

GE Rail Global Signalling

Requirements Engineering

A CENELEC approach

Carlo Becheri
GETS Verification & Validation



imagination at work



Index

- ❑ Railways RAMS - Verification & Validation
- ❑ Risks Analysis in the RFI view
- ❑ Requirements Flowdown
- ❑ From Risk Analysis to Requirements
- ❑ Requirements Specification
- ❑ Requirements Modelling and Simulation w/ FM
- ❑ Conclusions



Railways RAMS Verification & Validation



imagination at work

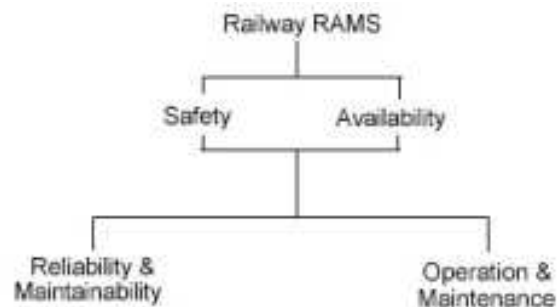
Railways RAMS

RAMS: stands for Reliability, Availability, Maintainability and Safety

Failure: a deviation from the specified performance of a system. A failure is the consequence of a fault or error in a system.

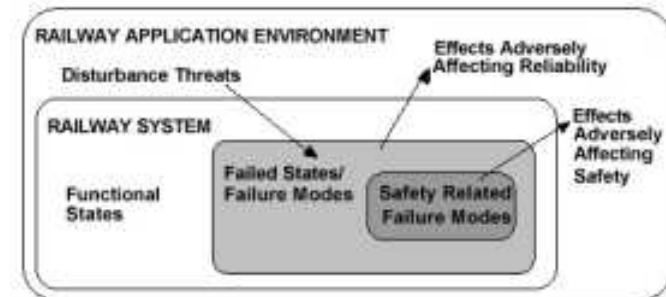
Error: a deviation from the intended design which could result in unintended system behaviour or failure.

Fault: an abnormal condition that could lead to an error or a failure in a system. A fault can be random or systematic.

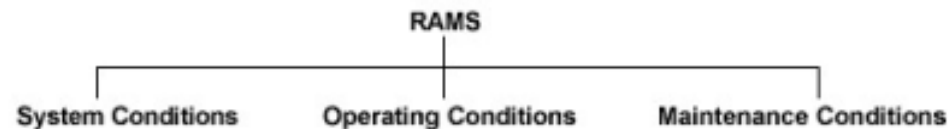


← Interrelation of Railways RAMS elements

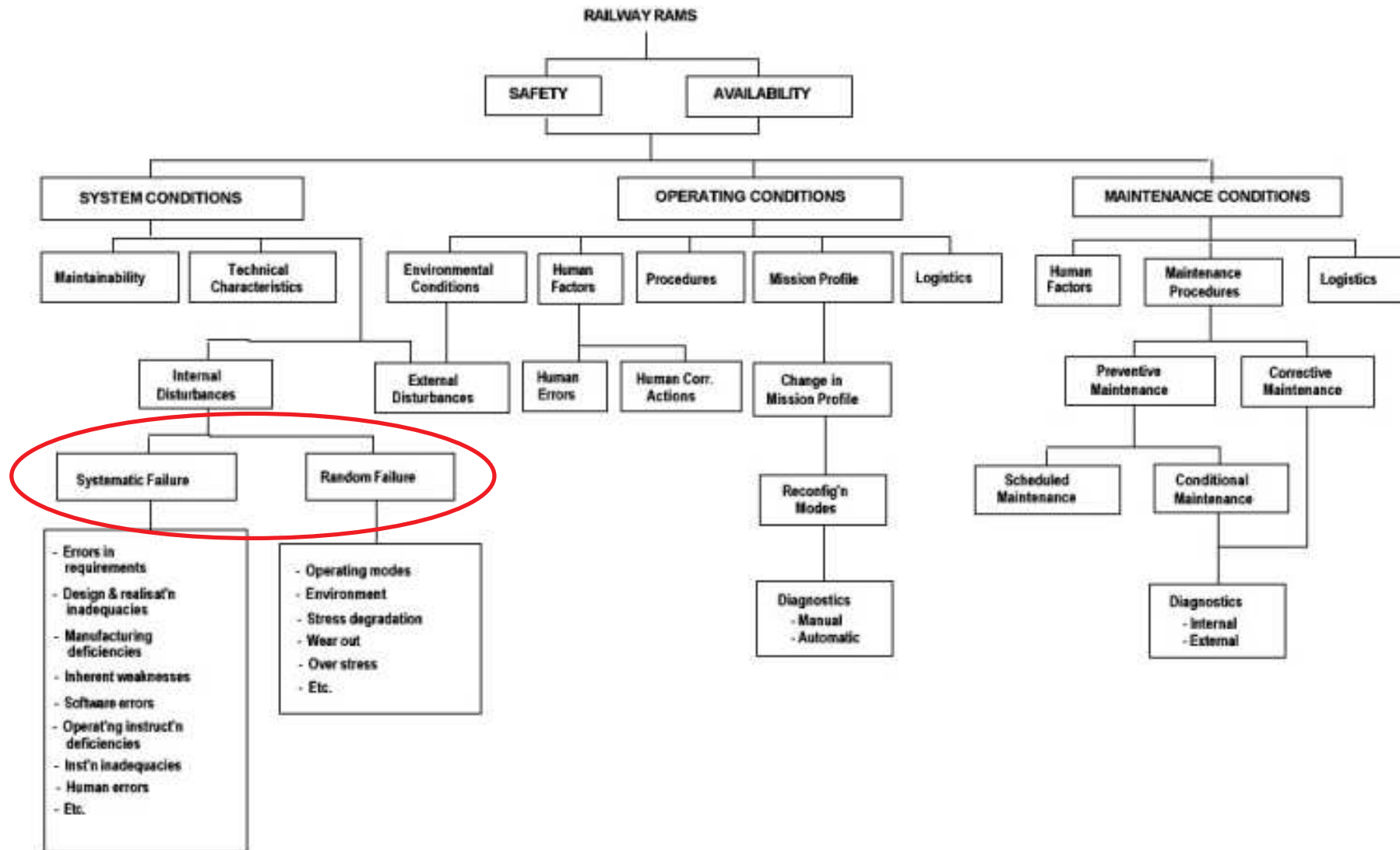
Effects of failures within a Railway system →



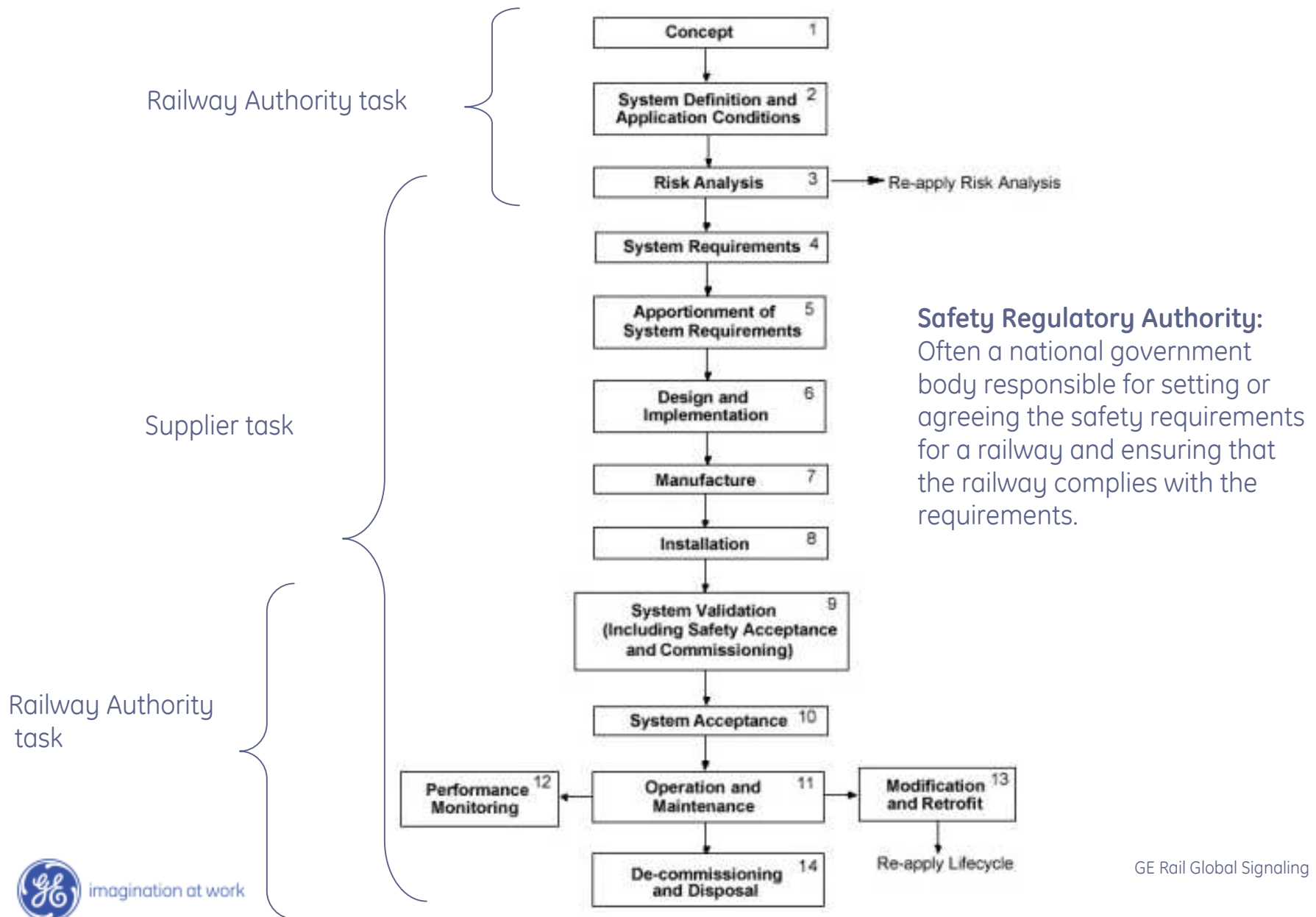
Influences on RAMS →



Influences on Railway RAMS

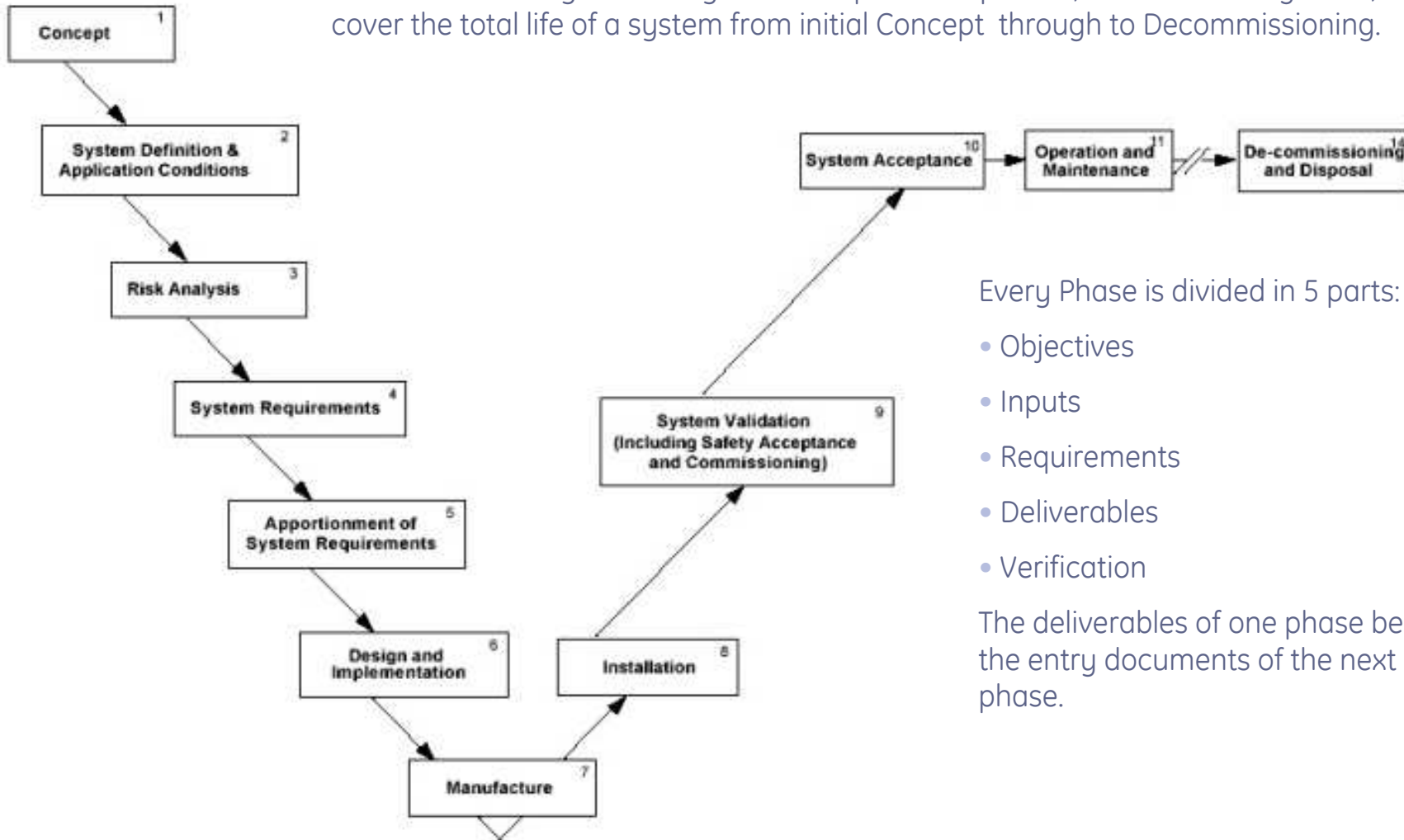


EN 50126 Life Cycle



EN 50126 Life Cycle – “V” representation

The certification system lifecycle is a sequence of phases, each containing tasks, which cover the total life of a system from initial Concept through to Decommissioning.



Every Phase is divided in 5 parts:

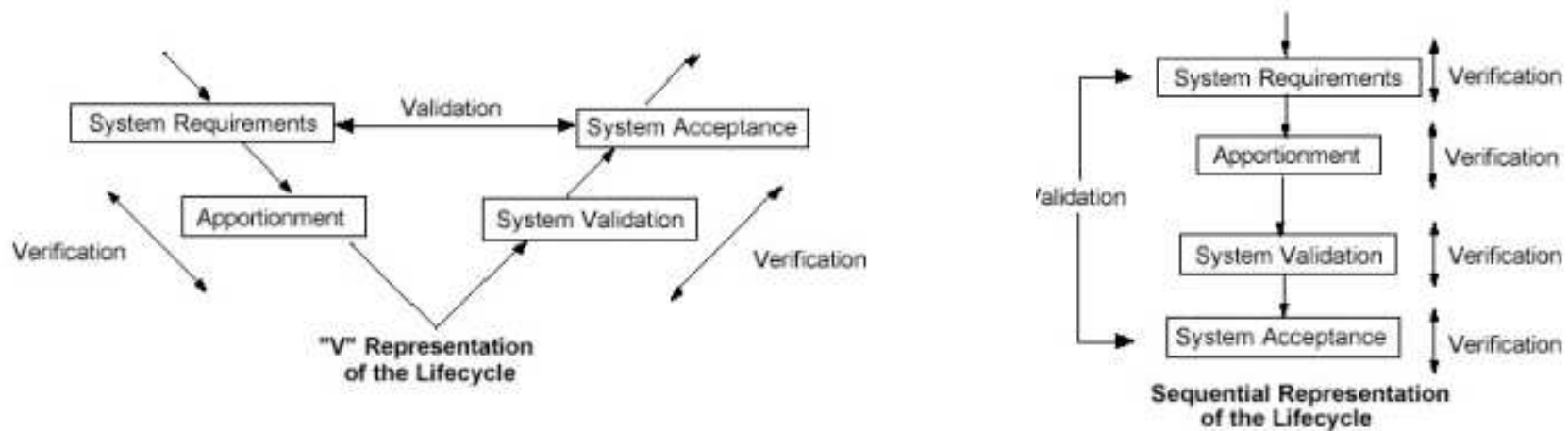
- Objectives
- Inputs
- Requirements
- Deliverables
- Verification

The deliverables of one phase become the entry documents of the next phase.

Verification & Validation

Verification: confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled.

Validation: confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled.



The objective of verification is to demonstrate that, for the specific inputs, the deliverables of each phase meet in all respects the requirements of that phase.

The objective of validation is to demonstrate that the system under consideration, at any step of its development and after its installation, meets its requirements in all respects.

CENELEC Standards

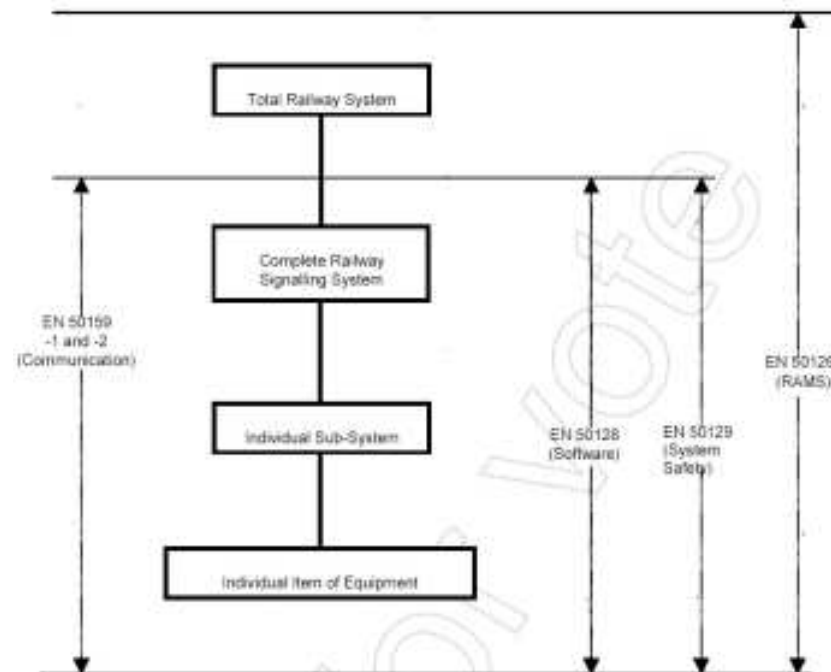
CENELEC is a European Committee for Electromechanical Standardization.
Normative references for Railway Applications are:

- EN 50126 Dependability (RAMS)
- EN 50128 Safety Software (Software process)
- EN 50129 Safety Electronic System (Hardware and Safety)
- EN 50159-1&2 Safety-related communication in closed (1) and open (2) transmission systems

Development of products which conform to European Standards for Homologation require strict adherence to the criteria for:

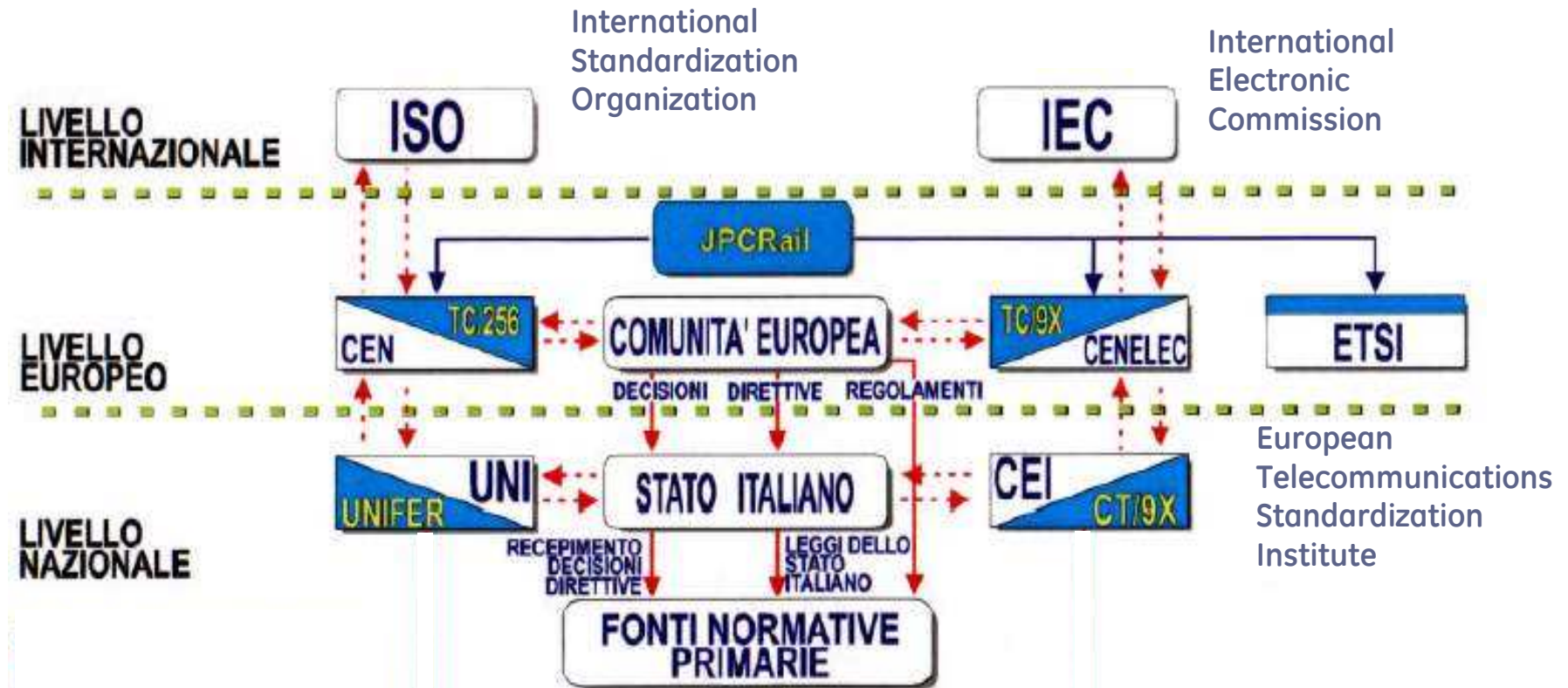
- Quality Management
- Safety Management
- Technical Safety Reports

The norms are applied either “entirely” or “partially” depending on the required System Safety Integrity level [SIL] which is to be achieved.



GE Rail Global Signaling

CENELEC Organization



JPCRail

European
Committee for
Standardization



European
Committee for
Co-ordination
the CEN-
CENELEC
Standardization



European
Committee for
Electrotechnical
Standardization



GE Rail Global Signaling

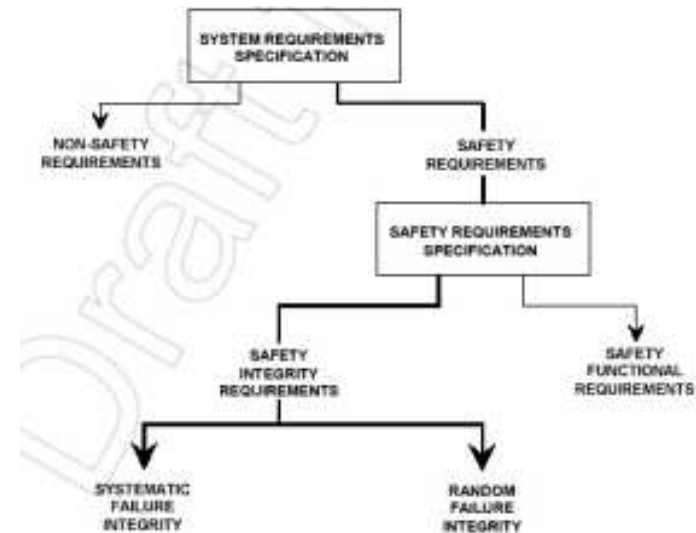
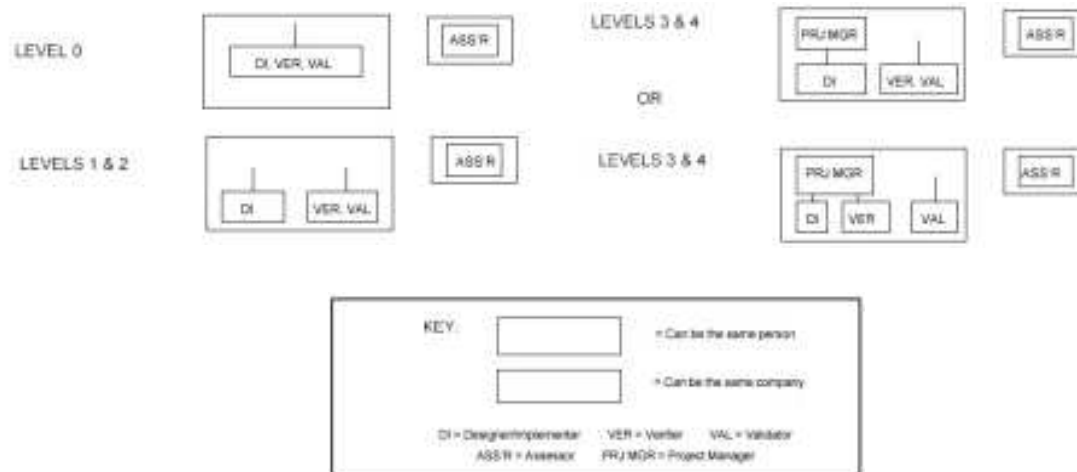
Safety and SILs

Safety: freedom from unacceptable risk of harm.

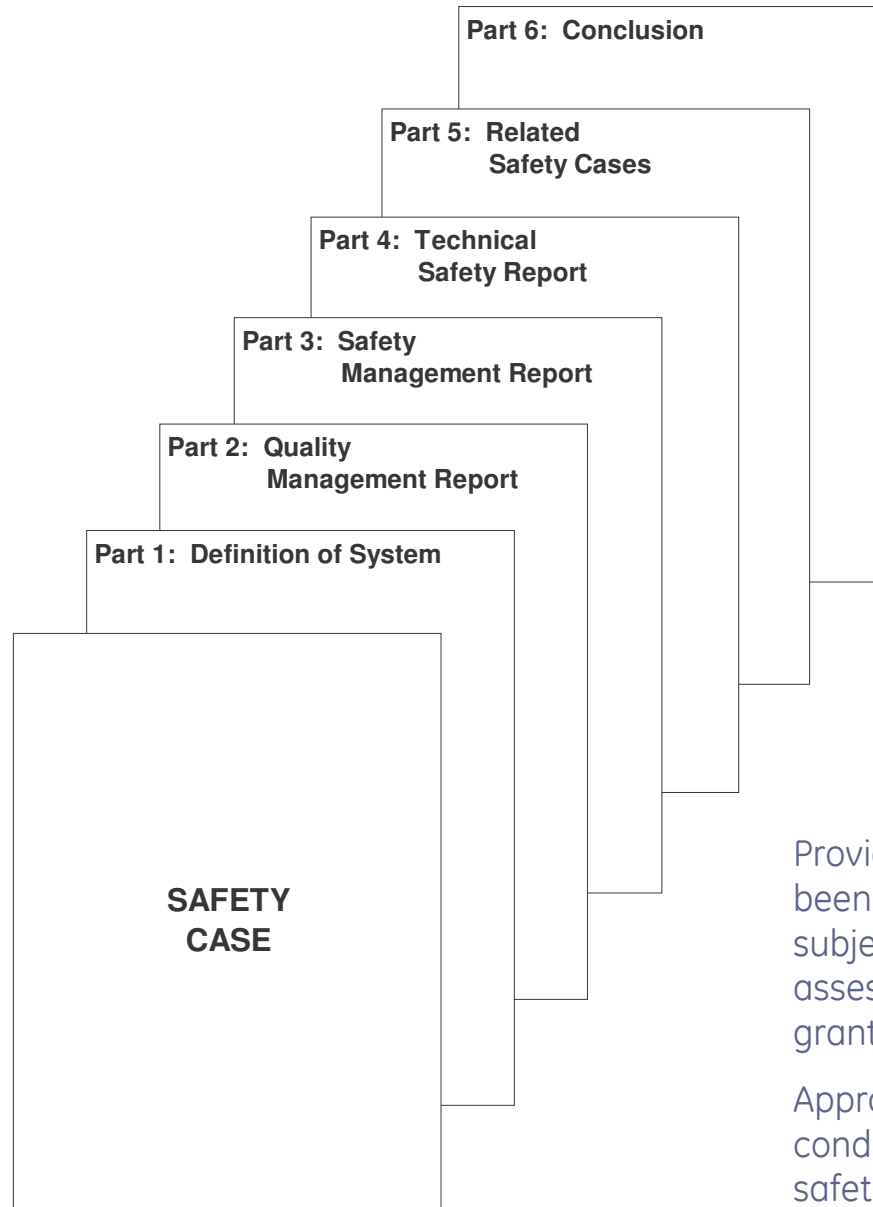
Safety Integrity: the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Safety Integrity Levels: one of a number of defined discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety related systems. Safety Integrity Level with the highest figure has the highest level of safety integrity.

- **SIL = 0** non-safety-related
- **SIL = 1, 2** only some specific functions are safety-related
- **SIL = 3, 4** the maximum safety level and is applied to all functions.



Safety Case



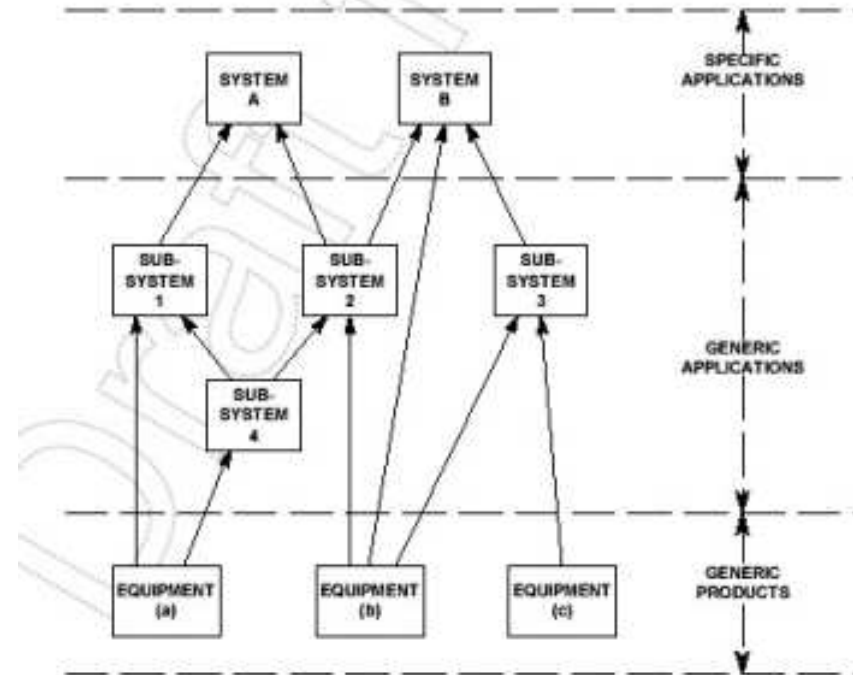
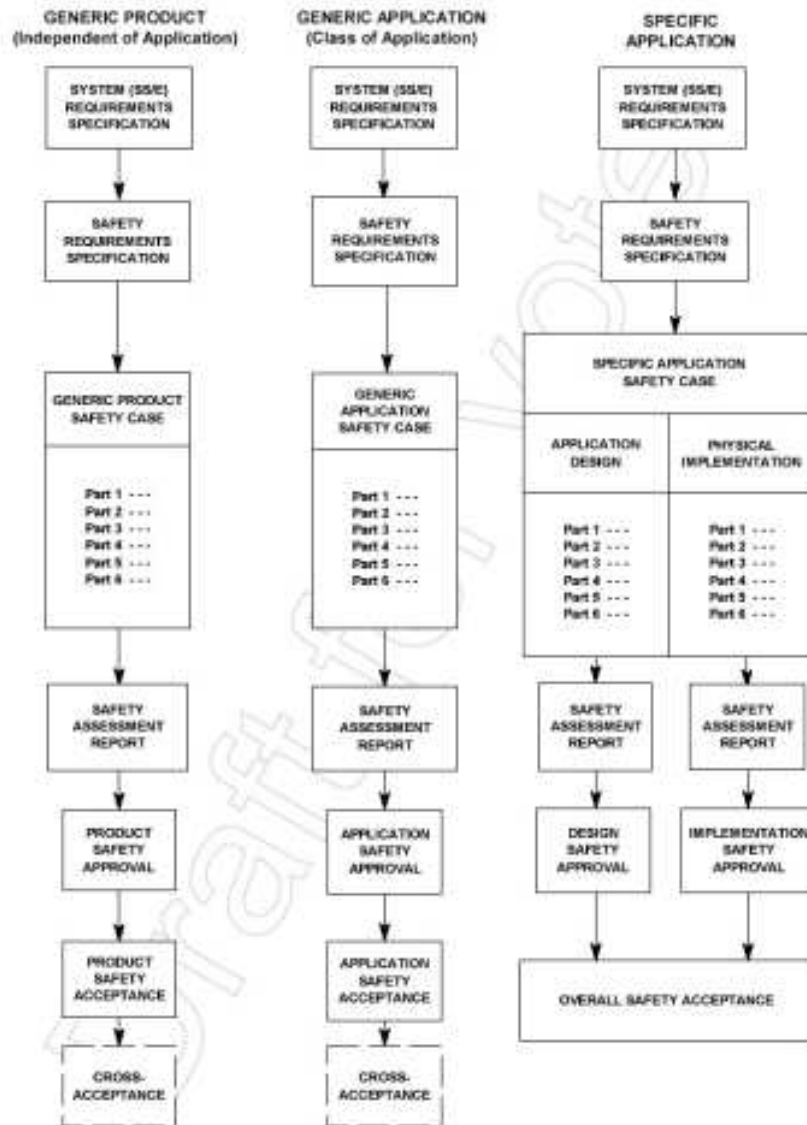
All product's information are contained into a safety Dossier called "Safety Case".

It is essential to demonstrate for each "specific" application that the environmental conditions and context of use are compatible with the "generic" application conditions.

Provided all the conditions for safety acceptance have been satisfied, as demonstrated by the Safety Case, and subject to the results of the independent safety assessment, the system/sub-system/equipment may be granted safety approval by the relevant safety authority.

Approval may be subject to the fulfilment of additional conditions (temporary or permanent) imposed by the safety assessor.

Generic & Specific Application



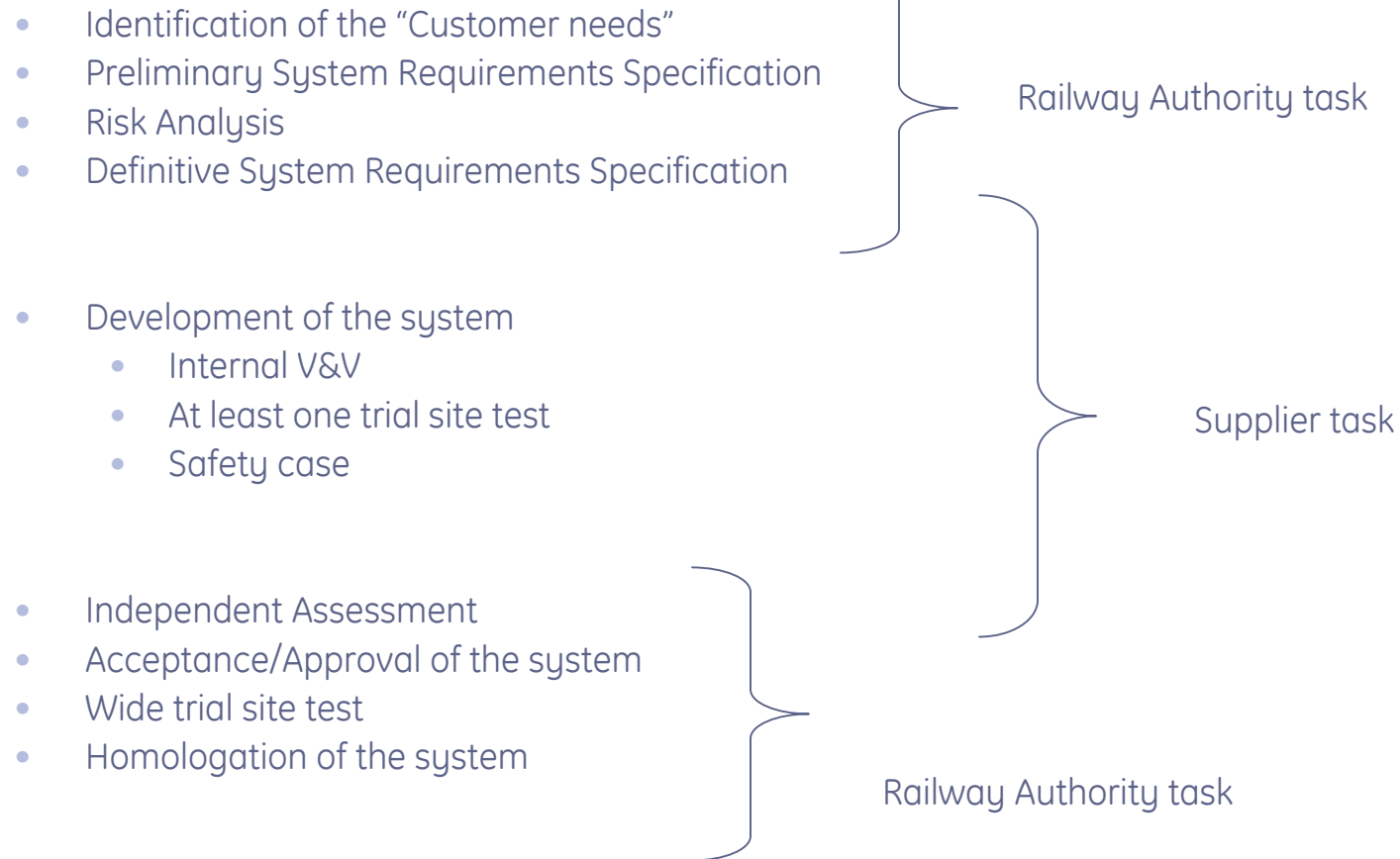
For a generic product (i.e. independent of application), and for a generic application (i.e. class of application), it should be possible for safety approval granted by one safety authority to be accepted by other safety authorities (i.e.: cross-acceptance). This is not considered possible for specific applications.

Risks Analysis in the RFI view



imagination at work

RFI Homologation process



The Risk Analysis process

The “Risk Analysis” process comprises:

- Hazards identification;
- Risk assessment;
- Definition of countermeasures for Risk cancellation or mitigation in respect to the “Tolerability of Risk” criteria defined by European and Italian law;
- Valuation of legal issues for the Risk Acceptance Criteria for every specific country.

Experts Team:

- Risk Analysis process (RFI)
- Supplier Technical side (RFI - Supplier)
- Installation and Maintenance (RFI - Supplier)
- Railway Operational Rules (RFI)

Hazard definition

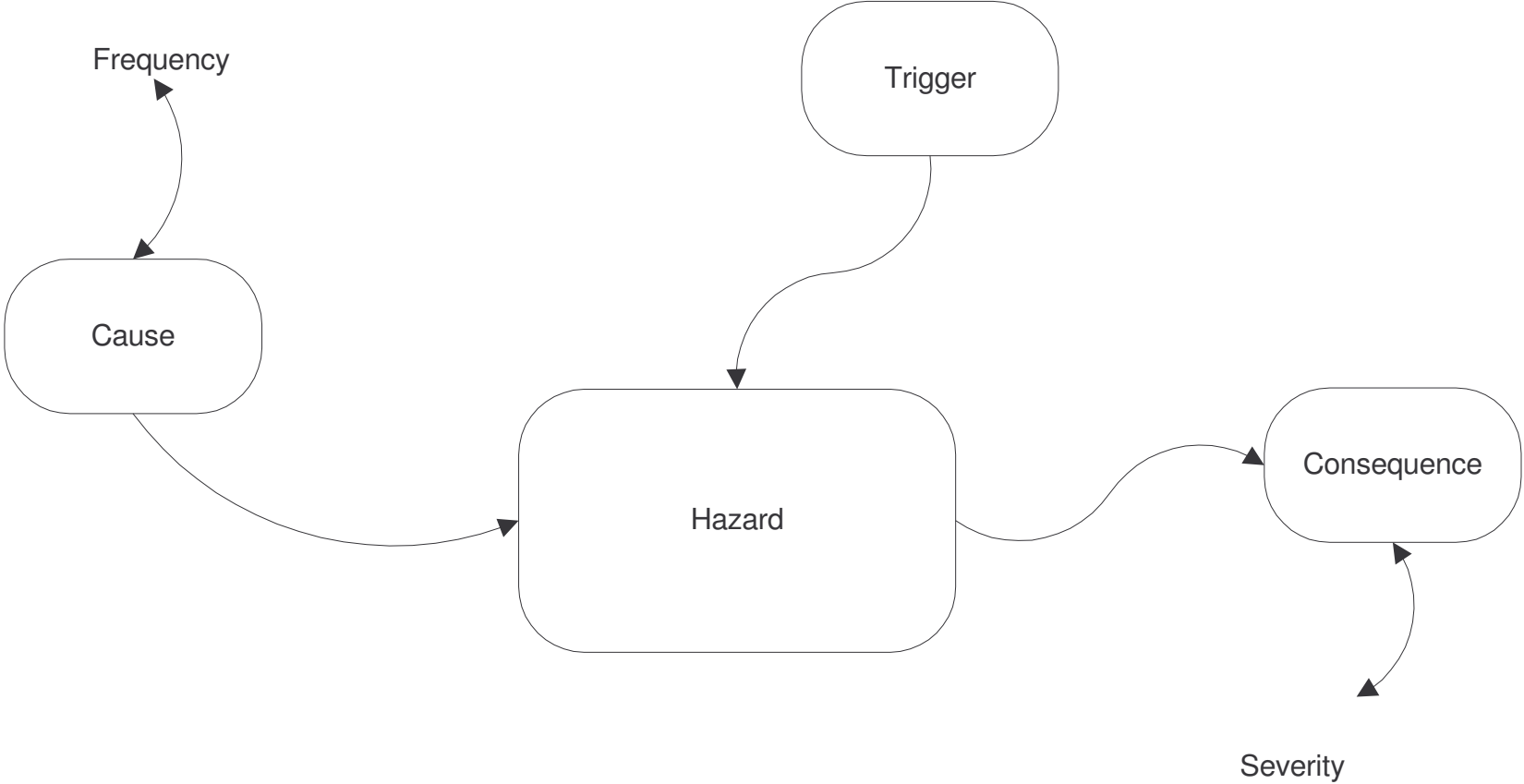
DEFINITION (1): a situation that could be the cause of an accident



An unexpected event or a sequence of events that causes harm to people, things or environment.

DEFINITION (2): a physical situation with a potential for human injury.

Hazard identification



Chain: Cause - Hazard - Consequence

Risk Assessment

Risk: the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm.

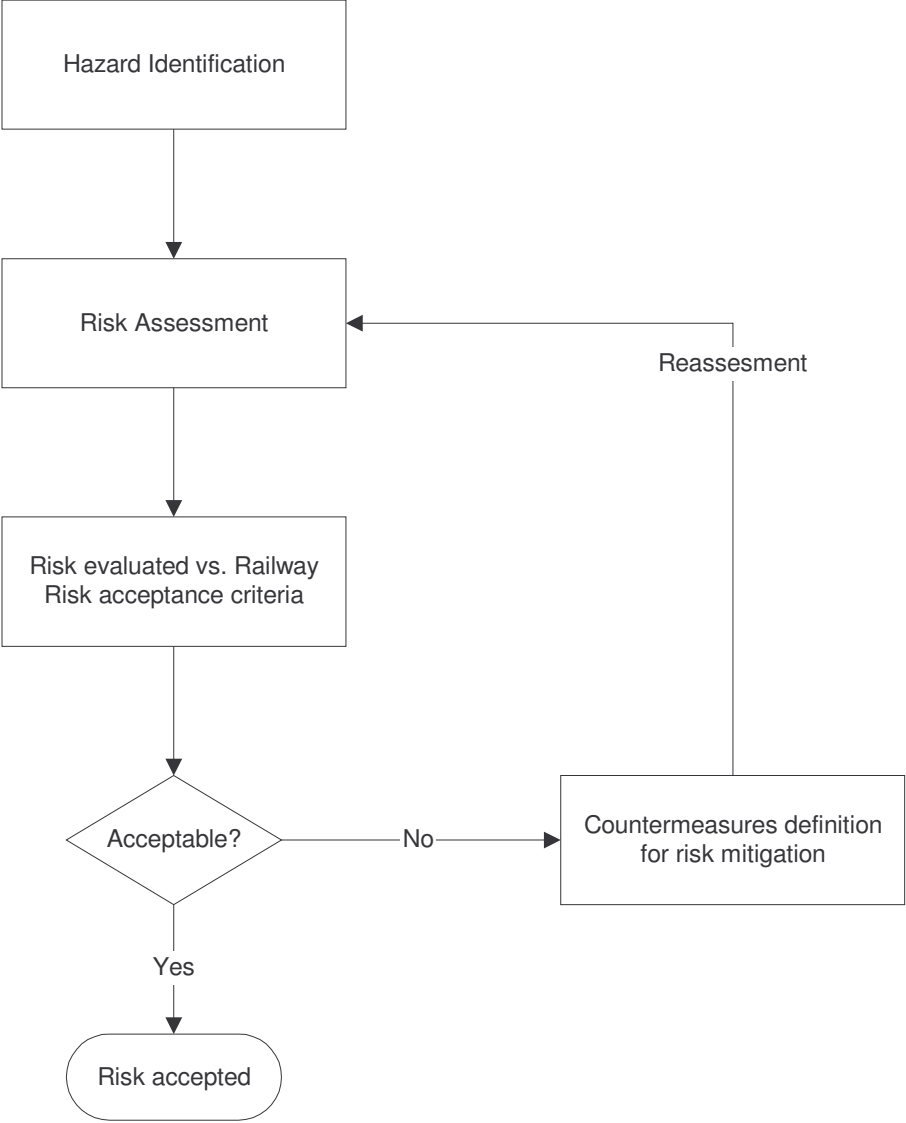
FREQUENCY OF DANGEROUS EVENT APPEARANCE	RISK LEVEL			
FREQUENT	undesirable	intolerable	intolerable	intolerable
LIKELY	tolerable	undesirable	intolerable	intolerable
CHANCE	tolerable	undesirable	undesirable	undesirable
LESS THAN A CHANCE	negligible	tolerable	undesirable	undesirable
UNLIKELY	negligible	negligible	tolerable	tolerable
INCREDIBLE	negligible	negligible	negligible	negligible
	INSIGNIFICANT	MARGINAL	CRITICAL	CATASTROPHIC
	CONSEQUENCES SEVERITY LEVELS OF DANGEROUS EVENTS APPEARANCE			

Example of table for "Risk Assessment" extracted from EN50126

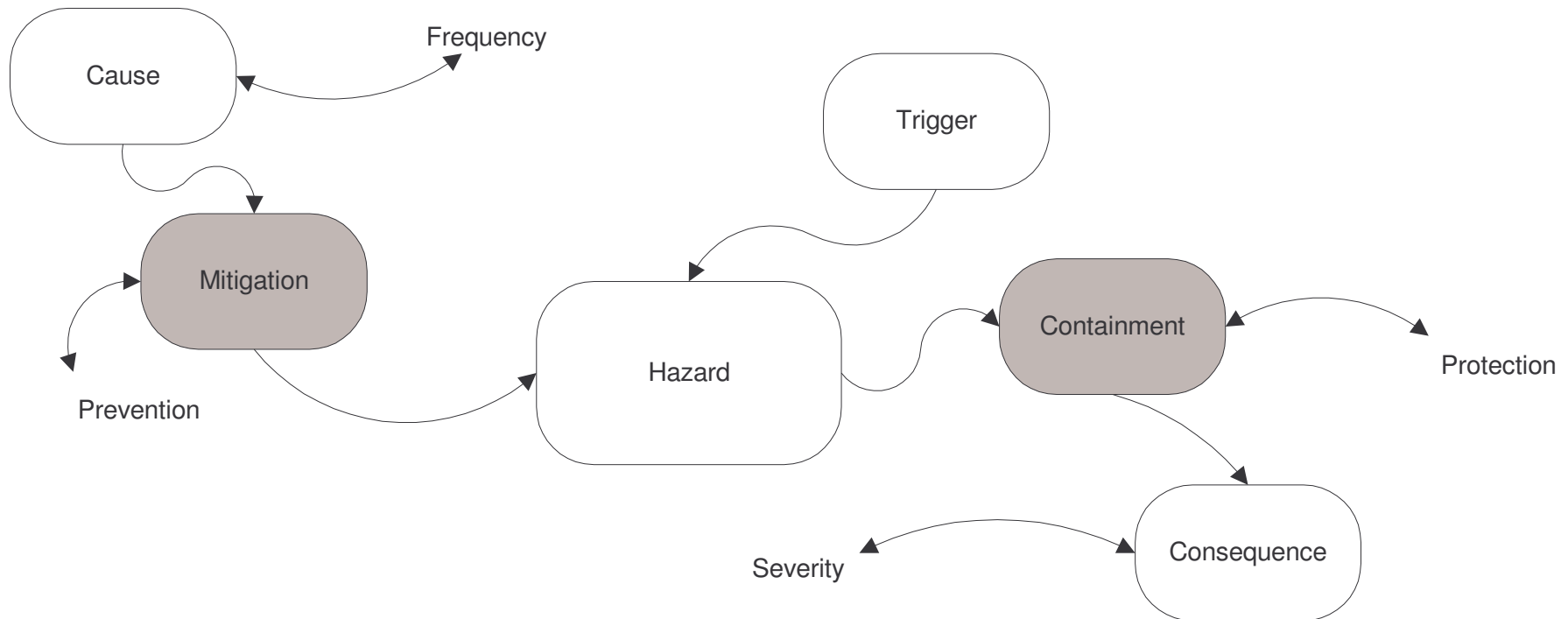
Qualitative Categories of risk

INTOLERABLE:	Must be eliminated;
UNDESIRABLE:	Must be accepted only when the mitigation of Risk is impossible and with the agreement with the Railway Authority or the Railway Security Authority;
TOLERABLE:	Acceptable only with a suitable control and with the agreement with the Railway Authority;
NEGLIGIBLE:	Acceptable with or without the agreement with the Railway Authority;

The Risk Assessment process



Events and Countermeasures



MITIGATION: countermeasure aiming to eliminate or decrease the chance of an Hazardous event;

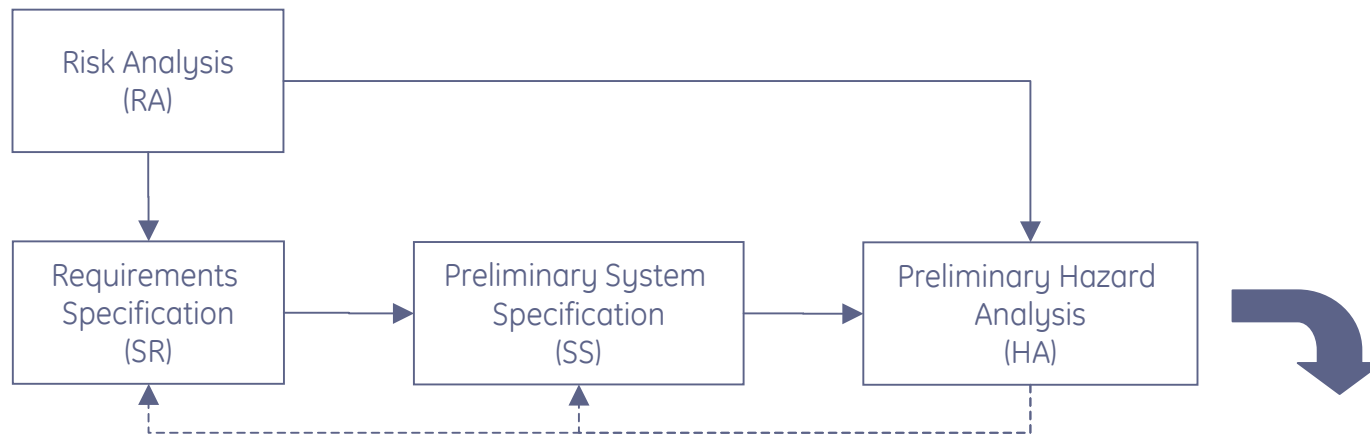
CONTAINMENT: countermeasure aiming to reduce the consequences of an Hazard.

Requirements Flowdown



imagination at work

Requirements flowdown



Preliminary system SIL allocation & Start of Hazard Log

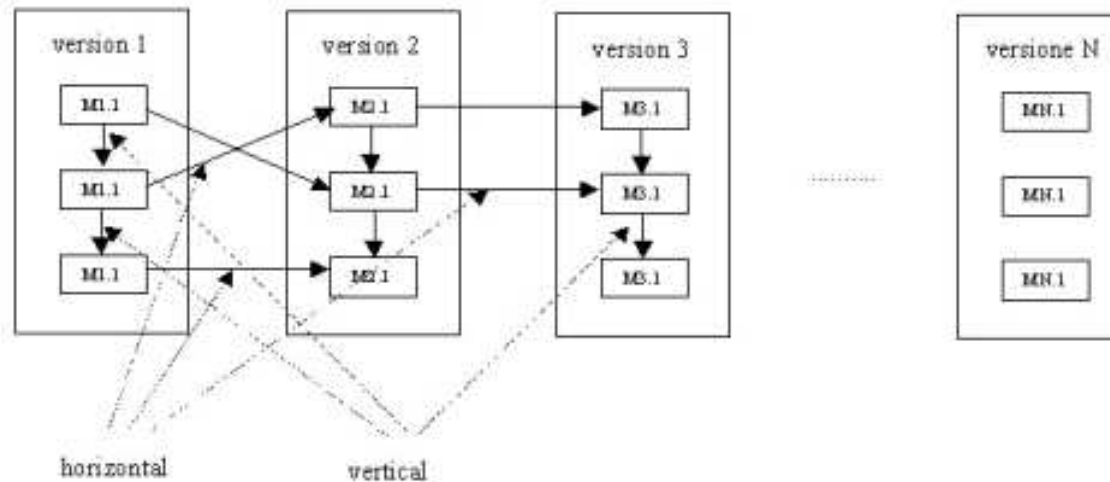
- **Risk Analysis (RA):** determine risks and opportunities for a new system in the Railway environment.
- **Requirements Specification (SR):** holds the high level requirements for the system.
- **System Specification (SS):** let the high level requirements flow in functional blocks (I/E/O) that will be later apportioned to hardware and software modules for the system.
- **Hazard Analysis (HA):** safety analysis of these functional blocks -> safety requirements apportionment.
- **Hazard Log (HL):** the system chronological record of safety issues with open/closed entries.

Requirements Traceability

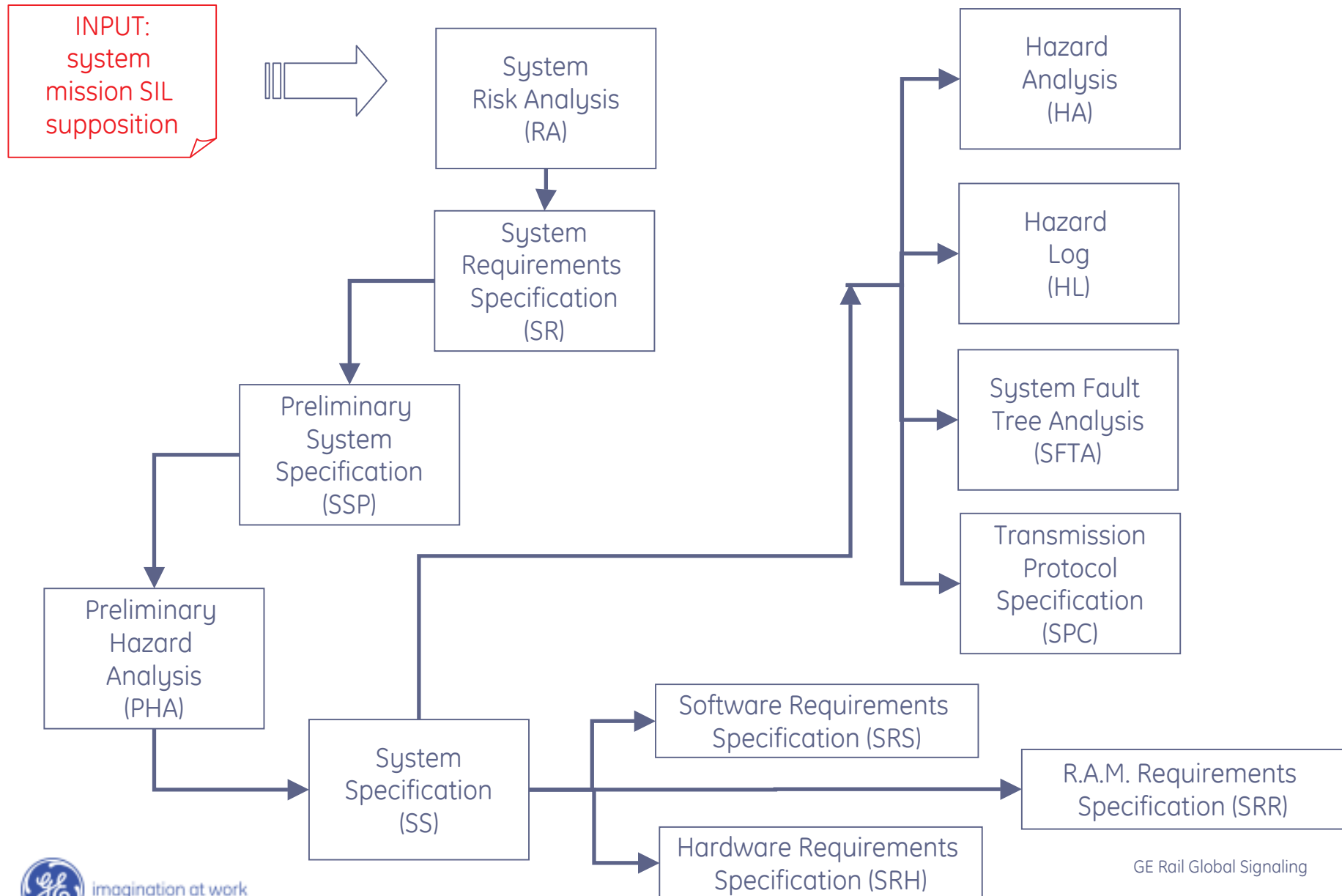
Traceability is used to meet established requirements and allows to reconstruct logical links and choices made, which brought about the actual conception and implementation of the system.

A high level of requirements traceability contributes to the clarity of the documentation, permits improvement of the effectiveness of the development process, and significantly facilitates the comprehension of the system realized;

All this produces a improvement in the maintenance phase, allowing a more precise analysis of the impact of the changes that the system may encounters, sometimes even during the development stage which precedes the delivery.



Requirements flowdown- details



From Risk Analysis to Requirements



imagination at work

Risk Analysis Application

The methodology used in this stage is based upon: “Seven stage process” described in the “Engineering Safety Management” (aka Yellow book).

This process is divided in the following phases:

- Hazard Identification
- Causal Analysis
- Consequence Analysis
- Loss Analysis
- Options Analysis
- Impact Analysis
- Demonstration of Compliance
(w/ ALARP)

Yellow Book	Risk Analysis Matrix
Hazard Identification	Lista degli Hazards
Causal Analysis	Causa degli Hazards
Consequence Analysis	Conseguenza Diretta
	Conseguenza Mitigata
Loss Analysis	Valutazione del Rischio Iniziale
	Valutazione del Rischio Finale
Option Analysis	Contromisure Preventive
	Contromisure di Protezione
Impact Analysis	-
Demonstration of Compliance	-

Risk Analysis Example

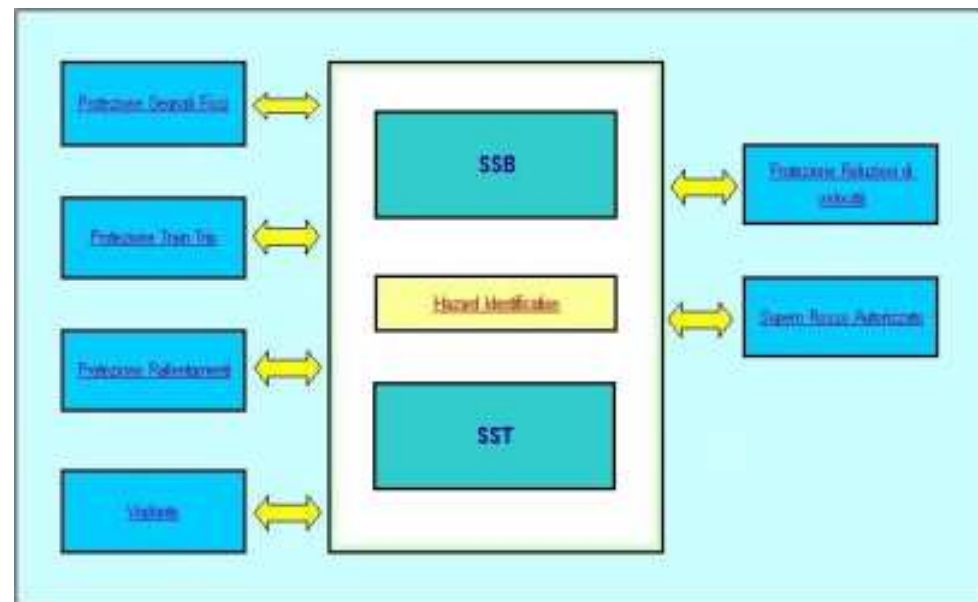
Function N°	System Functions
F1	Protezione dei segnali fissi
F3	Intervento della protezione di train trip
F12	Protezione rispetto ai rallentamenti
F13	Protezione rispetto alle riduzioni di velocità
F17	Supero rosso autorizzato
F30	Vigilante

This list of functions is part of the SCMT (Sistema di Circolazione Marcia Treno) set of system functions.

We'll analyze the risk related to the applicability of these functions in a new generation system.

As example, we will suppose to have a list of functions (a kind of specification) provided by the Customer.

This could represent a macro function, identified by the Customer, part of the total Railway system.



Hazard and Causes Identification

The analysis of the previous list of functions has brought the following list of hazards:

- Errore Umano del PdM;
- Errata Acquisizione Messaggio da parte del SSB;
- Mancata Acquisizione Messaggio da parte del SSB;
- Errata Trasmissione Messaggio da parte del SST;
- Mancata Trasmissione Messaggio da parte del SST;
- Errata Comunicazione tra SSB e SST;
- Mancata Comunicazione tra SSB e SST;
- Errata posa o Configurazione del SST;
- Errata posa o Configurazione del SSB;

The analysis is carried out by an experts team including RFI and Supplier(s) personnel.

In the following table system Hazards are listed with causes that could trigger them.

Hazards and Causes

N°	Funzione	Cod	HAZARD	Cod.	Causa dell'HAZARD
1	Protezione Segnali Fissi	H01	Superamento Segnale a V.I.	CH01.1	Errore Umano del PdM
				CH01.2	Errata Acquisizione del SSB
				CH01.3	Mancata Acquisizione del SSB
				CH01.4	Errata Trasmissione del SST
				CH01.5	Mancata Trasmissione del SST
				CH01.6	Errata Comunicazione tra SSB e SST
				CH01.7	Mancata Comunicazione tra SSB e SST
				CH01.8	Errata posa o Configurazione del SST
				CH01.9	Errata posa o Configurazione del SSB
H02	Mancato Riconoscimento del Segnale Restrittivo			CH02.1	Errore Umano del PdM
				CH02.2	Errata Acquisizione del SSB
				CH02.3	Mancata Acquisizione del SSB
				CH02.4	Errata Trasmissione del SST
				CH02.5	Mancata Trasmissione del SST
				CH02.6	Errata Comunicazione tra SSB e SST
				CH02.7	Mancata Comunicazione tra SSB e SST
				CH02.8	Errata posa o Configurazione del SST
				CH02.9	Errata posa o Configurazione del SSB

Reqs. Identification from Hazards

System Risk Analysis allows to identify Functional and Safety Requirements.

Other type of Requirements (like Operational or Environmental Requirements) are included in a later stage, when the System Requirements document is actually created.

This is not a problem because all non functional requirements that could lead to a risk are already included in the Risk Analysis.

N°	Functions	Cod	HAZARD
1	Protezione Segnali Fissi	H01	Superamento Segnale a V.I.
		H02	Mancato Riconoscimento del Segnale Restrittivo

N°	Functional Requirements
FR1	Ripete a bordo del treno l'aspetto dei segnali di linea, di stazione e di protezione di PL
FR3	Indica a bordo la presenza di una segnalazione restrittiva come avviso con prima luce al giallo ed altre
FR5	Indica a bordo la presenza di una segnalazione di aspetto rosso o di via impedita

Risk Analysis deliverables

N°	FUNZIONE	ID HAZ.	HAZARD	ID CH	CAUSA DEL HAZARD	CONSEGUENZA DIRETTA	VALUTAZIONE del RISCHIO	CONTRO MISURE PREVENTIVE	CONTRO MISURE DI PROTEZIONE	CONSEGUENZA MITIGATA	VALUTAZIONE FINALE del RISCHIO
1	Protezione dei Segnali Fissi	H01	Superamento Segnale a V.I.	CH011	Errore Umano del P dM	Collisione	Intollerabile	Procedure per il Personale di Macchina	SSB deve comandare la frenatura rapida	Arresto delTreno	Trascurabile
				CH012	Errata Acquisizione delSSB	Collisione	Intollerabile	Architettura in Sicurezza con Autotest della Centralina Elettronica di bordo	SSB deve comandare la frenatura rapida per messaggio errato in Rx	Arresto delTreno	Trascurabile
				CH013	Mancata Acquisizione delSSB	Collisione	Intollerabile	Implementazione della logica degli appuntamenti e Architettura in Sicurezza con Autotest delle Antenne di Ricezione	SSB deve comandare la frenatura rapida	Arresto delTreno	Trascurabile

This leads to a System Requirements Specification in which requirements coming from the Risk Analysis are completed by other types. System Requirements Specification is the main deliverable of Risk Analysis.

Req. N°	Description
FR 1	Dovrà indicare a bordo la presenza di una segnalazione restrittiva.

System Requirements Spec.

REQUIREMENTS CLASSIFICATION: Each System Requirement is classified into different types, in order to facilitate their consultation, traceability and updating.

- **Norms** (acronym **NR**)
- **Functional Requirements** (**FR**)
- **Performance Requirements** (**PR**)
- **Safety Requirements** (**SR**)
- **RAM Requirements**
 - **Reliability [RR] - Availability [AR] - Maintainability [MR];**
- **Diagnostic Requirements** (**DR**)
- **Maintenance** (**MNR**)
- **Portability** (**PoR**)
- **Usability** (**UR**)
- **Security** (**SeR**)
- **Health & Safety** (**HSR**)
- **Encumbrance & Bulk** (**EBR**)
- **Operational and Environmental Requirements** (**ER**)
- **Interface Requirements** (**IR**)
- **Structural Requirements** (**STCR**)
- **Configurations of the System** (**CM**)
- **System's Accessories** (**ACM**)

System Requirements Specification aims to define high level requirements without taking in account the actual (i.e. future) implementation of the system. No implementation issue should be considered.

Functional Blocks

SYSTEM DECOMPOSITION IN FUNCTIONAL BLOCKS: functional blocks are included in the next stage to introduce an additional detail level.

Functional blocks aims to define a detail level closer to system design and implementation.

System Specification is the input document for Hazard Analysis.

SST SUBSYSTEM		
N°	Block Name	Description
01	Lettura Ingressi Segnale	Lettura ciclica delle porte corrispondenti agli ingressi collegati al segnale.

Functional blocks are described in terms of: INPUT, PROCESS and OUTPUT. This description details only functional features of the block. After the Hazard Analysis, safety is allocated to functional blocks and for each block, a strategy to assure safety is implemented.

Functions and Functional Blocks

SYSTEM FUNCTIONS: each functional block is split in functions. Each PROCESS description shall include the list of its functions.

LETTURA INGRESSI SEGNALE
Ingressi
Prelievo di tensione in parallelo dalla lampada (SDO) che viene trasformato in condizione logica.
Processo
Lettura ciclica delle porte corrispondenti agli ingressi collegati al segnale. Di seguito si riporta l'elenco delle funzioni che tale processo sviluppa:
- Lettura e memorizzazione stato ingressi.
Uscite
Stato di ciascun ingresso campionato.

N°	Function	Functional Block
SST – 01	Lettura stato ingressi	§. 4.1.2
SST – 02	Memorizzazione stato ingressi	§. 4.1.2
SST – 03	Filtraggio Stato Ingressi	§. 4.1.3

Functions and Hazards

HAZARDS: are identified for each functions belonging to a functional block.

N°	Funzione	Hazard associati	ID
01	Lettura stato ingressi	Mancata Lettura stato ingressi	HT01
		Errata Lettura stato ingressi	HT02

Hazard Analysis plays a similar but different role in the process. Hazard Analysis is related to Hazards emerging inside of the system at a Functional Block level.

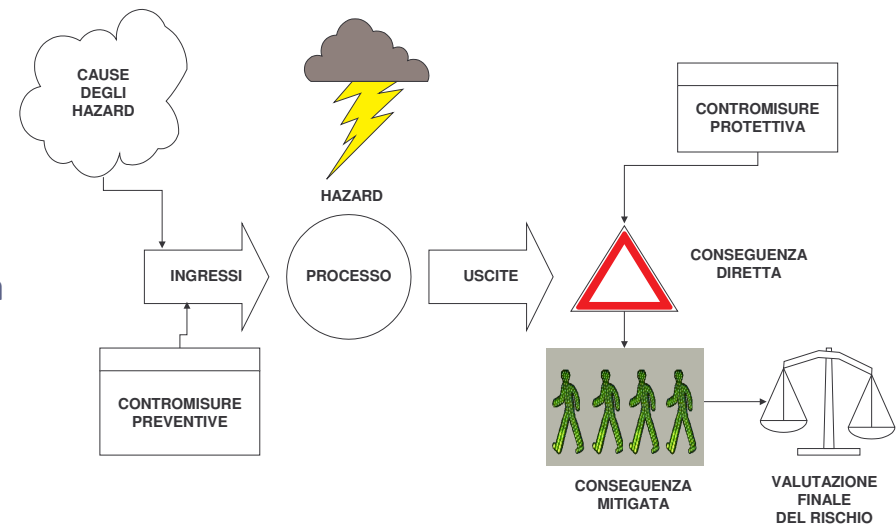
Hazard Analysis aims to define those blocks related with safety issues and allocate safety requirements to blocks.

The main difference is the boundaries of the analysis, the process is close.

Hazard Analysis

HAZARD causal analysis is composed by:

- Hazard identification;
- Risk Assessment;
- Definition of countermeasures for risk elimination or reduction;
- Verification vs. national criteria for risk acceptability.



For each hazard identified, the analysis allows to find its generating causes.

This brings to a preliminary risk evaluation, evaluating consequences without any protection and/or containment countermeasure.

The analysis of causes helps to estimate the hazard frequency and thus to find out countermeasures to reduce or eliminate it.

If the risk (i.e.frequency) is not wiped out, then countermeasures has to be identified and established to contain the severity of hazard consequences .

The mitigated consequences has to be appointed for approval to the National Railway Safety Authority to be checked against the national criteria for risk acceptability, defined by the law.

Hazard Analysis deliverables

RIF. SSP		CAP. §. 4.1.2			LETTURA INGRESSI SEGNALI							
N°	ELEMENTO DI INFLUENZA	ID HAZ.	HAZARD	ID CH	CAUSA DEL HAZARD	CONSEGUENZA DIRETTA	VALUTAZIONE DEL RISCHIO	CONTRO MISURE PREVENTIVE	CONTRO MISURE DI PROTEZIONE	CONSEGUENZA MITIGATA	VALUTAZIONE FINALE DEL RISCHIO	IMPATTO
1	Lettura stato ingressi	HT01	Mancata Lettura Stato Ingressi	CHT01.1	Guasto Random Hw	Messaggio Errato	Intollerabile	-	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	SR
				CHT01.2	Errata Installazione	Messaggio Errato	Intollerabile	Procedure di installazione (SM)	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	
				CHT01.3	Errata Manutenzione	Messaggio Errato	Intollerabile	Procedure di manutenzione (SM)	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	
				CHT01.4	Vandalismo	Messaggio Errato	Intollerabile	-	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	
		HT02	Errata Lettura Stato Ingressi	CHT02.1	Guasto Random Hw	Messaggio Errato	Intollerabile	Test ciclici ingressi (Architettura SST in sicurezza)	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	SR
				CHT02.2	Difetto Sw	Messaggio Errato	Intollerabile	Progetto e Validazione Sw	vediNOTA 2	Funzionamento Nominale	Trascurabile	
				CHT02.3	Errata Installazione	Messaggio Errato	Intollerabile	Procedure di installazione (SM)	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	
				CHT02.4	Errata Manutenzione	Messaggio Errato	Intollerabile	Procedure di manutenzione (SM)	Invio messaggio più restrittivo (Architettura SST in sicurezza)	Attivazione segnalazione restrittiva	Trascurabile	

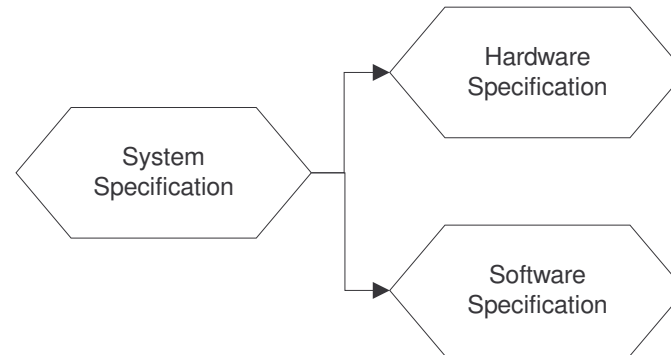
Requirements Specification



imagination at work

Formality vs. Informality

Requirements needs to be specified more and more in detail as long as the process go on.



This is because different people works at different stages and for every stage, needs vary.

As example, the step between System Specification and Hw/Sw Specification is very critical because a next step in detail and a change of context.

This is one of the main point to have a formal process for assuring the correct specification of requirements through the whole life cycle.

Lots of studies have been carried out to determine the best approach to Requirements Engineering, but the main lesson learnt is that as much effort as possible has to be put in the Specification phase(s).

Requirements and NL

A formal specification is defined as an unambiguous specification. Formality often matches with formal verification of requirements, because formality is naturally coupled with mathematics.

Since is nearly impossible to have a formal specification from the very beginning of a project (i.e. one provided by the Customer), we have to deal with a informal specification written in Natural Language.

Natural Language can be approached in two ways:

- Lexical/ Syntactical Analysis;
- Semantic Analysis.

Semantic analysis is something very difficult to implement in a real industrial application because capturing the complexity of the real world (even in a bounded environment) is something that still goes beyond the capability of actual tools.

Lexical/Syntactical analysis can help during the review of the Requirements Specification, but is not enough.

Lexical/Syntactical analysis must be enforced with rules for requirements statement.

Role of the Requirements

ROLE OF A REQUIREMENT IN A PROJECT DESIGN

- Show what a product must do
- Form a basis for the project design and to optimise the project design
- Test the system, or part of it during its development
- The traceability to the source, history and effort of the project design
- Consent a logical approach to changes
- Communicate basic aspects of the product to third parties using a limited number of technical terms
- Use as a base for a contract

DEFINITION OF A REQUIREMENT

- What is the nature of the problem that has to be resolved? (identification of the **limits of the system**).
- Where is the problem? (understanding of the **context** and **where the problem is found**).
- Whose problem is it? (identification of the **stakeholders**).
- Why does the problem have to be resolved? (identification of the scope of the **stakeholders**).
- How can our product contribute? (listing of some **goals, scenarios** and **examples of usage**).
- When and how must the problem be resolved? (identification of **development limitations**).
- What can stop us from resolving the problem? (identification of **feasibility** and the **risks**).

Role of the Specification

CHARACTERISTICS OF THE SPECIFICATION

- **Correct:** express the actual requirements.
- **Complete:** specifies what the system must do...And what it should not do.
- **Consistent:** does not contradict, all terms used are consistent.
- **Necessary:** does not contain anything which is not a "requirement".
- **Non ambiguous:** each statement (requirement) can be interpreted in only one way, terms that generate confusion must be clarified.
- **Verifiable:** each process, component, ... of the system exists to satisfy a requirement (or more than one requirement), each requirement is specified by the performance of the system.
- **Clear:** to all users of the system.
- **Changeable:** can be updated.
- **Independent from the platform:** the requirement indicates the function and not the solution.
- **Abstract:** must contain only the basic aspects.
- **Minimal:** must not be redundant.

POSSIBLE PROBLEMS IN DEFINING THE SPECIFICATION

- **Ambiguity:** text may be interpreted in more ways.
- **Contradiction:** text that defines a characteristic in different ways incompatible each other.
- **Rumour:** text that does not carry any relevant information concerning the characteristics of the problem.
- **Silence:** a certain characteristic is not defined by any part of the specification.
- **Super specification:** text which describes the solution instead of the function.
- **Advance references:** references characteristics not yet definite.
- **Inconsistent terminology:** text which cannot be validated, terms are invented.

Rules for Requirements 1/2

A structured process is required to manage requirements.

Every phase (System Requirements Spec., System Spec., Software Spec., Hardware Spec., ...) shall have its own process and template to define a set of requirements and then there must be rules to write these requirements.

RESTRICTED WORDING

The wording does not have to be rich and varied. Writing the requirements must not be a creative effort, requirement must not be written to impress the reader.

- The wording used to write the requirements must be precise and unequivocal.
- It is necessary to refer to international standards in order to understand the exact form of the terms to be used.
- Words defining requirements must not be invented.
- A glossary of terms must be compiled .
 - VAGUE TERMS (clear, well, ...)
 - WEAK VERBS (may, might, can, could, ...)
 - TERMS WHICH INDICATE OPTION (possibly, eventually, ...)
 - UNSPECIFIED TERMS (reliable, true, ...)
 - TERMS INDICATING SUBJECTIVITY (having in mind, considering, ...)

Rules for Requirements 2/2

CHARACTERISTICS OF THE SPECIFICATION

- **A requirement is a complete sentence:** an individual requirement (atomic), must be composed of only one sentence. Must have a subject (explicit) and a predicate.
 - The use of a subject permits association of a certain entity to the requirement
 - Must express an action or something that must be done for, with, by or to the subject.

- The use of the servile verb **must** (which indicates **obligation**) serves to define the requirements.
 - **Must (indicative future, Shall):** is normally used to indicate a functional characteristic
 - **Must (indicative, present, Must or must not):** is used to establish performance requirements or limitations

- The verb **Can** (which indicates **choice**) (**in an tense, Must**): must be avoided.

- Other verbs that can be used in different classes of requirements:
 - **Is required to, can:** to be used to state performance requirements, written in the passive form.
 - **Are applicable:** is normally used to include, as reference, standards or other additional documents.

- **Do not compose multiple requirements:** that are connected to each other by conjunctions such as: **and, or, with, also.**

- **Do not express possibility:** including “suggestions” that are not explicitly identifiable as requirements

Specification Analysis

Most of these rules can be enforced and verified through Lexical/ Syntactical Analysis, and tools exist to do this kind of verification (see NASA's ARM).

Unfortunately this approach cannot provide the final answer for:

- Gather requirements information;
- Analyze requirements information;
- Agree upon requirements;
- Communicate requirements;
- Efficiently keep requirements up to date.

Requirements need a rigorous approach and must be viewed in a context of a project where many stakeholders have their requests, starting from the external customer to the internal stakeholders.

A good methodology for dealing with these points is Requirements Modelling and Simulation.

Requirements Modelling and Simulation with Formal Methods



imagination at work

CENELEC & Formal Methods

CENELEC EN 50129 marks as “High Recommended” (HR) Formal Methods for the creation of a system structured Specification.

Techniques/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
Structured Specification	HR: manual hierarchical separation into subtasks, description of the interfaces		HR: hierarchical separation using <u>formalised methods</u> , automatic consistency checks, refinement down to functional level	
Formal or semiformal methods			R: computer-aided	

CENELEC EN 50128 marks as “High Recommended” (HR) Formal Methods for Software Design.

TECHNIQUE/ MEASURE	SWSIL 0	SWSIL 1	SWSIL 2	SWSIL 3	SWSIL 4
Formal Methods	-	R	R	HR	HR
Semi-Formal Methods	R	R	R	HR	HR
Structured Methodology	R	HR	HR	HR	HR

The project

The aim of the project was to verify the usefulness of Formal Methods (FM) in our CENELEC Software Life Cycle.



- ❑ It was studied a System Requirements Specification (SRS). This document is important:
 - for correct development during the Life Cycle;
 - because it's the "contract" with customer.
- ❑ The study was only based on the Customer's SRS that, as usual, was written in natural language.
- ❑ No implementation by Engineering Design Team has been considered.
- ❑ Was decided to study also the rainy days scenarios of the system.
- ❑ The project was carried on by Niccolò Zingoni during his graduation thesis. Now Niccolò is a member of GETS V&V team.



Rev.	Data	Descrizione	Verifica Tecnica	Autore/Revisione
0	21/11/2003	Versione Preliminare per la sperimentazione	Sim. Masetto, L. C. Neri	Ing. Diego CERRA

FM Tool

1. The FM tool used was Statemate (from I-logix), because:

- this tool allows to create a not ambiguous model of the system;
- it is also sponsored by our main Customer (RFI – Italian Railways).

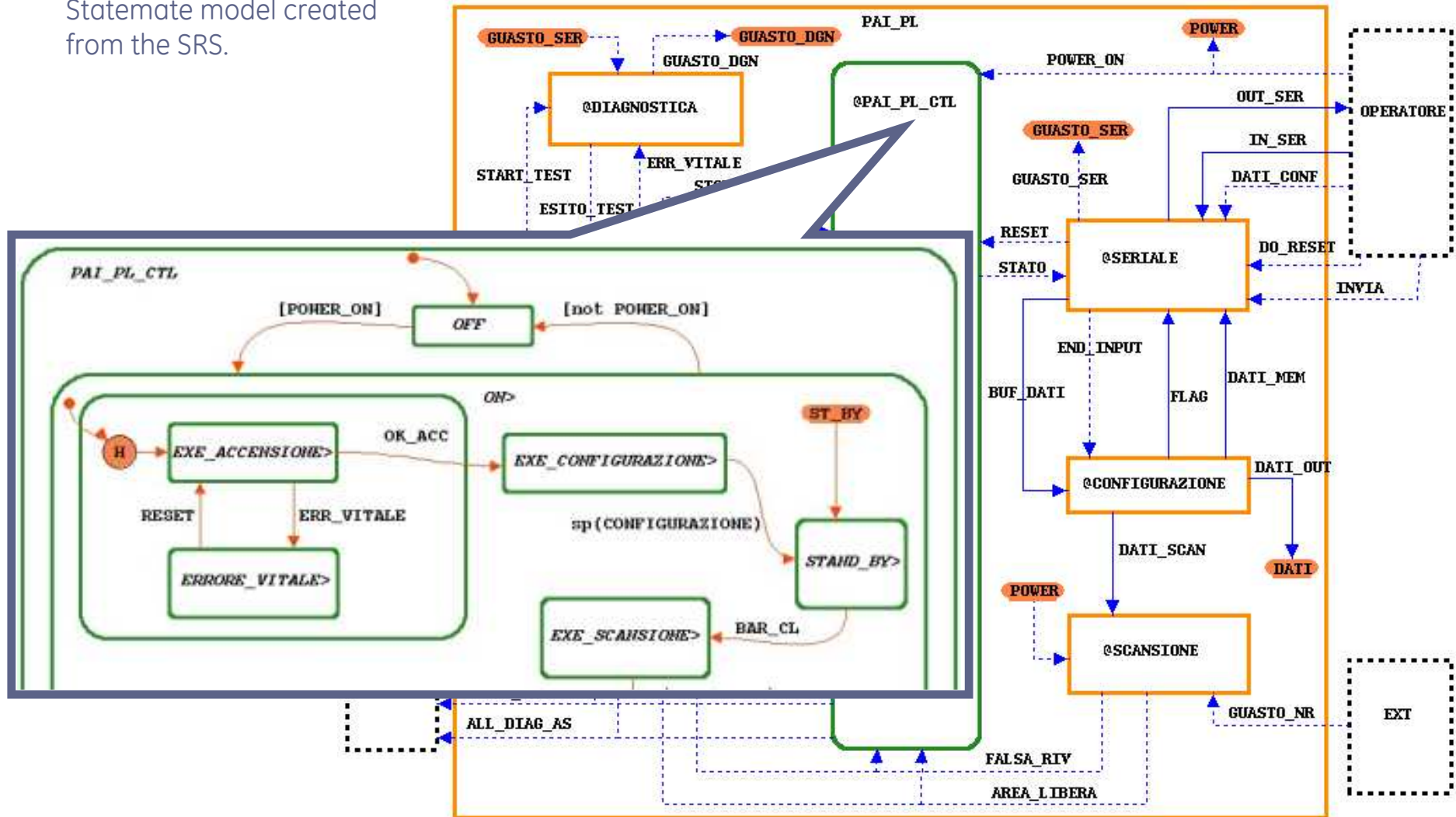


2. The SRS chosen to build the experimental model was the one from CROSSGUARD system.

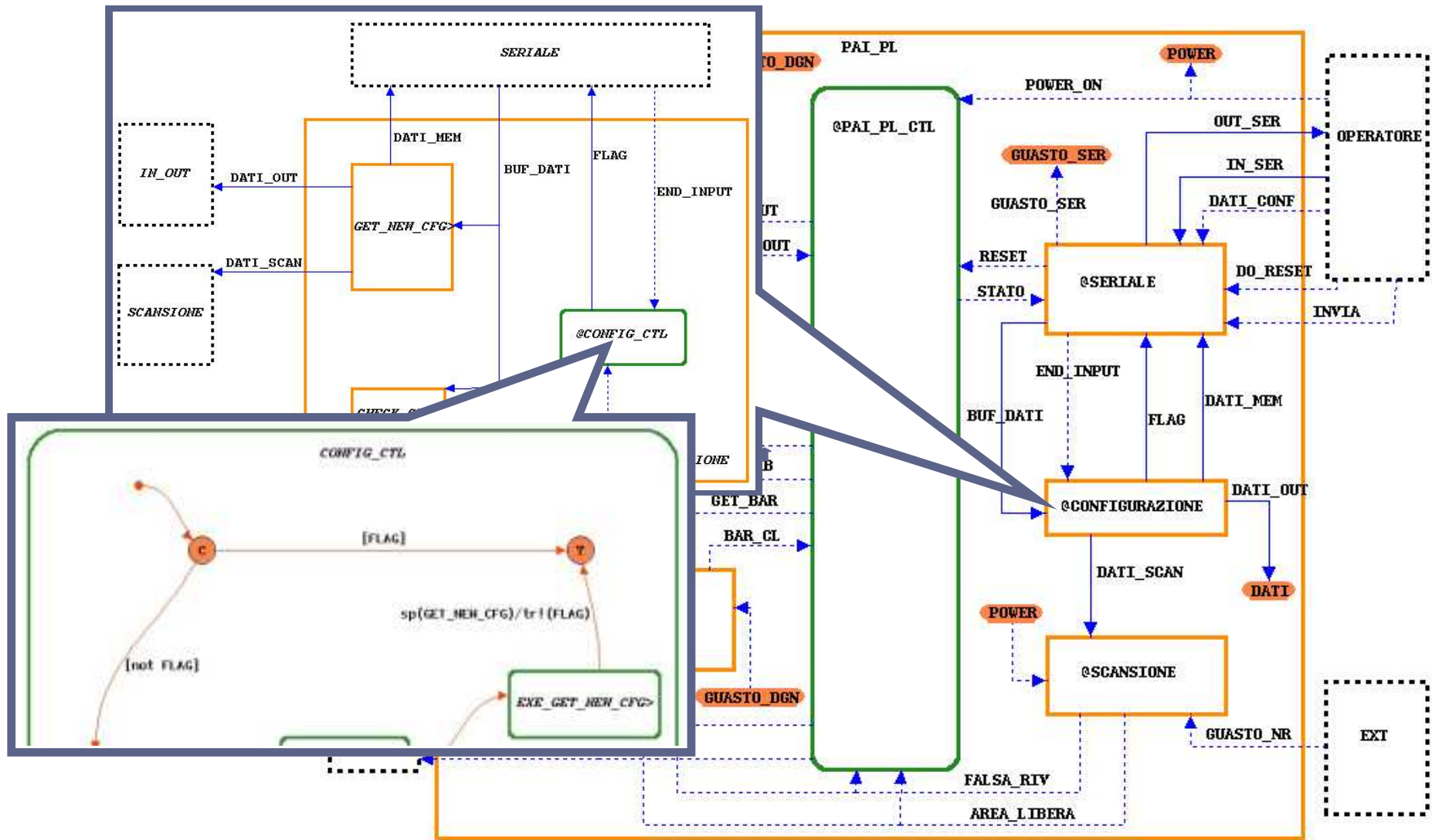


The system model 1/2

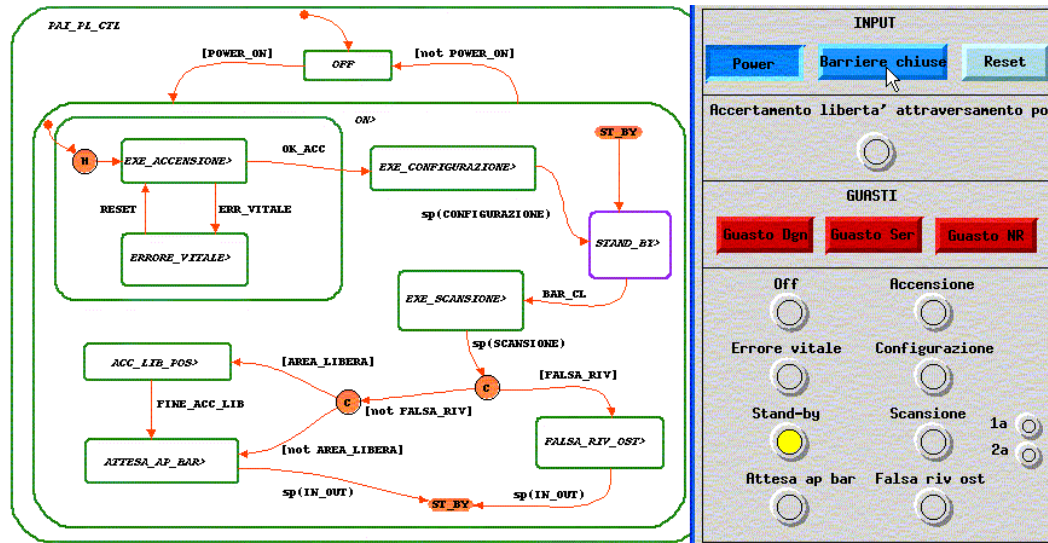
Some pictures of the Statestate model created from the SRS.



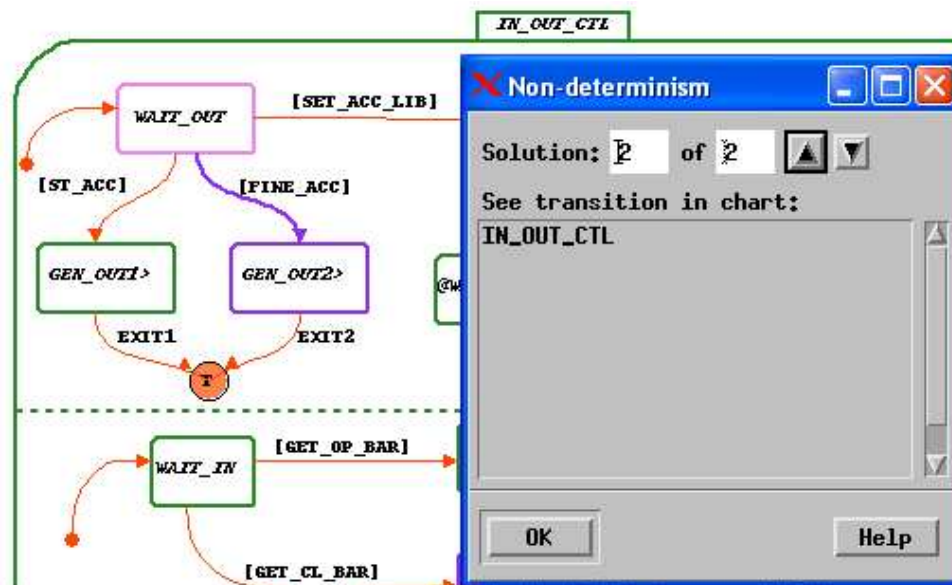
The system model 2/2



Model Verification



Model simulation with a customizable interactive panel (input selection – output observation).



Model analysis (Model Checker) – Example of a non-determinism found.

Results of the analysis

The building up of the model revealed misses in the original Customer's SRS about:

- ❑ incompleteness (lacks in the description of system's behaviour in some scenarios);
- ❑ behaviours not too clear (sometimes system's behaviour is not described clearly);
- ❑ contradictions (there was one contradiction about the definition of the "scanning time").

As example: the description of system's behaviour in case of a failure was obscure and spread in many requirements.



The SRS document was ambiguous because it's written in natural language and can hide mistakes.

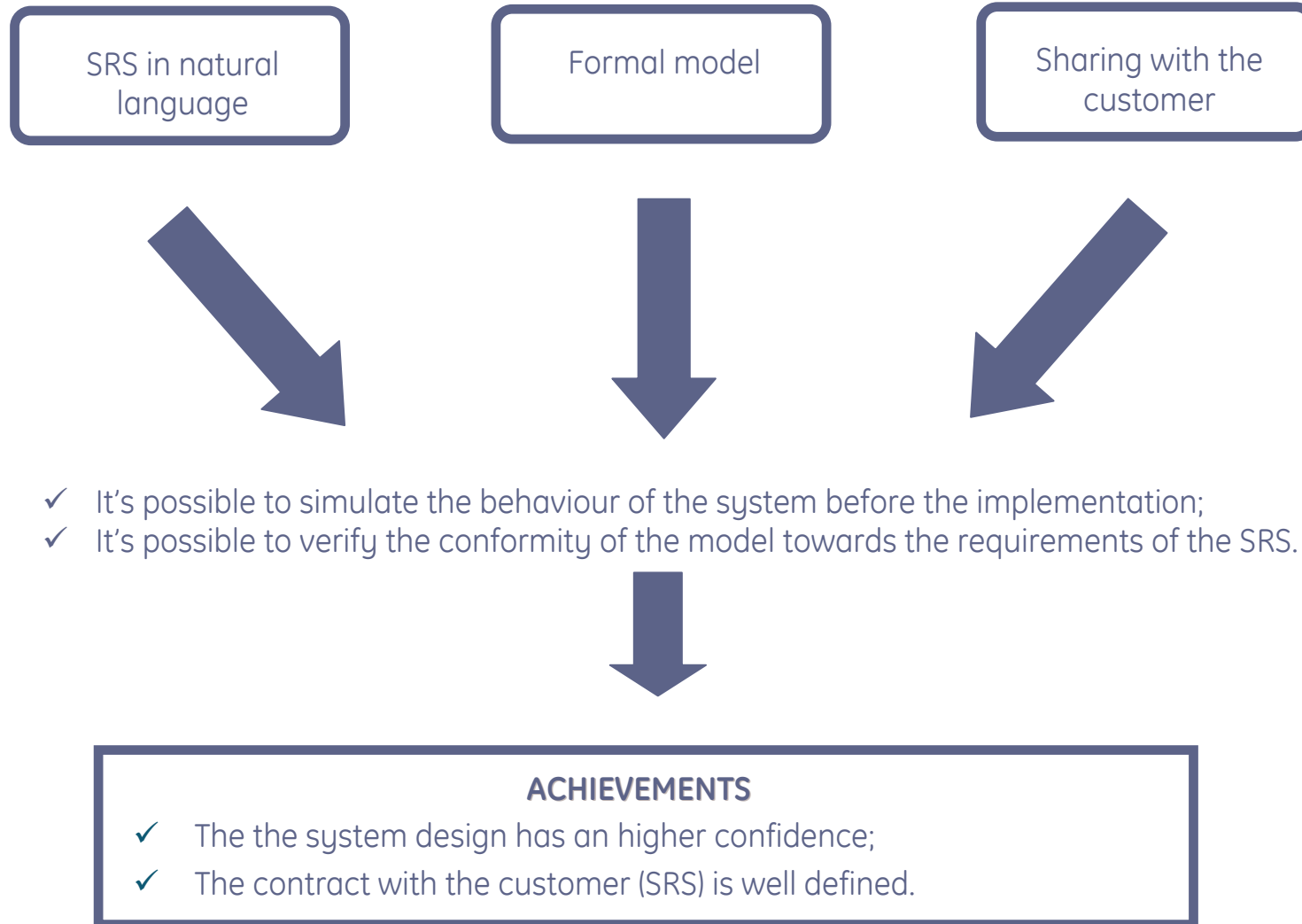
VS.

The StateMate model is not ambiguous thanks its mathematical language.

Therefore the thesis revealed that it's very important to share the model with the customer to fix all aspects of the system before starting the design.

During the real system design all misses were actually solved during design, V&V activities and meeting with the customer. Nevertheless, the work was important to show and understand the benefits in term of early clarification and costs saving with the introduction of FM in a former stage of the life cycle

Advantages of Formal Methods

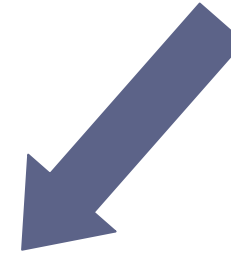
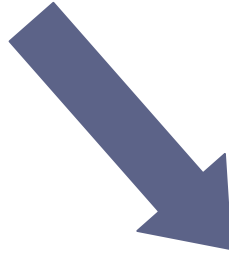


A global specification

Available specifications

Benchmarking

Domain experts

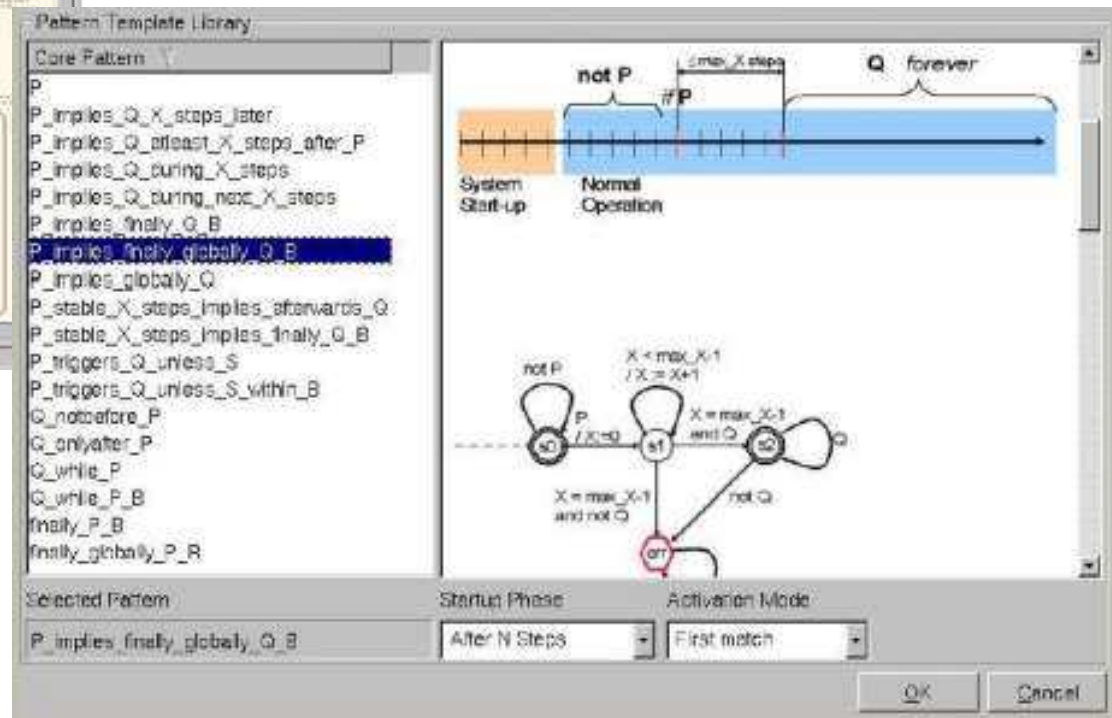
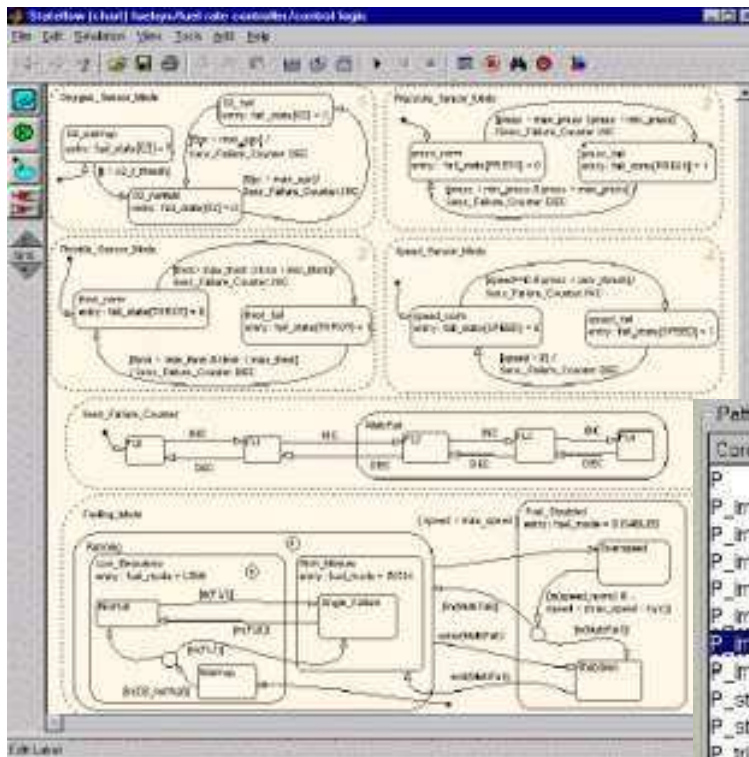


FORMAL MODEL OF THE SYSTEM

- ✓ The system design would have a higher confidence;
- ✓ Would be possible to simulate the behaviour of the system before the implementation;
- ✓ Would be possible to verify the conformity of the model towards the requirements of the known SRS and future ones;

A journey into FMs 2/2

Matlab -
Stateflow



Advantages of Modelling

Formal Methods are the application of discrete mathematics to system & software engineering involving modelling and analysis with an underlying mathematically precise notation.

A notation is formal if:

- comes with a formal set of rules which defines its syntax and its semantics;
- the rules can be used to analyze expressions to determine if they are syntactically well-formed or to prove properties about them.

Formalizing requirements helps to:

- remove ambiguity and improve precision;
- allows us to reason about the requirements and provides a basis for verification.
- allows us to animate/execute the requirements.

Modelling can:

- guide elicitation;
- provide a measure of progress;
- help to uncover problems;
- help us check our understanding.

Model Verification includes:

- consistency analysis and type checking;
- validation;
- verifying design refinement.

Model Checking:

- emphasis on partial verification of partial models;
- engineering view – checks whether properties hold.

Strength of FM

FM helps to design the Requirements Specification together with the Customer. Simulation and Animation are vital to show the Customer the advancement of the modelling and to receive a formal approval.

FM are well suited for Railways Signalling to create models (i.e. Interlocking systems).

Model Checking is a technology that can be applied to partial models to prove the correctness. Can be used together with other process methodologies to reach enough confidence on the set of requirements.

FM can be applied at least twice during the life cycle: at system specification level and at software architecture level. They can be used to build also a System and Software Test Specification that can be used after to validate the real system designed.

Conclusions



imagination at work

RE Conclusions

Requirements are one of the most important things in projects because they are important through all life cycle.

System's Verification & Validation and Homologation are all activities that deal with requirements.

Requirements are equally important for design and for sales teams, for supply and for production team. Customer and Management agree upon requirements because every contract is based upon a specification.

Requirements management *it's* the process itself, because the activities required to design a safety critical system deal with requirement specification, flowdown and satisfaction.

Safety systems put great care in requirements specification because requirements are the main cause of systems' failures.

Software itself can be viewed as a requirement management process, nowadays tools allow to design a formal specification and automatically generate the code.

References

CENELEC standards: EN 50126 - EN 50128 - EN 50129

<http://www.cenelec.org/Cenelec/Homepage.htm>

Safety Critical Systems Server

<http://archive.comlab.ox.ac.uk/safety.html>

Formal Methods Server

<http://vl.fmnet.info/>

University of York – Safety Critical System Mailing List

safety-critical@cs.york.ac.uk

NASA LaRC- Langley Formal Methods Site

<http://shemesh.larc.nasa.gov/fm/fm-what.html>

NASA SATC – Software Assurance Technology Center

<http://satc.gsfc.nasa.gov/tools/arm/>

MIT Opencourseware

<http://ocw.mit.edu/OcwWeb/Aeronautics-and-Astronautics/index.htm>

<http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/index.htm>

Nancy Leveson

<http://sunnyday.mit.edu/>

Steve Easterbrooks

<http://www.cs.toronto.edu/~sme/>

carlo.becheri@trans.ge.com

