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 2.2_Draft_Report_Ver2009-07-31**

Due date of deliverable	2009-06-30
Actual submission date	2009-08-14

Deliverable ID:	D.G.2.2
Deliverable Title:	Definition of short term goals
WP related:	Safety Case Process Strategy Development
Responsible partner:	Funkwerk
Task/Deliverable leader Name:	Carsten Trog
Contributors:	TUBS, Funkwerk, DLR, DB, BBR, RFI, Ansaldo, Invensys

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 2.2_Draft_Report_Ver2009-08-14
Revision: 5
Revision Date: 2009-08-14
Author: J. Schröder, Geltmar von Buxhoeveden, Jörg R. Müller
Dissemination level: CO

Approvals

	Name	Company	Date	Visa
WP leader	Jörg R. Müller	TUBS		
WS Leader	C. Trog/J. R. Müller	Funkwerk/TUBS		
Project Manager				
Steering Board				

Document history

Revision	Date	Modification	Author
1	2009-06-22	Creation of document	J. Schröder
2	2009-07-02	Moved attachment to report D.G.2.3	J. Schröder
3	2009-07-31	Revised and restructured, introduction of GSN integrated	J. R. Müller
4	2009-08-11	Short Term Goals added	G.Buxhoeveden
5	2009-08-14	minor modifications	J. R. Müller

TABLE OF CONTENTS

Glossary

The following abbreviations are applied in this document:

BBS	Bulletin Board System
C	Communication
CS	Creation of Safety Case
DB	Data Base
DMS	Document Management System
GSN	Goal Structuring Notation
SaCa	Safety Case
SM	Safety Management
W	Workflow

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

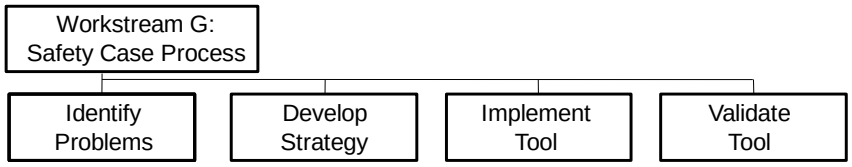

Figure 1: One can specify four phases to achieve the aim of Workstream G

According to the DoW for the second and third phase the following procedure was planned:

1. Define long term and short term goals (task 2.1 and task 2.2)
2. Estimate economical benefit (task 2.3)
3. Specify requirement description technique (task 3.2)
4. Specification of improved Safety Case Process (task 4.1)
5. Specification of system and software requirements (task 4.2)
6. Implementation of tools (task 5.1)

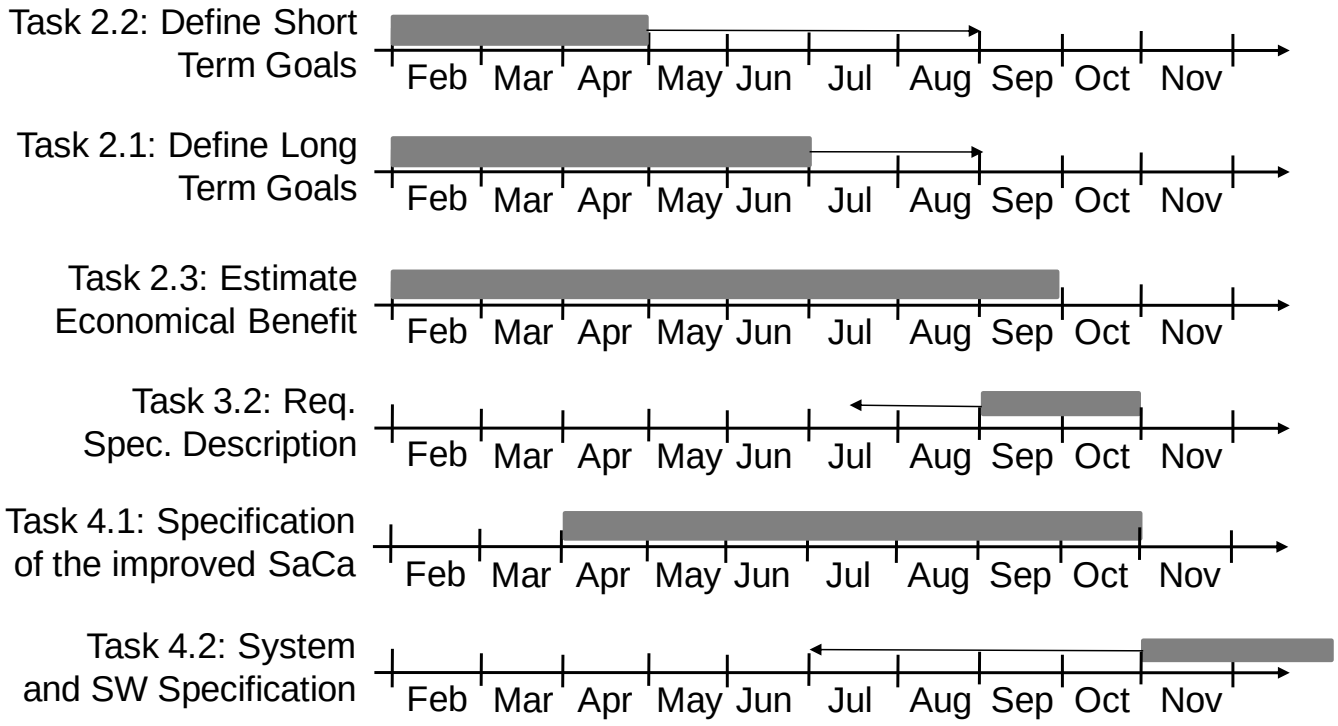

Figure 2: Rescheduling the Tasks in WS G

According to the interviews as well as to the findings of the second workshop, it became clear, that most problems to be solved are related to the realm of workflow and document management. Many of the desired functions have already been implemented in freely available open source applications. Therefore it was agreed, that resources shouldn't be wasted on implementing functions that are available elsewhere. The advantage of using open source software is that a lot of desired functions come "for free", thus offering "more benefit" for "less cost". The drawback on the other hand is that a few tasks have to be rescheduled. The new project plan is somewhat less sequential but more interwoven, as some tasks now happen in parallel – see figure 2.

1.2 The aim of task G.2.2

Some of the desirable goals that will lead to an improvement of safety case processes and thus to saving of cost (economical benefit) are so important that they should be achieved before the end of INESS project. In work package G.2.2 (short term goals) these goals are specified. Goals that cannot be achieved in INESS due to limited resources and time will be specified in WP G.2.1 (long term goals).

Work package G.2.2 is closely linked to work package G.2.1, as every goal fits in only one of the both categories.

An essential part of long and short term goals are the functions to be implemented in the tool that has to be developed in WS G, so results of both work packages will be lists of these functions. In addition, it turned out, that some of these functions have to be explained in more detail as they are not commonly known (e.g. the GSN-approach).

Section 2 – Definition of Short Term Goals

2.1 Approach and Strategy

The main goal of workstream G is to improve the safety case processes and thus to safe costs. In the scope of INESS this can be achieved by setting up a list of recommendations for a good process and/or by implementing software-tool functions that assist the users in following an efficient process. From the practical point of view, the main focus of this work package is on possible tool functions.

Possible tool functions can be derived from the findings of previous tasks. In Task G.1.2 (Collecting Users' Experiences) a list of good and bad practices in the Safety Case Process has been created by evaluating interview results and discussing them on a WS-G workshop on 2009-06-16. A possible tool function was derived from each of the practices and some additional helpful tool functions were identified by the practitioners.

Short term goals should be achieved within INESS. That means, only a reasonable number of functions that can be implemented in reasonable time can be assigned to short term goals. All others have to be assigned to long term goals (see D.G.2.1).

It has been realised that the WS-G tool will have to be based on existing open source software if a noteworthy part of the possible functions shall be implemented before the end of the INESS project. Accordingly, the implementation effort will heavily depend on the software chosen as a basis. Therefore, appropriate basic open-source software has to be evaluated with respect to the effort to implement the identified tool functions. Then, the implementation effort can be estimated credibly. The functions which are easy to implement and/or lead to a high benefit will be assigned to short term goals, all remaining functions will be assigned to long term goals.

2.2 The identified short Term Goals

The identified short term goals can be split up into three categories.

- Functions related to document management
- Functions related to workflow
- Functions related to the safety case argument

Figure 3: Function categories and their relationships

These functions are related to each other (see Figure 3):

The DMS is a system that can exist autonomously. Workflows are a special functions of a DMS and are interpreted by a DMS. As such, workflows can be seen as a set of rules for the DMS, that specify what to do under certain circumstances.

The workflows are designed by a workflow tool. Such a tool offers graphical representations of workflow elements and it is easier to work with it in comparison to the DMS which also offers (basic) workflow design functions.

The functions related to the safety case argument will be handled by the GSN-Tool. This tool will be used to model a safety case argument and link back to documents in the DMS, which support the safety case argument (see section 2.2.3.

Each category and the associated functions will be described in the following sections.

2.2.1 Functions related to Document Management

According to the interviews as well as to the findings of the second workshop, it became clear, that most problems to be solved are related to the realm of workflow and document management (see list of functions in D.G.4.2). Many of the desired functions have already been implemented in freely available open source applications. Therefore it was agreed, that resources shouldn't be wasted on implementing functions that are available elsewhere. The advantage of using open source software is that a lot of desired functions come "for free", thus offering "more benefit" for "less cost". Nevertheless a lot of work has to be put in adjusting the existing software to fit the needs of the project. The adjustment will on one hand be in the area of configuration on the other hand existing software has to be customized to make modules from different sources work together.

Therefore it can be expected that the "commonly" used document-management functions will be implemented in the final tool of WS-G.

The common functions of a Document Management System (DMS) are described in the following section.

2.2.1.1 Archiving, Backup

The DMS shall provide a single place for all documents related to the SaCa. Documents created by users will be stored within the DMS. Documents from third parties shall be uploaded and integrated in the DMS as well. The system shall provide backup facilities to guarantee constant availability to the user.

2.2.1.2 Collaboration

To enhance communication between all stakeholders of a SaCa, the DMS shall be used as a communication platform. Tools for scheduling meetings and milestones shall be available. Tools for information exchange (Bulletin Board System) shall be made available to inform users of the overall state of a SaCa.

2.2.1.3 Document centric functions

Once a document is stored within the DMS a variety of functions shall be available to make changes to a document, to link a document to other resources or to search within a document. From the interviews of Deliverable D.G.1.2 and from the 2nd workshop of WS G it became clear that the most benefit for practitioners involved in the safety case can be expected from a coherent management of documents. Stated problems of manually adjusted version numbers, wrong references of documents and unsatisfying search functions should be solved by using a DMS. The following functions shall be provided by the DMS:

- **Versioning / Tagging**: Every time a document is changed, a version number is incremented automatically. The strategy how major/minor numbers are incremented can be configured. Furthermore documents have a 'state' (e.g. 'approved', 'verified') and documents can be 'tagged' (e.g. 'safety relevant').
- **Notification**: Users of documents can be notified, if a document changed. Notification can be done within the DMS or via email.
- **Link functions**: Documents within a SaCa relate to each other. Such links shall be set within the DMS. Links to documents that are based on the type of document shall be used to realize the peculiarities of the SaCa. The following types of links shall be possible:
    - *link between any documents* (DMS standard): Any two documents can be linked to each other. The DMS shall take care that all parties involved in document creation are informed about changes of the document.
    - *link to hazard log* (SaCa peculiarity): Any document with information relevant to the hazard log shall link to the hazard log. The other way around from the hazard logs view it shall be possible to get to all the source documents that provide information to the hazard log. No information can get lost, an assessor gets better access to relevant documents.

- *link to risk analysis* (SaCa peculiarity): The results of a risk analysis will usually be calculated by a set of tools, that are not connected to the DMS. Nevertheless it shall be possible to link to documents which summarize the results of the calculation tools.
- *link to lessons learned database* (SaCa peculiarity): All information relevant to the safety case could be stored in the DMS. The user shall get the possibility to store his knowledge within the system, so other people can access this information for following projects, thus reducing practitioners search time for already known cases.
- *link to role and verification plan* (SaCa peculiarity): It shall be possible to see which persons are involved in the creation, validation and verification of a document. A link to a (project specific) role and verification plan shall offer this function within the DMS.
- *link to requirements* (SaCa peculiarity): Tracing of requirements is often done by hand (e.g. with Excel). This information is not connected to the creation and manipulation of documents related to the SaCa. Once requirements are linked within the DMS the fulfillment shall be checked more easily.

- **Search functions**: the following search functions shall be provided by the tool
  - Search within document meta-information (e.g. author, version, language etc.)
  - Search within all documents (i.e. all documents that can be indexed by the DMS)
  - Search within documents related to a project
  - Search within the BBS / Knowledge Database / Lessons learned Database / Product + Expert Database / Online Help
- **Checklists**: The system shall provide checklists for different stages of the SaCa. A checklist shall provide facilities to note information like degree of completeness, conformance to standard or fulfillment of requirement. The following checklists shall be provided:
  - *Open items checklist*: A user involved in the SaCa can easily see, which steps haven't been dealt with and who should be contacted to get missing information. Furthermore steps that a document will be in in the future can be gathered from such a checklist, thus enhancing the transparency of the workflow of a document.
  - *Workflow checklist*: Documents that are related to workflows can be "stuck" within a workflow because it did not get approval by a person, who might be out of office. The tool shall deal with such situations.
  - *Document status checklist*: In an overview the status of all SaCa related documents shall be shown to get a report of missing documents to complete a SaCa.
  - *Requirements checklist*: Requirements are not only linked to documents of the SaCa as mentioned above. The tool shall provide a checklist that reports the fulfillment of all requirements.
  - EN50128 / EN50129 conformance checklist: Practitioners are often unsure which part of EN 50128 / EN 50129 they currently deal with. A checklist shall make the processes of EN 50128 / EN 50129 more transparent to all parties involved.

2.2.2 Workflow Functions

Functions related to the workflow shall be modeled in a workflow tool (figure 4). The workflows shall be usable by the DMS. Workflows have to be modeled to fit in the environment of a company, therefore it cannot be predicted how complex workflows might get, as they might differ quite heavily from one company to another. The following basic workflow functions shall be reusable within every company and shall be realized by the workflow tool.

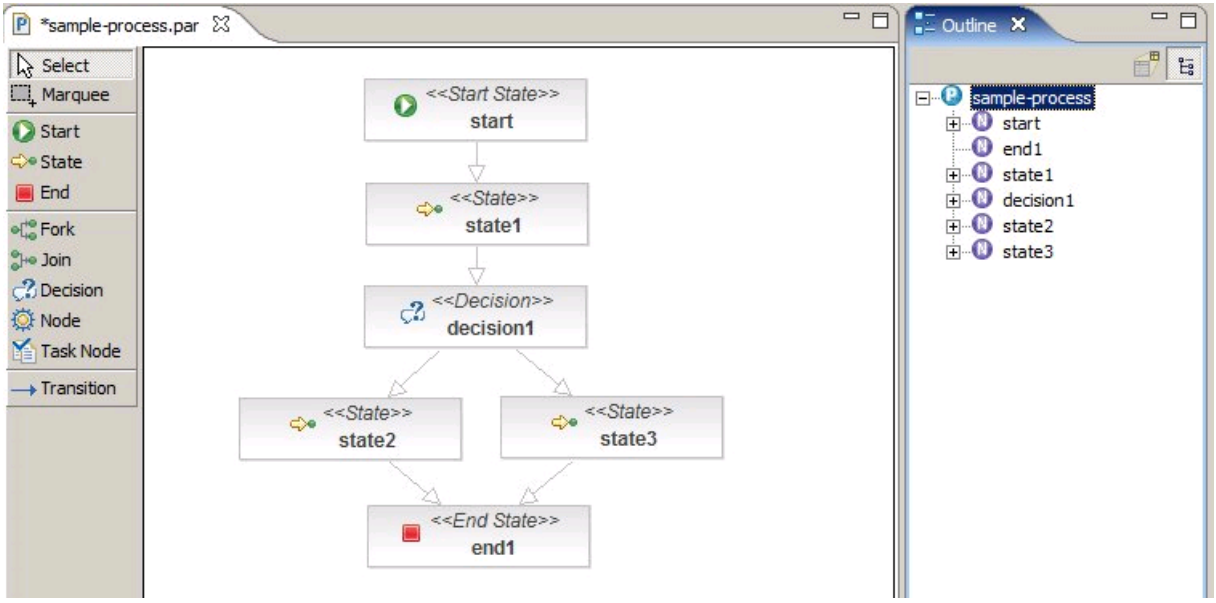

Figure 4: Workflow Tool

2.2.2.1 Approval / rejection processes

Within the SaCa workflow documents are committed from one party to another. Depending on the workflow, documents can change their state (e.g. from 'not approved' to 'approved') or can be propagated to another stage in the workflow process (e.g. move from 'testing' to 'verification').

The workflow tool shall provide a graphical user interface to define such workflows.

2.2.2.2 Document move

Depending on the structure of a workflow different automatic manipulations of a document can occur (e.g. a document is moved to a different folder, if another work group is responsible for the next step). The move of a document could also be used to assign a document to different roles in the SaCa process. Thus the document would only get to be reviewed by a person with the right role in the project. This would mean that depending on the SIL that has to be achieved different workflows would have to be configured. (I.e. in lower SIL development and verification could be done by the same person, while in higher SIL certain tasks have to be done by different people).

2.2.2.3 Document rename

A document is automatically renamed from e.g. 'draft' to 'final', as soon as it has been approved. Document names stay consistent opposed to manual naming conventions.

2.2.2.4 Document version change

A version number is incremented automatically if a document is saved, thus enforcing consistency of the documentation.

2.2.2.5 Document state change

A document changes its state, once a user has performed a certain action with the document (e.g. a user has approved a document).

2.2.3 Functions related to the safety case argument

The argumentation of the safety of e.g. a product has been identified as a critical part in the authorization of a safety critical system. As there are good experiences with a tool supporting this task, it has been decided to provide at least the basic functionalities of such a tool.

The principal objective of a safety case is to present an argument based on evidences that a system is acceptably safe to operate in a given context, i.e. that the system meets the requirements. However, the safety *argument* is often poorly communicated through the textual narrative of safety case reports (see e.g. [1, 2])

Therefore, one can state that a safety case consists of three principal elements: requirements, argument and evidence. The relationship between these three elements is depicted in the following Figure 5.

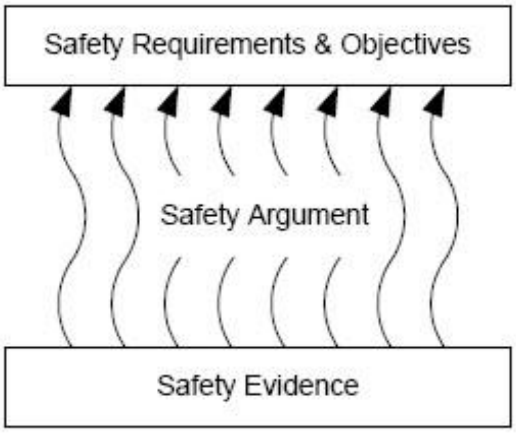

Figure 5: The Role of Safety Argumentation

The safety argument is that which communicates the relationship between the evidence and objectives. In practice, the reason of a failing of a safety cases is that the role of the safety argument is often neglected. In such safety cases, many pages of supporting evidence are often presented (e.g. hundreds of pages of fault trees or Failure Modes and Effects Analysis tables), but little is done to explain how this evidence relates to the safety objectives. The reader is often left to guess at an unwritten and implicit argument.

Both argument and evidence are crucial elements of the safety case that must go hand-in-hand. Argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without argument is unexplained – it can be unclear that (or how) safety objectives have been satisfied.

To overcome the problems of communicating the safety argument the Goal Structuring Notation (GSN) was developed at the University of York. The notation uses a graphical representation for goals, strategies and solutions to depict elements of the safety case (Figure 6). With GSN as a notational base a tool shall be developed to model safety arguments.

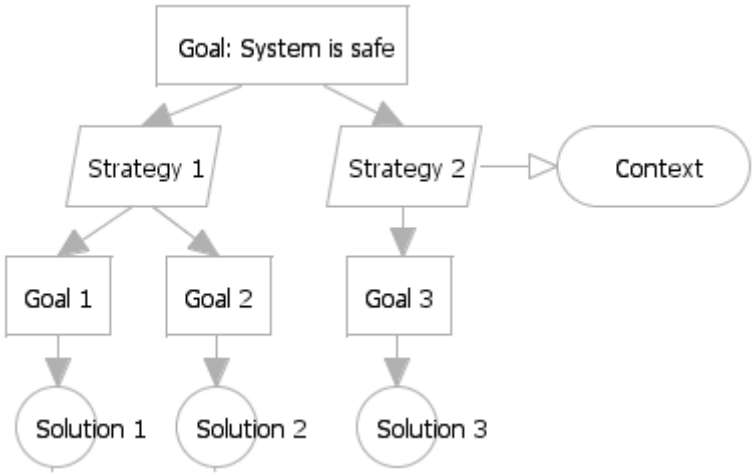

Figure 6: GSN example

2.2.3.1 GSN Tool

A unified representation of the SaCa shall help customers and assessors to get a better understanding of a system.

The GSN Tool shall provide the possibility to model a safety argument according to the Goal Structuring Notation. A first implementation shall offer a drawing facility to conform to GSN.

As the submission of this deliverable was rescheduled to provide time for evaluation of existing tools a production of a GSN Tool prototype could be realized. It is possible to draw models that conform to the Goal Structuring Notation.

2.2.3.2 GSN - DMS Connection

Whether this is a short term or a long term goal cannot be said at the moment. But it is regarded to be a helpful function to implement a connection from the GSN Tool to the DMS (as depicted in the screenshot, Figure 7). With such an implementation the GSN Tool would be a modeling tool for the safety argument on one hand and on the other hand could be a reporting tool to check if all documentation for a safety case is complete.

2.3 List of functions

A list of all functions that were discussed at the 2nd workshop and were identified as short term goals can be found in the attached Excel document INESS_WS G_Deliverable 2.2_DMS-Function_Comparison_short_term.xls.

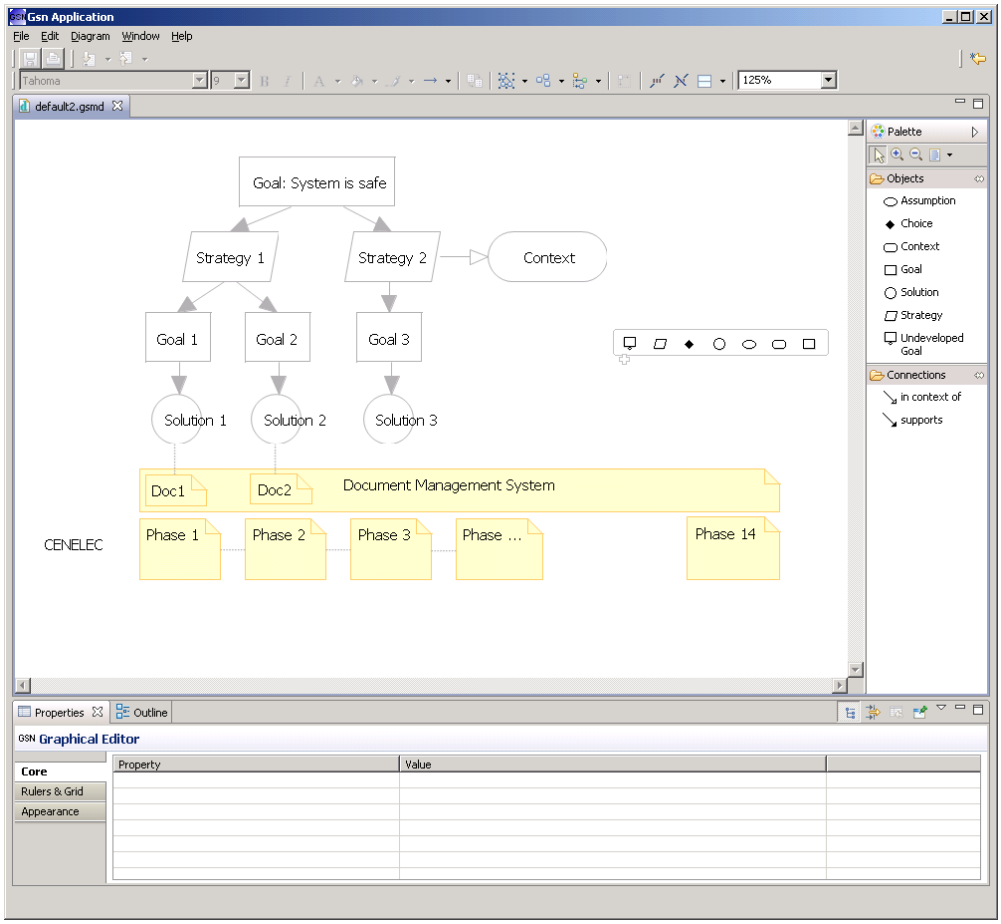

Figure 7: GSN Tool prototype

Section 3 – Conclusions

The decision to use an existing open source DMS shall offer the possibility to realize most of the desired functions to provide a system suitable to manage the SaCa process. The alternative to start "programming from scratch" and not using existing solutions would have provided only a single piece of "proof of concept software". With the strategy of using existing tools and adjusting them to the needs of the INESS project a usable prototype of a SaCa management system can be expected.

Section 4 – Bibliography

[1] T. P. Kelly: Arguing Safety – A Systematic Approach to Safety Case Management, DPhil Thesis YCST99-05, Department of Computer Science, University of York, UK, 1998.

[2] Tim Kelly and Rob Weaver: The Goal Structuring Notation – A Safety Argument Notation, Department of Computer Science and Department of Management Studies, University of York, UK.