The Formal Representation of the Safety Case Processes described in the EN 5012x norms

Jörg R. Müller, Institute for Traffic Safety and Automation Engineering, Technical University of Braunschweig, Germany

Jörn Drewes, TÜV SÜD Rail GmbH, Germany

Jörg May, IGT Bahn mbH, Germany

Carsten Trog, Funkwerk IT, Germany

Abstract: The European project called „INESS – Integrated European Signalling System“ aims at defining and developing specifications for a new generation of interoperable interlocking systems suitable to be integrated in ERTMS systems, with the objective of making the migration to ERTMS more cost-effective.

One essential part of INESS deals with the safety case process. The aim of this “workstream” is to reduce time and money for the development of the safety case in industry, i.e. operators as well as suppliers, by avoiding unnecessary or redundant procedures.

One basis to achieve this goal was the development of a generic and formal model of the safety-case related processes according to the RAMS norms EN 5012x of CENELEC.

This contribution presents the method guiding the transformation from the natural language documents specifying the normative safety case processes to a representation by the formal description language “Event driven Process Chains”.

1. Introduction

The aim of this paper is to describe the method to develop the normative model of the Safety Case Process in a formal way. In order to reach this objective, various commonly used description technologies to describe processes were examined and evaluated against this specific application background. In the end, Event Driven Process Chains (EPCs) were discovered to be the appropriate description technique to reach this aim.

After having introduced the corresponding evaluation criteria, 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.

On the basis of the developed model, the practitioner’s interpretations of the norms can be compared to the original norms according to CENELEC. The reason for such a comparison was to reveal time and money consuming tasks in the Safety Case Process and, based on this, identify possibilities to support suppliers as well as operators. The latter will be done by a software tool that is currently being developed.

2. The Analysis of Description Technologies

The description of the processes, tasks and conditions in the CENELEC RAMS norms (EN 50126, EN 50128 and EN 50129) has been done in natural language. In order to be able to develop a formal model of the Safety Case Process, one has to identify

1. a formal language that is suitable for this specific scope,
2. a modelling-method that guides the transformation from the description given in natural language to a description given as a formal model,
3. a SW-Tool that allows the use of the formal language given in 1. and supports the developed modelling-method.

The modelling language that is to be used to model the Safety Case Process in a formal way shall

- allow the unambiguous description of processes,
- support sequential as well as parallel processes,
- support the parallelisation as well as the synchronisation of processes,
- have appropriate tool support,
- be easy to understand by practitioners.

In order to reach this objective, the following description technologies to describe processes were examined and evaluated against these specific requirements:

- Makov chains
- Petri-nets
- Natural language
- Event driven Process Chains (EPCs)
- UML-Diagramms
    - Class diagramms
    - Use Cases
    - Sequential diagramms
    - Activity diagramms

2.1 Requirement Identification

The analysation of descprition languages has been done against certain characteristics. These characteristics have to be chosen against the requirements of the application area in focus. For example, one uses different languages to describe a system in a way that permits the quantitative calculation of RAMS-values in a complex system and to describe the static relations within this system.

Therefore, a selection of the designated, qualitative characteristics and requirements for prioritisation are to be consulted. The description language that is to be chosen shall make it possible to illustrate the following concepts:

Structure: The ability of the description language to model the structure of the process is one of the essential requirements. In this respect, the composition of a process made up of sub-processes that are related to each other and to the process' environment are to be demonstrated. Graphical structures and illustrations seem to be appropriate to fulfill this requirement.

Causality: Concerning causality, later states of the process can only be dependent on preceding states of the process. In addition, the influence of earlier states is often described in a (stochastically) determined way.

Parallel Processes: In parallel processes, events are causally independent.

Sequential Processes: In sequential processes, events are causally dependent.

Consistency: The description language should be applicable to as many development phases as possible in order to avoid information losses due to the changing of the languages in different phases.

Analyzability: The structural accuracy and correctness of the illustrated process shall be verifyable.

Tool Support: Tools are to be available for the development of a model using the selected description language.

Unambiguousness through clear symbolism: The meaning of the used symbols shall be unambiguous.

2.2 Result of the process description analysis

The evaluation against the requirements to model the Safety Case Process showed that EPCs are suitable for describing the Safety Case Process. EPC have been selected since this project group is an interdisciplinary work group and EPCs are very widely used in the area of business processes which does seem to be related to the Safety Case Process (see deliverable D.G.3.1 of the INESS-Project).

3. The Method to model the normative Safety Case Process

There are three main CENELEC standards related to RAMS:

- 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.

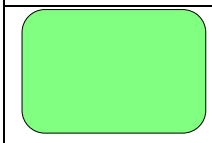
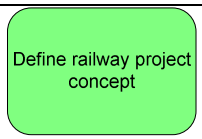
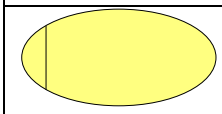
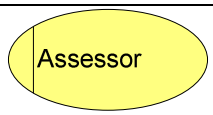
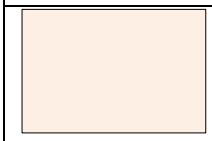
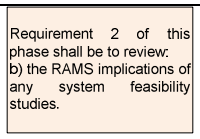
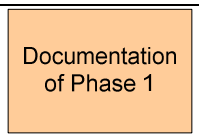
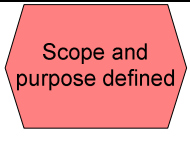
The EN 50129 specifies those lifecycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. It is therefore concerned with the evidence to be presented for the acceptance of safety-related systems and is highly related to the EN 50126.

Due to the 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 had to be built.

In this chapter, a method guiding the transformation from the natural language documents to a formal description is being developed. For this, a profound knowledge of the norms is necessary. Based on the developed method, a formal model has been 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) have been specified in a consistent and unambiguous way.

3.1 Event-driven Process Chains as a description language to model the Safety Case Process

Various description languages have been evaluated and EPCs were identified as the most appropriate description language to model the Safety Case Process. EPCs are a graphical description language. 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 specifiy 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 requirements. 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).

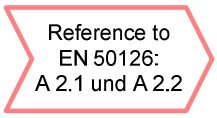
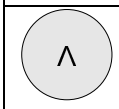
		Nodes of this shape indicate references to documents or processes (e.g. references to the EN 50126 or EN 50128 in the EN 50129).
		Yellow coloured rectangular nodes with round corners represent verification tasks in the EN 50128 e.g. “Software architecture verification”.
		Grey coloured circular nodes annotated with a logical “AND” symbolise the parallelisation or synchronisation of processes.

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 peformance, 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 the whole process can 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.

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.

3.2.1 General Principles of the method – modelling the EN 50126

The aim of the developed modelling method was twofold: Generally spoken, it has been attached great importance to the readability and understanding of the norm:

- Concerning the readability of the norms, the aim was to assure the accordance of the (rough) structure of the processes given in the norms to the formal model. On the basis of such accordance, a practitioner (or a newcommer in the field of the CENELEC-RAMS norms) is able to use both, the norms in natural language and the model in a formal language in a complementary way.
- Concerning the understanding of the norms, the huge amount of implicit knowledge covered by the norms had to be made explicit.

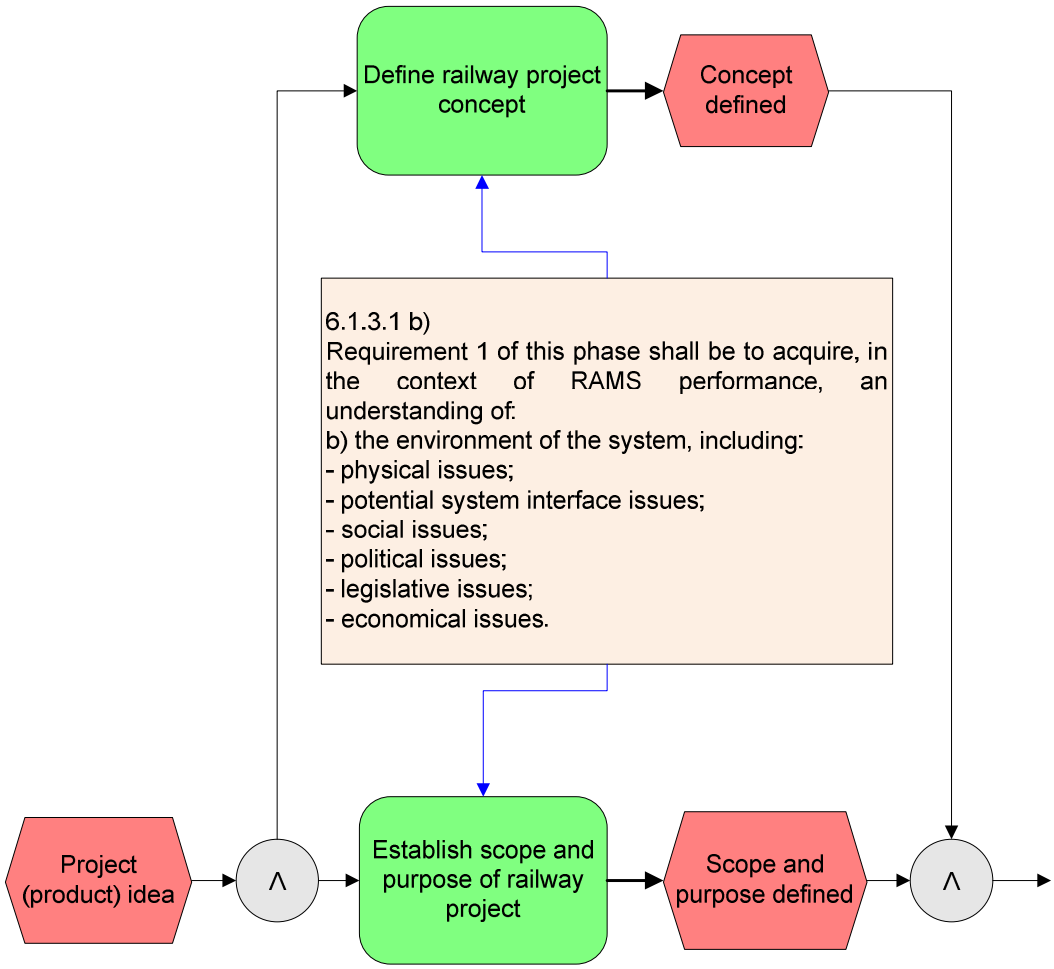


Figure 1: A cutaway from the EPC-model of the first phase of the EN 50126

General Principles of the method – modelling the EN 50126

Against this background, the following modelling approach has been chosen:

Concerning the readability, the EN 50126 lists the tasks that are to be carried out in each of the 14 phases. In addition these tasks are divided into three parts/types: general tasks, RAM tasks and safety tasks – see table 2 which is taken from EN 50126, page 28. This task-relating structure has been adopted in the method: In the model, 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 (see figure 2). In doing so, the correspondance between the norm and the model is revealed and can be reproduced.

Concerning the understanding and applicability of the norms, their implicit knowledge had to made explicit. Accoring to this, two questions had to be answered for every task:

1. What are the necessary requirements to perform the task?
2. For each phase, which of the tasks can be performed in parallel and which have to be performed in sequence?

Information of this kind is not explicitely given in the norms. Therefore, the given information had to be carefully examined and causalities had to be identified. The results of these analysations have been made explicit in the model: Here, for every task the necessary requirements are specified and in addition it has been specified which of the tasks can be performed in parallel and which have to be performed in sequence.

In the paragraphs of this subsection, the above outlined modelling method is being exemplyfied.

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 („S.1.2").

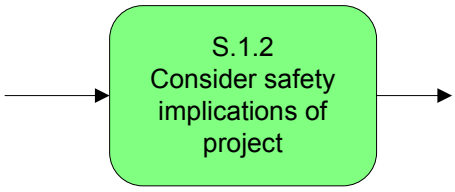


Figure 2: The second safety task of phase 1 (of EN 50126) is to consider the safety implications of the project

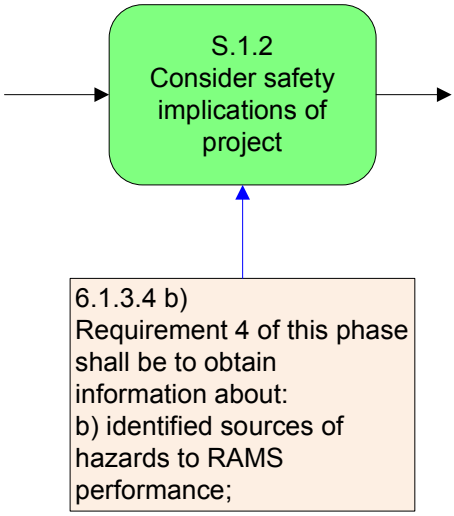


Figure 3: Part b) of requirement 4 that can be found in paragraph 6.1.3.4 is necessary to perform the task S.1.2

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).

After the completion of a task, a new state is reached indicating the fulfillment of that task. Parallelisations and synchronisations of processes are not explicitely defined in the CENELEC norms. They arise from practical knowledge and logical considerations.

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

LIFECYCLE PHASE	PHASE RELATED GENERAL TASKS (G)	PHASE RELATED RAM TASKS (R)	PHASE RELATED SAFETY TASKS (S)
1. CONCEPT	• Establish Scope and Purpose of Railway Project • Define Railway Project Concept • Undertake Financial Analysis Feasibility Studies • Establish Management	• Review Previously Achieved RAM Performance • Consider RAM Implications of Project	• Review Previously Achieved Safety Performance • **Consider Safety Implications of Project** • Review Safety Policy & Safety Targets
2. SYSTEM DEFINITION AND APPLICATION CONDITIONS	• Establish System Mission Profile • Prepare System Description • Identify Operation & Maintenance Strategies • Identify Operating Conditions • Identify Maintenance Conditions • Identify Influence of Existing Infrastructure Constraints	• Evaluate Past Experience Data for RAM • Perform Preliminary RAM Analysis • Set RAM Policy • Identify Long Term op & Mtce Conditions • Identify Influence on RAM of Existing Infrastructure Constraints	• 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 (see Note 6)	• Undertake Project Related Risk Analysis		• Perform System Hazard & Safety Risk Analysis • Set-Up Hazard Log • Perform Risk Assessment
…	…	…	…

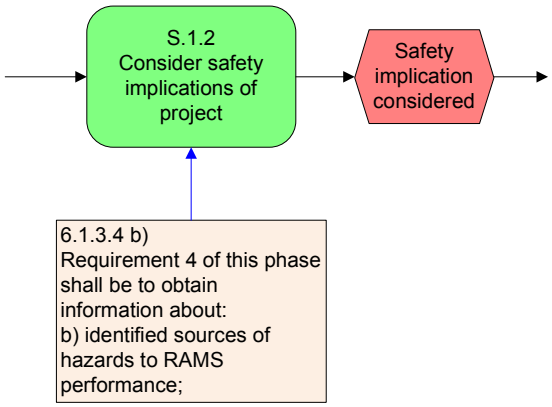


Figure 4: After the fulfilment of task S.1.2 the state "Safety implication considered" is reached

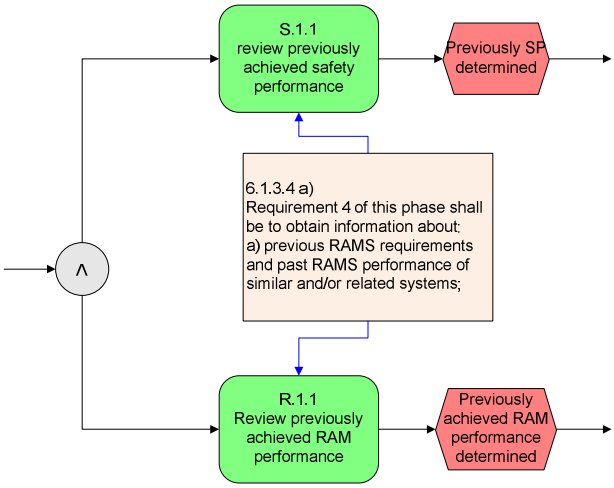


Figure 5: The review of the previously achieved safety and RAM performances can be done in parallel

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.

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.

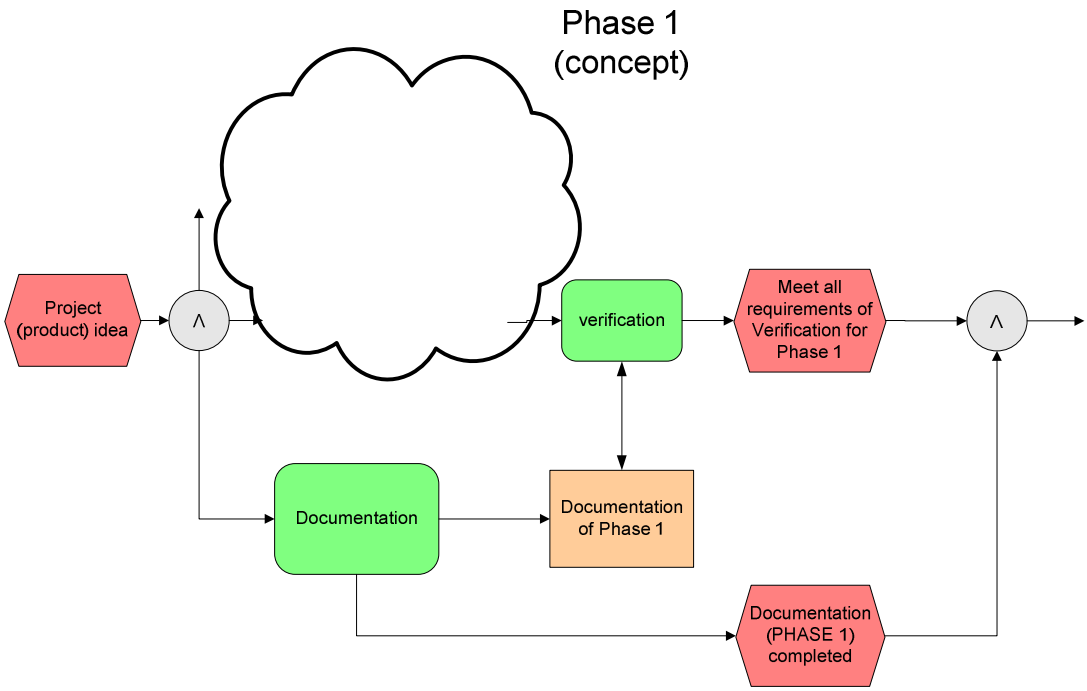


Figure 6: The documentation of a phase's tasks is done in parallel, the verification task at the phase's end. One can only enter the next phase when all the verification requirements are met and the documentation is completed

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).

Pecularities of the 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 descibed 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.

Pecularities of the 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.
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 documents:

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

For each of these documents 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 within one of these documents. This linkage is defined in the 5th 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 4th document of the Safety Case – Technical Safety Report), see figure 7.

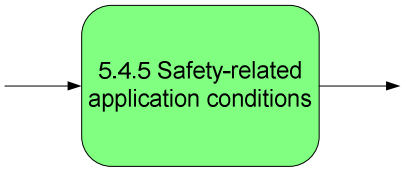


Figure 7: Chapter 5 of the EN 50129 indicates that in the 4th part of the Safety Case (i.e. the Technical Safety Case), the safety-related application conditions are to be described in section 5.

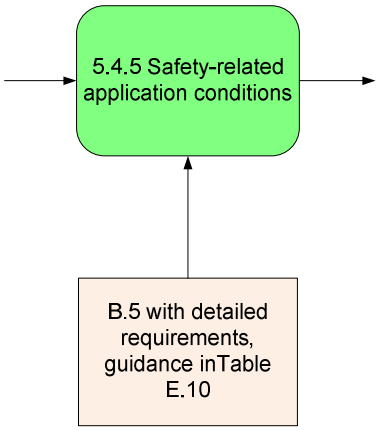


Figure 8: The requirements to specify the safety-related application conditions are specified in annex B.5 and in table E.10 of EN 50126

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.

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.

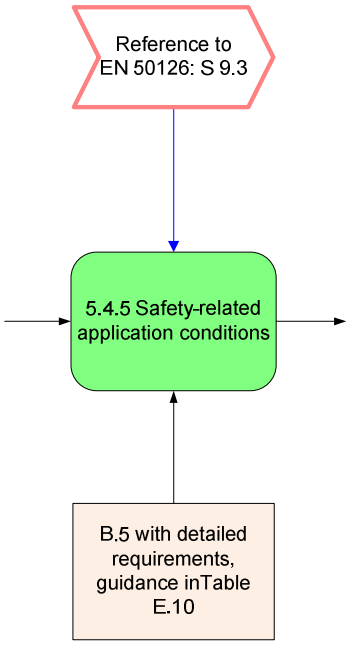


Figure 9: The safety-related application conditions refer to the third safety task of phase 9 described in the EN 50126, i.e. "Prepare Application Specific Safety Case".

4. Conclusion

After having identified EPCs as the description language that suits best the requirements to model the Safety-Case Process best, it has been the task 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 (Italien supplier)).

In the model that has been built is parted 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 constituted the basis for the INESS-task “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 was the overall goal oft he tasks so far.

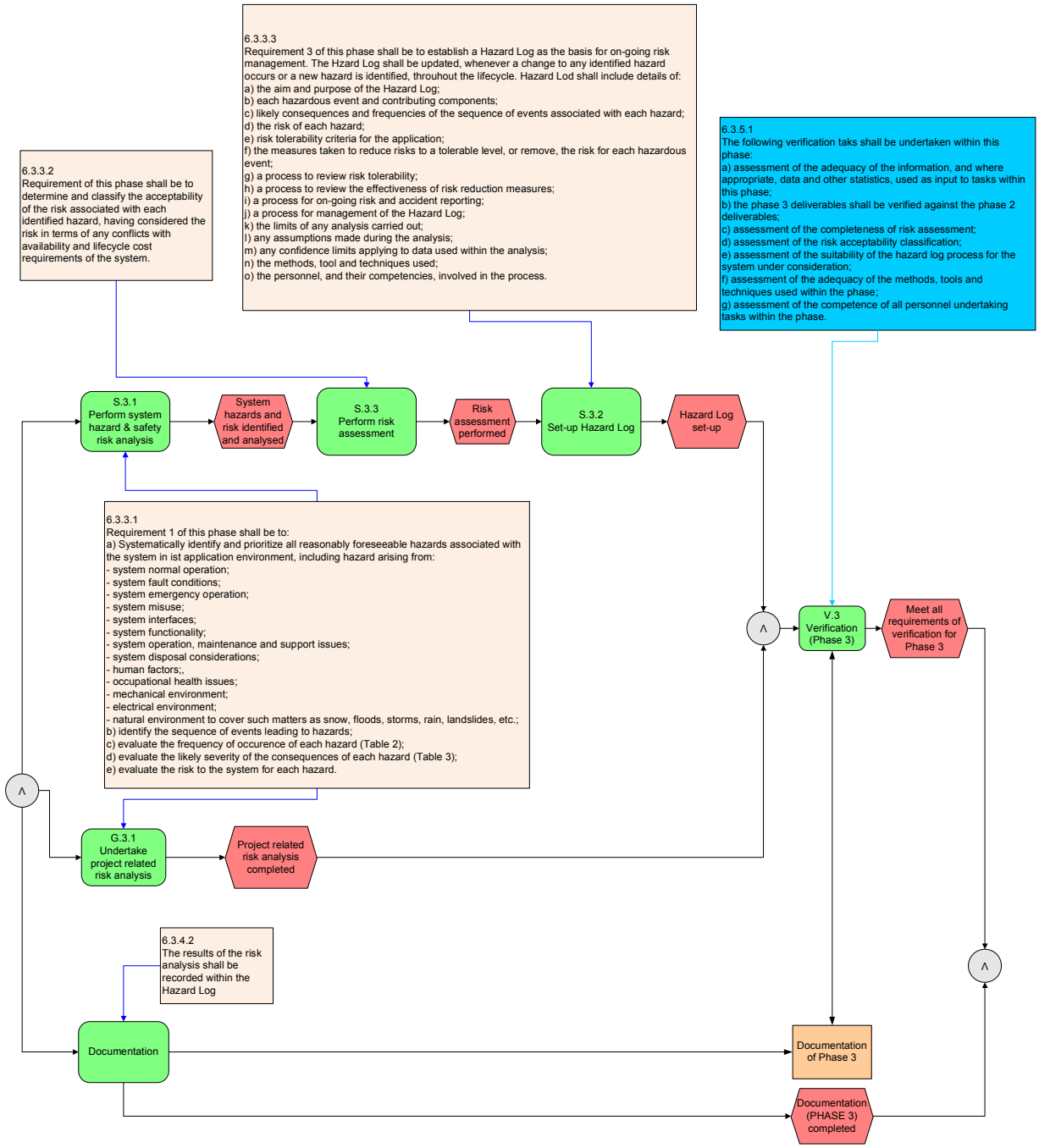
5. Bibliography

[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.

Annex – Phase "Risk Analysis"



As an example, this figure shows phase 5 „risk analysis" from the EPC-model specifying the normative safety case process in a formal way.