

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

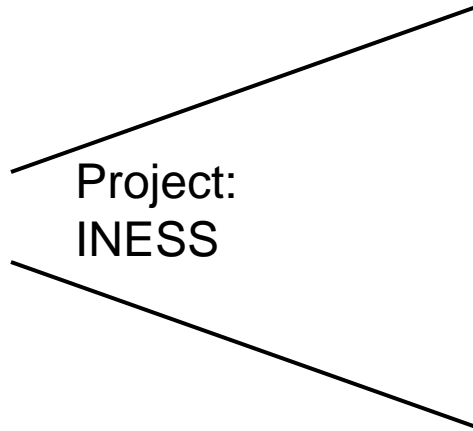


The work has been funded by the 7th framework program of the EU

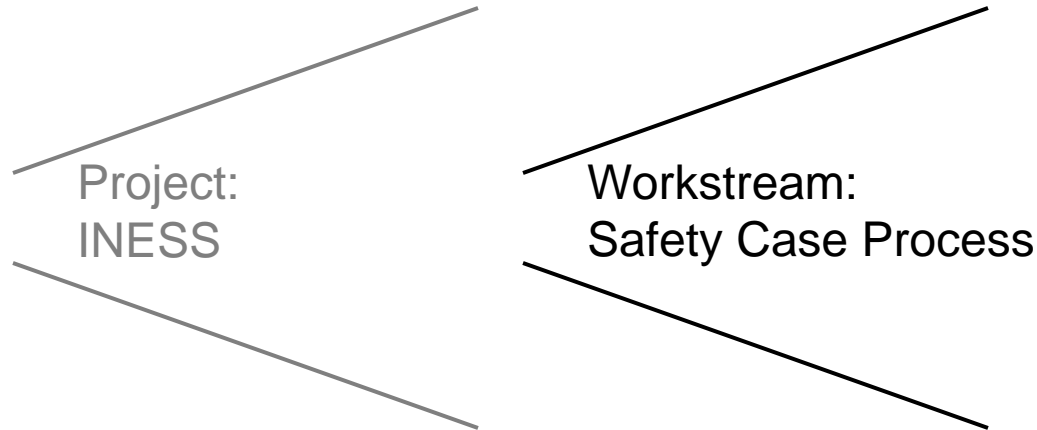


- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Presentation of the modelling method
- Relations between the 50126 and 50129
- Conclusion – What's the use of it all?

- The railways in Europe have been developed independently.
- Operating procedures and signaling systems differ.
- Accordingly, different interlocking systems have been developed.
- This led to a strong dependence of suppliers and operators.
- As the basic functionality of interlockings is quite the same, a “common core” of interlockings should be specifiable.
- Specific national characteristics are to be realized based on this core.



The European project called „INESS – **I**ntegrated **E**uropean **S**ignalling **S**ystem“ 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?

Introduction to the 5012x-CENELEC-Standards

Overview

EUROPEAN STANDARD	EN 50126	
NORME EUROPEENNE		
EUROPÄISCHE NORM	EN 50128	
ICS 29.280; 45.000		
	EUROPEAN STANDARD	EN 50129
	NORME EUROPÉENNE	
	EUROPÄISCHE NORM	February 2003
	ICS 93.100	Supersedes ENV 50126:1998
	English version	
	Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling	
	Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik
	This European Standard was approved by CENELEC on 2002-12-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.	
	Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.	
	This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.	
	CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.	
	CENELEC European Committee for Electrotechnical Standardization Comité Européen de Normalisation Electrotechnique Europäisches Komitee für Elektrotechnische Normung Central Secretariat: rue de Stassart 35, B - 1050 Brussels	
	© 2003 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.	
	Ref. No. EN 50129:2003 E	

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 seem time consuming difficulties that hinder an efficient handling of the safety case process.

EUROPEAN STANDARD

EN 50126

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 1999

ICS 29.280; 45.020

English version

**Railway applications - The specification and demonstration of
Reliability, Availability, Maintainability and Safety (RAMS)**

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.

EUROPEAN STANDARD	EN 50126
NC EUROPEAN STANDARD	EN 50128
EU NORME EUROPÉENNE	
ICS1 EUROPÄISCHE NORM	March 2001

ICS 29.280; 45.060.10

English version

**Railway applications -
Communications, signalling and processing systems -
Software for railway control and protection systems**

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.

EUROPEAN STANDARD	EN 50126		
NO	EUROPEAN STANDARD	EN 50128	
EU	NORM	EUROPEAN STANDARD	EN 50129
ICS 2	<u>EURO</u>	NORME EUROPÉENNE	
	CS 29.280;	EUROPÄISCHE NORM	February 2003
ICS 93.100		Supersedes ENV 50129:1998	
English version			
Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling			

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.

Introduction to the 5012x-CENELEC-Standards

The Aim

EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM	EN 50126
ICS 29.260, 45.020	
EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM	EN 50128
ICS 29.260, 45.060.10	March 2001
Railway appli Reliability,	
Applications ferroviaires démontrent la disponibilité de la main d'œuvre (FOMS)	
Communicati Software for	EN 50129
ICS 49.100	February 2003
Supersedes EN 50128:1995	
English version	
Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling	
Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation	Bahnwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitselektronische Systeme für Signaltechnik
This European Standard is identical with the CEN document EN 50128:1995 Up-to-date text and application to the CEN	
This European Standard language made by 1 member to the CEN	
CENELEC members France, Germany, Italy, Spain, Sweden, UK	
This European Standard is identical with the CEN document EN 50128:1995 Up-to-date text and application to the CEN	
This European Standard is identical with the CEN document EN 50128:1995 Up-to-date text and application to the CEN	
CENELEC members are Republic, Denmark, First Netherlands, Norway, Portugal	
This European Standard was approved by CENELEC on 2002-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.	
Up-to-date text and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.	
This European Standard exists in three official versions (English, French, German). A version in any other language made for translation under the responsibility of a CENELEC member into its own language and reflected in the Central Secretariat has the same status as the official version.	
CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.	
Europe CEN CEN CEN	
Central	
© 2001 CENELEC – All rights of exploitation	
CENELEC European Committee for Electrotechnical Standardization Comité Européen de Normalisation Electrotechnique Europäisches Komitee für Elektrotechnische Normung Central Secretariat: rue de Sluisbaat 35, B-1050 Brussels	
© 2003 CENELEC – All rights of exploitation in any form and by any means reserved worldwide for CENELEC members. Ref. No. EN 50128:2003 E	

transform



Formal Model

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**
 - Relations between the 50126 and 50129
 - Conclusion – What's the use of it all?

-
- Context of the presented work
 - Introduction to the 5012x-CENELEC Standards
 - **Presentation of the modelling method**
 - Example: Phase 3 “Risk Analysis” of EN 50126
 - Relations between the 50126 and 50129
 - Conclusion – What’s the use of it all?

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 are the requirements of a phase?

What are the (documented) deliverables?

What are the verification tasks to be done?



Presentation of the modelling method

The tasks and their types

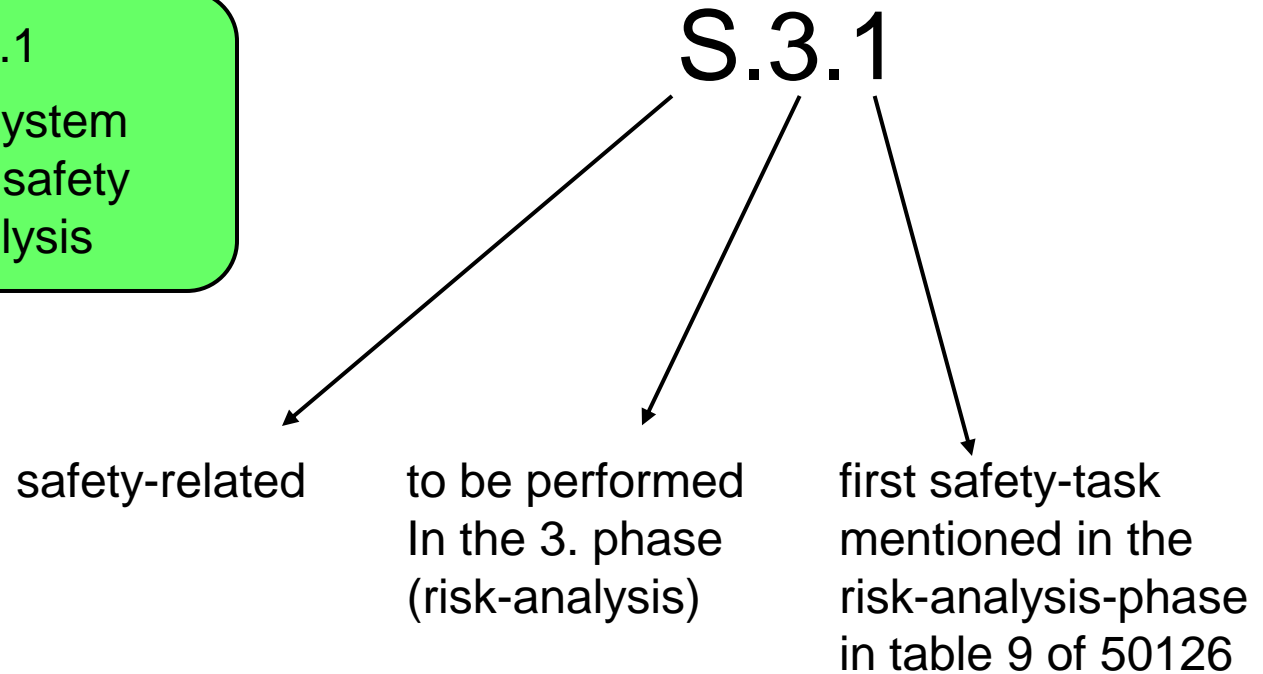
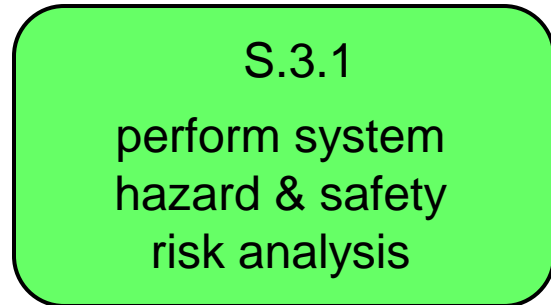
Lifecycle Phase	Phase related general tasks	Phase related RAM tasks	Phase related Safety tasks
1. Concept	<ul style="list-style-type: none">• Establish Scope and Purose ...• Define Railway Project Concept• ...	<ul style="list-style-type: none">• Review Previously Achieved RAM Performance• Consider RAM Implications	<ul style="list-style-type: none">• Review Previously Achieved Safety Performance• Consider Safety Implications• ...
2. System Definition ...	<ul style="list-style-type: none">• ...	<ul style="list-style-type: none">• ...	<ul style="list-style-type: none">• ...
3. Risk Analysis	<ul style="list-style-type: none">• Undertake Project related Risk analysis	-	<ul style="list-style-type: none">• Perform System Hazard & Safety Risk Analysis• Set-up Hazard Log• Perform Risk Assessment
...

In figure 9 of the 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.

General-tasks

RAM-tasks

Safety-tasks



Presentation of the modelling method

The tasks and their types

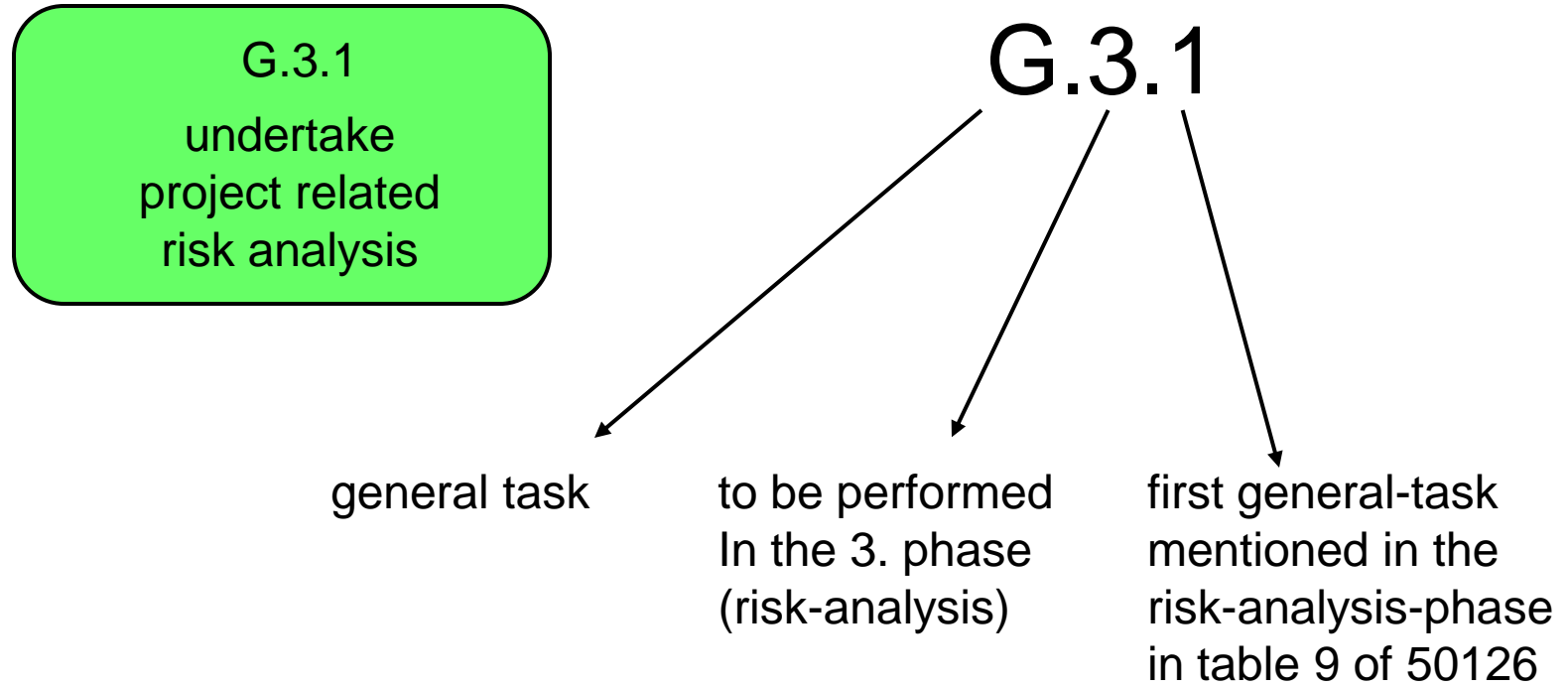
Lifecycle Phase	Phase related general tasks	Phase related RAM tasks	Phase related Safety tasks
1. Concept	<ul style="list-style-type: none">• Establish Scope and Purose ...• Define Railway Project Concept• ...	<ul style="list-style-type: none">• Review Previously Achieved RAM Performance• Consider RAM Implications	<ul style="list-style-type: none">• Review Previously Achieved Safety Performance• Consider Safety Implications• ...
2. System Definition ...	<ul style="list-style-type: none">• ...	<ul style="list-style-type: none">• ...	<ul style="list-style-type: none">• ...
3. Risk Analysis	<ul style="list-style-type: none">• Undertake Project related Risk analysis	-	<ul style="list-style-type: none">• Perform System Hazard & Safety Risk Analysis• Set-up Hazard Log• Perform Risk Assessment
...

In figure 9 of the 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.

General-tasks

RAM-tasks

Safety-tasks



What tasks are to be done at all?

What is the type of these tasks?

What is the result of these tasks?

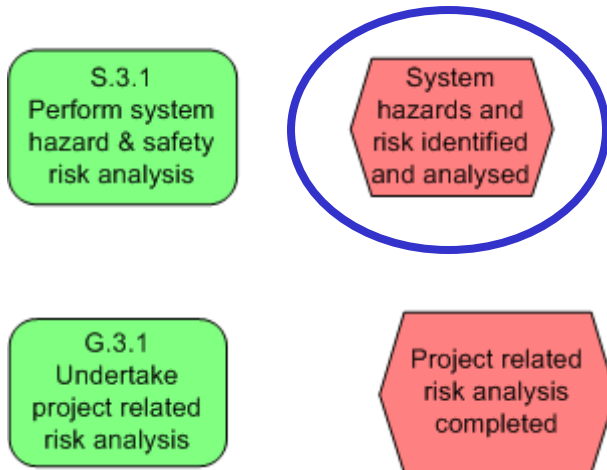
Which of the tasks can be done in parallel and which of them have to be performed in sequence?

What are the requirements of a phase?

What are the (documented) deliverables?

What are the verification tasks to be done?





After having performed the system hazard and safety analysis,
The system's hazards and risks are identified.

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 are the requirements of a phase?

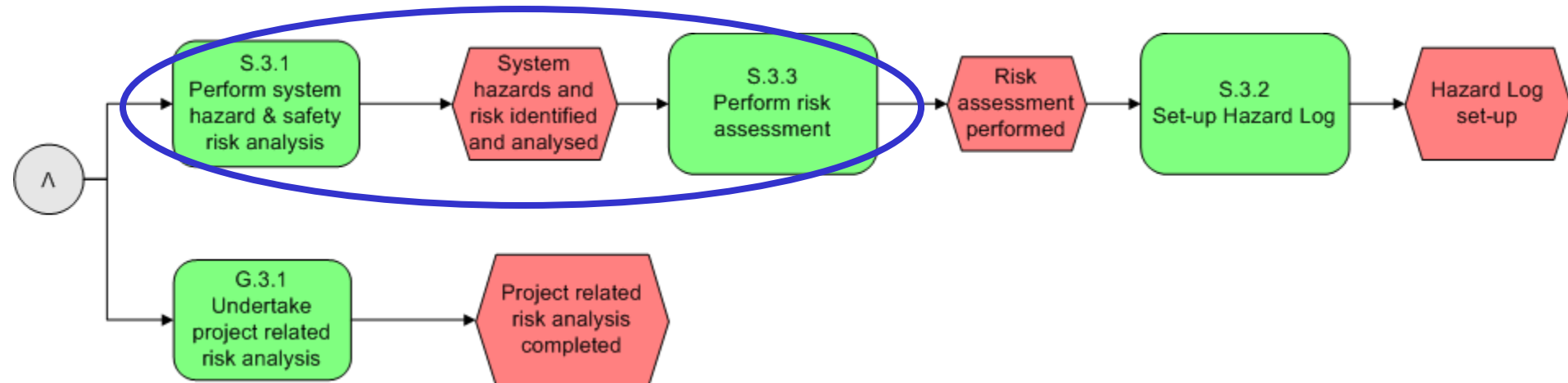
What are the (documented) deliverables?

What are the verification tasks to be done?





The hazard and safety risk analysis can be performed (more or less) independently from the project related risk analysis.



The risk assessment can only be performed after the hazard and safety risk analysis.

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 are the requirements of a phase?

What are the (documented) deliverables?

What are the verification tasks to be done?



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.

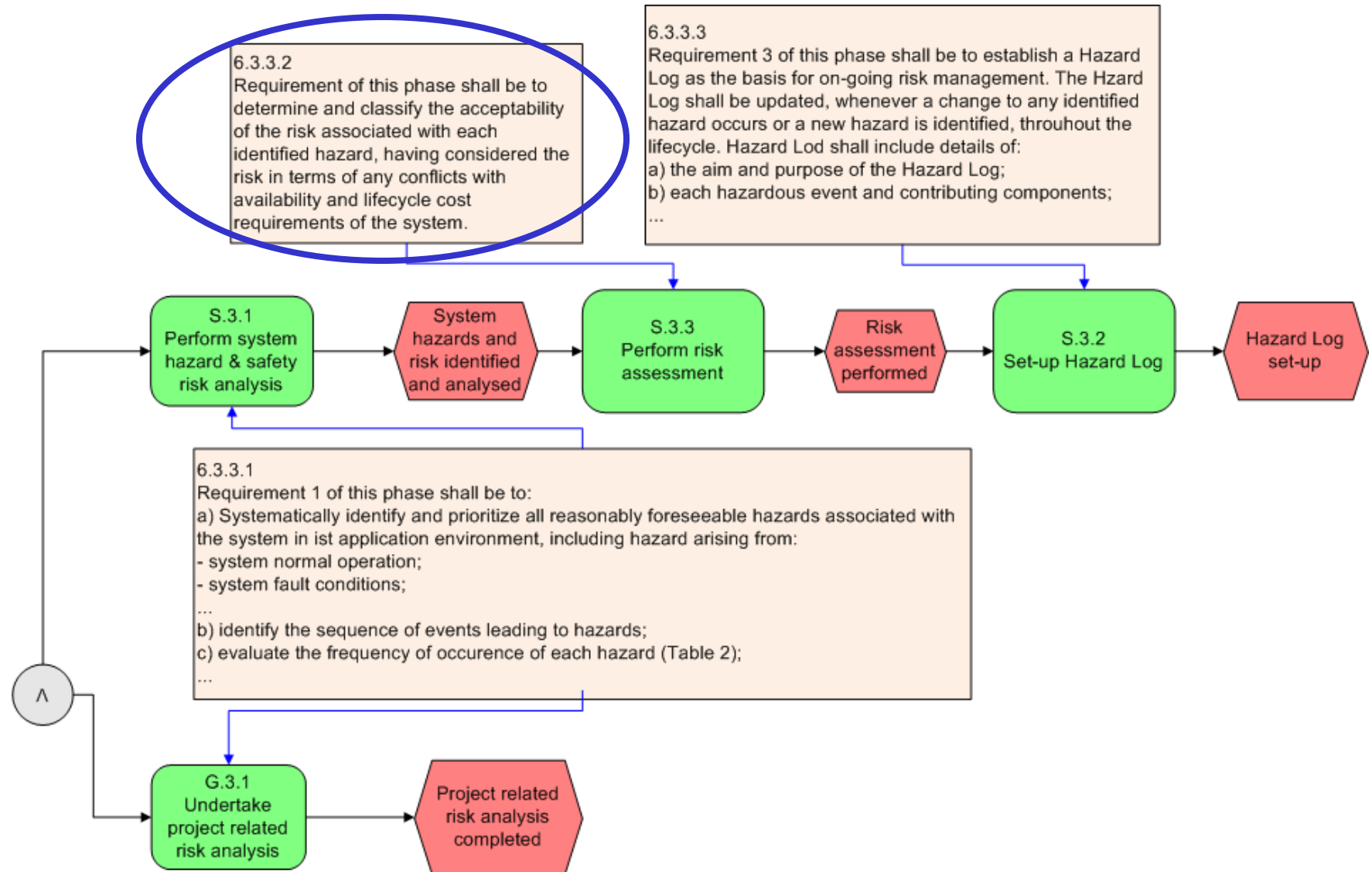
6.3.3.3 Requirement 3 of this phase shall be to establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of:

The EN 50126 lists to every phase a set of requirements.

These requirements have to be linked to the corresponding tasks.

Presentation of the modelling method

Requirements of tasks



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 are the requirements of a phase?

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.

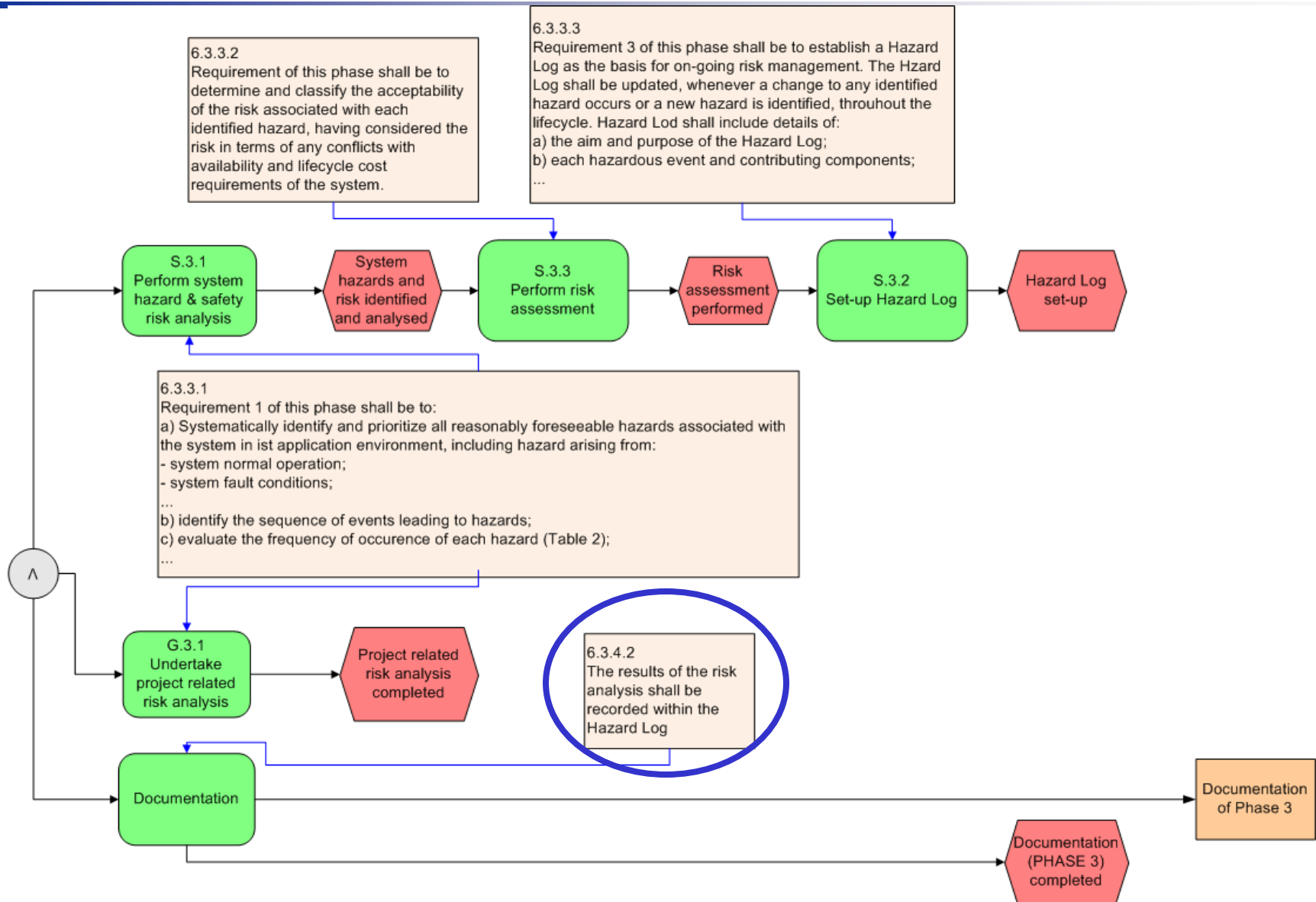
6.3.4.3 The deliverables from this phase form a key input to subsequent lifecycle phases.

The EN 50126 lists to every phase a set of deliverables. Some of these are quite general, others are phase specific.

In the formal model, we concentrated on the phase specific tasks.

Presentation of the modelling method

Documentation



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 are the requirements of a phase?

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.

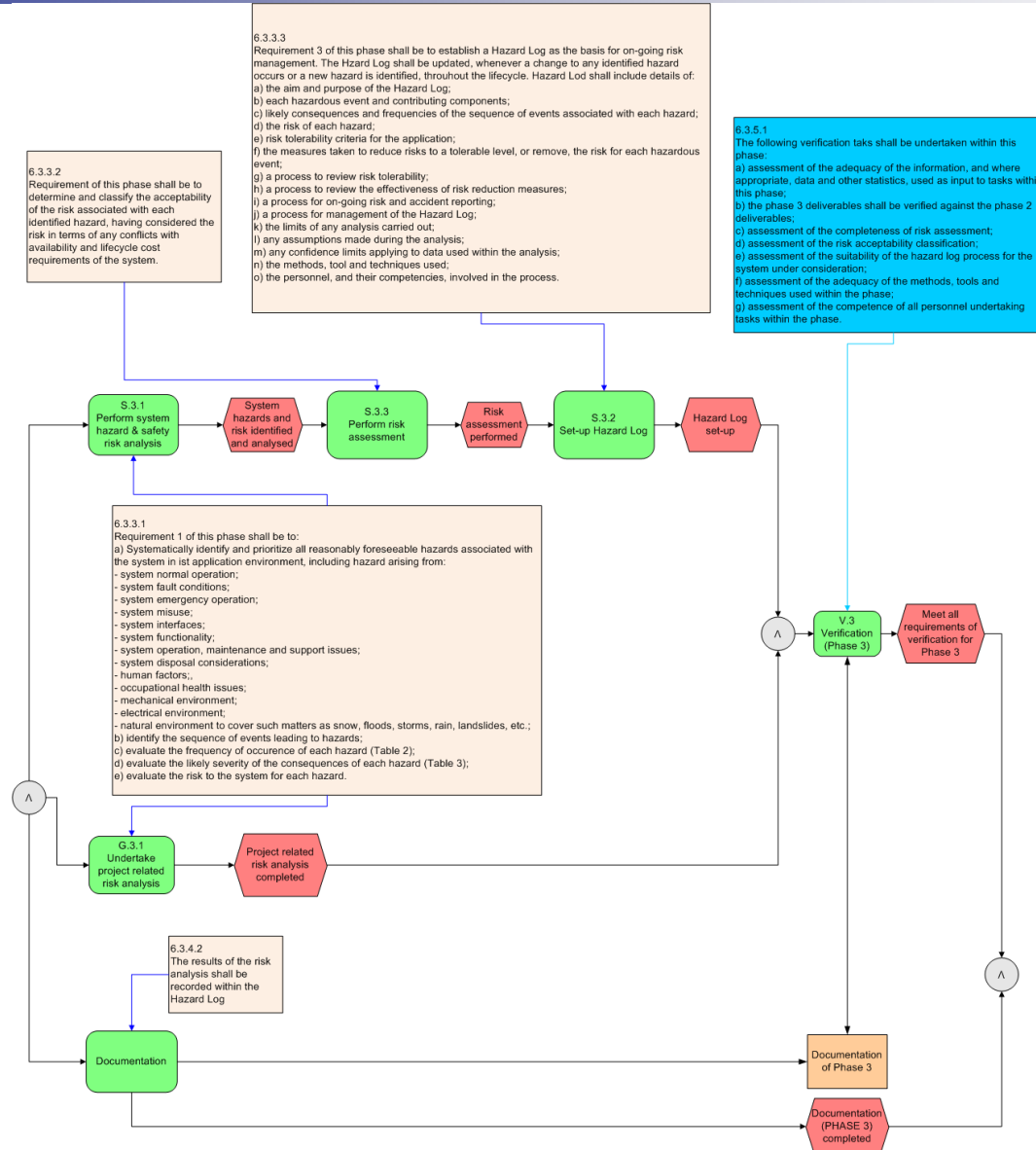
The EN 50126 lists to every phase a set of verification activities. These have been included into the model.

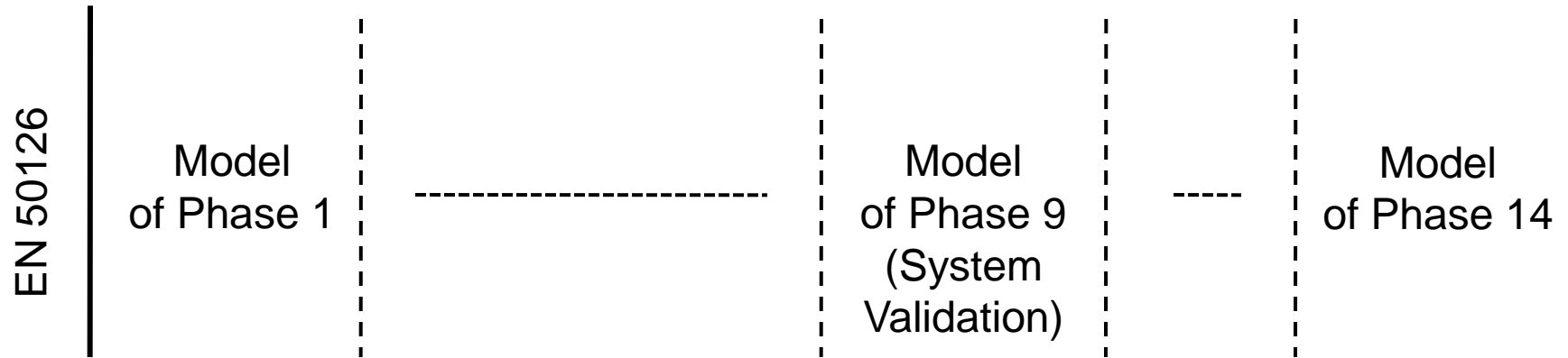
The verification of tasks



Presentation of the modelling method

The model for phase 3 "Risk analysis"

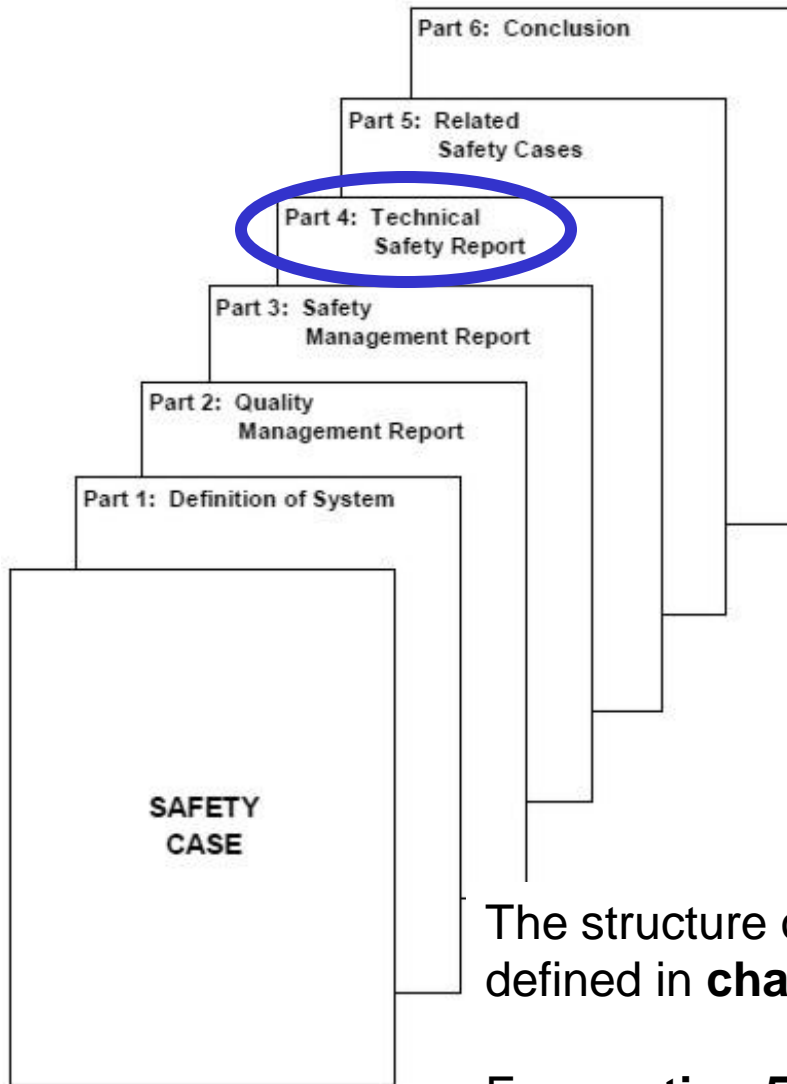




The EN 50126 describes the phases of the lifecycle-process and the corresponding activities.

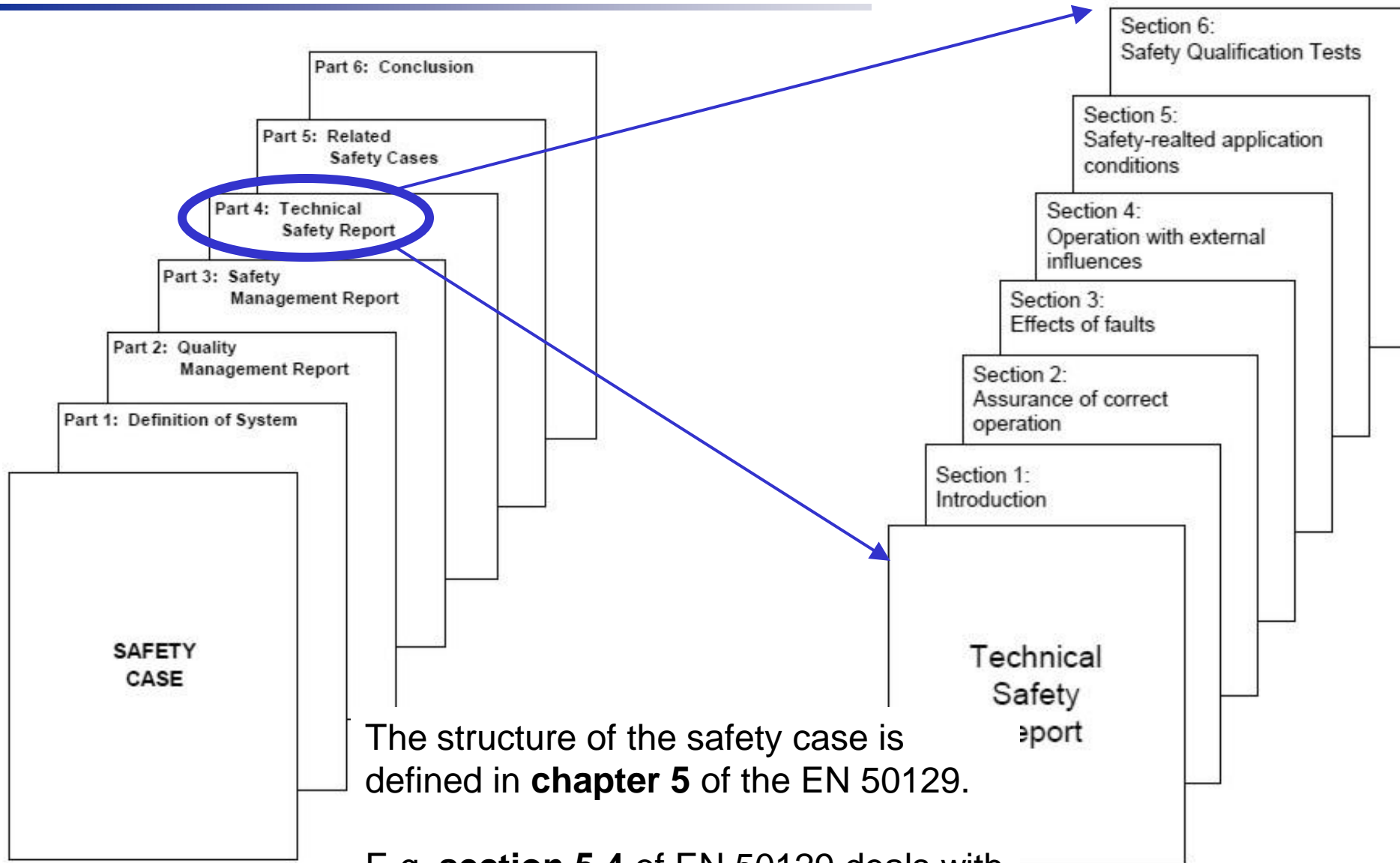
The EN 50129 describes the conditions that shall be satisfied and the structure of the corresponding documents.

-
- Context of the presented work
 - Introduction to the 5012x-CENELEC Standards
 - Presentation of the modelling method
 - **Relations between the 50126 and 50129**
 - Conclusion – What's the use of it all?



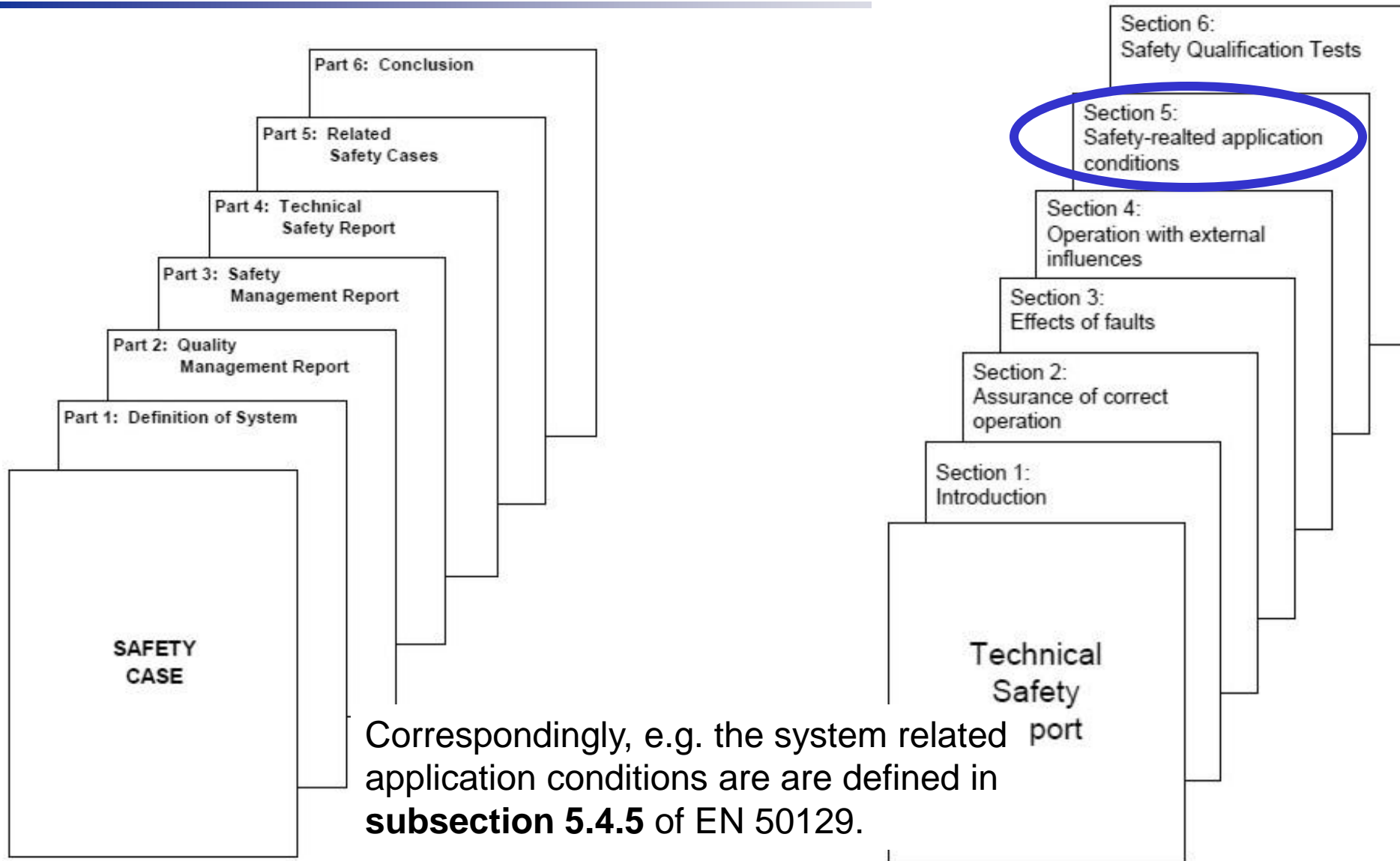
The structure of the safety case is defined in **chapter 5** of the EN 50129.

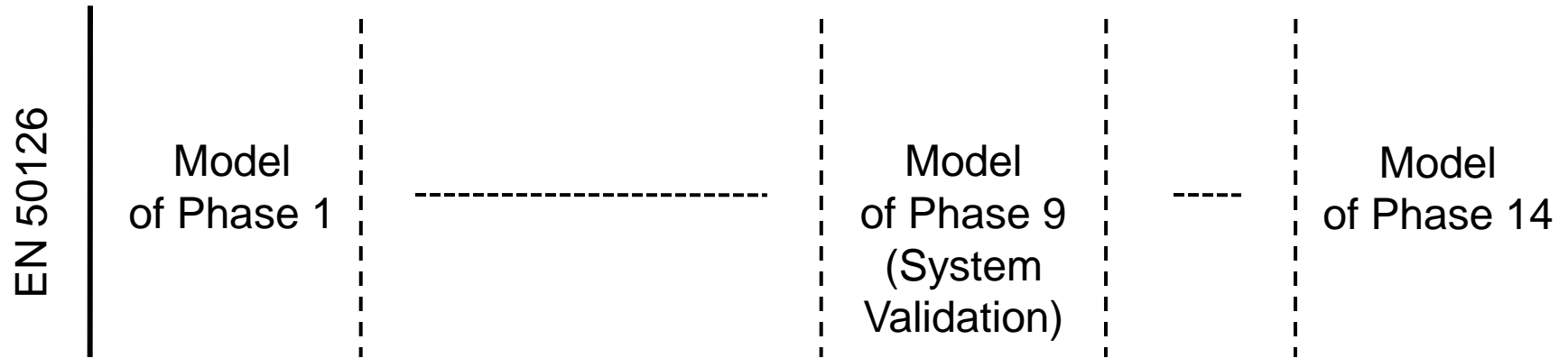
E.g. **section 5.4** of EN 50129 deals with the Technical Safety Report.



The 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.



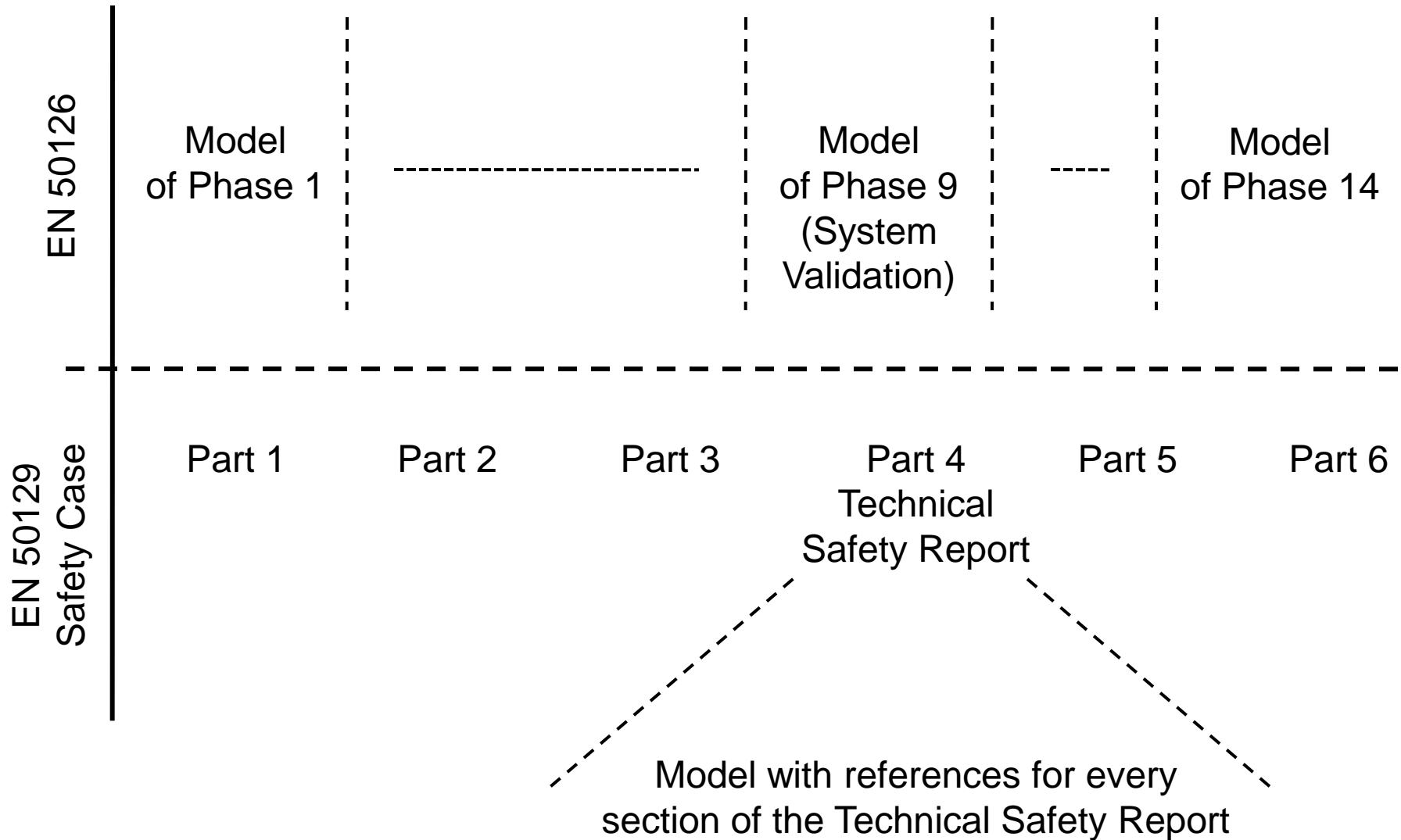


The EN 50126 describes the phases of the lifecycle-process and the corresponding activities.

The EN 50129 describes the conditions that shall be satisfied and the structure of the corresponding documents.

References between EN 50126 and EN 50129

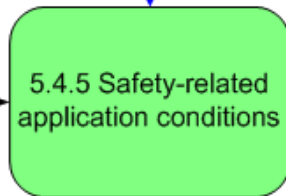
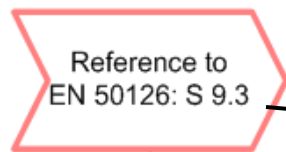
The Phases of the EN 50126 and the Chapters of the EN 129



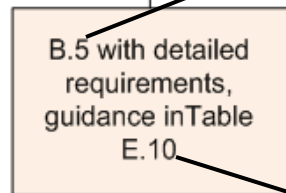
References between EN 50126 and EN 50129

References in Section "Safety-related application condition"

EN 50126



EN 50129



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:

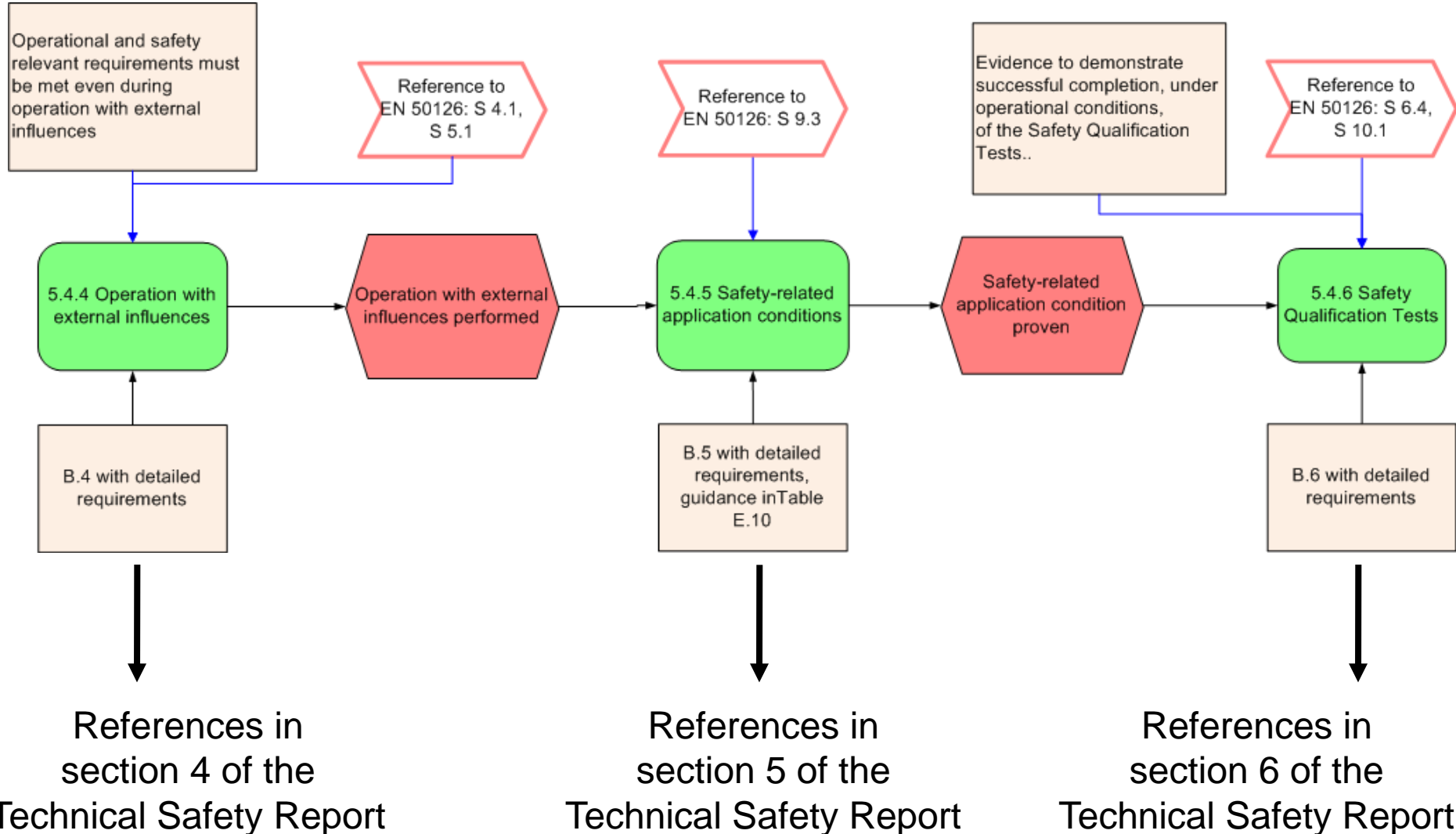
Table E.10 – Application, operation and maintenance (referred to in 5.3.12 and 5.4)

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Production of	R: all operational, application and		HR: all operational, application and	

Lifecycle Phase	Phase related general tasks	Phase related RAM tasks	Phase related Safety tasks
8. Installation	• ...	• ...	• ...
9. System validation	• ...	• ...	<ul style="list-style-type: none"> • ... • Prepare Application Specific Safety Case • ...
10. System Acceptance	• ...	• ...	• ...
...

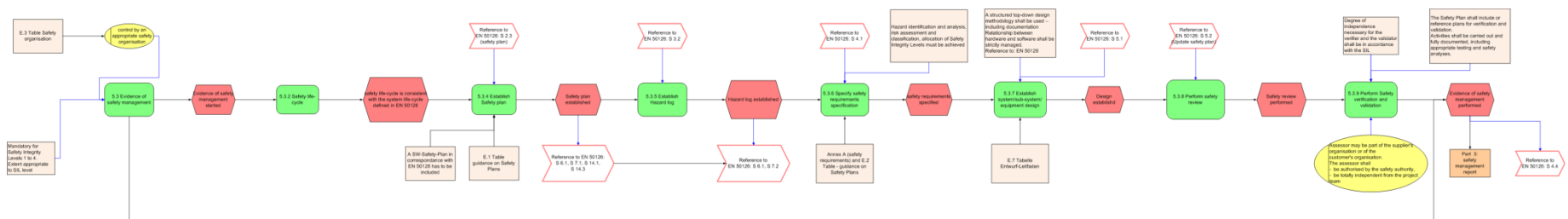
References between EN 50126 and EN 50129

Cutaway of the Model for the Technical Safety Report



References between EN 50126 and EN 50129

Cutaway of the Model for the Technical Safety Report



The model consists of about

- 200 activities
- 80 parallelizations and synchronizations
- 800 arcs

-
- Context of the presented work
 - Introduction to the 5012x-CENELEC Standards
 - Presentation of the modelling method
 - Relations between the 50126 and 50129
 - Conclusion – What's 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 newcomers to the RAMS-norms of CENELEC.

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