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:

Specification of improved safety case

Due date of deliverable
Actual submission date

Deliverable ID:	**D.G.4.1**
Deliverable Title:	Specification of improved safety case
WP related:	G.2.2, G.3.1.2
Responsible partner:	TUBS
Task/Deliverable leader Name:	Jörg R. Müller
Contributors:	Funkwerk, TUBS, DLR, DB, BV, ProRail, BBR, RFI, Ansaldo

Start date of the project: 01-10-2008 Duration: 36 Months

Project coordinator: Paolo De Cicco
Project coordinator organisation: UIC

Revision: Dissemination Level[1]: CO

[1] 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: Report
Document Name: INESS_WS G_ Deliverable G.4.1_WS_Finalized_Report _Ver2010-03-31
Revision: 3
Revision Date: 2010-03-31
Author: Jörg R. Müller
Dissemination level: **CO**

Approvals

	Name	Company	Date	Visa
WP leader	Jörg R. Müller	TUBS		
WS Leader	Jörg R. Müller, Carsten Trog	TUBS, Funkwerk		
Project Manager				
Steering Board				

Document history

Revision	Date	Modification	Author
0.1	2009-08-31	Creation of document	G. Buxhoeveden
1	2009-09-25	Added content from workshop	G. Buxhoeveden
2	2010-01-04	Introduction of structure of Improved SaCaProcess Model; Tasks / functionalities related to improving tasks and knowledge	Jörg R. Müller
3	2010-03-31	Results of discussions, workshop and recommendations of André Broersen taken into account,	Jörg R. Müller

TABLE OF CONTENTS

GLOSSARY

SaCaPro	Safety Case Process
SW	Software
BPM	Business Process Modell
DB	Database
DMS	Document Management System
WMF	Workflow Management System
GSN	Goal Structuring Notation
EPC	Event driven process chain
DoW	Description of Work
SaCA	Safety Case
GPSC	General Product Safety Case
SASC	Specific Application Safety Case
ALARP	As Low As Reasonably Practicable

Section 1 – EXECUTIVE SUMMARY

1.1 The context: Workstream G and task G.4.1

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. To achieve this aim one can identify four phases in workstream G (see Figure 1).

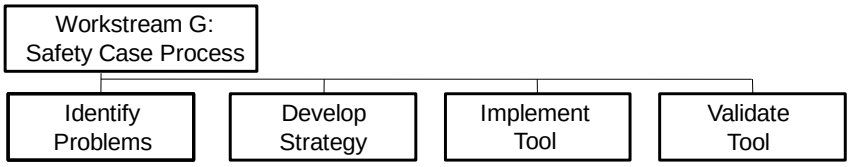

Figure 1: One can specify four phases to achieve the aim of Workstream G

The task G.4.1 “Specification of Improved Safety Case Process” is part of the second phase of this workstream. The goal of this task is to identify procedures or, more generally, ways to improve the safety case process in such a way that enables to overcome the obstacles identified during the interviews with WS-G’s partners (see D.G.1.2).

This improved safety case shall be defined, using the means of description equal or similar to the description of the safety case as performed in task G.3.1 (Definition of process description technology). Input from workshop findings and from the list of short term goals (task G.2.2) shall provide further information to define the improved safety case. Furthermore, the results of this task provide valuable input for task G.4.2 (specification of tools) and G.5.1 (implementation of tools).

Section 2 – INTRODUCTION

In the CENELEC 5012x norms, the normative safety case process (SaCaPro) is defined as a linear succession of phases. For each phase, the standards specify an integrated set of development and safety related tasks, their input information requirements and the deliverable documents. The normative SaCaPro has been modelled in task G.1.1 (see deliverable D.G.1.1).

Here, the aim is to improve the normative process. This has to be achieved without changing the normative process itself. It is neither the scope of WS-G nor the scope of the INESS-project to change the normative environment.

Therefore, the procedures to improve the normative SaCaPro have to be specified in parallel, sometimes in dependence of certain normative tasks. The improvement procedures will mainly take into account the results of WS-G' previous tasks and discussions (see e.g. D.G.1.2) and the obligations specified in the DoW.

In general, these additional procedures will tackle the identified obstacles. With the development of an appropriate SW-tool implementing these procedures, the very supportive functionalities will be provided. Although this SW-tool will be applicable to all of the 14 phases of the CENELEC-lifecycle, it turned out that especially the phases after system acceptance are not strictly followed in industry. Therefore, the tool to be provided will probably be used mainly in the phases before. The specific support of the phases after system acceptance as well as the "requirements specification phase" has been identified as being a long term goal (see D.G.2.1).

Against this background, it is being focused on the support-functionalities identified in D.G.2.2 (short term goals).

Section 3 – IMPROVED SAFETY CASE PROCESS

This section is divided into three subsections with the following topics. Subsection 3.1 describes the general methodology to implement the functionalities identified in task G.2.2. With these functionalities one overcomes the problems identified in task G.1.2. Additionally, subsection 3.2 addresses three essential challenges when it comes to safety cases, especially in an international environment: The dependencies between the various safety cases, the use of legacy systems (missing a safety case according to CENELEC), and cross acceptance of safety cases. Subsection 3.3 finally addresses the interfaces to related tasks of the safety case.

3.1 General Methodology

Deliverable D.G.3.1 describes the event-driven process chains (EPC) notation and how it has been applied to model the normative safety case processes (EN 5012x). The notation offered a transparent and easy to understand visualization of the sequential and parallel processes interacting with each other within the overall normative CENELEC safety case framework.

The improved safety case process will consist of

1. The normative safety case processes
2. The tasks that improve these processes.
3. The knowledge that is the basis for the improving tasks of 2.)

The model of the improved safety case process (see Figure 2) consists of several layers, fullfilling the strict separation of the normative development processes (see 1. in the list above) and the support functionality (see 2. and 3. in the list above). This separation is demanded by the DoW.

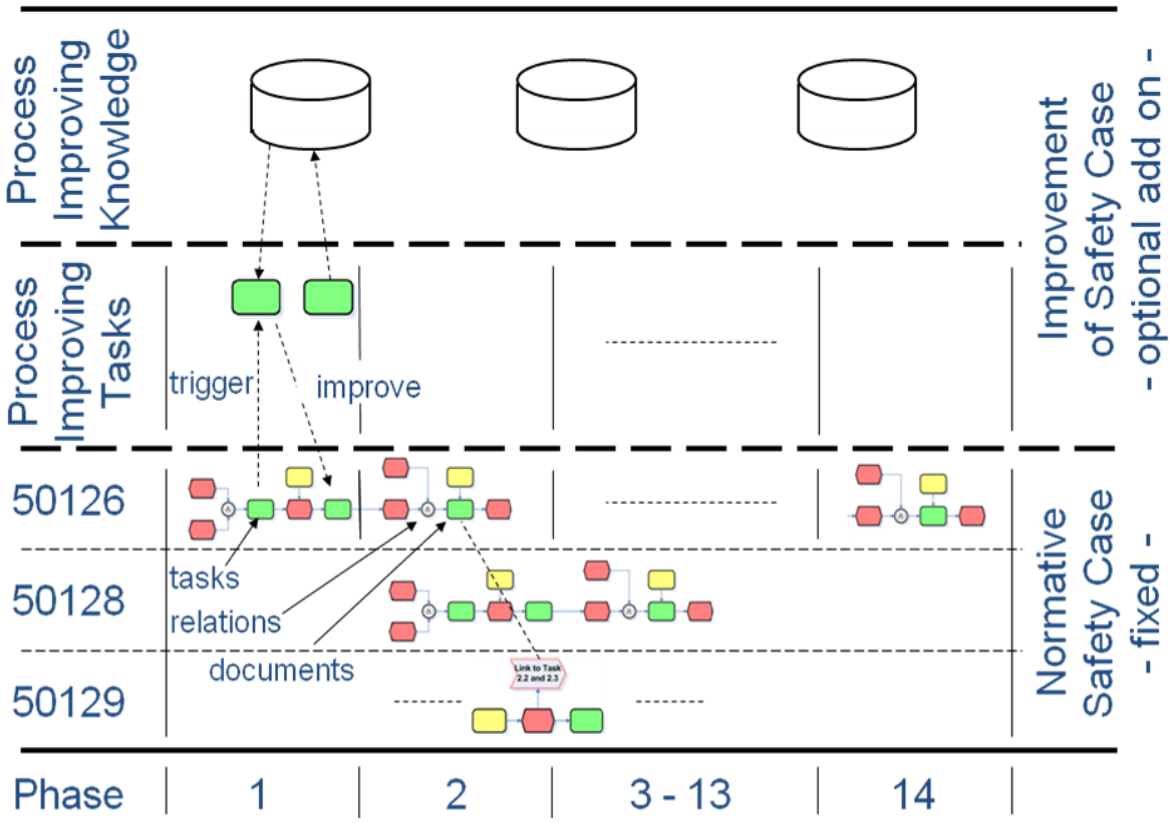

Figure 2: Structure of the improved safety case model

In the following paragraphs the content of the knowledge databases is specified in more detail. In addition the processes making use of these databases in order to realize the supporting functionalities are described.

3.1.1 Process improving knowledge

The processes to improve the normative SaCaPro revert to knowledge that may be stored in various ways and at different places. Here, “database” (DB) just means that the corresponding information is stored in an appropriate manner and can be accessed in some way. In Figure 3, some databases are presented. These will play an essential role to enable the SW-tool to perform the required functionalities.

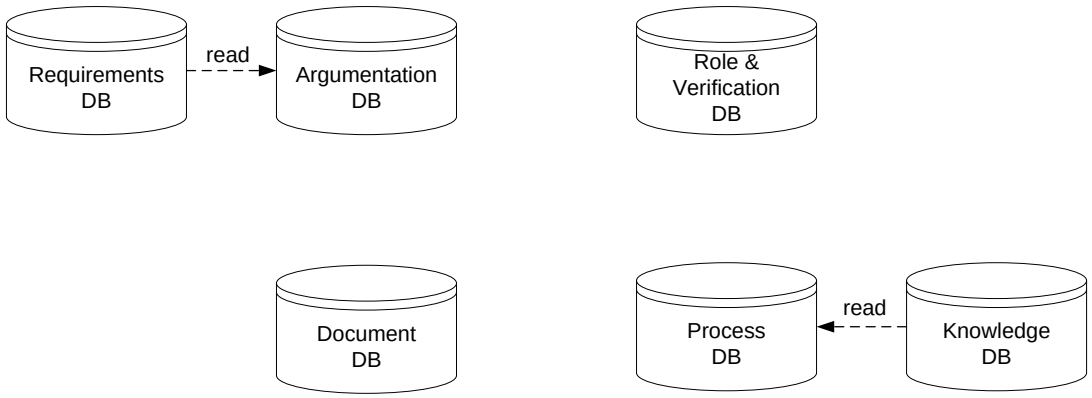

Figure 3: Some essential DB to perform the required supporting functions

Requirements DB:

In this DB all the requirements, especially the safety requirements that have to be met by the system are stored. The tool to be developed will link to these requirements to support the requirements tracing during the development phase of the project. The requirements itself will not be defined within WS-G. This workstream uses the input from e.g. WS-D and supports the tracing of the requirements.

Argumentation DB:

The purpose of the safety case is to present “a clear, comprehensive and defensible argument supported by calculation and procedures that a system is acceptably safe throughout its life” [4], or, shortly: “The safety case is a line of argumentation, not just a collection of facts.”[5] To achieve this, the structure of the argumentation of the overall system safety is represented within this DB. Here, the concept of the goal structured notation will be taken into account (see D.G.2.1 and D.G.2.2). As the safety argumentation very much depends on the (safety) requirements, these requirements will be linked to items in that DB. I.e. The overall safety is fulfilled, if all safety requirements are met. The clear structure of the safety-argumentation will support for discussions with the assessor.

Role & Verification DB:

In this DB to every document that has to be delivered a responsible project-member has to be identified. Additionally, in this DB the specific access rights of the employees and their contact details etc. are administrated.

Document DB:

All the developed documents will be stored in this DB. The document management system (DMS) will guarantee consistent and up to date referencing and versioning of these documents. In addition, it is foreseen that every document “knows” its responsible employee (see “Role & Verification DB”).

Process DB:

The normative processes and tasks as described in the CENELEC 50126 and 50128 norms will be represented within this DB. The workflow management system (WMF) will refer to the corresponding tasks, enabling it to “know” predecessor and successor tasks, the input and output documents, dependencies between tasks etc. In addition, to several tasks there may be additional knowledge e.g. from previous projects. This information is stored in the knowledge DB (see below) and will be linked to the Process DB.

Knowledge DB:

“Knowledge DB” here means all kinds of additional knowledge that may support the SaCa writer: That may be the knowledge from previous projects / products. Especially the knowledge corresponding to the country specific requirements for the acceptance of a safety case will play an essential role. Therefore, this information will be gathered by partners of WS-G in the months to come.

3.1.2 Process improving tasks

The way of using the information stored in the aforementioned databases can be seen in Figure 4. Depicted is a generic process with the following behavior:

Assume a document has been modified and uploaded to the document DB (1). If so, the DMS recognizes a new version or status of this document (e.g. from “draft” to “internal finalized”). That means, the argumentation DB will be updated (2a) and where appropriate, the next task(s) of the process DB will be triggered (2b). As the Process DB is linked to the Role & Verification DB (3), the skeleton of the documents to be developed next can automatically be generated (4) and the corresponding owner(s) will be notified (5).

As the requirements are linked to the Argumentation DB which itself is linked to the corresponding documents, one can identify the cornerstone that the very document plays in the overall safety argumentation. In addition, further hints may be given through the linkage with the knowledge DB.

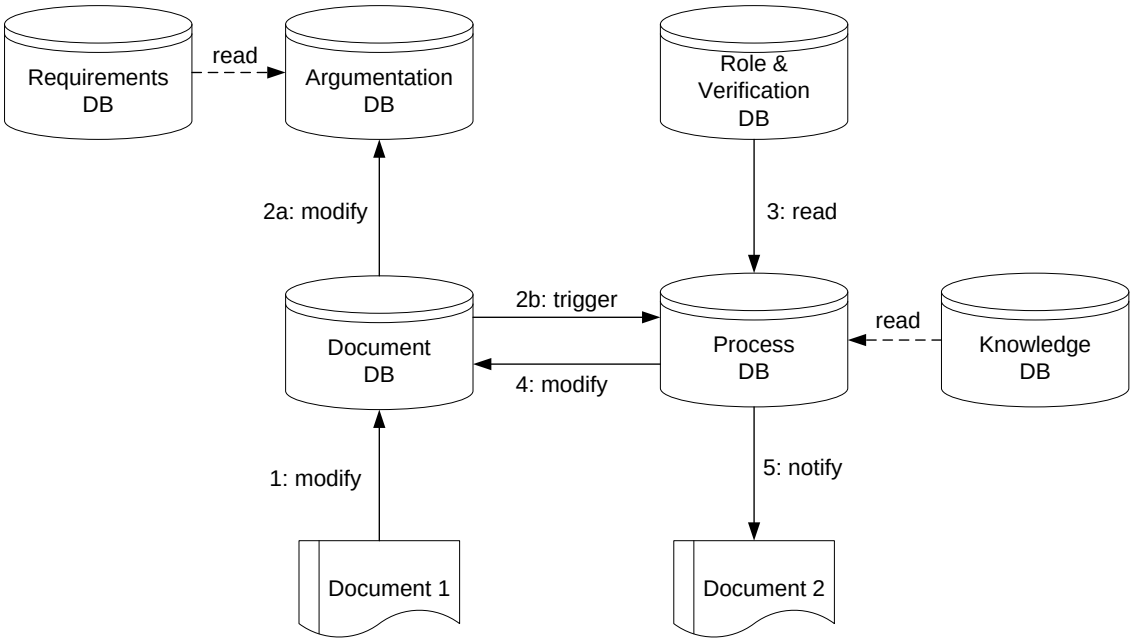

Figure 4: A generic process making use of the distributed information

The described principle is very generic. It can be applied to the most of the identified suporting functionalities, e.g.

- The development of a SaCa (Concept) right at the beginning of a project: All the information is in the Process DB and the Role & Verification DB (to appoint owners to the documents). In addition, the Argumentation DB links these docs to the required “line of argumentation”.
- Various notifications, e.g.
  - that a project risk analysis is to be performed.
  - that the assessor is to be contacted right at the beginning of the project.
  - that a hazard analysis, a risk assessment, have to be performed,
  - that the acceptable risk for each hazard has to be determined and
  - that the required risk reduction has to be calculated.
- As the required risk reductions can be seen as requirements, they are to be traced like “usual” requirements.

The uploading of the corresponding documents will lead to a consistent structure of documents, reflecting the evolution of the safety evidence.

3.1.3 The setup phase

To be able to use the tool in that way, it is necessary to set up and maintain the corresponding databases in a careful manner. It will turn out, that the essential and challenging part is the linkage of the requirements to the argumentation structure: As the demonstration of the fulfilment of a requirement is in general apportioned onto several documents, this apportionment needs thorough investigation of the overall safety argumentation structure and the requirements to be met. But, this is not an additional work – it has to be done in any case (at least it should have to be done). The presented approach does

not result in additional tasks, it only forces to structure and maintain them, leading to a consistent and up to date structure of documents.

3.1.4 Phase specific improving tasks

During the phases of the CENELEC process the following supportive functions for a guidance system have been taken into account. Their implementation on the basis of the aforementioned approach is quite easy. Here, we restrict onto the first 10 phases for the reasons given in the introduction of this section.

Phase 1 – Concept

Task: Define railway project concept

Support: Creation of a new project within the document management system and assistance to setup a folder and document structure. The setup of documents may consist of suitable templates.

Task: Review Safety

Support: Provide access to old projects within the document management system. In an early stage this function will be of no use, as there are no old projects within the system, but once practitioners get used to the system all information from old projects can be found (e.g. with a search based on categories or based on tagged document). To provide access to a knowledge database is another possibility to support the practitioner. The problem as stated above is the same. As long as the knowledge database is not filled with information it cannot be used to support the creation of a new safety case.

Phase 2 – System Definition

Task: Mission Profile + System Description

Support: Use of GSN Tool to design the new system. The GSN Tool is a component to provide an overview of the whole safety case. Up to now a short, but more detailed description of the tool can be found in deliverable D.G.4.2.

Task: Establish safety plan

Support: Setup the document and assign roles in the document management system.

Phase 3 – Risk Analysis

During this phase many different software tools are used to perform a risk analysis. As a long term goal import filters for various file formats might be supportive. Currently this is out of scope.

Task: Setup hazard log

Support: Setup the document within the DMS or provide a database table, blog or wiki to record all hazards. The proposed DMSs all provide such functionality. What is most practicable has to be decided by the practitioners, or even on a project to project basis.

Phase 4 – System requirements

Task: Define system requirements

Support: Setup documents for requirements. Provide import capabilities for requirements from other sources (files, databases). Assign requirements to the GSN Tree.

Phase 5 – Apportionment of system requirements

Task: Update safety plan

Support: Update the GSN Tree with the GSN Tool.

Phase 6 – Design and implementation

Task: Prepare generic safety case

Support: Update the GSN Tree with the GSN Tool. Setup the document skeleton for the generic safety case.

Phase 7 – Manufacturing

Task: Use hazard log

Support: Use the log, created in phase 3

Phase 8 – Installation

Task: Documentation

Support: Generate documentation from the DMS (e.g. tagged with 'user documentation'). Within the DMS it is possible to tag documents with arbitrary words. A concise index of tags could be valuable for a number of tasks where document retrieval is of major concern.

Phase 9 – System validation

Task: prepare application specific safety case

Support: Update the GSN Tree with the GSN Tool. Setup the document skeleton for the application specific safety case.

Phase 10 – System acceptance

Task: Documentation

Support: Use the document management system to generate the overall safety case documentation. Use the GSN Tool to verify completeness of the safety case. Use the GSN Tool to demonstrate soundness of the case to the assessor or the operator.

3.2 Further essential challenges

3.2.1 The dependencies between the various safety cases

The CENELEC 5012x norms differ between generic product SaCas (GPSC), generic application SaCas (GASC) and specific application SaCas (SASC). In the following their content and their relation will be outlined and the way of supporting the use of these different kinds by the supporting tool will be described:

The Generic Product Safety Case:

The term "generic product safety case" is somewhat misleading. Actually it should be named "generic safety case for a product", because the generic is the safety case, not the product [5]: If it is intended to use a certain product in a safety related application one has to specify the demands on the application, i.e. the conditions that have to be fulfilled in any safety related application if the very product is used. These are the "safety related application conditions" that have to be met, if the product is used.

In addition, one has to show, that the product itself fulfills the properties that were presumed when specifying the aforementioned application conditions. I.e. one has to demonstrate certain quality assurance routines were applied.

That means: In the GPSC one has to show two things:

1. A condition: ***Presumed that the product meets*** certain properties, ***then*** it can be used, if certain application conditions are met.
2. A presumption / fact: ***The product meets*** certain properties!

Only if the condition as well as the presumption has been shown for a certain product, it can be used in a certain application environment.

The Generic Application Safety Case:

If one does not specify exactly which particular products are being used in a given configuration but keeps to generic notions, that the application of these (unspecified / generic) products is a generic application. Similar to the GPSC one has to show again the fulfillment of a condition and a presumption:

1. A condition: ***a) Presumed that the products meet*** certain properties and

   b) Presumed that the planned configuration of products interacts in the intended way,

   then the planned configuration of the products is safe.

2. A presumption / fact: ***The planned configuration interacts in the intended way***!

The condition a) is to be shown by a GPSC, whereas condition b) as well as the presumption has to be shown in the GASC. Especially the presumption has to be argued by quality and safety assurance activities.

The Specific Application Safety Case:

The basis of a SASC are the GASA and specific products. In the SASC, three things have to be shown:

1. It has to be shown, that the chosen specific products “fit” into the generic application (this is condition a) of the GASC.
2. It has to be shown, that the conditions of the GASC are fulfilled by the specific use.
3. It has to be shown, that the overall system has been built correctly (this is similar to proving the facts of the GPSC and GASC).

The first two conditions are shown in the “Design Safety Case for the specific application”, the third condition is shown in the “Implementation Safety Case for the specific application”.

The tool to be provided by WS-G will take these relations into account and will guide the safety case writer through the process of developing the various safety cases and relating them to each other. Besides information in the knowledge DB, templates with explaining notes and sample SaCas will be provided.

3.2.2 The use of legacy systems

The scope of the CENELEC standards applies for systems that are newly developed. An approval according to CENELEC standards cannot be made retrospectively. If legacy systems are to be used, a comparison with the CENELEC requirements has to be made. In that way, missing technical evidence can be revealed and appropriate reasoning has to be prepared to make evident, that the existing and amended procedures comply with the major CENELEC requirements, as far as reasonably possible.

This approach is compliant with the ALARP principle and allows the CENELEC standards as a basis for the assessment, as required by the Authorities. In addition it allows to judge whether a comparable level of safety and confidence to the suitability of the system has been reached, as if it was originally developed according to CENELEC requirements.

Therefore, it is inevitable to contact the assessor right at the beginning of a project! One has to argue rights then, that complete compliance to the CENELEC standards is neither possible nor retrospectively foreseen by the standards. The certification process does not require strict adherence to the standards, but rather aims to reach a comparable level of systematic and random safety integrity.

Here again, the knowledge DB plays an essential role in the successful fulfillment of this tasks. The SaCa writer will be informed about these possibilities. Furthermore, an early coordination with the authorities and assessors is inevitable in this challenging and country- or even assessor-specific tasks!

3.2.3 Cross acceptance of safety cases

One aim of the CENELEC railway standards has been to create compatible rail systems based on common standards. This would result in cross-acceptance of safety approvals of sub-systems and equipment by the different railway authorities throughout Europe [6]. In practice, these possibilities are today only seldom used. One reason may be that safety cases differ essentially even if compliant to the 50129-structure.

WS-G aims at the provision of uniform SaCas developed with the corresponding tool. It is the long-term goal, to support cross acceptance by the provision of uniform SaCas.

In short term, only information in the knowledge DB and extensive discussions with assessors and authorities in early phase of the project may help.

3.3 Interfaces to related tasks of the Safety Case

In [7] it is stated that “The SaCaPro determines how the evidence produced in the progression of safety assessment can be structured in order to form an overall convincing argument about the safety of the system.”

That means, the evidence produced in the progression of safety assessment is *not* part of the safety case. The SaCa only uses these evidences and structures them in an appropriate way. This directly lays the basis to specify the system’s boundaries and interfaces: The results of the various phases, i.e. risk analyses (phase 3), the system requirements (phase 4) and apportionment (phase 5) etc. are used by the safety case process. The task of the safety case process is the appropriate linkage of these phase specific results to an overall safety argumentation.

Against this background, the tool to be implemented needs to provide interfaces to be able to link to appropriate results – e.g. an interface to read the safety and functional requirements, enabling the requirements tracing in an appropriate manner (see Figure 4). The results of other phases can be treated in a very similar way. In this context, risk analyses have already been mentioned. In the end, it is mostly about the structuring of the evidences that all the requirements and conditions have been fulfilled.

Section 4 – CONCLUSIONS

The functions that are needed by the practitioners as identified in interviews and on workshops have been aggregated and assigned to tasks within the safety case process. The approach to tackle the problems has been presented in the previous sections. The tool implementing these functionalities will support the SaCa writer in various ways:

1. Guidance through the processes;
2. Automation of tasks like notifications, consistent and up to date versioning and referencing;
3. The tracing of requirements, linkage to documents providing the corresponding evidence;
4. The structuring of safety evidences to an overall argumentation

are essential goals of the tool to be reached in the first step.

In the long term, a thorough integration of the various tools will be accomplished: A fully integration of the phase specific results in the SaCaPro-tool is the long term goal. Here, emphasis will be laid to support the phases after the system’s acceptance.

In addition, phase 3 – risk analyses – has been identified as one of the most challenging phases by the partners of WS-G. The long term goals will be to support this phase (see deliverable G.2.1).

Section 5 – BIBLIOGRAPHY

[1] 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.

[4] Wilson S. P., Kelly T.P., McDermid J.A.: “Safety Case Development: Current Practice, Future Prospects”, Proceedings of the 12th Annual CRS Workshop on Safety and Reliability of Computer Systems, Bruges1995, pp. 135-156, Springer-Verlag London Ltd.,1997.

[5] Nordland O.: “Safety Case Categories – Which One When?”, Redmill F., Anderson T.(Eds.):”Current Issues in Safety-critical Systems”, 11th Safety-critical Systems Symposium, February 2003 in Bristion, UK, Springer-Verlag London Ltd. 2003.

[6] Wigger P., vom Hövel R.: „Safety Assessment – Application of CENELEC Standards – Experience and Outlook, Copenhagen Metro Inauguration Seminar, 21.-22.11.2002, Copenhagen.

[7] Papadopoulos Y., McDermit J. A.: “The Potential for a Generic Approach to Certification of Safety-Critical Systems in the Transportation Sector”, Journal of Reliability Engineering and System Safety 63 (1999) 4e7-66, Elsevier Science, 1999.