The Formal Representation of the Safety Case Processes described in the EN 5012x norms

Jörg R. Müller, Technical University of Braunschweig
Jörn Drewes, TÜV Süd Rail GmbH
Jörg May, IGT Bahn mbH and
Carsten Trog, Funkwerk IT

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

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Presentation of the modelling method
- References between the 50126 and 50129
- Conclusion – What’s the use of it all?
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.
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.
One basis to achieve this goal was the development of a generic and formal model of the safety-case related processes according to the RAMS norms EN 5012x of CENELEC.

This contribution presents the method guiding the transformation from the natural language documents specifying the normative safety case processes to a representation by the formal description language.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Presentation of the modelling method
• References between the 50126 and 50129
• Conclusion – What’s the use of it all?
For the approval process of interlocking 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 is still a wide rage of interpretations possible and many instances of these have arisen causing difficulties in the efficient handling of the safety case process.
The EN 50126 defines the terms of RAMS, their interaction and a process based on the system lifecycle for managing RAMS.

In addition, a systematic process for specifying requirements for RAMS and demonstrating that these requirements are achieved is defined.
EN 50128

The EN 50128 specifies procedures and technical requirements for the development of programmable electronic systems for usage in railway control and protection applications, aimed at usage in any area where there are safety implications.

In contrast to the EN 50126, it is applicable exclusively to software and the interaction between software and the system which it is part of.
The EN 50129 specifies those lifecycle activities which shall be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage.

It is therefore concerned with the evidence to be presented for the acceptance of safety-related systems and is highly related to the EN 50126.
In order to have a common understanding of the textual described content inside the norms, a normative safety case model will be developed. For this purpose the use of more or less formal description languages will be used with the purpose of expressing the normative requirements user-friendly.

The Generic Safety Case Model is one basis for formulating a questionnaire used for discussions with the suppliers and railway operators.
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Presentation of the modelling method
• References between the 50126 and 50129
• Conclusion – What’s the use of it all?
Presentation of the modelling method
Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
Presentation of the modelling method
The tasks and their types

<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Phase related general tasks</th>
<th>Phase related RAM tasks</th>
<th>Phase related Safety tasks</th>
</tr>
</thead>
</table>
| 1. Concept      | • Establish Scope and Purpese ...  
• Define Railway Project Concept  
• ... | • Review Previously Achieved RAM Performance  
• Consider RAM Implications  
• ... | • Review Previously Achieved Safety Performance  
• Consider Safety Implications  
• ... |
| 2. System Definition ... | • ...  
• ... | • ...  
• ... | • ... |
| 3. Risk Analysis | • Undertake Project related Risk analysis  
• ... | • ... | • Perform System Hazard & Safety Risk Analysis  
• Set-up Hazard Log  
• Perform Risk Assessment  
• ... |

In figure 9 of the EN 50126, for each phase of the lifecycle, the main tasks are summarized. Beside RAMS-tasks, general tasks as representatives of common Industry practice have been specified.

<table>
<thead>
<tr>
<th>General-tasks</th>
<th>RAM-tasks</th>
<th>Safety-tasks</th>
</tr>
</thead>
</table>

Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
Presentation of the modelling method
The tasks and their types

S.3.1
perform system hazard & safety risk analysis

safety-related to be performed In the 3. phase (risk-analysis)

first safety-task mentioned in the risk-analysis-phase in table 9 of 50126
Presentation of the modelling method
The tasks and their types

G.3.1
undertake project related risk analysis

G.3.1
general task
to be performed in the 3. phase (risk-analysis)
first general-task mentioned in the risk-analysis-phase in table 9 of 50126
Presentation of the modelling method
Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
Presentation of the modelling method

The Result of the tasks

S.3.1 Perform system hazard & safety risk analysis
S.3.1 Undertake project related risk analysis

System hazards and risk identified and analysed
Project related risk analysis completed

S.3.3 Perform risk assessment
Risk assessment performed

S.3.2 Set-up Hazard Log
Hazard Log set-up
Presentation of the modelling method
Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
Presentation of the modelling method

Dependencies of tasks

- **S.3.1** Perform system hazard & safety risk analysis
- **System hazards and risk identified and analysed**
- **S.3.3** Perform risk assessment
- **Risk assessment performed**
- **S.3.2** Set-up Hazard Log
- **Hazard Log set-up**

- **G.3.1** Undertake project related risk analysis
- **Project related risk analysis completed**
Presentation of the modelling method
Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
Presentation of the modelling method
Requirements of tasks

6.3.3 Requirements

6.3.3.1 Requirement 1 of this phase shall be to:

a) Systematically identify and prioritize all reasonably foreseeable hazards associated with the system in its application environment, including hazards arising from:
   — system normal operation;

6.3.3.2 Requirement 2 of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and lifecycle cost requirements of the system.

6.3.3.3 Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:
Presentation of the modelling method
Requirements of tasks

6.3.3.2
Requirement of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and lifecycle cost requirements of the system.

6.3.3.3
Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:
- the aim and purpose of the Hazard Log;
- each hazardous event and contributing components;
...

6.3.1
Perform system hazard & safety risk analysis

S.3.1
Perform system hazard & safety risk analysis

G.3.1
Undertake project related risk analysis

Project related risk analysis completed

S.3.3
Perform risk assessment

Risk assessment performed

S.3.2
Set-up Hazard Log

Hazard Log set-up

6.3.1.1
Requirement 1 of this phase shall be to:
- Systematically identify and prioritize all reasonably foreseeable hazards associated with the system installation environment, including hazard arising from:
  - system normal operation;
  - system fault conditions;
  ...
- identify the sequence of events leading to hazards;
- evaluate the frequency of occurrence of each hazard (Table 2);
  ...

^
Presentation of the modelling method

Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
6.3.4 Deliverables

6.3.4.1 The results of this phase shall be documented, along with any assumptions and justifications made during the phase.

6.3.4.2 The results of the risk analysis shall be recorded within the Hazard Log.

6.3.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.
Presentation of the modelling method

Documentation

6.3.3.2
Requirement of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and lifecycle cost requirements of the system.

6.3.3.3
Requirement 3 of this phase shall be to establish a Hazard Log as the basis for ongoing risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:

a) the aim and purpose of the Hazard Log;
b) each hazardous event and contributing components;
...

S.3.1
Perform system hazard & safety risk analysis

System hazards and risk identified and analysed

S.3.3
Perform risk assessment

Risk assessment performed

S.3.2
Set-up Hazard Log

Hazard Log set-up

6.3.3.1
Requirement 1 of this phase shall be to:

a) Systematically identify and prioritize all reasonably foreseeable hazards associated with the system in its application environment, including hazard arising from:
- system normal operation;
- system fault conditions;
...

b) identify the sequence of events leading to hazards;
c) evaluate the frequency of occurrence of each hazard (Table 2);
...

G.3.1
Undertake project related risk analysis

Project related risk analysis completed

6.3.4.2
The results of the risk analysis shall be recorded within the Hazard Log

Documentation of Phase 3

Documentation (PHASE 3) completed

Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
Presentation of the modelling method
Things to take into account

What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What is required to perform these tasks?

What are the (documented) deliverables?

What are the verification tasks to be done?
6.3.5 Verification

6.3.5.1 The following verification tasks shall be undertaken within this phase:

a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase;
b) the phase 3 deliverables shall be verified against the phase 2 deliverables;
c) assessment of the completeness of the risk assessment;
d) assessment of the risk acceptability classification;
e) assessment of the suitability of the hazard log process for the system under consideration;
f) assessment of the adequacy of the methods, tools and techniques used within the phase;
g) assessment of the competence of all personnel undertaking tasks within the phase.

6.3.5.1 Any errors or shortfall may require the re-application of some or all of the activities of one or more previous lifecycle phases.
Presentation of the modelling method
The Verification of tasks

6.3.3.2 Requirement of this phase shall be to determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and lifecycle cost requirements of the system.

6.3.3.3 Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:
   a) the aim and purpose of the Hazard Log;
   b) each hazardous event and contributing components;
   ...

6.3.5.1 The following verification tasks shall be undertaken within this phase:
   a) assessment of the adequacy of the information, and where...

6.3.4.2 The results of the risk analysis shall be recorded within the Hazard Log.

Documentation

Meet all requirements of verification for Phase 3

Documentation of Phase 3
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Presentation of the modelling method
• References between the 50126 and 50129
• Conclusion – What’s the use of it all?
The structure of the safety case is Defined in chapter 5 of the EN 50129.

E.g. section 5.4 of EN 50129 deals with the Technical Safety Report.
The Technical Safety Report

The structure of the safety case is Defined in **chapter 5** of the EN 50129.

E.g. **section 5.4** of EN 50129 deals with the Technical Safety Report.
Correspondingly, e.g. the system related application conditions are defined in \textbf{subsection 5.4.5} of EN 50129.
References between EN 50126 and EN 50129

The Phases of the EN 50126

| EN 50126 | EPC-Model of Phase 1 | EPC-Model of Phase 9 (System Validation) | EPC-Model of Phase 14 |
References between EN 50126 and EN 50129

The Phases of the EN 50126

EN 50126

EPC-Model of Phase 1

EPC-Model of Phase 9
(System Validation)

EPC-Model of Phase 14

EN 50129

Safety Case

Part 1
Part 2
Part 3
Part 4
Part 5
Part 6

Technical Safety Report

EPC-Model with references for every section of the Technical Safety Report
### References between EN 50126 and EN 50129

References in Section "Safety-related application condition"

<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Phase related general tasks</th>
<th>Phase related RAM tasks</th>
<th>Phase related Safety tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Installation</td>
<td>• …</td>
<td>• …</td>
<td>• …</td>
</tr>
<tr>
<td>9. System validation</td>
<td>• …</td>
<td>• …</td>
<td>• …</td>
</tr>
<tr>
<td>10. System Acceptance</td>
<td>• …</td>
<td>• …</td>
<td>• …</td>
</tr>
</tbody>
</table>

### B.5 Safety-related application conditions

(Section 5 of the Technical Safety Report)

This section shall define the rules, conditions and constraints relevant to functional safety which need to be observed in the application of the system/sub-system/equipment.

General topics which shall be considered include the following:

**Table E.10 – Application, operation and maintenance**

(referred to in 5.3.12 and 5.4)

<table>
<thead>
<tr>
<th>Techniques/Measures</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Production of</td>
<td>R: all operational, application and</td>
<td>HR: all operational, application and</td>
<td></td>
</tr>
</tbody>
</table>
Operational and safety relevant requirements must be met even during operation with external influences.

5.4.4 Operation with external influences

Reference to EN 50126: S 4.1, S 5.1

Operation with external influences performed

Reference to EN 50126: S 9.3

5.4.5 Safety-related application conditions

Evidence to demonstrate successful completion, under operational conditions, of the Safety Qualification Tests.

Safety-related application condition proven

5.4.6 Safety Qualification Tests

References in section 4 of the Technical Safety Report

References in section 5 of the Technical Safety Report

References in section 6 of the Technical Safety Report

B.4 with detailed requirements

B.5 with detailed requirements, guidance in Table E.10

B.6 with detailed requirements
• Context of the presented work
• Introduction to the 5012x-CENELEC Standards
• Presentation of the modelling method
• References between the 50126 and 50129
• Conclusion – What’s the use of it all?
Conclusion
What is the use of it all?

The developed model was the basis to create a questionnaire with very accurate questions.

The model supports the navigation through the norms – especially for newcommers to the RAMS-norms of CENELEC.

The model is used as one basis to specify workflows in for supporting safety-case software tools.