 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

Milestone Report V1
D305.011

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	Milestone Report V1
Deliverable No.	D305.011
Dissemination Level	CO
Nature	R
Document Version	V1.0
Date	2014-01-29
Contact	Alberto Melzi
Organization	CRF
Phone	+39 011 9083158
E-Mail	alberto.melzi@crf.it

AUTHORS TABLE

Name	Company	E-Mail
Alberto Melzi	CRF	alberto.melzi@crf.it
Francesco Bellotti	DITEN	franz@elios.unige.it

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected
V0.1	2013-09-26	First emission	All
V0.2	2014-01-10	Internal revision	All
V0.3	2014-01-17	External revision (Daniel Hopp – DAIMLER)	All
V1.0	2014-01-22	Update after the external revision	All

CONTENT

Content of Figures

Content of Tables

1 Introduction

1.1 Role of the deliverable

The document describes the activity of the progressive evolution for the definition, implementation and integration of suited formal models, aiming at accelerating and making ISO 26262-compliant the overall engineering process of integrating critical components in a whole automotive vehicle system. This work is centered on the reference use case of an automotive climate system with safety critical implications, due to the presence of potentially flammable and toxic fluid, which is necessary for greenhouse emissions reduction.

This deliverable focuses on two main topics:

- A description of the use case and its challenges in terms of interoperability
- A preliminary definition of the IOS (InterOperability Standard) concept for the elements of the application

1.2 Relationship to other CRYSTAL Documents

This document is related to the corresponding deliverables D307.011 in WP307 (Automotive public use case) and D308.011 in WP308.

1.3 Structure of this document

This document is articulated in the following chapters, from 2 to 4:

Chapter 2: Use Case Definition and general process description for collection, formalization and harmonization of the requirements of the specific use case in view of applying a tailored ISO 26262 framework within the CRYSTAL platform.

Chapter 3: Detailed description of the use case process.

Chapter 4: Identification of the engineering methods in the engineering environment applied to the use case.

.

2 Use Case Process Description

2.1 User Story

The starting point is a current in-vehicle system that is to be upgraded.

The envisaged improvement is something quite new, at least in the automotive domain, and has some potential risks in relation to the safety of the vehicle, due to the presence of a potentially flammable and toxic refrigerant fluid, which is employed with the aim of reducing the greenhouse emissions, according to the new international normative.

The car manufacturer must formally introduce the new characteristics in the functional technical model of the upgraded system, in order to assess again its performance and to have a complete and updated model of the vehicle. But the new safety-relevant characteristics were out of the scope of the previous functional technical model and a new modeling approach should thus be developed for covering this issue.

The automotive reference for functional safety assessment is the ISO 26262 standard. Thus, in order to make the new modeling able to take into account the new safety critical characteristics and the functional safety requirements (functional safety concept) coming from the needs to comply with the ISO 26262 standard, a new system approach must be created for covering the functional safety requirements. This means that the safety-relevant characteristics must be analyzed within an appropriate framework related to the ISO 26262 requirements and linked to the original functional model.

The workflow of the ISO 26262 standard must be modeled accordingly, in order to make the process repeatable and traceable (impact analysis, change management).

After the definition of the system's safety goals and of the functional safety requirements, the functional safety concept is elaborated and verified, according to ISO 26262. Finally, the functional technical model will be updated accordingly, for performance assessment and safety goals validation, with respect to the criteria derived in relation to the functional safety concept.

2.2 Use Case Process Overview

The objective of the use case is to define the model for the concept of an automotive climate system, potentially safety critical, considering the functional safety constraints and the functional needs.

The above mentioned user story will be implemented according to the objective using the specific, real-world use case of a climate system (HVAC) with the indicated safety critical implications. The general block diagram of the system is reported in the following figure.

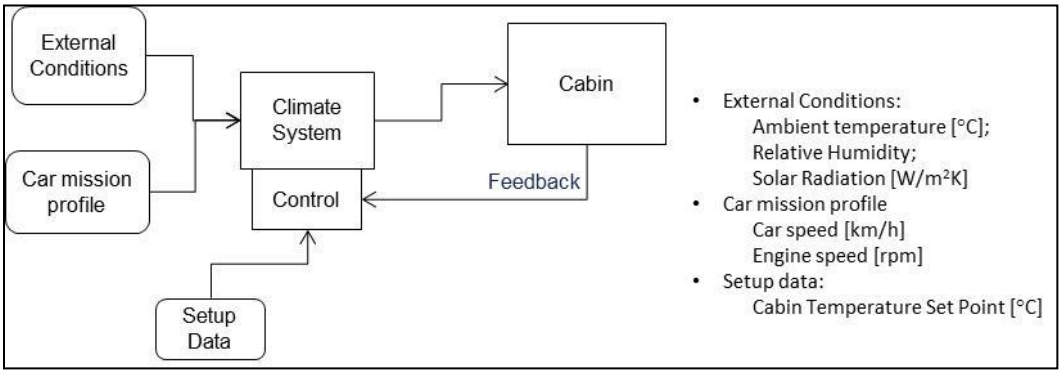

Figure 2-1: Climate system (HVAC) block diagram

The following picture depicts the system installed in a vehicle (the car body is blue, the engine system is in red, the air conditioning system is in green).

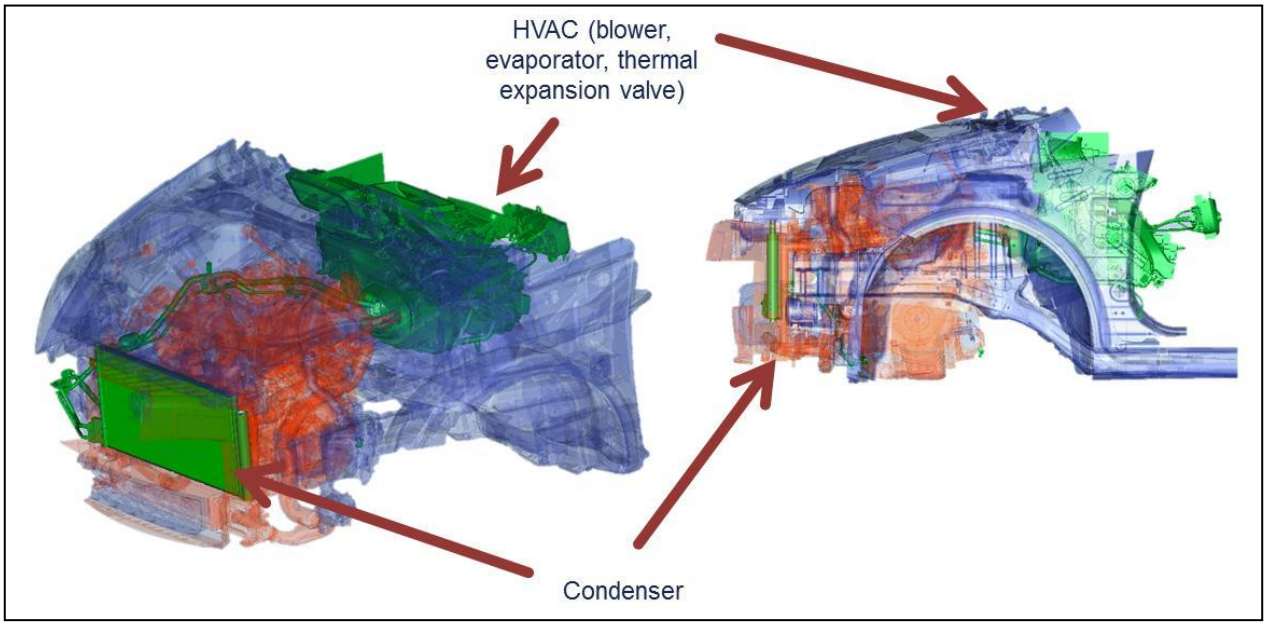

Figure 2-2: Climate system on board

Normally a climate system does not involve functional safety constraints, but in this case for environmental benefits (reducing the greenhouse effect) a new type of refrigerant fluid has been considered and the design of the application has to be revised because the new fluid is flammable and toxic.

The concept design of the system for functional needs is supported by the Matlab-Simulink tool. This implies a modeling of the system where the main target is to verify the functional needs in terms of refrigeration performance.

The running model simply receives in input the car mission profile data (e.g. these data could be the current vehicle's and engine's speed during a NEDC test), the ambient information (temperature, relative humidity, solar radiation) and the cabin temperature setting from the user (driver) command; the outputs are the temperature in the cabin (its actual value is monitored from the control as feedback) and the pressure in the circuit.

Also the new version of the system is modeled in the same way, but the new functional safety constraints concerning the possible hazards from the flammable and toxic fluid have to be considered.

In a scenario where the possible damages in the circuit can cause some leakages of the fluid over hot components (e.g. engine parts) or in the cabin, the pressure into the circuit has to be considered in the model.

This last value is the safety critical point to be kept under attention: the high pressure and high temperature section of the circuit, managed by the internal compressor, is protected by a pressure valve that monitors the current pressure value in a range from a minimum to a maximum. In a standard system this type of monitoring is managed by the engine's ECU, in order to make it effective the functionality of the compressor and to switch it off, signaling the fault, in case of any problem.

With the application of the new fluid the hazardous events eventually consequent to the circuit leakage should be covered by a redundant protection that has to be integrated into the climate system.

Therefore, the functional design of the system will be revised, considering the elements descending from the functional safety requirements derived from the application of the ISO 26262 standard criteria.

Then, the item definition of the system according to ISO 26262 has to be outlined for capturing all the aspects that imply functional safety relevance in relation to the pressure monitoring and the related scenarios of possible failure occurrence.

From this step, the hazard analysis and risk assessment of the item will determine the safety goals and the safe state to be considered. Determination will come through the analysis of the possible malfunctions associated to the pressure monitoring and their association to the safety-relevant operational situations of the system.

From the safety goals, all the functional safety requirements and the validation criteria will be derived, at the concept level. From the functional safety requirements the revision of the functional modeling will be provided, which will be tested again by simulation in order to verify the climate system performance, while the validation criteria will be applied to the safety goals considering the needs for the integration on the vehicle of the revised design according to the following picture.

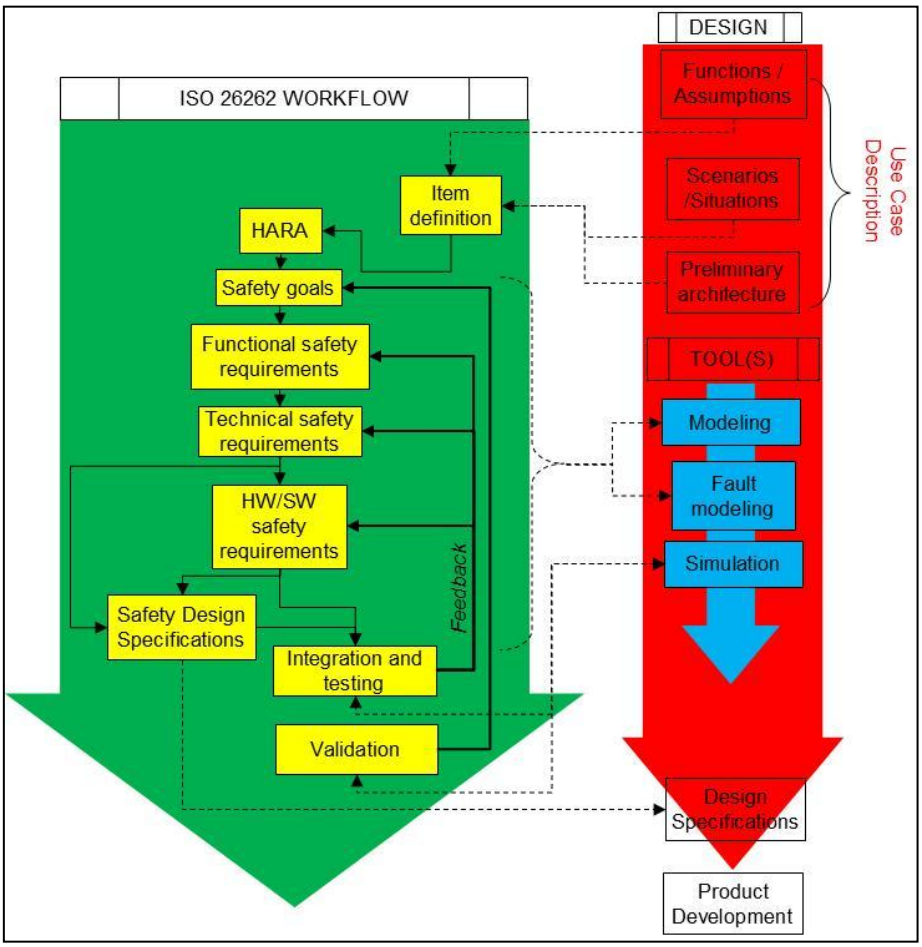

Figure 2-3: The general interactions of the processes in the use case.

3 Detailed Description of the Use Case Process

3.1 Activities

The above described use case application will consist in a process with the following activities.

Preliminary functional and architectural assumptions

This is the starting phase, where the system characteristics are defined in terms of the parameters suitable for evaluating the model performance. Additionally, considering also the functional safety possible implications, assumptions are made with respect to the target application related to a class of vehicle.

The data involved are collected into Word/Excel files.

Functional concept modeling

A Simulink model is built for simulating the expected performance. Equations are elaborated into the model and the results are compared to the performance and functional targets.

Item definition

According to the ISO 26262 standard the system is described, in relation to the preliminary functional and architectural assumptions, in terms of the functional requirements and operating scenarios that can affect the functional safety aspects. At this stage, a list of information in natural language is loaded in specific Excel templates, each describing the functional requirements and operating scenarios.

Hazard Analysis and Risk Assessment execution

Following the Item definition, the possible malfunctions related to the functional requirements are considered and cross checked with the detailed safety relevant operational situations linked to the operating scenarios.

Then, the hazards associated to the malfunctions and the related operational situations are derived: for each of these combinations, a hazardous event is defined, analyzed and classified in terms of controllability, occurrence and severity.

From these classifications, the safety goals and associated safe states, where applicable, are derived for each hazardous event.

At this stage, a specific template in Excel is populated with the overall analysis encompassing all the information related to the complete Hazard Analysis/Risk Assessment.

Functional safety concept definition

From the safety goals, the functional safety requirements are derived and, on the basis of them, the modeling is revised and the validation criteria are established.

Another Excel format collects the derived functional safety requirements and the validation criteria.

Validation by simulation

The revised modeling is tested by simulation with respect to a set of application data.

The overall process is described in the following figure.

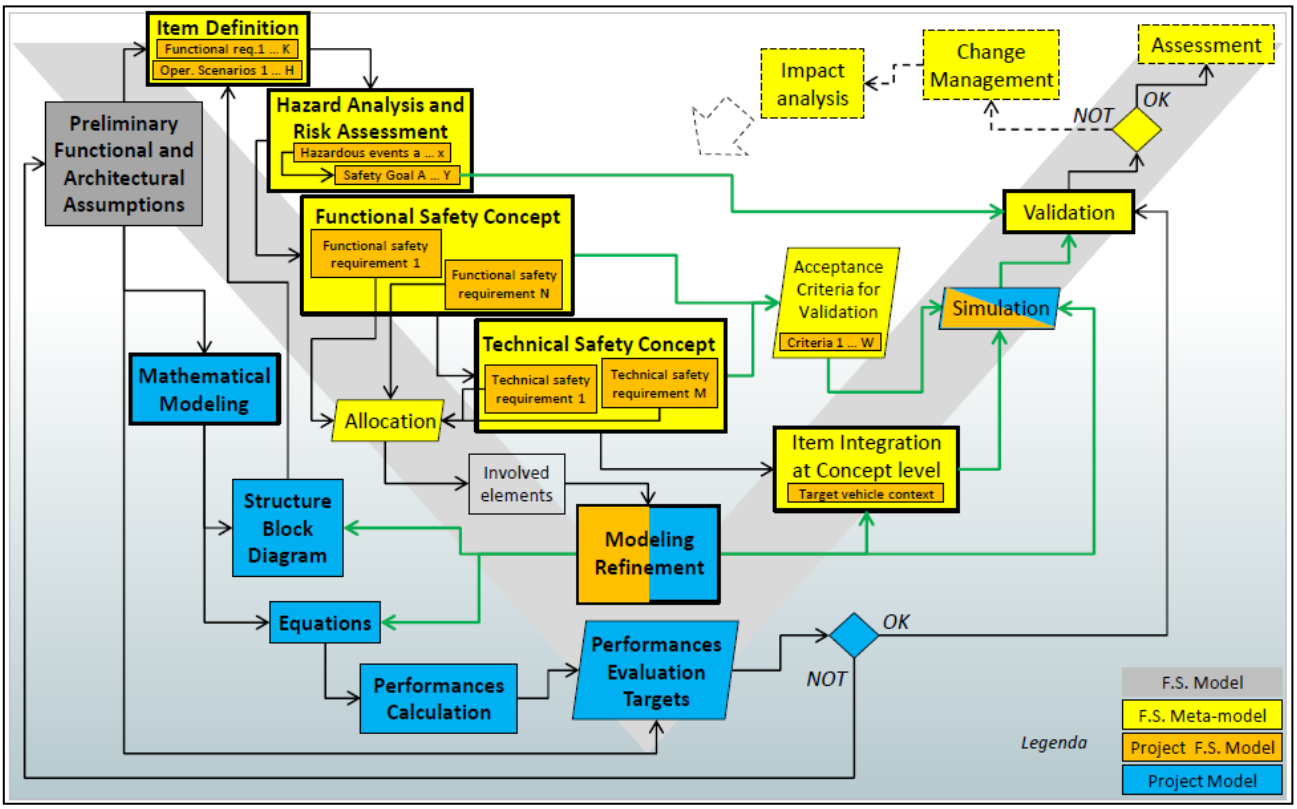

Figure 3-1: Overall process

The following picture resumes the engineering environment involved in the process.

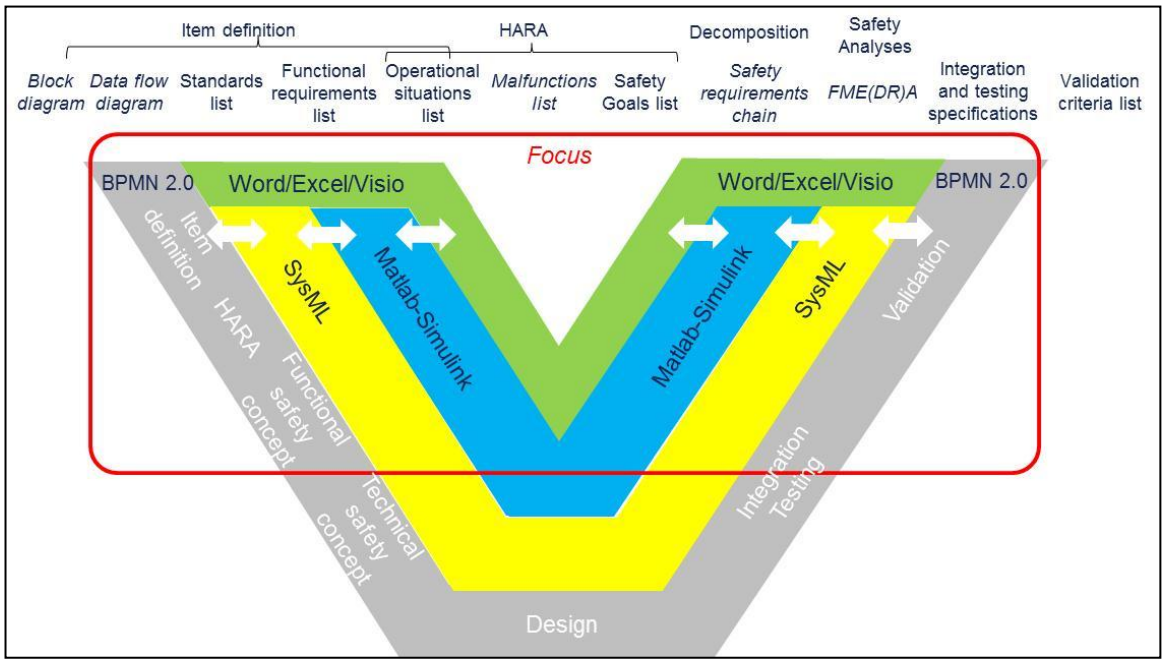

Figure 3-2: Tools and methods relationships in the process (SEE)

In the previously described process there are several challenges in terms of interoperability.

The workflow should be integrated into a semi-formal framework, using Enterprise Architect with SysML notation, for maintaining a link between the native information and the structure of the ISO 26262 modeled into the same framework. Moreover, this kind of integration allows the configuration management and change management of the various types of information, according to the standard itself.

The first step is to transfer all the Excel templates and their content into the framework, therefore the natural language information and/or quantitative data should populate through a semi-formal notation the SysML environment under Enterprise Architect tool.

The functional aspects must be linked also to the Simulink environment, where the system model can run for simulation; additionally the safety requirements coming from the semi-formal environment should be translated, where possible, into the equivalent models into the same environment, in order to run a model encompassing also the functional safety aspects.

The results of simulation should be finally compared to the functional targets, but also to the functional safety requirements should be evaluated, according to the developed framework in which the validation criteria have been also modeled from the initial descriptions. Then, the validation criteria from the SysML environment should be matched with the simulation results from Simulink.

The two different environments produce elements that, according to the management of configuration and change, must be organized and traced. To this aim, it is possible that an additional tool is needed, which should be in charge of maintaining the story of the entire process execution.

The following figures report in some details the progress of the process steps with a focus on the item definition and the hazard analysis and risk assessment phases.

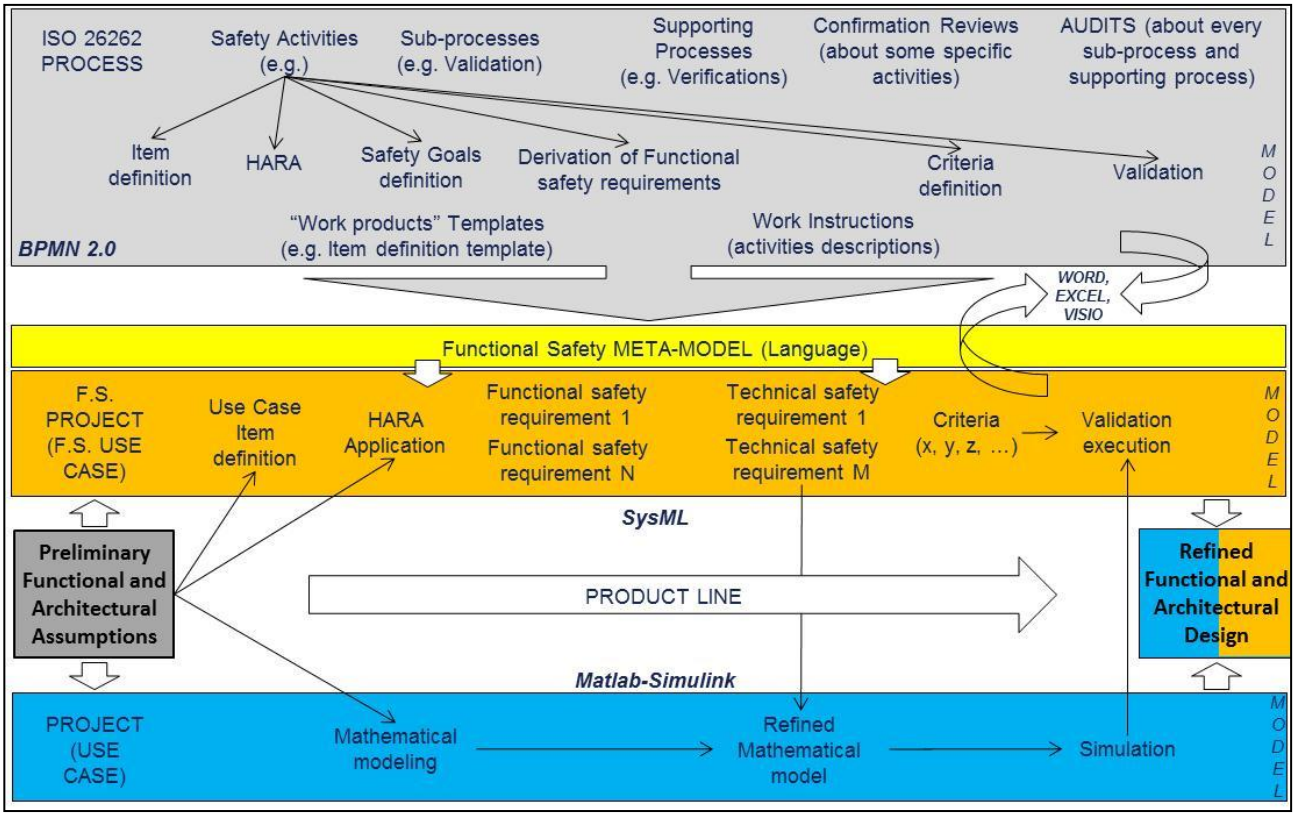

Figure 3-3: General framework

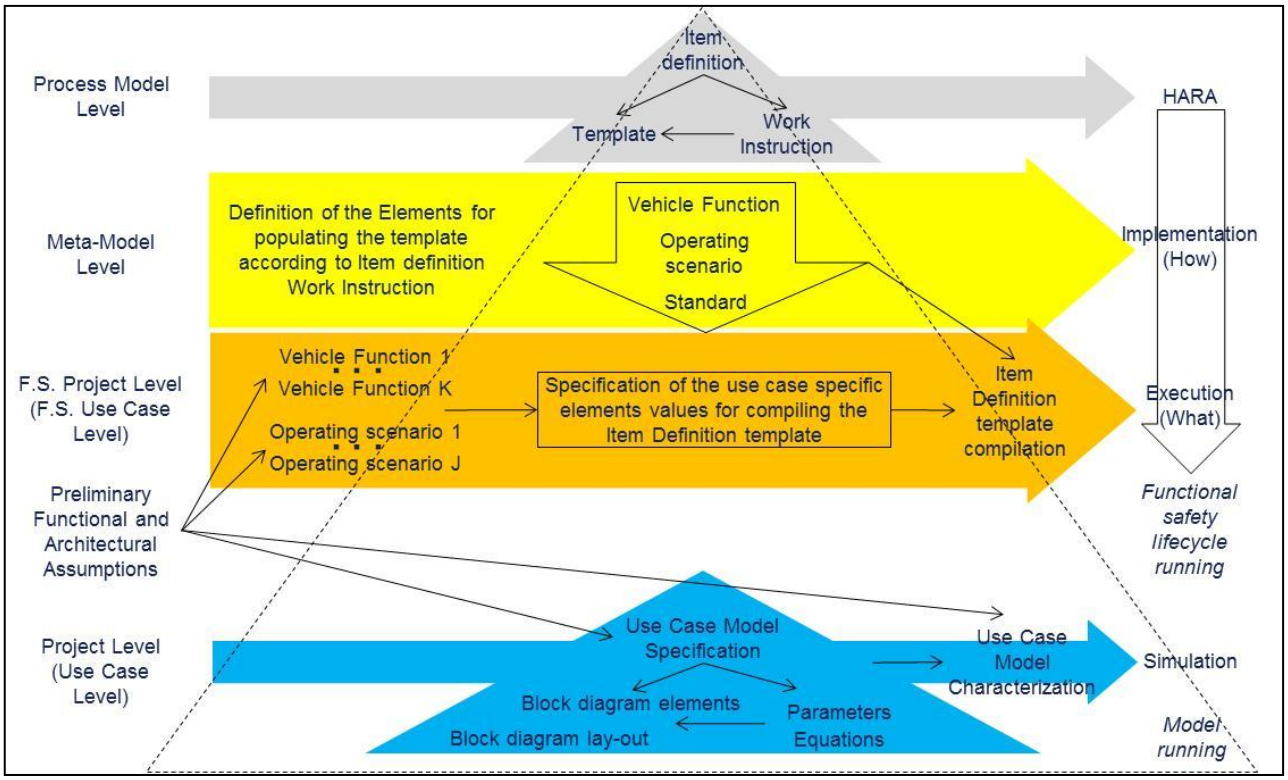

Figure 3-4: Item definition example

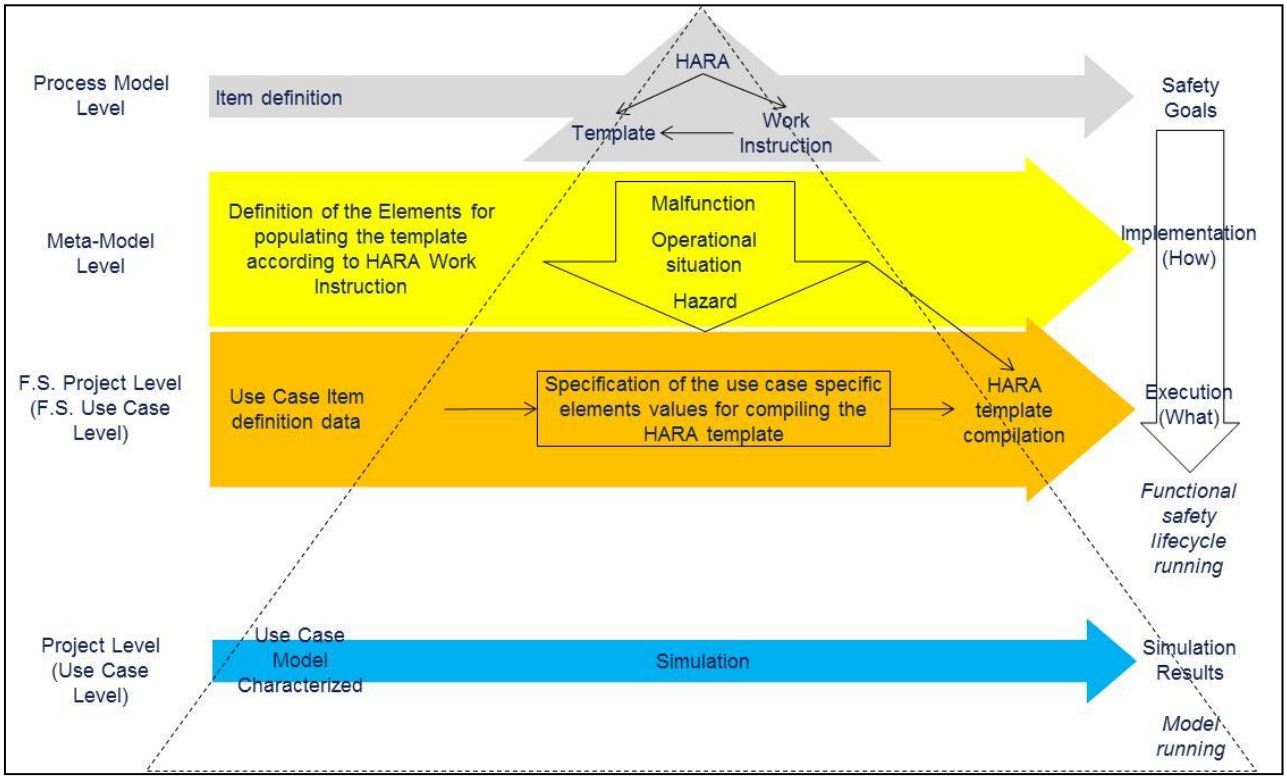

Figure 3-5: Hazard analysis and risk assessment example

3.2 Stakeholders & Roles

According to the previous Figure 2-3, continuous interactions have to be established between the general process design and the functional safety activities organized in the workflow outlined by the ISO 26262 standard. The main stakeholders and their roles are simply identified in the following table and picture.

More specializations could also be found, but for the scope of understanding of the relationships between the design and the functional safety assessment, the following are the most effective and consistent ones. Hardware and software details are not considered in the framework presented, considering only the high level structure. More specific distinctions are useless from the point of view of the process activities description finalized to the integration in a platform where the needs are mainly identified by the content of the work items and their structures/relationships.

Stakeholders	**Role**
Design Engineer	Definition of functional requirements
Project manager	Management and definition of design project
Functional safety engineer	Definition of functional safety requirements
Functional safety manager	Management of functional safety assessment

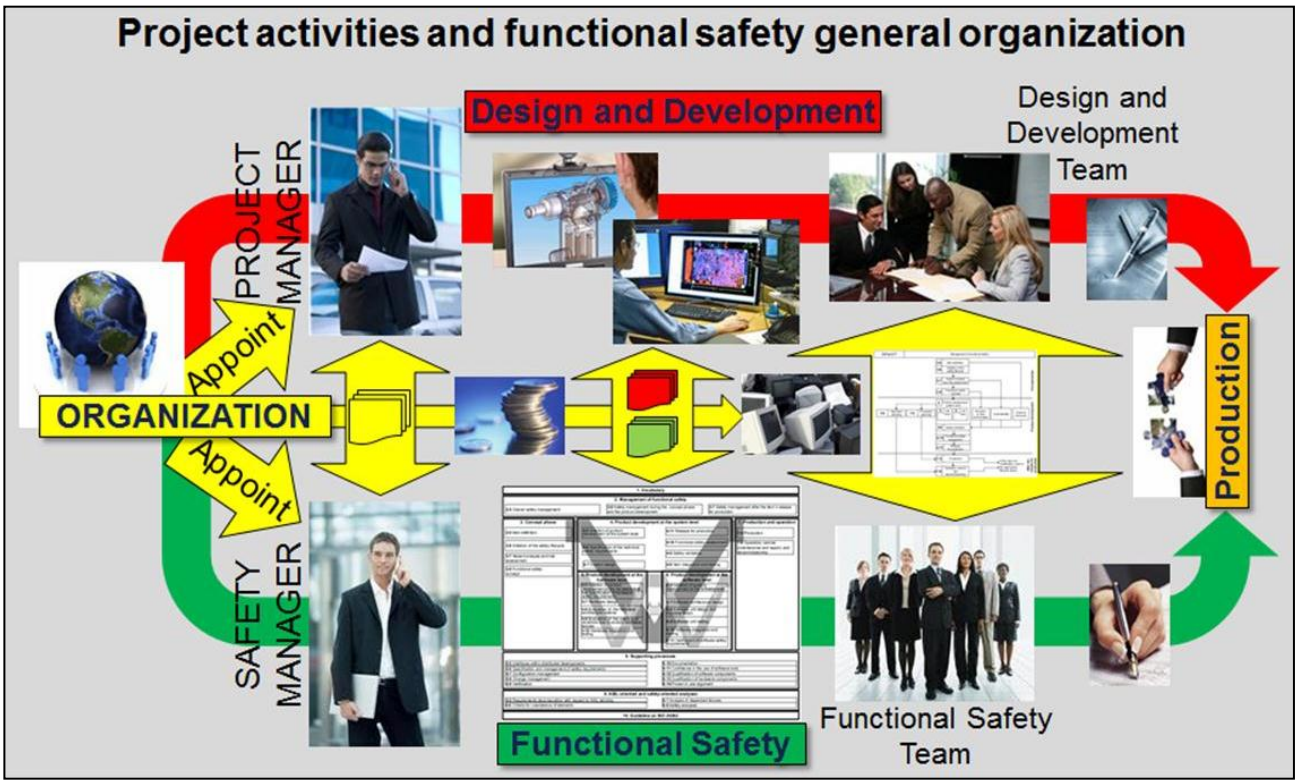

Figure 3-6: Stakeholders and roles between design and functional safety

4 Identification of Engineering Methods

The actual process needs building information in two separate tool environments: Enterprise Architect and Simulink. The first one is a semi-formal description of the application structure, while the second one is a formal mathematical-physical representation of the system.

Both the ways of modeling should be mapped between each other: the semi-formal notation describes the requirements in relation to the safety critical characteristics and can also contain the description of the other functional elements. The question is how to make an effective dependence relation between the semi-formal constructs and the formal model and this last one should be able to get the safety critical topics not yet represented.

The general method/purpose is to simulate the functional safety conformity assessment of a system, at concept level, on the base of a modeling environment.

As a first step, it is possible to run the Simulink model analyzing the performance. Then, it is necessary to define, with Enterprise Architect, a consequent structure of requirements, among which the safety relevant ones, leading to an expression in semi-formal notation of the constraints for assessing the requirements themselves. In this last step, we can find the conditions to be fulfilled for the acceptance of the system, but we have to substantiate them through a quantitative verification, that can be made with Simulink model.

With a look to the previous and the following pictures, the interaction between design process (red arrow) and functional safety process (green arrow) can be better shown by evidencing the IOS (possible/necessary) relationships.

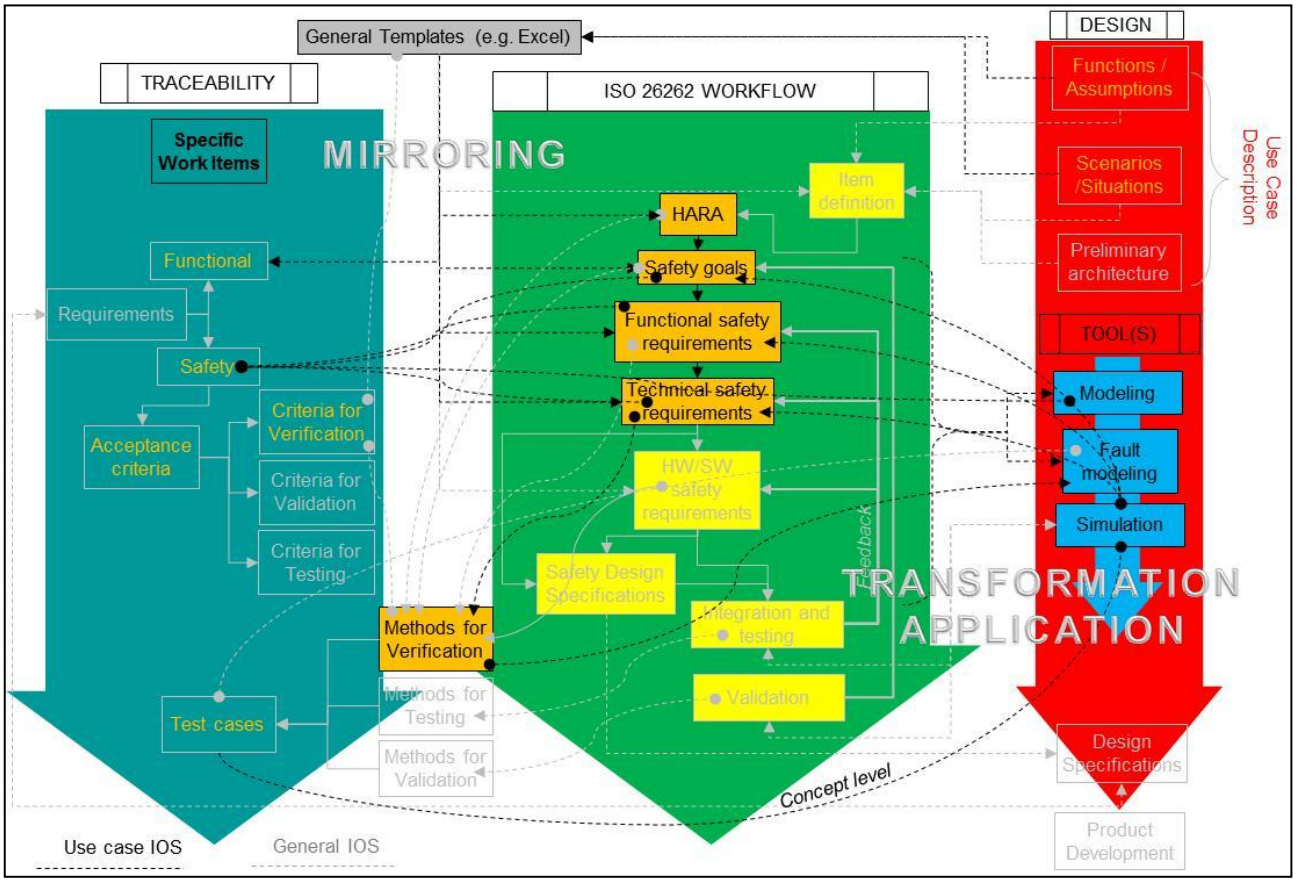

Figure 4-1: Engineering methods in the framework

In Figure 4-1 the black and gray lines distinguish the relation with respect to the current Use Case: black means covered, while gray stays for not covered but envisaged/desired for future implementation (out of scope for the moment); the dotted pattern simply indicates the absence of a direct, but envisaged/suitable/necessary link, manually operated for the moment, but also still manually operate (probably) in the future (gray color). The presence of a line, anyway (gray, dotted or not), represents the need for a link.

The “Mirroring” of work items for traceability and the Transformation/Application between models for interactions are general IOS issues for the use case, where the main challenges are to identify which links are necessary and which artifacts need to be linked and at which level of detail; this last problem is a matter of the “granularity” of the analysis required, depending at which level it is necessary to descend for having a complete description of all the necessary elements of the application under development.

In Figure 4-1, again, use case real data are indicated in orange (block and text): functional safety project model, design inputs and traceable work items, these last “mirrored” from the project model and design inputs.

“Mirroring” is something more complex than duplication: more precisely, it should be the "reflection" for traceability purposes of the "work items developed by the other frameworks (design and functional safety, this last described as in the ISO 26262 workflow). There is the possibility of providing traceability means also within the frameworks themselves, without an additional tool, according to the development stage of the related work items. This is still work in progress. The OSLC could help, but it is necessary to analyze/verify the possible impact versus the actual available frameworks. Some of the problems could be: to “rework” all the current work items and/or to redefine the design of the processes (but in the case of the ISO 26262 the process is firmly stated and cannot be "redesigned": it should be represented by the tool/tools). “Rework” could be to introduce links if it is possible, but if it not possible it means to restart quite from zero.

“Redesign” is something that can happen if the framework/tool does not match with the process: in this case, the process will have prevalence (e.g. ISO 26262: redesign not possible) and the framework unable to implement the process should be rejected.

In general a framework/tool that supplies a sufficient flexibility in the work items definition could be suitable. However, for several types of requirements, a single tool could be not sufficient: e.g. one need could be the traceability, while other needs could be related to the modeling of the process itself (e.g. ISO 26262 framework); from this last case, for instance, we could need a structure suitable for representing the requirements (but according to the standard anyway) and their relationships in a “safety case” and the traceability capability alone is not sufficient for this aim. A superior stage could be the way of integrating together modeling and traceability and to introduce a certain degree of automation where possible.

5 Terms, Abbreviations and Definitions

Please add additional terms, abbreviations and definitions for your deliverable.

CRYSTAL	**CR**itical S**YST**em Engineering **A**cce**L**eration
R	Report
P	Prototype
D	Demonstrator
O	Other
PU	Public
PP	Restricted to other program participants (including the JU).
RE	Restricted to a group specified by the consortium (including the JU).
CO	Confidential, only for members of the consortium (including the JU).
WP	Work Package
SP	Subproject
ECU	Electronic Control Unit
HARA	Hazard Analysis and Risk Assessment
HVAC	Heating, Ventilation and Air Conditioning
IOS	InterOperability Standard
ISO	International Standardization Organization
NEDC	New European Driving Cycle
SEE	System Engineering Environment
SysML	Systems Modeling Language

Table 5-1: Terms, Abbreviations and Definitions

6 References

Please add citations in this section.

[Author, Year]	Authors; *Title*; Publication data (document reference)
[ISO, 2011-2012]	Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 3, Electrical and electronic equipment; *ISO 26262 standard: Road Vehicles – Functional Safety [Part1-10]*

7 Annex I: Detailed Descriptions of the Engineering Methods

Engineering Method: UC305_CRF-EM_01					
Purpose: Simulate the functional safety conformity assessment of a system, at concept level, on the base of a modeling environment.					
Comments: -					
Pre-Condition		**Engineering Activities (made of steps)**		**Post-Condition**	
A previous model of a standard system is available, but a variant of this system has new characteristics that are safety relevant. All the functional data of the modified system are available as input, from Excel table(s) or Word sheet(s). The functional performances the system can be tested from a model simulation, but the previous model does not cover the possible functional safety implications: a modeling environment has to be built for simulating the new conditions. The functional safety requirements, according to ISO 26262, have still to be modeled.		1) Run the system model for the assessment of the functional performances. 2) Implement in SysML the model of the functional safety requirements of the system (from item definition, HARA, Safety Goals). 3) Derive the Technical safety requirements and the Validation criteria for updating the system model in Simulink. 4) Perform the Validation of the system according to the ISO 26262. Impact analysis and back to point 2 in case of not fulfilment. 5) Run the updated system model in Simulink for assessing again the functional performances. Revision of technical parameters and back to point 1 in case of not fulfilment.		Assessment simulation of performances and functional safety of the system with the new safety relevant characteristics.	
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	Input simulation model	Name	Simulink internal model	Name	Output simulation model
Generic Type: (Tool or language independend type)	Simulation model	Type:	Standard Simulink	Generic Type: (Tool or language independend type)	Simulation model
Required Properties: (Information required in interactions between steps)	- Simulation Model ID - Simulation Model Version - Simulation Model description (e.g. simulation of the functionalities of the system) - List of properties representing the inputs required by the simulation (e.g. physical and technical parameters, environment parameters)	Properties:	TBD	Provided Properties: (Information provided in interactions between steps)	List of properties representing the results of the simulation
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name	Requirement	Name	Internal model	Name	Requirement
Generic Type: (Tool or language independend type)	Natural Language Requirement	Type:	Functional safety model of the system	Generic Type: (Tool or language independend type)	Natural Language Requirement
Required Properties: (Information required in interactions between steps)	- Requirement ID - Requirement Statement in natural language - Requirement Version	Properties:	ISO 26262 compliant	Provided Properties: (Information provided in interactions between steps)	- Requirement ID - Requirement Statement in natural language - Requirement Version - Reviewing state
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name		Name		Name	
Generic Type: (Tool or language independend type)		Type:		Generic Type: (Tool or language independend type)	
Required Properties: (Information required in interactions between steps)		Properties:		Provided Properties: (Information provided in interactions between steps)	
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	