

PROPRIETARY RIGHTS STATEMENT

THIS DOCUMENT CONTAINS INFORMATION, WHICH IS PROPRIETARY TO THE CRYSTAL CONSORTIUM. NEITHER THIS DOCUMENT NOR THE INFORMATION CONTAINED HEREIN SHALL BE USED, DUPLICATED OR COMMUNICATED BY ANY MEANS TO ANY THIRD PARTY, IN WHOLE OR IN PARTS, EXCEPT WITH THE PRIOR WRITTEN CONSENT OF THE CESAR CONSORTIUM THIS RESTRICTION LEGEND SHALL NOT BE ALTERED OR OBLITERATED ON OR FROM THIS DOCUMENT. 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 **SY**STem Engineering **Acce**Leration

Use Case 5.3 definition

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	Use Case 5.3 definition
Deliverable No.	D503.010
Dissemination Level	CO
Nature	R
Document Version	V1.0
Date	2013-11-15
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	2013-11-15	Pascal POISSON
Internal Review	2013-11-15	Elie Soubiran
External Review		Frédérique VALLÉE
External Review		François Chastrette

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected
V1.0	2013-11-15	Initial document	



CONTENT

1	INTRODUCTION.....	7
1.1	ROLE OF DELIVERABLE	7
1.2	RELATIONSHIP TO OTHER CRYSTAL DOCUMENTS	7
1.3	STRUCTURE OF THIS DOCUMENT	7
2	USE CASE DESCRIPTION.....	8
2.1	RAILWAY USE CASE	8
2.1.1	CBTC	8
2.2	APPLICABLE PROCESS.....	9
3	DETAILED DESCRIPTION OF THE PROCESS.....	12
3.1	MBSE	12
3.1.1	Requirements management and development.....	13
3.1.2	Operational analysis	13
3.1.3	Functional analysis	13
3.1.4	Constructional analysis	13
3.1.5	V&V	14
3.1.6	Mapping modelling process to Alstom methodology	14
3.2	MBSA	15
3.2.1	Preliminary hazard analysis.....	16
3.2.2	System hazard analysis	16
3.2.3	Sub system hazard analysis.....	17
3.2.4	Hazard log.....	17
3.2.5	System Safety Case	18
3.3	TRANSVERSE ACTIVITIES	19
3.3.1	Change management and impact analysis	19
3.3.2	Configuration management	19
3.3.3	Requirement traceability	19
3.3.4	Interoperability	19
3.3.5	Tools.....	20
4	TERMS, ABBREVIATIONS AND DEFINITIONS	21
5	REFERENCES.....	22
6	ANNEX I: ENGINEERING METHODS.....	23

Content of Figures

Figure 2-1 Communication Based Train Control system (CBTC)	8
Figure 2-2 Use case based system development cycle	10
Figure 3-1 Requirements management and design modelling process	12
Figure 3-2 Relations between modelling process and Alstom specification documents	14
Figure 3-3 Global fault tree	15
Figure 3-4 Causal link between failure modes and system event	16

Content of Tables

Table 2-1 Carborne traffic control	9
Table 3-1 Hazard Log Result	18
Table 4-1: Terms, Abbreviations and Definitions	21

1 Introduction

1.1 Role of deliverable

The aim of this deliverable is to describe:

- Alstom's use case
- Alstom transport system life cycle approach
- Tools derived from the use case
- The way IOS could be applied to Alstom transport system life cycle approach

1.2 Relationship to other CRYSTAL Documents

This deliverable gives more details of the initial engineering methods template. The template is the Excel attached file in annex I.

1.3 Structure of this document

This document is organized as follows:

- First part describes the use case
- Second part focuses on the description of System development life cycle that should be applied.

2 Use case description

2.1 Railway use case

2.1.1 CBTC

The use case considers design activities of a CBTC system. The CBTC is the railway signalling system allowing telecommunications between the train and track equipment for the traffic management and infrastructure control. CBTC helps operators locate the precise position of the train.

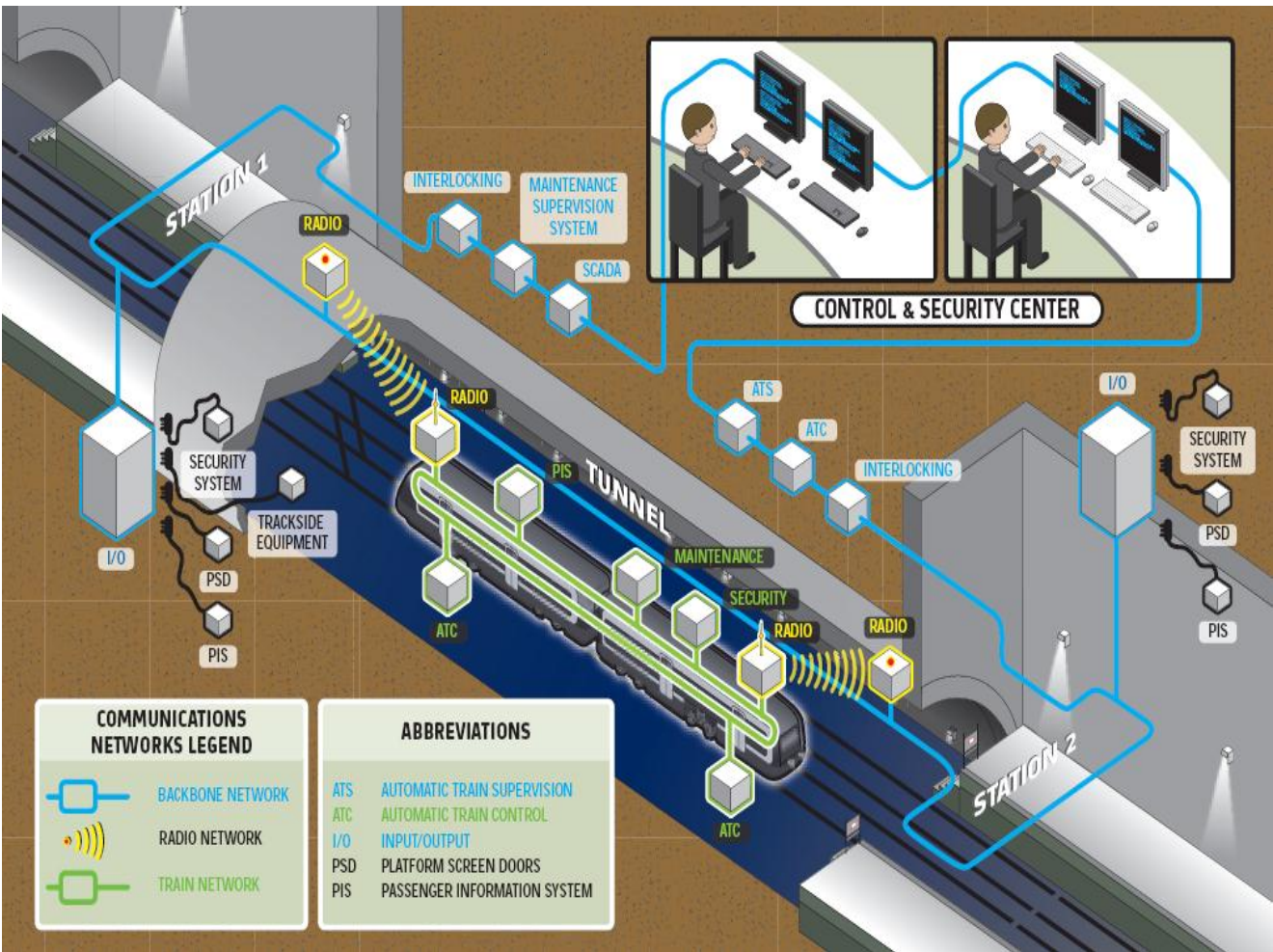


Figure 2-1 Communication Based Train Control system (CBTC)

The CBTC is more efficient and safe to manage the railway traffic control. CBTC is made of several components. Sequence of interaction among these components is ensured by the data communication system. For this use case, we focus on the ATC sub-system. ATC is in charge of managing train protection and train operation. A sub-set of ATC functions used in the railway use case is given in Table 2-1.

Functions	ATC
F4 Carborne Traffic Control	
F4.1 Ensure train protection	√
F4.1.1 Compute positive train detection and characteristics	√
F4.1.2 Supervise train movement	√
F4.1.2.1 Monitor train speed and energy	√
F4.1.2.2 Monitor train doors and PSD	√
F4.1.4 Authorize and assist train operation	√
F4.1.4.1 Manage train driving mode	√
F4.1.4.2 Manage individual train safe control	√
F4.1.4.1 Indicate speed to Rolling Stock	√
F4.2 Ensure train operation	√
F4.2.1 Compute train precise location and speed	√
F4.2.2 Compute the run profile	√
F4.2.3 Drive the train	√
F4.2.4 Display information on driver HMI	√

Table 2-1 Carborne traffic control

2.2 Applicable process

The applicable process for this use case is based on the standard Alstom process for CBTC development. Its overview appears on figure 2.2. Details of the process are described in section 3.

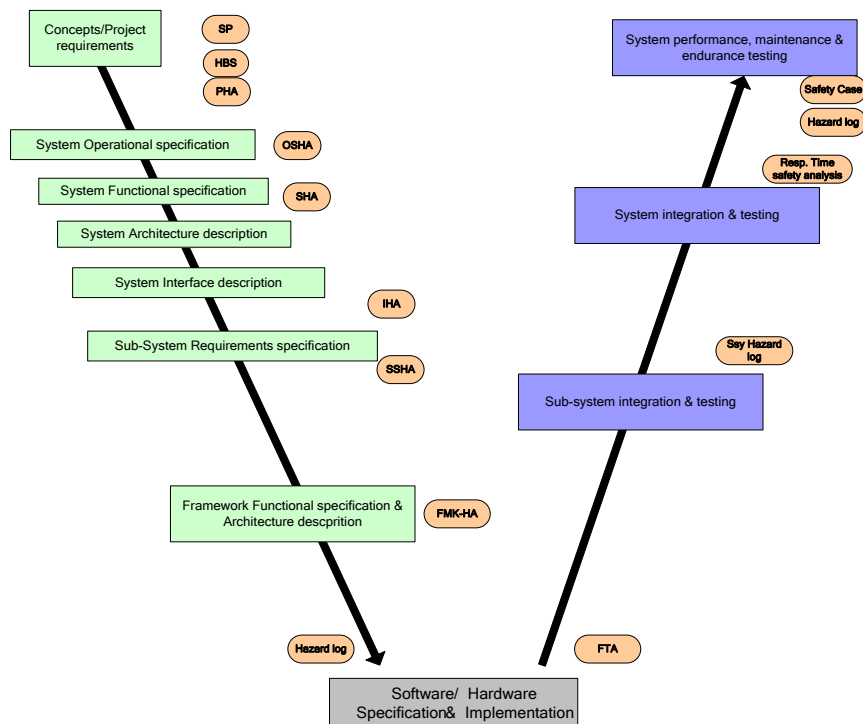


Figure 2-2 Use case based system development cycle

The system development cycle relies on MBSE and MBSA to achieve the specification, the design and the dysfunctional analysis of the system or project of interest. The process developed in the use case shall be compliant with Cenelec EN 50126 standard.

The figure 2-2 shows dualities between System Engineering and Safety analysis. The main phases are:

- In the early phase of the project, requirements are elicited and consolidated and then SP, HBS, and PHA analysis are executed. The purpose of the SP is to analyse and identify the potential hazardous situations and their causes related to the operational missions that the system shall fulfil, and to define the actions and the means that eliminate them, or reduce them to an acceptable level. The HBS activity is to identify and estimate the criticality of the potential hazards faced by the system on the basis of a typical list of accidents and to evaluate the risks that these hazards occur. The PHA activity defines the high level requirements to be applied with the design or to be exported in order to cover the hazards identified in the HBS.
- System Operational specification is checked by the OSHA in order to analyse and identify the potential hazardous situations and their causes related to the operational missions that system shall fulfil, and to define the actions and the means that eliminate them, or reduce them to an acceptable level.
- SHA analyses the causes of unsafe situations of the system related with the functions it implements. It defines the actions and the means that eliminate, or reduce the risks to an acceptable level.
- IHA is required during the system interface description to analyse the causes of unsafe situations of the system related with the devices, protocols and data used by sub-systems to communicate with each other or with external systems. And to define the actions and means that eliminate, or reduce to an acceptable level, the risks.
- SSHA analyses the causes of failures of sub-systems, and defines the means to eliminate or reduce them to an acceptable level the risks.

-
- FMK-HA activity is required to analyse the causes of failures of framework components, and to define the means to eliminate or reduce them to an acceptable level the risks.
 - The system life cycle includes FTA to show the way the system reaches the safety target.
 - Hazard log activity records and gives the status of safety requirements, and evidence that is used to validate these requirements.
 - System response time safety analysis is required to analyse the system response time and validate all the safety distances, and times considered by the system.
 - At the end of the cycle, we use the system safety case to demonstrate that the conditions for system safety acceptance are satisfied.

3 Detailed description of the process

Section 3.1 deals with Alstom transport MBSE process. Alstom transport MBSA process is described in section 3.2. Transverse activities and the associated processes are described in section 3.3.

3.1 MBSE

The system modelling used in this process is the Alstom Transport's ASAP process which is implemented with UML/SysML. ASAP is an advanced use case driven method that addresses requirements management, operational analysis, functional analysis and constructional analysis. Each phase of analysis is followed by V&V.

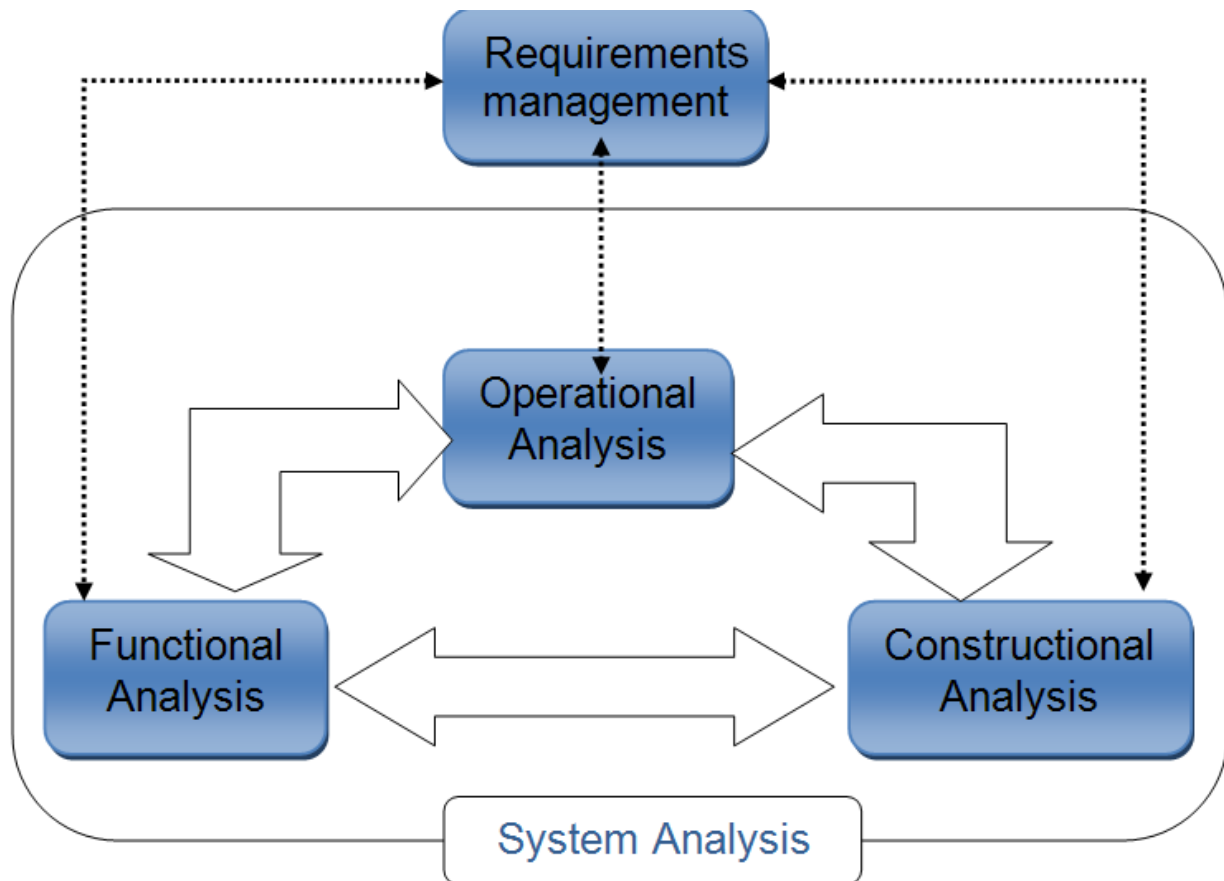


Figure 3-1 Requirements management and design modelling process

Section 3.1.1 gives an overview of requirements management. Section 3.1.2 describes the operation analysis. Section 3.1.3 describes the functional analysis. Section 3.1.4 describes the constructional analysis. Section 3.1.5 describes V&V. Modelling process and Alstom methodology is then described in section 3.1.6.

3.1.1 Requirements management and development

Requirement analysis allows a Requirement Engineer to capture customer needs. Requirements should be clarified during system analysis stage. Requirements are allocated to system functional & non-functional descriptions.

3.1.2 Operational analysis

During the operational analysis, System Engineer focuses on the environment of the system studied. At this stage, a Systems Engineers:

- Define the operational contexts of the system;
- Define the use cases involving the system studied and their actors;
- Define events views which model for each couple (mission, context) the sequences of messages to be exchanged between the system and its environment;
- Refine the operational data model which should specify business data exchanged between the systems and its corresponding actors;
- Refine operational requirements to operational model elements.

3.1.3 Functional analysis

Functional analysis is the way the system fulfil the operational view.

At this level, systems architects:

- Allocate steps of use cases to functions
- Identify steps inputs/outputs of each function and relationships between functions
- Describe the dynamic behaviour of each function
- Refine the functional data model
- Allocate functional requirements to functions

3.1.4 Constructional analysis

Constructional analysis focuses on the sub-systems and components that will be used to perform the functions previously modelled.

Here system architects:

- Refine the constructional design of the system by decomposing it into elements;
- Allocate previous defined functions on these elements in order to trace their relationships;
- Define the constructional interaction between elements;
- Define the constructional data model view which exhibit data exchanged between elements;
- Define interface typing the previously defined internal and external interactions and describing the dynamic behaviour of each interface;
- Allocate constructional requirements to constructional elements.

3.1.5 V&V

V&V is made during the system analysis in order to check whether the analysis matches system requirements. So system is directly analysed and tested. This is the way to limit error detections during later stages.

3.1.6 Mapping modelling process to Alstom methodology

Figure 3-2 illustrates the relationships between the global modelling process and the Alstom methodology.

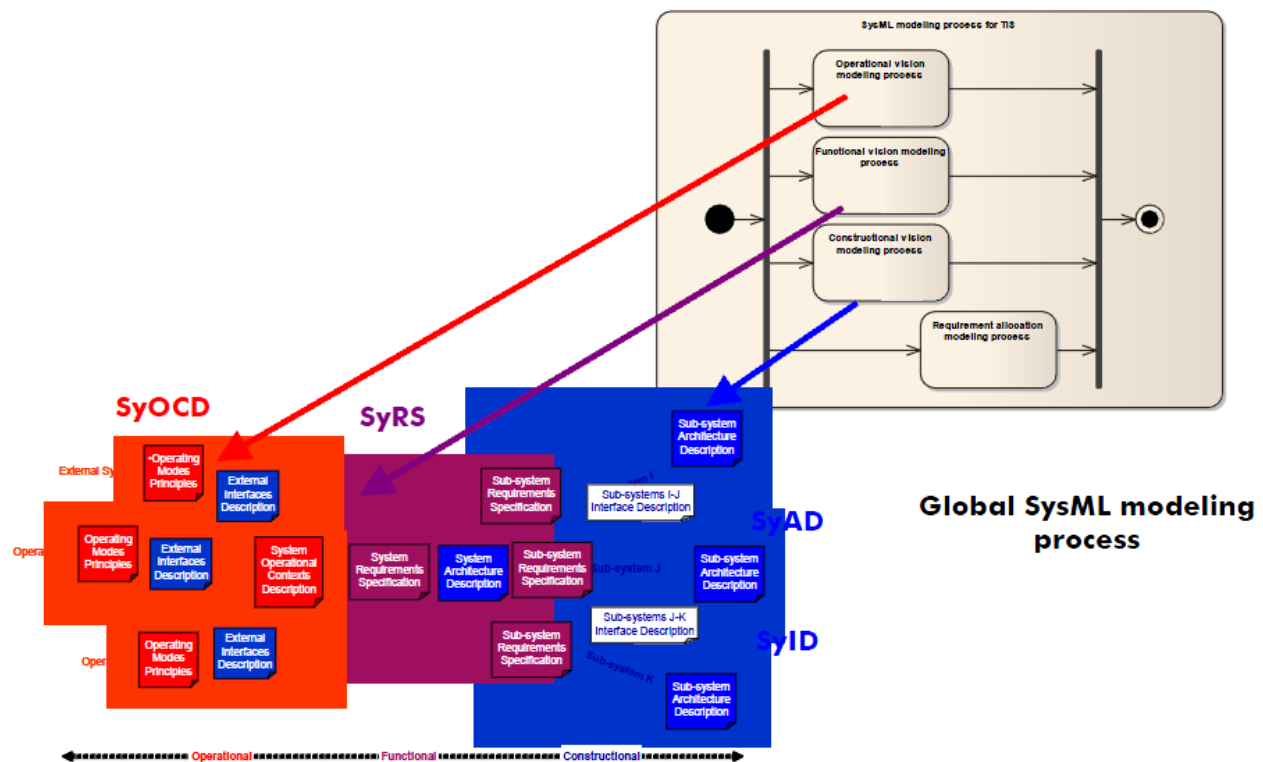


Figure 3-2 Relations between modelling process and Alstom specification documents

- The operational vision maps to SyOCD
- The functional vision maps to SyRS
- The constructional vision maps to SyAD and SyID

3.2 MBSA

The challenge of MBSA is to help Safety Engineer to build the “global fault tree” of a given system, linking accident scenario down to faults occurring within atomic components of the system. Figure 3-3 depicts this global fault tree structure where safety engineering activities are allocated; especially PHA, SHA and SSHA.

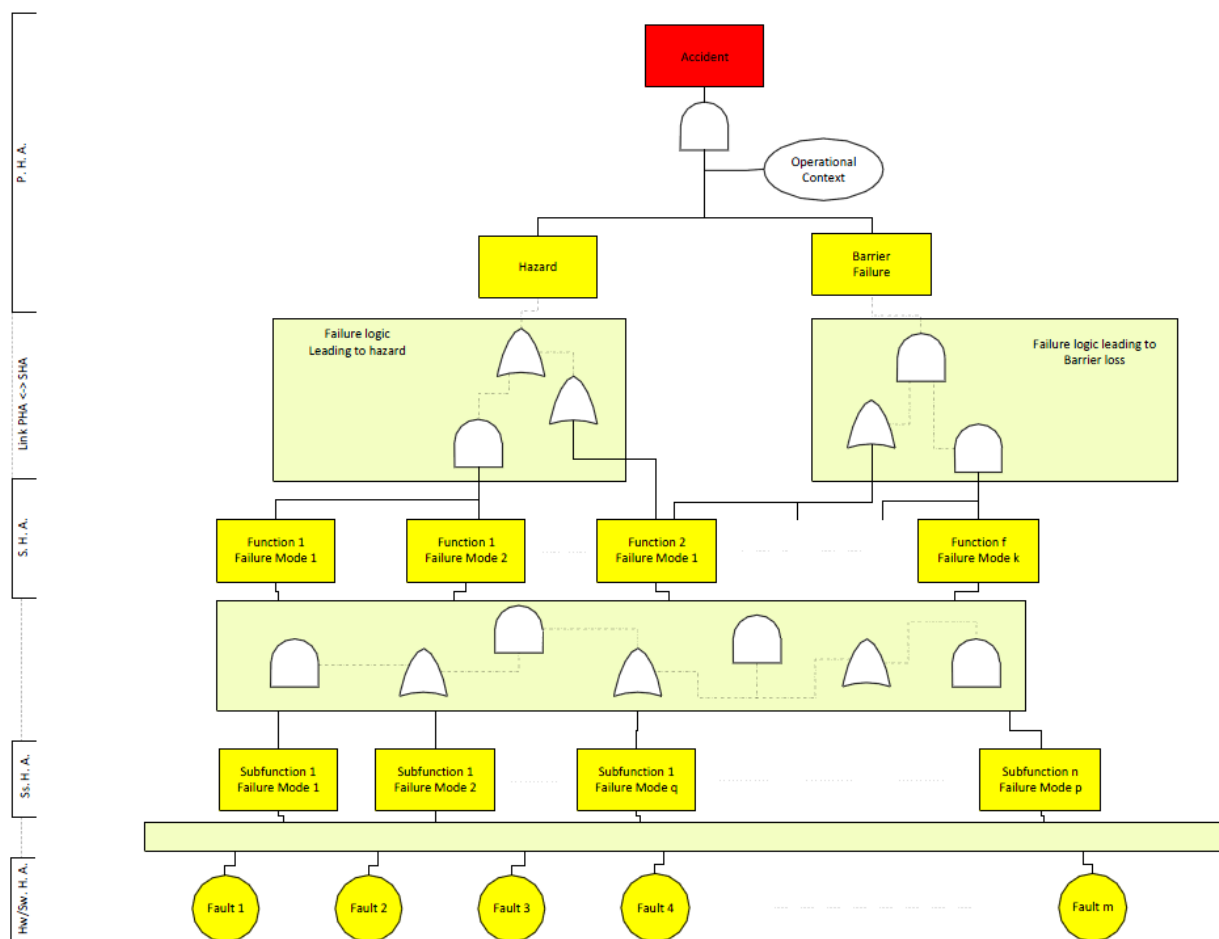


Figure 3-3 Global fault tree

During the preliminary hazard analysis phase, safety engineers identify accidents. Accidents depend on hazardous situation and operational context. SHA intends to identify the failure modes, causes and consequences related to the functions identified during system analysis. SSHA identifies failure modes, causes and consequences associated to the sub functions. Several failure modes of a function may be required in order to be developed into hazard cause or failure barrier. The general case is illustrated on Figure 3-4. When every failure modes of every function are identified, it is now possible to establish the causal analysis of the barrier failure or hazard cause. Then, the safety issue is the consequence of direct causes or concomitant causes.

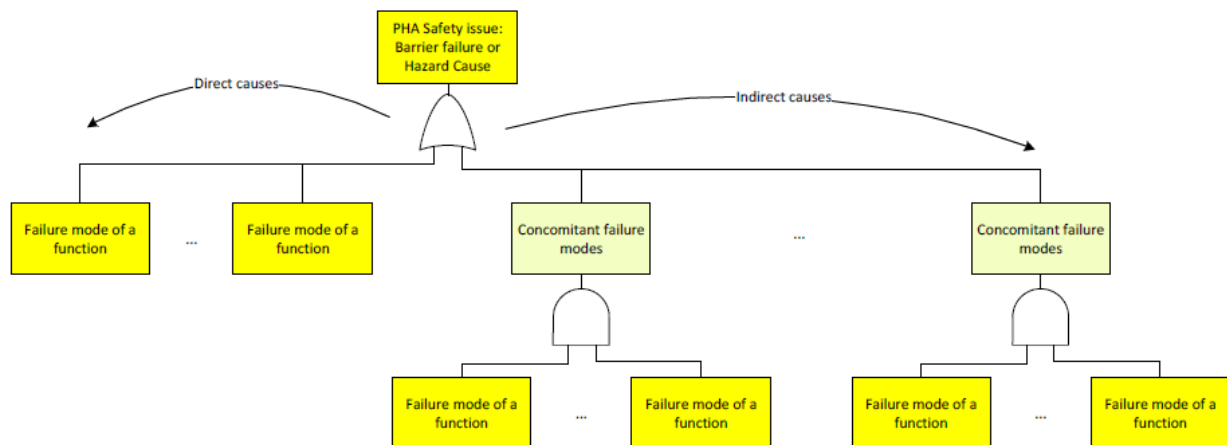


Figure 3-4 Causal link between failure modes and system event

Section 3.2.1 gives an overview of the preliminary hazard analysis; section 3.2.2 describes the system hazard analysis. Section 3.2.3 describes the sub system hazard analysis. Section 3.2.4 describes the Hazard log. Safety case is then described in the section 3.2.5.

3.2.1 Preliminary hazard analysis

Inputs

The PHA takes into account the Safety Plan, the system requirements and the Hazard Breakdown Structure.

Purpose

The purpose of this activity is to define the high level requirements to be applied on design or to be exported in order to cover the hazards identified in the HBS.

Description

PHA identifies protections necessary to eliminate or mitigate identified risks.

Outputs

At the end of the PHA, safety requirements at the system level, are defined and stored in Doors.

3.2.2 System hazard analysis

Inputs

Before starting SHA activity the following inputs are needed: the Safety Plan, the Preliminary Hazard Analysis, the Hazard breakdown structure, the System Functional Specification, the System Operational and Support Hazard Analysis.

Purpose

The purpose of SHA is to analyse the causes of unsafe situations of the system related with the functions it implements and to define the actions and the means that eliminate, or reduce to an acceptable level, the risks.

Description

SHA identifies all failures leading to potential hazards through a Failure Mode and Effects Analysis (FMEA). It determines and assigns the SIL of system functions. It identifies barriers and safety requirements against

hazardous situations. It identifies the necessary sub-system hazard analyses, specific hazard analyses and interface hazard analyses and records this information in the SHL. It then records identified hazards in the SHL.

Outputs

SHA also generates new safety requirements at system level and stores them in Doors.

3.2.3 Sub system hazard analysis

Inputs

SSHA takes into account the Safety Plan, System Hazard analysis, System Interface Hazard analysis and Sub-systems requirements specification.

Purpose

The purpose of this activity is to analyse the causes of failures of sub-systems, and to define the means to eliminate or reduce them to an acceptable level the risks.

Description

SSHA identifies all failures leading to potential hazards through a Failure Mode and Effects Analysis (FMEA). It determines and assigns the SIL of sub-systems functions. It also identifies barriers and safety requirements against hazardous situations.

Outputs

SSHA also generates new safety requirements at sub system level and stores them in Doors.

3.2.4 Hazard log

Input

The construction of the Hazard log begins with the first safety activities describe above and ends up with system validation.

Purpose

The Hazard log is in charge of recording and giving the status of safety requirements.

Description

Records for each identified hazard encompass 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
- People involved in safety related activities with their skills
- Methods, techniques and tools used for analysis

Output

Table 2-1 depicts the result of the Hazard log.

Version	Nature	Date	Page
V1.0	R	2013-11-15	17 of 27

Components	Description
SHL Identification	Identification of Hazard Log requirement, and its associated coverage.
ID	Identification of Safety Requirement
Responsibility	This field gives the responsibility associated to the type of requirements.
Modification	This field illustrates modification of the safety, modification of the coverage and impact in the previous requirement.
Validation Test Description Coverage	This field allows to verify the coverage of Test Plan
Safety Requirement	This field represents requirements identified during safety analysis.
Proof of document	This field describes in a synthetic way the answer and the result
Design coverage	This field Links the requirement and system design
Test results	This field gives the result of test. The results are the ones given in the Functional Validation.
Comments	This field gives the comments about the status choice or a precision about the line
Status	This field shows the design requirements status and safety requirements status

Table 3-1 Hazard Log Result

3.2.5 System Safety Case

Input

System Safety case takes into account, all system design, verification, validation, safety and quality documents Sub-system and System Hazard Logs.

Purpose

The purpose of this activity is to demonstrate that the conditions for safety acceptance are satisfied.

Description

System safety case gives a detailed description of the system, of its components and documentation. It provides evidence that the system has been developed according to quality management and processes compliant with quality standards prescribed by CENELEC EN 50129 which guarantee that it reaches the requested quality level such as

- Evaluating project quality process
- Evaluating project organisation and involved roles
- Evaluating system quality products.
- Evaluating system design process.

Version	Nature	Date	Page
V1.0	R	2013-11-15	18 of 27

- Evaluating system safety process
- Evaluating system validation and verification process
- Evaluating system design principles.
- Evaluating system safety principles.
- Evaluating system validation and verification principles.

3.3 Transverse activities

The following activities are mandatory to achieve a realistic industrial process. IOS and interoperability standards such as OSLC shall help engineers to set up a performing framework for managing change request, traceability, impact analysis, and configuration management.

3.3.1 Change management and impact analysis

The change management process is the process of requesting, determining attainability, planning, implementing, and evaluating changes to a system.

3.3.2 Configuration management

The objective of configuration management is to ensure effective management of the evolving configuration of a system, both hardware and software, during its life cycle. Fundamental to this objective is the establishment, control, and maintenance of software and hardware baselines. Baselines are reference points for maintaining development and control.

The primary output of the configuration management process is the maintenance of the configuration baseline for the system and system elements. Items are placed under formal control as part of the decision-making process. The required configuration baseline documentation is developed and approved in a timely manner to support required systems engineering technical reviews, the system's acquisition and support strategies, and production.

3.3.3 Requirement traceability

End-to-end requirement traceability is mandatory in order to conform to standards.

3.3.4 Interoperability

The main objective of Alstom is to develop a RTP that tools a system architecture framework (cf. ISO/IEC/IEEE 42010). This architecture framework should provide a collection of viewpoints representative of the disciplines and metiers peculiar to railway safety critical system engineering (RAMS viewpoints, operational viewpoints, validation viewpoints...). The RTP is composed of a set of tools, each metier having its own tools; the IOS of Crystal shall be the backbone for knowledge and data sharing between these tools and hence between the different teams (e.g. system designers, safety engineers, RAM engineers, configuration management engineers...).

The use case presented here focuses on system and safety engineering activities, taking into account traceability and configuration management. In that context, IOS shall be the mean to coherently share versioned system design artefact (functions, components...) between system and safety teams, so that Safety Engineer can produce a dysfunctional specification of the latter. On the opposite, Safety Engineer produces safety requirements, dysfunctional scenarios and operational recommendations that drive the system design. The IOS shall also be able to be the media for Hazard Log, indeed this item is cross-

Version	Nature	Date	Page
V1.0	R	2013-11-15	19 of 27

discipline and then very interesting from an interoperability point of view; it gathers safety requirements, system artefact, baselines, test cases, validation results, safety evidences... Coherently managing all these artefacts and ensuring an end-to-end traceability is one of the most difficult challenges for IOS.

3.3.5 Tools

Table 3-1 Tools

Name (Contributor)	Description
DOORS (IBM)	DOORS is a requirement management tools, it provides OSLC services for requirements management.
Papyrus (CEA)	Modelling Tool that provides an implementation of the OMG standards (UML, SysML, Marte). Papyrus is an open source modelling tool. While not used in production, it can integrate with our Alstom transport Use Case-Based Software Life Cycle
Safety Architect (All4Tec)	Safety Architect is a tool achieving risk analysis of complex systems using functional or physical architectures from usual modelling tools (for example SysML or UML).
Eclipse Platform	Eclipse provides a rich framework and implementation for development of models, hardware and software. Its basis is a platform including core editors for multiple text-based languages. An SDK (Lyo) to implement OSLC services is provided.

4 Terms, Abbreviations and Definitions

CRYSTAL	CR itical SYST em Engineering AcceL eration
DOORS	Dynamic Object Oriented Requirements System
MBSE	Model-Based Systems Engineering
MBSA	Model-Based Safety Analysis
SysML	Systems Modelling Language
UML	Unified Modelling Language
PHA	Preliminary Hazard Analysis
SHA	System Hazard Analysis
SSHA	Sub System Hazard Analysis
CBTC	Communication Based Train Control
ATC	Automatic Train Control
ASAP	Advanced System Architecture Program
V&V	Verification and validation
SP	Safety Principles
HBS	Hazard Breakdown Structure
OSHA	Operational and Support Hazard Analysis
IHA	Interface Hazard Analysis
FMK-HA	Framework Hazard Analysis
FTA	Fault Tree Analysis
FMEA	Failure Mode and Effects Analysis
SIL	Safety Integrity Level
SHL	Safety Hazard log
DSL	Domain Specific Language
SyAD	System Architecture Description
SyID	System Interface Description
SyOCD	System Operational Context Description
SyRS	System Requirements Specification

Table 4-1: Terms, Abbreviations and Definitions



5 References

UseCase

First point of contact:	Vidal Delmas TCHAPET NYA, ALSTOM TRANSPORT vidal-delmas.tchapet-nya-ext@transport.alstom.com
Second point of contact:	POISSON Pascal, SOUBIRAN Elie, BELMONTE Fabien pascal.poisson@transport.alstom.com elie.soubiran@transport.alstom.com

1	UC5.3_Preliminary_Hazard_Analysis
2	UC5.3_System_Hazard_Analysis
3	UC5.3 Subsystem hazard analysis

[illegible]

PRELIMINARY HAZARD ANALYSIS

Engineering Method: UC5.3_PreliminaryHazardAnalysis_001					
Purpose: safety engineer identifies the hazardous situations leading to an accident and the related requirements necessary to ensure safety					
Comments:					
Pre-Condition		Engineering Activities (made of steps)		Post-Condition	
1. System Requirements have been defined and stored in Doors 2. Safety assurance plan has been delivered 3. System engineers have modelled in SysML the system at operational level		1. Safety engineer identifies hazardous situations 2. Safety engineer identifies operational context 3. Safety engineer identifies combinations that cause accidents 4. Safety engineer identifies or creates barriers that can prevent hazards 5. Safety engineer identifies system safety requirements		1. PHA document has been delivered. 2. Safety requirements of the Preliminary Hazard Analysis have been defined 3. New safety requirements stored in Doors 4. hazard log has been opened	
Notes:		Notes:		Notes:	
Artefacts Required as inputs of the Activities		Artefacts used internally within the Activities (optional)		Artefacts Provided as outputs of the Activities	
Name	System Requirements			Name	Safety requirements
Generic Type: (Tool or language independent type)	System Requirements (Doors)			Generic Type: (Tool or language independent type)	safety requirements
Required Properties: (Information required in interactions between steps)	1. Requirement ID 2. Requirement description 3. Requirement source 4. Requirement priority 5. Responsibility 6. Requirement version 7. Comments			Provided Properties: (Information provided in interactions between steps)	Inherits properties from system requirements plus: 1. Requirement type (Design, Maintenance, Operation) 2. SIL (Safety Integrity Level) (optional at this stage)
Description & Interoperability Additional Constraints:				Description & Interoperability Additional Constraints:	
Name	Operational contexts			Name	Hazard Log
Generic Type: (Tool or language independent type)	Operational contexts (from SysML stereotype)			Generic Type: (Tool or language independent type)	List of hazard with barrier and verification means
Required Properties: (Information required in interactions between steps)	1. Phase 2. Mode 3. Zone			Provided Properties: (Information provided in interactions between steps)	1. Safety Hazard Log ID 2. Accident (from HBS) 3. Safety Requirement 4. Evidence (closure justification, test case...) 5. Status 6. Comments
Phase, mode and zone range other specific enumerated types or lists of values.				Properties 4 may be empty at this stage	
Name	Operational view of the system			Name	Hazard Analysis
Generic Type: (Tool or language independent type)	1. System and its environment defined as blocks 2. Scenario defined as use case and interaction objects			Generic Type: (Tool or language independent type)	List of accident scenario
Required Properties: (Information required in interactions between steps)	1. Element ID 2. Satisfied requirements 3. Element version			Provided Properties: (Information provided in interactions between steps)	1. ID 2. Accident (from HBS) 3. Hazard cause 4. Operational context 5. Safety Requirement 6. Barrier 7. Tolerable Accident rate 8. Scenario version
These elements are only imported for traceability issues and versioning coherency (system model vs safety analysis).					
Name	Hazard breakdown structure				
Generic Type: (Tool or language independent type)	Classified set of accident				
Required Properties: (Information required in interactions between steps)	1. Accident ID 2. Accident type 3. Sub accident type 4. Hazard 5. Gravity				
HBS library may be defined or not (i.e. re-use from previous)					
↑ Artefacts considered for Interoperability				↑ Artefacts considered for Interoperability	

SYSTEM HAZARD ANALYSIS

Engineering Method: UC5.3_SystemHazardAnalysis_001					
Purpose: Safety engineer leads a cause consequence analysis (FMEA) on each function of the system and identifies the necessary requirements to ensure safety					
Comments:					
Pre-Condition		Engineering Activities (made of steps)		Post-Condition	
1. Preliminary Hazard Analysis has been delivered and validated 2. System design has taken preliminary hazard Analysis safety requirements into account 3. Functional decomposition of the system has been modelled in SysML 4. System architecture has been modelled in SysML 5. Functions have been allocated to architectural elements		1. Safety engineer imports system functions 2. Safety engineer identifies failure mode (Erroneous output, output not sent) for every single function of the system 3. Safety engineer identifies the causes of each failure mode 4. safety engineer links the hazard cause to the involved subsystem 5. Safety engineer identifies failure mode effect (local and system) 6. Safety engineer identifies safety requirements and allocate a SIL		1. New safety requirements have been identified from system hazard analysis 2. System hazard analysis document has been delivered 3. New safety requirements stored in Doors 4. Hazard log has been updated/completed	
Notes:		Notes:		Notes:	
Artefacts Required as inputs of the Activities		Artefacts used internally within the Activities (optional)		Artefacts Provided as outputs of the Activities	
Name	System and safety requirements			Name	System and safety requirements
Generic Type: (Tool or language independent type)	System requirements/safety requirements			Generic Type: (Tool or language independent type)	Safety requirements
Provided Properties: (Information provided in interactions between steps)	1. Requirement ID 2. Requirement description 3. Requirement source 4. Requirement priority 5. Responsibility 6. Requirement version 7. Comments			Provided Properties: (Information provided in interactions between steps)	Inherits properties from system requirements plus: 1. Requirement type (Design, Maintenance, Operation) 2. SIL
Description & Interoperability Additional Constraints:				Description & Interoperability Additional Constraints:	
Name	Function breakdown structure			Name	Hazard log
Generic Type: (Tool or language independent type)	Hierarchy of functions defined as blocks or activities			Generic Type: (Tool or language independent type)	cf. previous sheet
Provided Properties: (Information provided in interactions between steps)	1. Function name 2. Function inputs 3. Function outputs 4. Super function (opt) 5. Sub functions (opt) 6. Function description 7. Dataflow link			Provided Properties: (Information provided in interactions between steps)	
All System artefacts shall reference a unique ID, a version number and a set of satisfied requirements					
Name	Product breakdown structure			Name	Dysfunctional specification
Generic Type: (Tool or language independent type)	System architecture (block hierarchy)			Generic Type: (Tool or language independent type)	Functions
Provided Properties: (Information provided in interactions between steps)	for each block: 1. Name 2. Interface 3. Supersystem (optional) 4. Subsystem (optional) 5. Allocated functions 5. Dataflow link			Provided Properties: (Information provided in interactions between steps)	Inherits from function plus: 1. Failure modes 2. Cause (events, wrong inputs...) 3. Effects (local and system) 4. Mitigating safety requirements
Description & Interoperability Additional Constraints:				A classical FMEA (Failure Mode and Effects Analysis) table should be generated from the dysfunctional specification of functions.	



Artefacts considered for Interoperability



Artefacts considered for Interoperability

SUBSYSTEM HAZARD ANALYSIS

Engineering Method: UC5.3_SubSystemHazardAnalysis_001					
Purpose: Safety engineer leads a cause consequence analysis (FMEA) on each function of each subsystems and identifies the necessary requirements to ensure safety					
Comments:					
Pre-Condition		Engineering Activities (made of steps)		Post-Condition	
1. System hazard analysis has been delivered and validated 2. System design has taken system hazard analysis safety requirements into account 3. Functional decomposition of subsystem has been modelled in SysML 4. Subsystem architecture has been modelled in SysML 5. Functions have been allocated to architectural elements		1. Safety engineer imports subsystem functions 2. Safety engineer identifies failure mode (Erroneous output, output not sent) for every single function of the subsystem 3. Safety engineer identifies the causes of each failure mode 4. safety engineer links the hazard cause to the involved subsystem 5. Safety engineer identifies failure mode effect (local and system) 6. Safety engineer identifies safety requirement and allocate SIL		1. New safety requirements have been identified from subsystem hazard analysis 2. SubSystem hazard analysis document has been delivered 3. New safety requirements stored in Doors 4. Hazard log has been updated/completed	
Notes:		Notes:		Notes:	
Artefacts Required as inputs of the Activities		Artefacts used internally within the Activities (optional)		Artefacts Provided as outputs of the Activities	
Name	System and safety requirements			Name	System and safety requirements
Generic Type: (Tool or language independent type)	System requirements/Safety requirements			Generic Type: (Tool or language independent type)	Safety requirements
Provided Properties: (Information provided in interactions between steps)	1. Requirement ID 2. Requirement description 3. Requirement source 4. Requirement priority 5. Responsibility 6. Requirement version 7. Comments			Provided Properties: (Information provided in interactions between steps)	Inherits properties from system requirements plus: 1. Requirement type (Design, Maintenance, Operation) 2. SIL
Description & Interoperability Additional Constraints:				Description & Interoperability Additional Constraints:	
Name	Function breakdown structure			Name	Hazard log
Generic Type: (Tool or language independent type)	Hierarchy of functions defined as blocks or activities			Generic Type: (Tool or language independent type)	cf. previous sheet
Provided Properties: (Information provided in interactions between steps)	1. Function name 2. Function inputs 3. Function outputs 4. Super function 5. Sub functions (optional) 6. Function description			Provided Properties: (Information provided in interactions between steps)	
System artefacts always reference a version number and a set of satisfied requirement					
Name	Product breakdown structure			Name	Dysfunctional specification
Generic Type: (Tool or language independent type)	SubSystem architecture (block hierarchy)			Generic Type: (Tool or language independent type)	Functions
Provided Properties: (Information provided in interactions between steps)	for each block: 1. Name 2. Interface 3. Supersystem 4. Subsystem (optional) 5. Allocated functions 5. Dataflow link			Provided Properties: (Information provided in interactions between steps)	cf. previous sheet
Description & Interoperability Additional Constraints:				1. A FMEA table should be generated from the dysfunctional specification of functions. 2. System effects shall trace causes from failure modes of the	

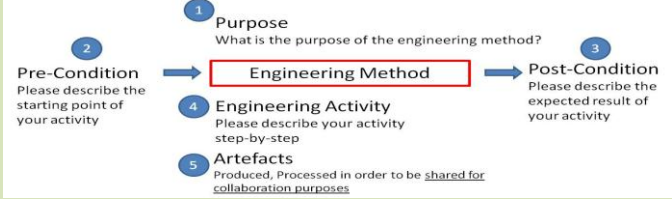
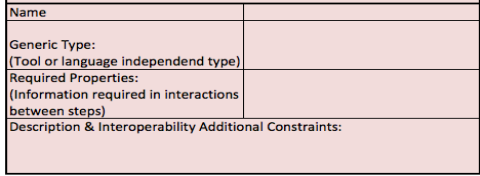
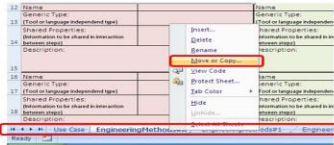
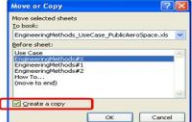


Artefacts considered for Interoperability



Artefacts considered for Interoperability

HOW TO...

How to guide for the Engineering Method Template	
0	Main Purpose of the Template a) Identify the interoperability needs of individual use cases, expressed in the form of activities and their steps b) Identify a pre-mapping between engineering methods used in activities and bricks provided by the technology providers
The Use Case Sheet a) Please provide information about your use case and the corresponding points of contact	
1	The Engineering Method Sheet b) An Engineering Methods describes how an activity can be conducted using guidelines, tools and languages which interoperate with each other. Due to the fact that an "Engineering Method" can be applied to one or more activities, there may be the need to implement multiple methods with using different inputs/outputs. Therefore a running number is needed to identify similar named methods (TBD...)
Note: Besides the information provided below, please have a look at the Guidelines (ou can download them from https://projects.avl.com/IOS_Needs_Capturing_Process-Guidelines)	
a) Describe your Engineering Method "Step-By-Step" based on what is needed to fulfil the corresponding Activity	
	
Additional fields of the sheet b) Artefact description using the lower part of the template. Each phase of your activity (start, middle, end) provides, produces or processes different artefacts. List and describe the artefacts, you want to be shared in a collaborative manner, using this sub-template so that we understand better your needs for artefacts which shall be shared between tools (look at the comments provided in "EngineeringMethod#X" sheet for more insights on what do we mean by "Generic Type" and "Required/Provided Properties").	
2	
c) Description & Interoperability Additional Constraints: Add comments but also information which are not covered by the template such as "non-functional requirements". d) Each Engineering Method needs to have its own individual sheet, therefore please copy the "EngineeringMethod#X", rename with the EngineeringMethod ID and fill out with the corresponding information.	
How to Copy the Template Sheet to create provide information about your Engineering Method	
1. Select with right click the sheet bar and select "Move or Copy"	
	
2. Select "Engineering Method #X" check the box "Create a copy"	
	
3. Right click on the new created sheet and select "rename". Enter the name of your engineering method ID <UC ID>_EM_<RunningNumber>	