The improvement of the safety-case process in practice: from problems and a promising approach to highly automated safety case guidance

J. R. Müeller[1], W. Zheng[2] & E. Schnieder[1]
[1] *Institute for Traffic Safety and Automation Engineering,*
Technical University of Braunschweig, Germany
[2] *School of Electrical and Information Engineering,*
Beijing Jiaotong University, China

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 leader of the 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.

Keywords: INESS, safety case, interlocking system, interoperability.

1 Introduction to the INESS project

1.1 Railway signalling systems transitioning 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

WIT Transactions on The Built Environment, Vol 114, © 2010 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR100721

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.

The convergence of the ERTMS vision in the railway sector, with the accompanying European Train Control System (ETCS) and Global System for Mobile Communications – Railways (GSM-R) standards, has brought about a degree of cross border co-operation not previously seen. Railway Operators and Infrastructure Managers are now engaging with a united supply industry to achieve the common goal of an interoperable system, within the framework of European legislation, which potentially forms a set of legal obligations all have to comply with. A set of standards has been created within these obligations but, as with any standardisation process, joint efforts are needed from all parties to translate such work into tangible results.

Furthermore, the new Technical Specifications for Interoperability (TSI) related to Command/Control/Signalling for Conventional Rail foresees that ERTMS will be rolled out over international corridors covering initial inception kernels (as well as on many other projects outside these kernels). The European Commission, the European Railway Associations together with the Railway Supply Industry have agreed to work closely together to define a realisable migration strategy for ERTMS. This unique co-operation has offered the possibility to co-ordinate the implementation of the constituent parts of ERTMS – the traffic-management layer, the train communication and train control system.

Further momentum can be added by ensuring that the most significant subsystems of railway command and control systems, such as interlockings (which are at the heart of 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 interlockings: huge potential market for new interlockings

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

One important method for reducing the costs of signalling renewal is considered to be the introduction of a greater degree of standardisation, both in terms of determining the functionality of signalling systems, and in terms of enabling a more modular approach to the various parts of the signalling subsystems and enabling renewals to better take into account the differences in the life expectancy of the various in- and outdoor devices including cabling, point operating equipment etc.

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 having the potential to reduce costs, speed up the migration to ERTMS and therefore, help increasing 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 interlockings 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 potential to lead, in addition, to the facilitation of the development of a harmonised approach by all such authorities.

2 Experiences of the practitioners – the basis to improve the safety case

The collection of the practitioner’s 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.

To collect the users’ experiences of railway operators and suppliers with the CENELEC development process in general and in its safety aspects in particular, interviews with the project partners have been held. With the intention of finding requirements for a future tool, the problems as well as promising approaches for solving problems in practice were brought into focus. Possible ideas for desirable functions of a future tool were collected. Existing tools used by the partners were also kept in mind as a future tool will not be allowed to interfere with them.

The task of interviewing the partners was performed mainly by the researchers from the Technical University of Braunschweig; this, 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.

3 The improved safety case process

3.1 What is the safety case?

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:

In the EN 50129 [1], a safety case is defined as "[…] the documented demonstration that the product complies with the specified safety requirements."). This definition is regarded as only of little help as it does not state how to demonstrate that the system complies with the requirements.

Odd Nordland defines in [5]: "The safety case is a line of argumentation, not just a collection of facts." This definition at least gives information what a safety case is not: "a collection of facts".

The most reasonable definition has been formulated by the British defence ministry [6]. 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.

3.2 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 Fig.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 the legal authorities as they achieve 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.

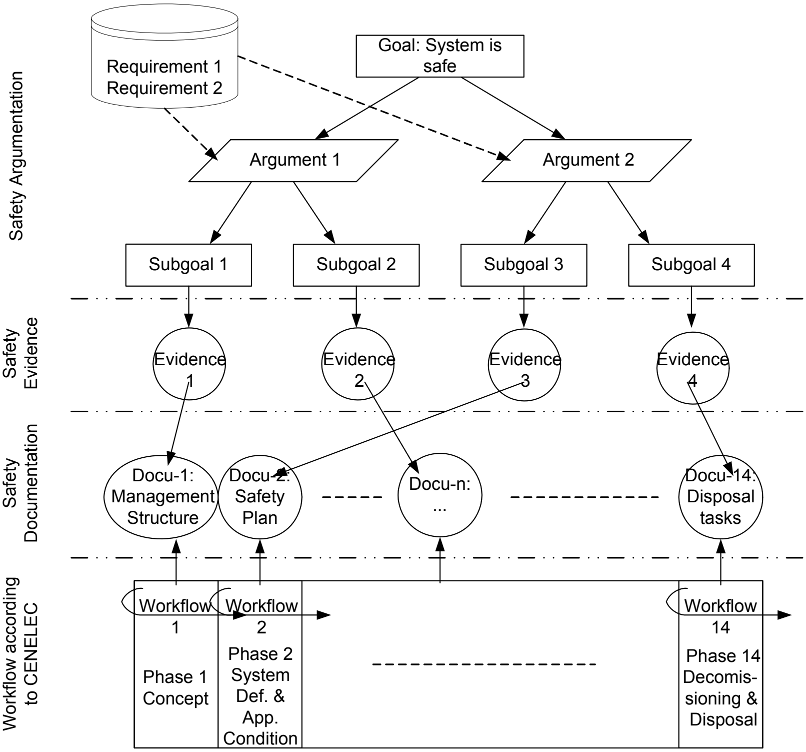

Figure 1: Safety argumentation versus safety evidence.

4 Improvement by automatisation

4.1 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

1) the normative safety case processes (EN 5012x),
2) the tasks that improve these processes,
3) and the knowledge that is the basis for the improving tasks of 2.).

The normative safety case processes have been modelled with event-driven process chains [4]. The result is 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. 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.

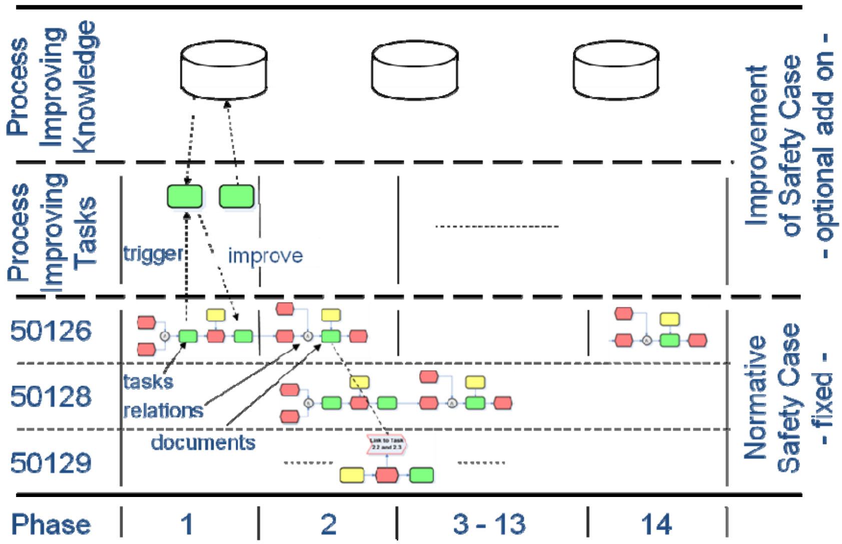

Figure 2: Structure of the improved safety case model.

The model of the improved safety case process consists of several layers, allowing the strict separation of the normative development processes and the support functionalities. The structure of the improved safety case model is depicted in Fig. 2.

The support functionalities encompass tasks related to the improving of the process knowledge as well as tasks improving the process itself.

4.2 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 (see Fig. 3):

1) 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).

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

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

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

5) 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.

4.3 A generic workflow

Assumed, 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 (see Fig.4). The uploaded document may in addition indicate the achievement of a milestone and therefore trigger – according to the normative description of the processes – a next 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 / tasks is automatically being informed (5).

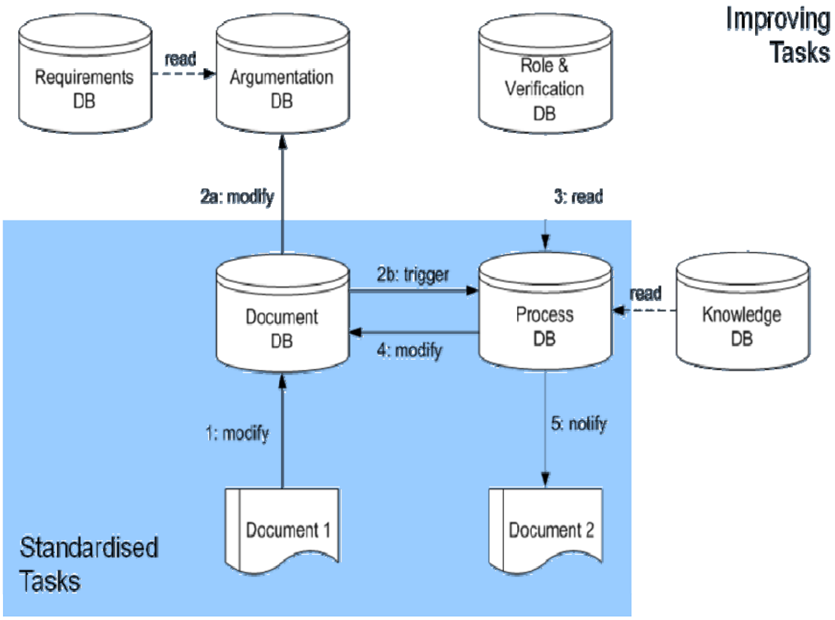

Figure 3: Using various sources of knowledge to automate the safety case processes.

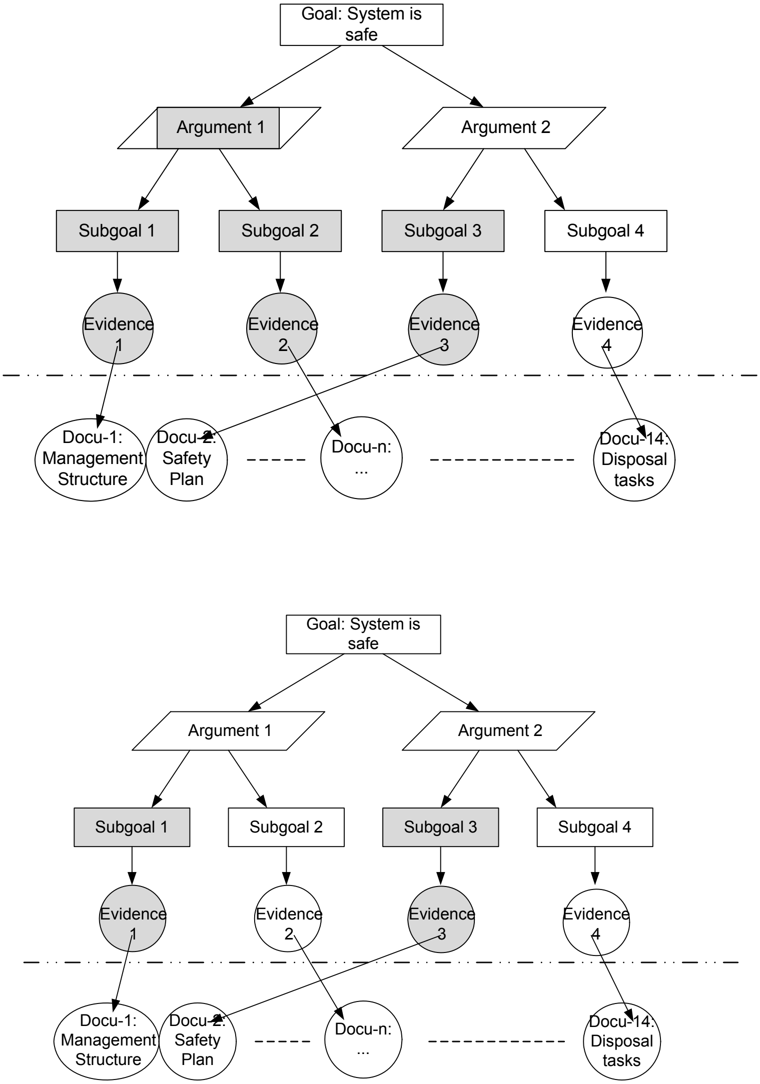

Figure 4: “High level” tracing of requirements in the argumentation tree.

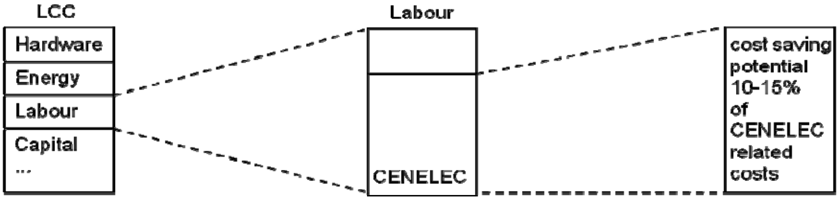

Figure 5: Estimated expected economical benefit.

5 Results: the estimated economical benefit

Within the INESS project, there is a subproject that deals with the life-cycle-costs of interlocking systems (see Fig. 5). Here, the costs to develop according to CENELEC have been subsumed to the labour costs. Fig. 5 depicts roughly the fraction of these costs in a development process. 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 with the 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 help and in this respect saves 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.

References

[1] EN 50129: Railway Applications – Communications, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling, 1999.

[2] Odd Nordland: "Safety Case Categories – Which One When?", Redmill F., Anderson T.(Eds.):"Current Issues in Safety-critical Systems", *Proc. Of the 11th Safety-critical Systems Symposium*, Springer-Verlag London Ltd: Bristol, UK, February 2003.

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

[4] Keller, G., Nüttgens, M., & Scheer, A.W., Semantische Przessmodellierung auf der Grundlage Ereignisgesteuerter Prozessketten (EPK). Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89 (in German), University of Saarland, Saarbrücken, 1992.