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

MODSafe Risk Analysis

Delivery D2.3

Contract No.	*218606*
Document type	*DEL*
Version	*V2.1*
Status	*Final*
Date	*310511*
WP	*WP 2*
Lead Author	*WP 2*
Contributors	*WP 2 partners*
Reviewer	*WP 10 Members*
Description	*Deliverable D2.3 Version 2.1*
Document ID	*DEL_D2.3_TUD_WP2_110531_V2.1*
Dissemination level	*RE*
Distribution	*WP10*

Document History:

Version	Date	Author	Modification [very short description]
V1.0	25.02.2011	WP 2	New document
V2.0	15.03.2011	WP 2	Accounting for WP2 comments
V2.1	19.04.2011	WP 2	Accounting for WP10 comments

Approval:

Authority	Name/Partner	Date
WP responsible	TUD / WP2 Approval	2011-03-15
EB members	WP 10 Approval	2011-05-11
Coordinator	TRIT	2011-05-31

Table of contents

List of figures

Not used in this document

List of tables

1. Summary of this Document

This deliverable represents the MODSafe risk analysis. For each hazard the severity of hazard consequences, an assumed probability and possible risk reducing factors are analysed.

1.1 References

Reference-ID	Document title, identifier and version
/1/	DEL_D2.1_TUD_WP2_091021_V2
/2/	D2.1_Annex_Hazard_Analysis_091102_v3
/3/	D2.2_Annex_Hazard_ Analysis_100427_v8
/4/	D4.1 State of the arte analysis and review of results from previous projects V2.2
/5/	D4.2 Analysis of safety requirements for MODSafe continuous safety measures V2.1
/6/	DEL_MODSYSTEM_WP23_D127annex_TUD_080328
/7/	DEL_MODSYSTEM_WP23_D86_TUD_060914
/8/	DEL_MODURBAN-D129_RATP_WP20_090317_V27 MODURBAN GLOSSARY
/9/	DEL_MODSYSTEM-D80_BVG_WP21_090317_V2-5
/10/	DEL_MODSYSTEM-D85_UNIFE_WP22_090515_V10-Final
/11/	EN 50126, CENELEC, Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999
/12/	EN 50129 CENELEC, Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling; 2003
/13/	IEC 62290-1 Railway applications - Urban Guided Transport Management and Command/Control Systems; Part 1: System Principles and Fundamental Concepts
/14/	IEC 62267 -Railway applications - Automated Urban Guideway Transport (AUGT) – Safety requirements

1.2 Terms and Abbreviations

1.2.1 Terms

Term	Description	Source
Accident	An accident is an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage.	EN 50129
Hazard	A condition that could lead to an accident.	EN 50129
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard or a threat) and the degree of severity of that harm.	MODSAFE
Safety measure	Means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.	Commission regulation (EC) No 352/2009

1.2.2 Abbreviations

(as used in the document and in the annex)

Abbreviation	Explanation
ATC	Automatic train control
ATO	Automatic train operation
ATP	Automatic train protection
ATS	Automatic train supervision
CCTV	Closed Circuit Television
CE	Clearance Envelope
GOA	Grade of Automation
HMI	Human-Machine Interface
MA	Movement Authority
N.A.	Not applicable
OCC	Operations Control Centre
PSD	Platform Screen Door
RATP	Régie Autonome des Transports Parisiens (Autonomous Paris Transport Authority)
UGTMS	Urban Guided Transport Management System
VL	Speed Limit
VT	Actual Train Speed

2. Introduction

This document is a further development of the hazard analysis of WP2 and summarises the risk analysis for the MODSafe hazards. For each hazard a risk estimation is performed which considers possible hazard consequences, e.g. accidents, the severity of the consequence and a probability.
The annex to this document contains the MODSafe risk analysis.

3. MODSafe Risk Analysis

3.1 General Approach

The basis of the MODSafe risk analysis is hazard analysis of D2.2 called “Consistency analysis and hazard analysis” /3/. All information and explanations on an understanding of the hazard list and the structure of the hazard can be found in the first and second deliverable of working package 2 (/2/, /3/).

The MODSafe risk analysis is performed for each hazard identified in the MODSafe hazard list of WP2.
The analysis contains the following parameters, which are described in more detail in the below table.

Risk parameter of the initial risk analysis:

- Hazard
- Hazard cause
- Type of accident
- Possible consequential accidents
- Severity of consequences
- Assumed probability
- Risk reduction
- Risk
- Remarks

Table 1 – Description of risk parameter

Risk parameter	Description
Hazard	• Describes the name of the hazard • The overall understanding of the hazard arises from the tree structure (cf. D2.1 /2/) • For each hazard a risk analysis is done
Hazard cause	• For each hazard possible hazard causes are given
Type of accident	• Assumed accident for each hazard
Possible consequential accident	• Accidents resulting from the primary accident
Severity of consequences	• For each hazard a level of severity of the possible hazard consequences is estimated • Four levels of severity are assumed • Basis for the estimation are the assumed accident of the hazard
Assumed probability	• Estimation of the frequency of occurrence of the hazardous situation • Does not consider existence of safety measure (initial probability) • Conservative assumptions are taken
Risk reduction	• Estimation of possible risk reduction • Represent the hazard exposure and/or a possibility to avoid the hazard
Risk	• Estimation of resulting risk • Notation according EN50126
Remarks	• Contains, if necessary, additional information on the risk parameter

The following basis i.e. situation for an urban guided rail system is assumed for an initial estimation of risk. This assumption provides circumstances and boundary conditions on a system to be able to perform a risk analysis.

The system consists of:

- Train cars (working, but initially without maintenance)
- Guideway and tracks (operation is possible)
- Stations (operation and passenger exchange is possible)
- No maintenance at all
- No evacuation procedures
- No ATC (incl. ATP; ATO; ATS)

The initial risk estimation is based on a system, where initially the safety measures (eg. an ATP) are not yet existing. The result is often an unacceptably high risk (eg. Train Collisions without an ATP). The safety measure is then added such, that it controls the hazard to acceptable regions. For further explanation see D4.1 /4/.

An estimation of risk after a consideration of possible safety measures is not done. It is assumed that safety measures would reduce risk to a tolerable level.

3.2 Severity level of hazard consequences

The following table describes the severity level of the possible hazard consequences as introduces in EN 50126 /11/ and used here for the MODSafe risk analysis as “Severity Consequences”.

Table 2 – Hazard severity level according to EN 50126

Severity level	Consequence to person or environment	Consequence 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 a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

3.3 Frequency of occurrence of a hazardous event

The following table contains the categories and descriptions for the frequency of occurrence of the hazardous event as used here in the MODSafe risk analysis as “Assumed probability”. The categories and the descriptions originated from the EN 50126 /11/.

Table 3 – Frequency categories 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 sometime in the system life cycle. The hazard can reasonably expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

For the Probability estimation, general clusters of hazards may be identified with different basic assumptions.
Those hazards that are typically covered by UGTMS functions are systematically assumed to be of “frequent” initial probability and the respective analysis of MODSAFE deliverable D4.2 /4/
is taken over. The concept behind is the assumption, that the unacceptable risk must be covered by a Safety Function (see D4.2) to reach acceptable rates, and, should the Safety Function not perform its service, the hazard must be more or less instantaneously assumed.

Another cluster of functions concern mechanical or other devices, where statistical probabilities or frequencies are problematic (eg. broken axle, broken wheels, brake failures). Here, it is assumed that the devices are designed such, that with regular maintenance they work safely during their lifetime, and probabilities of failure are rather Occasional to Remote.

On Force Majeure events (like earthquakes, flooding) and hazards with intended causes (eg. criminal acts) depend highly on location and context and are often qualified by “occasional” but require further analysis by the individual user.

3.4 Risk reduction

To estimate a risk reduction of the risk associated with the hazard, a conservative approach i.e. the worst case scenario is used. Therefore, for all the hazards no risk reduction can be considered.

In D4.2, three possible risk reducing factors can be applied, the exposure, already initially existing barriers and avoidance/escape of/from consequences (factors E, P, C). The three factors together can be grouped into one factor, the risk reducing factor. It appears as a numerical factor and is set to “1” if no initial risk reduction can be conservatively assumed, “0,1” if one initial risk reduction can be conservatively assumed, and “0,01” if two independent initial risk reductions can be conservatively assumed.
For SIL-Determinations in D4.2 it is applied numerically to the (numerical) Safety Target.

3.5 Risk matrix

To estimate a level of risk the following risk matrix is used. It is introduced in EN 50126 and represents a typical example of risk evaluation including an acceptance criterion.

Table 4 – Risk matrix according to EN 50126

Frequency of occurrence of a hazardous event	Risk Level			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity level of hazard consequences			

3.6 Remarks

The following remarks shall be considered in the MODSafe risk analysis:

- “Cf. D4.2” – hazard is already considered in MODSafe D4.2 during the analysis of MODSafe safety functions. The analyses with respect to hazard severity and probability are in line with the MODSafe deliverable 4.2 /5/. This applies to hazards (or hazardous situations) which are analysed in D4.2 and D2.3. For that purpose safety considerations, which have been performed in MODSafe D4.2 are incorporated into D2.3.
- “Cf. WP8 and 9” – hazard is assumed to be a security issue. Security aspects are analysed in MODSafe work package 8 and 9 in more detail.
- When the Safety Measure includes “Ensure Correct Initial Design” it shall be noted, that for UGTMS elements the initial design, the development, the validation and the safety assessment is assumed to be performed according the norms EN50126, EN50128 and EN50129. In general, detailed studies according state of the art rules and techniques are required.
- Whenever the Safety Measure includes “Regular Inspection and Maintenance” it is assumed, that the supplier of a product shall deliver a maintenance manual to the operator with the type and frequency for the inspection that are required for maintaining the safety level.
- For some hazards, no mandatory safety function was defined in D4.2, D5.1 (eg. broken elements in the clearance envelope of the train due to environmental impacts). In order to leave the hazard not uncovered, supervision of “optional” external devices/sensors had been suggested in the hazards analysis under “Generic Safety Measure”. On the level of Safety Requirements of optional measures, the detailed risk analysis approach as of D4.2 may be applied by the operator, if the hazard is assumed.
- Concerning Safety Measures such as training for Maintenance Alarm Response it shall be noted, that detailed risk assessments must be agreed between suppliers and operators to define the contents and roles of alarms, personnel at OCC, maintenance staff and others.

4. Conclusion

This deliverable represents the final deliverable of MODSafe working package 2. It contains among others all identified hazard, corresponding risk analyses and safety measures.

5. Annex – MODSafe Risk Analysis

The annex contains the MODSafe risk analysis and can be found in a separate document.