The Safety Case according to CENELEC 50129 – Efficient Preparation and Communication

J. R. Müller, G. v. Buxhoeveden, E. Schnieder, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Braunschweig;

Kurzfassung

Das europäische Projekt INESS (Integrated European Signalling System) stellt sich der Aufgabe die Spezifikation für eine neue Generation von interoperablen Stellwerken zu erstellen. Die Spezifikation soll eine Integration in das bestehende ERTMS (European Railway Traffic Management System) gewährleisten, sowie eine kosteneffiziente Migration ermöglichen. Die TU Braunschweig ist für das Teilprojekt „Sicherheitsnachweis“ (safety case) verantwortlich. Ziel dabei ist es den Sicherheitsnachweis in kürzerer Zeit zu führen und so den Herstellern und Betreibern unnötige oder redundante Tätigkeiten zu ersparen. Am Ergebnis dieses Teilprojekts waren zwölf weitere europäische Partner beteiligt.

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. The Technical University of Braunschweig is responsible for that part of INESS that deals with the safety case process. The aim of this essential subproject 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. In this workstream a dozen European partners have contributed to the results.

1 Introduction to the INESS project

1.1 Railway signalling: From traditional national solutions towards ERTMS compliance

Today there are over 20 rail signalling and speed-control systems operating in Europe, all of which are completely incompatible with each other. This complexity leads to additional costs and increased risk of breakdowns. Promoted by the European Commission and driven by the need for interoperability, opening of procurement markets, increase of efficiency and harmonising of safety in the European railway system, the European Rail Traffic Management System (ERTMS) aims to remedy this lack of unification in the signalling and speed control.

Further momentum can be added by ensuring that the most significant sub-systems of railway command and control systems, such as an interlocking (which is at the heart of a

traditional signalling subsystem by which commands can be issued to control devices and information can be obtained about the status of those elements with a defined level of safety) are developed in line with this programme.

1.2 The importance of interlocking: Huge potential market for new interlocking

In many European railway networks, there is a huge potential need for renewal of heritage signalling installations and the interlocking on which they depend. However, economical analyses of several railways show that a renewal at current cost levels is becoming increasingly more difficult to justify in cost-benefit terms.

For this reason, both UIC and UNIFE consider that it is now opportune to address these aspects within the context of the present INESS project.

The INESS project aims at contributing to the above mentioned European initiatives by 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. This approach is believed to have the potential to reduce costs, speed up the migration to ERTMS and therefore, help increase the competitiveness of the railway transport.

Railway Operators, Infrastructure Managers and the signalling supply industry agree that the key scope of the INESS project should be exploring and standardising the interfaces between interlocking systems and the adjoining command and control sub-systems such as centralised traffic control, neighbouring interlocking and ETCS Radio-block centres and possibly, depending on the economic justification, outdoor devices.

1.3 Scope of the safety case workstream

One of the main scientific and technological objectives of the INESS project is to identify an efficient way for an interpretation of the safety case process according to the relevant CENELEC standards and to develop improvement strategies coherent with the yet to be harmonised requirements of the various National Safety Authorities thus reducing time and money for the safety case in industry by avoiding unnecessary or redundant procedures. This activity has the additional potential to lead to the facilitation of the development of a harmonised approach by all such authorities.

2 Experiences of the practitioners and the improvement of the safety case process

2.1 Experiences of the practitioners

The collection of the practitioners' experiences and interpretation of the norms, the time and money consuming tasks as well as proposals for the support of the safety case process in practice were of main concern.

The task of interviewing the partners was mainly performed by researchers of Technical University Braunschweig – a research institution instead of an industry partner. This was necessary because the partners had to speak openly and had to admit where they had problems and saw difficulties. Thus, it had to be clear and assured that such an interview was not mixed up with an audit. In addition, the partners had to trust the interviewer that their

reputation would not be damaged. An industry partner as an interviewer might have hampered creating a trustworthy atmosphere.

2.2 What is the safety case process?

Before improving the safety case process, one has to agree on what the safety case actually is. Many definitions can be found in the literature. One of the most reasonable definitions has been formulated by the British Ministry of Defence (see [5]). They define a safety case as “a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.” In this definition, the distinction between the “argumentation” and the “evidences” is emphasised. From a logical point of view, this distinction corresponds to the distinction between rules and facts.

During the interviews it turned out, that some partners had very good experiences with this approach: The distinction between the safety argumentation and the evidences led to an improvement of the readability of safety cases and to an improvement of the discussions with the legal authorities.

2.3 The transparency of the safety argument

Starting from a set of requirements, the strategy to demonstrate the safety of a product is to be developed and graphically described (see figure 1). In general, the fulfilment of each requirement will be shown by a tree of argumentation. The leaves of these trees specify the corresponding evidences (e.g. test results or analysis results). These evidences have to be documented and the corresponding documents accrue during the corresponding phases of the CENELEC development process described in the EN 50126.

It turned out that such graphical argumentation structures ease the discussions with legal authorities as they understand the essence of the argumentation strategy in a very short time. In addition, through referencing the corresponding documents in the leaves of these trees, information retrieval is strongly supported.

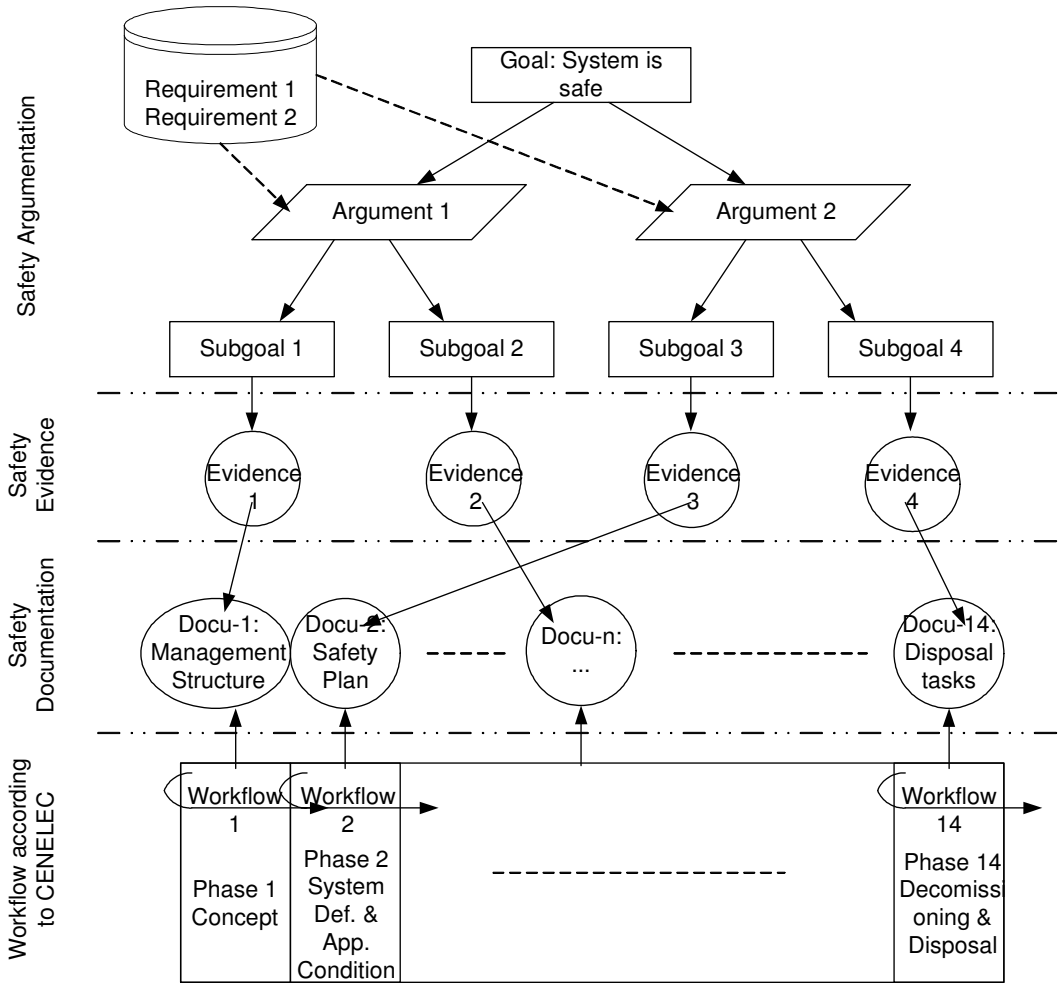

Figure 1: Safety case argumentation vs. safety evidence

3 Improvement by automation

3.1 The improved safety case process

The definition of an “improved” safety case process is the result of the shortcomings and promising approaches of the safety case process in practice. The improved safety case process consists of

- the normative safety case processes (EN 5012x),
- the tasks that improve these processes,
- and the knowledge archived in an adequate way as the basis for the improving tasks of 2.).

The normative safety case processes have been modelled with event-driven process chains (see [4]). The result is a transparent and easy to understand visualisation of the sequential and parallel processes interacting with each other within the overall normative CENELEC safety case framework (see [1-3]). Within this model it is possible to identify by just one look in which phase which requirements are to be complied with and which documents are to be developed etc.

3.2 The automation of the improved process

According to the results of the interviews 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 to use the advantages of open source software: In that way, a lot of desired functions come “for free”, thus offering “more benefit” for “less cost”. On the basis of freely available tools, the processes are currently being automated. To be able to do so, it is presupposed that various sources of information are available:

It is assumed that the documents that are to be produced during the development process are stored in a database (DB – please note, that “database” in this context only means “stored in an appropriate manner” – it may be an electronic folder as well).

The requirements have to be made available in an adequate, traceable manner.

In the “Process DB” the normative processes are represented by workflows. These workflows represent the core of the automation and control the process workflow.

In the “Role & Verification DB”, information about project members, their responsibilities and rights within the project is stored.

In the “Knowledge DB” nation specific requirements, lessons learned etc. are stored. Some of the interview-partners even store the specific interests of certifiers, to be able to align the certification-discussions to the corresponding specific expectations.

3.3 A generic workflow

Granted that during the development process a document has been uploaded to the document DB with a changed status, e.g. the status has changed from “draft” to “approved” (1), then through linking the argumentation tree with the document DB (2a), the argumentation tree is updated automatically and it is indicated that the corresponding requirement has been met. The uploaded document may in addition indicate the achievement of a milestone and therefore trigger – according to the normative description of the processes – a subsequent task (2b). If so, a skeleton of a new document is being generated with the corresponding information, e.g. the responsible project member (3) and information from previous projects concerning this document is made available. Accordingly, uploading this new document to the document DB (4) leads to its modification. Finally, the responsible person for this new document/task is automatically being informed (5).

4 Estimated benefit

Within the INESS project, there is a subproject that deals with the life cycle costs of interlocking systems. Here, the costs to develop according to CENELEC have been subsumed under the labour costs. Conservative estimations assume that at least 10% to 15% of the CENELEC related costs can be saved. Other estimations assume this fraction to be up to 50%.

The reasons for the difference between these two estimations are the following: First of all, there were no figures available about the costs of a safety case. None of the project partners could give more than just rough estimations. In addition, it is assumed that the costs vary significantly according to complexity and duration of a project: If project members are

replaced during the project time, the new members need to get an overview over possibly hundreds of documents. The structured argumentation and a concise versioning, document history and referencing is of great importance and helps to save time and money. Another reason for the different estimation lies in the variety of projects: Development or software projects have a huge fraction of CENELEC costs, whereas implementation projects do not.

5 Demonstration of the software tool

The participants of workstream G decided to use existing open source components to facilitate and ease the development of a safety case Tool. It was realised that many, if not most functions, that were identified in user interviews and in workshop discussions could be achieved with a Document Management System (DMS).

A generic system architecture, which depicts the system requirements, is shown in (figure 2). The whole system is client-server based. Most functions are based on exchangeable standard components (operating system, Java runtime environment, web browser, office software, and workflow tool).

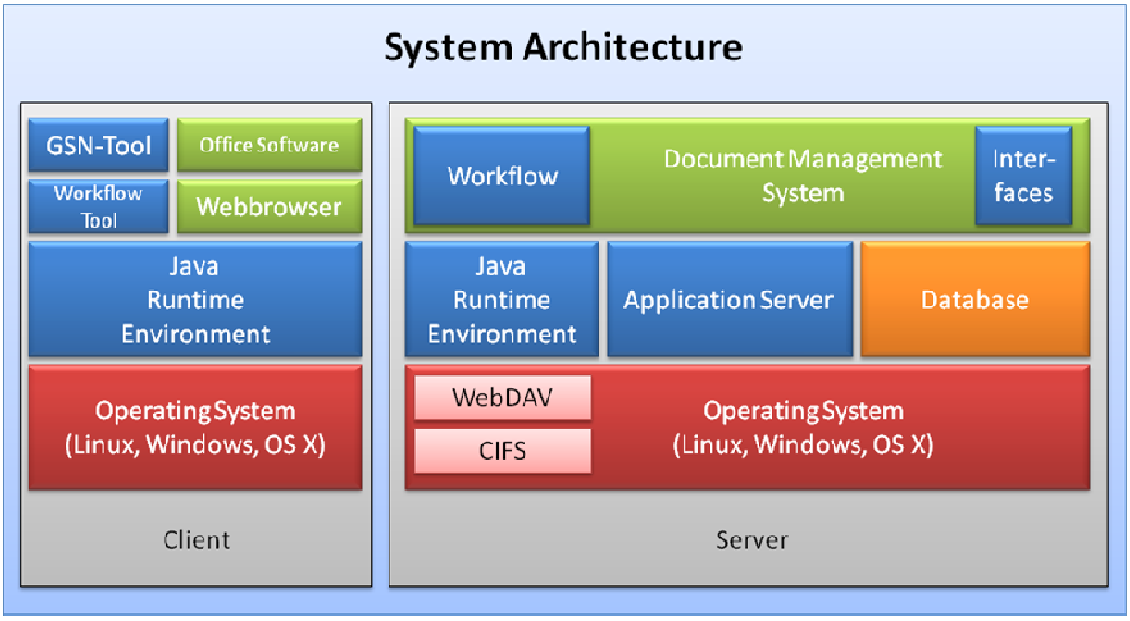

Figure 2: Software tool system architecture

In addition to the DMS, a special tool (the tool to define a goal structure (see [7]) will be developed to support the safety argumentation. Such a tool provides a defined view on all the documents relevant for the safety case. This tool should be easy to use and build on things already learned or already necessary for the safety case process. Therefore it was decided to use the same programming tools and methodologies to develop the GSN tool, as for the already existing workflow modelling tools. As the programming tools had to be evaluated in a 'real life' environment, it was already possible to produce a prototype. A screenshot of the GSN tool prototype can be seen in (figure 3).

6 Conclusions

The conduction of open interviews with practitioners of the CENELEC development process provided valuable insight in the adoption and application of processes described in a norm to the real life working environments found at the participating project partners.

Questionnaires on time spent for tasks related to the production of the safety case documents provided good information on the economical impact and cost reduction potential of an improved safety case.

The improved safety case procedure proposed in this paper is currently being implemented by one of the project partners. As a part of the INESS project the forthcoming software tool proposed in this paper will be used to produce the safety case documents for a real life industry project.

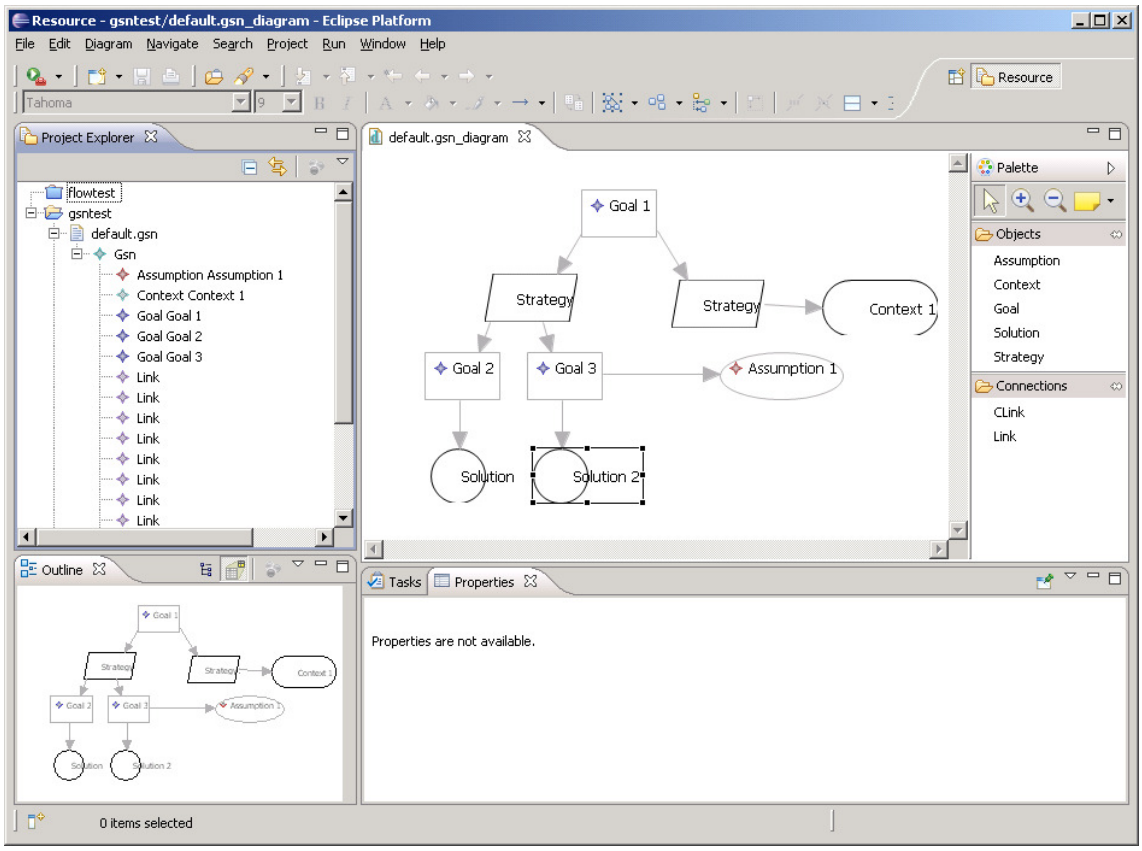

Figure 3: GSN-tool prototype

7 Outlook

As described in chapter 2 the main focus of safety case enhancement so far is on the supplier and operator side. On the 2nd year's EC review meeting it was pointed out that further enhancements could be realised by analysing the safety case processes within the national safety authorities (NSA) and syncing the achievements of INESS workstream G with them. Currently a questionnaire is being developed within the workstream which will be disseminated in the first quarter of 2011. Interviews with the NSAs similar to the interviews with the practitioners will take place in the second quarter of 2011.

8 References

[1] CENELEC (1999a). EN 50126: Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999.

[2] CENELEC (1999b) .EN 50128: Railway Applications – Communications, Signalling and Processing Systems – Software for Railway Control and Protection Systems, 1999.

[3] CENELEC (1999c). EN 50129: Railway Applications – Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling, 1999.

[4] Keller, G. et al. (1992). *Semantische Prozessmodellierung auf der Grundlage ereignisgesteuerter Prozessketten (EPK)*. Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89 (in German), University of Saarland, Saarbrücken, 1992.

[5] Ministry of Defence (2007). *Safety Management Requirements for Defence Systems*, Defence Standard 00-56 (Issue 4), U.K. Ministry of Defence, 2007.

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

[7] 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.