 THE RESEARCH LEADING TO THESE RESULTS HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S SEVENTH FRAMEWORK PROGRAM (FP7/2007-2013) FOR CRYSTAL – CRITICAL SYSTEM ENGINEERING ACCELERATION JOINT UNDERTAKING UNDER GRANT AGREEMENT N° 332830 AND FROM SPECIFIC NATIONAL PROGRAMS AND / OR FUNDING AUTHORITIES.

CRitical S**YST**em Engineering **A**cce**L**eration

IOS needs for RTP specification

D503.020

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	IOS needs for RTP specification
Deliverable No.	D503.020
Dissemination Level	CO
Nature	R
Document Version	V1.01
Date	2013-12-30
Contact	Pascal POISSON
Organization	ALSTOM
Phone	
E-Mail	pascal.poisson@transport.alstom.com

AUTHORS TABLE

Name	Company	E-Mail
Vidal Delmas TCHAPET NYA	ALSTOM	vidal-delmas.tchapet-nya-ext@transport.alstom.com

REVIEW TABLE

Version	Date	Reviewer
Internal Review	2013-12-02	Pascal POISSON
Internal Review	2013-12-02	Elie Soubiran
Internal Review	2013-12-02	Fateh GUENAB
External Review	2013-12-20	Frédérique VALLÉE
External Review	2013-12-20	Alexandre GINISTY

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected

CONTENT

Content of Figures

Content of Tables

1 Introduction

1.1 Role of deliverable

The aim of this document is to provide interoperability needs for RTP specification. Interoperability is the ability of two or more systems or components to exchange information and use the information that has been exchanged to do useful work [BSIE2013]. Our IOS needs take into account railway system components, ALSTOM TRANSPORT system life cycle process, software tools used in the use case 5.3 and stakeholders involved in the process.

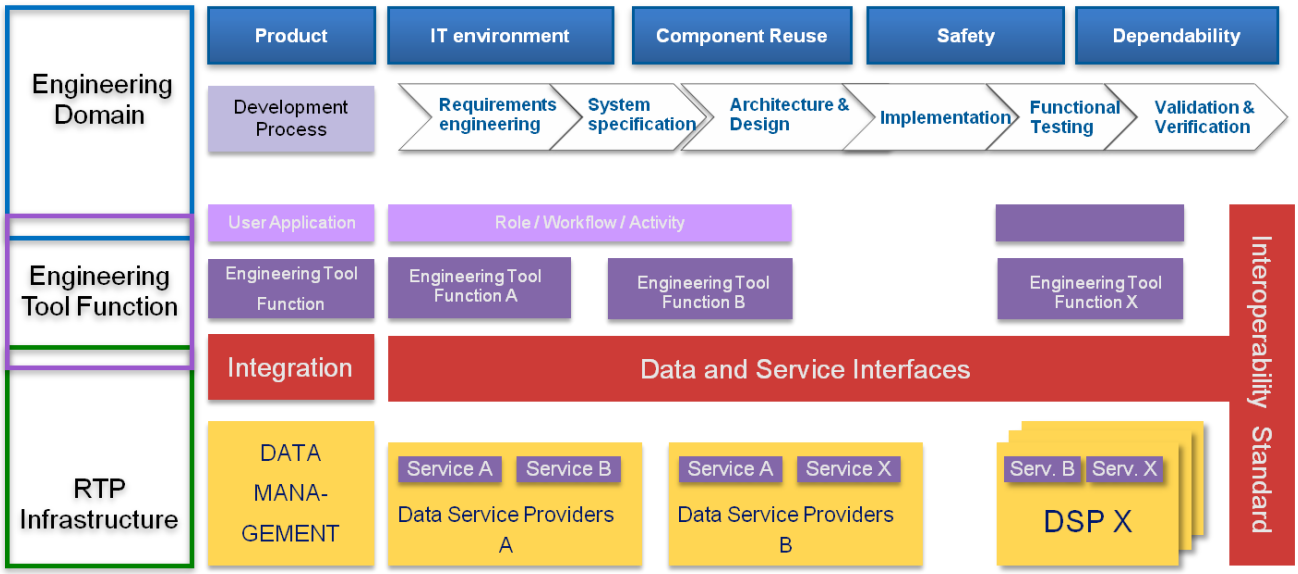
1.2 Structure of this document

This document is organized as follows:

- Chapter 2 gives an overview of CRYSTAL RTP implementation strategy
- Chapter 3 focuses on the IOS needs for RTP specification
- Chapter 4 Terms, Abbreviations and Definitions
- Chapter 5 References
- Chapter 6 Annex

2 RTP implementation strategy

Figure 2-1 gives an illustration of RTP implementation strategy and vision to achieve a common reference technology platform. RTP implementation strategy includes engineering domain, engineering tool function and RTP infrastructure.



2-1 RTP implementation strategy

The scope of the study is limited to engineering phase and associated engineering tool functions. We are going to identify IOS needs for RTP specification, based on the concepts such as:

- ALSTOM TRANSPORT engineering life cycle process
- Systems and subsystems that compose the railway systems
- Functions and sub functions that perform missions
- Requirements change management
- System design process
- Safety analysis process
- Tools used to perform global process
- Stakeholders involved in the global process such as requirements engineer, system engineer, safety engineer.

The strategy above is the one that must be adopted in order to implement IOS needs for RTP. In the next paragraphs, we are going identify these needs. IOS needs depend on traceability between all the system artefacts, across all life cycle stages. So, the system analysis and the safety analysis require a great attention in order to identify the IOS needs for RTP specification.

3 IOS needs

This chapter gives the IOS needs for RTP specification in the railway domain. We intend to establish traceability links between products involved in the global Engineering life cycle process. Traceability is the degree to which a relationship can be established between two or more products of a development process, especially those having a predecessor/successor or master/subordinate relationship to one another [CENELEC]. We require traceability in order to trace back any aspect of the system to its source requirements. Section 3.1 describes interoperability between system and subsystem; section 3.2 describes interoperability between engineering processes, section 3.3 describes interoperability between tools used in the global process, and section 3.4 describes interoperability between stakeholders as end users.

3.1 System paradigm

Safety analysis requires system components. As depicted below, a system is the combination of subsystems interconnected to accomplish system objectives. System functions define the way a system performs.

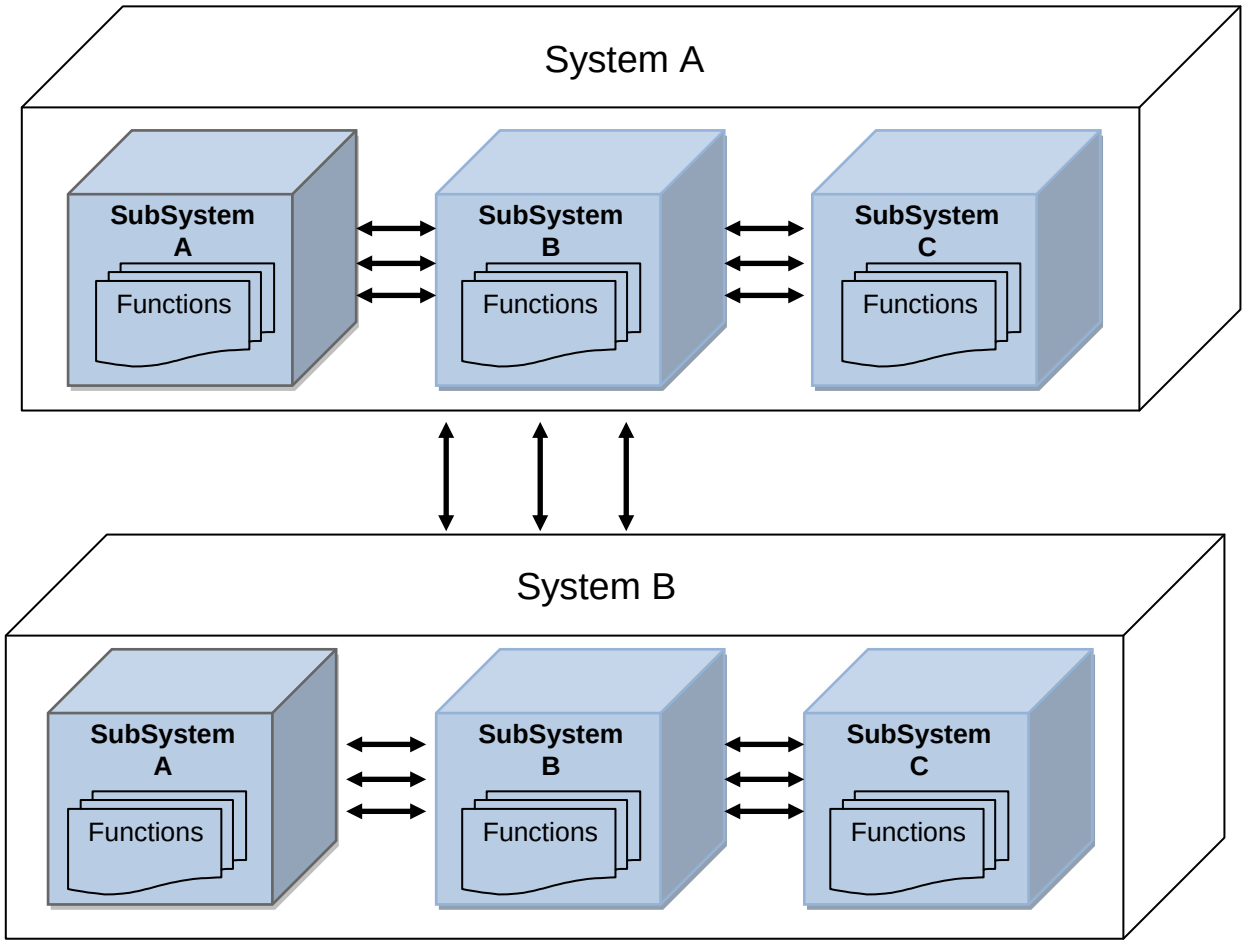


Figure 3-1 Generic system and interoperability needs

Interoperability can be identified at several levels. We can observe data exchanged between system, subsystem, function and sub function. Arrows illustrate the communication between Subsystems. Safety analysis takes into account the failure of some system attributes:

- Hardware: Failure modes
- Software: Design errors and design incompatibility
- Function: Erroneous outputs and inputs of the functions.

Safety engineer must address these system attributes in order to perform safety analysis. So, it should be a good idea to interoperate software, hardware and functions. We can extend interoperability between the system functions that fulfil the system needs.

3.1.1 Interoperability between systems' functions

The system functions have inputs and outputs. Safety analysis requires system's functions, their inputs and their outputs. It is a good idea to guarantee data exchange between functions and the sub functions. Therefore, we ease interoperability among functions. The challenge is to combine the software components into an overall software system in order to perform system functions. For instance, we can allow interoperability between automatic train operation, automatic train protection and their sub functions, such as compute positive train detection and characteristics , supervise train movement , Authorize and assist train operation , compute train precise location and speed, compute the run profile , drive the train , and so on. The communication among these functions contributes to ensure the safe running of trains.

After understanding the systems, the subsystems, the functions and sub functions, we can apply process from requirements analysis to safety analysis and identify IOS needs in the global process.

3.2 Global process

Figure 3-2 depicts ALSTOM TRANSPORT global process. The process includes requirements engineering process, system engineering process, and safety analysis process. We also represent stakeholders involved in the process and the role allocated to each of them. The process requires engineering tools such as IBM DOORS, Papyrus, Safety Architect tool, the configuration management tool and the change management tool. The interoperability needs must be defined from the requirements identified during the global process. Interoperability shall particularly address:

- Traceability between system design requirements
- Traceability between System design methods
- Traceability between Safety analysis methods
- Traceability between system design requirements and operational analysis design
- Traceability between system design requirements and functional analysis design
- Traceability between system design requirements and constructional analysis design
- Traceability between safety design requirements and Preliminary Hazard Analysis
- Traceability between safety design requirements and System Hazard Analysis
- Traceability between safety design requirements and Sub System Hazard Analysis
- Traceability between each function and its failure mode
- Traceability between requirements and stakeholders
- Traceability between system analysis and safety analysis
- Traceability between specification documents

- Traceability between safety design requirements and the failure modes identified.
- Traceability between safety design requirements and test requirements.
- Traceability between safety design requirements and test results.

Traceability requires configuration management in order to control changes throughout the system life cycle.

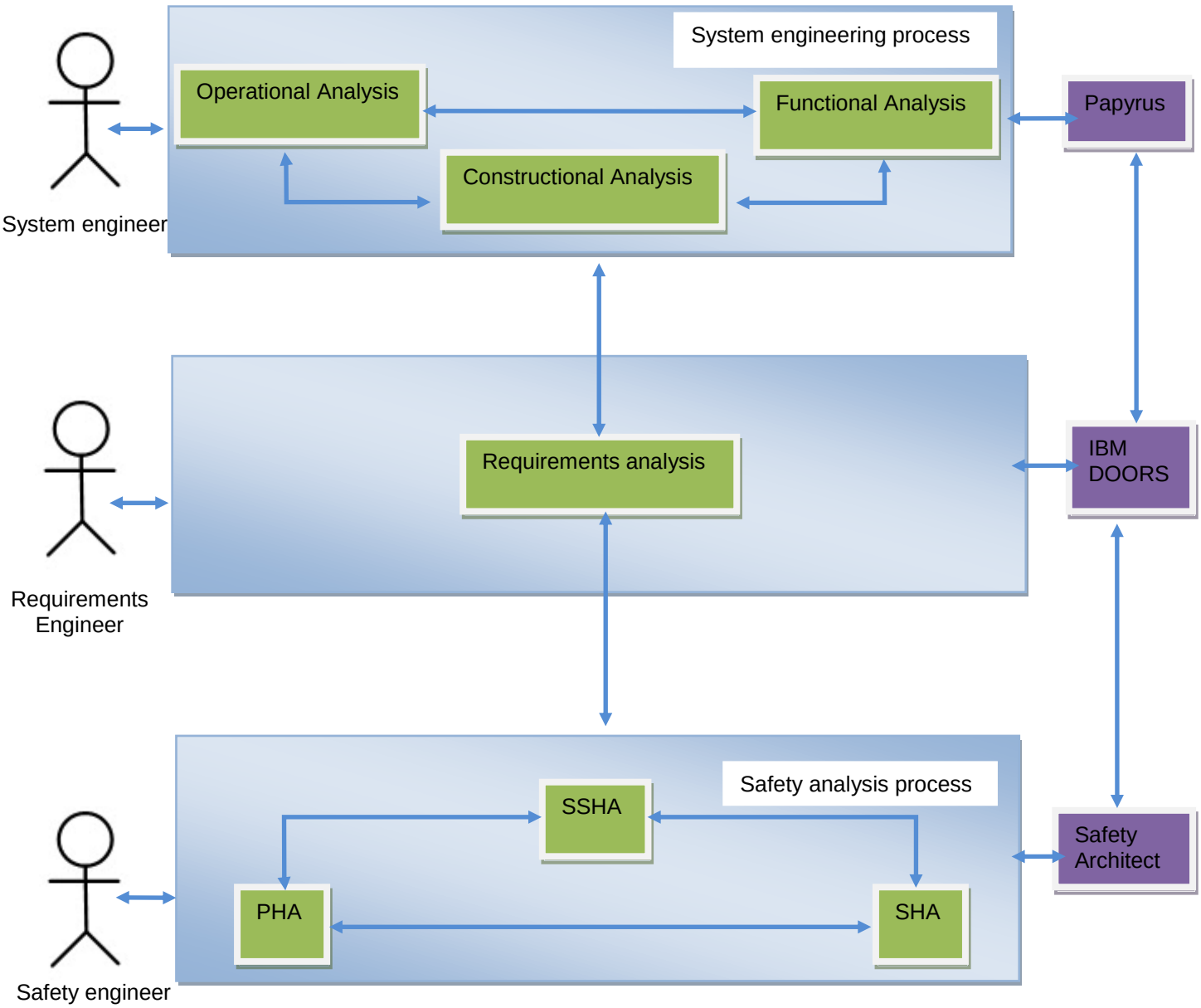


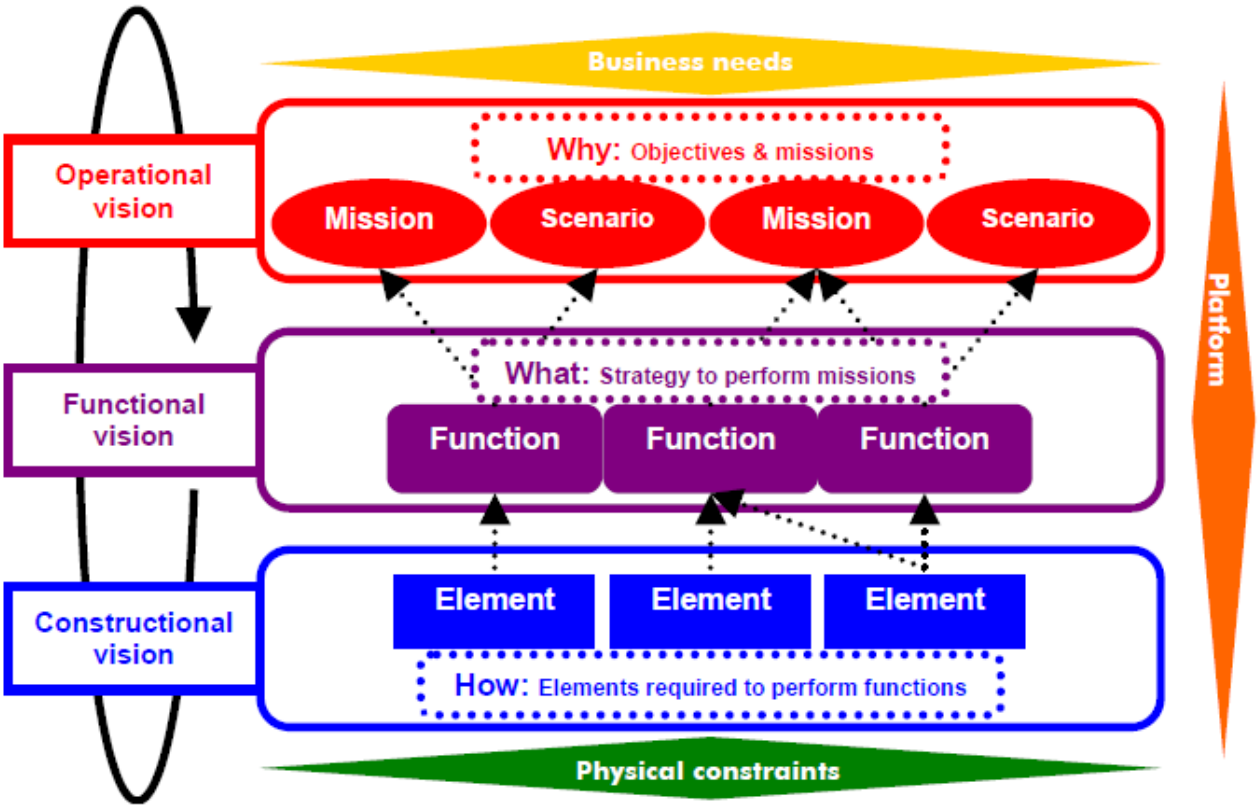
Figure 3-2 System life cycle process including IOS needs, the stakeholders and tools

Arrows illustrate interoperability needs that should be developed in the next paragraphs. Each process enhancement has impacts on others processes. IOS challenge is to establish the traceability relationships in order to capture dependencies between processes.

3.2.1.1 System specification and design

System analysis requires traceability to trace back design of Functional Analysis to design of Operation Analysis and design of Constructional Analysis to design of Operational Analysis. We can extend traceability

between the elements of model at different views. Traceability must be applied in order to ensure the compliance between the three system analysis views. Figure 3-3 depicts system views and the way they interoperate. Data exchange can be observed between operational view, functional view, and constructional view. As we can see, a function performs the assigned missions during the operational stage. At the constructional phase, we require elements to perform functions.



3-3 System view and interoperability

The next paragraphs give an overview of activities allocated to each stakeholder involved at different system analysis level. All stakeholders are considered as tools end users.

3.2.1.1.1 Stakeholders and activities

The stakeholder in charge of system analysis is the System Engineer. The main activities are shown in different views; such as produce operational views, functional views, and constructional views. System design requires the modelling tool called Papyrus.

3.2.1.1.2 Operational view

System Engineer activities during operational view are shown as follows:

- Identifying actors and external systems that interact with the system studied,
- Defining use cases which specify the system' missions that may yield to an observable result for one or more actors or other stakeholders of the system,

- Defining contexts which specify the environment states in which the system will operate. At this level, the interfaces between the system and the environment (actors) will be exhibited,
- Defining scenarios which describe the sequences of exchanges between the system and its environment in order to perform a use case in a specific context,
- Defining operational data models which refer to the operational information exchanged between the actors and the system within all scenarios,
- Defining requirements which describe the initial customer needs.

3.2.1.1.3 Functional view

In this view, the System Engineer activities are defined as follows:

- Defining functions which refer to what must be performed to achieve a desired mission,
- Defining processes which refer to the sequence of functions used to perform a function of higher level,
- Identifying functional data models which refer to the functional information manipulated/transformed by the functions of the system,
- Identifying requirements which must be satisfied by model elements defined at that level.

3.2.1.1.4 Constructional view

In this view, the system Engineer activities are defined as follows:

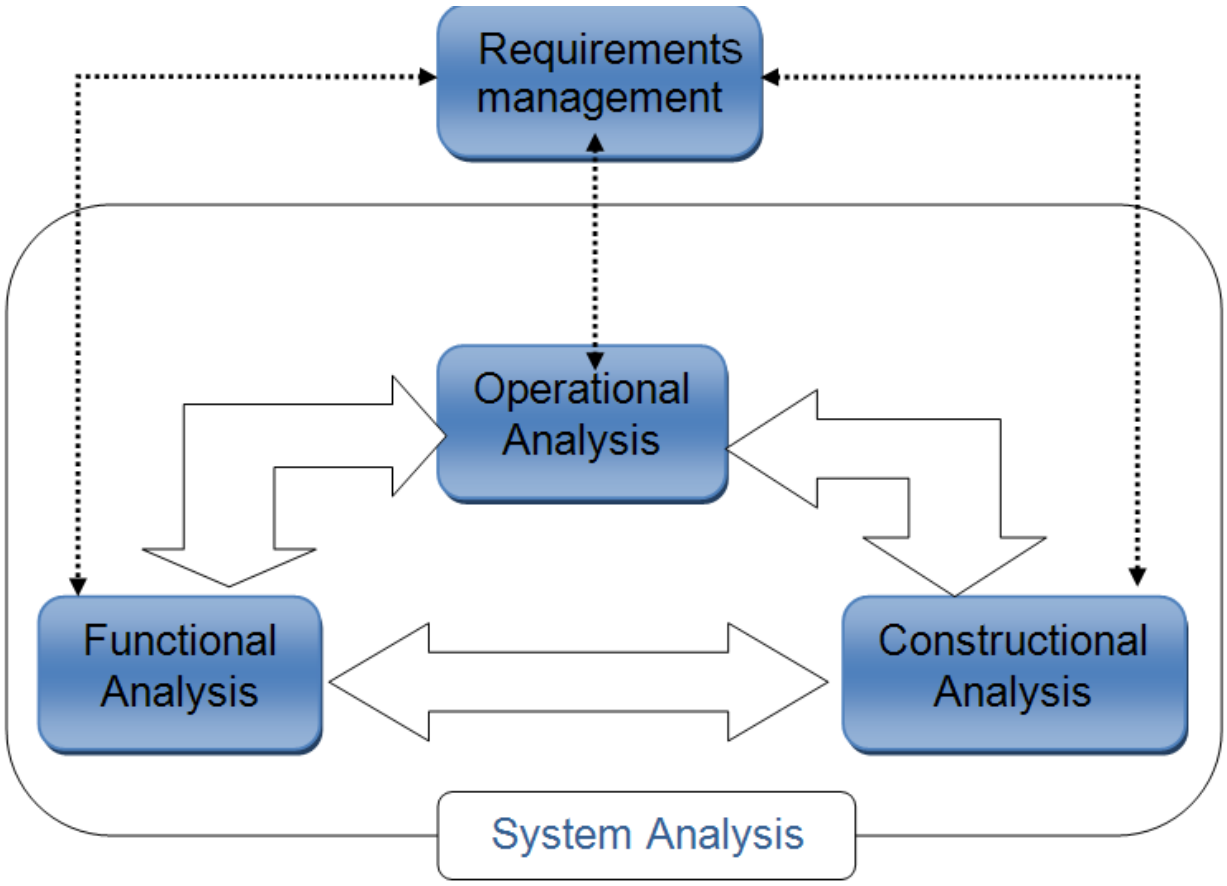
- Defining the elements which refer to a given system, sub-system, module or part without any distinction,
- Defining the flow ports which specify an interaction point between an element and its environment or between internal system elements. A flow specification which details data exchanged (name, type, direction, format) will be used at this level to type each flow port,
- Defining the interfaces which specify a contract between two or more flow ports,
- Defining the constructional data models which refer to the concrete information really manipulated/transformed by the system in practice,
- Defining the requirements (initial or derived requirements) which must be satisfied by model elements defined at this level.

3.2.1.1.5 Interoperability needs

In term of interoperability, we must ensure data exchange between operational view, functional view and constructional view. It is necessary to establish traceability relationships in order to check consistency and compliance between all the views of model. We must establish traceability links between mission and functions, and between elements and functions.

Interoperability can also be seen in term of requirements allocation during modelling process. The requirements allocation modelling process deals with the relationships between the requirements process and the design modelling process. This process results from requirements traceability view.

We will model relationships between requirements and the three main system views. In fact, requirements view will be used to trace on which modelling objects is allocated each requirement. That is why, for each modelling specification and design, we must define a requirement traceability view which models the mapping between requirements and SysML modelling objects. Figure 3-4 illustrates traceability relationships between requirements management and design modelling process. It illustrates the way design modelling process is linked to the requirements management process.



3-4 Relations between the requirements management process and design modelling process

The requirements management process encompasses three sub-processes such as:

- Requirements capture modelling process: This process consists in identifying and capturing the customer needs and constraints stated as a set of requirements. When they are not sufficiently precise and clear, requirements must be discussed, clarified and rewritten resulting in a new set of requirements (derived requirements).

- Requirements allocation modelling process: This process deals with the relationships between the requirement development process and the specification and design modelling process. Customer needs are stated as a set of requirements. These requirements are then clarified and new requirements (called derived requirements) are consequently transformed during the specification and design step, which must be mapped with operational, functional and constructional specifications and designs.

- Requirements validation modelling process: This process is to identify how each requirement is verified. Requirement may be verified through different methods (tests - the process will then describe how test cases can be represented in SysML - inspection, demonstration, analysis – in these cases a reference must be made to documents describing the verification method).

3.2.1.2 Safety analysis process

During this process, we intend to establish traceability relationships between safety design requirements and the failure modes identified. The process requires traceability matrix of all safety design requirements to test requirements and test results. From the traceability relationships we derive the IOS needs for RTP. The main actor in charge of safety analysis is the Safety Engineer. The Safety analysis requires the Safety Architect tool from All4Tec partner. ALSTOM TRANSPORT Safety analysis process encompasses Preliminary Hazard Analysis, System Hazard Analysis and Subsystem Hazard Analysis. An overview of each Hazard Analysis is given in the next paragraphs.

3.2.1.2.1 Preliminary Hazard Analysis

Preliminary Hazard Analysis (PHA) is performed in order to identify hazards and their associated failure cause and failure effects. The PHA includes the measurement of risk level of each hazard.

3.2.1.2.1.1 Activities

Table 3-1 illustrates Preliminary Hazard Analysis scenario. The table includes the goal of the Preliminary Hazard Analysis. As shown in Table 3-1 , to perform the Preliminary Hazard Analysis we require some inputs data such as Safety Plan, System User needs, Hazards list and operational context. Outputs from The Preliminary Hazard Analysis include Accident Scenario Model, Preliminary Hazard Analysis report. The Preliminary Hazard Analysis document is an Excel sheet where we report the potential Hazards, the ID to identify each Hazard and avoid confusion, the Hazard cause, the safety design requirements to mitigate or eliminate Hazards, the person in charge of requirement, the accident gravity, the train operation mode, the requirements revisions, and so on.

GOAL	Identify and estimate the criticality of the potential hazards faced by the system on the basis of a typical list of accidents, Evaluate the risks that these hazards occur. And define the high level requirements/barriers to be applied with the design in order to cover the identified hazards.
INPUTS	Safety Plan System User Needs (Imported requirements from Requirements Management Tool (RMT)) Hazards Breakdown Structure (HBS): list of accidents and hazards. Operational Context (OC)
OUTPUTS	Accidents Scenarios Model (ASM) PHA document Optional: HBS, OC
RESPONSIBILITY	SAM (Safety Assurance Manager) / Safety Assurance Engineer (SAE)
STEPS	The Safety Engineer will:

	Step 1	Import Requirements from Requirements Management Tool (RMT)
	Step 2	Import accidents and hazards list (HBS) and operational context list (from database)
	Step 3	Identify potential accidents and their associated hazards situations on the basis of HBS and OC lists.
	Step 4	Evaluate risks in terms of severity (S), and tolerable frequencies (TAR) of accidents. Quantitative values table is used (Categories of S and TAR are considered).
	Step 5	Identify or create the necessary protections (barriers) to eliminate or mitigate identified risks.
	Step 6	Allocate Tolerable Hazard Rate (THR) to each Hazardous situation basing on corresponding severity (S) and tolerable frequencies (TAR) of accidents and taking into account “Risk Reduction Factors (RRF)” of barriers and OC.
	Step 7	- Identify and export new system safety-related requirements to RMT - Identify existing requirements that have become safety requirements
	Step 8	Record hazards in the System Hazard Log
	Step 9	Enrich HBS & OC databases
	Step 10	Commit ASM in Configuration Management Tool (CMT)

Table 3-1 Preliminary Hazard Analysis Scenario

3.2.1.2.1.2 PHA Interoperability needs

When performing the Preliminary Hazard Analysis, the Safety Engineer takes into account the System design, the Hazard Breakdown Structure, and the system design tools. In term of interoperability needs, these factors must be interoperable in order to ease data exchange, to improve the Preliminary Hazard Analysis and to generate the Preliminary Hazard Analysis Report.

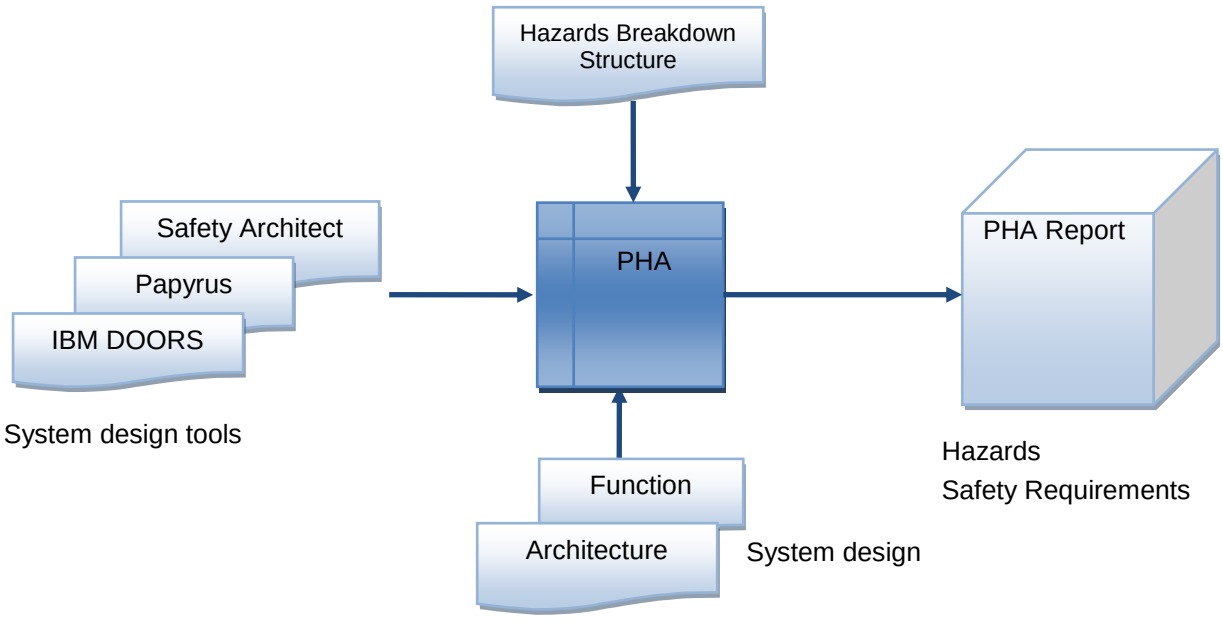


Figure 3-5 Interoperability at PHA level

In term of interoperability needs, the following information is required:

- Traceability Relationships between the safety requirements and the systems
- Traceability Relationships between potential accidents and hazards identified
- Traceability Relationships between the safety requirements and the potential hazards identified
- Traceability Relationships between the safety requirements and the system requirements in order to update and improve system requirements
- Traceability matrix of all potential Hazards to Hazard causes

3.2.1.2.2 System hazard analysis

The purpose of System Hazard Analysis (SHA) is to evaluate risk and safety compliance at the system level. SHA takes into account design errors, hardware failures, human errors, software errors and so on.

3.2.1.2.2.1 Activity

Table 3-2 illustrates System Hazard Analysis scenario. The table includes the goal of the System Hazard Analysis. As shown in Table 3-2, to perform the System Hazard Analysis we require some inputs data such as Accidents Scenarios Model, System Functional Specification, and Preliminary Hazard Analysis. Outputs from The System Hazard Analysis include the System Dysfunctional Model and the System Hazard Analysis report. The System Hazard Analysis document is also an Excel sheet where we store the system functions, the ID to identify functions, the failure mode, the failure cause, the failure effects, the potential accidents, the Risk Reduction Factor (RRF) to reduce the probability of accident occurring, the safety design requirements to mitigate or eliminate Hazards, the person in charge of requirement, the requirements revisions, the traceability links between requirements, the train operation mode, The Safety Integrity Level (SIL) allocated to each function, The tolerable Hazard Rate (THR), and so on.

GOAL	Analyse the causes of unsafe situations of the system related with its functions. And define the actions that eliminate, or reduce risks to an acceptable level.	
INPUTS	Accidents Scenarios Model (ASM) System Functional Specification (FBS) Preliminary Hazard Analysis (PHA)	
OUTPUTS	System Dysfunctional Model (SDM) System Hazard Analysis document (SHA)	
RESPONSIBILITY	SAM (Safety Assurance Manager) / Safety Assurance Engineer (SAE)	
STEPS	The Safety Engineer will:	
	Step 1	Import functions from System Functional Breakdown Specification (FBS).
	Step 2	For each imported function and using Failure Modes and Effects Analysis (FMEA): ○ Identify all failures modes (of each function) leading to potential hazards. ○ Identify the causes of each failure mode. ○ Determine the effects (system effects) of each failure mode.
	Step 3	Trace failure modes to identified accidents in “Accidents Scenarios Model”.
	Step 4	Identify, if necessary, barriers (countering the cause) and safety requirements against hazardous situations (for associated function which is source of cause).

	Step 5	Allocate SIL to functions which are sources of causes leading to accidents. This is performed using a correspondence table (THR<->SIL) taking into account the “Inefficiency Factors (IF)” of barriers.
	Step 6	- Identify and export new functional safety-related requirements to RMT - Identify existing system requirements that have become safety requirements
	Step 7	Identify the necessary sub-system hazard analysis, specific hazard analysis and interface hazard analysis and record this information in the system hazard log.
	Step 8	Record hazards in the System Hazard Log.
	Step 9	Commit SDM
	Step Change Request	When FBS changes, perform impact analysis and update consequently SDM

Table 3-2 System Hazard Analysis Scenario

3.2.1.2.2.2 SHA Interoperability needs

When performing the System Hazard Analysis, the Safety Engineer takes into account the System Detailed design, the Hazard Breakdown Structure, the Preliminary Hazard Analysis and the system design tools. These artefacts must be interoperable in order to ease data exchange, to improve the System Hazard Analysis and to generate the System Hazard Analysis Report.

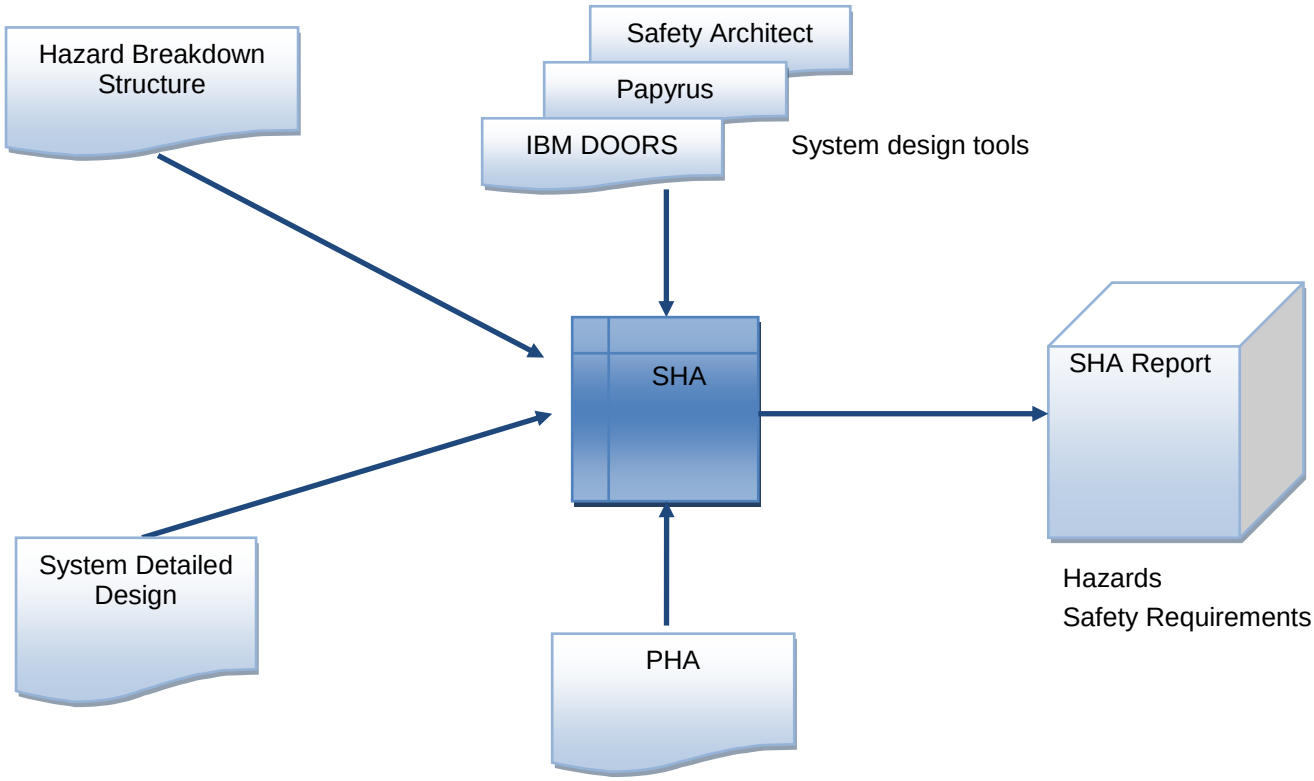


Figure 3-6 Interoperability at SHA level

In term of interoperability needs, the following information is required:

- Traceability Relationships between the safety requirements and the systems
- Traceability Relationships between the system functions and the failure modes
- Traceability Relationships between the safety requirements and the failure modes identified
- Traceability Relationships between the safety requirements and the system requirements in order to update and improve system requirements
- Traceability matrix of all failure modes to failure causes and failure effects

3.2.1.2.3 Sub System Hazard Analysis

The purpose of Sub-System Hazard Analysis (SSHA) is to analyse the causes of failures of sub-systems, and to define the means to eliminate or reduce to an acceptable level the risks. This activity is performed when detailed design information is available.

3.2.1.2.3.1 Activities

Table 3-3 illustrates Sub-System Hazard Analysis scenario. The table includes the goal of the Sub-System Hazard Analysis. As shown in Table 3-3, to perform the Sub-System Hazard Analysis, we require some inputs artefacts such as System Dysfunctional Model, Sub-System Functional Specification, and System Hazard Analysis. Outputs from The Sub-System Hazard Analysis include the Sub-System Dysfunctional Model and the Sub-System Hazard Analysis report. The Sub-System Hazard Analysis document is also an Excel sheet where we store the Sub-System functions, the ID to identify each function, the failure modes, the failure causes, the failure effects, the potential accidents, the Risk Reduction Factor (RRF) to reduce the probability of an accident occurring, the safety design requirements to mitigate or eliminate Hazards, the person in charge of requirements, the requirements revisions, the traceability links between requirements, the train operation mode, The Safety Integrity Level (SIL) allocated to each function, The tolerable Hazard Rate (THR), and so on.

GOAL	Analyse the causes of failures of sub-systems, and define the means to eliminate or reduce to an acceptable level the risks.	
INPUTS	System Dysfunctional Model (SDM) Sub-System Functional Specification (FBS) System Hazard Analysis	
OUTPUTS	Sub-System Dysfunctional Model (SSDM) Sub-System Hazard Analysis document (SSHA)	
RESPONSIBILITY	SAM (Safety Assurance Manager) / Safety Assurance Engineer (SAE)	
STEPS	The Safety Engineer will:	
	Step 1	Import functions from Sub-System Functional Breakdown Specification (FBS).
	Step 2	For each sub-function, by using Failure Mode and Effects Analysis (FMEA): ○ Identify all failures modes leading to potential hazards. ○ Identify the causes of each failure mode. ○ Determine the effects (local & system effects) of each failure mode.
	Step 3	Trace failure modes (of sub-functions) to identified causes (functions) in “System Dysfunctional Model” leading to accidents.

	Step 4	Identify, if necessary, barriers (countering the cause) and safety requirements against hazardous situations (for associated sub-function which is source of cause).
	Step 5	Allocate SIL to sub-functions which are sources of causes of the identified causes (functions) in “System Dysfunctional Model” leading to accidents.
	Step 6	- Identify and export new functional safety-related requirements to RMT - Identify existing system requirements that have become safety requirements
	Step 7	Identify the necessary components hazard analysis, specific hazard analysis and interface hazard analysis and record this information in the Sub-System Hazard Log
	Step 8	Record hazards in the Sub-System Hazard Log.
	Step 9	Commit SSDM
	Step 10	When FBS changes, perform impact analysis and update consequently SSDM

Table 3-3 Sub-System Hazard Analysis scenario

3.2.1.2.3.2 SSHA Interoperability needs

When performing the Sub-System Hazard Analysis, the Safety Engineer takes into account the Sub-System Detailed design, the System Hazard Analysis and the system design tools. These artefacts must also be interoperable in order to ease data exchange, to improve the Sub-System Hazard Analysis and to generate the Sub-System Hazard Analysis Report.

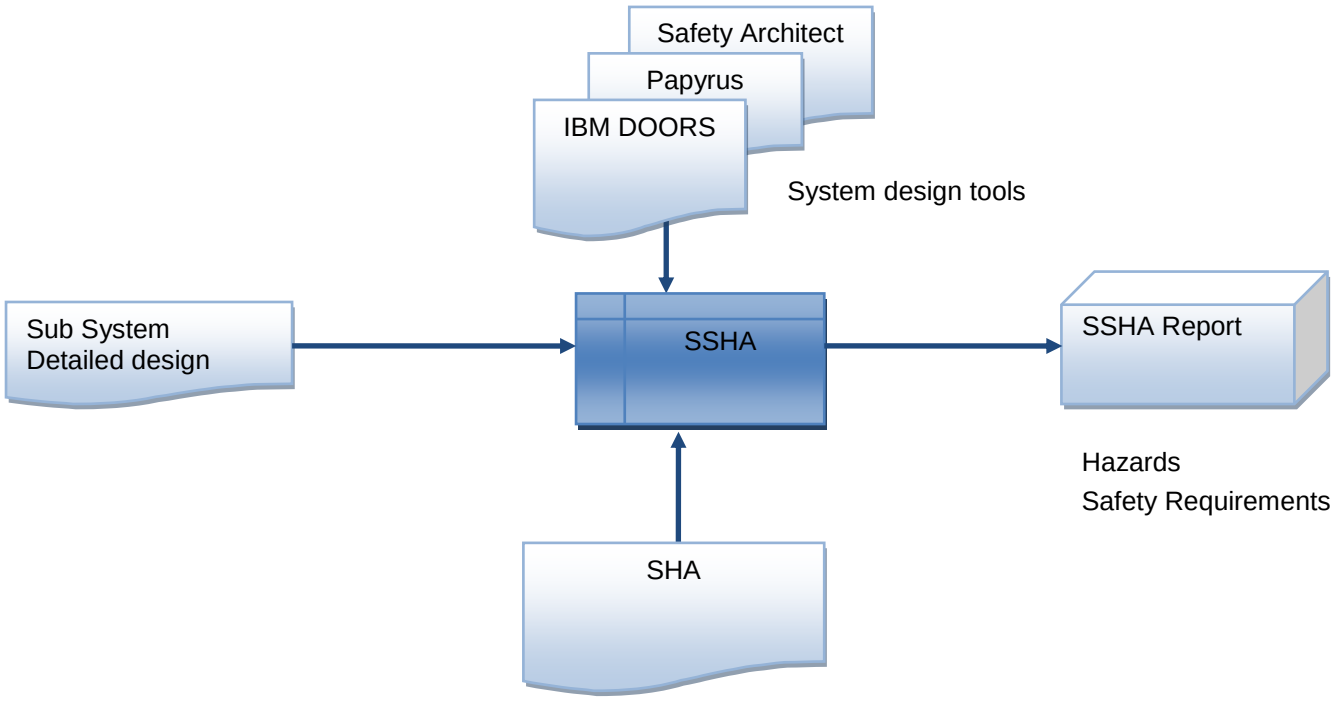


Figure 3-7 Interoperability at SSHA level

In term of interoperability needs, the following information is required:

- Traceability Relationships between the safety requirements and the Sub-Systems
- Traceability Relationships between the Sub-System functions and the failure modes
- Traceability Relationships between the safety requirements and the failure modes identified
- Traceability Relationships between the safety requirements and the system requirements in order to update and improve system requirements
- Traceability matrix of all failure modes to failure causes and failure effects

3.2.1.2.4 Hazard Log

Hazard log is dedicated for analysing safety requirements identified during PHA, SHA and SSHA. Hazard Log records and gives the status of safety requirements. Hazard Log ensures that every safety requirements are successfully validated.

Table 3-4 gives an illustration of the System Hazard Log Scenario. The table includes the goal of the System Hazard Log. As shown in Table 3-4, to perform the System Hazard Log we require some inputs artefacts such as Hazard breakdown structure, System Preliminary Hazard Analysis, System Interface Hazard Analysis, System Requirements Specification, System and sub-system Requirements Tests Plans, System and sub-system Requirements Tests Descriptions, System and sub-system Integration Tests Descriptions, System and sub-system Requirements Tests Reports, Operational and Support Hazard Analysis, System Hazard Analysis, Sub-system Hazard analysis. Outputs from The System Hazard Log Analysis include the System Hazard Log document. The System Hazard Log document is also an Excel sheet where we store all the safety design requirements, all the system design requirements, the test of the requirements, and the test results.

GOAL	The purpose of this activity is to record and give the status of safety requirements
INPUTS	Hazard breakdown structure System Preliminary Hazard Analysis System Interface Hazard Analysis System Requirements Specification System and sub-system Requirements Tests Plans System and sub-system Requirements Tests Descriptions System and sub-system Integration Tests Descriptions System and sub-system Requirements Tests Reports Operational and Support Hazard Analysis System Hazard Analysis Sub-system Hazard analysis
OUTPUTS	System Hazard Log document
DESCRIPTION	Safety Engineer will: ➢ Record for each identified hazard the following attributes: • An identification number, • A complete description, • Its consequences, • Its estimated frequency, • The components it involves,

	• The protections, • The associated actions, • Its status (open, resolved, closed), • The related safety requirements, ➢ Record people involved in safety related activities with their skills; ➢ Record methods, techniques and tools used for analysis; ➢ Record hypothesis used for analysis; ➢ Record known limits of analysis; ➢ Record level of confidence on used data for analysis. ➢ Verify the coverage of safety requirements by tests cases

Table 3-4 System Hazard Log scenario

3.2.1.2.4.1 Hazard Log Interoperability needs

Here we intend to establish a safety requirement matrix. So we interoperate global safety requirements with test requirements, software requirements and design requirements. That is the way to make sure that each hazard has a corresponding safety requirement and each safety requirement has a corresponding design. If a safety requirement isn't taken into account, in design, it cannot be validated. Therefore the hazard associated to that requirement cannot be closed.

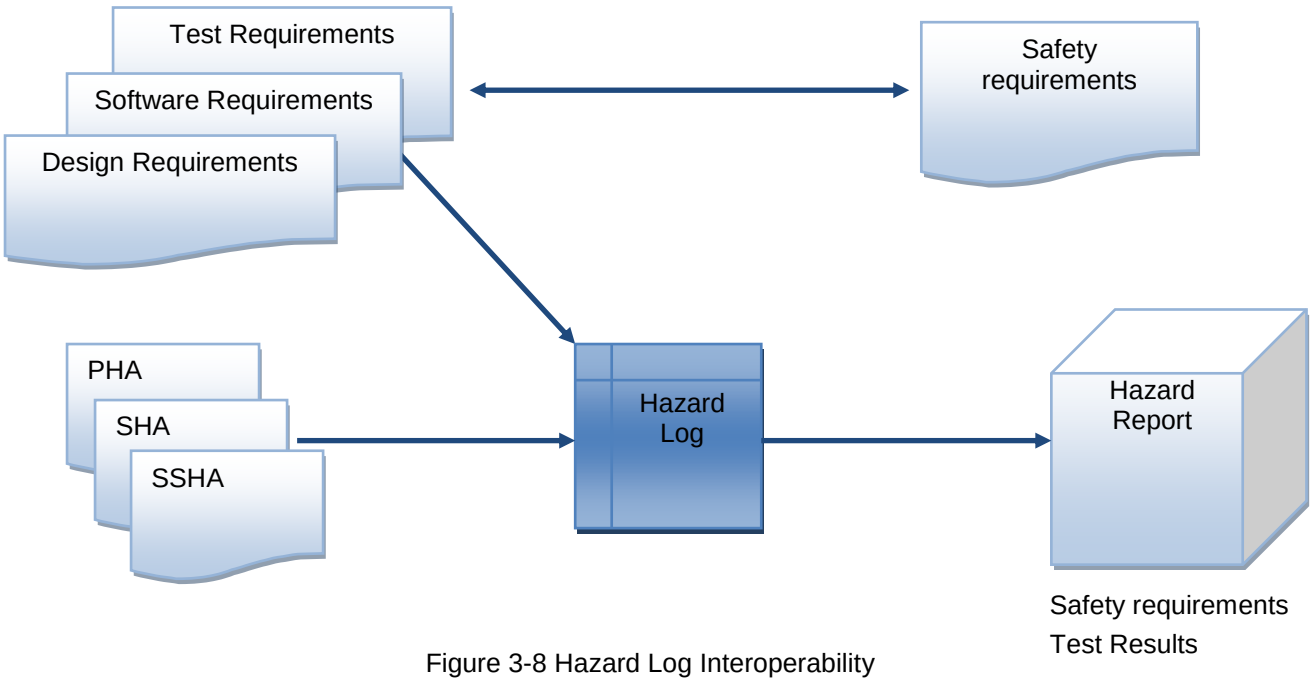


Figure 3-8 Hazard Log Interoperability

Figure 3-10 illustrates the way safety requirements interoperate with design and test requirements. Safety requirements are traced to ensure that all safety requirements are tested.

3.3 Interoperability between tools

Advanced System Architecture Program (ASAP) approach requires a number of tools to handle different number of systems analysis activities. The tools are provided by different vendors. Each vendor provides specific functionality. IBM DOORS supports requirements analysis, Papyrus integrates system analysis, safety architect supports safety analysis, configuration and change management tools are then required for versioning and traceability. Figure 3-11 illustrates ALSTOM approach to guarantee collaboration between tools used during ALSTOM TRANSPORT system life cycle.

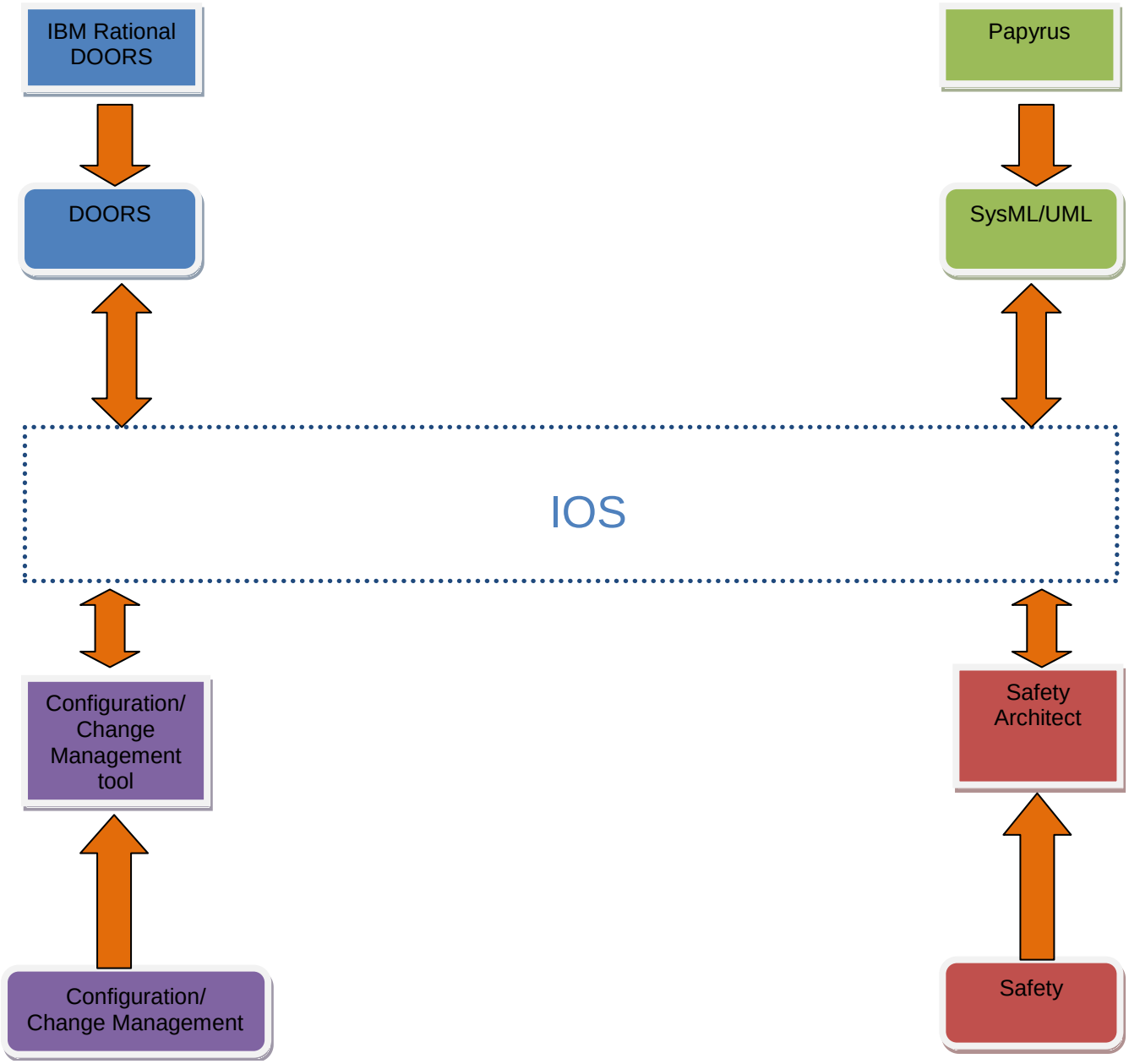


Figure 3-9 Interoperability among engineering tools

As depicted in Figure 3-11, our interoperability approach requires only one adaptor for every tool. Therefore, we only require one data share platform to ease collaboration among all tools users.

3.4 Interoperability between stakeholders as end users

ALSTOM TRANSPORT lifecycle process requires stakeholders such as Requirements Engineer, System Engineer, Safety Engineer, and Safety Expert as end users. We intend to ease communication among these actors. This may avoid misunderstanding between stakeholders. Why not implementing a data exchange platform where stakeholders can share data.

3.5 Configuration management

We require configuration management in order to control changes throughout the system lifecycle. So we can evaluate changes before they are approved. We need to control product releases and updates, to record and report components status, to manage the process execution and its tools. Configuration management must facilitate team work. It can also manage revision of requirements through version control.

3.6 Requirements change management

Requirements change management activities include:

- Analysing changes management: Any change request must be documented and recorded. An impact analysis can be performed and the decision whether the change has to be implemented or not.
- Implementing changes management: Existing requirement must be considered as obsolete when it has been deleted or replaced by the new requirement.

The traceability links must be established between obsolete requirements and new requirements. This must allow registering modifications that have been performed.

4 Terms, Abbreviations and Definitions

CRYSTAL	CRitical SYSTem Engineering AcceLeration
ASAP	Advanced System Architecture Program
ASM	Accident Scenario Model
DOORS	Dynamic Object Oriented Requirements System
FMEA	Failure Mode and Effects Analysis
HBS	Hazard Breakdown Structure
IF	Inefficiency Factors
IOS	Interoperability Specification
OC	Operational Context
PHA	Preliminary Hazard Analysis
RMT	Requirement Management Tool
RRF	Risk Reduction Factor
RTP	Reference Technology Platform
S	Severity
SAE	Safety Assurance Engineer
SAM	Safety Assurance Manager
SDM	System Dysfunctional Model
SHA	System Hazard Analysis
SHL	Safety Hazard Log
SIL	Safety Integrity Level
SSHA	Sub System Hazard Analysis
SysML	Systems Modelling Language
THR	Tolerable Hazard Rate
UML	Unified Modelling Language

Table 4-1: List of Acronyms

Accident	Uninspected even that results in the death or injury of personnel, system loss, or damage to property, equipment or the environment
Barrier	Actor that prevents a hazard (operational or technical) from developing into a Railway hazard and finally a potential accident. A barrier can be implemented by: • A procedure (e.g. operational and/or maintenance procedures with trainings of the involved staff). • A Function
Failure	Inability of a system, subsystem, or component to perform its required function
Failure cause	Process or mechanism responsible for initiating the failure mode. The possible processes that can cause component failure include physical failure, design defect, manufacturing defects, and environmental forces.
Failure effects	Consequence (s) a failure mode has on the operation, function, or status of an item and on the system.
Failure mode	The manner by which an item fails
Failure mode and Effects analysis	Tool for evaluating the effects of potential failure modes of subsystem, assemblies, components, or functions. It is primary the reliability tool to identify failure mode that would adversely affect overall system reliability. FMEA has the capability to include failure rates for each failure mode in order to achieve a quantitative probabilistic analysis.
Fault	Undesired anomaly in the functional operation of an equipment or system.
Fault tree	Model that logically and graphically the various combinations of possible events occurring in a system that leads to a previously identified hazard or undesired event
Fault tree analysis	System analysis technique used to determine the root cause and the probability of occurrence of a specified undesired event.
Function	A mode of action or activity by which a product fulfils its purpose.
Hazard	Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.
Hazard Breakdown structure	Lists all potential accidents to be considered, the operational contexts in which they may occur, and links them (through a consequence analysis) with the Railways and technical hazards that could lead to such potential accidents.
Mitigation	Action taken to reduce the risk presented by a hazard, by modifying the hazard in order to decrease the incident probability and or the incident severity. Mitigation is generally accomplished through design measures, use of safety devices, warning devices, training or procedures. It is also referred to as hazard mitigation and risk mitigation.
Operational context	Feature where, when and how a Railway Hazard may develop into a potential Accident
RRF	Risk Reduction factor is a factor that allows reducing the probability of an accident occurring. It takes into account a specific operational context or the presence of a protection function (barrier).
Safety barrier	A system or action, intended to reduce the rate of a Hazard or a likely Accident arising from the Hazard and/or mitigate the severity of the likely Accident.

Safety requirements	Safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) necessary to meet legal or company safety targets
SIL	A number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures.

Table 4-2 Glossary

5 References

[Author, Year]	Authors; *Title*; Publication data (document reference)
[SPRINT2012]	Andreas Keis, Parham Vasaiely, Systems Engineering Tools Integration and Interoperability using OSLC in the SPRINT project, 2nd February 2012
[D601.010]	Parham Vasaiely , D601.010 State of the art – Interoperability, November 2013
[BSIE2013]	Annemarie Hamedler;Christian El Salloum, Business Scenario: The Interoperable Enterprise, November 2013
[CENELEC]	EN50128:2011/CENELEC, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, June 2011
[ECHATSS]	Ericson Clifton A, Hazard Analysis Techniques for System Safety, 2005

6 Annex

6.1 Annex I: Process of SIL allocation to the system functions

During the System life cycle, we identify the potential accidents to be considered, the operational contexts in which they may occur. We also allocate a SIL to each system functions. Before allocating the SIL, we define the Accident Severity, the Accident Frequency, the Risk Acceptability Matrix, the Tolerable Accident Rate, and the Tolerable Hazard Rate.

6.1.1 Accident Severity

All potential accidents are allocated a severity of their consequences, which depends on the operational contexts in which they may occur. Table 6-1 depicts accident severity categories.

Class		Definition
I	Catastrophic	Possible multiple deaths or total system loss.
II	Critical	Possible single death, multiple severe injuries or major system damage.
III	Marginal	Possible single severe injury, multiple minor injuries or system damage.
IV	Negligible	At most singles minor injury or unscheduled maintenance.

Table 6-1 Accident Severity categories

6.1.2 Accident frequency

The next step concerns the accident frequency per operating hour. Table 6-2 illustrates Accident Frequency.

Cat.	Description	Definition	Guide Frequency (per operating hour)
A	Frequent	Likely to occur frequently. The hazard will be continually experienced.	$10^{-3} \leq f$
B	Probable	Will occur several times. The hazard can be expected to occur often.	$10^{-5} \leq f < 10^{-3}$
C	Occasional	Likely to occur several times. The hazard can be expected to occur several times.	$10^{-7} \leq f < 10^{-5}$
D	Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably be expected to occur.	$10^{-8} \leq f < 10^{-7}$
E	Improbable	Unlikely to occur, but possible. It can be assumed that the hazard may exceptionally occur.	$10^{-9} \leq f < 10^{-8}$
F	Incredible	Extremely unlikely to occur. It can be assumed its occurrence may not be experienced.	$f < 10^{-9}$

Table 6-2 Tolerable Frequency categories

6.1.3 Risk Acceptability matrix

Table 6-3 establishes the Risk Acceptability matrix.

Risk acceptability matrix Accident Frequency Category		Accident Severity Category			
		I Catastrophic	II Critical	III Marginal	IV Negligible
A	Frequent	IN	IN	IN	UN
B	Probable	IN	IN	UN	TL
C	Occasional	IN	UN	UN	TL
D	Remote	UN	UN	TL	NEG
E	Improbable	TL	TL	NEG	NEG
F	Incredible	NEG	NEG	NEG	NEG

Table 6-3 Risk Acceptability matrix

Table 6-4 defines the Risk Acceptability Category depicted in Table 6-3.

Risk Index	Definition
IN : Intolerable	Risk is not acceptable from a safety point of view. It shall be rejected, eliminated.
UN : Undesirable	Risk reduction shall be implemented in order to reach the acceptable level. If the risk reduction is covered by a design modification, it shall be accepted by the Urban Safety Assessor. If the risk reduction is covered by an operating procedure, it shall be accepted by the line operator. When risk reduction is impracticable, it shall only be accepted with the agreement of the Railway Authority and/or Urban Safety Assessor.
TL: Tolerable	Acceptable with adequate control and the agreement of the Railway Authority and/or Urban Safety Assessor.
NEG: Negligible	Risk is negligible.

Table 6-4 Risk Acceptability Category definition

The next paragraph focuses on the Tolerable Accident Rate (TAR). We are going to show the way to compute the Tolerable Accident Rate (TAR).

6.1.4 Tolerable Accident Rate (TAR)

The TAR derives from the Frequency Category defined in Table 6-2. We compute the TAR by using the minimal value of the frequency Category. For instance, an Accident with a catastrophic severity and an improbable frequency category ($10^{-9} \leq f < 10^{-8}$), The TAR is equal to 10^{-9}. Therefore, an accident may occur per 10^{9} operating hours.

6.1.5 Tolerable Hazard Rate (THR)

The THR depends on the minimal value of the frequency and the minimal value of the Risk Reduction Factor (RRF). The RRF itself depends on the barrier and the operational context. Table 6-5 gives an illustration of the RRF category.

Barrier Cat.	Description	Risk Reduction Factor
a	Basic	$1 \leq RRF < 10$
b	Useful	$10 \leq RRF < 10^2$
c	Very useful	$10^2 \leq RRF < 10^3$
d	Essential	$10^3 \leq RRF < 10^4$
e	Very essential	$10^4 \leq RRF < 10^5$

Table 6-5 Barrier effectiveness categories

Table 6-6 computes the THR. For instance, an accident scenario with a catastrophic gravity, the barrier used to avoid this accident has been considered to be very useful. As shown in the table, we obtain the THR at Remote level: $10^{-7} < F < 10^{-6}$

Accident Gravity		Catastrophic	Critical	Marginal	Negligible
Tolerable Accident Rate (Category – Frequency per h.)		Improbable $10^{-9} < F < 10^{-8}$	Remote $10^{-8} < F \leq 10^{-6}$	Occasional $10^{-6} < F \leq 10^{-4}$	Frequent $10^{-3} < F$
Risk Reduction Factor (Category - Range)	Basic $1 \leq RRF < 10$	Improbable $10^{-9} < F < 10^{-8}$	Remote $10^{-8} < F \leq 10^{-6}$	Occasional $10^{-6} \leq F < 10^{-4}$	Frequent $10^{-3} < F$
	Useful $10 \leq RRF < 10^2$	Remote $10^{-8} < F < 10^{-7}$	remote $10^{-7} < F \leq 10^{-5}$	Occasional $10^{-5} \leq F < 10^{-3}$	Frequent $10^{-2} < F$
	Very Useful $10^2 \leq RRF < 10^3$	Remote $10^{-7} < F < 10^{-6}$	Occasional $10^{-6} \leq F < 10^{-4}$	Probable $10^{-4} \leq F < 10^{-2}$	Frequent $10^{-1} < F$
	Essential $10^3 \leq RRF < 10^4$	Occasional $10^{-6} < F < 10^{-5}$	Occasional $10^{-5} \leq F < 10^{-3}$	Frequent $10^{-3} \leq F < 10^{-1}$	Frequent $1 < F$
	Very Essential $10^4 \leq RRF < 10^5$	Occasional $10^{-5} < F < 10^{-4}$	Probable $10^{-4} \leq f < 10^{-3}$	Frequent $10^{-2} \leq F$	Frequent $10 < F$
		Tolerable Hazard Rate (Category – Frequency par h.)			

Table 6-6 Tolerable Hazard Rate

The THR allows allocating the safety integrity to the functions that can generate accidents. To allocate the SIL to these functions, we use the correspondence table THR to SIL.

Tolerable Hazard Rate (per hour)	SIL
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1
$10^{-5} \leq THR$	0

Table 6-7 THR to SIL (CENELEC EN 50129)