



MODURBAN

FP6 Project: IP 516380

EC Contract n°: TIP4-CT-2005-516380

MODSYSTEM WP23 SUBPROJECT

– DELIVERABLE REPORT –

Deliverable ID:	D126
Deliverable Title:	Preliminary safety plan
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 safety plan
Document ID: D126
Revision: V4
Revision Date: 17 February 2009
Author: TUD – Forchmann, Schütte
Security: PUBLIC

Approvals

	Name	Company	Date	Visa
<i>Technical Management Committee</i>	B. VON WULLERTSORFF G. POITRASSON-RIVIÈRE D.DIMMER G. LEGOFF L. LINDQVIST U. HENNING / A. PRICE M. NOCK JP RICHARD/D. COINEAU Y. AMSLER C. GOUTORBE	UNIFE ALSTOM THALES CSEE BOMBARDIER SIEMENS KNORR BREMSE RATP UITP ALMA		
<i>Coordinator</i>	B. VON WULLERSTORFF	UNIFE	17/02/09	OK
<i>Quality Manager</i>	B. VON WULLERSTORFF C. GOUTORBE	UNIFE ALMA	17/02/09	OK

Documents history

Revision	Date	Modification	Author
Draft 1	08/05/29	First version for comments	TUD
Draft 2	08/06/30	Consideration of comments received during review of draft 1	TUD
V3	08/09/12	Consideration of comments received during review of draft 2	TUD
V4	09/02/17	Glossary updated	RATP



The scope of the document applies to:

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

(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

D126 - Preliminary safety plan

Deliverable ID , associated WP & Subproject	D126 MODSYSTEM / WP 23
Type of Deliverable	Report
Input / Starting stage	
Output / Final stage	

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

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

Associated Risk analysis	Type, solution envisaged, action, actors	Actual Reduction
Before start		
During task implementation		



D126 - Preliminary safety plan

Deliverable Abstract

For the design, construction and operation of an urban guided rail system, safety shall be planned. Throughout a system lifecycle every safety relevant activity and responsibility shall be scheduled. An early safety planning for the overall system is done in a document called safety plan. A safety plan shall schedule all safety roles and activities for the particular project. This safety planning is done in order to provide a framework to achieve and ensure safety.

The preliminary safety plan which is described in this deliverable, shall serve as a guideline for the establishment of a safety plan for MODURBAN like realisation projects. It provides advice on the safety process steps (including safety organisation and documentation), system requirements, design and implementation, system certification and demonstration. Additionally, steps for approval as well as the system acceptance are discussed.

Associated Milestone (if relevant):



SECTION 2 – DELIVERABLE DETAILED DESCRIPTION

Table of Contents

- 1 Introduction to the deliverable.....9**
 - 1.1 Purpose and scope.....9**
 - 1.2 Structure.....10**
 - 1.3 Objectives.....10**

- 2 Terms, definitions and abbreviations11**
 - 2.1 Terms and definitions11**
 - 2.2 Abbreviations.....13**

- 3 The conception of a safety plan14**
 - 3.1 Introduction – background14**
 - 3.2 Definition and purpose of a safety plan.....17**
 - 3.2.1 Definition of a safety plan17
 - 3.2.2 The safety plan in the system lifecycle18

- 4 Content of a safety plan20**
 - 4.1 Introduction.....20**
 - 4.1.1 Aim and purpose of a safety plan20
 - 4.1.2 Structure of a safety plan21
 - 4.1.3 Document control.....21
 - 4.1.4 Legal framework21
 - 4.1.5 System description22
 - 4.2 Safety process22**
 - 4.2.1 Safety process steps23
 - 4.2.2 Safety organisation25
 - 4.2.2.1 Operator.....26
 - 4.2.2.2 Supplier.....27
 - 4.2.2.3 Safety authority28
 - 4.2.2.4 Safety assessor29
 - 4.2.2.5 Summary - the safety process and allocating responsibilities30
 - 4.2.3 Safety documentation32



- 4.2.4 Safety principles 35
- 4.2.5 Approval and acceptance process..... 36
- 4.2.6 Other safety relevant activities..... 37
- 4.3 System requirements and system design 38**
 - 4.3.1 Hazard identification 38
 - 4.3.2 Risk analysis..... 39
 - 4.3.3 System requirements..... 40
 - 4.3.4 Safety requirements..... 40
 - 4.3.5 System design 41
 - 4.3.6 Verification and validation 42
 - 4.3.7 Safety audits and assessment..... 43
- 4.4 System certification and approval 44**
 - 4.4.1 System certification..... 44
 - 4.4.2 System approval 47
- 4.5 System demonstration and acceptance 48**
 - 4.5.1 System demonstration 48
 - 4.5.2 System acceptance 49
- 5 Conclusion..... 50**
- 6 Bibliography 51**
 - 6.1 Referenced documents 51**
 - 6.2 Further reading 52**



List of tables and figures

List of tables

Table 1 – Project safety related tasks according to EN 50126 16

Table 2 – Safety plan in the system lifecycle 19

Table 3 – Example of responsibilities in the safety process..... 25

Table 4 – Example of a safety process in the lifecycle 31

Table 5 – Examples of documents in the system lifecycle 33

Table 6 – Example of an approval and acceptance process 36

Table 7 – THR and SIL table according to EN 50129 40

Table 8 – Examples of MODURBAN safety functions - including possible SIL allocation 41

List of figures

Figure 1 – System lifecycle according to EN 50126..... 15

Figure 2 – Purpose of a safety plan 18

Figure 3 – Example of system architecture 22

Figure 4 – Example of safety process 24

Figure 5 – Example of a structure of safety roles..... 28

Figure 6 – Arrangement for independence according to EN 50129..... 30

Figure 7 – Verification and validation in the lifecycle according to EN 50126..... 42

Figure 8 – Structural elements for a safety case..... 45

Figure 9 – Structure of safety case according to EN 50129..... 46

Figure 10 – Structure of technical safety report according to EN 50129 46

Figure 11 – Example of system approval process 47

Figure 12 – Example of system demonstration and acceptance process..... 49

1 Introduction to the deliverable

This clause shall give an overview about the purpose and the scope of the MODURBAN deliverable 126. Moreover, the chosen structure of the deliverable is presented as well as the aspired objectives.

1.1 Purpose and scope

The establishment of safety is of paramount importance for urban guided rail systems. Safety must be assured throughout design and operation of a transportation system to protect passengers, workers and the public from any unacceptable risk. Therefore, all activities which concern safety matters shall be planned and conducted in the most thorough manner. Especially, at the beginning of a project a safety management structure, safety related activities and safety milestones shall be determined. The European standard EN 50126 recommends for this purpose of safety planning the preparation of a safety plan. However; a safety plan shall describe how it is planned to achieve safety.

This deliverable describes the conception and preparation of a safety plan. It shall act as a guideline for urban guided rail systems, to support an early establishment of a safety plan. This deliverable is not restricted to one particular lifecycle phase; it describes safety planning for the overall system lifecycle. This preliminary safety plan shall give recommendations for the system lifecycle in order to give an overview of the processes and activities for system safety and system approval and acceptance. The recommendations are extended by several examples with an emphasis on the MODURBAN project.

Particularly, the following functions and elements of a safety plan are outlined in this deliverable:

- safety process steps
- safety organisation
- safety approval process
- system requirements and system design
- system certification and approval
- system demonstration and acceptance

This deliverable shall act as an overall safety plan which describes safety matters, as mentioned above, and leaves specific tasks of suppliers out of scope.

The addressee of this deliverable shall be the operator, which is responsible for the safety plan. The establishment of the safety plan shall be done by the operator or, in case of an early involvement of the supplier in the lifecycle the supplier might contribute to, or take over,

the establishment of a safety plan. Operators may delegate editorial work to contractors; however the operator remains accountable for the safety plan.

Since other MODURBAN tasks address also issues like system approval, system acceptance or safety certifications the presented safety plan deliverable shall be read in conjunction with other related MODURBAN documents, in particular D92 and D93.

1.2 Structure

This deliverable is structured in the following way. First of all, the principle conception of a safety plan shall be presented. Subsequently, clause four aims at outlining the main elements of a safety plan. (Clause four can be seen as a commented template for a safety plan.) This includes a description of the safety process steps, the system requirements and system design, system certification and demonstration. Additionally, steps of approval and acceptance are explained. Clause five shall summarise the main findings.

Within the deliverable, sentences like: “this section of the safety plan shall describe ...” shall provide guidance on necessary elements of a safety plan. Additionally, several examples are given, which shall illustrate an actual implementation of a safety plan. For example, a required element of a safety plan is the description of procedures for a risk analysis, subsequently; examples for different ways to perform risk analyses are presented.

1.3 Objectives

- (1) Provision of idea and conception of a safety plan
- (2) Description of the main elements of a safety plan:
 - a. safety process steps
 - b. safety organisation
 - c. approval and acceptance process
 - d. system requirements and system design
 - e. system certification
 - f. system demonstration
- (3) Presentation of examples for a realisation of a safety plan

2 Terms, definitions and abbreviations

The following clause summarises all definitions and abbreviation used in the deliverable. All terms are complemented by short descriptions.

2.1 Terms and definitions

Term	Definition	Reference
Assessment	The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product.	EN 50126
Audit	A systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives.	EN 50126
Hazard	A condition that could lead to an accident.	EN 50129
Hazard log	The document in which all safety management activities, hazards identified, decisions made and solution adopted, are recorded or referenced.	EN 50129
Independent safety assessor	A person or an entity (appointed to carry out safety assessment of a system) with a degree of independence from the system design/project organisation. The degree of independence must be appropriate to the required safety integrity for the system.	EN 50126-2
Public	Persons who are inside of the boundary of MODURBAN system but not staff nor passenger.	WG45/AUGT
(Railway) Authority	The body with the overall accountability to a regulator for operating a (railway) system.	EN 50126
(Railway support) Industry	Generic term denoting supplier(s) of complete (railway) systems, their sub-systems or component parts.	EN 50126
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.	EN 50126-2
Safety	Freedom from unacceptable level of risk of arm.	EN 50129
Safety acceptance	The safety status given to a product by the final user.	EN 50129
Safety approval	The safety status given to a product by the requisite authority when the product has fulfilled a set of predetermined conditions.	EN 50129
Safety authority	The body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements. Compare EN 50126: Safety regulatory authority - Often a national government body responsible for setting or agreeing the safety requirements for a railway and ensuring that the railway complies with the requirements.	EN 50129
Safety case	The document demonstrating that the product complies with the specified safety requirements.	EN 50129



Term	Definition	Reference
Safety integrity	The ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period of time.	EN 50129
Safety integrity level	A number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures.	EN 50129
Safety plan	The implementation details of how the safety requirements of the project will be achieved.	EN 50129
Safety process	The series of procedures that are followed to enable all safety requirements of a product to be identified and met.	EN 50129
Technical safety report	Documented technical evidence for the safety of the design of a system/sub-system/equipment.	EN 50129
Validation	The activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements.	EN 50129
Verification	The activity of demonstration, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements.	EN 50129

2.2 Abbreviations

Abbreviation	Definition
ALARP	As low as reasonable practicable
BOSTrab	Bau- und Betriebsordnung für Strassenbahnen (German federal regulations on the construction and operation of light rail transit systems)
CENELEC	Comité européen de normalisation electrotechnique (european committee for electrotechnical standardisation)
EN	European standard
EMC	Electromagnetic compatibility
ESM	Engineering safety management
ETA	Event tree analysis
FMEA	Failure mode and effects analysis
FRACAS	Failure reporting and corrective action system
FTA	Fault tree analysis
GAME	Globalement au moins equivalent (globally at least equivalent)
GOA	Grade of automation
GSN	Goal structuring notation
HAZOP	Hazard and operability analysis
HMI	Human machine interface
ISA	Independent safety assessor
ISO	International organization for standardization
MGS	Mindestens gleiche Sicherheit (at least identical level of safety)
MTBF	Mean time between failures
MTTR	Mean time to repair
OCC	Operations control centre
PHA	Preliminary hazard analysis
RA	Railway authority (operator)
RAM	Reliability, availability, maintainability
RAMS	Reliability, availability, maintainability, safety
RSI	Railway support industry (supplier)
RSSB	Railway safety and standards board
SIL	Safety integrity level
SRA	Safety regulatory authority
THR	Tolerable hazard rate
TSR	Technical safety report
US	United States

3 The conception of a safety plan

This clause shall introduce the idea and the conception of a safety plan. This is done by providing background information on the system lifecycle. Subsequently, the question is highlighted: what is a safety plan? Finally, the actual way of the implementation of a safety plan is outlined.

3.1 Introduction – background

First of all, the system lifecycle for railway systems shall be introduced. This lifecycle can be applied to urban guided rail systems as well, and shall be the foundation of this deliverable. The system lifecycle is recommended by CENELEC standards such as EN 50126 and has been proven as an orientation during the realisation of railway and metro projects (confer to [01]¹ as an example).

For this purpose the following figure presents the system lifecycle according to EN 50126 in a “V”-model representation. Figure 1 illustrates the various steps of a transportation system which have to be passed through its lifecycle. It comprises planning, design, implementation and the actual operation of a system, divided into grades of e.g. “concept”, “system definition”, etc. In a railway application, firstly, system requirements shall be established to define the customer needs. This is done via a system definition and a hazard and risk analysis. On the basis of these requirements a supplier shall be able to design and implement the required system. Finally, the customer accepts the system for operation and maintenance. At the end of the lifecycle, the system shall be decommissioned.

¹ This article about the metro of Copenhagen describes among other things the experience gained from the use of the application of EN 50126.

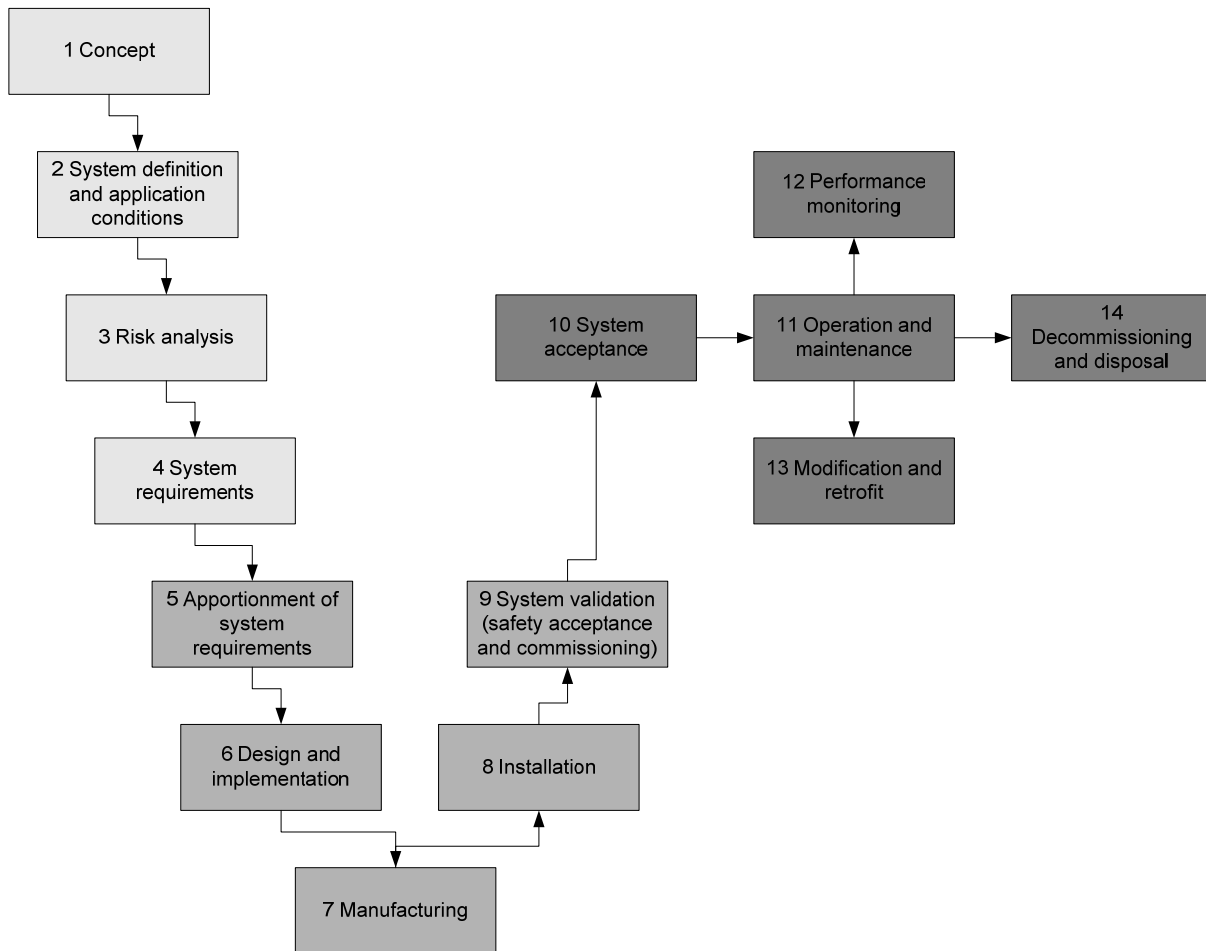


Figure 1 – System lifecycle according to EN 50126

Additionally, a table is provided with recommended safety tasks according to the system lifecycle phases. Since a safety plan shall schedule most of these tasks, they are shown in Table 1. However, these safety tasks are a recommendation of EN 50126. For each individual system or project, safety related tasks shall be adjusted according the required needs of the customer. Admittedly, this table excludes phase related general tasks and RAMS related tasks, which are part of the original figure 9 of EN 50126.

On the basis of the recommended system lifecycle and some examples of phase related safety tasks, the actual conception of the safety plan shall be presented.

Table 1 – Project safety related tasks according to EN 50126

Lifecycle phase	Phase related safety tasks
1 – Concept	<ul style="list-style-type: none"> ▪ Review previously achieved safety performance ▪ Consider safety implications of project ▪ Review safety policy and safety targets
2 – System definition and application conditions	<ul style="list-style-type: none"> ▪ Evaluate past experience data for safety ▪ Perform preliminary hazard analysis ▪ Establish safety plan (overall) ▪ Define tolerability of risk criteria ▪ Identify influence on safety of existing infrastructure constraints
3 – Risk analysis	<ul style="list-style-type: none"> ▪ Perform system hazard and safety risk analysis ▪ Set-up hazard log ▪ Perform risk assessment
4 – System requirements	<ul style="list-style-type: none"> ▪ Specify system safety requirements (overall) ▪ Define safety acceptance criteria (overall) ▪ Define safety related functional requirements ▪ Establish safety management
5 – Apportionment of system requirements	<ul style="list-style-type: none"> ▪ Apportion system safety targets and requirements: <ul style="list-style-type: none"> - specify sub-system and component safety requirements - define sub-system and component safety acceptance criteria ▪ Update safety plan
6 – Design and implementation	<p>Implement safety plan by review, analysis, testing and data assessment, addressing</p> <ul style="list-style-type: none"> ▪ Hazard log ▪ Hazard analysis and risk assessment ▪ Justify safety related design decisions ▪ Undertake programme control, covering: <ul style="list-style-type: none"> - Safety management - Control sub-contractors and suppliers ▪ Prepare generic safety case ▪ Prepare (if appropriate) generic application safety case
7 – Manufacturing	<ul style="list-style-type: none"> ▪ Implement safety plan by review, analysis, testing and data assessment ▪ Use hazard log
8 – Installation	<ul style="list-style-type: none"> ▪ Establish installation programme ▪ Implement installation programme
9 – System validation (including system acceptance and commissioning)	<ul style="list-style-type: none"> ▪ Establish commissioning programme ▪ Implement commissioning programme ▪ Prepare application specific safety case
10 – System acceptance	<ul style="list-style-type: none"> ▪ Assess application specific safety case
11 – Operation and maintenance	<ul style="list-style-type: none"> ▪ Undertake on going safety centred maintenance ▪ Perform on going safety performance monitoring and hazard log maintenance
12 – Performance monitoring	<ul style="list-style-type: none"> ▪ Collect, analyse, evaluate and use performance and safety statistics
13 – Modification and retrofit	<ul style="list-style-type: none"> ▪ Consider safety implications for modification and retrofit
14 – Decommissioning and disposal	<ul style="list-style-type: none"> ▪ Establish safety plan (for decommissioning and disposal) ▪ Perform hazard analysis and risk assessment ▪ Implement safety plan

3.2 Definition and purpose of a safety plan

3.2.1 Definition of a safety plan

When initiating a project in terms of design and commissioning of a completely new transportation system or a major change to an existing system, all duties and responsibilities have to be planned. Besides all financial and managerial tasks, safety shall be planned and a corresponding organisation has to be defined. However, before conducting any safety activity every organisation must plan all safety activities before carrying them out. (Compare fundamentals from volume 1 of the ESM Yellow Book [02].) The document that schedules safety roles and activities and presents the possible means for its realisation is usually called safety plan².

A safety plan aims at planning or referencing all activities throughout the system lifecycle regarding the definition, achievement, maintenance and proof of safety of a product. In general, this includes a description of safety-relevant activities, a schedule of responsibilities and requirements on the documentation. This is complemented by a determination of safety milestones and a description of a process of steps for approval and acceptance (compare [03]³).

Additionally, to provide a full understanding of the definition of a safety plan, the European standard EN 50126 shall be applied; it defines a safety plan in the following manner:

- *“A safety plan is a documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project.”*

Additionally, the ESM Yellow Book states:

- *“The safety plan is a document detailing activities to be carried out, and responsibilities of people to ensure the safety of work being carried out.”*

Similar to both definitions is the emphasis on the description of safety activities and roles and responsibilities to realise these activities. Therefore, these topics are a major focus of this deliverable.

The following figure concludes the main elements of a safety plan for the system lifecycle. On a superior level the safety plan shall describe safety roles and activities for the overall system lifecycle, which can be seen as a framework to achieve safety. Within this framework safety activities shall be performed.

² The terms system safety programme plan, system assurance programme plan or safety management plan are used for a safety plan alternatively.

³ This article describes RAMS management activities throughout the lifecycle according to CENELEC standards.

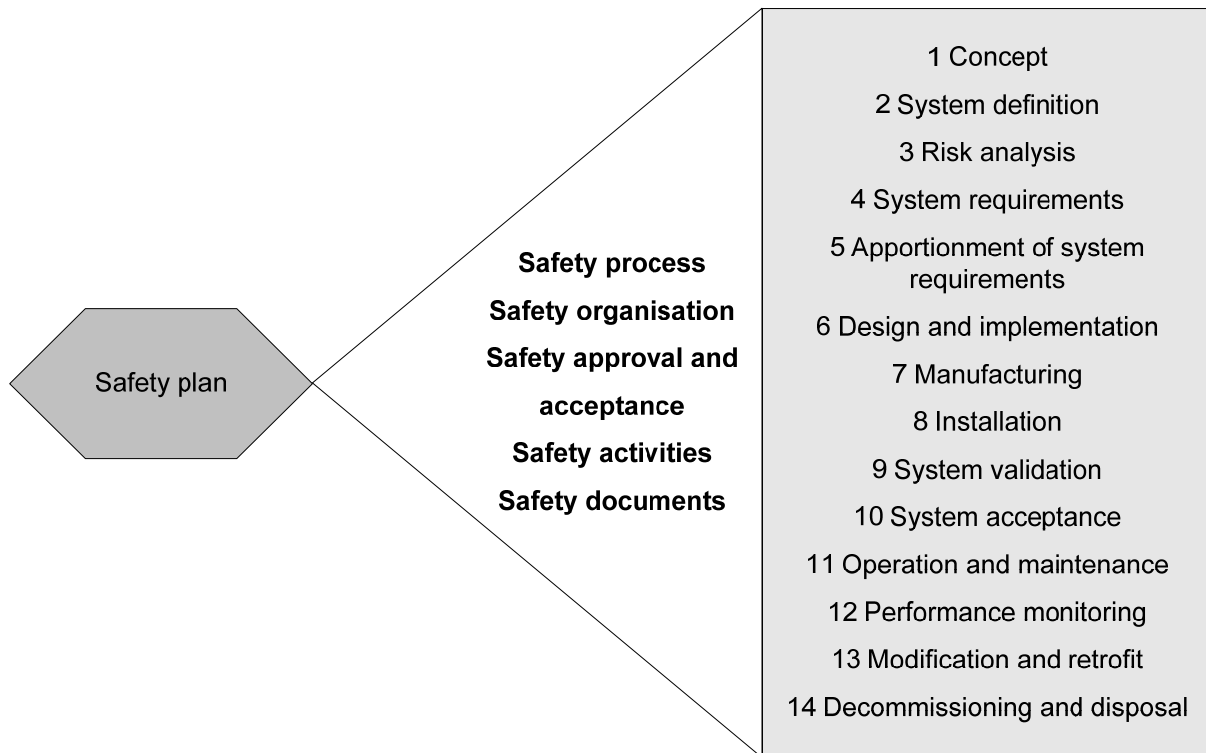


Figure 2 – Purpose of a safety plan

Since a safety plan shall schedule such fundamental safety roles and activities it can be seen as a project kick-off document i.e. an early lifecycle planning artefact. If the activities and responsibility structures, described in the safety plan, are implemented correctly, it will provide confidence in the ability to achieve compliance with initially specified requirements.

Regarding the legal status and meaning, a safety plan is highly recommend for all types of projects - following the CENELEC standards. Even the review of the safety plan is “*highly recommended*” by EN 50129 for systems which shall be realised according to SIL 1 – SIL 4. Additionally, a safety plan can be seen as “*it is also a good barometer to measure the commitment to safety of the project management team*” [04].

3.2.2 The safety plan in the system lifecycle

The development and realisation of a safety plan runs down several steps, this is illustrated in the following table. Table 2 collects a selection of steps a safety plan shall pass through in a system lifecycle. Moreover, it describes the lifecycle of a safety plan from the early establishment of a preliminary safety plan until its actual implementation.

The establishment of the safety plan shall fall into the responsibility of the operator since (a) the safety plan is recommended to be established in lifecycle phase two and (b) the operator is recommended to be responsible for the phase two. Alternatively, if a supplier is involved early in the lifecycle the supplier might establish a safety plan.

After the establishment and a continuous review and updating, the safety plan shall be implemented by review, analysis, testing and data assessment on e.g. the hazard log, hazard and risk analysis, design and safety case, etc. – this is recommended at the beginning of lifecycle phase six.

Table 2 – Safety plan in the system lifecycle

Lifecycle phase	Role of safety plan
1 – Concept	Review and evaluation of safety plans of previous projects
2 – System definition and application conditions	Establishment of preliminary and overall safety plan Assessment of adequacy of safety plan
3 – Risk analysis	Updating of safety plan
4 – System requirements	Updating of safety plan
5 – Apportionment of system requirements	Review and update the safety plan Production of an updated safety plan Verification of revised safety plan
6 – Design and implementation	Review and update the safety plan Implementation of safety activities and management of safety plan
7 – Manufacturing	Review and update the safety plan Implementation of safety activities and management of safety plan
8 – Installation	Update the safety plan Implementation of safety activities and management of safety plan
9 – System validation (including system acceptance and commissioning)	Update the safety plan Implementation of safety activities and management of safety plan
10 – System acceptance	Update the safety plan Implementation of safety activities and management of safety plan
11 – Operation and maintenance	Implementation of safety activities and management of safety plan
12 – Performance monitoring	Implementation of safety activities and management of safety plan
13 – Modification and retrofit	Implementation of safety activities and management of safety plan
14 – Decommissioning and disposal	Establishment and implementation of safety plan for the purpose of decommissioning and disposal

After the description of necessary background information about the system lifecycle and its associated safety related tasks and a general introduction to the conception of a safety plan, the actual elements of a safety plan are illustrated in the subsequent clause.

4 Content of a safety plan

The following clause aims at describing elements which shall be part of a safety plan. Firstly, a safety plan shall include an introduction to the safety plan itself as well as a description of the system or project. Secondly, delineations for a safety process, including e.g. safety organisation and safety documentation are presented. Subsequently, steps for system design and certification as well as its according approval are outlined. Finally, system demonstration and the system acceptance are described.

4.1 Introduction

4.1.1 Aim and purpose of a safety plan

A first element of a safety plan shall be the provision of the reason why this document is being written. This shall embrace a statement about the importance of safety to the overall system including all aspects of the lifecycle from concept until decommissioning.

Safety must be achieved for transportation systems. Therefore, a safety plan shall detail the global aim of the plan which shall be established. This implies the target to establish safety throughout the system lifecycle i.e. the protection of health and safety for engineers, workforce, passengers and members of public throughout the lifecycle. This might be refined by defining further essential safety goals e.g. the prevention of collisions and derailments.

Subsequently, the policy and strategy by which safety can be achieved shall be mentioned. For example, within the introduction of a safety plan it shall be mentioned that the safety plan contains contents concerning the establishment of safety organisation, safety process and activities as well as safety relevant documents.

Additionally, the first section of a safety plan shall give information about possible assumptions and constraints to the project or system. Therefore, a safety plan shall assign and state the domain and the context to which it is dedicated to e.g. the overall system or a particular sub-system. The scope of the safety plan concerns the participants in the system lifecycle as well. The addressees shall be determined to which a safety plan shall be dedicated to. For example, this might be the operator, safety authority or supplier. The safety plan shall determine whether this document is dedicated to the operator and its planning process only, or if the safety plan regards the supplier to ensure a safe construction. Alternatively, a safety plan might also be established for operation and maintenance issues only. Interfaces with other related programmes and plans shall be determined as well.

Furthermore, a safety plan shall state whether certain details about safety planning are given as a reference within the safety plan or are fully described in the safety plan.

4.1.2 Structure of a safety plan

This section of a safety plan shall introduce the aspired structure of the plan i.e. which safety aspects shall be covered by a safety plan. The recommended structure is:

Part 1 – introduction

Part 2 – safety process

Part 3 – safety organisation and responsibilities

Part 4 – system requirements and system design

Part 5 – system certification and approval

Part 6 – system demonstration and acceptance

4.1.3 Document control

This section of a safety plan shall describe processes for the maintenance of the safety plan document. The safety plan shall be subject to review and checks. It shall be determined whether these reviews and updates are taking place on demand or at selected time intervals e.g. prior to each lifecycle phase. For every change made to the safety plan, it shall be re-assessed and approved from the affected parties, for instance from the supplier or an independent safety assessor.

Independent of the size of the project under consideration the safety plan shall be subject to a version control management to prevent any usage of documents out-of-date and to keep track of any changes and amendments. Hence, a safety plan shall describe how a version control shall be managed.

4.1.4 Legal framework

This section of a safety plan shall identify standards and guidelines as well as the legal requirements for the particular project. It shall be clarified which law is appropriate and shall be applied, for instance in terms of European and national legislation.

Examples for guidelines for the development of urban guided rail systems are European standards like EN 50126, EN 50128 or EN 50129 etc. Moreover, the ESM Yellow Book of the RSSB [02] or US military standards like [06] might give advice and assistance for planning and construction of safety-related systems. Additional legal requirements shall be adhered, like regulations of fire protection, health and safety at work or EMC regulations etc. In addition, legal conditions and requirements which are specific to the project shall be named as well.

4.1.5 System description

This section of a safety plan shall describe the particular system which shall be designed. This might embrace a new system or a change/modification to an already existing system. It is important for the prevention of misunderstanding and a hazard identification, to describe the system in a proper manner.

A system description shall include e.g.:

- description of the system architecture (an example is pictured below),
- possible functional and operational descriptions,
- relevant interfaces within or to other systems - with respect to objects and functions.

Regarding MODURBAN, an initial system prescription and interface definitions can be found in the deliverable 122 [07].

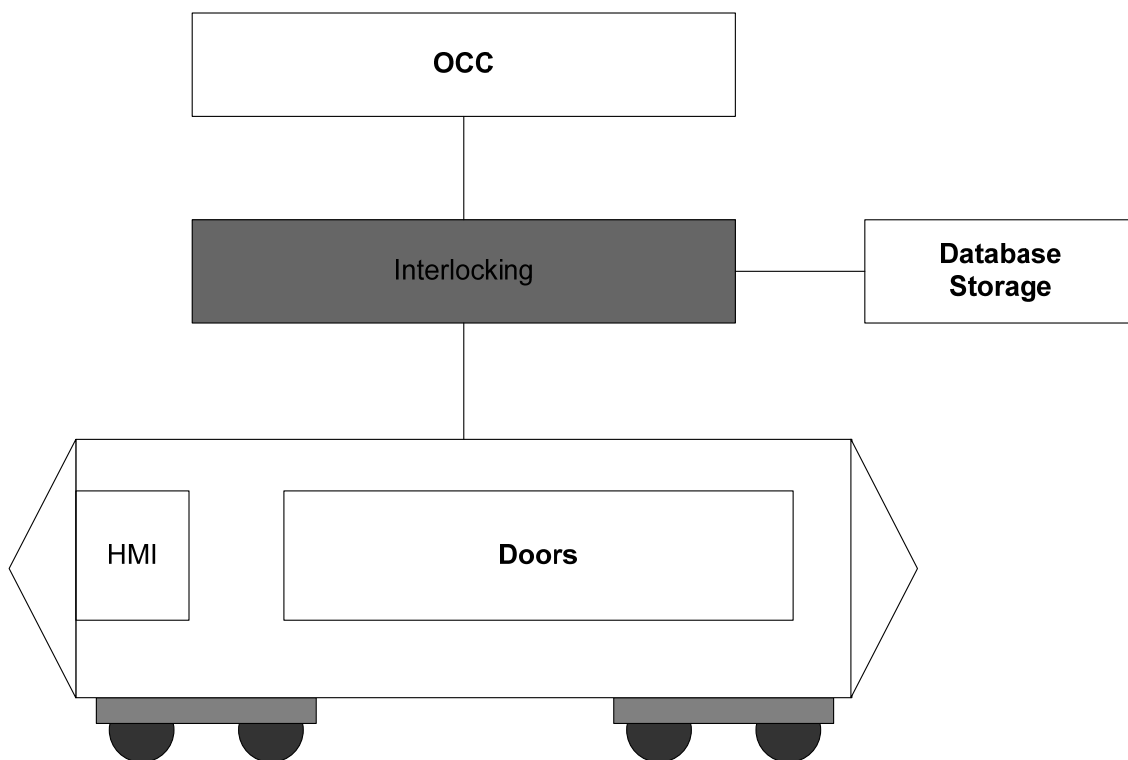


Figure 3 – Example of system architecture

4.2 Safety process

This part of a safety plan regarding safety processes, shall describe pre-requisites for safety planning which are basis for later lifecycle phases. This is done via describing general safety process steps, safety organisation and safety documentation as well as safety principles and safety acceptance processes and identifying the responsible individuals.

4.2.1 Safety process steps

This section of a safety plan shall describe steps of the safety process. One option to divide this process into steps is detailed below. In brackets there are preliminary suggestions for a breakdown of the roles and responsibilities. For a particular project the system lifecycle and its according safety related tasks and roles shall be adjusted.

Safety process steps:

- System concept (operator)
- System definition (operator)
- Establishment of safety plan (operator)
- Hazard and risk analysis (operator)
- System requirements (operator)
- Approval of system requirements (safety authority)
- Hazard control(including apportionment of system requirements) (supplier)
- System design and implementation (supplier)
- Approval of design plans (safety authority)
- System manufacturing and installation (supplier)
- Establishment of safety case (supplier)
- System commissioning and tests (operator and supplier)
- Establishment of safety assessment report (independent safety assessor)
- Approval of system (safety authority)
- System demonstration (supplier)
- Acceptance of system (operator)
- Operation and maintenance (operator)
- Performance monitoring (operator)
- Modification and retrofit (operator)
- Decommissioning and disposal (operator (and supplier))

The safety plan shall appoint safety milestones which shall be reached before any subsequent step shall begin. These milestones are for instance the design or system approval by the safety authority.

As an example, the following figure concludes the safety process steps which shall be detailed in a safety plan. The following figure might support the establishment of a safety

process for a safety plan. Figure 4 shall serve as a starting point and therefore, further details can be found in the subsequent sub-clauses.

Starting with the operator, who establishes system requirements, the supplier shall build the required system. System requirements as well as the final system shall be matter of assessment and approval. After system demonstration the operator shall accept the system. The bent arrows between operator, supplier and the independent safety assessor (ISA) shall indicate a permanent communication and exchange regarding possible reviews and audits of safety processes and documents of operator or supplier. Non-solid arrows shall describe the route of the safety case (confer to sub-clause 4.4.1).

Figure 4 represents an idealised safety process with respect to the tasks of an operator. Alternatively, the supplier might perform major parts of the system lifecycle phases.

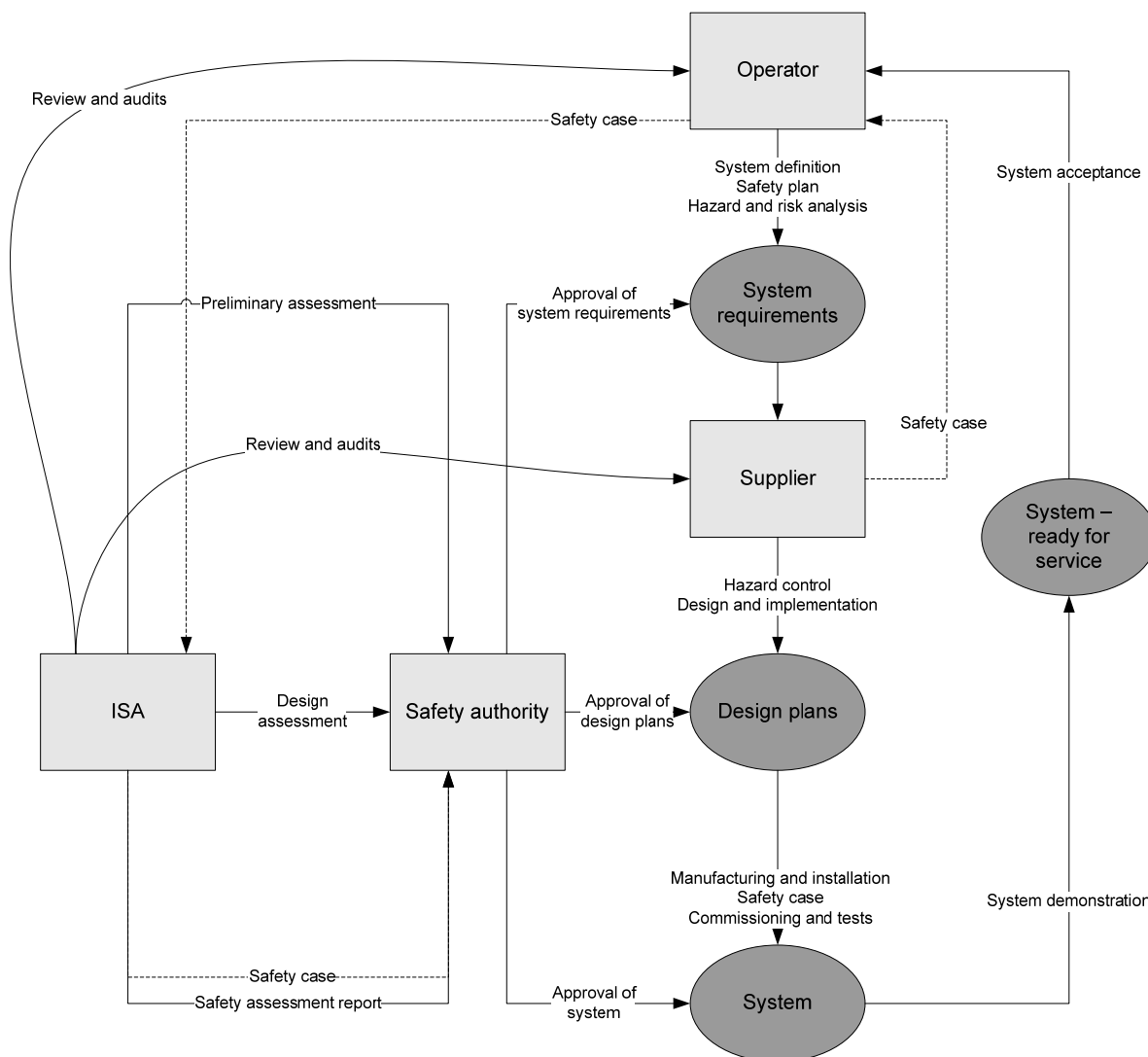


Figure 4 – Example of safety process

A safety plan requires a more detailed description of the safety roles. Therefore, further details concerning the safety participants are given in the following sub-clause.

4.2.2 Safety organisation

This section of a safety plan shall outline the responsibilities which are involved in the safety process. The purpose to describe these safety tasks and roles is to assign responsibilities and to identify the responsible individuals in the respective organisations, to avoid later uncertainties regarding the realisation of a safe system.

For the purpose of providing an example, safety roles and responsibilities shall be defined on a generic level. However, the safety approval process varies within the European Union, in terms of an actual implementation and labelling of safety tasks and functions.⁴ However, key roles can be defined as examples, which contribute to safety of the project and the final system acceptance. For national details refer to [08] and [09]. These documents compare different national safety approval processes. For an actual establishment of a safety plan national approval procedures have to be considered and shall be described in the safety plan.

As a minimum, four participants shall be described and are shown on the left hand side of Table 3. This table provides additional equivalent terms of the duty holders to prevent mistakes.

Table 3 – Example of responsibilities in the safety process

Role	EN 50126	EU safety directive	Abbreviation
Operator	Railway authority	Infrastructure manager Railway undertaking	RA
Supplier	Railway support industry	Supplier Manufacturing industry	RSI
Safety authority	Safety regulatory authority	Safety authority	SRA
Independent safety assessor	---	---	ISA

Regardless of the specific task, all safety participants shall be sufficiently experienced and competent for their safety task. A safety plan shall show how competence in terms of education and training for staff and engineers is assured for all planning processes as well as operation and maintenance. Any organisation of safety responsibilities shall be realised according to quality standards like EN ISO 9001, EN ISO 9002 and EN ISO 9003, appropriate CENELEC standards (e.g. EN 50129) and site specific conditions and guidelines of the particular company. The safety plan shall reference to, or justify directly, the competence for the safety responsibilities as well as the applied rules for quality management. A quality management plan shall be established.

⁴ For example, in [10] the difficulty is explained to find an approval process for Germany - between European standards like EN 50129 and the relevant transportation acts like BOStrab (which is the German ordinance on the construction and operation of rail systems for light-rail transit).



Furthermore, the safety plan shall give information about the independence of the different roles within a company. Following EN 50129, the level of independence shall depend on the implementation type of the safety integrity level (see Figure 6).

Additionally, a safety plan shall outline a process for the establishment of a company wide safety culture, which shall cultivate the commitment to safety, general competence and an awareness of risk.

4.2.2.1 Operator

The safety plan shall outline the role of an operator in the system lifecycle. For this reason the operator is described in more detail. The operator shall hold the responsibility for the starting phases in the system lifecycle. In particular the operator shall perform tasks which are related to the lifecycle phase one until four (as recommended in EN 50126). After system definition, hazard and risk analysis, establishment of a hazard log, the operator shall produce system requirements. System requirements shall specify the needs of the operator for the aspired system on a functional level and contain in particular the safety requirements. These requirements shall be the input and basis for a supplier for the design and construction of the system.

For the purpose of establishing system requirements the operator shall nominate a safety manager. The safety plan shall indicate whether this is an internal safety manager (employed by the operator) or an external safety manager i.e. an external company is entrusted with safety management tasks (e.g. for a risk analysis or safety requirements validation). Especially for rather small operators (in terms of e.g. number of employees or annual turnover) it might be an advantage to involve the supplier at the beginning of lifecycle phase two or three. This might be due to a lack of manpower or competence of the operator (compare [11] regarding signalling systems for regional infrastructure⁵). In every case the safety plan must identify who is responsible for which task.

Additionally, the operator shall incorporate the safety authority and an independent safety assessor into the planning procedures. The safety plan shall state how safety authority and assessor shall be involved in the establishment of documents regarding reviews or audits of e.g. risk analyses or system requirements. This shall be done in order to be consistent with national law or European standards to prevent the operator from misunderstanding and subsequent changes to the already created documents and requirements.

Concerning the final safety case or safety report (see sub-clause 4.4) it shall also be noted that the full safety case requires not only safety proofs for the technical equipment but also acceptance of the “exported” risks from the technical system supplier back to the operator (e.g. requirement of processes in degraded modes, resetting procedures etc. involving

⁵ This article describes the difficulty for small and regional operators to conduct lifecycle phases one till four. It suggests entrusting an external party or the supplier with the requirements development process.

operator's staff). It is therefore a task of the operator to provide an operationally-technical safety analysis showing the interfaces and maintaining the framework hazard log with all possible emerging hazards that must ultimately be closed.

Also, should a MODURBAN system be procured in sub-lots, then it is the obligation of the operator to control the safety of the interfaces and the related integration tasks. Furthermore, one supplier could take the responsibility of integration of the different sub-lots according to the clause of the initial call for tender issued by the operator. In turnkey full system procurements this task becomes the supplier's task. In lot by lot procurements the task may be delegated to the supplier (if he acknowledges reception and responsibility of this task).

The safety plan shall for all MODURBAN like projects contain a paragraph where this particular issue is addressed.

4.2.2.2 Supplier

Within a safety plan the responsibilities of a supplier shall be described. The supplier shall be responsible for design and construction of the system. Following the recommendations of EN 50126 the supplier holds responsibility for the lifecycle phases five till nine (compare Figure 1). The major inputs for the supplier are the system requirements, established by the operator. These requirements shall be continuously reviewed to guarantee its full consideration and correct realisation.

A nominated safety manager and identified engineers shall be in charge of the system design and the concurrent safety activities. The supplier holds full liability for the system and its safety, even when a sub-system is produced by sub-contractors. Due to the system liability the supplier shall entrust an independent safety assessor with the assessment of design and actual construction of the system. The ISA shall be subject to approval by the safety authority and by the operator. Safety assessment shall in general not affect the internal verification and validation of the supplier. To demonstrate safety of the system, the supplier shall establish a safety case (for more details refer to sub-clause 4.4). The safety case shall be assessed by the independent safety assessor and can be seen as a basis for system approval by the safety authority.

As an example, the following figure aims to give an organisational structure of safety roles of operator and supplier. The central points of this figure are the two safety managers of the operator and the supplier. The latter is supported by team of independent verification and validation engineers as well as a design team. Between all three parties interfaces and communication shall exist. Additionally, both the safety managers and the safety authority shall establish a means of continuous communication.

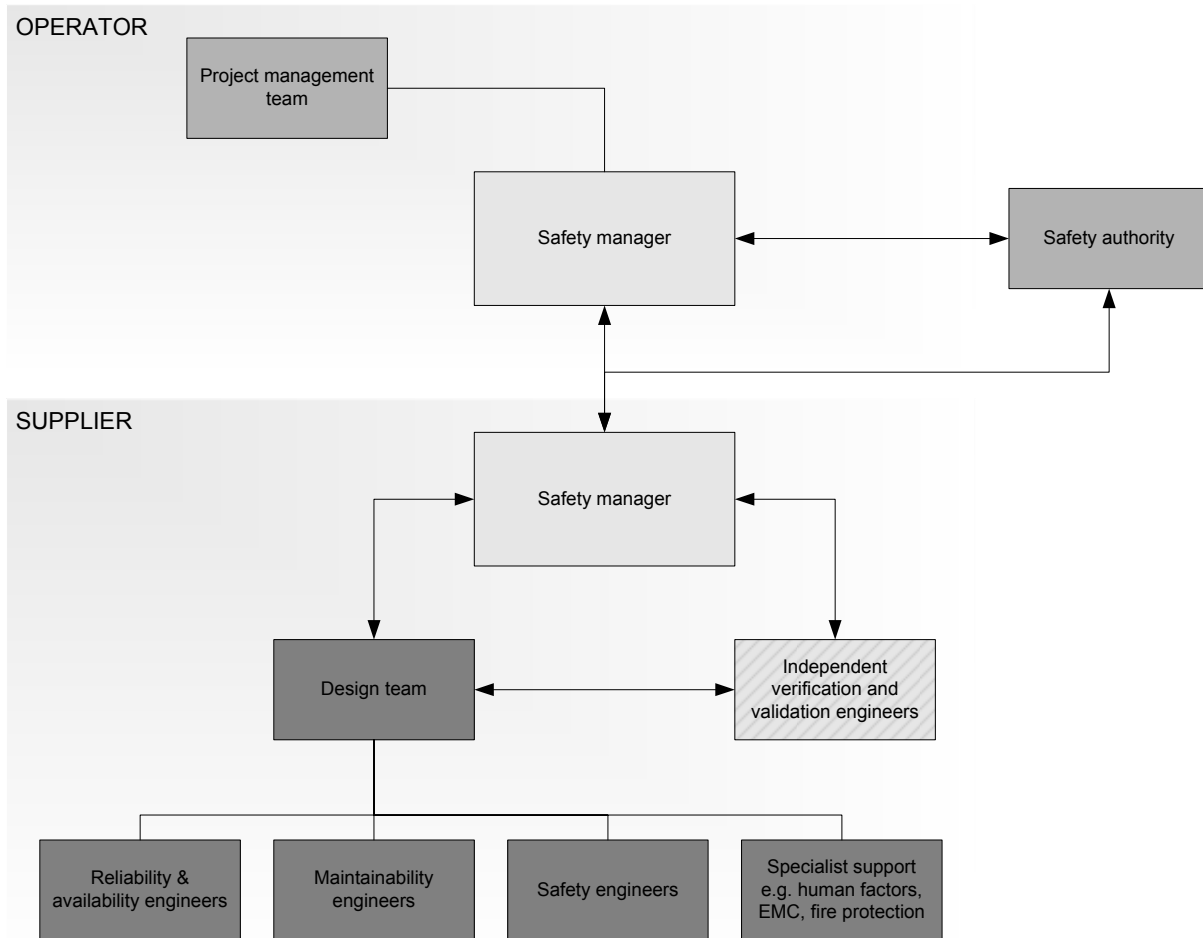


Figure 5 – Example of a structure of safety roles

4.2.2.3 Safety authority

Within a safety plan the role of the safety authority shall be explained. A governmental/national or local body e.g. a supervisory authority shall be responsible for design approval and system approval. The safety plan shall detail the correct and responsible safety authority for the project under consideration. The safety authority shall approve all documents within the lifecycle.

While EN 50126 speaks of “railway authority” this document uses the term as an equivalent to the respective “ultimate approving authority” for urban guided transport projects, which are often national or local governmental organisations different to the railway authority. Every MODURBAN like realisation project shall identify the entity that plays the equivalent role of this authority; failure to do so means the safety plan would be incomplete.

Furthermore, the safety plan shall state how the safety authority will support the operator in its planning process e.g. by providing risk acceptance criteria or document assessment.

4.2.2.4 Safety assessor

Subsequently, the safety plan shall determine the role and task of an independent safety assessor. The activities of an independent safety assessor shall cover the review, audit and assessment of documents – produced during the lifecycle – and the actual system. An independent safety assessor shall compile judgement and recommendation in order to evaluate whether national/legal requirements or European standards or quality and safety requirements have been met.

The ISA can be employed internally or externally to a company i.e. by operator or supplier. However, the independent safety assessor shall be impartial to ensure that the assessment is unbiased and of proven independence. The independence applies to all tasks of the supplier's design teams as well as the operator's team. Arrangements for the independence of the safety assessor, according to the aspired safety integrity level of the system, are described in figure 6 of EN 50129 (refer to Figure 6 of this document).

Every assessment shall be performed by qualified safety experts acceptable to the authority and to the supplier on their individual and personal profile.

The safety plan shall state who appoints the independent safety assessor, for example, operator or safety authority and what the tasks for independent safety assessors are, e.g. list of documents to be assessed and schedule of audits and remuneration of the ISA.

Regarding the establishment of a safety plan, the Yellow Book Application Note for an Independent Safety Assessment of the Yellow Book recommends the following: *“For instance, in respect of the Safety Plan the ISA could support that the processes detailed in the Safety Plan were satisfactorily carried out. Alternatively, or indeed additionally, the ISA could support that the Safety Plan is fit for the system being developed.”* [12].

As conclusion of the statements made in sub-clause 4.2 about the safety process, a table with safety roles and its according activities is provided in the following sub-clause (see sub-clause 4.2.2.5).

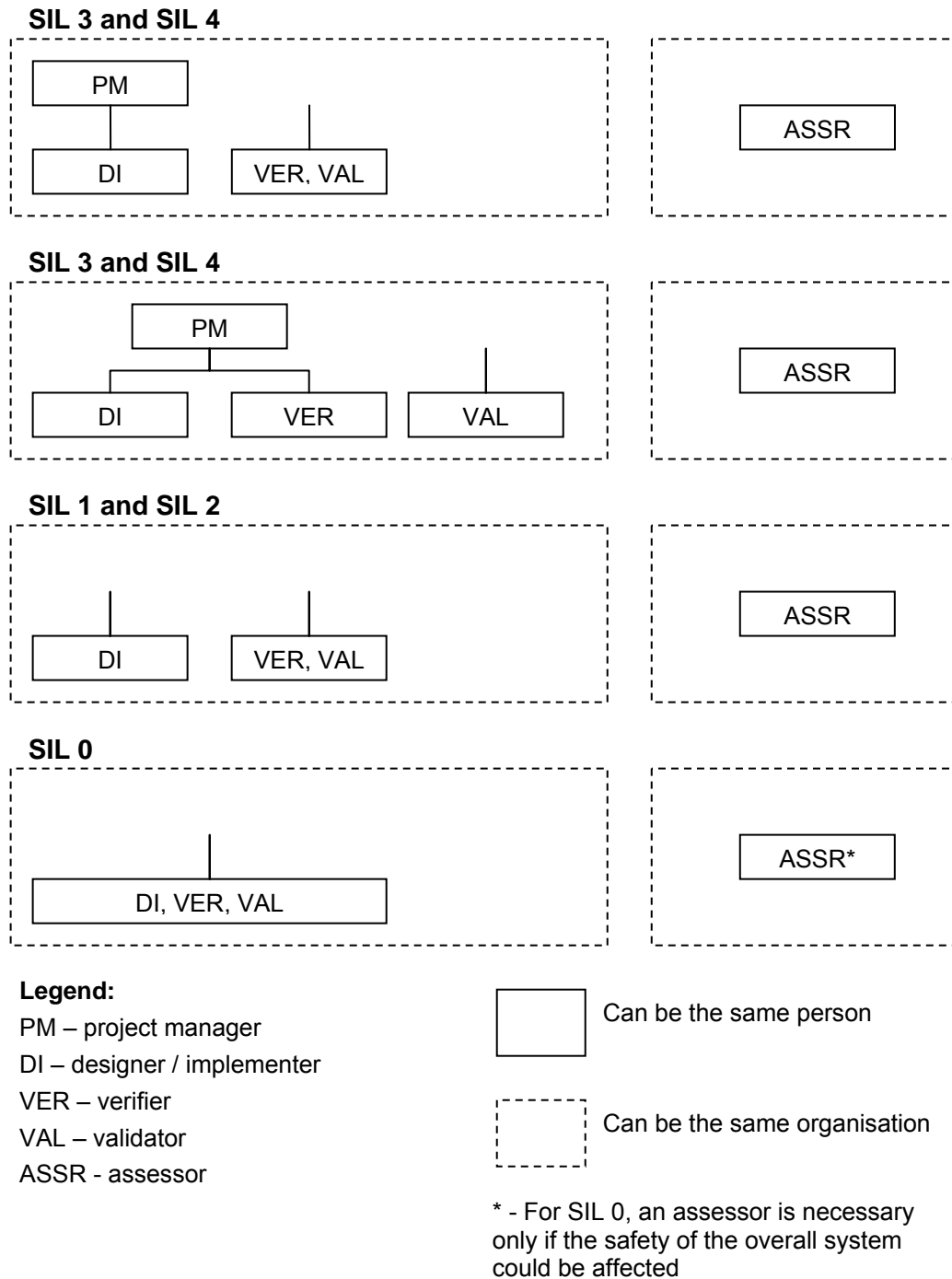


Figure 6 – Arrangement for independence according to EN 50129

4.2.2.5 Summary - the safety process and allocating responsibilities

The following table gives an exemplified summary of a safety process and allocation of responsibilities. It shows a selection of necessary safety approval steps. Potential safety milestones like system requirements and design approval, system approval and system acceptance are highlighted in bold font. The basis of this table is mainly EN 50126.



Table 4 – Example of a safety process in the lifecycle

Lifecycle phase	Operator	Supplier	ISA	Safety authority
1 – Concept	Project/system concept Review of previous projects			
2 – System definition and application conditions	System definition Safety plan PHA Hazard log Risk criteria			Risk criteria Review of documents
3 – Risk analysis	Hazard and risk analysis		Review and audit of plans of operator	
4 – System requirements	Operation and maintenance procedures System requirements specification			Examination of documents
				Approval of system requirements
5 – Apportionment of system requirements		Causal analysis Apportionment of system requirements		
6 – Design and implementation	Operation and maintenance procedures	Hazard management (export & monitoring) Design verification Generic safety case Operation and maintenance principles	Review and audit of plans of supplier	Examination of documents
				Approval of design plans
7 – Manufacturing		Manufacturing Operation and maintenance procedures	Optional audit and assessment of activities of supplier	
8 – Installation		Installation System tests		
9 – System validation (including system acceptance and commissioning)	Safety case approval Commissioning	Application specific safety case System validation Commissioning	Audit and assessment of safety plan, hazard log and safety case and system	Examination of documents
				Approval of system
10 – System acceptance	System demonstration	System demonstration	Consistency check of exported requirements and operational procedures	
	Acceptance of system			
11 – Operation and maintenance	Operation, maintenance, performance monitoring and modification/retrofit of system			
12 – Performance monitoring				
13 – Modification and retrofit				
14 – Decommissioning and disposal	Planning and performance of decommissioning and disposal			

4.2.3 Safety documentation

This section of a safety plan shall mention documents which shall be produced and managed during the system lifecycle. All safety activities shall be planned and documented during the lifecycle and therefore, phase relevant plans, reports and documents shall be determined. This means safety documentation shall be the notification of documents and a description of processes for the maintenance of safety-related documentation i.e. the management of documents. The documentation shall be done to provide a later foundation for the proof of a safe system and compliance with system requirements.

A list of documents shall be established which might be called a documentation plan. The documentation plan shall be either included directly in the safety plan or alternatively, a reference to the documentation plan shall be given.

As an example, the following table shall support the establishment of a documentation plan regarding safety relevant documents. For each lifecycle phase, examples for possible safety relevant documents are named. However, not every document shall be attached to a particular lifecycle phase. Documents might be established earlier or later in the lifecycle. Certain documents are established in one phase but affect the overall lifecycle, e.g. the hazard log. This depends for instance on the time of participation of the supplier or an independent safety assessor during the lifecycle. Hence, this list of documents does not contain any responsibilities, because this might be dependent on the particular project. Furthermore, every project is different in terms of age of the system, national law or degree of modernisation etc. and therefore not every document is necessarily relevant.

Not mentioned in this list of examples are verification and validation reports and safety audit reports. These reports shall be performed continuously throughout the lifecycle.

Again, this table serves as an example and might only give a broad orientation about documents in the system safety lifecycle.

Table 5 – Examples of documents in the system lifecycle

Lifecycle phase	Documents
1 – Concept	<ul style="list-style-type: none"> ▪ Conceptual documents ▪ Feasibility studies
2 – System definition and application conditions	<ul style="list-style-type: none"> ▪ Safety principles specification ▪ Preliminary hazard analysis ▪ Preliminary risk analysis ▪ Preliminary system specification ▪ Overall system specification (general, functional, RAMS) ▪ Preliminary safety plan ▪ Safety plan ▪ Documentation plan (may be included in safety plan) ▪ Safety case plan (may be included in safety plan) ▪ Quality assurance plan (may be included in safety plan) ▪ Customer development plan ▪ Configuration management plan (hardware, software) ▪ Assessment plan (system, hardware, software) ▪ Environment management plan ▪ Human factor plan ▪ Audit plan
3 – Risk analysis	<ul style="list-style-type: none"> ▪ Hazard analysis ▪ Risk analysis ▪ Hazard log ▪ Hazard owner action plan ▪ Safety log ▪ RAM log ▪ Quality log
4 – System requirements	<ul style="list-style-type: none"> ▪ System requirements specification ▪ (Final) System specification, includes system architecture description ▪ Functional and safety requirements specification ▪ RAM programme plan ▪ RAM requirements specification ▪ System acceptance plan ▪ Operational scenario plan ▪ Maintenance plan ▪ Modification management plan ▪ Communication management plan ▪ System test specification (functional, safety, other system interfaces) ▪ System safety demonstration plan ▪ Assessment reports

Table 5 - Examples of documents in the system lifecycle (continued)

<p>5 – Apportionment of system requirements</p>	<ul style="list-style-type: none"> ▪ Hazard log (supplier) ▪ Hazard management/risk export (e.g. report) ▪ Supplier development plan (system, hardware, software) ▪ Software and hardware development tools description ▪ Sub-system hazard analysis ▪ Sub-system risk analysis ▪ Sub-system specification ▪ Sub-system functional and safety requirements specification, includes system architecture for sub-systems ▪ Sub-system RAM requirements specification ▪ Sub-system test specification (functional, safety, other interfaces) ▪ System FMEA analysis ▪ System FTA analysis ▪ Hazard and operability study ▪ Report of verification of sub-system requirements and architecture ▪ RAM analysis ▪ Verification and validation plan (system, hardware, software)
<p>6 – Design and implementation</p>	<ul style="list-style-type: none"> ▪ Hardware requirements specification ▪ System design documents (functional description, safety analysis, electrical diagram, block diagram, materials list, assembly documents, test procedure) ▪ Failure test report ▪ (Operational and) Technical Safety Report according CENELEC including Safety Cases ▪ Hardware validation report ▪ Hardware-software integration test plan ▪ Hardware-software integration test report ▪ Software project management plan/reports ▪ Software quality assurance plan/reports ▪ Software development plan/reports ▪ Software coding standards ▪ Software requirements specification ▪ Software verification and validation plan ▪ Software verification and validation report ▪ Software architecture description (system and sub-system) ▪ Data preparation plan ▪ Data test plan ▪ Data test report ▪ Type test plan ▪ Type test report ▪ System/sub-system test plan ▪ System/sub-system test report ▪ Installation plan ▪ Installation manual ▪ Maintenance manual ▪ Commissioning plan ▪ Quality audits ▪ Plan for data acquisition and assessment during operation ▪ Generic safety case (may include: definition of system, quality management report, safety management report, technical safety report, related safety cases, conclusion) ▪ RAM demonstration plan ▪ Intermediate RAM report ▪ Manufacturing and inspection plan

Table 5 - Examples of documents in the system lifecycle (continued)

7 – Manufacturing	<ul style="list-style-type: none"> ▪ Test report for manufactured systems
8 – Installation	<ul style="list-style-type: none"> ▪ Installation report ▪ Customer training courses plan
9 – System validation (including system acceptance and commissioning)	<ul style="list-style-type: none"> ▪ Preliminary safety assessment report ▪ Final validation report (supplier internal document) ▪ Field validation test plan ▪ Field validation test report ▪ System demonstration plan ▪ Application safety case
10 – System acceptance	<ul style="list-style-type: none"> ▪ Functional assessment report ▪ Safety assessment report ▪ Overall assessment report ▪ Certification of homologation ▪ System demonstration report
11 – Operation and maintenance	<ul style="list-style-type: none"> ▪ Setting up of failure reporting and corrective action system (FRACAS) ▪ Preventive action plan
12 – Performance monitoring	<ul style="list-style-type: none"> ▪ Periodic test plan ▪ Final RAMS report
13 – Modification and retrofit	<ul style="list-style-type: none"> ▪ System modification plan (after homologation) ▪ RAM and safety impact analysis
14 – Decommissioning and disposal	<ul style="list-style-type: none"> ▪ Decommissioning and disposal plan

4.2.4 Safety principles

This section of a safety plan shall determine the safety principle i.e. the risk tolerability criterion which shall be applied for the assessment of risk. The risk tolerability criterion shall be the measure to identify whether risk associated with a certain hazard can be tolerated or not. Different principles for risk acceptance are used worldwide.

The notification of a safety principle shall be extended by a short description as well as an explanatory statement for the selection. Furthermore, necessary risk reduction activities shall be explained in case the risk of a hazard is intolerable or negligible. The choice of the safety principle shall be consistent with national law and in agreement with the relevant safety authority.

As an example, a selection of safety principles shall be presented. These safety principles are:

- GAME
- ALARP
- (Others)

The GAME (Globalement Au Moin Equivalent) safety principle can be formulated as follows: *“All new guided transportation systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system”* [05]. Therefore, a reference system has

to be appointed. Subsequently, the level of risk shall be compared between the system under consideration and the reference system. Equivalent is the MGS (Mindestens Gleiche Sicherheit) principle practiced in Germany that compares the level of risk of the system under consideration with a reference value. This reference value might either arise from a reference system or from national state-of-the-art technology (German: Anerkannte Regeln der Technik).

The ALARP (As Low As Reasonable Practicable) safety principle is based on a cost-benefit-analysis. It compares the costs of a safety measure with the value of the gained safety i.e. the avoided losses from an accident.

4.2.5 Approval and acceptance process

The safety plan shall describe the approval and acceptance process for the particular project i.e. the safety plan shall determine milestones for the different steps of approval and acceptance. An example for an approval and acceptance process is shown in the following procedure displayed in Table 6. (These processes are pictured in Figure 4 - page 24 - as well.)

Before the commencement of operation the system shall pass through e.g. three phases of approval. This shall include the approval of system requirements, approval of design and approval of final the system. Finally, the system shall be accepted by the operator.

Table 6 – Example of an approval and acceptance process

Project phase	Approval	Responsibility	Pre-requisites
System description and requirements	Approval of system requirements	Safety authority	System definition, hazard and risk analysis, system requirements, etc.
System design	Approval of design plans	Safety authority	Design and implementation plans, etc.
System implementation	Approval of system	Safety authority, Independent safety assessor	Safety case, safety assessment report, test reports, etc
System demonstration	Acceptance of system	Operator	Demonstration report, etc.

The first project phase – system description and requirements - might encompass lifecycle phases one till four and is finalised by an approval of system requirements by the safety authority, which is responsible for approval. This approval includes the requirements i.e. needs of the operator. Pre-requisites for an approval shall be mainly the system description, hazard and risk analysis, system requirements and recommendations of an ISA.

The final design might include the design of the actual system and these plans shall be approved. The approval of design covers the actual plans for realisation of the system. On

the basis of the approved plans the system shall be manufactured and installed. This shall cover the requirement stated in EN 50129: “*The safety authority shall approve both, risk analysis and the hazard control.*”

After system implementation, an approval shall be issued by the safety authority which covers the approval of the installed system and is based on recommendations of an ISA.

Finally, during the phase of system demonstration the system shall prove its final quality. The operator shall accept the system when all requirements are fully met.

4.2.6 Other safety relevant activities

This section of the safety plan shall describe the following additional safety management activities. These activities shall be planned in the beginning of a project and are mostly not restricted to a particular lifecycle phase and shall be applied to the overall planning and operation process.

Configuration management – The safety plan shall describe how configuration of products, functions or documents shall be identified, how change and status controlled as well as assessed. If a separate document is produced the safety plan shall give a reference to the configuration management plan.

Contractor management – The safety plan shall give information about sub-contractor or sub-supplier arrangements for when the awarded supplier employs sub-contractors. The safety management of sub-contractors shall be monitored. External items, produced or delivered by sub-supplier, shall be verified and validated, assessed and approved to ensure safety of the final system. In other words, the safety plan shall provide clear guidance for safety management of sub-contractors.

Maintenance and operation management – Regarding operation and maintenance, a safety plan shall describe a process for the establishment of procedures and manuals for the actual service. Furthermore, the safety plan shall describe a controlled method of data production for analysing operation and maintenance performance to ensure that the level safety is compliant with the requirements. This includes the handling of non-conformity events for analysis of incidents and accidents (for more details see MODURBAN deliverable 91 [13]).

Evacuation management – Regarding safe service and a safe performance of system tests, evacuation matters shall be planned. The safety plan shall describe how these evacuation procedures shall be arranged.

Modification management – In case modification and changes to the system are necessary after final system approval and acceptance, a process shall be described how modifications shall be handled. This might be in accordance to the scale of the modification, whether a full system lifecycle shall be worked through and mainly which parties and tasks shall be required for a re-approval.

Decommissioning and disposal – The safety plan shall describe how the decommissioning and disposal is planned to take place.

Miscellaneous – For contentious large scale projects it might be of advantage to regulate media appearance to reduce disturbance of the design team and to ensure a straightforward planning process. In these cases the safety plan shall describe a process for public attendance.

After a description of the safety process, which shall be applied to the overall lifecycle, the different project phases are explained in more detail.

4.3 System requirements and system design

This part of a safety plan shall describe the safety analysis and system design process. This includes the establishment of system requirements and the processes of the supplier to design a system which complies with the system requirements. In particular the safety plan shall outline the hazard identification and risk analysis, the establishment of system and safety requirements, the hazard control phase, verification and validation activities and finally, safety audits and assessments.

4.3.1 Hazard identification

This section of a safety plan shall describe methods for hazard identification and analysis. The basis for every effort regarding hazard identification shall be the previously established system definition. Within a hazard analysis all hazards, including the actual system hazards, its future operation and maintenance hazards etc., shall be identified. Moreover, the hazard analysis shall also identify the “exported” risks from the technical system back to the operator. The identified hazards shall be listed and documented.

Furthermore, a safety plan shall outline methods for hazard identification. As an example, standard EN 50129 recommends a combination of an analytical and creative phase for a systematic identification of hazards. For instance, brainstorming techniques and checklists as well as hazard and operability analyses (HAZOP) or failure mode and effects analyses (FMEA) shall be performed for hazard identification. The identification of hazards shall be extended by interface analyses including e.g. physical, functional and operational or software interfaces.

For the hazard management process a hazard log shall be established and maintained throughout the entire system lifecycle. The hazard log shall record the identified hazards (e.g. in form of a list) and shall describe measures for risk reduction as well as its responsibilities. The safety plan shall determine how hazard logs shall be managed since operator, supplier or sub-contractor might establish individual hazard logs. Moreover, the safety plan shall describe methodologies, for instances that a hazard is identified and no

responsibility can be determined or an identified hazard shall be transferred or exported to another responsibility.

As an example, the preliminary hazard log for the MODURBAN project shall be mentioned, this is described in the MODURBAN deliverable 127 [14]. This hazard log is realised in form of a Microsoft Excel sheet. It contains examples of hazards, its associated risk, responsibilities and possible measures for risk reduction.

4.3.2 Risk analysis

This section of a safety plan shall outline processes for the analysis of risk. This analysis applies to technical as well as human failures. Once hazards are identified, their associated risk shall be assessed in order to understand whether risk can be accepted or further action has to be taken to reduce risk.

First of all, the consequences and characteristics of a hazard shall be analysed and estimated. For example, event tree analyses (ETA) or markov-models shall be applied.

Secondly, this section of a safety plan shall give information about how risk shall be assessed and which methods shall be applied. As an example, a selection of methods for risk assessment is shown below (further detail can be found in [22]).

- Risk priority numbers – This method tries to assess risk by defining priority numbers for the severity of hazard consequences and the likelihood of its occurrence. Afterwards these numbers are added or multiplied to derive a level of risk.
- Risk matrix – This method is recommended in EN 50126 and embraces a qualitative description of severity, likelihood and the associated risk. The risk parameters are connected within a matrix.
- Risk graph – Through a graphical chart risk shall be assessed, considering the severity, likelihood, exposure and defence against consequences.
- Risk formula – Risk is assessed through a mathematical combination of several risk factors like severity, exposure, likelihood, latency period, reduction factors etc.
- MODURBAN method – For the purpose of urban guided rail system the MODURBAN project recommends a method for risk analysis. This is described in the MODURBAN deliverable 86 [15]. This semi-quantitative method is based on a combination of four risk factors. These are; severity of consequences, exposure probability of hazard, accident probability and consequence reduction.

Attention shall be paid to systems where human-machine-interfaces must be considered. To understand and support a risk assessment based on human factors, the MODURBAN deliverable 128 shall be mentioned. This deliverable presents a “methodology that evaluates the probability of human errors in urban train driving procedures” [24].

4.3.3 System requirements

This section of a safety plan shall describe the approach for the establishment of system requirements. Requirements shall be established, for instance regarding system definition, operational and functional issues, on reliability, availability, maintenance and safety. These requirements shall be expressed as RAMS requirements for the overall system (for example in accordance with EN 50126).

System requirements shall be defined on system level and shall be expressed as e.g. mean time between failures (MTBF) for reliability, delay times in minutes or hours for availability, mean time to repair (MTTR) for maintainability and safety integrity levels (SIL) for safety.

The safety plan shall describe or reference to a RAMS programme. Demonstration and acceptance criteria as well as the monitoring for RAMS requirements shall be documented within this programme.

Safety requirements shall be established by defining requirements on functions which shall act as a risk reduction measure for hazards with unacceptable risk.

4.3.4 Safety requirements

This section of a safety plan shall describe how quantitative safety requirements i.e. safety targets shall be defined. The concept of safety integrity levels (SIL) shall be applied to express safety requirements for system or sub-systems functions, hardware or software. The dimensioning of the SILs shall be in accordance with the results of hazard and risk analysis. These analyses yield tolerable hazard rates (THR) for the analysed hazards. For the apportionment of THRs to system functions and according SILs, Table 7 shall serve as an example.

Table 7 – THR and SIL table according to EN 50129

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

The apportionment of safety requirements to actual functions and the subsequent design shall be supported by an on-going review, assessment and maintenance of the adequacy of the safety requirements. Special attention has to be paid to functions which are not continuously used e.g. functions for fire protection. A hazard and risk analysis for these on-demand functions shall rather serve as an indicator for safety requirements.

As an example, Table 8 shows a selection of MODURBAN safety functions and its according suggestion for safety integrity levels. These SILs are derived from a risk analysis documented in the MODURBAN deliverable 86 [15].

Table 8 – Examples of MODURBAN safety functions - including possible SIL allocation

Safety function	Safety integrity level			
Train integrity supervision	SIL 4			
Train door status supervision	SIL 4			
Absolute train location measurement	SIL 4			
Relative train location measurement	SIL 4			
Speed determination/calculation	SIL 4			
Over-speed detection	SIL 4			
Travel direction measurement (GOA 1b,2)		SIL 3		
Travel direction measurement (GOA 3,4)	SIL 4			
Train side determination (left/right)	SIL 4			
Train length	SIL 4			
Platform doors in normally crowded operations		SIL 3		
Train door obstruction detection			SIL 2	
...				

If a safety integrity level cannot be allocated, for instance to systematically hazardous behaviour of staff, procedures or manuals shall be produced as mitigation. For example, this applies to operation or maintenance issues.

After successful establishment of system definition, performance of hazard and risk analysis and the final specification of system requirements, the safety authority shall express a statement. For example, the safety authority shall examine or approve the established plans and documents. Additionally, documents shall be reviewed by an independent safety assessor.

4.3.5 System design

This section of a safety plan shall describe approaches for the actual system design and implementation. This shall include the hazard control phase i.e. causal analysis of hazards and the apportionment of system requirements to safety functions as well as the system design and implementation (including hardware and software). These activities shall result in final system description i.e. final design plans.

Regarding hazard or causal analysis the safety plan shall describe approaches and techniques for its conduction. As an example, in [16] the fault tree analysis (FTA) and markov-models are recommended for an analysis of hazard causes.

Subsequently, requirements shall be apportioned and refined for the system, sub-system and equipment until the final design is reached. Furthermore, the safety plan shall describe a hazard management process i.e. an iteration of risk assessment and hazard control to determine whether risk has been reduced effectively by the taken actions.

Regarding software requirements, the safety plan shall reference to EN 50128 [17]. This European standard describes processes to achieve software requirements.

During design of hardware and software safety techniques, practices, material selections etc. shall be employed such, that all design entities respect the corresponding safety characteristics (derived from the safety requirements).

Additionally, the safety plan shall determine a process to establish an on-going review of the system requirements whether all requirements have been met or further analysis is necessary. This shall be documented in a RAMS programme report or a system assurance report.

Finally, the safety authority shall provide a statement about the final design created by the system supplier. For example, the safety authority shall examine or approve the established final plans and documents. Additionally, documents shall be reviewed by an independent safety assessor.

4.3.6 Verification and validation

This section of a safety plan shall delineate processes and arrangements for verification and validation activities during the system lifecycle. Verification and validation shall be performed according to the recommendation given in EN 50126. The recommendation is pictured in the “V” – model representation, e.g. in the figure below.

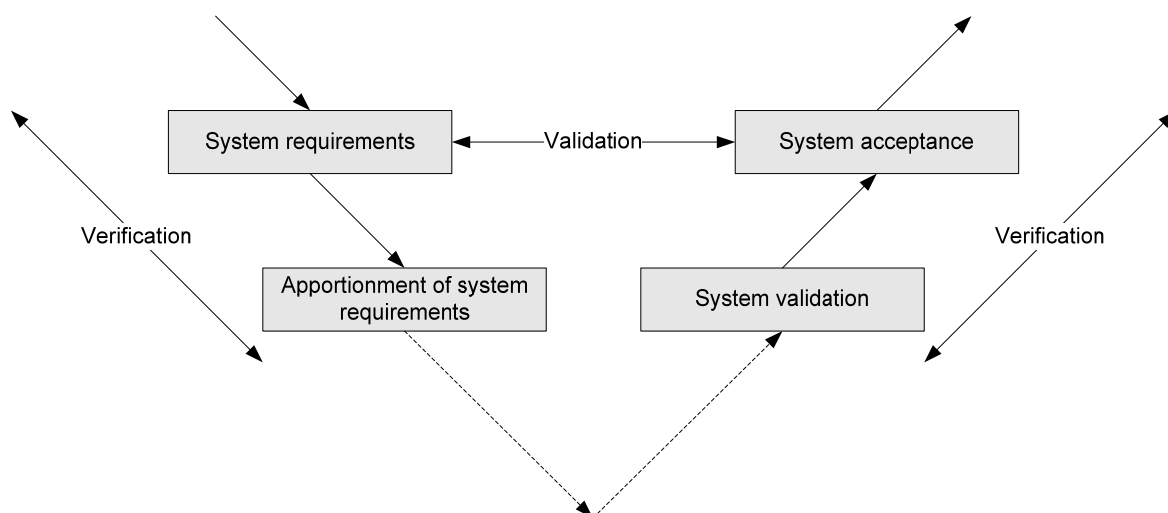


Figure 7 – Verification and validation in the lifecycle according to EN 50126

Verification processes are indicated on the left and right hand side of the figure. Verification shall demonstrate by review and analyse whether the requirements of a particular lifecycle phase have been met, in terms of actual results and output and the fulfilment of the form (e.g. paper form, planning methods, etc.).

At the head of the figure validation procedures are indicated. Validation efforts shall demonstrate whether the actual system complies with the initial system requirements i.e. whether the transportation system meets the requirements of the customer/operator.

All verification and validation activities shall be planned throughout the lifecycle and shall be documented in verification and validation reports. The safety plan shall determine milestones for the different steps of verification and validation activities. Successful verification activities usually allow the project to proceed from one phase to another. Additionally, the safety plan shall provide a reference to verification and validation plans where measures and techniques for verification and validation activities are specified.

Furthermore, the safety plan shall give advice on the required degree of independence of verifier and validator with respect to the planning and design team. CENELEC standards provide guidance upon the required degree of independence for the safety integrity level of the system (see Figure 6).

4.3.7 Safety audits and assessment

This section of a safety plan shall determine conditions on audits and assessments on safety issues. The safety plan shall specify periods, intervals, extent and responsibilities of audits and assessments throughout the lifecycle.

All audit and assessment activities shall be planned and documented. The number and extent of audits and assessments shall be in accordance with e.g. the complexity or the level of risk of the system. Safety audits shall be held in order to assess compliance with safety processes and management systems described in the safety plan. Safety assessment activities shall prove whether the system realisation is compliant with the intended design and whether safety requirements are achieved. During the system lifecycle; system, sub-system and equipment shall be assessed.

For system approval by the safety authority a safety assessment report shall be provided by an independent safety assessor. Key elements for a final safety assessment report shall be the safety plan, hazard log and the safety case. Further details on the safety assessor can be found in sub-clause 4.2.2.4.

4.4 System certification and approval

This part of a safety plan shall describe the approach for system safety certification and final system approval. Once the system is installed, certification of safety shall be provided. Finally, the system shall be approved.

4.4.1 System certification

This section of a safety plan shall cover the concept and process for preparation of the safety case.

After design approval, the system shall be installed and tested. During this phase a safety case shall be established to prove system safety. Following EN 50126 a safety case shall be prepared during lifecycle phase 6 - design and implementation. EN 50129 states that the safety case shall be *“the documented demonstration that the product complies with the specified safety requirements”* [18].

For that purpose, the safety case shall be established by the supplier and shall be complemented by the operator subsequently. This safety case shall be submitted to the independent safety assessor who assesses the safety case and issues a recommendation. Afterwards the safety case shall be passed to the safety authority. When all objections are resolved the safety authority shall approve the safety case, this shall be indicated to operator and supplier (refer to Figure 4 – non-solid arrows).

The final safety report or safety case documents should be kept as a sealed original with the approval granting ultimate authority.

For the establishment of a safety case its purpose shall be defined. As an example, [19] defines the following: *“a safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context”*. The compliance of the system implementation with safety requirements and objectives shall be realised in the safety case by safety arguments with supporting safety evidence.

Concerning a safety case concept and its corresponding presentation of safety arguments, the safety plan shall describe methods and techniques for the realisation. As an example, the goal structuring notation (GSN) – a graphical argumentation notation - shall be given. By defining graphical elements for “goal”, “solution”, “strategy”, “context” and “undeveloped goal” a safety argument can be noted.⁶

Furthermore, a safety case concept shall include a systematic approach for safety case management. For instance, this might be necessary in case pre-approved sub-systems and

⁶ GSN is widely used within the defence, aviation and railway industry. Further details can be found in [02], [19] and [20].

safety cases for generic products or applications are used. Within the safety case concept the timing and delivery of safety cases shall be planned as well.

For a categorisation of safety cases EN 50129 suggests:

- Generic product safety case (independent of application): a generic product can be re-used for different independent applications.
- Generic application safety case (for a class of application): a generic application can be re-used for a class/type of application with common functions.
- Specific application safety case (for a specific application): a specific application is used for only one particular installation.

For all types of safety cases the following structure of the elements is recommended. Figure 8 illustrates an example of structural elements of the overall safety case. On the basis of safety plan, hazard and risk analysis and system requirements, safety cases shall be issued. Details for the actual structure of a safety case and the technical safety report (TSR) can be found in Figure 9 and Figure 10.

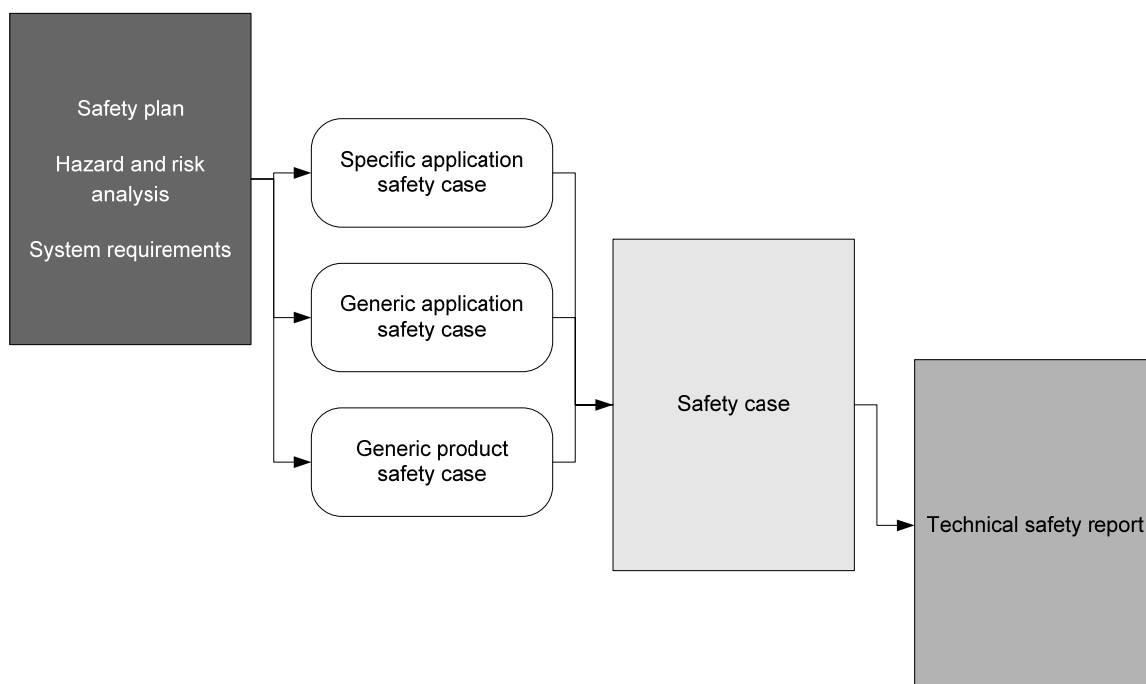


Figure 8 – Structural elements for a safety case

The safety plan shall describe a structure of the actual safety case. A recommendation of EN 50129 is shown in the following figure (see Figure 9).

Additionally, the structure of the technical safety report is pictured in Figure 10. The TSR shall explain the technical principles e.g. design principles and calculations, test specifications and results and safety analyses. The TSR covers safety qualification tests as well as a process for analysing operation and maintenance performance to ensure that the required level of safety is compliant with the requirements.

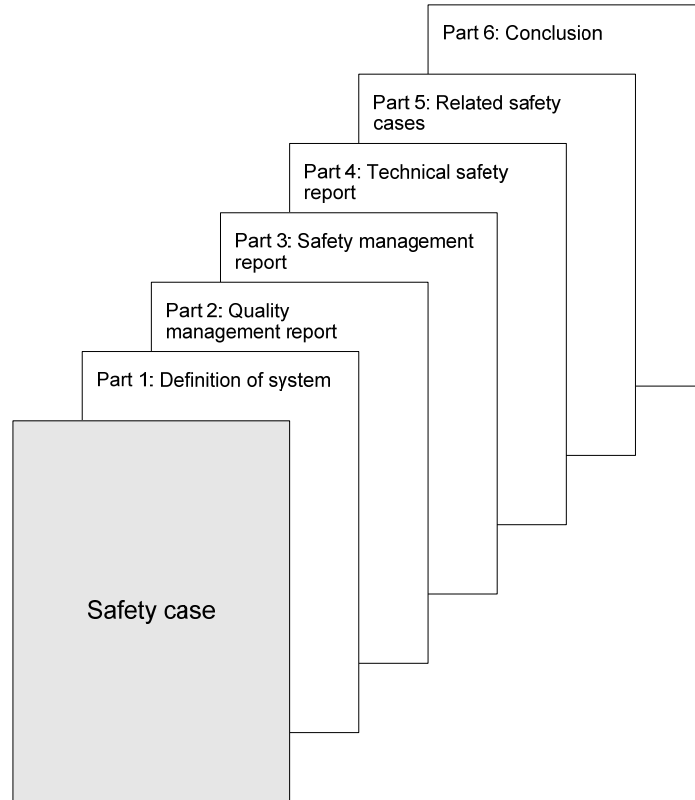


Figure 9 – Structure of safety case according to EN 50129

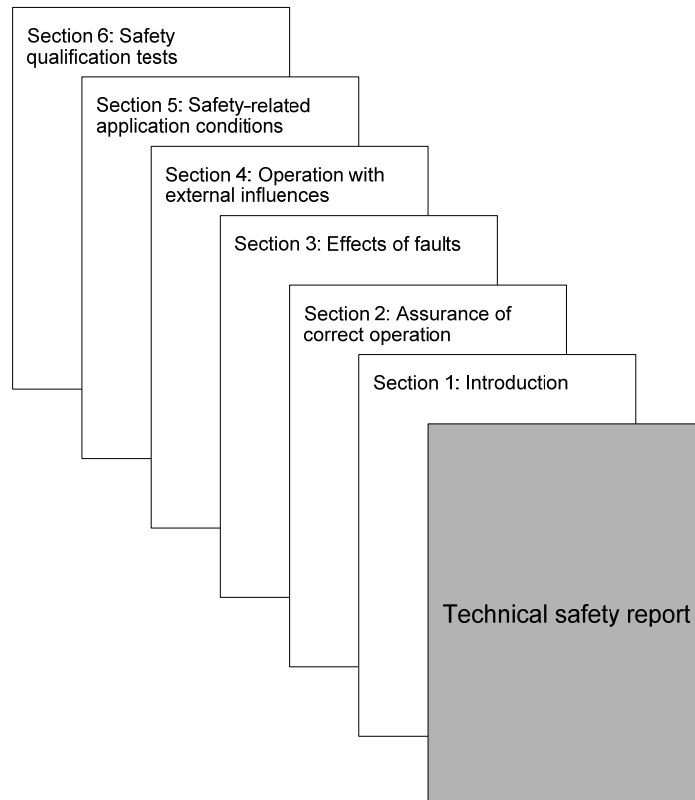


Figure 10 – Structure of technical safety report according to EN 50129

4.4.2 System approval

This section of a safety plan shall outline the process for system approval. First of all the supplier shall demonstrate – by means of the safety case – that the final product complies with the initial requirements. On the basis of the safety case, safety plan and hazard log and additional documents an independent safety assessor shall issue a safety assessment report. Subsequently, a system approval might be issued by a safety authority in case no safety critical objections exist.

As a conclusion the following figure shall give an example of the system approval process. For system approval by the safety authority the safety case shall be complemented by a safety assessment report by an independent safety assessor.

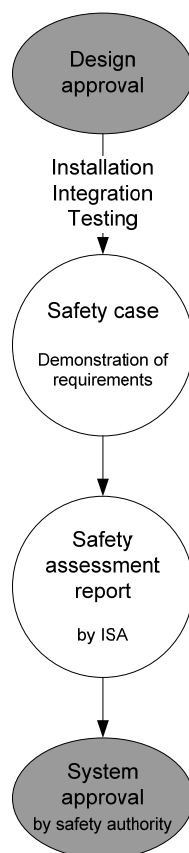


Figure 11 – Example of system approval process

Regarding different certification processes refer to the MODURBAN deliverable 93 [21]. This document describes approval processes for safety certification for urban guided transportation systems throughout Europe.

4.5 System demonstration and acceptance

This part of the safety plan shall determine conditions for system demonstration and acceptance.

4.5.1 System demonstration

This section of a safety plan shall describe the process of system demonstration, which shall be performed on the basis of the previously approved system. The system demonstration shall serve as a final system confirmation for the operator that the system is safe and ready for service.

For this purpose, a system demonstration plan shall be issued e.g. by the supplier or in co-operation with the operator. The safety plan shall provide general constraints for a system demonstration. This includes among others:

- duration of system demonstration,
- how the operation will take place e.g. in regular service and without passenger,
- which scenarios shall be performed e.g. regular operation and
- test cases for e.g. turn backs, evacuation or emergency situations.

Furthermore, the safety plan shall describe the responsibilities and tasks of operator and supplier within the phase of system demonstration.

Additionally, the safety plan shall delineate what condition shall be fulfilled for a successful system demonstration. For that purpose, a safety plan shall give advice on how modification and possible re-construction during or after the system demonstration shall be handled. Since the system used for demonstration is already system approved, major safety related failures are not expected.

However, if changes are necessary the safety plan shall define periods for re-design, procedures to incorporate the modification into the overall design and planning documents and how to continue the demonstration and acceptance process. Moreover, the safety plan shall give advice of how to cope with a re-approval of the system and its changes, for instance, a system modification after the system demonstration might affect the assessment report of the independent safety assessor.

4.5.2 System acceptance

This section of a safety plan shall determine the final conditions for system acceptance. If the system demonstration is successfully completed and no complaints or objections exist on the system, a final system acceptance can be issued. The basis for system acceptance shall be a system demonstration report, which documents all demonstration and test results. System acceptance shall be issued by the operator if full functionality, safety and reliability are achieved and all relevant documents are submitted to the operator.

The following picture concludes the system demonstration and acceptance process, described above.

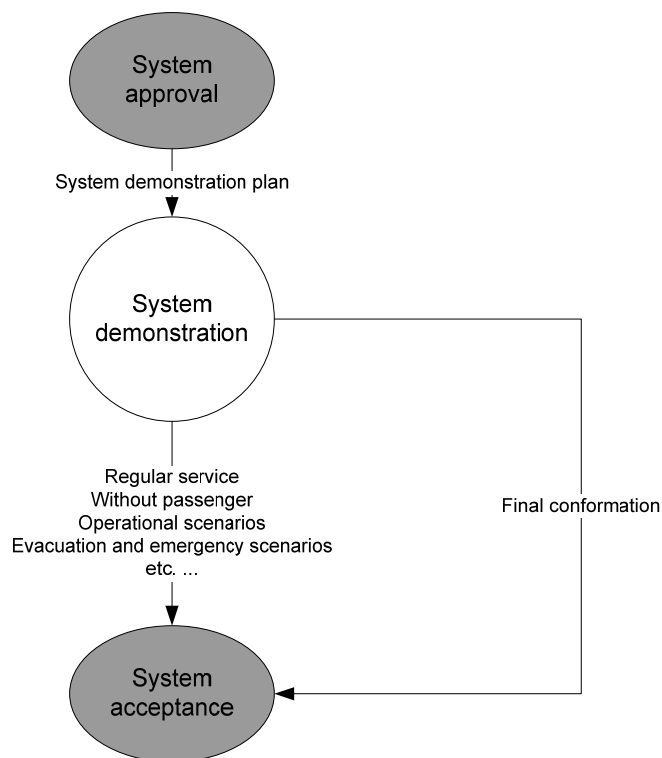


Figure 12 – Example of system demonstration and acceptance process

5 Conclusion

On the basis of the considerations made above, the following findings can be extracted:

- I. A safety plan is a document planning activities and detailing safety roles for the overall lifecycle.
- II. The safety plan shall provide the confidence in the ability to establish system requirements and that the final system complies with these requirements.
- III. The safety plan shall describe the overall safety process steps.
- IV. The safety plan shall describe a safety organisation and identify the responsible individuals.
- V. The safety plan shall give advice on the required safety documentation.
- VI. The safety plan shall describe methods and procedures for the establishment of the system design e.g. hazard and risk analysis or hazard control.
- VII. The safety plan shall provide a basis and structure for a safety case for achievement of safety certification.
- VIII. The safety plan shall determine requirements for an assessment and approval of planning documents, design and the realised system.
- IX. The safety plan shall describe system demonstration and system acceptance processes and requirements.

6 Bibliography

6.1 Referenced documents

- [01] – FREDERIKSEN, GUNNI S.: “Safety Concepts for the Copenhagen Metro using the German BOStrab regulations and the CENELEC Norms, Status and Experiences”, www.m.dk 2001
- [02] – RAIL SAFETY AND STANDARDS BOARD: “Engineering Safety Management (Yellow Book) – Issue 4”, RSSB 2007
- [03] – SOLLEDER, THOMAS; MAGG, PETER: “RAMS-Management nach CENELEC in der Praxis”, Eurailpress Tetzlaff-Hestra GmbH&Co.KG – Signal + Draht (96) 1+2/2004
- [04] – Mann, Paul: “Successful Application of System Assurance on Large Scale Railway Projects”, PM Safety Consultant Limited 2007
- [05] – CENELEC: “EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)”, CENELEC 1999
- [06] – UNITED STATES OF AMERICA - DEPARTMENT OF DEFENCE: “Standard Practice for System Safety – MIL-STD-882D”, Department of Defence – 2000
- [07] – UNION DES INDUSTRIES FERROVIAIRES EUROPÉENNES: “D122 – First Version of D85 covering the relevant data for the Matro Madrid test”, MODURBAN – MODSYSTEM WP22 2008
- [08] – INSTITUT NATIONAL DE RECHERCHE SUR LES TRANSPORTS ET LEUR SECURITE: “D92 - Second conformity assessment, guidelines for functional and technical prescriptions”, MODURBAN – MODSYSTEM WP23 2007
- [09] – NATIONAL ECONOMIC RESEARCH ASSOCIATES: “Safety regulations and standards for European railways – Final Report Vol. 1”, NERA 2000
- [10] – KOCH, THOMAS; KORN, HANS H.: „Die SIG RZA des VDV aus der Sicht von Prüflaststellen und Gutachtern“, Eurailpress Tetzlaff-Hestra GmbH&Co.KG – Signal + Draht (94) 11/2002
- [11] – EICKMANN, CLARA; SCHWARTZ, STEFANIE: “Leit- und Sicherungstechnik CENELEC- konform für regionale Infrastrukturen“, Eurailpress Tetzlaff-Hestra GmbH&Co.KG - Der Eisenbahningenieur (58) 07/2007
- [12] – RAIL SAFETY AND STANDARDS BOARD: “Engineering Safety Management (Yellow Book) – Issue 4, Application Note 4 – Independent Safety Assessment, Issue 2.0”, RSSB 2003
- [13] – Kite Solutions: “D91 - Database of non-conformity events” MODURBAN – MODSYSTEM WP23 2007
- [14] – TECHNISCHE UNIVERSITÄT DRESDEN: “D127 - Preliminary Hazard Log“, MODURBAN – MODSYSTEM WP23 2008
- [15] - TECHNISCHE UNIVERSITÄT DRESDEN: “D86 – Safety conceptual approach for functional and technical prescriptions“, MODURBAN – MODSYSTEM WP23 2006
- [16] – BRABAND, JENS: “Methoden zur Sicherheitsanalyse und ihre praktische Anwendung“, Eurailpress Tetzlaff-Hestra GmbH&Co.KG – Signal + Draht (94) 1+2/2002
- [17] – CENELEC: “EN 50128 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems”, CENELEC 2001
- [18] – CENELEC: “prEN 50129 Railway application – communication, signalling and processing systems – safety related electronic systems for signalling”, CENELEC 2002
- [19] – KELLY, TIM: “A Systematic Approach to Safety Case Management”, SAE International 2003

[20] – CHINNECK, PAUL; PUMFREY, DAVID; KELLY, Tim: “Turning Up the HEAT on Safety Case Construction“, University of York/UK, www-users.cs.york.ac.uk 2004

[21] – INSTITUT NATIONAL DE RECHERCHE SUR LES TRANSPORTS ET LEUR SECURITE: “D93 - Conformity assessment, guidelines for functional and technical specifications“, MODURBAN – MODSYSTEM WP23 2008

[22] – BRABAND, JENS: „Risikoakzeptanzkriterien und -bewertungsmethoden – Ein systematischer Vergleich“, Eurailpress Tetzlaff-Hestra GmbH&Co.KG – Signal + Draht (96) 4/2004

[23] – CENELEC: “EN 50126-2 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“, CENELEC 1999

[24] – UNIVERSITÉ DE VALENCIENNES – “D128 - Risk assessment based on human factors“, MODURBAN – MODSYSTEM WP23 2008

6.2 Further reading

1. *EN 50126 [05] – sub-clause 6.2.3.4 Requirement 4:*

This paragraph recommends contents which shall be included in a safety plan.

2. *RSSB ESM Yellow book 4 [02] – sub-clause 11.3.5:*

This paragraph provides detailed information about the contents of a safety plan.