

## FP7 Project 2007- Grant agreement n°: 218575

### Project Acronym: **INESS**

### Project Title: **INtegrated European Signalling System**

Instrument: Large-scale integrating project

Thematic Priority: Transport

### Document Title: **INESS\_WS G\_Deliverable D.G.1.1\_WS\_Finalised\_Report\_Ver2009-03-16**

Due date of deliverable	30.11.2008
Actual submission date	16.03.2009

Deliverable ID:	<b>D.G.1.1</b>
Deliverable Title:	Normative Safety Case Process Analysis
WP related:	Safety Case Process Appraisal
Responsible partner:	TUBS
Task/Deliverable leader Name:	Jörg R. Müller
Contributors:	TUBS, DLR, Funkwerk

Start date of the project: 01-10-2008

Duration: 36 Months

Project coordinator: Paolo De Cicco  
Project coordinator organisation: UIC

Revision: Dissemination Level<sup>1</sup>: CO

#### DISCLAIMER

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

#### PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the INESS 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 INESS consortium.

<sup>1</sup> PU: Public, PP: Restricted to other programme participants (including the Commission Services), RE: Restricted to a group specified by the consortium (including the Commission Services), CO: Confidential, only for members of the consortium (including the Commission Services).

**Document Information**

**Document type:** Template  
**Document Name:** INESS\_WS G\_Deliverable D.G.1.1\_WS\_Finalised\_Report\_Ver2009-03-16  
**Revision:** 2  
**Revision Date:** 2003-03-20  
**Author:** Jörg R. Müller / TUBS  
**Dissemination level:** CO

**Approvals**

	<b>Name</b>	<b>Company</b>	<b>Date</b>	<b>Visa</b>
<i>WP leader</i>	Jörg R. Müller	TUBS		
<i>WS Leader</i>	Jörg R. Müller	TUBS		
<i>Project Manager</i>				
<i>Steering Board</i>				

**Document history**

<b>Revision</b>	<b>Date</b>	<b>Modification</b>	<b>Author</b>
1	2009-03-10	Description of the models aim and the modelling method	Jörg R. Müller
2	2009-03-20	Rewritten and Layout	Jörg R. Müller

**TABLE OF CONTENTS**

Chapter 1 – EXECUTIVE SUMMARY .....4  
    1.1 The context of workstream G .....4  
    1.2 The aim of work package G.1.1 .....4  
Chapter 2 – INTRODUCTION .....5  
Chapter 3 – EPCs AND THE METHOD OF MODELLING THE NORMATIVE SAFETY CASE .....6  
    3.1 Event-Driven Process Chains as a description means to model the Safety Case Process .....6  
    3.2 The method to model the normative Safety Case Process .....8  
Chapter 4 – CONCLUSIONS .....14  
Chapter 5 – BIBLIOGRAPHY .....15

## GLOSSARY

The following abbreviations are applied in this document

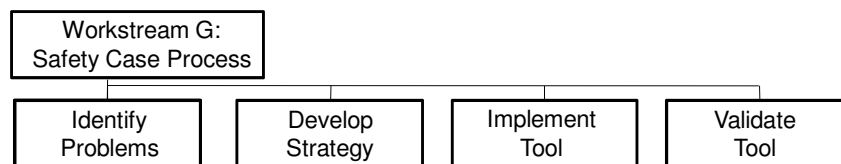
CENELEC	Comité Européen de Normalisation Electrotechnique
EPC	Event-driven Process Chains
RAMS	Reliability, Availability, Maintainability and Safety
EN	European Norm

***Table 1: Abbreviations used in this document***

## Chapter 1 – EXECUTIVE SUMMARY

### 1.1 The context of workstream G

The aim of workstream G is to reduce time and money for the Safety Case in industry, i.e. operators as well as suppliers, by avoiding unnecessary or redundant procedures. In order to achieve this aim, one can identify four phases in workstream G (see figure 1).



**Figure 1: One can specify four phases to achieve the aim of Workstream G**

The first phase “identify problems” subsumes the following three tasks:

- G.3.1 Definition of Process Description Technologie
- G.1.1 Generic Safety Case process Model according to the CENELEC norms
- G.1.2 Collecting Users Experiences

After having identified (or defined) the technology to describe the Safety Case Process (task G.3.1), the Safety Case Process model according to the CENELEC norms is to be developed in a generic and formal way (task G.1.1), see [1], [2] and [3]. On the basis of this model, the experiences as well as the interpretations of the norms are to be collected (task G.1.2).

### 1.2 The aim of work package G.1.1

The aim of this work package is to develop a generic Safety Case Process model according to the CENELEC norms – see file “INESS\_CENELEC-Generic-Safety-Case-Process-Model”. This has been done in two steps:

1. An analysis of the normative process description is to be made.
2. The formal Safety Case Process model is to be developed.

The analysis of the normative process description, i.e. the analysis of the CENELEC norms EN 50126, EN 50128 and EN 50129 aims at gaining a profound knowledge of their structure and inherent causalities, as well as the dependencies between these and on other norms. This knowledge paves the way to develop a method that makes it possible to build up a formal model.

Knowing the method to transfer the normative process description that is given in natural language into a formalised description, event-driven process chains (EPCs) are used to generate the formal model. EPCs have been identified in task G 3.1 to be the most adequate description means to model the Safety Case Process (see deliverable D.G.3.1). In this document, the method to model the normative Safety Case Process is presented. The formal Safety Case Process model can be found as a Microsoft Visio file, see “INESS\_CENELEC\_Generic-Safety-Case-Process-Model.vsd”.

Based on this model, a structured and detailed questionnaire was developed – see deliverable D.G.1.2. With this questionnaire, the deviations from the description of the Safety Case given in the norms and the interpretations of practitioners in practice are to be revealed (task 1.2). In addition, the problems in general, time consuming tasks, but also good solutions to particular tasks are to be identified. This is the overall goal of the WPs G 3.1, G 1.1 and G 1.2.

## Chapter 2 – INTRODUCTION

The CENELEC RAMS norms for railway applications consist of three parts:

- EN 50126 – Railway applications – The specification and demonstration of Reliability, Availability Maintainability and Safety (RAMS)
- EN 50128 – Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems
- EN 50129 – Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

The EN 50126 defines the terms of RAMS, their interaction and a process based on the system lifecycle for managing RAMS. In addition, a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved is defined.

The EN 50128 specifies procedures and technical requirements for the development of programmable electronic systems for usage in railway control and protection applications, aimed at usage in any area where there are safety implications. In contrast to the EN 50126, it is applicable exclusively to software and the interaction between software and the system which it is part of.

The EN 50129 specifies those lifecycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. It is therefore concerned with the evidence to be presented for the acceptance of safety-related systems. Against this background it is in line with, and uses relevant sections of EN 50126. Due to their natural language, these documents lack a precise and unambiguous description of the Safety Case Processes. To improve the comprehensibility and reduce ambiguities, a formal model of the Safety Case Processes is to be built.

In task G 3.1, the description means Event Driven Process Chains (EPCs) has been identified as the most appropriate description means for building the formal model.

In task G.1.1, a method guiding the transformation from the natural language documents to a formal description is to be developed. For this, a profound knowledge of the norms is necessary which is gained by analysing the norms. Based on the developed method, a formal model must be built. In this model, the processes described in EN 50126 and EN 50128 as well as the conditions for safety acceptance and approval (EN 50129) are to be specified in a consistent and unambiguous way.


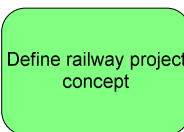

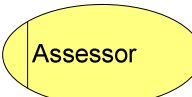
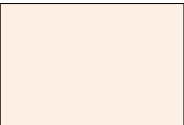
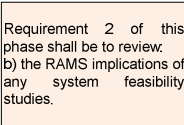

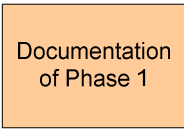

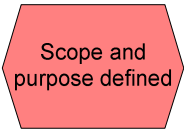

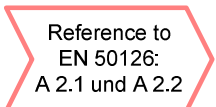
On the basis of this model, the practitioner's interpretations of the norms can be compared to the original norms according to CENELEC. The reason for such a comparison is to reveal time and money consuming tasks in the Safety Case Process (task G 1.2) and, based on this, identify possibilities to support suppliers as well as operators with these tasks. The latter will be done by a software tool developed in WPs 4.1, WP 4.2 and WP 5.1.

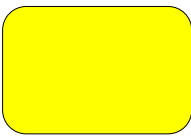


After having introduced EPCs as a description means to model the normative Safety Case, the modelling method that has been developed is described in the following way: The major and general principles of the method are described on the basis of the EN 50126. As the general principles stay the same when modelling the EN 50128 and EN 50129, only the corresponding norm-specific adjustments of the method are explained in detail.

# Chapter 3 – EPCs AND THE METHOD OF MODELLING THE NORMATIVE SAFETY CASE

## 3.1 Event-Driven Process Chains as a description means to model the Safety Case Process

In WP G.3.1 various description means have been evaluated and EPCs were identified as the most appropriate description means to model the Safety Case Process. EPCs are a graphical description means. Thus, using EPCs to describe the CENELEC processes will lead to a graphical representation of the norms. The resulting graphs consist of various nodes whose shape and colour depend on the matter they represent in the model. In addition, directed arcs between these nodes specify the predecessor and successor relations of the modelled matters (see Table 1).

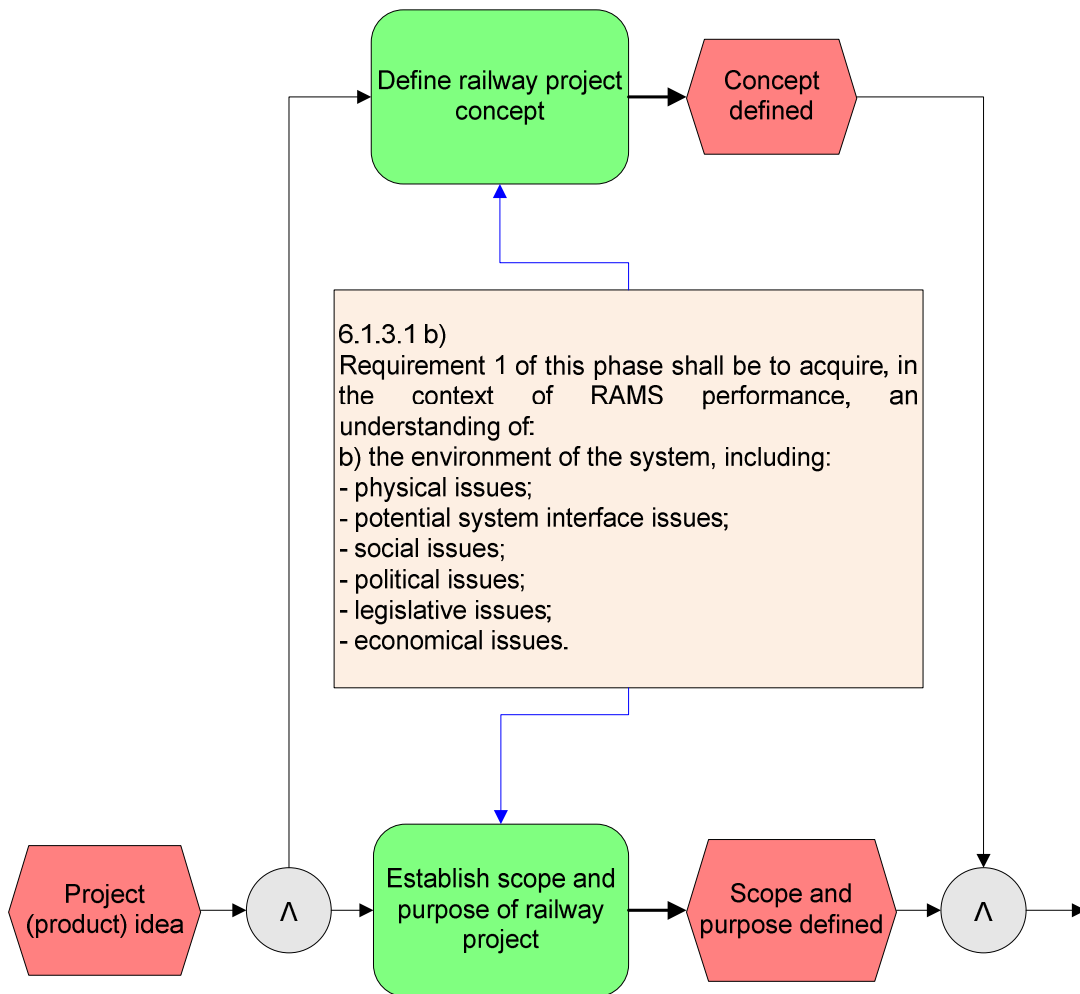
Node	Example	Meaning
		Green coloured rectangular nodes with round corners represent activities (tasks), e.g. “Define railway project concept” or “Establish scope and purpose of railway project“ in the EN 50126.
		Yellow coloured oval nodes are allocated to activities. They represent an organizational unit (or a role) that is assigned to the corresponding activity, e.g. “Assessor” or “Safety Organisation” in the EN 50126.
		Pinkish coloured rectangular nodes are allocated to activities. They indicate information or requirements that are necessary to perform the corresponding activity. For example, to develop a railway project concept (in the EN 50126), it is required” to acquire, in the context of RAMS performance, an understanding of the environment of the system, including physical issues,, potential system interface issues, social issues, political issues, legislative issues and economical issues.
		Orange coloured rectangular nodes indicate documents that result from preceding activities, e.g. “Documentation of phase 1” (in the EN 50126).
		Red coloured hexagons represent states before or after an activity, e.g. “Concept defined” or “Scope and purpose defined” (in the EN 50126).
		Nodes of this shape indicate references to documents or processes (e.g. references to the EN 50126 or EN 50128 in the EN 50129).

		<p>Yellow coloured rectangular nodes with round corners represent verification tasks in the EN 50128 e.g. “Software architecture verification”.</p>
		<p>Grey coloured circular nodes annotated with a logical “AND” symbolise the parallelisation or synchronisation of processes.</p>

**Table 1: Nodes in the EPC-Models to specify the CENELEC-norms**

**Example:**

Figure 1 shows a cutaway from the EPC-model describing the first phase of the EN 50126. The state “Project (product) idea” is the state that indicates the start of the process. After that, the process is parallelised into two subprocesses, i.e. the tasks “Define railway project concept” and “Establish scope and purpose of railway project” may be executed in parallel. To perform these tasks, requirements are to be fulfilled, here: In the context of RAMS performance, an understanding of the environment of the system is to be acquired. After the completion of the two tasks, the corresponding states “Concept defined” and “Scope and purpose defined” are reached. Only after the synchronisation of these two threads can the whole process proceed, i.e. according to the EN 50126 it is necessary that a concept as well as the scope and purpose of the project are defined.



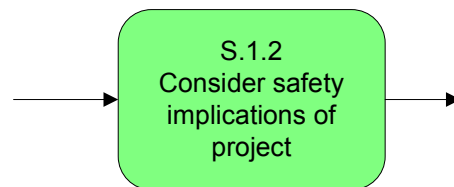
**Figure 1: A cutaway from the EPC-model of the first phase of the EN 50126**

### 3.2 The method to model the normative Safety Case Process

After having examined the three CENELEC-norms, an EPC for each of the three documents has been built. In the following, the method that has been developed is described individually for each norm.

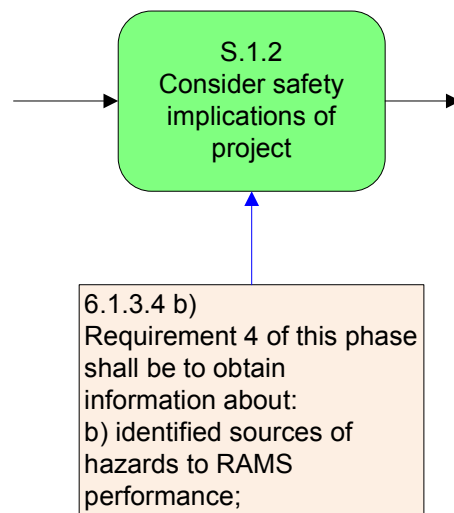
#### General principles of the method – modelling the EN 50126

The EN 50126 consists of 14 phases; the phase related tasks can be divided into general tasks, RAM tasks and safety tasks – see table 2 which is taken from EN 50126 page 28. Each of these tasks can be found in the corresponding phase of the model. Here, general tasks are indicated by task nodes whose inscription starts with a “G.”. The RAM and safety tasks are indicated by task nodes whose inscription starts with an “R.” and “S.”, respectively. Besides indicating the type of the task, the number of the phase in which it occurs, as well as its position within the corresponding table field is denoted. For example, the element in figure 2 indicates that the task “Consider safety implications of project” is a safety related task that is to be performed in phase one, and it is the second safety related task given in the corresponding table field.



**Figure 2: The second safety task of phase 1 (of EN 50126) is to consider the safety implications of the project**

To almost every task that is to be performed in the EN 50126, the necessary requirements have been identified in the description of the corresponding phase. The paragraph of the norm that contains the respective requirement as well as the requirement’s number (also specified in the norm) has been adopted for better understanding and navigation (see figure 3).



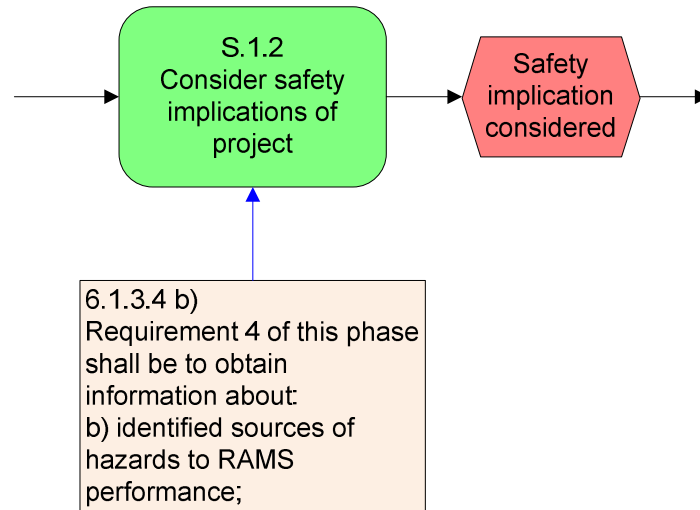
**Figure 3: Part b) of requirement 4 that can be found in paragraph 6.1.3.4 is necessary to perform the task S.1.2**



LIFECYCLE PHASE	PHASE RELATED GENERAL TASKS (G)	PHASE RELATED RAM TASKS (R)	PHASE RELATED SAFETY TASKS (S)
1. CONCEPT	<ul style="list-style-type: none"> <li>Establish Scope and Purpose of Railway Project</li> <li>Define Railway Project Concept</li> <li>Undertake Financial Analysis Feasibility Studies</li> <li>Establish Management</li> </ul>	<ul style="list-style-type: none"> <li>Review Previously Achieved RAM Performance</li> <li>Consider RAM Implications of Project</li> </ul>	<ul style="list-style-type: none"> <li>Review Previously Achieved Safety Performance</li> <li><b>Consider Safety Implications of Project</b></li> <li>Review Safety Policy &amp; Safety Targets</li> </ul>
2. SYSTEM DEFINITION AND APPLICATION CONDITIONS	<ul style="list-style-type: none"> <li>Establish System Mission Profile</li> <li>Prepare System Description</li> <li>Identify Operation &amp; Maintenance Strategies</li> <li>Identify Operating Conditions</li> <li>Identify Maintenance Conditions</li> <li>Identify Influence of Existing Infrastructure Constraints</li> </ul>	<ul style="list-style-type: none"> <li>Evaluate Past Experience Data for RAM</li> <li>Perform Preliminary RAM Analysis</li> <li>Set RAM Policy</li> <li>Identify Long Term op &amp; Mtce Conditions</li> <li>Identify Influence on RAM of Existing Infrastructure Constraints</li> </ul>	<ul style="list-style-type: none"> <li>Evaluate Past Experience Data for Safety</li> <li>Perform Preliminary Hazard Analysis</li> <li>Establish Safety Plan (Overall)</li> <li>Define Tolerability of Risk Criteria</li> <li>Identify Influence on Safety of Existing Infrastructure Constraints</li> </ul>
3. RISK ANALYSIS (see Note 6)	<ul style="list-style-type: none"> <li>Undertake Project Related Risk Analysis</li> </ul>		<ul style="list-style-type: none"> <li>Perform System Hazard &amp; Safety Risk Analysis</li> <li>Set-Up Hazard Log</li> <li>Perform Risk Assessment</li> </ul>
...	...	...	...

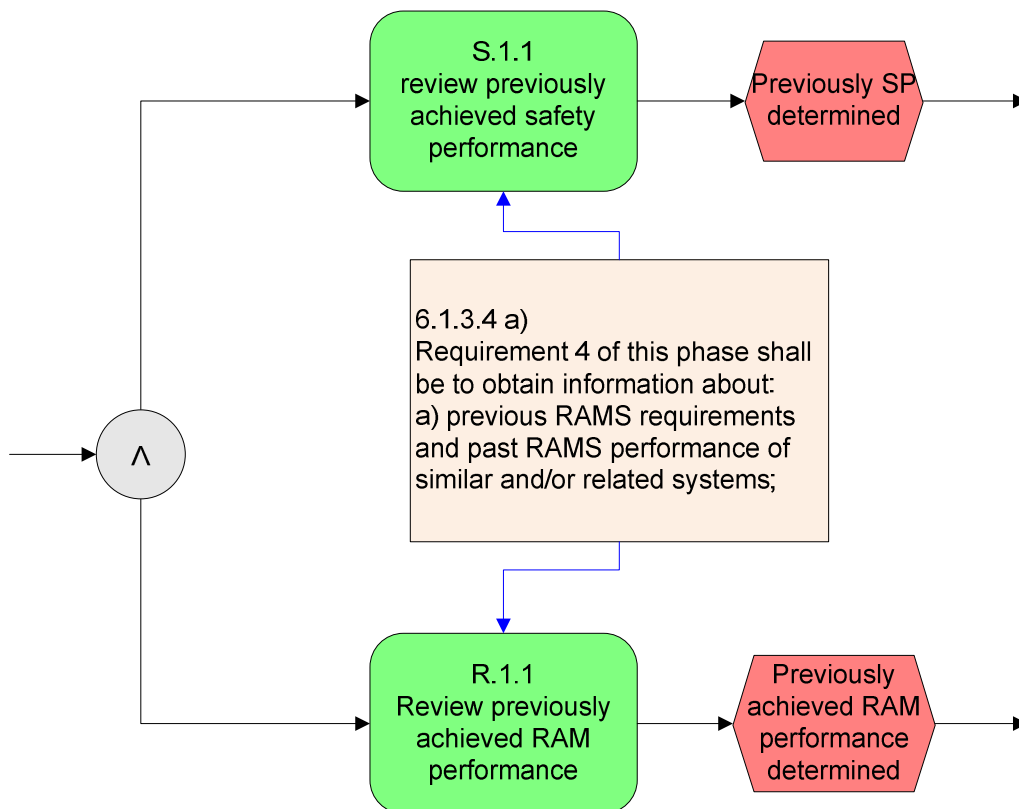
**Table 2: Project Phase Related Task (cut-out of table to be found in EN 50126)**

After the completion of a task, a new state is reached indicating the fulfillment of that task.



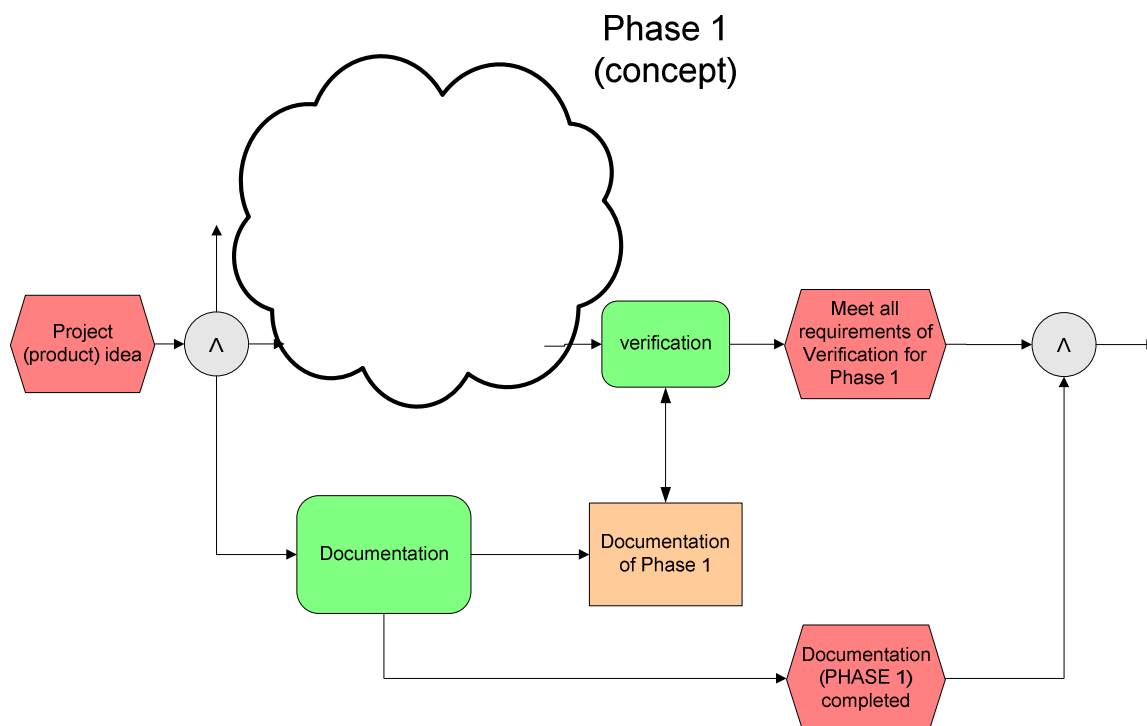
**Figure 4: After the fulfilment of task S.1.2 the state “Safety implication considered” is reached**

Parallelisations and synchronisations of processes are not explicitly defined in the CENELEC norms. They arise from practical knowledge and logical considerations. For example, the revision of previously achieved safety performances and the revision of previously achieved RAM performances can be performed independently from each other, i.e. in parallel (at least in theory) – see figure 5.



**Figure 5: The review of the previously achieved safety and RAM performances can be done in parallel**

Concerning documentation and verification for every phase, the following holds: The task “documenting” is to be performed in parallel to each tasks of a phase. In contrast to this, the verification is specified as a task that is performed at the end of each phase. Both, the output of the verification task as well as the whole documentation that has been done in parallel form the documentation of a phase. To pass from one phase to another, the phase-specific documentation has to be completed and all the verification requirements have to be met (see figure 6).



**Figure 6: The documentation of a phase's tasks is done in parallel, the verification task at the phase's end. One can only enter the next phase when all the verification requirements are met and the documentation is completed**

## Peculiarities of EN 50128

Regarding software development, the EN 50128 distinguishes nine activities: From software requirements specification (chapter 8 of EN 50128) to software maintenance (chapter 15 of EN 50128). Basically, the same method of modelling has been used for EN 50128 and EN 50126. However, in contrast to the description of the EN 50126, the described activities do not specify phases that are to be performed in sequence. In fact, a number of the described activities run across the software development, for instance the verification and the quality assurance.

Against this background, the described activities had to be rearranged to improve readability: E.g. a planning phase has been introduced to establish quality and test plans that are used in later phases has been introduced. In addition, the activity "verification and testing" had to be split into several parts to model the actual circumstances more adequately, as verifications and tests are performed after every phase in the development.

The same nodes as in EN 50126 were used. Therefore, its readability is as easy as that of EN 50126 and needs no further explanation.

## Peculiarities of EN 50129

The EN 50129 defines the conditions that shall be satisfied in order for a safety-related electronic railway system/sub-system/equipment to be accepted as adequately safe for its intended application. The documentary evidence that these conditions have been satisfied shall be included in a structured safety justification document, known as the Safety Case.

This background leads to two characteristics of the EN 50129:

1. It describes a structure of the Safety Case rather than a process: The global structure of the Safety Plan consisting of six chapters as well as the structure of each of these chapters is described. This leads to six

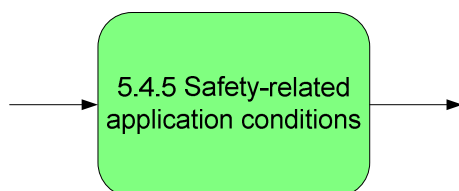
processes, each describing the development of one chapter of the overall Safety Plan. This in turn generally results in quite small processes – exceptions to this are the descriptions of the development of the safety management report and the technical safety report.

2. It is highly dependent on documents that are developed in the processes described in EN 50126 and EN 50128. Therefore, lots of cross references to the other documents can be found in EN 50129.

The Safety Plan consists of the following six parts:

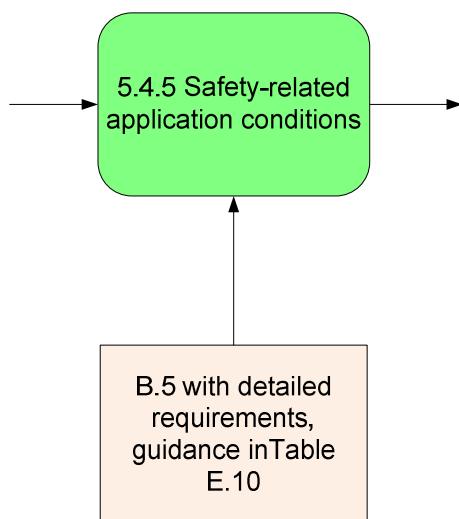
1. Definition of System
2. Quality Management Report
3. Safety Management Report
4. Technical Safety Report
5. Related Safety Cases
6. Conclusion

To each of these parts a process model has been established. Similar to the description of EN 50126, every task to be performed can be linked to a (sub-)section of one of these documents. This linkage is defined in the 5<sup>th</sup> chapter of EN 50129. For example, the system related application conditions are to be defined in subsection 4.5 (i.e. they are part of the 4<sup>th</sup> document of the Safety Case – Technical Safety Report), see figure 7.



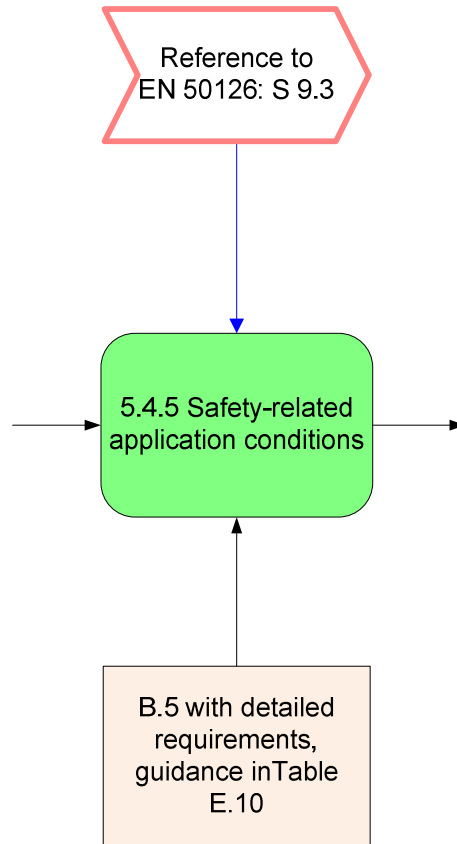
**Figure 7: Chapter 5 of the EN 50129 indicates that in the 4<sup>th</sup> part of the Safety Case (i.e. the Technical Safety Case), the safety-related application conditions are to be described in section 5.**

Just like in the description of EN 50126, requirements could be identified for each of the corresponding tasks. In EN 50129, many of these requirements are comprehensively defined in the annexes. In order to improve readability, the model refers to these annexes – see example in figure 8.



**Figure 8: The requirements to specify the safety-related application conditions are specified in annex B.5 and in table E.10 of EN 50126**

EN 50129 often refers to documents or requirements that have been produced or are described in the processes of EN 50126 or EN 50128. For example, the safety-related application conditions refer to the application conditions contained in the Safety Case of any related sub-system or equipment.



**Figure 9: The safety-related application conditions refer to the third safety task of phase 9 described in the EN 50126, i.e. “Prepare Application Specific Safety Case”.**

## Chapter 4 – CONCLUSIONS

The aim of workpackage G.1.1 was to build a formal and generic model with the purpose of expressing normative requirements of the CENELEC norms for railway applications in a user-friendly way. This has been achieved, as the model serves by now as a basis to introduce the CENELEC processes (e.g. at BBR (German supplier) and ANSALDO (Italian supplier)).

The model that has been built is parted, roughly spoken, into three parts: one for each of the processes described in every CENELEC norm. The whole model consists of

- 80 parallelisations and synchronisations
- 185 states
- 192 activities
- 189 requirements and
- 805 arcs.

Despite its size, the model is readable quite easily and gives therefore not only a very good overview of the processes, their tasks and their interrelations, but also a deep insight in the relations between requirements and tasks. In addition the relations between the documents developed in certain (project)phases and the corresponding parts of the safety case is understood quite easily.

This model constitutes the basis for the task G.1.2 “Collecting the Users Experiences”: It will be the basis to reveal the deviations of the description of the safety case given in the norms and the interpretations in practice. In addition the problems in general, time consuming tasks but also good solutions to particular tasks are to be identified. Altogether, this shall lead to proposals for the safety case in practice, which is the overall goal of the WPs G 3.1, G 1.1 and G 1.2.

## Chapter 5 – BIBLIOGRAPHY

- [1] EN 50126: EN 50126: Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999.
- [2] EN 50128: Railway Applications – Communications, Signalling and Processing Systems - Software for Railway Control and Protection Systems, 1999.
- [3] EN 50129: Railway Applications – Communications, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling, 1999.