included within the assessment of the numbers/categories of the consequence barriers, exposition etc.

MODTRAIN firstly describes a method ensuring the identification and traceability of the functions, human factors and external events that may lead to accidents, ending with the specification of safety requirements on functions, products and operational rules. Traceability is achieved by the use of standard lists for each entity referred in the safety analysis (e.g. accidents, hazards, operational contexts, functions and products). MODTRAIN then proposes semi-quantitative methods for the evaluation of risks, and qualitative methods for the control of risks, calling on this structured model. Depending on their role, the safety entities are featured by some categories (e.g. severity, frequency, tolerability, efficiency, SIL) or values (e.g. TAR, THR). However, MODTRAIN decided to detail the method only, i.e. to determine no THR on hazards and SIL on functions in a generic way because quantifications and allocations are project dependent.

Method 2 (risk matrix) of MODURBAN is a semi-quantitative method which provides (reduction-) values by orders of magnitude relying on the identified risk reducing

aspects that are easy to apply. The first method (risk graph) of MODURBAN on the other hand is a pure qualitative method which only deals with categories. Nevertheless it bears the concept of risk reduction by orders of magnitude in mind when it uses the SIL concept – the application of one risk reduction factor typically leads to a lower SIL (factor 10).

4.2 Identification of Boundary Hazard and Accident Types

The identification of hazards and accidents is carried out in different ways. MODURBAN identifies the hazards associated to the failure or absence of a safety function and the resulting accidents for each function separately. Theoretically every function has its individual hazards or accidents. But due to the fact that the number of hazards and accidents is limited, similarities are likely regarding the hazards and accidents. In contrast to this MODTRAIN provides lists for boundary hazards and accident types. They include a number of different boundary hazards or accident types to support their identification and therefore give a valuable orientation what might happen for a certain function. Even though these lists are given in a generic way for the mainline trains, they should be checked by every project (e.g. because of additional or superfluous hazards). These boundary hazards and accident types have been found on the basis of the MODTRAIN system architecture and therefore are not transferable to an actual application of MODURBAN.

4.3 Comparison of Parameters

4.3.1 Severity of consequences

In method 1 of the MODURBAN approach, severity is found via a risk graph. The user can choose between four levels of severity, whereas severity level four is not in use for transportation applications. These are either “Minor injury” - S1, “One or several serious irreversible injuries, or one fatality” - S2, or “Several fatalities” - S3.

Method 2 of the MODURBAN approach deals with four levels of severity. This method is a semi-quantitative approach, therefore the levels of “Catastrophic” - SL 4 ($10^{-9}/h$), “Critical” - SL 3 ($10^{-8}/h$), “Marginal” - SL 2 ($10^{-7}/h$), “Insignificant” - SL 1 ($10^{-6}/h$) are defined. Detailed verbal description of the terms catastrophic or critical etc. can be found in EN 50126.

The MODTRAIN approach classifies four levels of severity as well. These categories are “Catastrophic”, “Critical”, “Marginal” and “Insignificant”. Detailed descriptions are explained in EN 50126. However, no values are directly adopted for the severity levels. A suggested interpretation of how to determine the numerical value for the severity level is outlined in sub-clause 5.1 “Adjustments for the application”.

Table 7- Comparison of Severity Levels

MODURBAN		MODTRAIN
Method 1: Several Injuries – S3 Fatalities/Injuries – S2 Minor Injury – S1	Method 2: Catastrophic – $THR4=10^{-9}/h$ Critical – $THR3=10^{-8}/h$ Marginal – $THR2=10^{-7}/h$ Insignificant – $THR1=10^{-6}/h$	Catastrophic Critical Marginal Insignificant

To conclude: Method 1 of MODURBAN uses three graduations of qualitative descriptions. Method 2 of MODURBAN uses numerical values to describe four levels of the severity of consequences. MODTRAIN provides four qualitative descriptions only (but with a reference for estimation for a TAR).

4.3.2 Operational context

The operational context comprises the exposure to danger or the exposure probability to a hazard in MODURBAN and the operational context in MODTRAIN. In both methods it describes the case that the risk group (e.g. passengers or staff) is assumed to be permanently exposed to the hazard. To identify the operational context the question to ask is: is there any reason to assume that the risk group is not permanently exposed to the danger, in terms of probability.

Method 1 of MODURBAN differentiates between two stages of the exposure to danger. These are A1 - “Rare or infrequent exposure to danger” and A2 - “Frequent or constant exposure to danger”.

The second method of MODURBAN knows three stages of the exposure probability to a hazard; “frequent or permanent” with an adopted factor of $E=1$, “rare or exceptional” - $E=10^{-1}$ and “very rare”- $E=10^{-2}$.

Compared to this relatively static description of the exposure to danger MODTRAIN has a far more flexible system to determine the operational context. After the definition of the operational mode, phase, zone and conditions of the operational context, an operational mode probability can be selected. Four probability categories are available: “Frequent”, “Probable”, “Occasional” and “Remote”. Also a list of operational contexts is provided. Due to the operational mode, phase and area a detailed description of the operational context is possible. All three factors (mode, phase and area) can be combined in every way to describe the operational context in the most appropriate way. The probability category is attached to the operational mode of the operational context. The “normal operation” mode is allocated with the category “frequent” because the risk group is permanently exposed to danger. For example, the operational context: “Normal Operation – Train is running” is defined with “frequent”. The other operational modes (e.g. “degraded mode”, “emergency case”) can be allocated with the appropriate category (i.e. “frequent”, “probable”, “occasional” or “remote”).

The following table summarises the possible stages of the operational contexts. The data from method 1 of MODURBAN are from sub-clause 3.2.1 and the data from



method 2 of MODURBAN from sub-clause 3.2.2. For the comparison the frequency categories of MODTRAIN are transferred from percentage to 0..1. The origin of the numerical values of MODTRAIN in table 8 is extracted from table 3 in sub-clause 3.1.3.1. These descriptions and the actual values of the operational contexts of MODTRAIN are connected to the operational phases and modes.

Table 8 - Comparison of Operational Contexts

MODURBAN		MODTRAIN
<i>Method 1:</i> Frequent – A2 Rare – A1	<i>Method 2:</i> Frequent – E=1 Rare – E=0,1 Very rare – E=0,01	Frequent – [1 - 0,1] Probable – [0,1 - 0,01] Occasional – [0,01 – 0,001] Remote – [0,001 - 0,0001]

4.3.3 Consequence barrier/reduction

To identify consequence barriers or consequence reducing measures a possible question could be: what functions or circumstances may prevent a certain hazard turning into an accident. The above mentioned functions (or circumstances) are meant as additional functions to the investigated safety function itself.

Both methods of MODURBAN have two different types of risk reduction factors. These are the “defence against danger and its consequence(s)” - (method 1) or “consequence reduction probability” - (method 2) and the “probability of danger occurrence” - (method 1) or “accident probability reduction” - (method 2). Method 1 knows two stages for the “defence against danger/consequence”: “Possible” and “Hardly possible”. For the “probability of danger occurrence” there are three stages: “Very low”, “Low” and “Relatively high”. Due to the risk graph method 1 of MODURBAN has five possible variations to describe the consequence barrier. Method 2 uses three stages for both, “accident probability reduction” and “consequence reduction probability”. For both reduction factors there are either “no barrier”, “one barrier” or “two independent barriers”.

In the MODTRAIN method, after the identification of the different functions which could act as a consequence barrier, the efficiency category of each barrier has to be determined. This is followed by the computation of the efficiency category of the combination of all barriers. Values for the efficiency categories are: “Low”, “Medium”, “High”, “Very High” and “Exceptional”.

With respect to consequence barriers or consequence reducing measures, the fundamental difference between these methods is, MODURBAN only asks with respect to the Probability of danger occurrence W (Method 1) or the Accident Probability Reduction P (method 2) if there are barriers or not. For the Defence against danger/consequences G (Method 1) respectively the Consequence Reduction Probability C (Method 2) it is a bit more quantitatively, especially for method 2 it is asked for the probability by orders of magnitude.

Once MODURBAN considers a barrier to be efficient it does not make a difference whether this barrier is very efficient or less efficient. The only difference which could be made is to differ between either *no* barrier or *one* barrier or *two* independent barriers. The degree of efficiency of a single barrier is not taken into account. In contrast to this, MODTRAIN collects all possible functions, which could act as a safety barrier and estimates their magnitude of efficiency (e.g. “Low” or High” or “Very High”). Finally, a computation of the overall efficiency category of all consequence barriers can be accomplished.

The following table (table 9) summarises the possible stages of the consequence barriers. For the comparison the efficiency categories of MODTRAIN are transferred from percentage to 0..1.

Table 9 - Comparison of Consequence Barriers

MODURBAN		MODTRAIN
<i>Method 1:</i>	<i>Method 2:</i>	
<i>Defence against danger:</i>		
Hardly Possible – G2	No barrier – C=1	
Possible – G1	One barrier – C=0,1	Low – [1 - 0,4]
	Two barriers – C=0,01	Medium – [0,4 - 0,1]
		High – [0,1 - 0,01]
<i>Probability of danger occurrence:</i>		Very High – [0,01 - 0,001]
Relatively high – W3	No barrier – P=1	Exceptional – [0,001 - 0,0001]
Low – W2	One barrier – P=0,1	
Very low – W1	Two barriers – P=0,01	

4.3.4 Cause barrier

Cause barriers are functions which could prevent causes related to one hazard to occur. Once these functions are identified a probability category has to be found. Each cause barrier is associated with one efficiency category and probability category respectively. The causal analysis to identify possible cause barriers is only part of MODTRAIN. MODURBAN does not perform a causal analysis. The computation of the overall efficiency of cause barriers is done only for the barriers which affect a certain hazard cause. In table 10 the efficiency categories of MODTRAIN are transferred from percentage to 0..1.

Table 10 - Comparison of Cause Barriers

MODURBAN	MODTRAIN
Not part of this method, investigated function considered as its own cause barrier	Low – [1 - 0,4] Medium – [0,4 - 0,1] High – [0,1 - 0,01] Very High – [0,01 - 0,001] Exceptional – [0,001 - 0,0001]

5 Application of MODURBAN/MODTRAIN methods

This clause embraces the actual application of MODURBAN functions to the MODTRAIN approach. The problem is that this is not directly possible and some adjustments are required. First an explanation is provided for every adjustment which has been made. Consequently, a proposal for an adjusted version of the MODTRAIN approach is illustrated. The following part highlights the selection of certain functions for the set of the MODURBAN functions. An example of an application finalises this clause. The detailed protocols of the applications for the selected MODURBAN functions can be found in the annex.

5.1 Adjustments for the application of MODTRAIN to MODURBAN

Several changes to the MODTRAIN approach are necessary. In the 2006 version of "Guidance for safety analysis" document, MODTRAIN did not describe a way of a final calculation for the SIL. For MODURBAN this approach has been completed as shown in sub-clause 5.1.2. However, not every step of the original application protocol is necessary for the application to MODURBAN functions. In conclusion, these modifications have been made regarding the final calculation, the parameters and the general procedure. The intention is not to change the logic, i.e. the actual approach of the procedure of MODTRAIN. Hence, the procedure of the MODTRAIN approach is kept, but adaptations on constraints are made as well as further suggestions.

Note: In the version 2.0 of the "Guidance for Safety Analysis" document, MODTRAIN described how to calculate the TAR (accidents) and THR (boundary hazards). In contrast to that, MODTRAIN adopted a qualitative approach for the SIL allocation to functions, guided by:

- the safety role of the functions,
- the mapping of functions on the subsystems,
- return of experience and reference to existing solutions,
- a set of tables giving qualitative links between the categories of parameters.

5.1.1 Changes to the parameters

To compute quantitatively a risk level and consequently a SIL, the following parameters have to feature necessarily a numerical value: severity category, operational context and the efficiency of barriers. Since these parameters are only associated with categories, no numerical values are given. Hence, the suggestion is: a conceivable means to obtain these precise numerical values is to choose the most conservative value of the category (cf. table 11). These values (cf. table 11) could be the input for the calculation of TBHR and THCR (cf. sub-clause 5.1.2).

The procedure of identification and determination of the categories for the safety barriers and operational contexts are likewise. The severity categories are not directly associated with a category. But conferring to sub-clause 3.1.1, stage 4 roughly outlines a way to determine a tolerable accident rate (TAR). A suggestion of how this procedure could be interpreted might be as follows: Once a severity level of a hazard consequence is known (e.g. catastrophic or critical), it is possible to say which level



of frequency of occurrence of a hazard (e.g. frequent or probable) could be “tolerable”. This correlation is specified in the risk tolerability matrix (see “Risk Matrix”, EN 50126). In terms of frequency of occurrence of a hazard a tolerable risk rate, which is equal to the tolerable accident rate, could be assigned. The MODTRAIN approach provides categories for this frequency (cf. table 4). Therefore, these categories could be adopted to determine a TAR. So, the TAR is “the maximum rate of occurrence of an accident that is tolerable” as defined above. The TAR is an essential input for the calculation of the TBHR.

Table 11 - Suggestion for the Use of the Parameters

Severity – TAR	Operational Context	Consequence Barrier	Cause Barrier
Catastrophic = $10^{-9}/h$	Frequent = 1	Low = 1	Low = 1
Critical = $10^{-9}/h$	Probable = 0,1	Medium = 0,4	Medium = 0,4
Marginal = $10^{-7}/h$	Occasional = 0,01	High = 0,1	High = 0,1
Insignificant = $10^{-5}/h$	Remote = 0,001	Very High = 0,01	Very High = 0,01
		Exceptional = 0,001	Exceptional = 0,001

With respect to the value for the severity “critical” = $10^{-9}/h$, this value originates from a straightforward application of the risk tolerability matrix (cf. table 5) and the frequency categories of table 4 “Risk categories given in EN 50126 standard“ of MODTRAIN.

It has to be stressed that this choice is in contrast to the MODURBAN approach where the severity category (SL) for critical consequences equals $10^{-8}/h$.

5.1.2 Final calculation

The first important point to stress is that all numbers, values and categories are project dependent for MODTRAIN and for illustration only. But, even though these numbers are project dependent, due to the applied decade system the possibilities for the choice of numerical values are rather small. And finally the user of a certain risk analysis method chooses suitable numbers for the applied system. Therefore, it is possible to find a way to determine and suggest numerical values, as described above. The second point is to find a general basis for calculation, because MODTRAIN does not give any outline or advise regarding a final calculation. But, as the context is fairly simple a formula can be derived; starting from the severity of an accident, the safety barriers and the operational context acting as means reducing the risk. Basically, this approach is based on the applied formula of MODURBAN⁷. Starting from a level of severity in combination with risk reduction factors it yields a THR. But, due to the fact that in this formula (formula 1) cause barriers are included as well, it yields a THR on sub-system level, which accords with the THCR.

⁷ So the MODTRAIN-approach is more or less transferred to the MODURBAN-approach.

Note: Instead of a computation and allocation of THR to functions in order to get a SIL, MODTRAIN finally recommends (see "Guidance for safety analysis" version 2.0) a qualitative approach to the SIL allocation, based on a propped-up reasoning and a set of tables giving qualitative links between categories of parameters (THR to SIL, Efficiency to SIL, SIL combination rules).

Precisely:

$$(1) \quad THCR = \frac{TAR}{OC * COB * CAB}$$

THCR – Tolerable Hazard Cause Rate
TAR – Tolerable Accident Rate
OC – Operational Context
COB – Consequence Barrier
CAB – Cause Barrier

For a later application the following formula can be used:

$$(2) \quad TBHR = TAR / (OC * COB)$$

$$(3) \quad THCR = TBHR / CAB$$

For the case a certain function or a boundary hazard might have two or three consequence barriers the formula for TBHR could be as follows:

$$(4) \quad TBHR = TAR / (OC * COB_1 * COB_2 * COB_3)$$

In case a certain function or a boundary hazard might have two or three cause barriers the formula for THCR could be the following:

$$(5) \quad THCR = TBHR / (CAB_1 * CAB_2 * CAB_3)$$

But, formula 5 only considers cause barriers which are associated to a certain hazard cause.

COB and CAB represent the efficiency of the consequence and cause barrier.

To compute THCR the values of table 11 can be used.

5.1.3 Changes to the procedure

The following list of changes refers to table 1 - "Procedure of MODTRAIN" in sub-clause 3.1.2. Again, the logic of the MODTRAIN approach has not been changed, only a bunch of steps have been crossed out of the procedure. All efforts of justification and decisions for safety requirements are cancelled, because they are not part of this analysis (Step: 4d, 6d, 7, 8, 10a, 11a, 11c, 15, 16, 17). All steps of justification and decisions for safety requirements are on the top of an actual risk analysis and do not affect the approach of MODTRAIN by cancellation. Further changes affect all steps regarding the determination of the safety impact. It has been cancelled due to the fact that all the MODURBAN functions, which are of interest in this deliverable (i.e. selected safety functions of D 86), are already safety relevant and therefore it is not necessary to prove their status again (Step: 2, 5d). It is



assumed that the steps of recap are natural and do not need any further mention (Step: 3, 3a, 3b).

5.1.4 Suggestion or the procedure of an adjusted MODTRAIN version

On the basis of the considerations done above, the following table 12 is a proposal for an adjusted version of the MODTRAIN approach for the application of MODURBAN functions. Table 12 is based on table 1 - "Procedure of MODTRAIN". In particular, table 1 is the original procedure of MODTRAIN. After consideration of changes, which are described in sub-clause 5.1.1 Changes to the parameter, 5.1.2 Final calculation and 5.1.3 Changes to the procedure, one can yield table 12 from table 1.

Table 12 - Suggestion for the procedure of an adjusted MODTRAIN version

Stage	Description	Comments
Input	System Definition – identified function	
Hazard Identification	Define Accident Case	
	Identify Operational Context	PC
	Identify Boundary Hazards	
	Identify Accident Type	
Consequence Analysis	Identify Consequence Barriers	
	Identify Functional Barriers	Add purpose
	Identify Human Factors	Operation or HF
	Efficiency of each Consequence Barrier	EC
Cause Analysis	Identify Hazard Causes	Which lead to BH
	Identify Failures of Sub-Functions	
	Identify specific Failures	e.g. mechanical
	Identify Human Factors	
	Identify Cause Barriers	
	Identify Sub-Functions	
	Identify Human Factors	Operation or HF
	Determine Efficiency of each CAB	EC
Risk Estimation, SIL and THR Allocation	Determine Tolerable Accident Rate	SC, RTM
	Determine Tolerable Boundary Hazard Rate	Formula (4)
	Compute the efficiency of each COB	In combination
	Compute TBHR of BH	TAR, OC, COB
	Determine Tolerable Hazard Cause Rate	Formula (5)
	Allocate THCR to HC	CAB, TBHR
	Select the lowest THCR of each HC among all ACs	
	Allocate SIL to each function involved in HC according to its THCR	

5.2 Selection of Safety Functions

Two aspects are covered in this deliverable. On the one hand the mere comparison of the different approaches (the two of MODURBAN and the one approach of MODTRAIN). And on the other hand a discussion, comparison and a potential confirmation of the results for MODURBAN functions. These MODURBAN functions are those where in D 86 no consensus has been achieved. For these ambiguous functions of D 86 further investigations is indispensable and therefore the MODTRAIN approach shall be applied to reach a basis for a discussion.

The numbering of the safety functions of MODURBAN like “MU 1.11 Obstacle Detection in Front of Train” refers to D 86.

For a general illustration the following MODURBAN function has been chosen:

- MU 1.1 Train Integrity Supervision

The group of MODURBAN function which are due to further investigations consists of:

- MU 1.11 - Obstacle Detection in Front of Train
- MU 2.1.1 - Door Obstruction Detection
- MU 2.1.2 - Gap Supervision/Protection
- MU 2.3 - Train Departure Supervision/Management
- MU 4.6 - Safe Emergency Brake from OCC
- MU 5.1.1 - Emergency Stop Request (onboard, by passenger)
- MU 5.1.2 - Emergency Stop Request (from Station Platform)
- MU 5.2 - Safe Manual (Emergency) Door Opening

Most of these functions are on-demand-functions and therefore it is assumed that the application of the SIL-concept is difficult. EN 50129 notes the following:

“In contrast to other standards the SIL table in this standard has only one column for frequencies (formerly called high demand or continuous mode) and does not have a column for failure probabilities on demand (formerly called demand mode). The reasons to restrict to one mode are

- less ambiguity in determination of SIL,
- all demand mode systems can be modelled as continuous mode systems,
- continuous control and command signalling systems are clearly the majority in modern railway signalling applications.”

5.3 Application of safety functions

This clause illustrates the application of the MODURBAN functions with the MODTRAIN approach. Out of a number of selected MODURBAN functions one is shown in this section, because a clear arrangement is strived. All MODURBAN functions, which are of interest for this deliverable, can be found in the annex.

The structure of the application of this adjusted version of MODTRAIN is as follows: Firstly the original function of MODURBAN is displayed. This safety analysis of MODURBAN is extracted directly from D 86. This is followed by the actual application of the adjusted MODTRAIN version. A virtual confirmation of MODURBAN results by means of the adjusted MODTRAIN version is not really allowable because all numbers and categories of MODTRAIN are for illustration only. But due to the decade system and the individual choice of the grade of the parameter for certain system architecture it is acceptable for a practical application.

In the application of the adjusted MODTRAIN version two cases are described: “with a driver” and “without a driver”. It can be assumed that “with a driver” equals the MODURBAN Grade of Automation GOA 0...2 and “without a driver” GOA 3 and 4, in other words:

- GOA 0 - On-sight train operation
- GOA 1a - Non-automated train operation with intermittent supervision
- GOA 1b - Non-automated train operation with continuous supervision
- GOA 2 - Semi-automated train operation
- GOA 3 - Driverless train operation
- GOA 4 - Unattended train operation

5.3.1 Safety function MU 1.1 Train Integrity Supervision

Function Summary Description:

The completeness or integrity of the train is monitored by trainlines/sensors and the CC.

Operating Modes:

Optional: GOA 1b, 2; Mandatory GOA 3, 4

5.3.1.1 MODURBAN approach

Possible Wrong Side Failure:

Train Integrity signals complete train consists while in fact train has parted in two.

Associated Hazard:

Train cars may get to close

Possible Consequence/Accidents:

Collision at $v > 30 \text{ km/h}$

Exposition:

Passengers are permanently onboard of trains, exposed to open door (A2 / E=1)

Possible Barriers:

No additional barrier can be conservatively assumed (W3 / P=1)

Possible Consequence Reduction:

Passengers can in general not escape or reduce consequence (C=1)

Table 13 - Train Integrity Supervision MODURBAN method 1

SIL allocation – qualitative	
Train Integrity Supervision	
S – Damage/Severity	S3
A – Typical Exposition to Hazard	A2
G – Risk Reduction Potential	
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 4

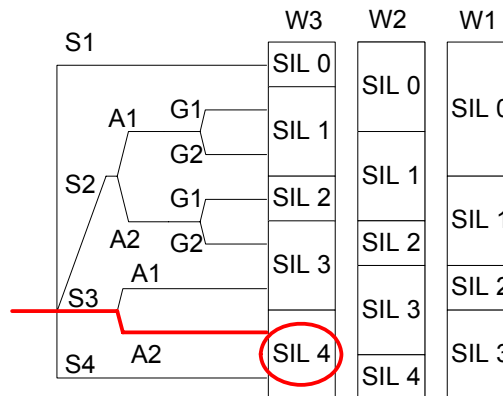


Table 14 - Train Integrity Supervision MODURBAN method 2

SIL allocation – semi quantitative	
Train Integrity	
SL – Damage/Severity	SL4
E – Exposition Probability	1
P – Accident Probability	1
C – Consequence Reduction	1
THR4/1	THR4
Safety Integrity Level (SIL)	SIL 4

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

Train Integrity Supervision needs to be supervised with SIL 4.

5.3.1.2 MODTRAIN approach

Description: This function simply describes the supervision of the train integrity. In case the train would loose units without the detection by the supervision system, a collision might be the consequence. Conceivable safety barriers are; the driver, of the following train notices the lost units and applies the emergency brake as soon as possible.

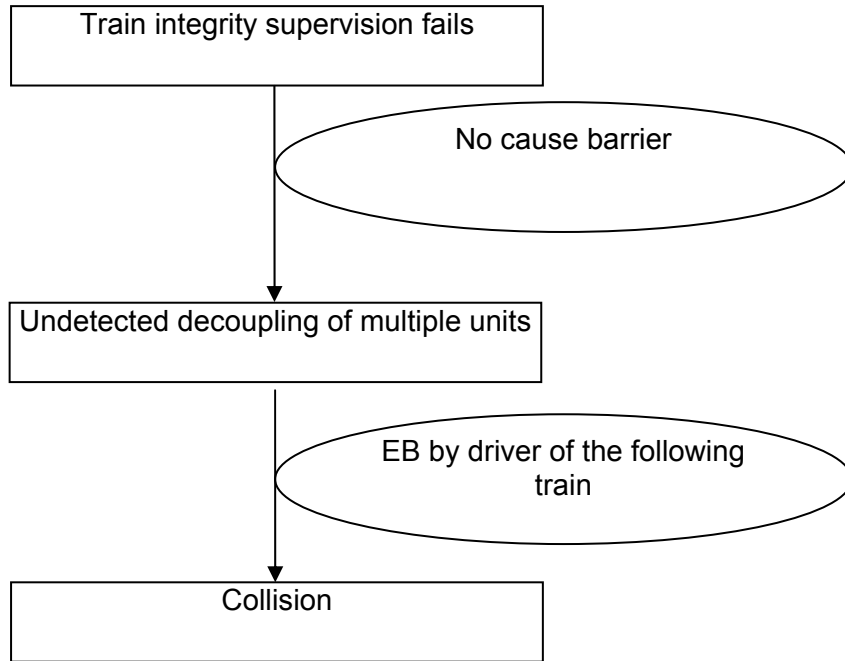


Figure 4 - Train Integrity Supervision MODTRAIN approach

Accident Context:

- Operational Context = Normal Operation – Train is running [Probability = Frequent]
- Boundary Hazard = [Undetected decoupling of units]
- Accident Type = [Collision] [Severity = Catastrophic]

Consequence Barriers:

Consequence barrier 01 = [Human Factor] [Driver of following train notices the lost unit] (applies emergency brake) [Efficiency = Low]

Hazard Causes:

Cause 01 = [Train Integrity Supervision] [Train integrity signals complete train, in fact train has parted in two]

Cause Barriers:

Barrier 01 / Cause 01 = no cause barrier

Final Calculation:

With driver

TAR = $10^{-9}/h$
 TBHR = $10^{-9}/h / 1 / 1 = 10^{-9}/h$
 THCR = $10^{-9}/h / 1 = 10^{-9}/h$
 Result: **SIL 4**

Without driver

TAR = $10^{-9}/h$
 TBHR = $10^{-9}/h / 1 / 1 = 10^{-9}/h$
 THCR = $10^{-9}/h / 1 = 10^{-9}/h$
 Result: **SIL 4**



Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

The adjusted MODTRAIN version (SIL4) confirms the result of MODURBAN (SIL 4). No safety barriers can be assumed.

With a driver:

The result is SIL 4. This analysis has been given as a reference. The stated consequence barriers has been estimated with an efficiency of “low”, because the driver of the following train will not be able to brake the train in time to reduce the consequences of an accident.

A cause barrier does not exist, because there are no means to prevent the boundary hazard i.e. an undetected decoupling of the units.

6 Comparison and evaluation of applications

This clause covers the comparison and the evaluation of the results of the application of the adjusted MODTRAIN version. It compares the application of the MODURBAN approach, described in D 86 and the adjusted MODTRAIN version, applied to selected MODURBAN functions. It comprises a discussion about simplicity, unambiguity and transferability of the application.

6.1 Introduction

First, it is not possible to apply the original MODTRAIN approach to MODURBAN functions. The major reason for this is that the methodologies applied in both research projects differ. Therefore, adjustments and assumptions to MODTRAIN are necessary, which have two effects:

- A comparison is only possible between the adjusted version of MODTRAIN and MODURBAN.
- Only the mere application of the three methods is comparable.

This is mainly due to the fact that MODTRAIN uses project depended numerical values and categories.

6.2 Transferability

The safety functions of MODURBAN are from a different project, in comparison to MODTRAIN, and are therefore from different system architecture. Hence, it is necessary to separate the method of MODTRAIN from its system architecture to gain the mere procedure. On this basis it is possible to apply the MODTRAIN method to MODURBAN functions. All assumptions, which have been made, affect mainly the handling of the numerical values of the parameters. This is not part of the methodology, because especially the graduation of the efficiency categories is project dependent and should be done for each individual project and system. The other adjustments have been assumed to be dispensable for the application.

To conclude, every way of description to analyse the selected function which is possible with MODURBAN is possible with MODTRAIN as well. Additionally, MODTRAIN provides more possibilities for the safety analysis, e.g. the causal analysis or the graduation of the parameters – which is based on the different overall approach. Nevertheless, this shows that is feasible to transfer MODTRAIN to the MODURBAN system.

6.3 Simplicity

With reference to the application, it is easier to apply the MODURBAN approach. Substantially, this has two reasons; first of all, the simple approach to determine the severity level and secondly the straightforward way of the application of the risk reduction factors. Using the first method of MODURBAN one simply follows the risk graph. Even though, MODURBAN is not applied to safety functions from other

systems, it seems that further adjustments would not be necessary, because of the simple procedure.

In MODTRAIN the number of steps of the procedure is higher compared to MODURBAN. A more detailed estimation and identification of the different parameters is needed.

In the 2006 version of "Guidance for safety analysis" the way for computing the THR and SIL was not sufficiently explained and therefore could be misinterpreted.

Assumptions and adjustments for a certain project are necessary, e.g. efficiency categories, numerical values and list for hazards and accidents. Admittedly, because the underlying model of safety entities is more developed, more flexible applications for safety functions are possible, but getting more traced results implies more efforts (see next sub-clause).

6.4 Unambiguity

A general statement whether MODTRAIN or MODURBAN is more or less ambiguous is not possible. The MODURBAN approach provides a simple procedure in combination with precise described parameters featured with numerical values i.e. factors. Furthermore, the stages per parameter (e.g. the graduation of the risk reduction factors E, P and C, cf. sub-clause 3.2.2) seem to be not sufficient enough for a good description of every problem. Especially the fact that the depth of the efficiency of a barrier is not considered could be problematic. Another problem is that sometimes the two methods of MODURBAN yield two different results. Because of exclusions of the risk graph of method 1 of MODURBAN results can be in contrast to method 2.

The application of MODTRAIN requires a precise execution of the detailed procedure. The mere identification of most of the parameters is described well. This can prevent ambiguities. But due to the fact that the values featuring the categories of efficiency, probability and frequency are given for illustration only a margin for adjustments and assumptions is left. *But, with reference to the original MODTRAIN approach, for example, the application is based on an exact and well defined system definition and lists for possible boundary hazards and accidents (and operational contexts).* The identification of the accident, hazard, hazard cause and safety barriers arises from this system. In comparison to the MODURBAN approach it is much more traceable where certain characteristics and parameter (e.g. accident types or boundary hazards) originated. So it is foreseen that different projects applying the MODTRAIN-approach may come to different results due to the difference of context between projects.

6.5 Reason for different Results

With respect to the application of the adjusted MODTRAIN approach to some problematic functions of MODURBAN (see annex of D90), the results are concluded in the following table.

Table 15 - Examples for possible deviations for On Demand Functions

	Function	Results – without a driver		
		MU Method 1	MU Method 2	MODTRAIN
1.11	Obstacle Detection in Front of Train	SIL 3	SIL 3	SIL 4
2.1.1	Door Obstruction Detection	SIL 2	SIL 2	SIL 2
2.1.2	Gap Supervision/Protection	SIL 1	SIL 2	SIL 1
2.3	Train Departure Supervision/Management (Onboard and wayside train departure)	SIL 4	SIL 4	SIL 4
4.6	Safe Emergency Brake from OCC	SIL 3	SIL 3	SIL 1
5.1.2	Emergency Stop Request (from Station Platform)	SIL 1	SIL 1	SIL 1
5.2	Safe Manual (Emergency) Door Opening	SIL 3	SIL 2	SIL 1

Out of the analysed examples of problematic functions, in three cases the results of the three methods are in accordance with each other (2.1.1; 2.3; 5.1.2). For the rest of the functions MODTRAIN comes to different results, here; with a lower level for safety integrity. These differences have various reasons. Detailed information can be taken from the annex of D90.

Exclusions

The different results of the two methods of MODURBAN arise mainly because of exclusions made by the risk graph of method 1 of MODURBAN. A second difference which affects the approach of MODURBAN as well as MODTRAIN is the stages or graduation of the parameters. For example, method 1 of MODURBAN provides only two stages to describe the exposure to danger, whereas, method 2 provides three possibilities. Finally, MODTRAIN features four stages for the exposure to danger. Different numerical values and therefore different final result are the consequence when taking for example the lowest stage in the application. In other words; MODTRAIN does not provide as much limitations – in terms of stages per parameter - as the two methods of MODURBAN, therefore, MODTRAIN provides the user with more possibilities for an application. This effects mainly the analysis of on-demand function e.g. for emergency cases. In these cases MODTRAIN allows different values i.e. a different stage of parameter for the analysis and therefore produces different results.

A more developed approach and harmonised description regarding the graduation of the stages per parameter is presumably subject to future projects.

Efficiency of Barriers

Another point is that MODURBAN does not identify the efficiency of a barrier/safety function, once a barrier has been identified. It only determines if there are no, one or two efficient barriers. This makes the application of the method much more easy, but it does not distinguish between non-quantifiable barriers (which do not have to be “safe”, e.g. SIL 1) and safety related functions which act independently from the safety function which is investigated.

Rare Events

The next problem envelops emergency cases. Even though, MODURBAN states “the use of EB will be a very rare event” and defines the exposure of a very rare event with $E=0,01$ it assumes $E=0,1$ only. In the application of the adjusted MODTRAIN version the emergency case has been assumed to be “remote”. Here again the assumed problem of the so called On-Demand-Functions arises. As stated in sub-clause 5.2 however, these kinds of functions are excluded from the SIL-concept.

Numerical Values

The last major difference arises from the different use of the numerical value of the term “critical” as description for the severity level. As explained in sub-clause 5.1.1 “critical” is featured with a numerical value of $10^{-9}/h$ in the adjusted MODTRAIN version and with $10^{-8}/h$ in MODURBAN.

All differences are explained for every analysed function in detail and can be found in the annex D90.

7 Findings and Recommendations

Resulting from the above comparisons the following observations and recommendations are expressed:

1. The MODURBAN project has studied and applied three different approaches to allocate Safety Integrity Levels to safety functions (the MODURBAN ATP Functions). All three methods have sound backgrounds and reasonable arguments for application. All three methods are in general compatible with the European Cenelec Standards EN50126-129 and involve the concepts of risk, severities, frequencies, exposures and barriers.
2. The two MODURBAN approaches of D 86 yield identical results for all continuous train protection functions (in term of SILs) but sometimes divergent functions for the On Demand Functions like Platform Edge Protection. The two approaches (Qualitative and Semi-Quantitative MODURBAN Approaches) are relatively straightforward in application, involve however a Hazards and a Risk Analysis.
3. For more detailed analysis, this deliverable D 90 investigates the applicability and consistency of the MODTRAIN analysis approach with the MODURBAN approach. In MODTRAIN allocation methods have been developed, but no THR on hazards and SIL on functions have been determined in a generic way because MODTRAIN considers that quantifications and allocations are project dependent. MODURBAN made some numerical and other assumptions to apply the MODTRAIN process concretely.
4. For Continuous Protection Functions, the MODTRAIN process is likely to yield the same results as the two MODURBAN approaches. For the critical On Demand Functions the application of the MODTRAIN process yielded again different results from the MODURBAN approaches, sometimes even a third value is derived in terms of SILs.
5. The MODURBAN project confirms therefore the CENELEC working group findings that a SIL value cannot be allocated in a straightforward way and with the same (statistical) meaning as for Continuous Safety Functions.
6. The project further observes that the MODTRAIN processes are well engineered but require additional concrete decisions and inputs before being able to be applied to concrete functions.
7. In order to define Safety Integrity Level Requirements for continuous urban train control safety functions, the application of either of the two MODURBAN approaches is recommended. Only in case of high dependency from operational contexts it is recommended to apply in addition the MODTRAIN process.
8. For On Demand Functions, the direct allocation of a SIL value is not recommended. If analysed anyway, the resulting SIL requires complex interpretation considerations and implication of the operational context in any event.

References

- CENELEC: Railway Applications- Safety related Electronic Systems for Signalling. EN 50129, 2003
- CENELEC: Railway Applications- The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). EN 50126, 1998
- MODTRAIN/MODCONTROL: Guidance for Safety Analysis, Draft Version, March 2006