



MODURBAN

FP6 Project: IP 516380

EC Contract n°: TIP4-CT-2005-516380

MODSYSTEM SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D 127
Deliverable Title:	Preliminary Hazard Log
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: Preliminary Hazard Log
Document ID: D 127
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	08/01/31	First version for comments	TUD
Draft 2	08/02/28	Consideration of comments received during review of Draft 1	TUD
Final Draft	08/03/31	Consideration of comments on Draft 2	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

**D 127
 Preliminary Hazard Log**

Deliverable ID , associated WP & Subproject	D 127 MODSYSTEM / WP 23
Type of Deliverable	Report
Input / Starting stage	D77, D78, D81, D86
Output / Final stage	

Lead partner(s)	
Achievement to date (%)	
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	

D 127 Preliminary Hazard Log

Deliverable Abstract

To support a risk assessment a Hazard Log is used to record possible Hazards and its corresponding measures for risk reduction. The objective of deliverable D127 is to create a generic Hazard Log for a MODURBAN application. To achieve this goal, first the theoretical conception of a Hazard Log is investigated. This is done by an analysis of the role of the Hazard Log in the system lifecycle according to EN 50126. Secondly, methods for Hazard Identification are discussed, because the identified Hazards are the first input and basis of the Hazard Log. Thirdly, functions and elements for a Hazard Log are investigated. For a final creation of a generic Hazard Log, various examples of different industries are provided. On the background of the gathered results and the analysed examples a generic Hazard Log is created. This Hazard Log is applied to MODURBAN under the usage of MODURBAN PHA Hazards and MODURBAN functions as possible Risk Reduction Measures. For an adequate treatment of open issues regarding measures for risk reductions various suggestions and assumption are made in the application of the Hazard Log.

Associated Milestone (if relevant):



SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

Table of Contents

- 1 Introduction..... 9
 - 1.1 Purpose and Scope..... 9
 - 1.2 Structure of the Study..... 10
 - 1.3 Objectives 10
- 2 Term, Definitions and Abbreviations..... 11
 - 2.1 Terms and Definitions 11
 - 2.2 Abbreviations 12
- 3 The Conception of the Hazard Log..... 13
 - 3.1 Preface..... 13
 - 3.2 Hazard Log in the Overall System Lifecycle..... 13
 - 3.2.1 The RAMS Lifecycle according to EN 50126 13
 - 3.2.2 Hazard Log in the RAMS Lifecycle..... 16
 - 3.3 Hazard Identification as Input to the Hazard Log 20
 - 3.4 Functions and Elements of a Hazard Log 24
 - 3.4.1 Description of Functions in a Hazard Log 24
 - 3.4.2 Description of Elements in a Hazard Log 27
- 4 Approach for the Development of the Structure of a Hazard Log 29
 - 4.1 Lifecycle of a Hazard Log..... 29
 - 4.2 Approach for the Development of a Structure 30
 - 4.2.1 Theoretical Approaches for the Creation..... 30
 - 4.2.1.1 Intuitive Approach 30
 - 4.2.1.2 Example of Abstract Model 30
 - 4.2.2 Tool Support for the Development 32
 - 4.3 Examples of Hazard Logs 32
 - 4.3.1 Hazard Logs in the Railway Industry 33
 - 4.3.2 Hazard Log in Aviation 34
 - 4.3.3 Hazard Log in Military 35
 - 4.3.4 Conclusion of the Illustration of Examples of Hazard Logs 37
- 5 The Preliminary Hazard Log for MODURBAN..... 38
 - 5.1 Approach for the Development of the Hazard Log 38
 - 5.1.1 The Idea to the Development of the Structure..... 38
 - 5.1.2 The Software Tool..... 38
 - 5.1.3 Initialisation of the Hazard Log 38
 - 5.2 Documentation of the Hazard Log..... 40
 - 5.2.1 Approach to the Application 40
 - 5.2.2 Structure for the Hazard Log..... 40
 - 5.2.3 The Development of the Hazard Log 42
 - 5.2.3.1 Hazard Description 44
 - 5.2.3.2 Risk Evaluation – Before..... 46
 - 5.2.3.3 Risk Reduction Measure 48
 - 5.2.3.4 Risk Evaluation – After..... 50



5.2.3.5	Closure.....	50
5.2.3.6	Status.....	51
5.2.3.7	Notes and Comments	51
5.2.3.8	Journal and Glossary	52
5.3	Application of the Hazard Log	52
5.3.1	Assumptions for Application of the Hazard Log.....	52
5.3.2	Example of the Hazard Log for MODURBAN	53
6	Analysis of the Application of the Hazard Log	57
6.1	The Application of the Hazard Log for MODURBAN	57
6.1.1	Results of the Hazard Log – Closure of Hazards	57
6.1.2	Manageability of the Hazard Log.....	58
6.1.3	Hazard Description.....	58
6.1.4	Risk Evaluation	59
6.1.5	Risk Reduction Measure	59
6.1.6	Closure.....	60
6.1.7	Status.....	60
6.2	Discussion about Export of Hazards	60
6.3	General Recommendations and Future Steps	61
7	Conclusion.....	62
8	References	63
9	Appendices.....	65
Appendix A	65

List of Figures and Tables

List of Figures

Figure 1 - System Lifecycle according to EN 50126	14
Figure 2 - Hazard Log in the System Lifecycle	17
Figure 3 – RAMS Documents in the System Lifecycle [SOL 04]	19
Figure 4 – Process Details of Risk Analysis [MOK 04]	21
Figure 5 – Example of Risk Categories according to [EARL].....	26
Figure 6 – Hazard Log Lifecycle	29
Figure 7 – Conceptual Model for a Hazard Log [HAM 04]	31
Figure 8 – Hazard Log – Railway [FAR 04]	33
Figure 9 – Hazard Log – Civil Aviation [CAA 02]	34
Figure 10 – Hazard Log - Australian Navy 1 [ADE 07]	35
Figure 11 – Hazard Log – Australian Navy 2 [ADE 07].....	36
Figure 12 – PHA for MODURBAN Excerpt A.....	39
Figure 13 – PHA for MODURBAN Excerpt B.....	39
Figure 14 – Hazard Log Action Procedure.....	43
Figure 15 – Example of Hazard Log for MODURBAN	55

List of Tables

Table 1 – Example of Risk Matrix according to [EARL]	25
Table 2 – Status Control according to [PAS 03]	27
Table 3 – Functions and Elements of a Hazard Log.....	28
Table 4 – Structure of Hazard Log for MODURBAN.....	41
Table 5 – Risk Matrix according to EN 50126.....	46
Table 6 – Frequency of Occurrence of Hazardous Events according to EN 50126..	46
Table 7 – Hazard Severity Level according to EN 50126	47
Table 8 – Qualitative Risk Categories according to EN 50126	47

1 Introduction

1.1 Purpose and Scope

The European market for light rail and metro systems for urban public transport becomes increasingly important. This is mainly due to two facts. First of all, there is the growing need for bigger, faster and more environmentally compatible modes of urban transportation. This goes along with the rising interest for financial investment regarding future urban guided rail systems (cf. [SCH 07]¹). To meet these chances for a future development and to cope with an increasing demand for public transportation, European research and development projects are launched. MODURBAN (Modular Urban Guided Rail Systems) is one of these projects. The main goal of MODURBAN is to design, develop and test an innovative, interchangeable and open common Automatic Train Control core system and its key interfaces to pave the way for the next generations of urban-guided public transport systems. A sub-project of MODURBAN is MODSYSTEM. It deals with the overall system approach and the functional and technical specification. Furthermore, MODSYSTEM investigates - amongst other tasks - a global risk assessment and safety targets. One major part of a risk assessment is the Hazard and Risk Analysis. The Hazard Analysis shall identify all conceivable Hazards of a transportation system with possibly dangerous consequences. A Risk Analysis estimates the associated risks which evolve from the identified Hazards. This deliverable investigates a tool to support Hazard and Risk Analysis throughout the life cycle of a MODURBAN like project. This tool is a log file and is called Hazard Log. It aims to record and document all conceivable Hazards of a system in combination with possible Risk Reduction Measures. This Hazard Log is of utter importance for a safe system design, because it logs all Hazards in order to pay attention and provide coverage for all possible dangerous situations. Moreover, it supports not only the Risk Analysis; but is further a central document for all phases of the system lifecycle.

This guideline for a Hazard Log applies mainly to the system operator. This analysis, which is conducted here, is predominantly on system level. Following EN 50129, the Hazard and Risk Analysis on system level (including the set-up and maintenance of a Hazard Log) should be performed by the operator. However, the Hazard Log is always used by the supplier particularly in the Hazard Control phase. The operator and the supplier have to perform Hazard Logs and prove their equivalence.

¹ This article describes the worldwide perspectives and chances of metros and light rail systems with respect to an economic growth and an increasing urbanisation

1.2 Structure of the Study

This deliverable is divided into five major parts. On top of an initial introduction about the topic of a Hazard Log, the third clause deals with the theoretical conception of the Hazard Log. It considers the Hazard Log in the overall system lifecycle according to EN 50126, the Hazard Identification and a discussion of alternative approaches to the Hazard Log. The fourth clause “Approach for the Development of the Structure of a Hazard Log” describes a suggestion for a Hazard Log lifecycle. Furthermore, clause 4 gives examples for the development of Hazard Logs and examples of Hazard Logs of different industries. Subsequently, an actual Hazard Log is created in clause 5. This Hazard Log is applied to the MODURBAN project, which is shown in clause 5 in detail. Finally, clause 6 comprises an analysis and further recommendations for the Hazard Log and its application.

Additionally, D127 contains an annex. This annex is an excel sheet with the Hazard Log for the MODURBAN application, including examples for the contents of a Hazard Log application (i.e. MODURBAN Hazards and functions). Again, Annex A is an example and has to be assessed for each project.

Moreover, references of quotations are indicated by squared brackets e.g. [EN 50126]. To support the structure of the text, keywords are marked in a bold font.

1.3 Objectives

- (1) Provision of theoretical knowledge about Hazard Logs in the urban guided rail business
- (2) Creation of a generic Hazard Log
- (3) Application of the generic Hazard Log to the MODURBAN project
- (4) Draft suggestions for possible risk mitigation for the MODURBAN application

2 Term, Definitions and Abbreviations

2.1 Terms and Definitions

Term	Definition	Reference
<i>Accident</i>	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
<i>Hazard</i>	A condition that could lead to an accident.	EN 50129
<i>Hazard Log</i>	The document in which all safety management activities, hazards identified, decisions made and solutions adopted. Are recorded and referenced.	EN 50129
<i>Human Factor</i>	Parameter to describe physiological, social and cognitive interactions between a human and a technical system.	Own definition
<i>Maintenance</i>	The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform its required function.	EN 50129
<i>Risk Reduction Measure</i>	Measure, actions or functions to reduce the risk of a Hazard.	Own Definition
<i>Safety Plan</i>	The implementation details of how safety requirements of the project will be achieved.	EN50129
<i>System Lifecycle</i>	The activities occurring during a period of time that starts when a system is conceived and ends when the system is no longer available for use, is decommissioned and is disposed.	EN 50126

2.2 Abbreviations

<i>ATC</i>	Automatic Train Control
<i>CSR</i>	Component Safety Requirement
<i>EN</i>	European Standard
<i>FMEA</i>	Failure Mode and Effects Analysis
<i>FTA</i>	Fault Tree Analysis
<i>GOA</i>	Grade of Automation
<i>HAZOP</i>	Hazard Operability Study
<i>HMAS</i>	Her Majesty's Australian Ship
<i>HRI</i>	Hazard Risk Index
<i>LOT</i>	Level of Trust
<i>MODURBAN</i>	Modular Urban Guided Rail Systems
<i>OCC</i>	Operations Control Centre
<i>PHA</i>	Preliminary Hazard Analysis
<i>RAMS</i>	Reliability, Availability, Maintainability, Safety
<i>RCM</i>	Remote Condition Monitoring
<i>SIL</i>	Safety Integrity Level
<i>SSR</i>	System Safety Requirement
<i>THR</i>	Tolerable Hazard Rate
<i>UITP</i>	International Union of Public Transport
<i>ULH</i>	Upper Level Hazard
<i>UNIFE</i>	Union of the European Railway Industries
<i>WP</i>	Work Package

3 The Conception of the Hazard Log

The goal of this clause is to create knowledge about the idea and the concept of a Hazard Log. Furthermore, clause 3 describes the role of the Hazard Log in the system lifecycle and the system approval process. This clause is finalised by a description of the strived functions and elements of a Hazard Log.

3.1 Preface

During the conception and a final approval of an urban guided rail system it has to be proved that a transportation system in operation is safe. Safety is the “freedom of unacceptable risk” [EN 50126]. By an identification of possible Hazards of the transportation system the risk of this system can be estimated. EN 50126-2 defines a Hazard in the following way: “A condition that could lead to an accident.” [EN 50126-2] For the purpose to **record the identified Hazards** a Hazard Log is used. This can be realised preferably by a **software database**. The objective of these kinds of logs is to record all possible Hazards during the system lifecycle in order not to forget possible dangerous events. The final motivation for a documentation of Hazards is to **cover all Hazards with Risk Reduction Measures** in order to minimise “conditions that could lead to an accident” [EN 50126-2] to an acceptable level. This is done to support the design and justification of a safe system. Additional reasons for the development of a Hazard Log are that for an average transportation system easily 1000 Hazards can be identified. A Hazard Log supports the handling and management of these amounts of Hazards to **minimise human errors**.

In conclusion; the Hazard Log is a tool to record all Hazards which might evolve in the system lifecycle. Moreover, the Hazard Log documents Risk Reduction Measures for each Hazard.

3.2 Hazard Log in the Overall System Lifecycle

3.2.1 The RAMS Lifecycle according to EN 50126

In the following section the Hazard Log is analysed against the background of the system lifecycle to investigate the **meaning of the Hazard Log** for the approval process. The foundation for a discussion and a later analysis about a Hazard Log in the railway industry is the system lifecycle described in EN 50126. It states: “The system lifecycle is a sequence of phases, each containing tasks, covering the total life of a system from initial concept through to decommissioning and disposal.” [EN 50126] Figure 1 describes the system lifecycle².

² Figure 1 is slightly adjusted for the purpose of this deliverable.

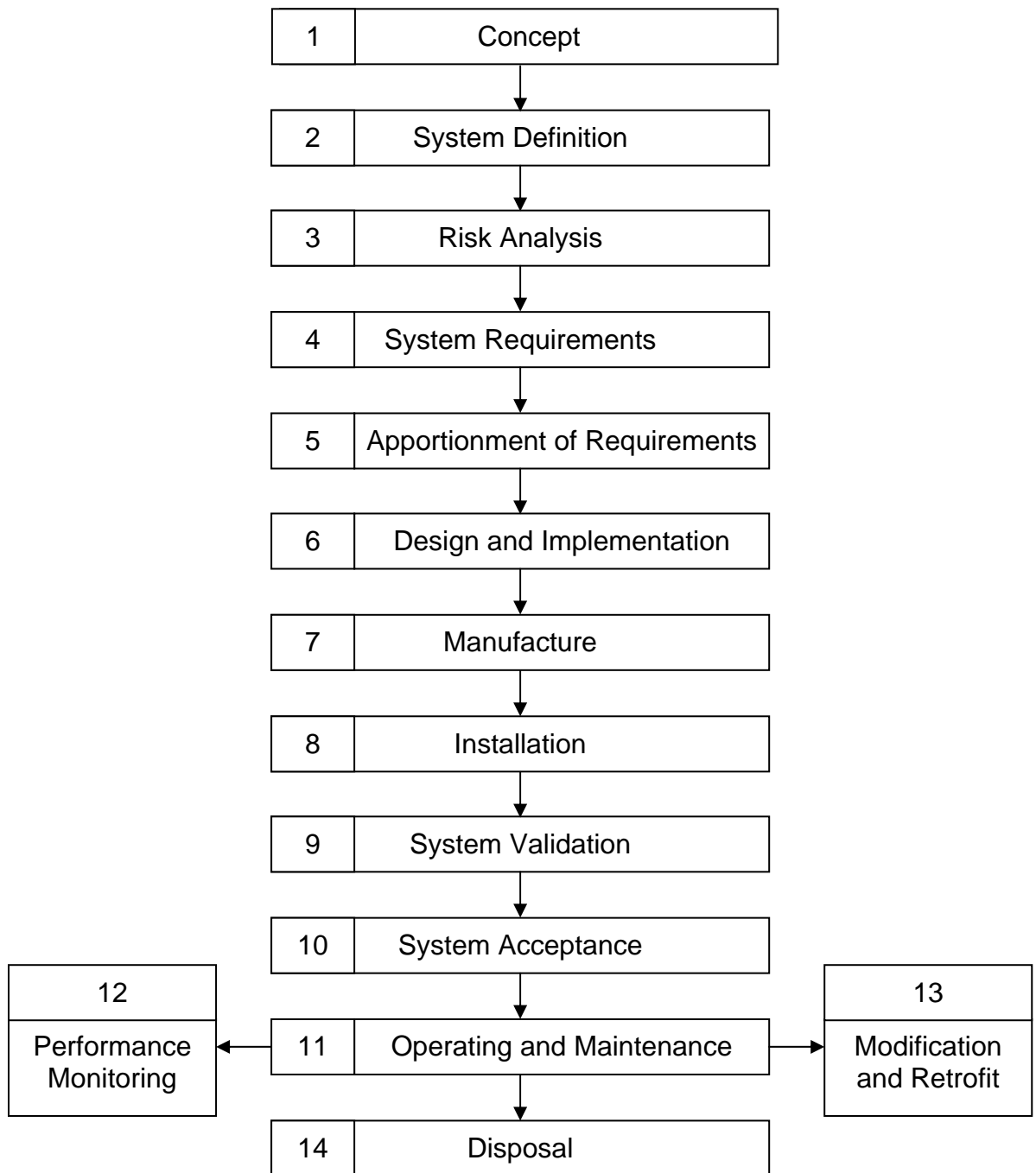


Figure 1 - System Lifecycle according to EN 50126

The following section describes the different system lifecycle phases in more detail.

1 Concept

The purpose of this phase is to establish the scope, purpose, concept and management of the railway project. Furthermore, financial analyses and feasibility studies are undertaken.

2 System Definition and Application Conditions

The objective here is to establish a system mission profile as well as to prepare system descriptions. The identification of operation and maintenance strategies and operation and maintenance conditions are mainly conducted.

3 Risk Analysis

The goal of this phase is to undertake a project related risk analysis. On the basis of an identification of possible Hazards of the system, a consequence analysis is conducted to finally estimate the evolving risk.

4 System Requirements

In this phase, firstly a requirements analysis is undertaken. It follows a specification of the system overall requirements and environment as well as the definition of the system (and safety) demonstration and acceptance criteria. To establish a validation plan as well as management, quality and organisation requirements are the next steps.

5 Apportionment of System Requirements

In this phase the system requirements are apportioned. This is done by a specification of sub-systems and components requirements and the definition of sub-system and component acceptance criteria.

6 Design and Implementation

The goals of this phase are the performance of planning, design, development, design analysis and testing, design verification, implementation and validation.

7 Manufacturing

This phase is dominated by the performance of the production planning, the actual manufacturing and testing. Moreover, the preparation of relevant documentation and the establishment of training procedures are performed.

8 Installation

The targets of the installation phase are assembling and installation of the system.

9 System Validation (as part of Safety Acceptance and Commissioning)

During this phase the system is commissioned and tested. In addition training for staff is undertaken.

10 System Acceptance

The execution of the acceptance procedures, based on the acceptance criteria, is performed. Moreover, the termination of this phase leads to the entry into service.

11 Operation and Maintenance

The intended operation and maintenance are continuously performed in this phase. This performance is supported by ongoing training of staff.

12 Performance Monitoring

This phase, which is in parallel to phase 11, is dominated by the collection and analysis of statistical data of operation and maintenance.

13 Modification and Retrofit

This phase is in parallel to lifecycle phase 11. The implementation of modifications and changes are the main tasks.

14 Decommissioning and Disposal

The planning and execution of the decommissioning and disposal is performed during the last phase of the system lifecycle.

3.2.2 Hazard Log in the RAMS Lifecycle

The creation and usage of the Hazard Log is not restricted to one system lifecycle phase. This is pictured in the following figure (see Figure 2 - Hazard Log in the System Lifecycle). This figure shows that the Hazard Log is part of the overall system lifecycle. Figure 2 **stresses the substantial meaning** of the Hazard Log.

In the **first two phases** of the system lifecycle the check of previous Hazard Logs is one of the main objectives. EN 50126 recommends to “review previously achieved safety performance” [EN 50126] during the concept phase and to “evaluate past experience data for safety” [EN 50126] during the system definition phase. To **gather previous experience**, Hazard Logs of former projects can be consulted. Admittedly, it is rather difficult to adapt an old Hazard Log of an old project to a new project. This is mainly due to the fact that there are sometimes considerable differences and variations between old and new projects. It is problematic to compare Hazard Logs of projects of different countries with different railway signalling systems. But, general approaches and assumptions can be transferred in every case.

The next phase of the system lifecycle is the **Risk Analysis**. This is probably the main phase for the Hazard Log. EN 50126 explicitly states to set-up a Hazard Log as the basis for an on-going risk management. First of all, a structure for the Hazard Log has to be created. (Possibilities to derive a structure as well as examples for a Hazard Log can be found in clause 4). The contents of the Hazard Log are highly influenced by the manner of performance of the risk assessment. Since one mission of the Hazard Log is to **record possible Hazards**, it is obvious that the method of Hazard Identification influences the identified Hazards (see sub-clause 3.3). The next step in the Hazard Log is to **estimate the risk** of the identified Hazards. One example to estimate the risk is to use the Risk Matrix of EN 50126. (Further details can be found in sub-clause 3.4). Finally, Risk Reduction Measures for each Hazard have to be identified and justified.



1	Concept	Check previous Hazard Logs
2	System Definition	
3	Risk Analysis	Identify Hazards, Risk, Measures
4	System Requirements	Derive Requirements
5	Apportionment of Requirements	Support from Hazard Log to implement Safety Plan Close Hazards Update Hazard Log
6	Design and Implementation	
7	Manufacture	
8	Installation	Update Hazard Log
9	System Validation	
10	System Acceptance	
11	Operating and Maintenance	Update Hazard Log
12	Performance Monitoring	
13	Modification and Retrofit	
14	Decommissioning and Disposal	

Figure 2 - Hazard Log in the System Lifecycle

The next phase of the system lifecycle covers the derivation of **system requirements**. In the previous stage of risk assessment a need for risk reduction arises. This need for Risk Reduction Measures can be expressed in system requirements. In other words, the Hazard Log **supports the specification** for the system safety requirements as well as the definition for the safety related functional requirements by identifying measures for risk reduction.

The subsequent stages (lifecycle phase 5, 6, 7) includes the **design and manufacturing** of the actual system. Here, the Hazard Log is mainly used to support the **Safety Plan**, especially during the design and implementation and the manufacturing phase. The Safety Plan is: “the implementation details of how safety requirements of the project will be achieved” [EN 50129]. This is because Risk Reduction Measures, and the relevant responsibilities, for every Hazard are identified and therefore, give evidence of how safety requirements will be achieved. This is

done by covering (or closing) Hazards with Risk Reduction Measures. In the Hazard Log it will be proved that every Hazard is covered with justified and referenced Risk Reduction Measures. Additionally, the Hazard Log is used to record the **updates** regarding the Hazards and their Risk Reduction Measures, which arise during system review, analysis and testing. During phase 5 - the apportionment of system requirements - the Hazard Log is often used as a support for a Fault Tree Analysis to justify system safety requirements. This is plausible because Hazards as well as their Hazard Causes are recorded and documented in a Hazard Log.

In the following phases – **installation, system validation and system acceptance** – the use of the Hazard Log is dominated by **ongoing updating**. This includes adding Hazards which have been newly identified as well as the identification of new Risk Reduction Measures. EN 50126-2 recommends, closing “Hazards by system functions or procedural measures” [EN 50126-2] before system acceptance.

The phase **operation and maintenance**, as well as performance monitoring and modification and retrofit, demand continuously updating of the Hazard Log. This **updating** process is different to the previous stages. This is mainly because the updating not only includes adding newly found Hazards or Risk Reduction Measures, it can be seen as an **ongoing validation** of the Hazard Log and identified Hazards and Risk Reduction Measures. All Hazards, estimated risk and Risk Reduction Measures are proved against real operation and maintenance conditions. As a consequence, changes have to be made to the content of the Hazard Log. This updating during lifecycle phase 11, 12 and 13 is absolutely essential for further projects in order to validate Hazard Identification methods, risk assessment and Risk Reduction Measures.

For the last system lifecycle phase - the **decommissioning and disposal** – the Hazard Log is a support for a Hazard management during decommissioning and disposal. Additionally, **updates** regarding newly found Hazards or Risk Reduction Measures can be made.

So far the advantages of the Hazard Log to support an ongoing updating are emphasised. But, “any change to the architecture, for safety reasons or otherwise, becomes dramatically more difficult and expensive once designs are frozen and components are in manufacture” [CHI 03]. Therefore, a thorough performance of each of these system lifecycle phases has to be strived in order to **prevent later amendments and changes**. On the other hand, in practice, the chain of lifecycle phases is mostly not shaped like a V (cf. V-Model of EN 50126). It is rather an iterative recurred spiral, where the different steps of the lifecycle are repeated to fully achieve its goals. Still, [CHI 03] states that due to the fact that the Hazard Log is a dynamic document, it might become difficult to prove the quality and completeness of earlier work if a document has been continuously updated. Hence, a systematic and solid Hazard Log management should be aimed to cope with the complexity. Moreover, EN 50126-2 even recommends a responsible (e.g. a Hazard Log Manager) for the maintenance and upkeep of the Hazard Log. This complex task embraces at least the management of new Hazards arising during the various lifecycle phases, the continuous updating of the status of Hazards and Hazards transference or export to other systems or responsibilities.

To emphasise the role of the Hazard Log in the lifecycle as well as the overall safety approval process, Figure 3 – RAMS Documents in the System Lifecycle [SOL 04] is

shown³. Here, the main documents for a unified European approval process are pictured. This figure combines the **V-Model with the required RAMS documents** for the system approval (R-Reliability, A-Availability, M-Maintainability and S-Safety). It starts on the left hand side with Phase 1 – Definition. This conception and specification phase contains e.g. the Validation Plan as well the Safety Plan. Phase 2 – Implementation covers the design, development and integration of the aspired system. In this example e.g. Hazard and RAMS analyses have to be compiled. Finally, Phase 3 deals with the validation. Hence, for example, the Safety Case is issued. In conclusion this leads to the final certification and system approval. In the bottom box the log files are mentioned as files which are needed for certification and eventual approval. It can be seen that the Hazard Log is one of these log files and affects the whole lifecycle.

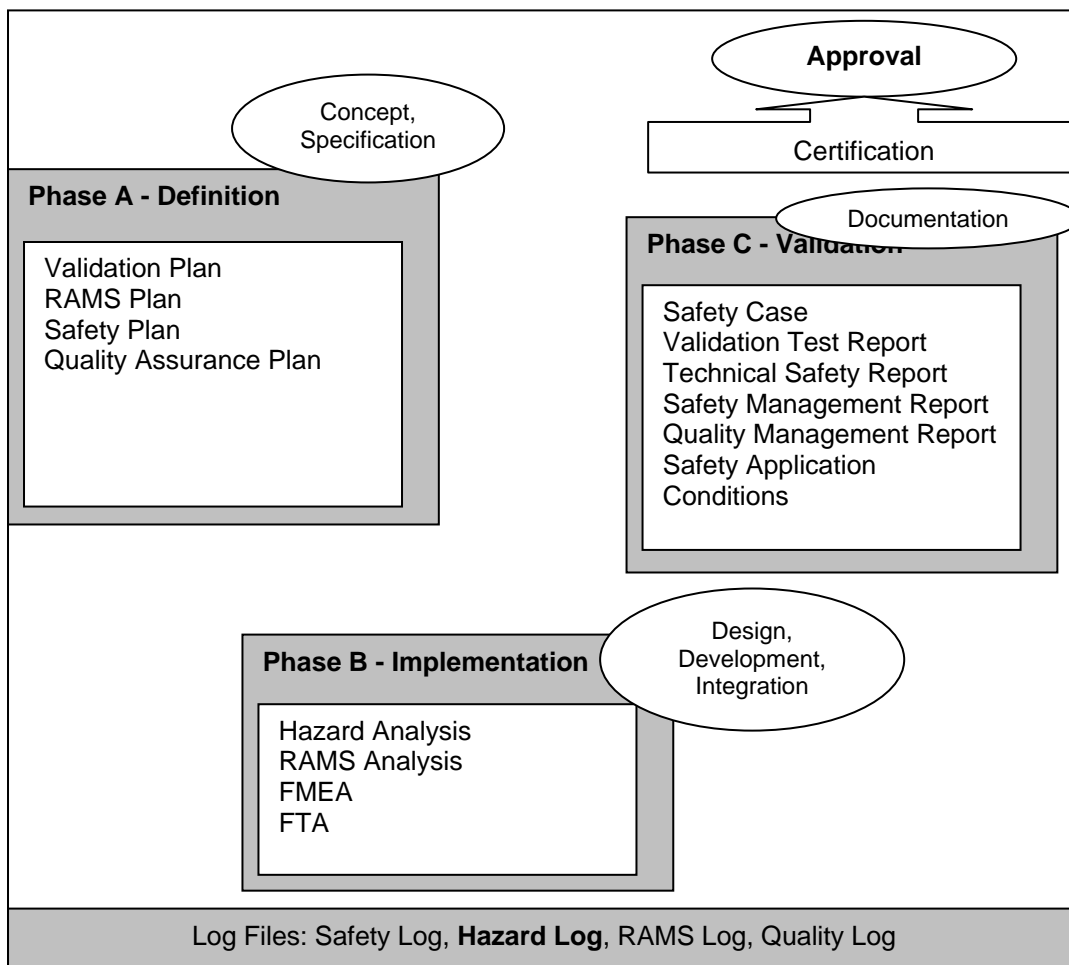


Figure 3 – RAMS Documents in the System Lifecycle [SOL 04]

To conclude; the fundamental meaning of the Hazard Log is proved by the illustration that the Hazard Log affects the overall lifecycle and the whole approval process.

³ Figure 3 has been adopted from [SOL 03]. This article deals with the applied RAMS management according to the CENELEC standards. It describes the successful approval of the axle counter AzLM by the manufacture Alcatel.

3.3 Hazard Identification as Input to the Hazard Log

For the creation of the Hazard Log the Hazard Identification plays the most important role. EN 50129 states: “Hazard identification involves systematic analysis of a product, process, system or an undertaking to determine those adverse conditions (hazards) which may arise throughout the life-cycle” [EN 50129]. The Hazard Identification is usually **done during the Risk Analysis in the Hazards Analysis**. To give a full overview, the process of the Risk Analysis is pictured in Figure 4 below.⁴ The Risk Analysis starts with a system definition and analysis of the operational context. This is the basis for the Hazard Identification. Hazards arising from this phase are the **first input to the Hazard Log**. Consequently, Hazard rates (i.e. the probability of occurrence) can be estimated. To identify possible Hazard consequences is the next step. This is followed by a determination of risk. Finally, a THR (Tolerable Hazard Rate) is derived.

Figure 4 shows that on the basis of system definition Hazards can be identified, which are ultimately input to the Hazard Log. Therefore, the way and modality of performing the **Hazard Identification directly affects the nature of the resulting Hazard Log** and the Risk Analysis. Consequently, different ways of performing a Hazard Identification are presented and briefly explained below.

⁴ Even though, Figure 4 is cited from [MOK 04], it is based on the principles described in EN 50126.

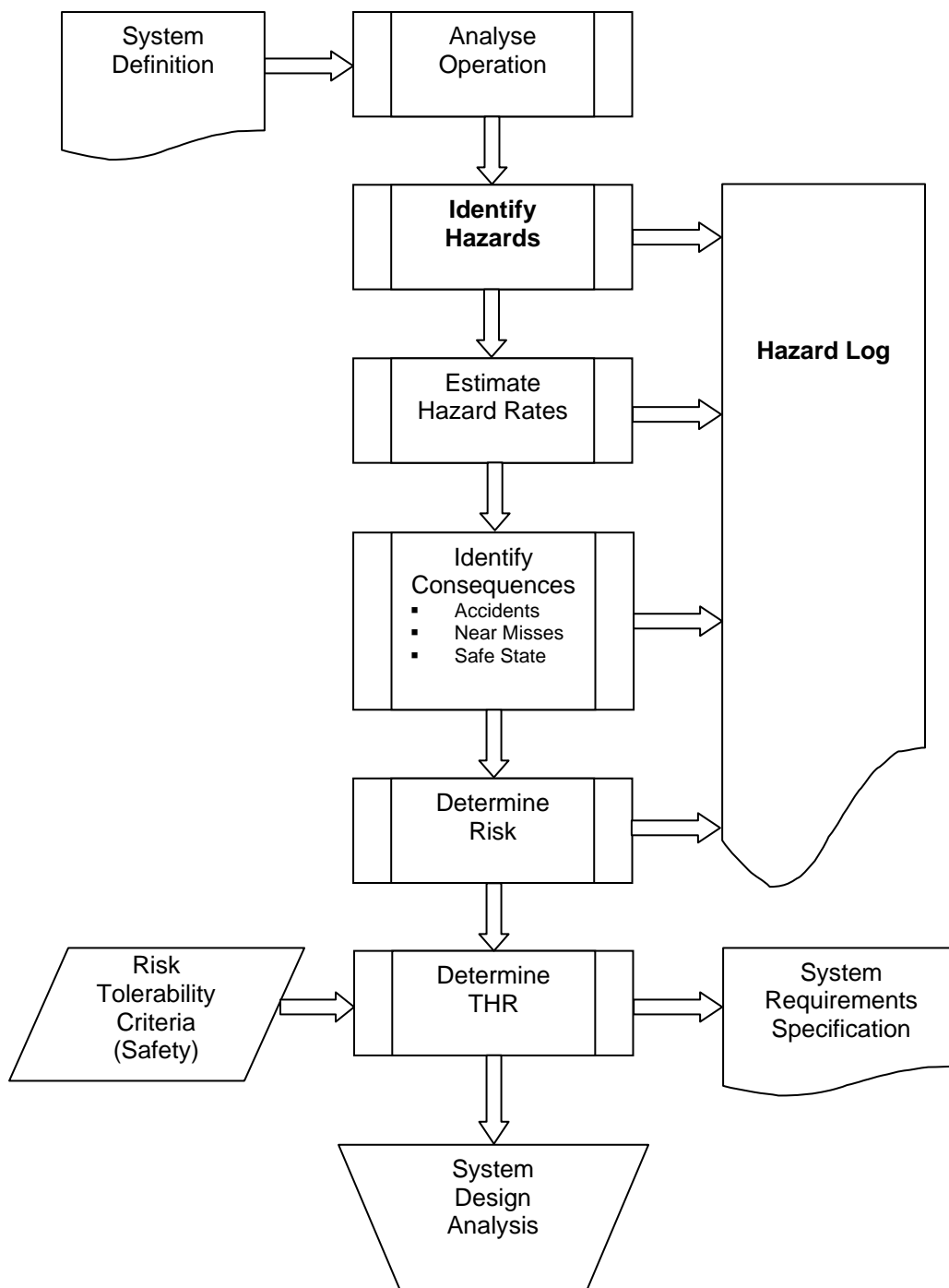


Figure 4 – Process Details of Risk Analysis [MOK 04]

Brainstorming

To conduct a brainstorming, **safety meetings** are held with railway professionals. These professionals are highly experienced and have appropriate knowledge of the analysed system. The bases for analysis are **checklists** resulting from past experience and previous analyses. The goal is to go through these checklists in order to identify all possible Hazards. For further details confer to [LEM 07]. One advantage

of a brainstorming is the straight forward and easy performance. On the other hand it is a rather unstructured approach and may lead to incompleteness of possible Hazards.

FMEA

FMEA stands for Failure Mode and Effects Analysis. It starts with clearly defined system architecture and functional descriptions – e.g. description of components and functions. These descriptions are the basis for a list of items which are analysed – e.g. a **list of sub-components**. Once the items for the analysis are found different kinds of **failure modes** are defined (e.g. component working, component partly working...). On the basis of the failure mode, causes and effects can be derived for each item. Advanced references are described in the Yellow Book – Engineering Safety Management [YB 07] and [FEN 07]. A benefit of this analysis is the easy performance. Additionally, if all items i.e. the list of sub-components and all failure modes are correctly described, subsequently, almost every failure cause and effect can be identified. But, on the other hand to develop an exhaustive list of failure modes is highly difficult.

Recommendation of EN 50129

The both methods described above (Brainstorming and FMEA) can be used for a Hazard Identification which is recommended in EN 50129. The European Standard recommends a **creative phase** e.g. realised by a Brainstorming or FMEA and an **empirical phase** performed by exploiting past experience e.g. checklists. EN 50129 does not explicitly mention it, but, the empirical phase can be extended by checking previous projects and systems as well as usage of results and findings of the analysis of incidents and accidents.

HAZOP

The abbreviation HAZOP stands for Hazard Operability Study. It is a systematic and creative examination of the system. The HAZOP approach starts with the construction of a Functional Block Diagram, which represents the components of the system. The following step is to use a full functional breakdown of the system and system documentation to continue the analysis. On this basis, possible Hazards can be derived by applying a list of **guide words** to the **actual intention of the system components**. This is conducted by a multidisciplinary team. The Yellow Book [YB 07] gives the following example: For an intended function of a system component the guide word can be NO or NOT which means: “No part of the intention is achieved but nothing else happens” [YB 07]. Further details can be found in [YB 07]. A merit of HAZOP is the structured approach which is in contrast to the rather complex application.

Interface Analysis

A different method for the derivation of Hazards is an analysis of interfaces between components of a system. Here, the basis for analysis is the **interaction between components e.g. technical or human**, which have a shared interface. The result of this approach is a matrix of interfaces between the different components of a system. Once a connection i.e. interaction between certain components is found, it gives information about possible Hazards. In the foreground of this approach are mainly physical interfaces between a pair of components. The approach provides a detailed

analysis but due to the fact that mainly physical interfaces are covered, incompleteness cannot be excluded. More details about an interface analysis are documented in [LEM 07].

Hierarchical definition of Hazards

A hierarchical definition and derivation of Hazards can be carried out in different ways. One way is to clearly define what a Hazard is. Given that a Hazard is “a condition that could lead to an accident” [EN 50126-2] - at system level (i.e. the system boundary) - it is possible to derive Hazards on the sub-system level. A different, but still hierarchical, approach is to identify different areas where Hazards might evolve. On the basis of these starting Hazards a **physical breakdown** can be conducted with the target to derive causes for these starting Hazards. For example, Hazards can be assumed during train movements or maintenance. In the next step causes for the train movement or maintenance Hazards are analysed. This approach is taken for the MODURBAN Preliminary Hazard Analysis (PHA). This approach provides a high degree of details at the price of a complex and extensive analysis.

Additional Methods

A **process-oriented method** for the identification of Hazards in railway signalling systems is described in [LEM 07]. The starting point of this analysis is an identification of the different processes in the system. Once these processes are found the system components can be allocated to these processes. Now, all relations and interactions between the processes can be derived. A Hazard must be assumed if a process is incorrectly executed.

Another approach for identification of Hazards is illustrated in [DRE 07]. This analysis depends on an explicit definition of system and its functions. For identification of Hazards a functional breakdown structure is used. This is done by **analysing possible malfunctions of the intended functions**. In other words, a Hazard is assumed if a function or a sub-function does not achieve its intended process.

Conclusion

It can be stated that no unique strategy i.e. Hazard Identification methods exists. But, a probable solution lies in a **combination of different kinds of methods**. Empirical as well creative approaches can be combined in order to yield a maximum complete list of Hazards. The key to a successful Hazard Identification is a **high-quality system definition** of system components and system functions, because on the foundation of thorough defined system architecture all sub-system and sub-function can be derived. Alternatively, in the particular case of Safety or Protection Systems, the system functions may themselves be seen as risk control measures and be analysed accordingly by associating the Hazards they cover against the functions. Hazards can be deduced from a discussion of malfunctions e.g. by failure modes or guide words. Additionally, empirical approaches for Hazard Identification can be combined with creative approaches.

The Hazard Identification is the foundation for a later Risk Analysis and final system approval and therefore, **affects the quality of the system**. In case, not every Hazard is identified and therefore, not covered by a measure for risk reduction, this reduces the value of the approval documents and the resulting system. Moreover, special attention has to be paid to the fact that a high quality of Hazards - rather than a large

quantity of Hazards - is important. [FEN 07] assures that this is proven by analyses of accidents.

3.4 Functions and Elements of a Hazard Log

3.4.1 Description of Functions in a Hazard Log

The main functions of the Hazard Log are illustrated in Figure 4 – Process Details of Risk Analysis [MOK 04]. These are: Identify Hazards, Estimate Hazard Rates, Identify Consequences and Determine Risk (and additionally, the investigation of measures for risk reduction). To fulfil its intended purpose a Hazard Log shall contain the following sections and functions:

- Introduction
- Journal
- Hazard Data
- Accident Data
- Risk Evaluation
- Risk Reduction Measures
- References
- Responsibilities
- Status Control
- Further Descriptions, Notes or Comments

For a later development of a generic Hazard Log the intended sections, functions and its alternatives are discussed in the following section.

Introduction

Since a Hazard Log is not only a database it also contains an introduction which describes the **purpose, aim and structure** of the Hazard Log. It shall be described which system or sub-system is analysed and therefore what the contents of the Hazard Log are. Furthermore, a reference to safety documentations e.g. the **Safety Plan** and the Hazard Log management process (e.g. rights for access, reading or modification etc.) shall be given.

Journal

A Journal of the Hazard Log **records all changes** and amendments to the Hazard Log which are made during usage. This is mainly due to traceability reason. In any case, causes and the responsible person for a certain change can be identified.

Hazard Data

The section for Hazard Data contains information and references for all identified Hazards. This includes a detailed description and references of the Hazard and its **causes**. It can be extended by specifying certain Hazard limitations and operational or environmental conditions. One entry to the Hazard data is about the



responsibility of the identified Hazard. Data about responsibility shall clearly define a party or person who takes care and action about the Hazard. It includes a possible transference or export of the Hazard, if it cannot be solved by the initial Hazard responsible.

Accident Data

Accident data characterise the **accident** which might evolve from a certain Hazard. The descriptions can be completed by an accident trigger to fully describe the possible accident.

Risk Evaluation

The risk evaluation is meant to **estimate the level of risk** which might evolve from an accident. According to EN 50126 a level of risk can be divided into four categories: a) negligible, b) tolerable, c) undesirable or d) intolerable. The level of risk indicates the **demand for action** on certain Hazards. For example, if the level of risk of a Hazard is “intolerable” there is a high demand for action regarding possible risk reduction. The risk evaluation can be conducted twice; first of all, before any implementation of Risk Reduction Measures and secondly after the implementation of Risk Reduction Measures. The second time is to check whether a certain safety implementation can lead to a lower level of risk or not.

An **alternative to the risk evaluation of EN 50126** is an approach which is used in the project of the Edinburgh Airport Railway Link [EARL]. The risk evaluation uses a risk matrix as well, but differs between three categories of risk only. To evaluate the risk, risk priority numbers are used e.g. a frequent likelihood of a Hazard has the value of 5 and if the severity of consequences is critical, the value is 4. The evolving risk can be derived from an addition or multiplication of both, likelihood and consequence (see Table 1). Figure 5 shows the emerging categories of risk: “Low Risk”, “Medium Risk” and “High Risk”. This approach is appealing because even with rough estimations of the likelihood and consequences a level of risk can be yield, because only three categories of risk are used. Furthermore, the description of risk does not contain information about the tolerability of the estimated risk. For a first estimation of the risk of a Hazard this might be fully sufficient.

Table 1 – Example of Risk Matrix according to [EARL]

Likelihood	Consequence					
		Minor (1)	Marginal (2)	Major (3)	Critical (4)	Catastrophic (5)
Frequent (5)		Amber	Red	Red	Red	Red
Probable (4)		Amber	Amber	Red	Red	Red
Occasional (3)		Green	Amber	Amber	Red	Red
Remote (2)		Green	Green	Amber	Amber	Red
Improbable (1)		Green	Green	Green	Amber	Red

Significance	Colour
Low Risk	Green
Medium Risk	Amber
High Risk	Red

Figure 5 – Example of Risk Categories according to [EARL]

Risk Reduction Measure

Finally, Risk Reduction Measures give evidence of which action is taken to reduce the risk which evolves from a Hazard. Examples for measures for risk reductions are: **design measures, testing, operational procedures or maintenance measures**. Here, the question about the **responsibility** arises again. It is of utter importance to clearly identify a party or a person who takes care for the realisation of the Risk Reduction Measure. Again, in case the initial owner of the Risk Reduction Measure cannot close the Hazard, a possible transference or export of the responsibility for the Risk Reduction Measure shall be considered.

References

To ensure a certain Risk Reduction Measure is designed and implemented, references have to be given in order to **prove its correctness**. It is fundamental to show where it is documented how the Risk Reduction Measures are realised.

Responsibility

As mentioned above, one of the major tasks of a Hazard Log is to **clarify who has the responsibility** for certain Hazards or Risk Reduction Measures. The responsibility mainly depends on the system which is about to be analysed and what party realises the actual system design. Due to the complex task to manage a Risk Analysis and a Hazard Log, it might be of advantage to break down the system into sub-systems and subsequently, into “sub-responsibilities”. A safety agent, only responsible for a section of Hazards or Risk Reduction Measures, might be able to conduct a more thorough and solid work on Hazards or Risk Reduction Measures (cf. [BRA 05]).

Status Control

The status control is a practical function to indicate what the status of a Hazard is. The status control can be applied to Hazards and to the Risk Reduction Measures. The status can switch between “**Open**” and “**Closed**”. This can be extended by terms of “Cancelled”, “Reviewed”, “Resolved” or “Exported”. The purpose is to show the progress of the Hazard Log and to indicate where open issues are. One example of how the values of the status control can be interpreted is shown in [PAS 03]. Table 2 describes the meaning of the status of the Hazards.

Table 2 – Status Control according to [PAS 03]

Values	Meaning
Open	States that the action to close the Hazard has not been formally agreed.
Cancelled	The item has been determined not to be a Hazard or is encompassed within another identified Hazard.
Resolved	The action to close the Hazard has been agreed, but has not been completed.
Transferred	The item has been recognised to be out of the scope of the present system and should be allocated to another Hazard Log.
Closed	The action to close the Hazard has been formally completed and accepted.

Further Descriptions

Further descriptions are needed for any types of **comments**. This is especially regarding possible insufficient information or problems to solve or close the Hazard (for instance, explanations whether to export the Hazard or not).

3.4.2 Description of Elements in a Hazard Log

The following table (see Table 3) summarises the functions which should be fulfilled by a Hazard Log. Furthermore, necessary elements for a later creation of a Hazard Log are collected.

Table 3 – Functions and Elements of a Hazard Log

General Function	Elements in Database
Introduction	Written document - no database
Journal	Date
	Entry number
	Person
	Description of change - Cause
	Referenced documents
Hazard Data	Reference number
	Name
	Description
	Responsibility
	Hazard Cause
Accident Data	Reference
	Description
	Accident Trigger
Risk Evaluation	Severity of consequences
	Likelihood of occurrence
	Risk
Risk Reduction Measure	Reference number
	Description
	Date
	Responsibility
Reference	Referencing document
Status Control	Status of Hazard
	Status of Risk Reduction Measure
Further Description	Notes and Comments

4 Approach for the Development of the Structure of a Hazard Log

Based on the principals for a Hazard Log, found in clause 3, this clause describes approaches for the development of an actual Hazard Log. First of all, a lifecycle for a Hazard Log is designed. This is followed by a discussion of different approaches for the development of a structure. Furthermore, examples of Hazard Logs of different industries are shown to support a later creation of a Hazard Log.

4.1 Lifecycle of a Hazard Log

The following figure concludes the gathered knowledge so far. It paves the way for the further analysis of a generic Hazard Log. In particular the creation of the actual structure is prepared.

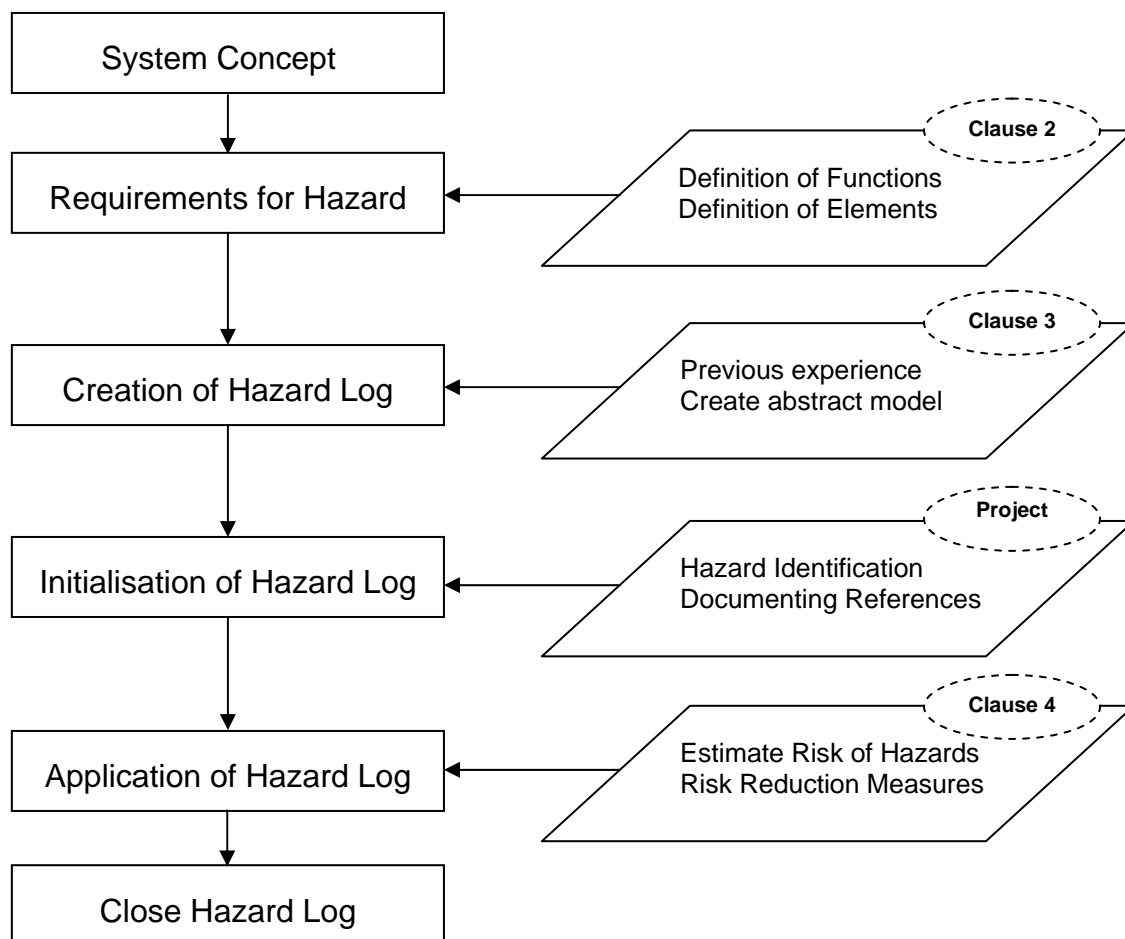


Figure 6 – Hazard Log Lifecycle

Figure 6 shows a suggestion for a lifecycle of a Hazard Log. It is meant to give a quick overview what the main steps for the creation and application of a Hazard Log are. It starts with a system concept where basic characteristics for the project and the resulting Hazard Log are determined. These characteristics e.g. size of the metro system or the available financial budget, directly affect the requirements for a Hazard Log. The following step, to define requirements covers the determination of the targeted functions and elements for the Hazard Log. Once requirements for a structure are found the actual creation process can be performed (clause 4.2). To initialise the Hazard Log, project-dependent data are used (e.g. from MODURBAN) and all identified Hazards are put into the Hazard Log. For a later application, documenting references have to be provided. Finally, the Risk Evaluation for the Hazards is carried out in order to allocate Risk Reduction Measures. After the termination of the project, or resolution of all Hazards, the Hazard Log can be closed.

4.2 Approach for the Development of a Structure

4.2.1 Theoretical Approaches for the Creation

In principal there is no formal way in order to create and design a structure for a Hazard Log. However, two approaches are chosen to demonstrate different procedures.

4.2.1.1 Intuitive Approach

The intuitive approach covers a **review of examples** of Hazard Logs. These examples of different projects give a first idea of how a future Hazard Log might look like. A collection of examples can be found in sub-clause 4.3. These **examples are analysed** and in combination with the strived requirements regarding functions and elements for a Hazard Log, a structure can be designed. This approach is chosen for the generic Hazard Log for the MODURBAN project.

4.2.1.2 Example of Abstract Model

A more structured way for creation of a Hazard Log is given in [HAM 04] – “*HazLog*: Tool support for hazard management” - and is briefly concluded below. This application arises from the Australian Department of Defence and “describes a prototype tool, called *HazLog*, that has been built on top of the DOORS tool in order to support the Def(Aust) 5679 hazard management process” [HAM 04]. The centre point of this approach for the development of a structure is an **association diagram** shown in Figure 7.

The squared boxes represent the objects and the solid lines represent relationships between these objects. The notation **1..1** means exactly 1, **1..*** means one or more and ***** means zero or more. For instance, each SSR has exactly one LOT but each LOT can have zero or more than one SSRs.

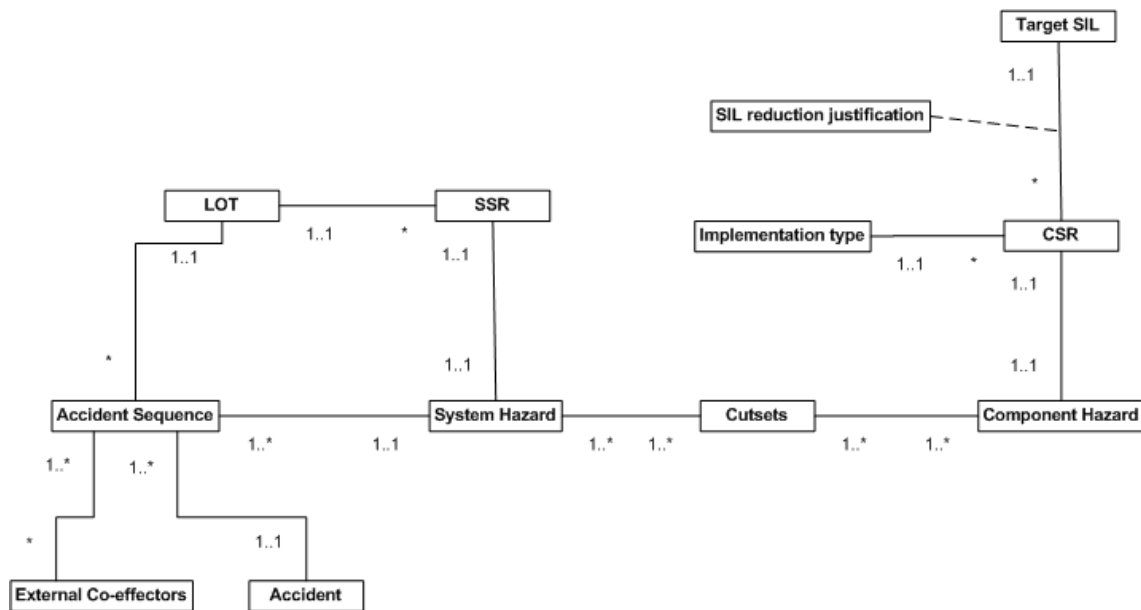


Figure 7 – Conceptual Model for a Hazard Log [HAM 04]

The main emphasis for this deliverable lays in the **demonstration of the approach** to describe a structure of a Hazard Log. Therefore, only the different elements of this application are explained, without considering the actual application the Hazard Log is build for.

Each of the objects, like SSR or “system hazard”, describe an element of the Hazard Log. The elements result from functional requirements for the Hazard Log. Each object is represented by certain features and characteristics. For example, each “system hazard” features an identification number, a title and a description. (This is not pictured in Figure 7.) This conceptual model is the foundation for the design of the Hazard Log with the software tool DOORS.

The “**system hazards**” represent the identified Hazards at system level. Exactly one **SSR** (System Safety Requirement) is assigned to each “system hazard”. The SSR is the exact negation of the “system hazard”, to ensure the “system hazard” does not occur. Furthermore, “each **accident** has an associated **accident sequence**, which is a chain of events, such as system-level hazards, together with events external to the system, which can lead to the accident” [HAM 04]. In combination of “accident sequence” and SSR, a **LOT** (level of trust) is determined. The level of trust “represents the desired level of confidence to be provided that the system meets the safety requirement.” [HAM 04] The “accident sequence” itself is described as a link between an “accident”, “system hazard” and “external co-effectors”. “**External co-effectors**” are external events e.g. like an accident trigger, expressed in terms of a probability. The “system hazard” is broken down into a set of “**component hazards**”. The combinations of “component hazards” which lead to a “system hazard” are represented by so called “**cutsets**”. Exactly one **CSR** (Components Safety Requirement) is assigned to a “component hazard”. The CSR is the exact negation of the “component hazard”. Each CSR has an associated **SIL** (Safety Integrity Level) and an “**implementation type**”. A SIL is assigned to the CSR by the system developer. In cases a possible SIL reduction has to be justified, this is indicated by “**SIL reduction justification**”.

In conclusion; the approach creates a structure for a Hazard Log in an **abstract model**; each element of the Hazard Log is represented by one **object**. The relationships between these objects are described with **lines** and a **mathematical notation**. Each element arises from a requirement which function the Hazard Log should fulfil. Further characteristics are assigned to each object.

In comparison with the intuitive approach – mentioned above – the approach for the development of an abstract model is highly complex. It has to be considered what the characteristics of the intended Hazard Log are. For a preliminary solution it might be **sufficient to conduct an intuitive approach** to create a Hazard Log. But, for more extensive projects the creation of an abstract model might be more appropriate. Especially for companies which are entrusted with the design of different Hazard Logs (e.g. software companies), it might be of advantage to use a formal method - e.g. an abstract model - for the creation of a basis for a Hazard Log. An abstract model supports the comparison of different Hazard Logs and therefore, assists a fast development of new Hazard Logs.

4.2.2 Tool Support for the Development

The major contributor to an actual realisation to design a Hazard Log is the software tool support. One of the most popular software tools is **Microsoft Excel**. The biggest benefit is the worldwide circulation and the easy access to this tool, because nearly every computer is equipped with Microsoft Excel, regardless whether professional or private user. Its drawbacks are the limited possibilities in terms of complexity. It is a simple tool, which is useable for everyone at the costs of the fact that not every complex requirement is presentable.

Another product is **Microsoft Access**. It is a database software tool. The advantage is that more complex solutions are possible as in comparison to Excel. But, the design of such databases is more challenging. In the railway supplier industry Microsoft Access is used to create and manage a Hazard Log.

Telelogic DOORS (abbreviation for: Dynamic Object-Oriented Requirement System) is a tool for requirements management for advanced systems. Its biggest advantage is probably the possibility to link information i.e. requirements and if needed, to trace these requirements back. Complex Hazard Logs can be modelled. Following [HAM 04] and [FAR 04], DOORS is a rather widespread and accepted system.

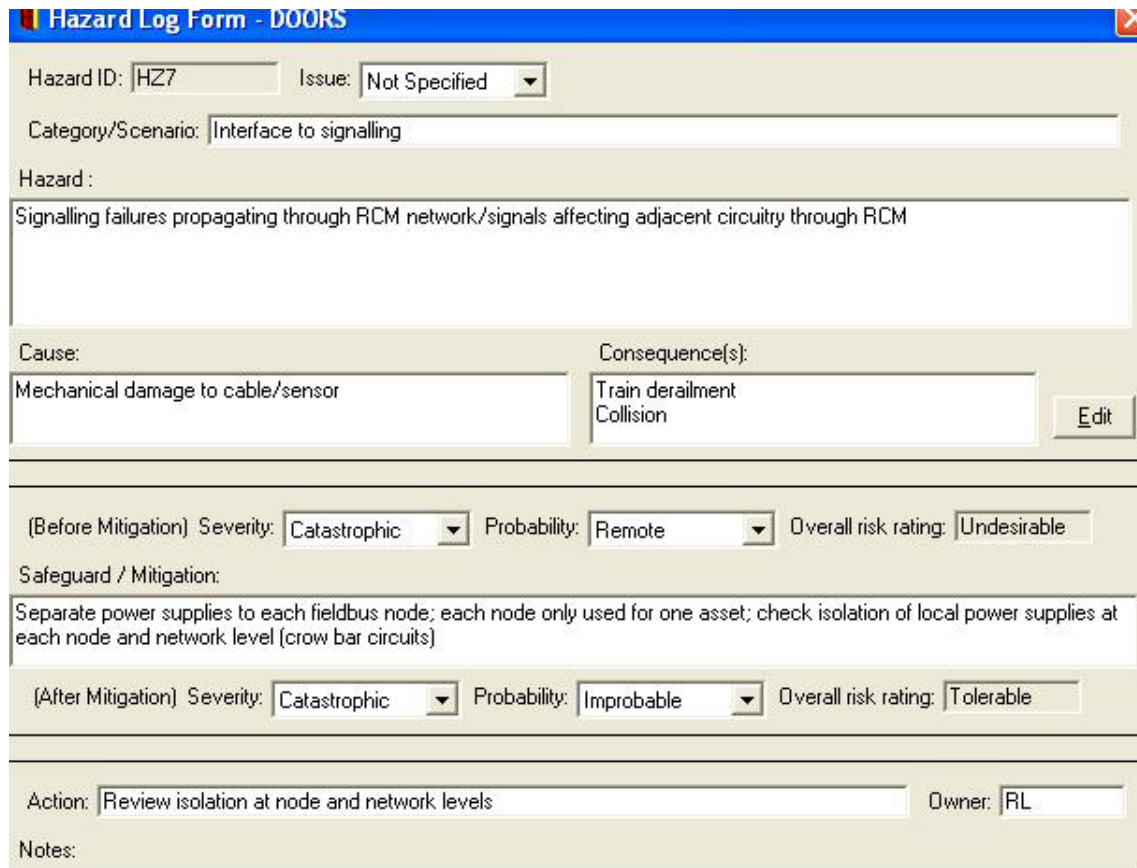
Rational Requisite Pro, a requirements management tool, **Lotus Notes**, a database tool and **Inteco Primavera**, a project management tool, are other examples for software support tools to design a Hazard Log. These systems are used in practice to create and manage Hazard Logs.

4.3 Examples of Hazard Logs

This sub-clause illustrates different approaches of the design of Hazard Logs, which are used in the industry. These examples introduce further approaches and applications. The examples provide the basis and support the creation of the generic Hazard Log.

4.3.1 Hazard Logs in the Railway Industry

The following example of a Hazard Log can be found in [FAR 04] – “Managing a System Safety Case in an Integrated Environment”. The article deals with the Railwise Remote Condition Monitoring (RCM) system and aims to demonstrate the elements of a Safety Case. It is developed in an academic - industry collaboration at the University of Birmingham (UK).



Hazard Log Form - DOORS

Hazard ID: Issue:

Category/Scenario:

Hazard :

Cause: Consequence(s):

(Before Mitigation) Severity: Probability: Overall risk rating:

Safeguard / Mitigation:

(After Mitigation) Severity: Probability: Overall risk rating:

Action: Owner:

Notes:

Figure 8 – Hazard Log – Railway [FAR 04]

Figure 8 shows a Hazard Log designed with the software tool DOORS. It contains a Hazard Identification (see top left corner), a not further specified issue and a Hazard category/scenario. Further properties of the Hazard are a description, the Hazard cause and consequence(s). After the description of the Hazard a first risk evaluation is carried out. This evaluation before mitigation is conducted by an estimation of severity of consequences and the Hazard probability. As a result an overall risk rating can be derived. This is followed by the consideration of Risk Reduction Measures, called safeguard/mitigation. After a possible mitigation of risk, a second risk evaluation is held. Finally, actions and an owner for these actions are recorded. Below further notes can be taken.

4.3.2 Hazard Log in Aviation

The example below is developed by the UK Civil Aviation Authority. In “Safety Management Systems for Commercial Air Transport Operations – A Guide to Implementation prepared by the Air Transport Operations - Safety Management Group” [CAA 02] an application of a Hazard Identification and Risk Assessment Log is described.⁵

Risk Ref:	Generic Risk	Risk Description	Current Measures to Reduce Risk	Risk Rating ¹			Further Actions to Reduce Risk	Responsibility
				L	S	No.		
M-5	Human Error	Non-compliance with a company maintenance procedure.	1. Minimum Competency requirements 2. Effective Safety Culture in company (maintenance department) 3. Effective Task Planning 4. Availability of procedures 5. Procedure reviews and simplification into task cards 6. QA requirements for certifying staff 7. Recurrent Training 8. Human Factors Training	5	4	20	1. Introduce Compliance Monitoring 2. Effective supervision including work compliance assessment 3. Competency assessments 4. Maintenance Policy to reinforce need for compliance	Quality Assurance Line Manager Maintenance Manager Maintenance Manager

Figure 9 – Hazard Log – Civil Aviation [CAA 02]

Chapter 3 of [CAA 02] covers “An Effective Organisation for Delivering Safety”. Among other tools a Hazard Log is recommended to achieve safety. This Hazard Log starts with a risk reference on the left hand side. This is followed by a risk description for the generic risk. This example deals with a human error which is described as the “Non-compliance with a company maintenance procedure” [CAA 02]. To cope with this, current measures to reduce risk are given; e.g. measure 1 demands “Minimum Competency requirements” [CAA 02]. To evaluate the measures for risk reduction regarding the generic risk – here: human error – a risk rating is used. A level of risk is computed by the product of L – likelihood and S – severity. For this purpose a priority number system is used. Likelihood has four levels; for example “probable” has number 4, whereas “extremely improbable” has number 1⁶. The same applies to severity; e.g. “catastrophic” has number 4 and a “minor” severity has number 1. Finally, further actions to reduce risk are given. For each of these further actions to reduce risk a clearly defined responsibility is appointed. For instance, the action number 3 – “Competency assessment” – is in responsibility of the maintenance manager.

⁵ This example of the Hazard Log from the aviation industry represents only one possible format of a Hazard Log. Since the aviation industry is an also complex business it is assumed that far more complex Hazard Logs are used as well.

⁶ In the example above, the likelihood has a level of 5 to rate the risk. This is in contrast to the explanation of [CAA 02].

4.3.3 Hazard Log in Military

One example of a Hazard Log in a military application originates from the Royal Australian Navy. This Navy Hazard Log is developed in 2003 with the software tool Lotus Notes of the software company Agileware. The approach is to find a way to identify and manage risk for personnel and equipment in the workplace i.e. ships or submarines. The targets of this Hazard Log are:

- “Encourage quick and accurate identification of the underlying hazard (i.e.: equipment or process that was the cause of the incident);
- Track the number of incidents/accidents that have occurred as a result of each hazard;
- Ensure hazards that affect other ships classes, areas or processes are highlighted to those affected; and
- Record the mitigation action to be applied” [ADE 07]



The screenshot shows a web application interface for the Navy Hazard Log. At the top, there are navigation tabs: "New Hazard", "New OHSIR", "Hazards", "OHSIRS", "Search", and "MHQ OHSIR Web". Below these are utility links: "Welcome Justin Freeman", "Add this page to My Favourites", "Print this Page", "User Preferences", "Help Topics", and "Log out". The main content area is titled "Navy Hazard Log: All Ship Hazards" and contains three sub-tabs: "Own Ship Hazards", "Own Class Hazards", and "All Hazards". A "View the Help for this page" link is also present. The main heading is "Hazards - All Hazards". Below this, it states "All Hazards are listed below." and displays a table with the following data:

Hazard Title ^	Ship Name	Mitigated HRI	Status	Date Created
Radiation Hazard from signals tower	HMAS ARUNTA	1	Proposed	07/03/2005
Fuel containers on deck must be secured using 2/8" cable during rough weather	HMAS CANBERRA	1	Proposed	07/03/2005

At the bottom of the page, it says "Powered by Agileware Pty Ltd Copyright © 2000-2004".

Figure 10 – Hazard Log - Australian Navy 1 [ADE 07]

In this example (confer to Figure 10) different types of Hazards are defined. It is differed between “Own Ship Hazards”, “Own Class Hazards” and “All Hazards”. The example above describes the Hazard “Radiation Hazard from signal tower”, which is assigned to “All Hazards”. Apparently, each Hazard is assign to a certain ship; in this case, this Hazard occurs on the ship HMAS Arunta. In addition a HRI – Hazard Risk Index - is given regarding mitigation. This example indicates that the evolving risk is intolerable (due to the indicated value of 1). The next point is the status of this Hazard. In this case, the Hazard has the status: “Proposed”. Finally, a date of creation is given.

Another extract from the Navy Hazard Log is an index card about a certain Hazard. This example (see Figure 11) shows the Hazard: “Fuel containers on deck must be secured using 2/8” cable during rough weather”. The Hazard Risk Index is 1 and therefore, the risk is intolerable. Below a Hazard priority is given. Here, the priority “Routine” is chosen. An issue serial and the status – here: “Proposed” – is indicated as well. Moreover, four additional Hazard specifications are pictured. These are: a Hazard description, mitigation/treatment, tracking details and administration. The Hazard description is shown in more detail. For each Hazard, classes and the affected establishments are given. A further Hazard description regards the unmitigated probability and the unmitigated severity for personnel, equipment and missions. For instance; the unmitigated probability for the equipment, regarding this Hazard, is “frequent” and the unmitigated severity “catastrophic”.

HAZARD

Hazard Overview

Hazard Risk Index: ■ - 1 - **Intolerable**

Priority: Routine

Title: Fuel containers on deck must be secured using 2/8" cable during rough weather

Issue Serial: HMAS CANBERRA/F02/FFG/000001

Status: Proposed

Hazard Description
Mitigation/Treatment
Tracking Details
Administration

Title:	Fuel containers on deck must be secured using 2/8" cable during rough weather		
Classes/Establishments Affected:	AO, AOR, AUSCDT, FCPB, FFH, MSA		
Hazard Description:	TEST		
	Personnel	Equipment	Mission
Unmitigated Probability: ?	Frequent	Frequent	Frequent
Unmitigated Severity: ?	Catastrophic	Catastrophic	Catastrophic

Figure 11 – Hazard Log – Australian Navy 2 [ADE 07]

The big difference in comparison to other Hazard Logs is that the Navy Hazard Log is not developed primarily for the design of new systems. The emphasis lies mainly in ongoing updating of the Log during operation and maintenance. Furthermore, a continuous validation of the performed risk mitigations is conducted to identify open issues regarding unsolved Hazard.

4.3.4 Conclusion of the Illustration of Examples of Hazard Logs

The formats and the surfaces of the three examples of **Hazard Logs are very different**. A rather simple Hazard Log is illustrated, which originates from the aviation industry. This example is on a very generic level. The aviation Hazard Log is in contrast to the complex Hazard Log of the Royal Navy of Australia. Nevertheless, all Hazard Logs have certain functions and elements in common. These are: Hazard description, risk evaluation, measures for risk reduction and responsibilities.

Considering the differences of the examples of Hazard Logs above and in addition to the fact that **certain functions are similar**; it can be assumed that these functions and elements are essential for the structure and application of a Hazard Log.

5 The Preliminary Hazard Log for MODURBAN

This clause describes the development and the actual application of the Hazard Log for MODURBAN. The main objective is to delineate the structure and application to give a sound understanding of how the Hazard Log is used.

5.1 Approach for the Development of the Hazard Log

5.1.1 The Idea to the Development of the Structure

To develop a structure for the Hazard Log for MODURBAN, an **intuitive approach** is chosen. By analysing examples of Hazard Logs and a thorough reading of the European Standards and available literature a generic structure is generated. It is strived to keep the structure and the realisation of the Hazard Log **as simple as possible** to support an easy usage. One major requirement for the development is that a **generic structure** is aimed, which is independent of an actual system architecture. More precisely, the Hazard Log shall be a generic starting solution with a generic structure and generic Hazards. On the basis of this generic Hazard Log, suggestions for an application on top of the MODURBAN system are made. Thinking in long terms, the Hazard Log shall be applicable to every urban guided transportation project.

5.1.2 The Software Tool

To realise a structure for the Hazard Log the software tool **Microsoft Excel** is selected. This is mainly due to the point that the software is widespread around Europe. It has been assumed that in European research and development projects, like MODURBAN, it is pertinent to use the **most accessible and widespread** software. In other words, no extra software has to be obtained, because all MODURBAN partners are in possession of Microsoft Excel. The drawback that Excel does not support highly complex solutions is acceptable, because only a preliminary Hazard Log is about to be created.

5.1.3 Initialisation of the Hazard Log

As a first input two sources are given. Firstly, a Hazard Identification is performed. This is done in form of a **Preliminary Hazard Analysis** (PHA), arranged during an earlier stage of the MODURBAN project (see [D86]). The MODURBAN PHA is structured in form of a Fault Tree. It contains eight starting point (or system) Hazards (see Figure 12 – PHA for MODURBAN Excerpt A). Examples of the system Hazards are: “Train Movement Hazards” or “Emergency and Evacuation Hazards”. These Hazards are broken down to analyse the causes of these Hazards (see Figure 13 – PHA for MODURBAN Excerpt B) at generic levels (independent of a concrete implementation of the ATC). These Hazard Causes are the main input for the Hazard

Log. For a later **analysis only basic events** of these Hazard Causes are considered. It is assumed that upper level Hazards are generated by basic events. These upper level Hazards, in other words Hazards which have Sub-Hazards beneath them, are generated by these Sub-Hazards, Consequently, only basic events, i.e. Hazards without Sub-Hazards, are analysed.

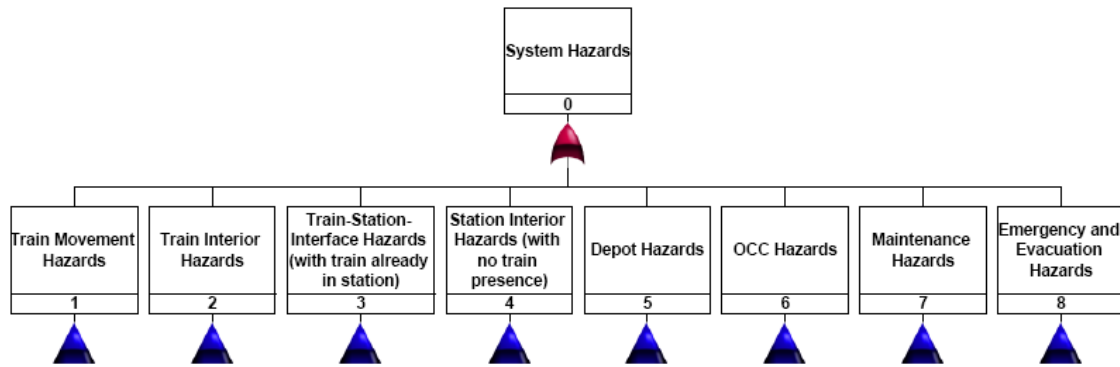


Figure 12 – PHA for MODURBAN Excerpt A

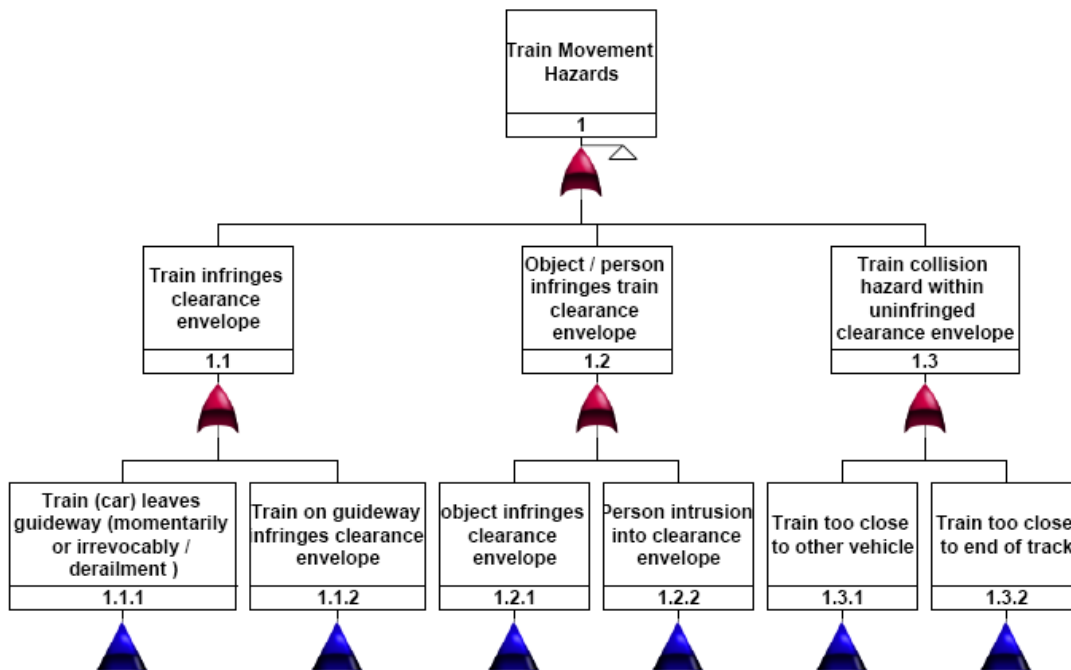


Figure 13 – PHA for MODURBAN Excerpt B

Secondly, the **functional prescription of the overall MODURBAN system** is considered. This embraces system functions which can act as safety barriers i.e. Risk Reduction Measures. In particular the following MODURBAN documents are considered:

- D77 – Train protection MODURBAN functional specification
- D78 – Non train protection MODURBAN functional specification
- D81 – MODURBAN prescription: overall architecture and allocation of vital functions.

The functions of D77 and D78 address mainly ATC functions. This is in contrast to the generic Hazards of the MODURBAN PHA for a complete guided rail system.

5.2 Documentation of the Hazard Log

5.2.1 Approach to the Application

On the basis of the identified Hazards and information about the MODURBAN functions and architecture, the task is to check whether a Hazard is covered by the MODURBAN system design or not. The final questions are:

- *Is there a MODURBAN function or architectural design which can act as a measure for risk reduction to cover a Hazard?*
- *If not, what assumptions can be taken for a Risk Reduction Measure to cover the Hazard?*

The approach for an application of the Hazard Log is described in Table 4 – Structure of Hazard Log for MODURBAN and Figure 14 – Hazard Log Action Procedure and is explained in detail below.

5.2.2 Structure for the Hazard Log

The following structure is designed for the Hazard Log for MODURBAN (see Table 4 – Structure of Hazard Log for MODURBAN). On the left hand side the major categories for the Hazard Log can be found. The categories represent the strived functions of the Hazard Log. Each of these major categories is subsequently divided into further sub-categories. For example, the major category Hazard description contains 10 sub-categories, from numbering until type of accident. The sum of all sub-categories represents the structure of the Hazard Log. The Hazard Log for MODURBAN can be found in the appendices.



Table 4 – Structure of Hazard Log for MODURBAN

Hazard Description	Numbering
	Name of Hazard
	Initial Risk Owner
	MODURBAN Relevance
	Input by
	Reference Source
	Remarks
	Date of Change
	Hazard Cause
	Type of Accident
Risk Evaluation – Before (of initial system design – without risk reduction)	Severity
	Likelihood
	Risk
Risk Reduction Measure	Reference
	Measure / Function
	Description
	Responsibility
	Grade of Automation
Risk Evaluation – After (after consideration of risk reduction)	Severity
	Likelihood
	Risk
Closure	Documenting Reference
	Date
Status	Hazard
	Measure
Notes and Comments	
Journal (History of Changes)	Number
	Date of Change
	Hazard Numbering
	Hazard Name
	Initial Aspect of Change
	Result of Change
	Reason for Change
	Further Descriptions
Responsibility	
Glossary	Abbreviation
	Explanation

The usage of the Hazard Log starts with the input of the identified Hazards of the MODURBAN PHA (cf. D86). The Fault Tree structure of the PHA is adopted in the Excel application. First of all, for each starting point Hazard of the PHA a single worksheet in the Excel application is used. The resulting structure is:

- Worksheet 1 – Train Movement Hazards
- Worksheet 2 – Train Interior Hazards
- Worksheet 3 – Train-Station-Interface Hazards (with train already in station)
- Worksheet 4 – Station Interior Hazards (with no train presence)
- Worksheet 5 – Depot Hazards
- Worksheet 6 – OCC Hazards
- Worksheet 7 – Maintenance Hazards
- Worksheet 8 – Evacuation and Emergency Hazards

Additionally, two extra worksheets are included:

- Worksheet 9 – Journal
- Worksheet 10 – Glossary

Secondly, the structure of the PHA Fault Tree is imitated in the Excel application to display the structure of this Fault Tree. The numbering of the Hazards in the Hazard Log is directly adopted from the Fault Tree.

5.2.3 The Development of the Hazard Log

The following section describes the actual application of the Hazard Log for MODURBAN; this is illustrated in Figure 14 – Hazard Log Action Procedure. This figure describes the procedure which is applied to develop the Hazard Log against the background of the MODURBAN project. In contrast to the approach to create a generic structure for the Hazard Log, the application - pictured in Figure 14 - is restricted to the MODURBAN application only.

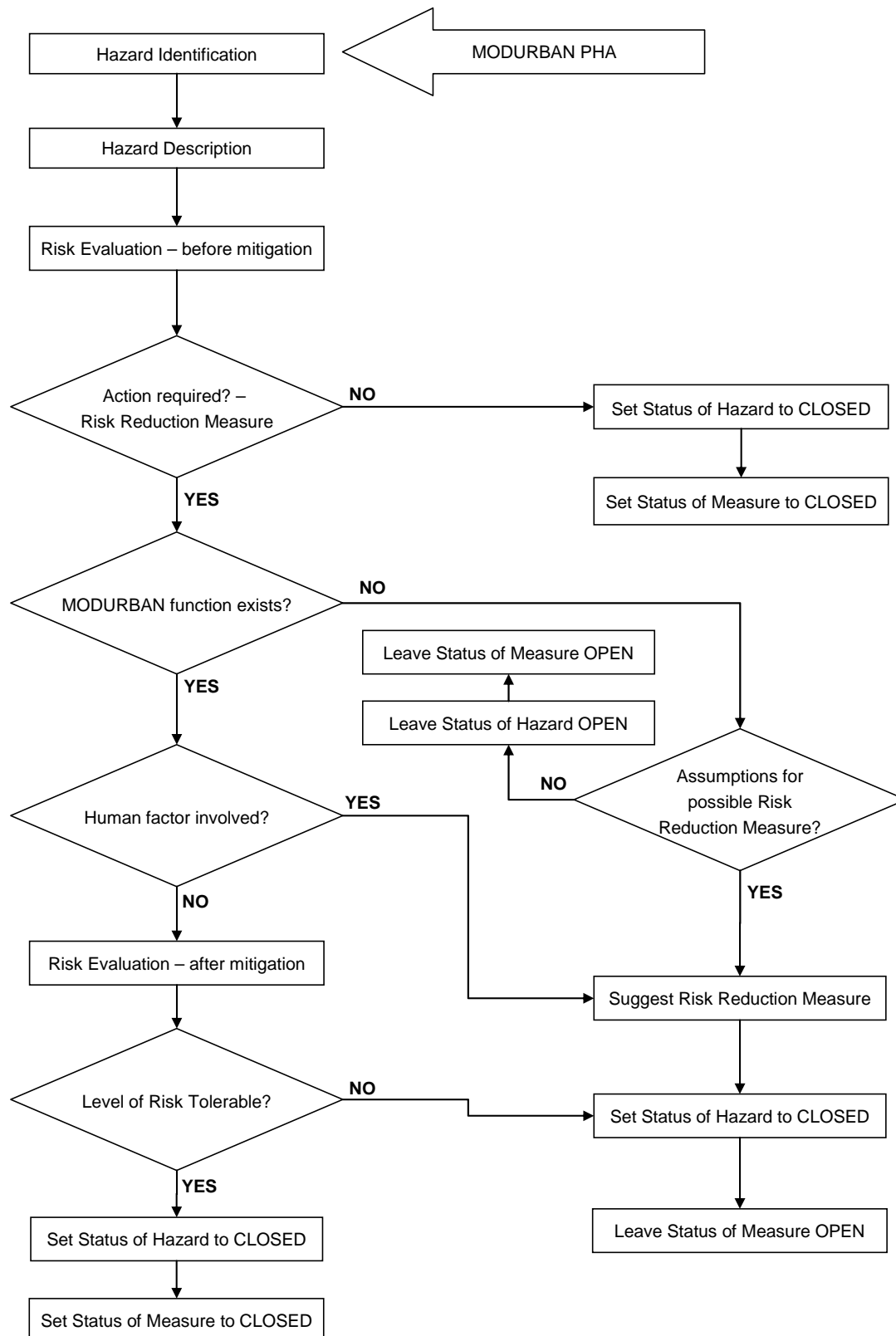


Figure 14 – Hazard Log Action Procedure

5.2.3.1 Hazard Description

On the basis of the identified Hazards, arising from the MODURBAN PHA, as shown in Figure 14 (arrow on the right hand side), the Hazard can be described. This Hazard description covers firstly the identification of the **initial risk owner**. Following the recommendation of the European Standards, regarding railway applications, the operator conducts the Risk Analysis and, therefore, the Hazard Identification. For that reason, the operator of every Hazard is the initial risk owner. For the first approach to develop a generic Hazard Log the operator, as the initial risk owner, is the default setting. In later applications it is possible to further specify the initial risk owner.

The second aspect of the Hazard description is about the **MODURBAN relevance**. The MODURBAN relevance is subdivided into three categories: These are: Yes – Hazard is MODURBAN relevant, No – Hazard is not MODURBAN relevant and ULH – Hazard is an upper level hazard. The decision whether a Hazard is MODURBAN relevant or not is made on the basis of the MODURBAN deliverables D77, D78 and D81. This distinction is made for two reasons. Firstly, to identify those Hazards, which shall be analysed, because only basic events are analysed (compare sub-clause 5.1.3). Hazards which are marked with ULH are not analysed. Secondly, the description of Yes or No gives information whether the Hazard is of relevance for the MODURBAN project and a possible later implementation of MODURBAN functions. But, due to the fact that the decisions, whether a Hazard is MODURBAN relevant or not, are only assumptions, every Hazard, regardless if Yes or No, is analysed. In conclusion; Hazards which are marked with Yes or No are analysed and Hazards which are marked with ULH are not analysed. In future projects the MODURBAN relevance may not be mandatory in which case it can be replaced or renamed. For the application for MODURBAN, this column is added because of the PHA, to identify basic event and to identify MODURBAN relevant Hazards.

Further descriptions of the Hazard cover the **input** and the **reference source**. In this application of the Hazard Log, all Hazards are an input by MODURBAN. This is self-evident. But, for a later application in future projects it might be necessary to distinct which Hazards arise from MODURBAN and which Hazards are newly added to the original Hazard Log. Therefore, a future user of the Hazard Log can consider the one, who added a new Hazard. Basically, the same applies to the reference source. For this application of the Hazard Log for MODURBAN it is self-evident that the Hazards arise from the MODURBAN project, i.e. the MODURBAN Preliminary Hazard Analysis. But for future projects, where this Hazard Log might be used as a first input, it seems necessary to provide possibilities to differ between the original MODURBAN Hazards and the newly added ones, which are probably project-dependent.

Another aspect of the Hazard description is about further **remarks**. This field is mainly used to refer to other Hazards in the Hazard Log. These are those Hazards, which are similar and therefore, the same analysis is made and a second similar analysis is not necessary. For instance, for the Hazard “object / person infringes train clearance envelope” (numbering 2.1.1.3.1) it says in the field remarks: See Sub-tree 1.2. Under 1.2 the same analysis for the Hazard is already made. Furthermore, the

field for remarks is used to show if new Hazard are added to the original version of the PHA. Additionally, the column can be used for further descriptions of the Hazard.

For future applications it might be necessary to change Hazards of the initial MODURBAN Hazard Log. Therefore, a domain **date of change** is provided. This aspect is not used for this MODURBAN Hazard Log. Dates are not allocated because a generic Hazard description is aimed and in general this application is the first input to the Hazard Log, and therefore nothing is changed.

One of the two major aspects to describe the Hazard is the **Hazard Cause**. The Hazard Cause indicates what the causes for a possible occurrence of the Hazard are. In this application of the Hazard Log for MODURBAN, this aspect is used in the following way: For each Hazard all conceivable Hazard Causes are identified. In case, more than one Hazard Cause is investigated; subsequently, each single Hazard Cause is analysed individually. This means that for a Hazard with e.g. three Hazard Causes, three analyses regarding risk and possible Risk Reduction Measures are made. In other words, for each investigated Hazard Cause, Risk Reduction Measures have to be identified. Information about the status - in terms of "open" or "closed" - of this Hazard Cause can be given. The separation of the Hazard Causes, with the consequence to analyse them individually, is done to increase the degree of detail in order to describe the Hazard in the most appropriate way. The individual analysis of the Hazard Causes, regarding risk and possible Risk Reduction Measures, is necessary due to the fact that in most cases, for every Hazard Cause different Risk Reduction Measures are needed.

The second major aspect of the Hazard description is about the **type of accident**. To each Hazard or Hazard Cause an individual type of accident is allocated. For example the accident can be described with: derailment, collision or electrocution or burns on passenger. The type of accident is later on used to evaluate the risk of the Hazard or Hazard Cause. To support the identification of the types of accident a list with possible accidents is developed. The following list is used for the identification of the types of accidents for this application:

- Asphyxia
- Burns
- Collision
- Contamination
- Derailment
- Drowning
- Electrocution
- Fall of person
- Fire
- Injury of person
- Objects striking person
- Passenger hit by train
- Suffocation
- Trapping of person



5.2.3.2 Risk Evaluation – Before

The risk evaluation is divided into two parts. The first risk evaluation is held before and the second after the consideration of Risk Reduction Measures. This sub-clause covers the basic approach to the risk evaluation and, in more detail, the risk evaluation before the consideration of Risk Reduction Measures.

The basis of the risk evaluation, which is chosen for this application for MODURBAN, is the **risk matrix**: an example - issued in EN 50126 - is given in Table 5. To evaluate a level of risk a user can choose from four levels of Hazard consequences to describe the **severity** and from five levels to describe the **likelihood** i.e. the frequency of occurrence of a Hazard. The combination of likelihood and severity gives a risk level, which indicates whether a Hazard is e.g. intolerable or tolerable.

In order to be compliant with European standards such as EN 50126 it is recommended to use the risk matrix shown in Table 5. Additionally, this approach for a risk evaluation provides a straightforward and easy use. (Notwithstanding, sub-clause 3.4.1 describes different approaches of a Hazard Log and a risk evaluation.)

Table 5 – Risk Matrix according to EN 50126

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			

To identify the level of risk the following descriptions for the terms of severity and likelihood are used (see Table 6 and Table 7). These descriptions are in accordance with EN 50126.

Table 6 – Frequency of Occurrence of Hazardous Events according to EN 50126



Category	Description
Frequent	Likely to occur frequently. The Hazard will be continually experienced.
Probable	Will occur several times. The Hazard can be expected to occur often.
Occasional	Likely to occur several times. The Hazard can be expected to occur several times.
Remote	Likely to occur sometimes in the system lifecycle. The Hazard can reasonably expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the Hazard may exceptional occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

Table 7 – Hazard Severity Level according to EN 50126

Severity Level	Consequences to person and environment	Consequences to service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment.	
Critical	Single fatality and/or severe injury and/or significant damage to the environment.	Loss of major system
Marginal	Minor injury and/or significant threat to the environment.	Severe system(s) damage
Insignificant	Possible minor injury.	Minor system damage.

The following table shows the different risk categories. These categories are used to identify the action which should result from a certain risk category (derived from Table 5). In other words, the determined risk category gives indications how big the need for Risk Reduction Measures is.

Table 8 – Qualitative Risk Categories according to EN 50126

Risk Category	Risk Reduction / Control
Intolerable	Shall be eliminated.
Undesirable	Shall only be accepted when risk reduction is impracticable and with agreement of the Railway Authority.
Tolerable	Acceptable with adequate control and agreement of the Railway Authority.
Negligible	Acceptable without any agreement.

For the actual application of the Hazard Log a first risk evaluation is done before any consideration of possible measures for risk reduction. This means that for every Hazard or Hazard Cause the terms of severity and likelihood are estimated and a level of risk is determined, which indicates the need for Risk Reduction Measures. The estimation of the terms severity and likelihood is based on assumptions and general system knowledge.

5.2.3.3 Risk Reduction Measure

On the basis of the Hazard description and an according level of risk it can be determined whether there is **need for action**, in terms of Risk Reduction Measures, for the analysed Hazard (see Figure 14). This means, to identify or indicate to a requirement which covers a Hazard. In case the level of risk is intolerable or undesirable immediate action is required. In case the level of risk is tolerable or negligible no further action is needed. The meaning of “Action is required” (cf. Figure 14) is; for a Hazard with an intolerable or undesirable level of risk a measure for risk reduction has to be identified. This shall be done in order to minimise the risk - evolving from the Hazard - to an acceptable level of risk.

For the development of the Hazard Log the level of risk has the following consequences. If the level of risk for a certain Hazard or Hazard Cause is tolerable or negligible the Hazard can be assumed to be closed. This means, no further analysis or investigation for this Hazard has to be performed. Regarding the **status of the Hazard**, it can be set to “closed”. Regarding the **status of the Measures** it can be set to “closed” as well (for further information about the use of the status see sub-clause 5.2.3.6). Note, the status of the Measure can only be closed when the implementation of the solution is proved.

In case, action for risk reduction is required it has to be investigated whether there are **MODURBAN functions**, which could act as a Risk Reduction Measure for the Hazard. This question can be answered by an examination of the appropriate MODURBAN deliverables regarding which of these functions is suitable for the analysed Hazard. These MODURBAN deliverables are D77, D78 and D81. An example is Hazard 3.1.1 – “Incorrect Train Alignment”. This Hazard is a Train – Station – Interface Hazard (with train already in station). For this Hazard a MODURBAN function is determined which acts as a Risk Reduction Measure. This function is from the MODURBAN deliverable D77 and can be found in sub-clause 3.2.2. Hence, the Hazard of an “Incorrect Train Alignment” can be reduced by the function “Determine Train Location”. This function determines the location of MODURBAN trains. Once the MODURBAN functions are identified further Risk Reduction Measures can be investigated. This can be done by assuming possible measures, which could act as an additional risk reduction. To continue the example of Hazard 3.1.1, one assumption for a further Risk Reduction Measure is; the driver can be supported with signs to stop at the right place.

If no MODURBAN function for a Hazard can be determined **assumptions for possible Risk Reduction Measures** have to be taken. These assumptions comprise suggestions for actions, rules or procedures which can act as a Risk Reduction Measure. If it is possible to assume and suggest measures for a possible risk reduction the status of the analysed Hazard can be set to “closed”. In case, no assumption or suggestion for a Risk Reduction Measure can be determined the status of the Hazard can be left “open”. The same applies to the status of the Measure, the status has to be left “open”. These assumptions for Risk Reduction Measures provide a basis for a later work on the Hazard Log. The assumptions shall support a continuous development of the Hazard Log for the MODURBAN application in cases where open issues emerging.

A full description of the Risk Reduction Measure covers additional aspects. First of all, if a MODURBAN function is identified, an unambiguous **reference** has to be given. This reference has three parts for the MODURBAN functions: a) the number of the MODURBAN work package e.g. WP 21, b) the title of the MODURBAN deliverable e.g. D77 and c) the sub-clause of the MODURBAN deliverable e.g. 3.1.7. Finally, it looks like this: WP21 D77 3.1.7. For assumptions regarding Risk Reduction Measures, i.e. no MODURBAN functions, no reference is stated. For a future application of the Hazard Log with project-dependent functions the reference can be given according to the individual project. Secondly, every function of MODURBAN is described with the actual title of this **function and the original description** of the function. This description of the MODURBAN function is similar to the one which can be found in the actual MODURBAN deliverable e.g. D77 or D78. It has been seen appropriate to add the description to the MODURBAN function, because the title of this MODURBAN function is often rather short and this might lead to misunderstandings. Therefore, especially for a good reading and understanding of the Hazard Log these descriptions of the MODURBAN functions are given. Thirdly, there is room for **further descriptions** regarding the Risk Reduction Measure. This can be used to explain the Risk Reduction Measure in more detail, regardless whether this is a MODURBAN function or an assumption. One of the major problems regarding the Risk Reduction Measure is the **responsibility**. It is the question about, who is responsible for the realisation and implementation of the Risk Reduction Measure. In case, a MODURBAN function is identified, it is the system supplier who is in charge of a realisation for the Risk Reduction Measure. In case, an assumption regarding a Risk Reduction Measure is taken, a responsibility is estimated as well. For example, the operator or the vehicle supplier has to take care about a Risk Reduction Measure. Finally, for all MODURBAN functions the **Grade of Automation (GOA)** is stated. The MODURBAN deliverable D77 defines the Grade of Automation in the following way:

- 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

The assignment of the GOA is done in order to give an understanding of the type of implementation of the MODURBAN functions. The GOA shows that a differently implemented Grade of Automation affects the way a Hazard is covered by a Risk Reduction Measure. In case, a particular MODURBAN function is mandatory for e.g. GOA 4 only, it would only cover the analysed Hazard for this implementation type (e.g. GOA 4). For GOA 1 – 3, the particular MODURBAN function contributes only in an obligatory way to a Risk Reduction Measure.

5.2.3.4 Risk Evaluation – After

After the determination of Risk Reduction Measures this risk evaluation shall prove whether the achieved level of risk is tolerable. In other words, after the consideration of Risk Reduction Measure the **resulting level of risk** is analysed. Is it possible to change the status of the Hazard as well as the Measure to “closed”? The approach to evaluate this level of risk is the same as described for the risk evaluation – before (see sub-clause 5.2.3.2) i.e. using the risk matrix of EN 50126.

The risk evaluation after the consideration of Risk Reduction Measures depends on two circumstances. Firstly, a risk evaluation can only be performed if a **MODURBAN function** for Risk Reduction Measure is identified. On the basis of assumptions for Risk Reduction Measures no risk evaluation can be performed. It is assumed that only in case there is a system design or implementation in form of a MODURBAN function it is justifiable to close the Hazards. This is due to the fact, that MODURBAN functions – and the resulting system design - can be proved by documents i.e. MODURBAN deliverables. For assumptions for Risk Reduction Measures there is no proof about their actual implementation to the system design. Secondly, it is important whether a **human factor** is involved in the Risk Reduction Measures. In this case, it is not possible to evaluate the resulting risk. This is because it is rather difficult to determine the main characteristics for a human being concerning the availability and the reliability to fulfil the strived task e.g. the risk reduction function. For instance, if maintenance procedures are involved in the chain of Risk Reduction Measures, to which extend one can rely on the correct execution of these procedures? Since this question cannot be answered so far, no risk evaluation can be performed for Hazards where a human factor is involved. Additionally, this applies to Hazards where only one human factor is involved, whereas the rest of these Risk Reduction Measures are MODURBAN functions only.

But, if only MODURBAN functions act as Risk Reduction Measures and no human factor is involved, a risk evaluation can be performed to estimate the resulting level of risk for the analysed Hazard. In case, the resulting level of risk is tolerable, the status of the Measure can be set to “closed”. If the level of risk after the consideration of Risk Reduction Measures is undesirable or intolerable it is not possible to set the status of the Measure to “closed”. Therefore, the status has to be left “open”.

5.2.3.5 Closure

To finally prove where a certain Risk Reduction Measure is justified and sufficient, a **closing document** has to be given. This document references where and how the Risk Reduction Measure is realised and implemented. In case, the Risk Reduction Measure is a MODURBAN function, the documenting reference states “covered by system design”. This means that the Hazard is covered by MODURBAN system design in form of the MODURBAN function. For the MODURBAN functions the proving documents are D77, D78 and D81. If assumptions for Risk Reduction Measures are taken, assumptions for a possible closing document are given as well. For example, the Hazard is “incorrect maintenance” and the assumption for a Risk Reduction Measure is “correct and regular inspection and maintenance”. Consequently, the documenting reference would be: “maintenance procedures”. For

future project-dependent applications of the Hazard Log, the closing document is of utter importance, because if no, or only insufficient references i.e. documents can be given, it is not possible to close the Hazard.

Finally, a date is given to identify when the Risk Reduction Measure is proved. This is not used in this application of the Hazard Log but might be useful for further project-dependent applications.

5.2.3.6 Status

Two kinds of states are used in this Hazard Log. This is the **status for the Hazard** and the **status of the Measure** i.e. Risk Reduction Measure. They are used in the following way. First of all, both states are set to “open” by default. The status of the Hazard indicates if, in general, a Risk Reduction Measure for the Hazard is found, regardless whether this Risk Reduction Measure is a MODURBAN function or an assumption. Hence, the status of the Hazard is “closed” if a Risk Reduction Measure is determined. The status of the Measure is used to show if the Risk Reduction Measure can be proved and justified by the system design. If a Risk Reduction Measure is a MODURBAN function and, therefore, can be proved and referenced by a MODURBAN document, then the status of the Measure is “closed”. In case, no valid closing document for the Risk Reduction Measure exists, the status of the Measure has to be left “open”. This applies to all Risk Reduction Measures where assumptions are taken. Hence, all Hazards where assumptions for measures for risk reduction are suggested, the status of the Measure is “open”.

Regarding a **combination of different states** of Hazards and Measures, it is obviously possible that both states can be “closed” or “open”. Furthermore, it is possible that the status of the Hazard is “closed”, but the status of the Measure is “open”. However, in the moment that no Risk Reduction Measure is identified the status of the Hazard is left “open” and therefore, the status of the Measure is automatically “open” too. Finally, a Hazard is fully closed from that moment both states are “closed”. (It has to be noticed; the status of a Hazard or Measure, in terms of “open” and “closed”, is different to the expression that a Hazard is closed. The latter means that the Risk Reduction Measure is justified and referenced to cover a Hazard and no further action is necessary. The status control of Hazard and Measure, in terms of “open” and “closed”, describes the mere actual state.)

This approach of two states control for Hazards (i.e. the identification of Risk Reduction Measures) and Measures (i.e. whether a valid document for closing is referenced), is used to **differ between the action and its justification**. Hence, the action for risk reduction can be controlled separately from the justification, where the design or implementation is documented. It gives detailed view of progress which has been made, while developing the Hazard Log. For this first draft of the Hazard Log for MODURBAN it has been seen appropriate to use only two possibilities for the states i.e. “open” and “closed”.

5.2.3.7 Notes and Comments

This column is used to give further details about the Hazard or its Risk Reduction Measure. In this application it is mainly employed to **mark problems**, where it is not

clear what is e.g. meant by the Hazard or it is not possible of how to treat that particular Hazard. The second point is the indication and the suggestion whether it is possible to export and **transfer a certain Hazard** to a different system.

For a future application this column can be used for more general information and in addition to the worksheet - journal, more detailed explanations regarding a particular Hazard can be written.

5.2.3.8 Journal and Glossary

On top of worksheets for Hazards two additional worksheets are given. The first one is regarding a Hazard Log journal i.e. a **history of changes**. For later applications all changes to the Hazard Log can be recorded in the journal. It contains firstly a number and the date of change. Then, it is described what is about to be changed. This covers the numbering of the Hazard, the Hazard name and the initial aspect what shall be changed e.g. risk evaluation – before, severity (“critical”). Subsequently, the result, the reason and further descriptions for the particular change are specified. An entry into the journal is finalised by the person who is responsible for this change.

Finally, a glossary can be found in the Hazard Log. It gives a brief explanation about the used **abbreviations**.

5.3 Application of the Hazard Log

5.3.1 Assumptions for Application of the Hazard Log

During the actual application and development of the Hazard Log for MODURBAN additional assumptions and adjustments are made.

Firstly, in some cases **Hazards are newly added** to the original PHA. This is necessary where a more detailed level of Hazards is needed. Reason for this is the intention to reach similar levels of detail for all Hazards; hence, the addition of Hazards is sometimes necessary to comply with this target. One example is Hazard 2.4.1 – “fire in train” and 2.4.2 – “fire on guideway”. In this instance, Hazards are added to identify Sub-Hazards like “ignition” or “explosion” to give a more detailed explanation, what the reasons for these Hazards are. This is mainly done in comparison to Hazard 4.10 – “fire in station” where this level of detail is reached.

Another problem arises if a certain **Hazard is mentioned twice**, or more, in different contexts. In these cases, it is necessary to clearly identify the circumstances which shall be analysed. Once these Hazard circumstances are determined, the Hazard is analysed for the particular situation only. The target of this approach is to minimise redundancies and to cover all situation a Hazard might evolve in. This applies mainly to Emergency and Evacuation Hazards, where Hazards mentioned in this category are mentioned before under different Hazard categories. For these Hazards only the actual emergency or evacuation situation is analysed. For example, the Hazard “slippery floor” might lead to a fall of a person. In the category of Hazards concerning Train-Station-Interior Hazards (with no train in station) the causes are, among others, “faulty design of the station” or “incorrect maintenance or cleaning of station”. In case

of Emergency and Evacuation Hazards these causes are not analysed a second time. Here, the mere emergency situation is investigated. In this instance, one cause might be: “water or chemicals due to flooding or fire-fighters”.

One approach to identify Hazard Causes is used very often and, therefore, worth mentioning. For a lot of Hazards, mainly the ones of components or equipments, Hazard Causes arise from **faulty design or incorrect maintenance**. For these Hazard Causes a major contributor is the human error. In case, the Hazard Cause arises from faulty design but, an additional MODURBAN function is identified, it is assumed that this Hazard can be closed. This is indicated by setting the status of Hazard and Measure to “closed”. This is done on the assumption that faults during the design phase are rather seldom. In case, the Hazard Cause originates from faults occurring during maintenance, it is assumed that the Hazard cannot be closed. So far, it is not possible to estimate the reliability of maintenance procedures. Therefore, no evidence can be given about how often a maintenance Hazard occurs. In this cases of incorrect maintenance no risk evaluation – after is conducted. And, subsequently, the status of Measure has to be left “open”.

Alternatively and/or at a later stage, safety requirements to a maintenance procedure could close the Hazard, shifting the further validation works from risk analysis to procedure verification.

A further difficulty emerges from the question, what are valid Risk Reduction Measures. To support the **identification of Risk Reduction Measures** the following idea is used. Obviously every Hazard has a cause and a consequence. To reduce the risk evolving from this Hazard, measures can be taken against the cause as well as the consequence. For example for a Hazard, a person might fall into the track, the cause might be the station platform has no sufficient lightning system. The person would fall into the track because she or he would not see the platform edge. This can be covered and protected by providing enough brightness i.e. sufficient lightning in the station. On the other hand, if a guideway intrusion detection system exists, this system would detect the person on the track and stop approaching trains. This system is a Risk Reduction Measure which covers the consequences of a fall of a person.

Regarding the assumptions for possible measures for risk reduction, no formal way for their identification is used. Since no documents with functions or implementation types are available, the **assumptions for Risk Reduction Measures** are specific to the Hazard. Nevertheless, popular examples for Risk Reduction Measures are; “Ensure correct initial design” and “Regular inspection and maintenance”. For a future application, these assumptions can be used to support the investigation of referenced documents and functions to finally identify reliable Risk Reduction Measures.

5.3.2 Example of the Hazard Log for MODURBAN

The final appearance of the Hazard Log for MODURBAN is shown in Figure 15. To illustrate the actual application an example for one Hazard is given.

The Hazard which is exemplified is a train movement Hazard, which can be found in the worksheet 1 of the excel sheet (see appendices of this deliverable). It is Hazard



1.1.1.2.3.3.1 – “train not detected”. This Hazard leads to wrong train detection and finally that a switch might be moved under the running train. Since this Hazard is not an upper level Hazard this Hazard is analysed.

The first step is to give a **Hazard description**. This includes identifying an **initial risk owner**. For this application it is assumed, the “operator” is the initial risk owner. Secondly, the **MODURBAN relevance** is analysed. Here, the Hazard is first of all no upper level Hazard (i.e. the Hazard is a basic event) and the Hazard is MODURBAN relevant, therefore a “Yes” is entered in this field. The following field about the **input** and **reference source** are set by default, because this is a MODURBAN application and consequently the Hazard is input by “MODURBAN” and the reference source is the “MODURBAN PHA”. The next two items are about further **remarks** about the Hazard and a possible **date of change**. For the particular Hazard no remarks are necessary and the item for a date of change is not used, because this is the initial entry. The most important parts of the Hazard description are the following. On the one hand this is the **Hazard Cause**. For the Hazard – train not detected – two Hazard Causes are identified. These are: “unequipped or failed train” or a “data communication failure e.g. a data loss”. From now on, two separated analyses are performed. One for the first Hazard Cause: “unequipped or failed train” and one analysis for the second Hazard Cause: “data communication failure e.g. a data loss”. On the other hand and to finalise the Hazard description, a **type of accident** has to be identified. For this Hazard the accident is given by the PHA (upper level hazard 1.1.1 is Train (car) leaves guideway (momentarily or irrevocably / derailment). The type of accident is “derailment”. This applies to both Hazard Causes.

The subsequent step is to perform a **risk evaluation** for the first Hazard Cause. It can be assumed that for a derailment the **severity** of consequences are “catastrophic”. On the basis of the initial design and with respect to the fact that no measures for risk reduction are considered, the **likelihood** of occurrence of the Hazard is estimated with “probable”. Hence, the emerging **risk** of the particular Hazard (or Hazard Cause) is “intolerable”. This is a very rough estimation mainly because of the difficulty to evaluate a level for the likelihood of occurrence. But, no Risk Reduction Measure is considered and therefore, in every case the likelihood is rather frequent. However, it does not matter if the likelihood is frequent, probable or occasional. In case of catastrophic consequences the risk is intolerable for every instance.

The next section of the Hazard Log covers the identification of the **Risk Reduction Measure**. For the Hazard of an unequipped or failed train, a MODURBAN function can be identified, which covers this Hazard. It is **function 3.2.5** of D77: “detect unequipped or failed train”. “This function determines whether a section of track is occupied by an unequipped or failed train.” [D77] For every **Grade of Automation** the implementation of this function is “mandatory”. Since a MODURBAN function is identified it can be assumed that the **responsibility** lies with a future “system supplier”. Furthermore, since in general a Risk Reduction Measure is identified the **status of the Hazard** can be set to “closed”.

To evaluate the risk after consideration of the Risk Reduction Measure, it has to be proven whether a **human factor** is involved. In this example it is assumed that no human is involved and therefore a **risk evaluation** can be conducted. The possible **severity** of consequences of the Hazard is still “catastrophic” but due to the MODURBAN function the **likelihood** of occurrence is lowered to a minimum. Hence, the likelihood is estimated with a value of “improbable”. Therefore, the **resulting risk** can be assumed to be “tolerable” (according to the Risk Matrix of EN 50126).

With respect to the **closure** and a **documenting reference**, the implementation of the Risk Reduction Measure is “covered by the system design”, because a traceable MODURBAN function is identified.

Finally, since a MODURBAN function is used, no human factor is involved and the resulting level of risk is tolerable, the **status of the Measure** can be set to “closed”.

No further **comments** are necessary.

6 Analysis of the Application of the Hazard Log

This clause summarises the experience which is made during the application of the Hazard Log for MODURBAN. Moreover, it includes a discussion about the export of Hazards. Further recommendations, regarding the Hazard Log in general as well as the MODURBAN application, are given.

6.1 The Application of the Hazard Log for MODURBAN

6.1.1 Results of the Hazard Log – Closure of Hazards

The basis of this Hazard Log is 443 Hazards from the MODURBAN PHA. Out of this 443 Hazards 315 Hazards are basic events. These 315 Hazards are analysed and, after the identification of Hazard Causes, in total 604 Hazard Causes are identified. Consequently, for **604 Hazards a full analysis** in the Hazard Log is performed.

Since the goal of a Hazard Log is to cover Hazards with Risk Reduction Measures, the information about how many Hazards are actually closed is crucial. For the first draft of the Hazard Log only partly reliable information can be given, because most of the data in the Log are based on assumptions and estimations. Nonetheless, an analysis is performed to discover reasons for open and closed Hazards respectively.

Firstly, out of the 604 analysed Hazards for 598 the status of the Hazard is “closed”. This means that for 598 Hazards Risk Reduction Measures are found, regardless whether MODURBAN functions or assumptions are identified. To cover Hazards with Risk Reduction Measures, for 211 Hazards a MODURBAN function is used. In all other cases assumptions regarding a risk reduction are made. In other words, **for 99% of the Hazards a Risk Reduction Measure can be assumed**. This relatively high number is plausible because the identification of Risk Reduction Measures is made on assumptions, based on a general knowledge about urban guided rail systems and the knowledge of MODURBAN functions.

Secondly, the number of Hazards, where the **status of the Measure is “closed” is 161**. It is assumed that if both states (Hazard and Measure) are “closed” the Hazard in total can be seen as closed. Arguing with the methodology used to develop this Hazard Log (see Figure 14 – Hazard Log Action Procedure), the status of Measure can be set to “closed” if a **MODURBAN function** as Risk Reduction Measure is identified and no **human factor** is involved. In reverse, if no MODURBAN function or a human factor is identified as Risk Reduction Measure, it is not possible to set the status of Measure to “closed”. This is the major reason that the status of Measure for 442 Hazards is still “open”. In most instances no MODURBAN function is identified. For 64 Hazard a MODURBAN function is identified, but the status of Measure is still “open”, because a human factor is involved. Especially maintenance errors are responsible for the involvement of human factors.

6.1.2 Manageability of the Hazard Log

Overall it can be kept; the Hazard Log for MODURBAN is relatively **easy to apply**, regarding the mere structure. This is due to the fact that only one view of a table is used and this table is not too large. The user can straightforward follow the table from the left to the right in order to analyse a Hazard. This is possible because no sub-table or links to other parts of the Hazard Log are used.

A major drawback of this Hazard Log arises from the PHA of MODURBAN. To fully understand a Hazard it is necessary to mind the actual Hazard name as well as the upper level Hazards. In plain words, one needs to check all Hazards which are above the analysed Hazards to completely understand the Hazard and its consequences. But due to the fact that up to nine levels for the Fault Tree of the PHA are used it is often **difficult and time-consuming to comprehend a Hazard**. (Again, the structure is kept to retain the compliance with the PHA of MODURBAN.)

Another deficit of the Hazard Log - i.e. the Excel sheet application - is the missing linkage between various cells. **No automatism** are used (e.g. for the final determination of the resulting level of risk). Hence, the user has to enter all entries (e.g. resulting level of risk) into the Hazard Log manually.

6.1.3 Hazard Description

One problem originates from the **difficulty to identify Hazard Causes**. No formal way or method is used to investigate Hazard Causes. Consequently, no reliable information can be given whether these Hazard Causes are complete or not. A further investigation might be appropriate to cover all Hazard Causes. So far, the analysis of the Hazard Causes has mainly the consequence to show where the human factor is contributing to a Hazard. Admittedly, further analysis is maybe subject to a future research project.

But, on the other hand, it is questionable if the Hazard Cause analysis is that helpful (i.e. analysing causes for the Hazards of the MODURBAN PHA). This is because for a generic approach like this, it might be satisfactory to compare only the Hazards, given as basic events in the PHA, with the available safety functions (i.e. MODURBAN functions). Finally, this matter leads to the question: on what level of a Fault Tree is it possible to prove that all Hazards are covered with a Risk Reduction Measure? This matter directly affects the problem evolving from the **degree of detail** or itemisation of the original PHA. For example, in some cases the PHA stops with Hazard Cause “fire” as basic event. In other examples the Hazard “fire” is analysed in more detail. Hence, the subsequent Hazard Cause is e.g. “ignition” which then leads to “fire”. To overcome this problem new Hazards are added. But this is not possible for every instance.

Moreover, the analysis of the **MODURBAN relevance is discussable**. For this application of the Hazard Log for MODURBAN it makes perfect sense to distinct between relevant and non-relevant, mainly to identify the MODURBAN problems. But for a future application it does not matter whether this is a MODURBAN problem or not. The Hazard has to be covered with a Risk Reduction Measure, regardless if from MODURBAN or not.

6.1.4 Risk Evaluation

Probably the most arguable aspect of the Hazard Log is the evaluation of a level of risk for the analysed Hazard. Comparing the two aspects for the determination of risk, the estimation of severity is in the majority of the cases obvious. For types of accidents like derailment, collision, fire or explosion, a severity of consequences is mostly estimated with “catastrophic”. The estimation of **likelihood of occurrence of a Hazard is difficult**. For this application of the Hazard Log only assumptions are made. This is done to give a first idea of the level of risk and therefore, of how the need for action regarding risk reduction is. But, for the majority of the Hazards a level of severity of “catastrophic” or “critical” is assumed (around 90%). Considering this, and in combination with the fact that for “catastrophic” or “critical” the likelihood “remote”, “occasional”, “probable” and “frequent” lead to, at least, an undesirable or intolerable level of risk, inaccuracies are acceptable. It can be accepted because this risk evaluation mainly estimates a need for action.

6.1.5 Risk Reduction Measure

The first difficulty arises to discover suitable MODURBAN functions for the particular Hazard. However, this is done in the most thorough way. But, due to the large number of MODURBAN functions and Hazards it **cannot be completely assured that every Hazard is covered** with the correct MODURBAN function. This needs further investigation. Regarding the made assumptions for Risk Reduction Measures, it is mostly no problem to find these suggestions for a risk reduction.

On top of the Risk Reduction Measure an evaluation about the reached level of risk is made. This is numerous times impeded by the difficulty to estimate the **influence of a human factor** to the Risk Reduction Measure. A rough estimation of the reliability of humans during operation or maintenance could help to overcome this demerit.

With reference to the given **responsibility** for a Risk Reduction Measure it is strived to use only a minimum of responsibilities. For this application five major types of responsibilities are used. These are:

- System supplier
- Operator
- Vehicle supplier
- Station owner
- Infrastructure owner

The advantage of using only five major responsibilities is the straightforward approach. However, this is directly connected to its drawback of a too low level of detail. A further clarification is needed to identify clearly the responsibilities to subsequently close Hazards.

One question, which evolves during the development, regards the **Grade of Automation** and the subsequent implementation of MODURBAN functions. What is the Risk Reduction Measure in case the protecting MODURBAN function is only

mandatory in e.g. GOA 4? For example the MODURBAN function “Supervise Condition of Start of Train Movement” (see 3.5.2 of D77) is only mandatory for GOA 4. For GOA 1-3 it is an optional function. Consequently, e.g. for GOA 1 the driver or station personnel have to ensure safe train departure conditions.

6.1.6 Closure

The list of **closing documents** used for this application of the Hazard Log is long. This is arguable. On the one hand this Hazard Log is seen as a first generic approach. Ultimately, preferably rather general documents should be applied. On the other hand an individual closing document is of advantage to prove clearly how the Risk Reduction Measure is implemented. Further clarification is needed to find general closing documents which can support a misunderstanding-free application.

6.1.7 Status

So far a **simple approach** is used to indicate the states of a Hazard and its Measure. This is advantageous and sufficient for this application. But for a further application, which considers the actual export and transference of Hazards and different states regarding an achieved closure, more states for a Hazard or Measure can be introduced. However, the question stays whether it is useful to raise the level of complexity for generic application.

One demerit of the chosen status control embraces the terms of Hazard and of Measure. The meaning of these **terms is rather misleading** and insufficient in comparison with the actual words. A clear and unambiguous terminology should be aspired in future applications.

6.2 Discussion about Export of Hazards

For about 30% of the Hazards MODURBAN functions can be identified that directly cover a Hazard. For the rest of these Hazards two questions evolve: firstly about the Risk Reduction Measure and subsequently about its responsibility. On top of the made assumption the problem is, **what happens if neither operator nor system supplier is responsible** for the Hazard and its Risk Reduction Measure. One solution is to either transfer the Hazards to a different MODURBAN sub-project (for the application of this Hazard Log within MODURBAN e.g. to MODACCESS) or to export the Hazard to an external, say the vehicle supplier. In these cases, the problem arises of how to monitor these Hazards and whether they are treated correctly. This treatment should cover a full supervision of the particular Hazard with an adequate Risk Reduction Measure. For a future application of the Hazard Log it might be appropriate to investigate mechanisms and procedures to ensure a correct transference and export of Hazards, which cannot be solved by the operator. An additional open point is; what solution shall be considered if the operator cannot solve a Hazard and no one else takes the Hazard over. A popular example for the matter is the maintenance of vehicles, station and infrastructure. Is the operator the only responsible for these Hazards? In this application of the Hazard Log it is assumed the operator is the only responsible. This is done mainly not to complicate



this topic. But, the operator can not be in full charge of all vehicle or station maintenance.

It shall be mentioned, that it is in particular those Hazards here discussed, where the Hazard Log shows most of its usefulness. Measures exported to “someone” during system design needs to be remembered permanently and a project can not be finally authorised to go into passenger operations if not all of the unclear or exported risk control elements are finally unambiguously be resolved.

6.3 General Recommendations and Future Steps

The first recommendation to fully develop the Hazard Log for the MODURBAN application is to thoroughly check all MODURBAN references again, in order to cover all aspects of relevant MODURBAN functions. This includes mainly the latest **update of the deliverable D80**.

Secondly, which is probably a major future task, for the assumptions, which are made for the Risk Reduction Measures and its responsibilities, relevant **MODURBAN functions or Risk Control Measures** have to be found. If this is not possible the particular Hazards shall be transferred inside of the MODURBAN project to other sub-projects. Otherwise the unresolved Hazards shall be exported to an external reference supported by a clear export of the responsibility and subsequent monitoring.

To ultimately close a Hazard where a **human factor** is involved, it is of high importance to estimate a level of reliability or safety, even with uncertainties. The reliability of the human factor can give evidence of whether a certain Risk Reduction Measure can be accepted. In other words, it has to be estimated if a Risk Reduction Measure (involving human factors) covers a Hazard in a way that leads to an acceptable level of risk. This applies mainly to Hazards where a MODURBAN function is identified and an additional Risk Reduction Measure, involving a human contribution, is assumed. So far, it is not possible to close these Hazards.

Finally, the different alternatives for a **software tool support** may be reconsidered in more detail. Bearing in mind the benefits of the tool Microsoft Excel, still a requirement management tool may be more appropriate. The Hazard Log is a database which combines a lot of references e.g. the origin of the actual Hazards, the Risk Reduction Measures or mainly the various closing documents. To trace these references back clearly, the software tool may support these requirements. However, for this application of the Hazard Log things shall be kept simple - if sufficient also for future projects and applications this might be difficult to be retained. Therefore, a tool which supports more complex structures can be of advantage. Nonetheless, for a short term solution, the Excel sheet may be extended. For example Hazards or closing documents can be referenced by cross-references to the appropriate document (i.e. by insertion of Excel hyperlinks). Additionally, links and interconnections between the Excel cells can be inserted to support a better manageability; e.g. for the risk evaluation or the states of Hazards and Measures.

7 Conclusion

- The Hazard Log is an essential part of a risk assessment, because it combines a record of all identified Hazards and measures for the risk reduction for these Hazards.
- The Hazard Log has its fundamental purpose in the system lifecycle because the Hazard Log is not restricted to a single phase of the lifecycle. The Hazard Log is a dynamic document which is permanently updated throughout the system lifecycle.
- It is possible to create a generic Hazard Log on the basis of European Standards, available literature and analysed examples of various Hazard Logs.
- This Hazard Log is applied to the MODURBAN project. This application is done by considering identified Hazards from the MODURBAN PHA and possible measures for risk reduction arising from MODURBAN deliverables (D77, D78 and D81).
- After analysing the Hazard Causes of the identified Hazards of the MODURBAN PHA, about 600 Hazards are subject to analysis.
- For about a third of these Hazards a direct sufficient coverage solution is found i.e. these Hazards are closed. This is done by covering the Hazard with a MODURBAN function with adequate Safety Requirements.
- The reasons for about 70% of the Hazards still unresolved are mainly that no MODURBAN function is directly appropriate or a human factor is involved in the Risk Reduction Measure without clear estimation of sufficiency of safety at this stage. It shall be noted, that these effects show only, since a more complete guided transport analysis is performed while MODURBAN addresses mainly Automatic Train Control functions.
- The Hazard Log becomes evidently a mandatory tool for MODURBAN like application projects since it is obviously the only instance that monitors - from the beginning until commissioning and revenue service - all possible Hazards and to what level of satisfaction these Hazards are covered/resolved. Unresolved problematic circumstances remain “open” (as long as this status persists). It is therefore an indispensable tool, in particular for the sponsor of the project and for the safety authorities granting permission to operate.

8 References

- [ADE 07]** – Australian Government, Department of Defence – Navy News - <http://www.defence.gov.au/news/NAVYNEWS/editions/4902/feature/feature07.htm>
- [BRA 05]** – “Risikoanalysen in der Eisenbahn- Automatisierung”, Jens Braband – EurailPress 2005
- [CAA 02]** – „Safety Management Systems for Commercial Air Transport Operations” – UK Civil Aviation Authority - www.caa.co.uk 2002
- [CHI 03]** – “Turning up the HEAT on Safety Case Construction”, Paul Chinneck, David Pumfrey, Tim Kelly – www.cs.york.ac.uk 2003
- [D77]** – “Train protection MODURBAN functional specification” - Berliner Verkehrsbetriebe BVG, MODURBAN – MODSYSTEM WP21 D77 2006
- [D78]** – “Non train protection MODURBAN functional specification” – Berliner Verkehrsbetriebe BVG, MODURBAN – MODSYSTEM WP21 D78 2006
- [D81]** – “MODURBAN prescription: overall architecture and allocation of vital function” – UNIFE, MODURBAN – MODSYSTEM WP22 D81 2005
- [86]** – “Safety conceptual approach for functional and technical prescriptions” - TU Dresden, MODURBAN – MODSYSTEM WP23 D86 2006
- [DRE 07]** – “Entwicklung strukturierter Gefahrenlisten am Beispielsystem „Stellwerk””, Jörn Drewes, Jörg May - Tetzlaff Verlag (Hamburg) Signal + Draht (99) 1+2/2007
- [EARL]** – Edinburgh Airport Railway Link, Project Safety Management Plan (December 2006) – Revision A - www.earlproject.com 2006
- [EN 50126]** – CENELEC Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (EN 50126) 1999
- [EN 50126-2]** – CENELEC Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for Safety 2006
- [EN 50129]** – CENELEC Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling 2002
- [EN 50129-2]** – CENELEC Railway application - Communication, signalling and processing systems – Safety related electronic systems for signalling – Application Guideline of EN 50129 2005

[FAR 04] – “Managing a System Safety Case in an Integrated Environment”, Saeed Fararoy (rcm2 limited) - <http://www.sei.cmu.edu> 2004

[FEN 07] – “Handbuch - Eisenbahninfrastruktur”, Lothar Fendrich (Editor) - Springer Verlag Berlin Heidelberg 2007

[HAM 04] – “HazLog: Tool support for hazard management”, Christian Hamoy, David Hemer, Peter Lindsay – 9th Australian Workshop on Safety Related Programmable Systems (SCS '04) – Australian Computer Society, Inc 2004

[LEM 07] – “Prozessorientierte Identification von Gefährdungen in Eisenbahnsicherungssystemen”, Meike Lemke, Dieter Kaufholdt, Saeid Arabestani - Tetzlaff Verlag (Hamburg) Signal + Draht (99) 10/2007

[MOK 04] – “A Practical Risk and Safety Assessment Methodology for Safety-Critical System”, Chinnarao Mokkalpati - www.arnea.org 2004

[NHL 07] – Agileware, Hazard Log for the Royal Australian Navy - <http://www.agileware.net/navyhazardlog>

[PAS 03] – “Hazard Analysis of Complex Distributed Railway Systems”, di Tommaso Pasquale, Esposito Rosaria, Marmo Pietro, Orazio Antonio – Proceedings of the 22nd International Symposium on Reliable Distributed Systems (SRDS '03) – IEEE 2003

[SCH 07] – “Weltweite Wachstumsperspektiven von U-Bahnen und Light Rail”, Andreas Schwilling, Tobias Schönberg – Der Nahverkehr 06/2007

[SOL 04] – „RAMS-Management nach CENELEC in der Praxis“, Thomas Solleder, Peter Magg – Tetzlaff Verlag (Hamburg) Signal + Draht (96) 1+2/2004

[YB 07] – Engineering Safety Management Issue 3, Yellow Book 3, Published by Railtrack on behalf of the UK rail industry 2000



9 Appendices

Appendix A - Example of an Application of the Preliminary Hazard Log for MODURBAN