Supporting the Safety Management – Automated Safety Case Processes

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

The work has been funded by the 7th framework program of the EU

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit
Context of the work
Project: INESS

- 20 nation-specific rail signalling and speed control systems all of which are completely incompatible with each other.
- This leads to additional costs and increased risks of breakdowns.
- ERTMS aims to remedy this lack of unification in the signalling and speed control.
- One important method for reducing costs (of signalling renewal) is considered to be the introduction of a greater degree of standardisation.
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.

→ Standardize the core of interlocking systems.
Context of the work
Workstream: Safety Case Process

One 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.

→ Improve the performance of the Safety Case Process.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Transparency of the Safety Argumentation
• Automated Processes
• Results – estimated economical benefit
For the approval process of railway operating systems the CENELEC norms EN 50126, 50128 and 50129 are obligatory standards for European countries. The norms describe the life cycle process for safety relevant railway systems that is integrated into the development process.

Even though the norms have been published and used for about 10 years now, there seem time consuming difficulties that hinder an efficient handling of the safety case process.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Transparency of the Safety Argumentation
• Automated Processes
• Results – estimated economical benefit
A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

A safety case is “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.” [3, UK Defence Standard]
A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.” [2]

A safety case is “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.” [3, UK Defence Standard]
A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

A safety case is “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.” [3, UK Defence Standard]
Transparency of the Safety Argumentation
What is the Safety Case?

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

A safety case is “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.” [3, UK Defence Standard]
A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

A safety case is “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.” [3, UK Defence Standard]
A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.” [2]

A safety case is “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.” [3, UK Defence Standard]
Transparency of the Safety Argumentation
The relation between safety cases and court cases

The defendant convinces the lawyer of his innocence.

The advocate convinces the judge of the innocence of the defendant.

The defendant convinces the lawyer of his innocence.
Transparency of the Safety Argumentation
The relation between safety cases and court cases

The defendant convinces the lawyer of his innocence.

The advocate convinces the judge of the innocence of the defendant.

The defendant convinces the lawyer of his innocence.
Transparency of the Safety Argumentation
The relation between safety cases and court cases

Conclusion: Innocent!

legislative background

structured argument

body of evidence

fact

fact

fact

fact

fact

fact

fact
Transparency of the Safety Argumentation
The relation between safety cases and court cases

Lawyer

Judge

Defendant

fact

fact

fact

fact
Transparency of the Safety Argumentation
The relation between safety cases and court cases

**Structured argument**

- **Conclusion:** Safe!
- **Safety Manager**
  - **normative background**
  - **arg₁**
  - **arg₂**
  - **rslt₁**
  - **rslt₂**
  - **rslt₃**
  - **rslt₄**

**Body of evidence**

- **Defendant**
- **Critical System**
- **Assessor**

**Lawyer**

- **Judge**

**rslt₁**

**31.01.2011, ESREL – European Safety and Reliability Conference 2010, Rhodes, Greece**
Transparency of the Safety Argumentation
The relation between safety cases and court cases

Safety Manager
Assessor
Safety Critical System

result
result
result
Transparency of the Safety Argumentation
The “Goal Structured Notation“

Document Management System
Transparency of the Safety Argumentation
The “Goal Structured Notation“

Database of Documents

Document Management System
Transparency of the Safety Argumentation
The "Goal Structured Notation"

body of evidence

Database of Documents

Document Management System
Transparency of the Safety Argumentation

The “Goal Structured Notation“

“Goal Structure“
structured argument

body of evidence

Database of Documents

Document Management System

31.01.2011, ESREL – European Safety and Reliability Conference 2010, Rhodes, Greece
• Legal authorities get a quick overview over the structure of the safety argumentation.
• The safety case writer knows more precisely what to do and why.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Transparency of the Safety Argumentation
• Automated Processes
• Results – estimated economical benefit
Automated Processes
The “Goal Structured Notation“

“Goal Structure“
structured argument

body of evidence

Database of Documents

Document Management System
Automated Processes
Using various sources of knowledge to support safety case related workflows
Automated Processes
Using various sources of knowledge to support safety case related workflows
Automated Processes
Using various sources of knowledge to support safety case related workflows

1: modify
2a: modify
2b: trigger
3: read
4: modify
5: notify

Requirements DB | read | Argumentation DB | Role & Verification DB
Document DB | 2a: modify | Process DB | Knowledge DB

Document 1 | Document 2

Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
Automated Processes
Using various sources of knowledge to support safety case related workflows

1: modify
2a: modify
2b: trigger
3: read
4: modify
5: notify

Requirements DB → read → Argumentation DB → Role & Verification DB

Document DB → 2b: trigger → Process DB → read → Knowledge DB

Document 1 → 1: modify → Document 2

normative Tasks

improving Tasks
Automated Processes
The “Goal Structured Notation“

“Goal Structure“
structured argument

body of evidence

Database of Documents

Document Management System

Requirement 1
Requirement 2

Goal: System is safe

Argument 1

Subgoal 1
Evidence 1

Subgoal 2
Evidence 2

Subgoal 3
Evidence 3

Subgoal 4
Evidence 4

Docu-1: Management Structure
Docu-2: Safety Plan

Docu-n: ...

Workflow 1
Phase 1 Concept

Workflow 2
Phase 2 System Def. & App.

Workflow 14
Phase 14 Decommissioning & Disposal

Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
Automated Processes

Benefits

- The safety manager is continuously informed of the actual state of the safety case through continuous and automated update of the safety case status.
- “high level“ requirement tracing.
- The access to the documents is given through links.
- Consistent referencing and versioning.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Transparency of the Safety Argumentation
• Automated Processes
• Results – estimated economical benefit
Results – estimated economical benefit

What is the expected economical benefit?

The cost saving potential for the creation of the Safety Case varies between 15% and 75% (that means 10-15 % of the overall CENELEC costs).

The broadness of the margin is explained through the following influences:

- The complexity and duration of a project
- The basis of comparison: The benefit of a company following even today exactly the CENELEC processes and using sophisticated SW-tools will be lower than that of the most interviewed partners.
