Présentation Jalon 4 du projet S2C

Référence IRT Saint Exupéry: S085L05-045
Référence IRT System X: : ISX-S2C-DOC-463
Version : V1
Date : 22/03/2023

Author(s)	*Fonction(s) & name(s)*	*IRTs Team*	*S. Delavault* *S. Guilmeau* *J.. Perrin* *N. Christofi*	*A. Dubois* *S. Creff* *M. Batteux* *S. Champion*
Checker(s)	*Fonction(s) & name(s)*	*Pilote IRT SystemX*	*A. Dubois*	
Approver	*Fonction & name*	*Chef de projet IRT Saint Exupéry*	*J. Perrin*	

Fin de projet S2C

- Jalon J4 -

23 mars 2023

Programme de la journée

09h00 **Conférence - Présentation des résultats S2C** *- Auditorium -*

12h15 **Déjeuner** *- Salle réception -*

13h30 **3 Ateliers Démonstrations & Echanges :**

- Processus global de cohérence SE-SA *- Salle 2 -*
- Guide MBSA *- Auditorium -*
- Cohérence MBSE / MBSA *- Salle 1 -*

15h45 ***Pause*** *- Salle réception -*

16h00 **Synthèse de la journée et Perspectives** *- Salle réception -*

16h30 **Visite libre du musée Aéroscopia** *- Musée -*

Agenda de la matinée - Conférence

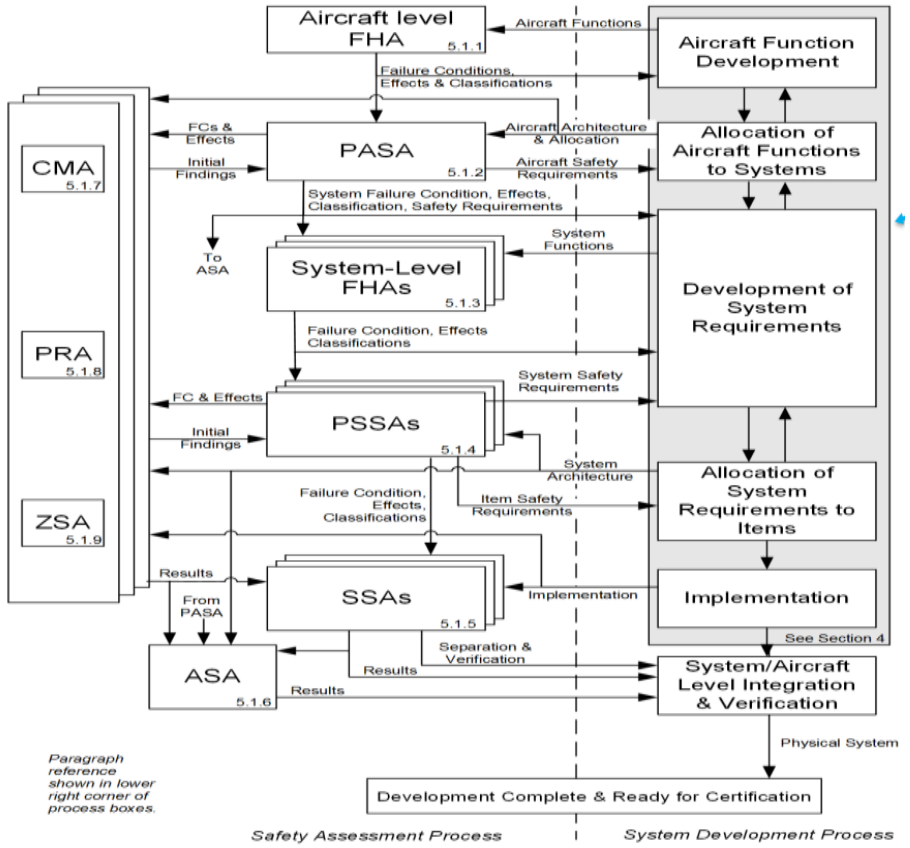
9h00	Présentation de la journée
9h05	Introduction de la problématique
09h15	Processus global de cohérence SE-SA
10h00	Méthodologie de MBSA
10h30	La cohérence entre MBSE et MBSA
11h15	- Pause -
11h30	Organisation du projet et synthèse des résultats
12h15	*Départ vers le déjeuner*

Avec la participation de la FIT, de l'ANR et de la Presse !

Problematic Introduction

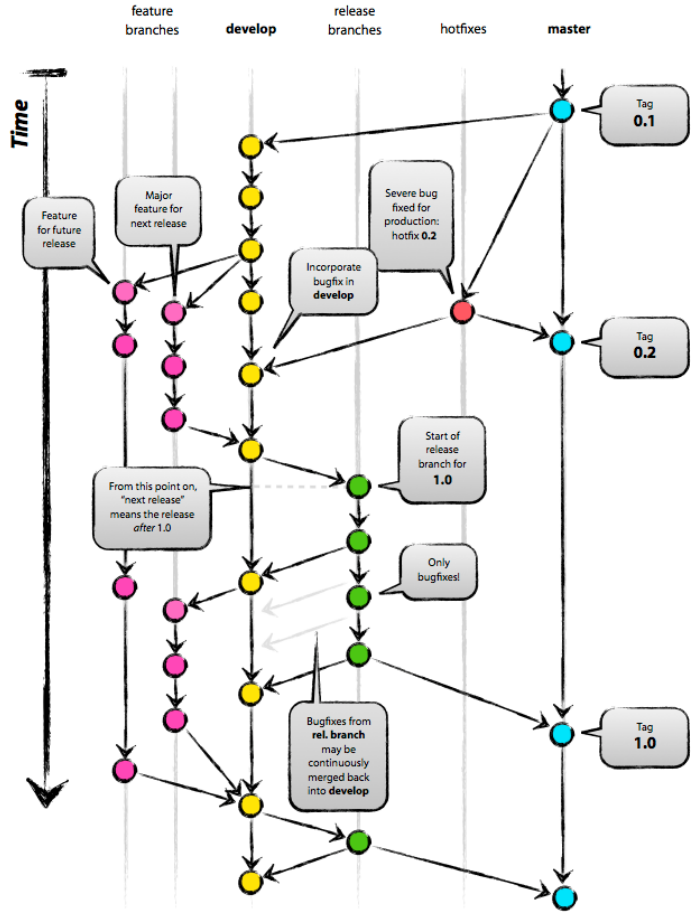
Origin of the need of consistency

- Theory : One top-down approach



From SAE ARP4761 / Eurocae ED-135

- Real life: Multiple iterations from past projects



http://nvie.com/posts/a-successful-git-branching-model/

Origin of the need of consistency

Reference

- Safety analyses are based on a set of requirements defined by a given architecture
- Assumptions made by each domain should be shared
- Waiting for the final architecture is too risky

Iterations

- Split the work into predefined scopes
- Changes may occur in previous scopes so impact analysis is important
- New scope can jeopardize previous results -> automation of non regression tests is mandatory

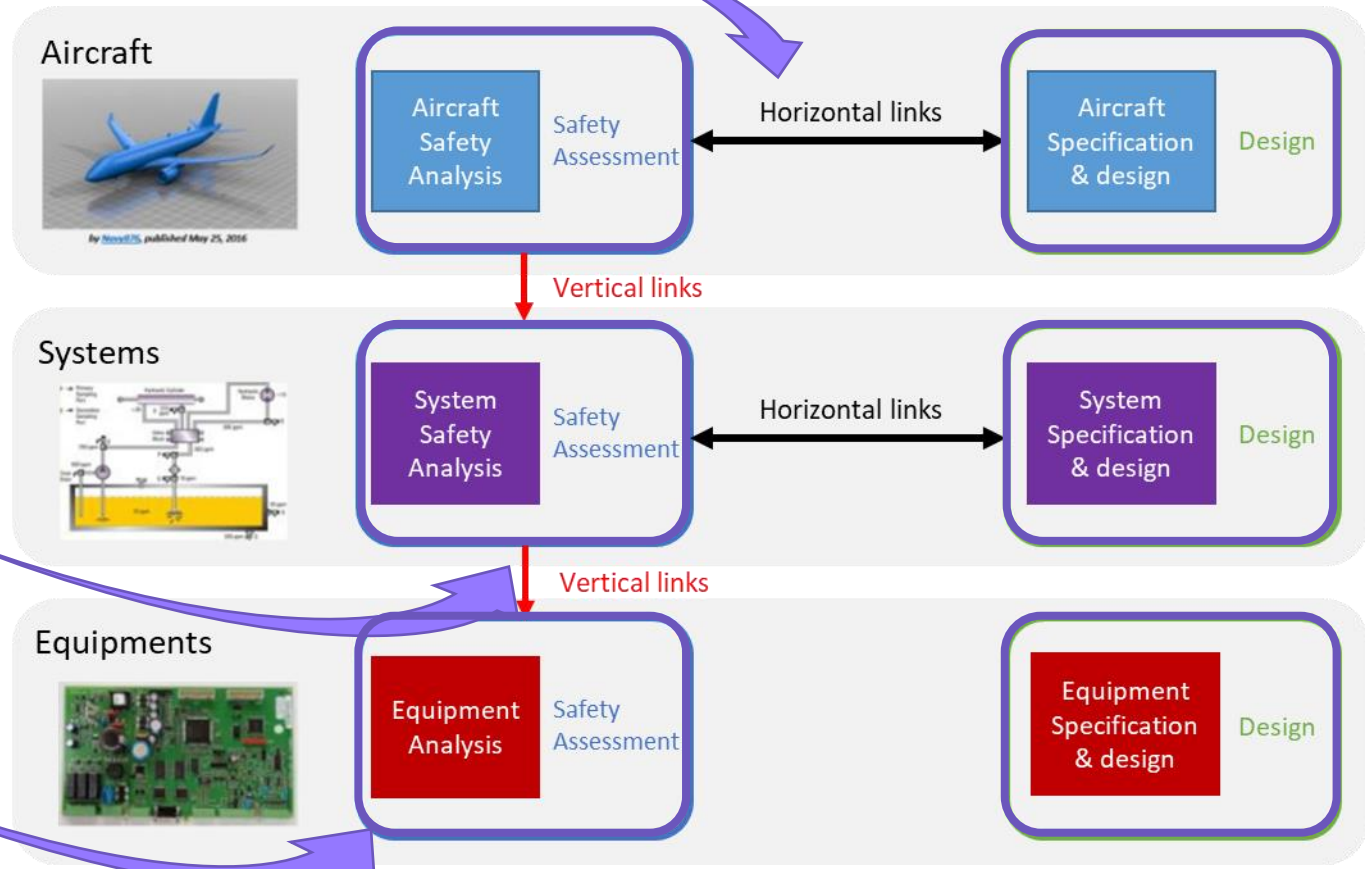
Complexity

- More and more complex systems with highly configurable software
- (Dys)Functional Behaviour is hard to handle
- Need of dynamic analyses (e.g. simulation)

Origin of the need of consistency

On Aircraft development context : Each boxes and links are concerned by consistency.

Reference
Iterations
Complexity



S2C Project Approach

Objectives :

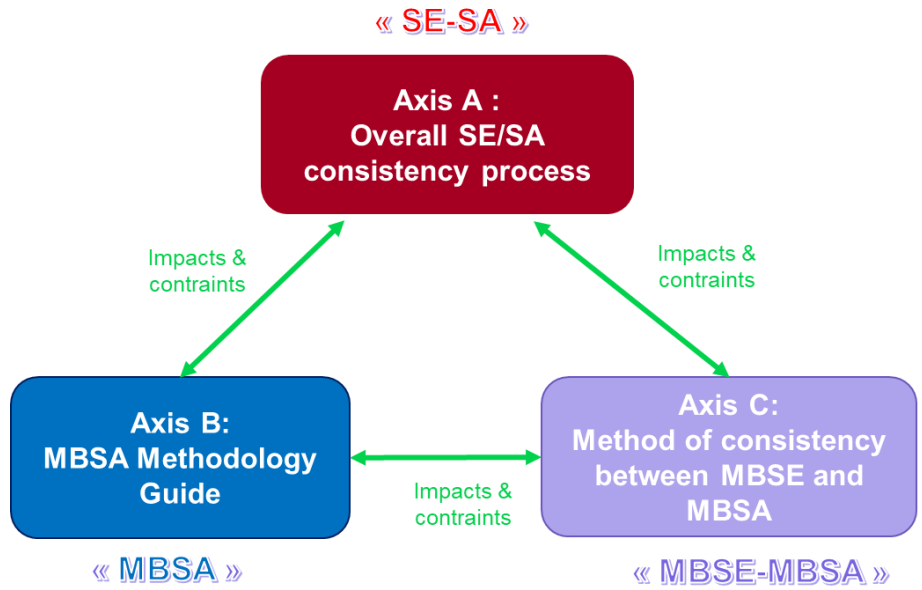
To define **processes, methods and tools** that allow to guarantee that **safety analyses** and system modelling done by system architect **(MBSE)** are **consistent**, in a context of numerical continuity, **during all iterative development cycles** of products and systems, and answering to **certification constraints**.

S2C Project Approach

The project has followed 3 axes to address the problematic at different level :

Axis A	« SE-SA »	Overall SE/SA consistency process
Axis B	« MBSA »	MBSA Methodology Guide
Axis C	« MBSE-MBSA »	Method of consistency between MBSE and MBSA

- The 3 axes are inter-related.
- They have illustrated their work on a **common Use Case**.
- They have also produced a **State Of the Art** at the beginning of the project.

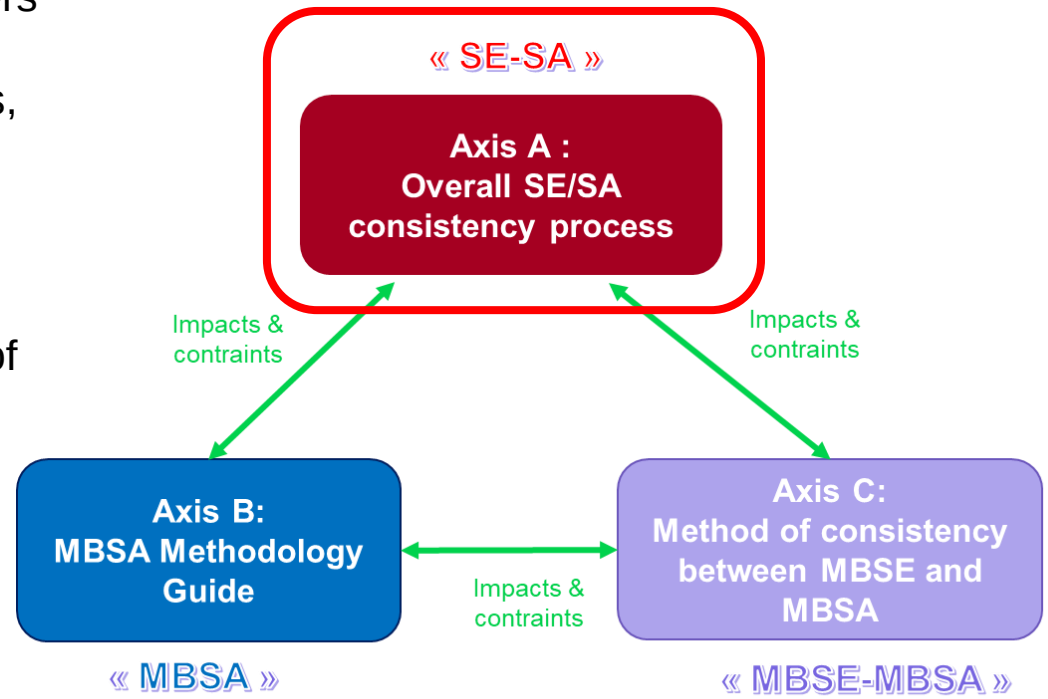


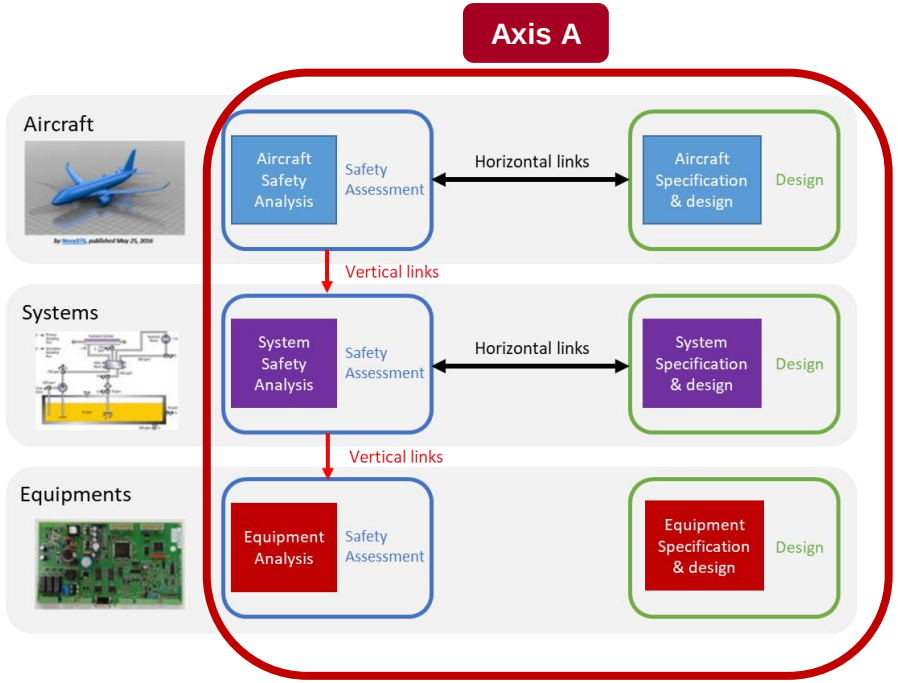
Axis A - Overall SE/SA consistency process

Overview of Axis A

Objectives :

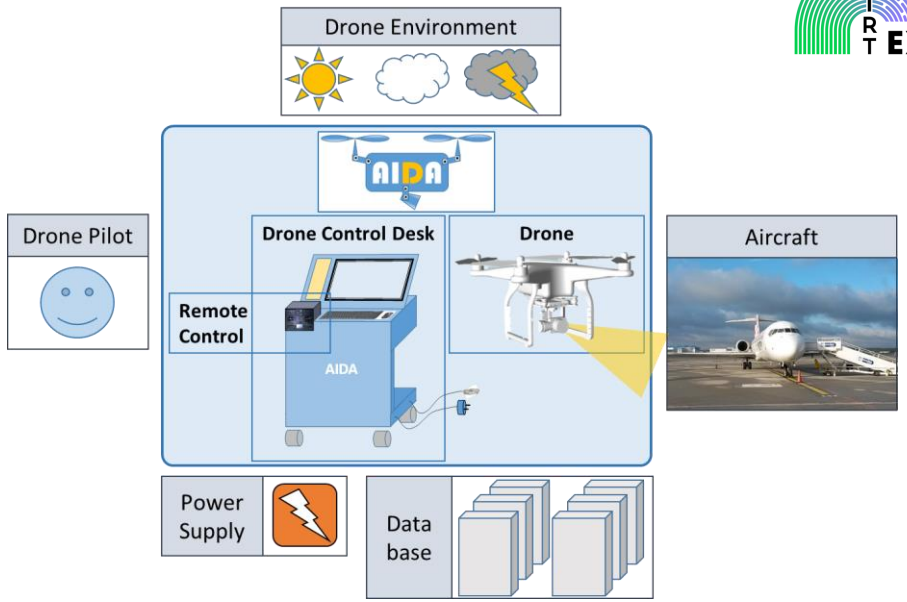
- Provide a **global SE/SA process** between System Engineers and Safety analysts (SE/SA) to :
  - ensure **global consistency** of Systems/Safety outputs, **all over systemic levels**;
  - maintain and guarantee the consistency **in time (dynamic consistency)**
- Provide **Tools** to support this process
- Enrich the AIDA use case to support the different activities of the project





Reference Use Case - AIDA

- Drone system for pre-flight inspection
- Open Source Study Case from MOISE project
- For S2C, Failure Conditions inspired by aeronautical regulations have been fixed



- **Study case content:**
  - **SE** : architectural models on Capella (static) and on Cameo (executable), associated documentation, requirement set (partial) at different levels. The system has been decomposed artificially to be in line with SAE ARP4754 / Eurocae ED-79 layers: Aircraft, Systems, Items.
  - **SA** : MBSA SimfiaNeo model based on functional architecture and associated documentation, SdF deliverables of SAE ARP4761 / Eurocae ED-135 process (FHA, PSSA, FMEA/FMES,…).
- **Use in the project**:
  - **Axis A** : SE-SA process illustration. At the end of the project, the maximum coverage possible of the process is envisaged.
  - **Axis C** : used for the PoC of SSR method (full coverage, limited to functional architecture), and for experimenting with validation of BSR method (use of behavior requirements in shape of truth tables) and BCC method (use of executable model in Cameo).
  - **Axis B** : realization of models with different tools for the physical architecture to be done following the created guide recommendations.

FRENCH INSTITUTES OF TECHNOLOGY

AIDA Open Source Use Case : https://sahara.irt-saintexupery.com/AIDA/

Axis A Roadmap

Deliverable release

2019 2020 2021 2022 2023

Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1

SE/SA Process

- L1.1 V1 (deliverable)
- L1.1 V1 (process model)
- First formalization of an SE/SA and consistency process (BPMN, draw.io)
- Formalization of the SE/SA process in VP (multi view) modeling
- Partners practices analysis
- Checklist for SE/SA review
- L1.1 V2 (deliverable + model)

Traceability plan

- Generic traceability plan
- Traceability tools cartography
- L1 – COTS analysis and CR spec
- Application of traceability plan on AIDA UC
- Plan Optim.
- Feed back

POC dynamic consistency management

- internrship : dynamic consistency
- POC stearing
- Impact study
- L1.3 POC
- Tool specification & implementation

Compatibility

- internrship : compatibillity tool
- Generalization to SE/SA context

Agenda

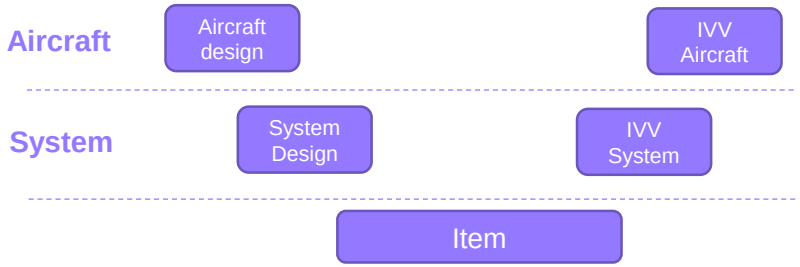
- **SE/SA Consistency Process**
- **Traceability plan**
- **POC dynamic consistency management**
- **Compatibility**

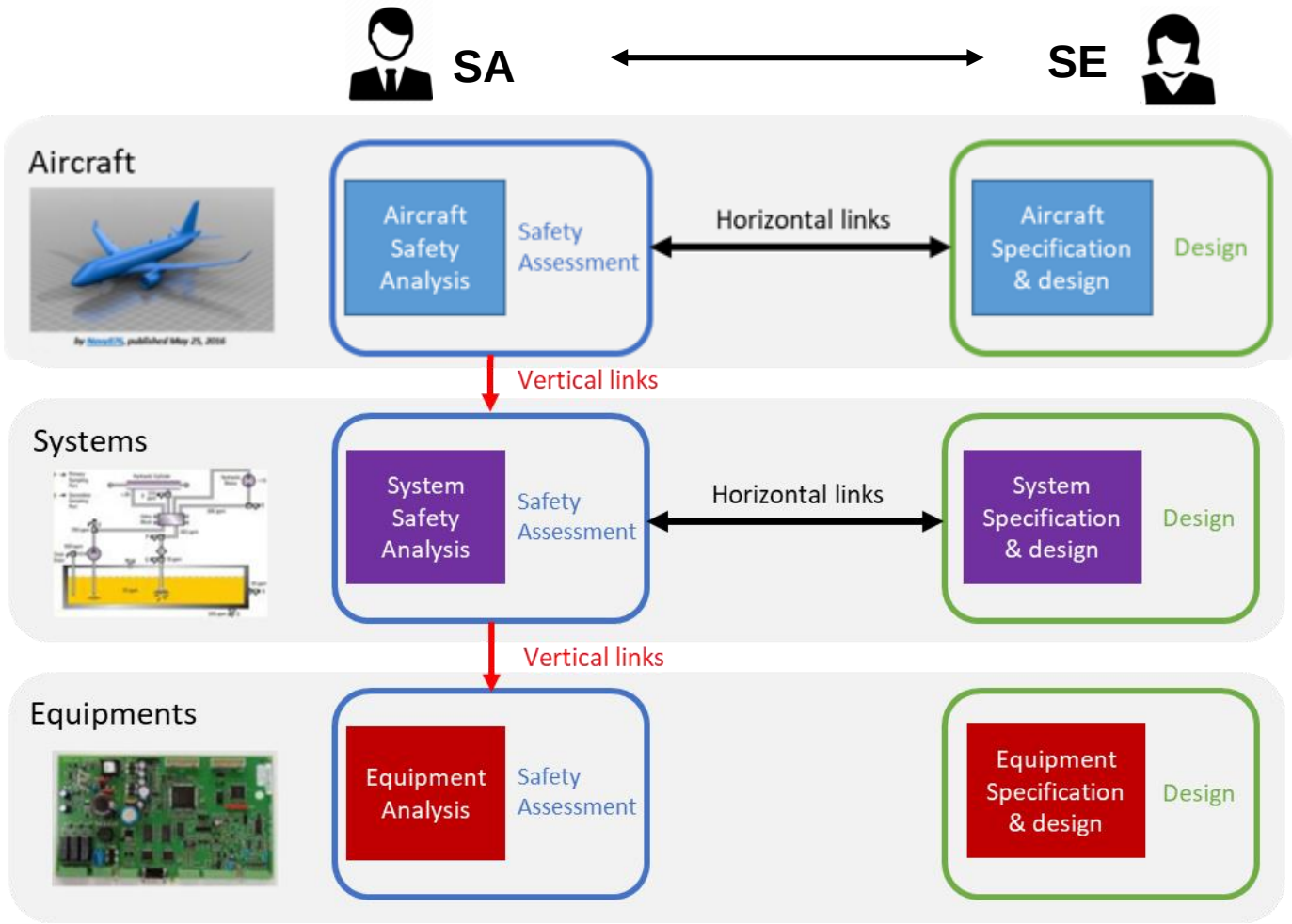
Short overview
(details during WS)

Axis A - SE/SA Consistency Process

SE/SA consistency Model

- The Model describes:
  - The collaboration between the SE and the SA teams (data, activities and interactions between the System Architect and the Safety Analyst...)
  - In the aeronautic context (process guided by ARP)
  - For the different systemic levels: aircraft manufacturer, system provider, equipments (items)
  - Among the different phases of development





SE/SA consistency Model

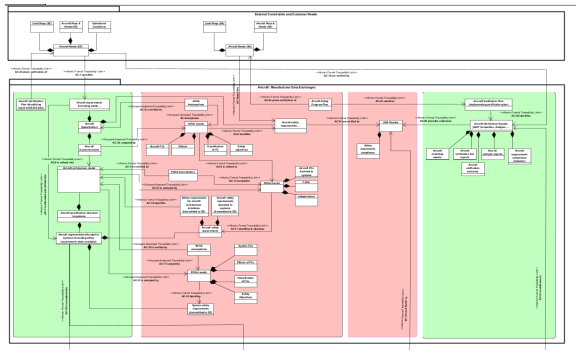
• The model is « high level » and quite generic, so that it can be instantiated in different domains.

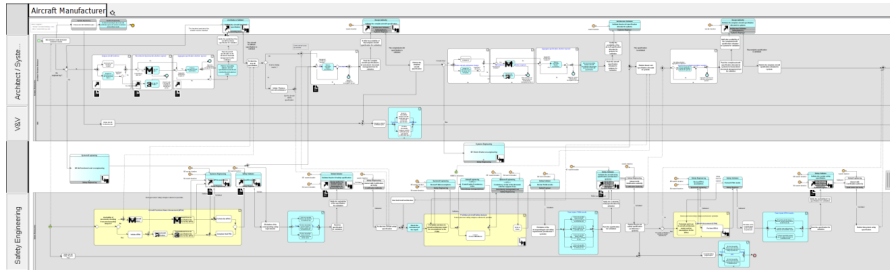
• The model focuses on the consistency activities (or patterns) that have to be led at each level to ensure global consistency :

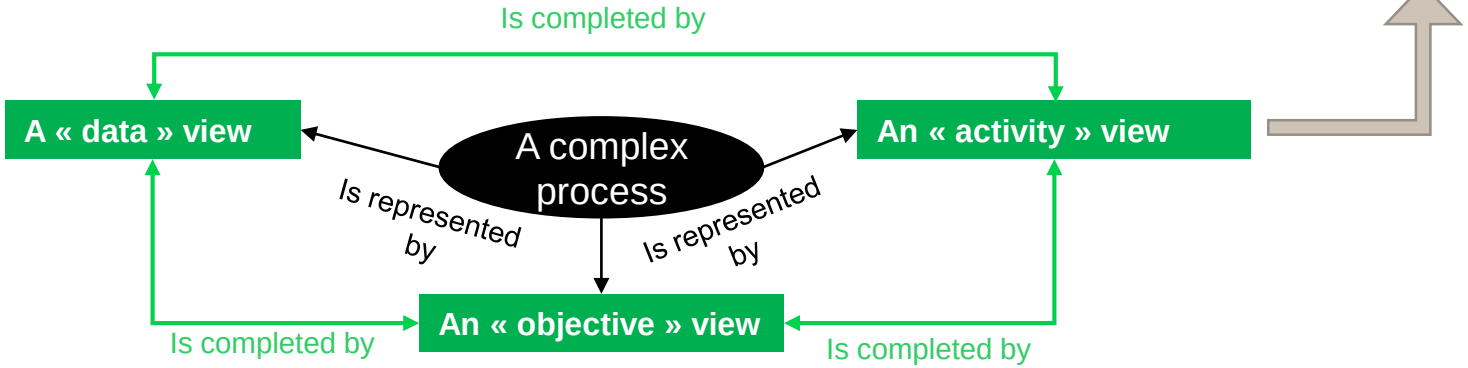
- Activity to detect inconsistencies (review)
- Activity to solve inconsistencies (formalism, syntactic or semantic recommendations for instance, « iteration » process)
- Activity of configuration management
- Activity of traceability
- Activity of assumptions management
- Activity of document aggregation (for a consolidated and consistent specification)
- Activity of MBSE/MBSA consistency management (Axis C)
- Activity of MBSA (guidance for modelling) (Axis B)

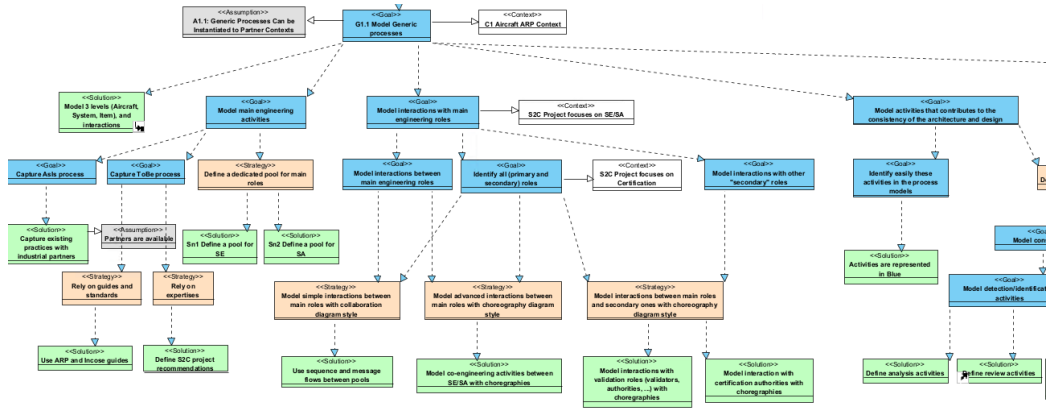
SE/SA consistency model

- **Strategy : multi-view modelling**





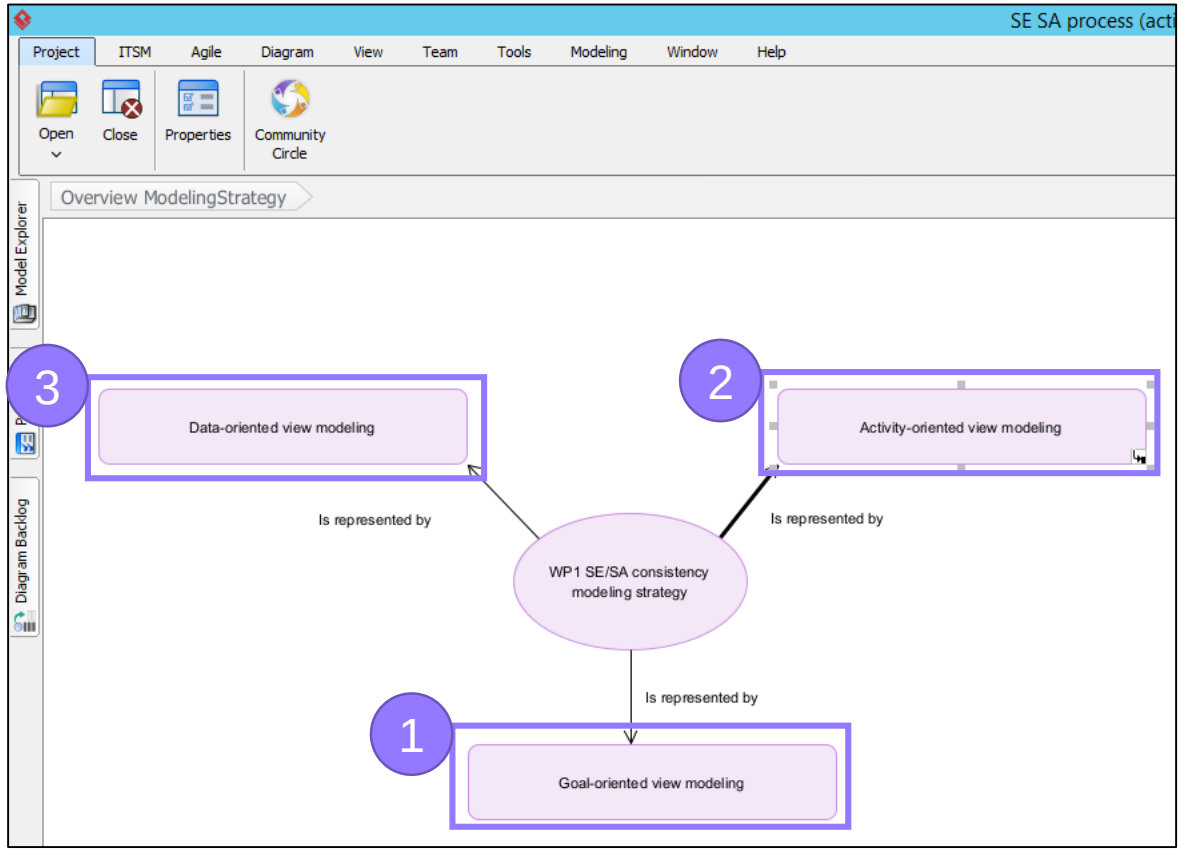




The SE/SA consistency model... in Visual Paradigm

Use of Visual Paradigm (Visual Paradigm Project Viewer):

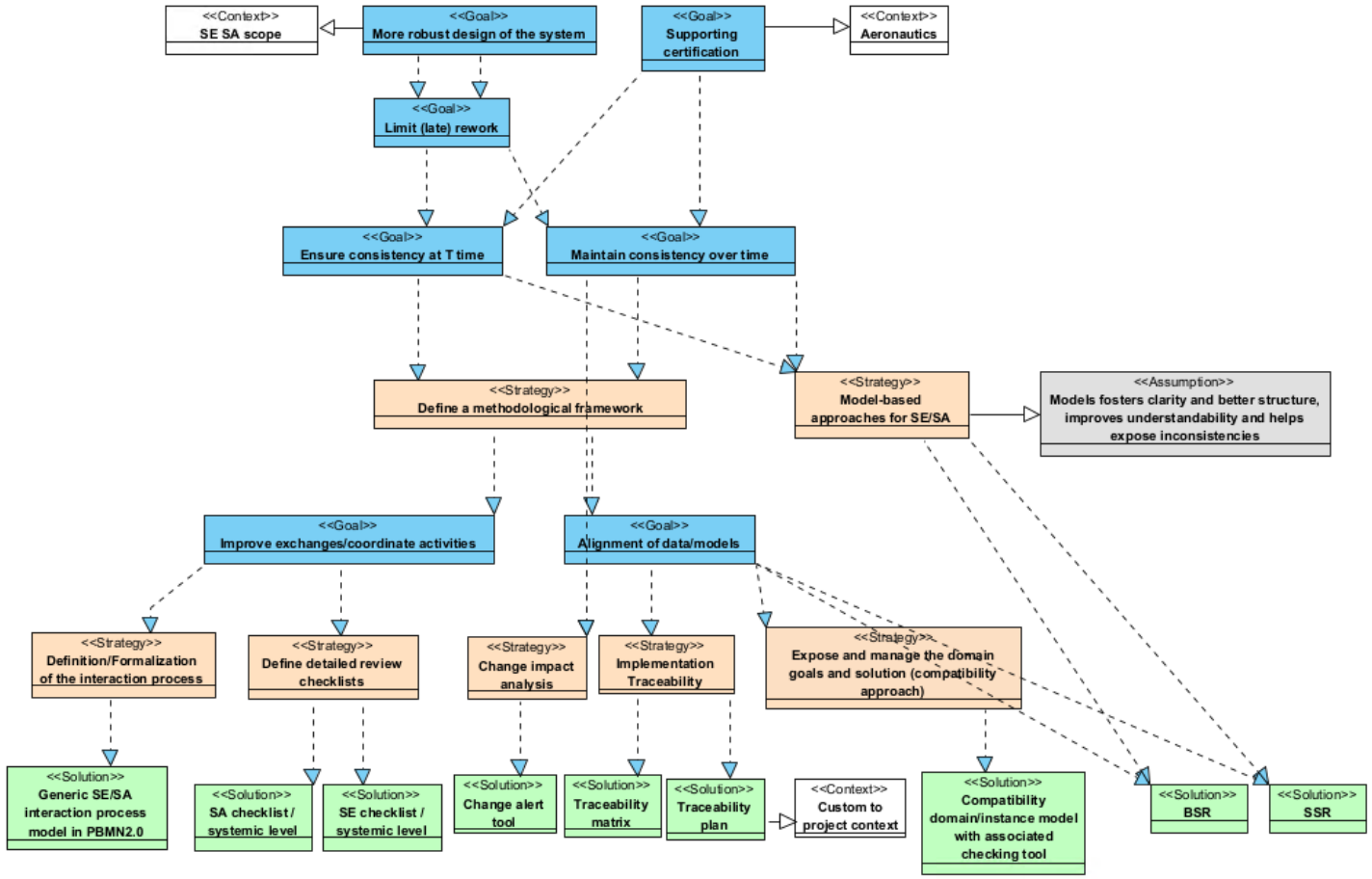
- Three views
- Direct access to these views from this overview panel



SE/SA consistency Model: Objectives view

- Different views to describe

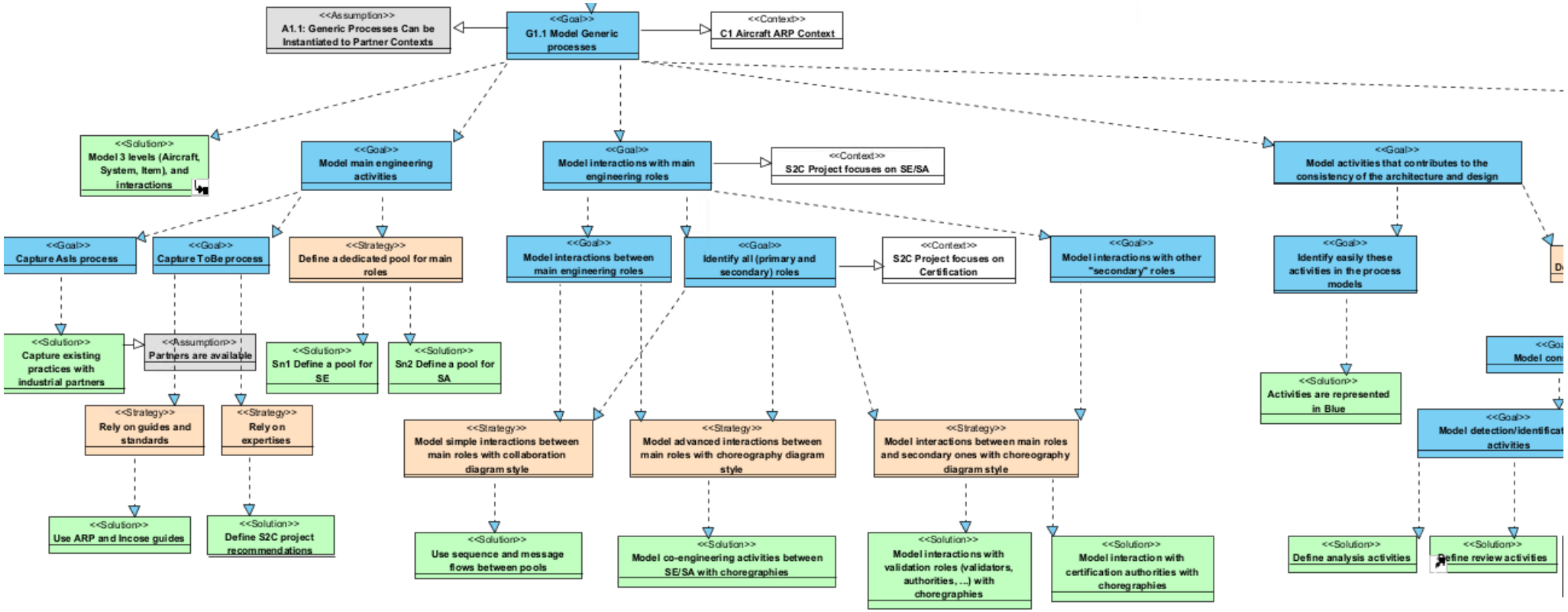
The objectives focused by the SE/SA consistency, the strategy and means to reach these objectives on S2C project.



SE/SA consistency Model: Objectives view

- Different views to describe

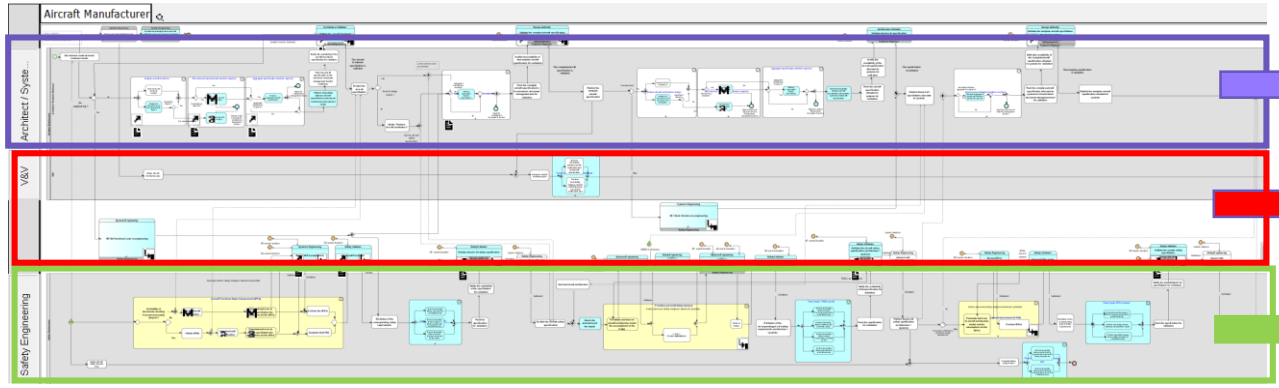
how the **global consistency Process** is constructed (keys for understanding).



SE/SA consistency Process: Activity view

- 3 models are available, modeled in BPMN2.0:
  - 1_SE SA process (Activity-driven A/C Manufacturer) diagram

Aircraft



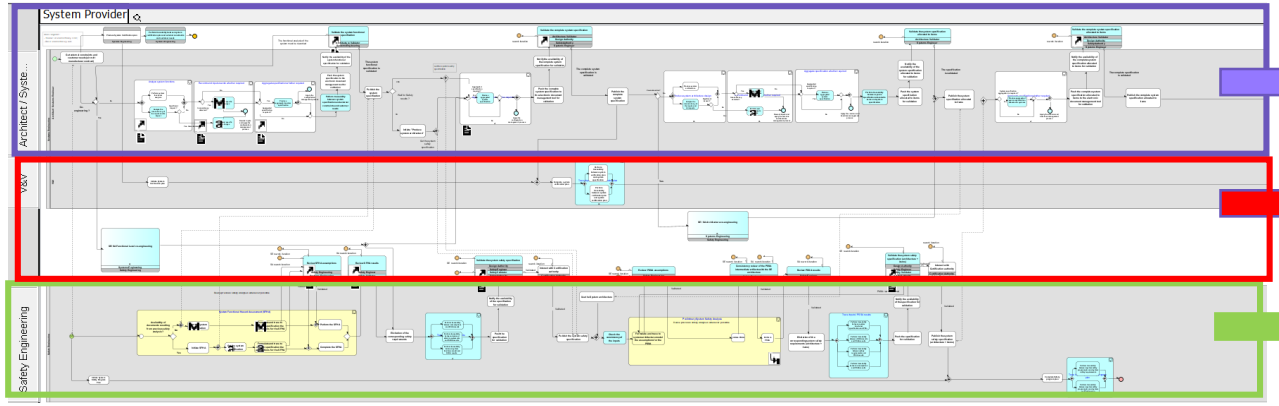
Description of SE activities

Description of SE/SA interaction activities

Description of SA activities

  - 2_SE SA process (Activity-driven System Provider) diagram

System



Description of SE activities

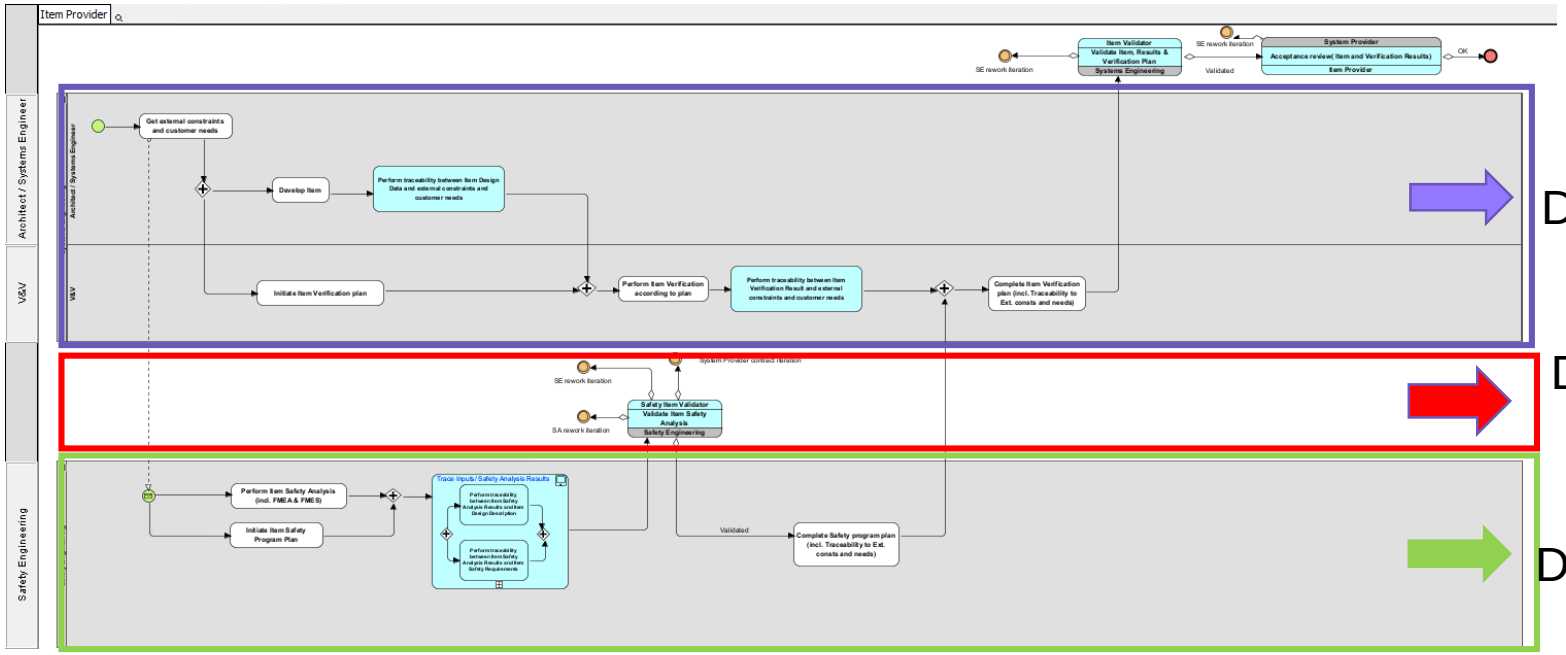
Description of SE/SA interaction activities

Description of SA activities

SE/SA consistency Process: Activity view

- 3 models are available, modeled in BPMN2.0:
  - 3_SE SA process (Activity-driven Item Provider) diagram

Item



Description of SE activities

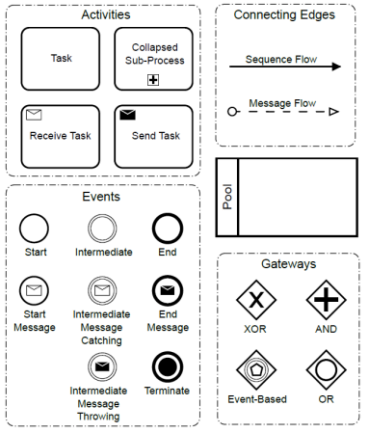
Description of SE/SA interaction activities

Description of SA activities

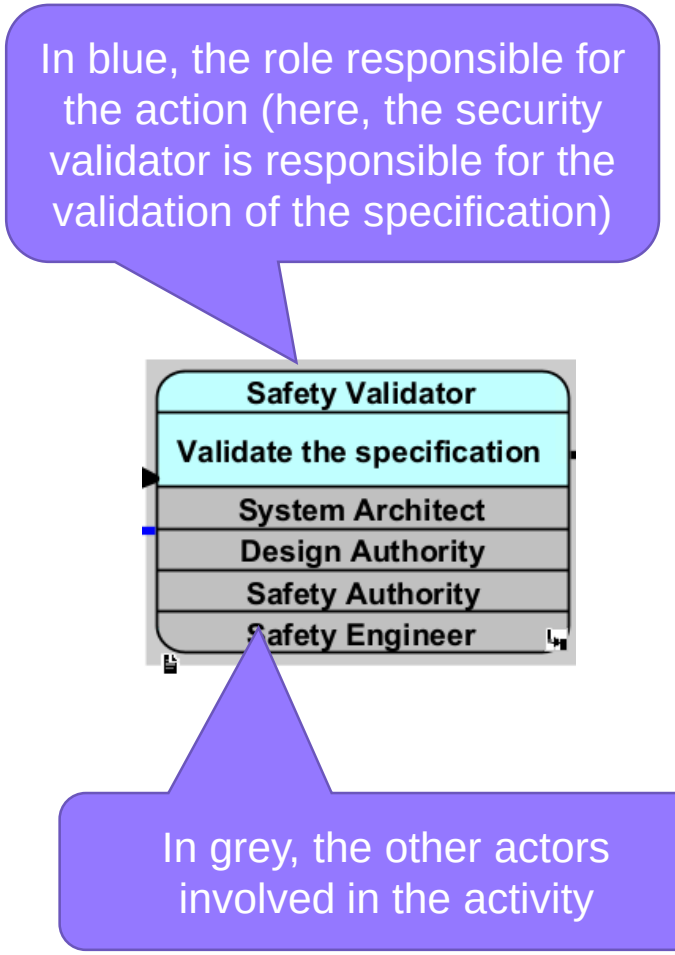
Use of BMPN2.0

- Use of an SE and SA pool to delineate the activities performed by the SE team or the SA team

- Use of current modeling item
  - Events to make a process start, or end or to model intermediate event
  - Activities and sub processes to describe the tasks performed on SE and SA side
  - Gateway to model different possible ways of working, depending on the internal work habits of the industrial partners

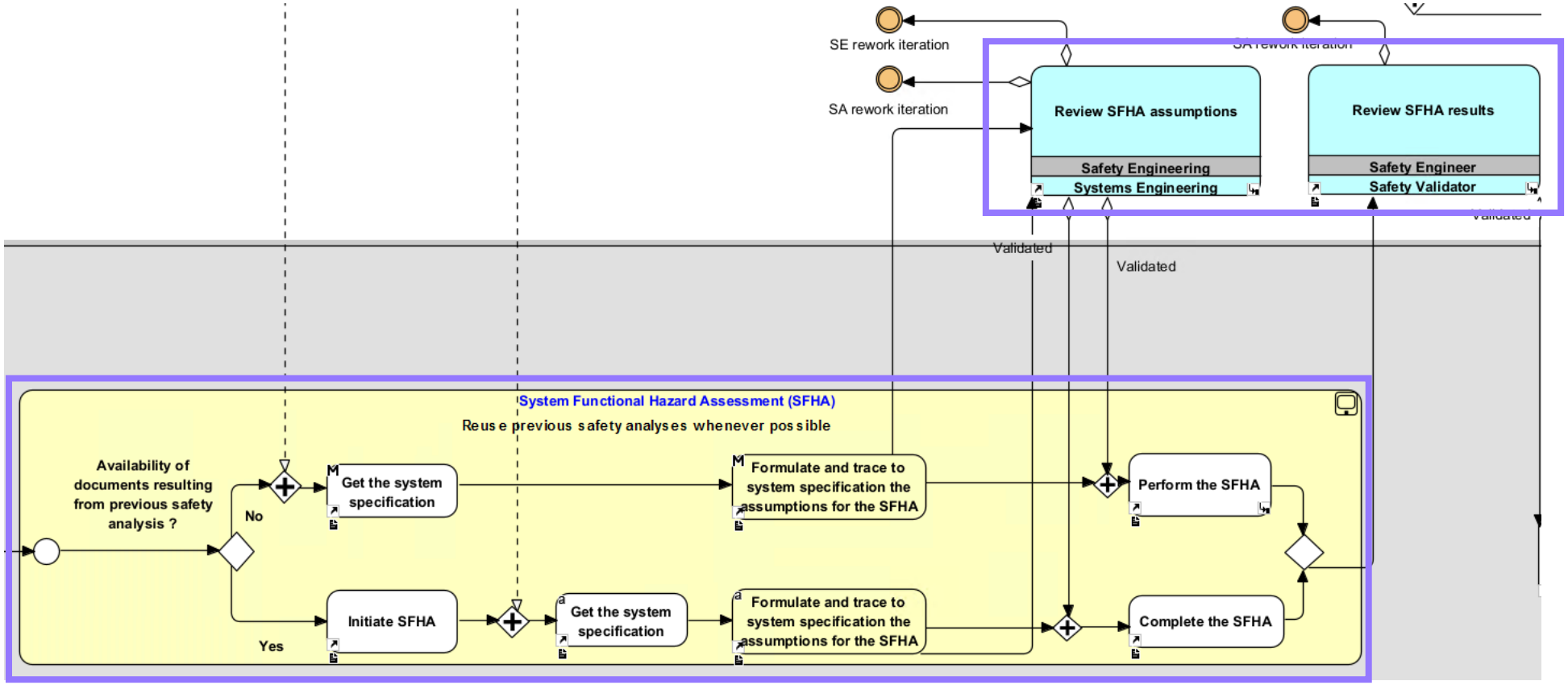


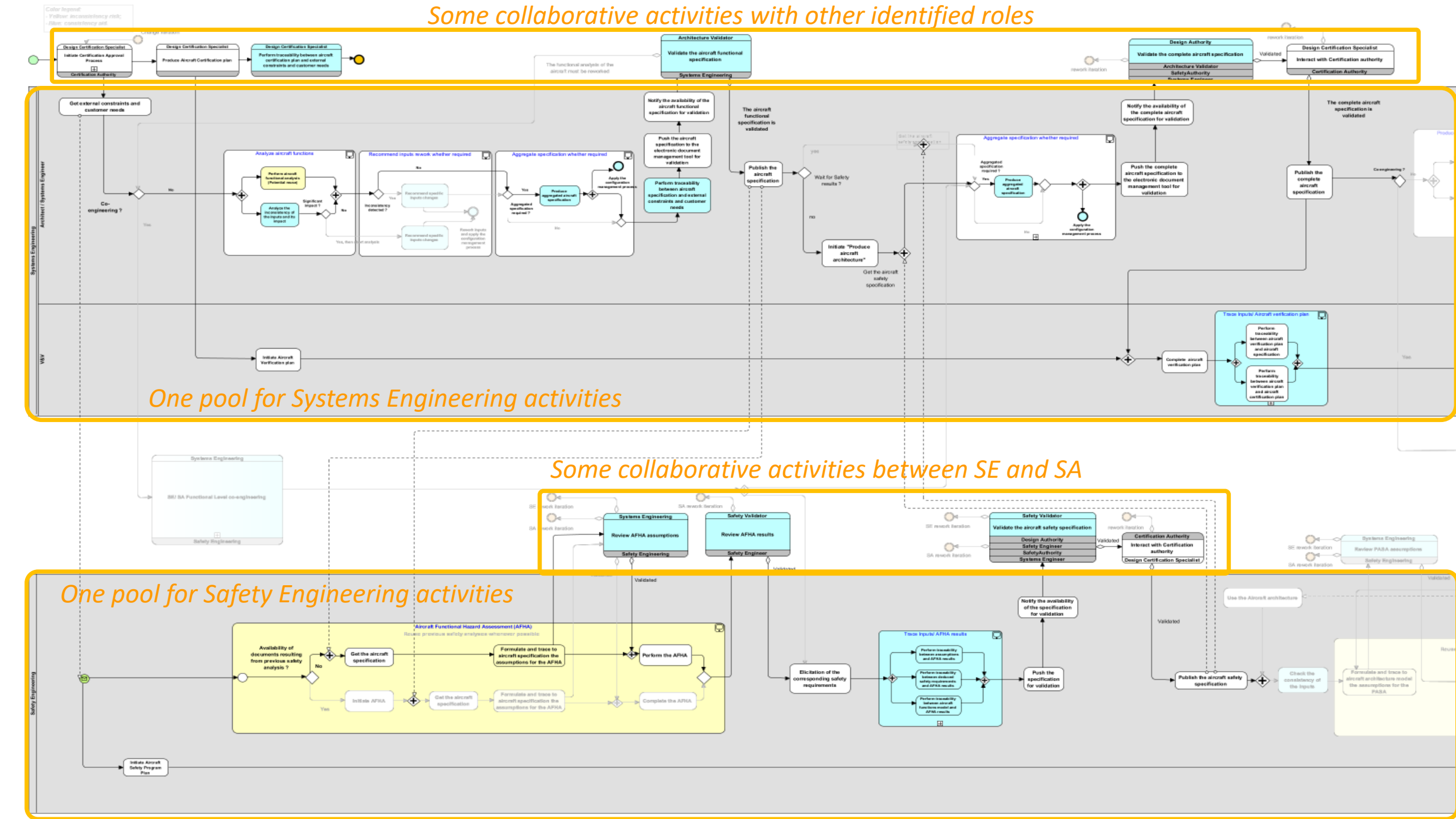
- Description of the interaction or collaborative activities between people by the use of choregraphy, between the different pools



Use of a color code

- Blue for the consistency activities
- Yellow for the activities that can induce inconsistencies (often due to “reuse”)



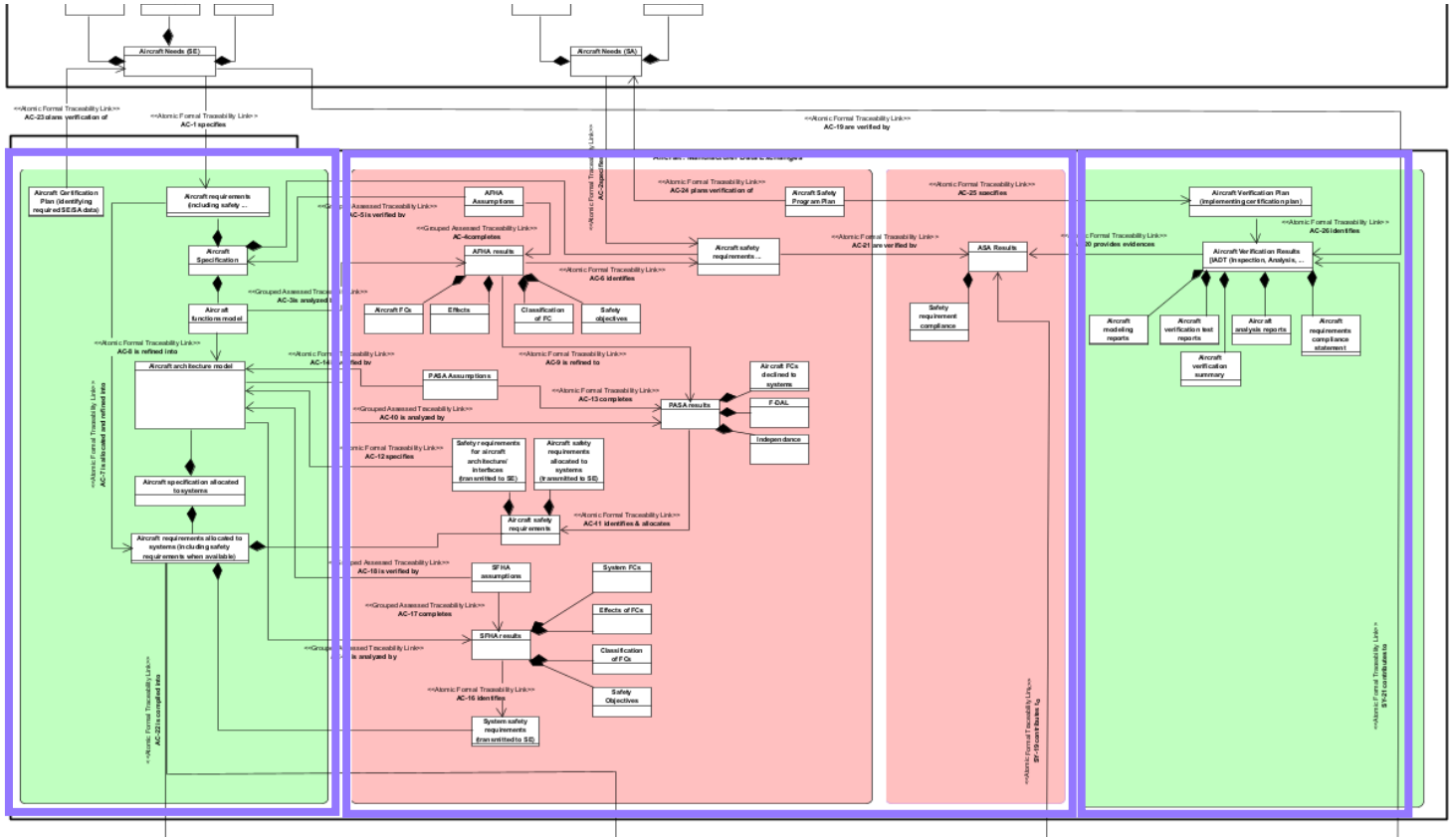

Some collaborative activities with other identified roles
One pool for Systems Engineering activities
Some collaborative activities between SE and SA
One pool for Safety Engineering activities

Axis A – Traceability plan

SE/SA consistency Method: Data & traceability view

Traceability:

- Production of a SE/SA Data Model and its generic traceability plan (UML Class diagram), for each systemic level (and between systemic level)
- And all over V cycle



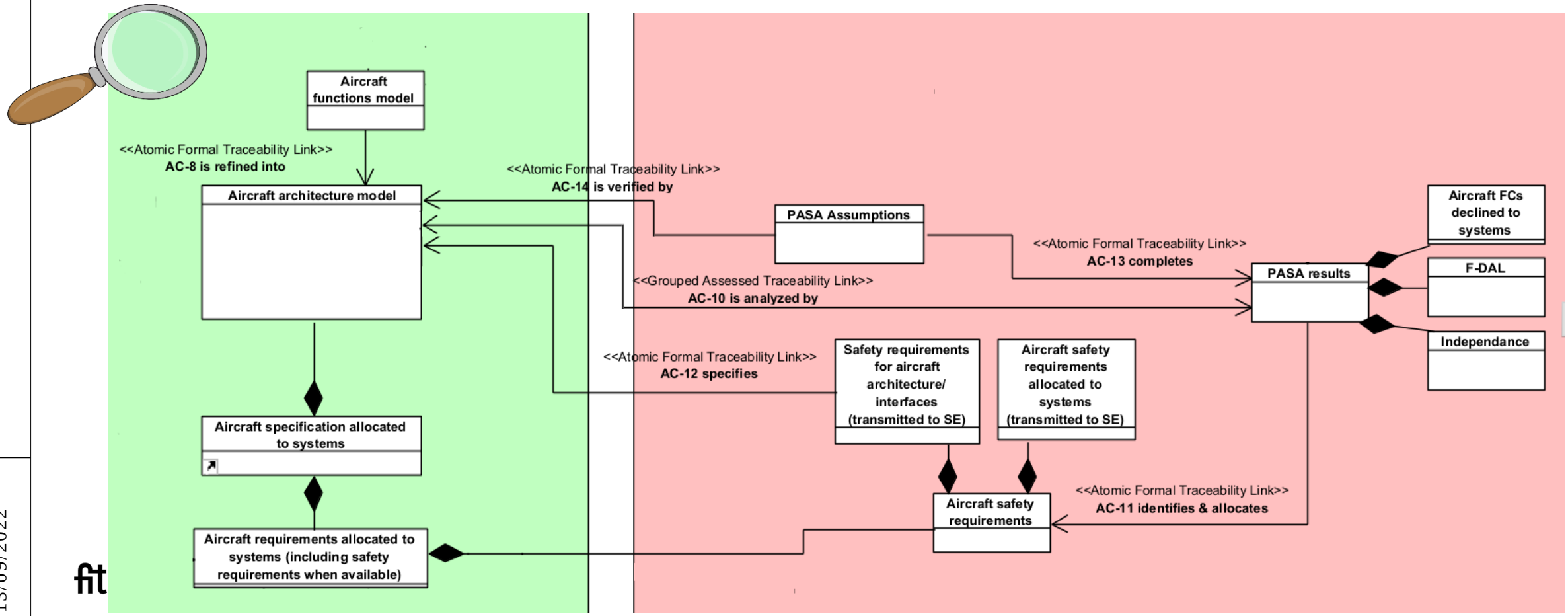
SE Data (green)

V&V (SE) Data (green)

SA Data (pink)

SE/SA consistency Method: Data & traceability view

- Description of each link : atomic or grouped traceability, traceability rationale, semantic of the link…
- Composition link ◆ or relation link ⟶



SE/SA consistency Method: Data & traceability view

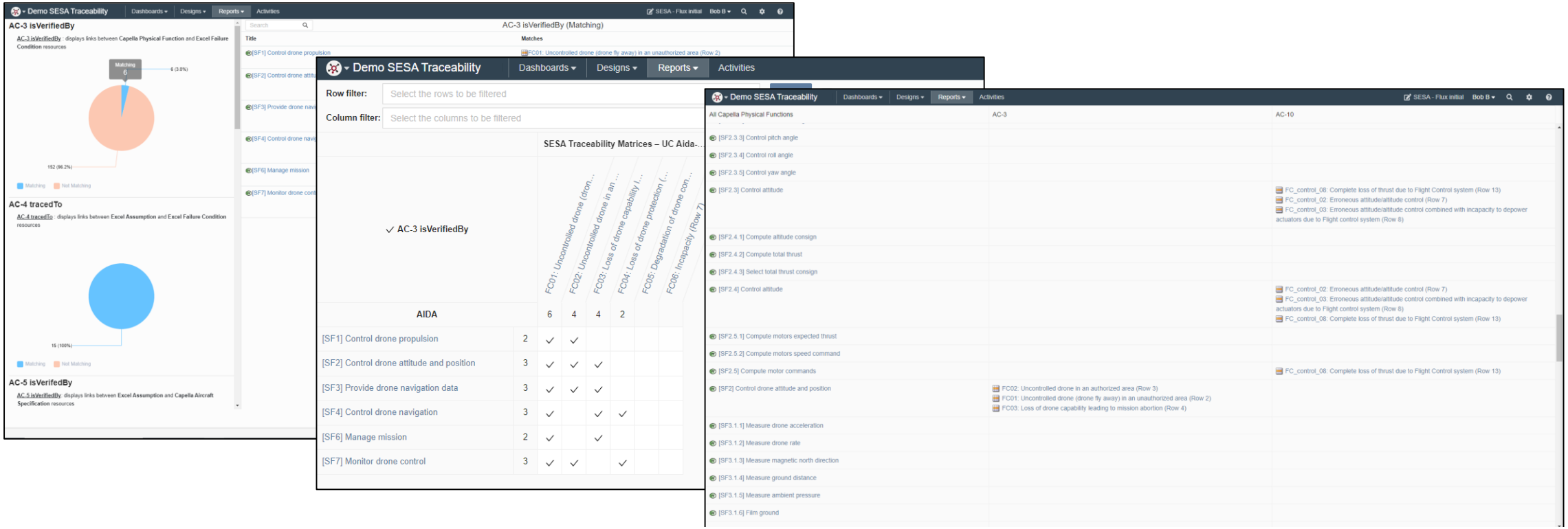
- Application of this traceability plan to a part of the AIDA Use Case
- It revealed 2 inconsistencies!
- Some recommendations have been proposed to limit the number of link to be manually traced
  - AFHA/SFHA Form recommendations
  - Classification of the links of the traceability plan :

=> More details this afternoon!

Axis A – POC of consistency management

S2C Dynamic consistency management PoC

- A cartography of traceability tools has been produced with an analysis of some COTS tools: Syndeia, SECollab, Reuse Company tool, Kovair.
- Implementation of the AIDA traceability plan on SECollab for analysis of the tool's capabilities.

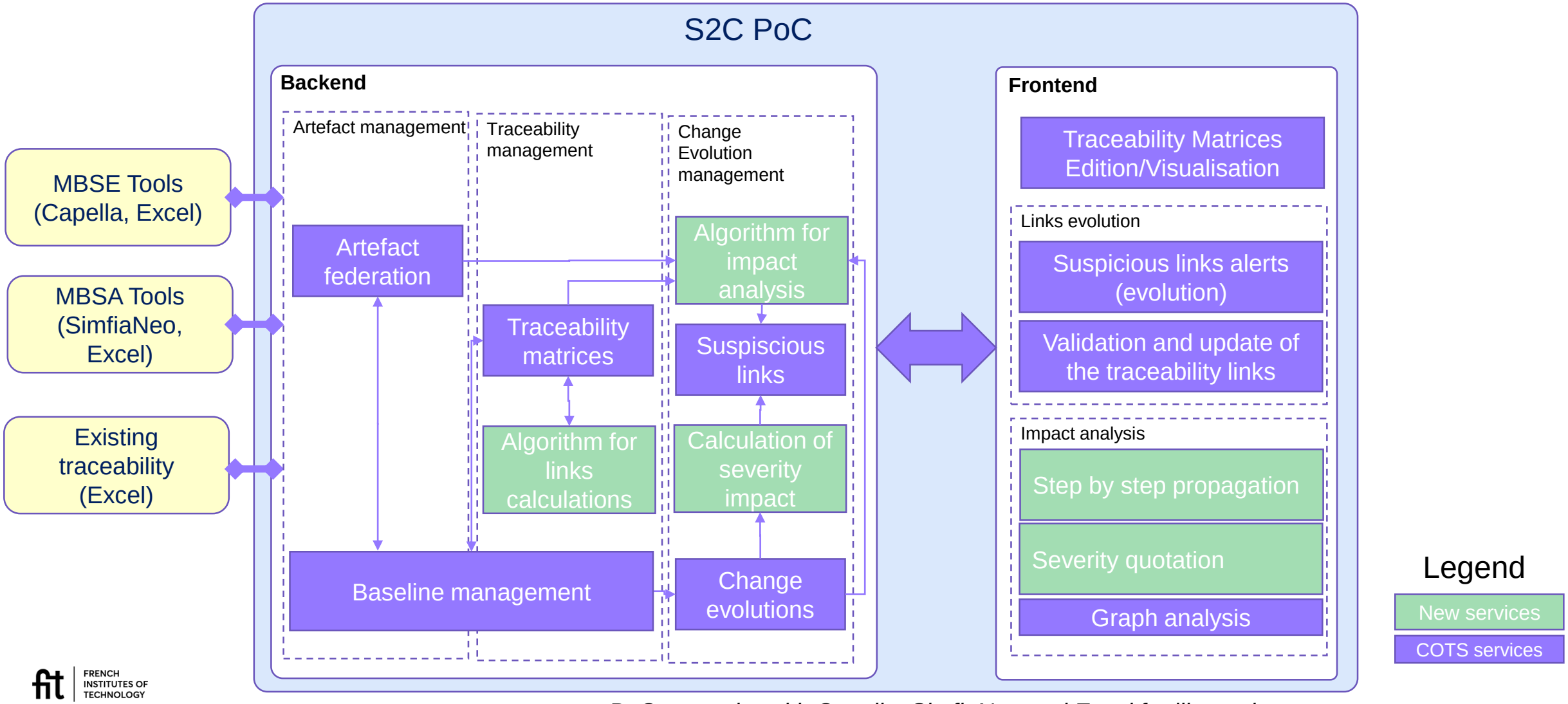


These tools don’t propose (yet) capabilities to analyse the impact of artefact evolutions => objectives of the S2C POC

S2C Dynamic consistency management PoC

Additional services of the PoC (vs COTS) :

- Suggestion of traceability links when artefact change;
- Impact analysis;
- Severity quotation of the impact

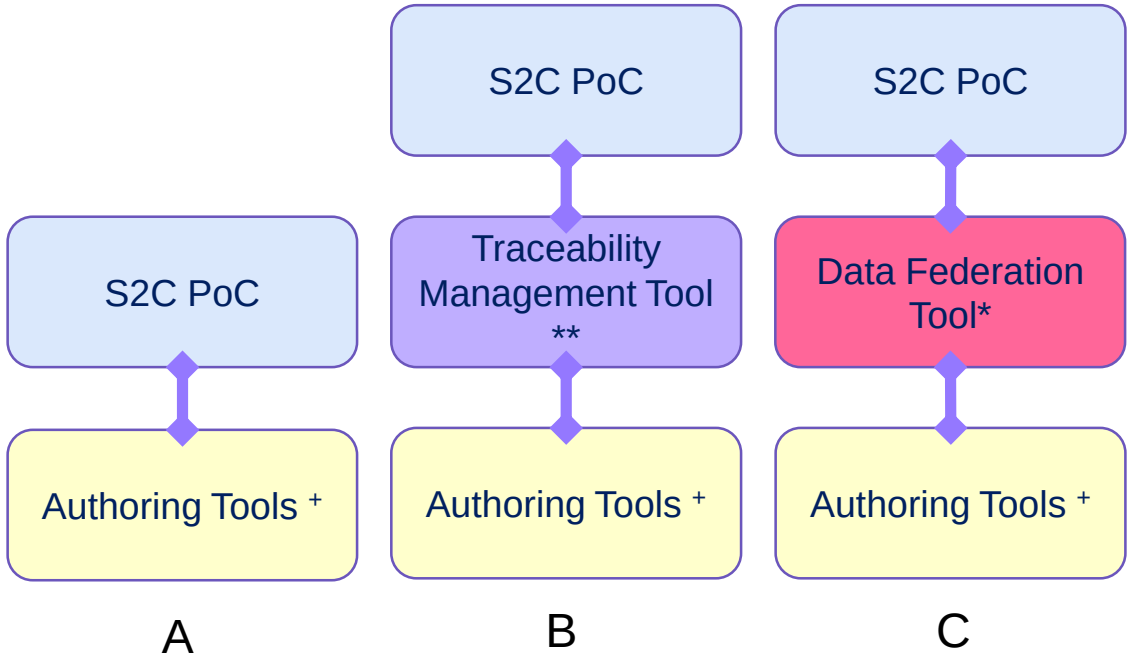


PoC example, with Capella, SimfiaNeo and Excel for illustration purpose

FRENCH INSTITUTES OF TECHNOLOGY

S2C Dynamic consistency management PoC

Different possible tooling configurations:



Services from COTS:

- Data Federation tool
  - Heterogeneous data integration (mapping)
  - Baseline management
  - Data evolution management (diff/merge)
  - Link evolution management (suspicious links)
- Traceability management tool
  - Traceability management
    - Customized plan,
    - Matrix edition
  - Navigation between traced items and traceability links,
    - Switch to Related Element
    - View Related Element Properties
  - Technical impact analysis
  - Produce customized reports and audits
    - Produce Export (Excel)

+ e.g. Excel, Capella, SimfiaNeo
* e.g. syndeia, SECollab, System Traceability, …
** DOORS, rectify, …

Axis A – Compatibility pre-study

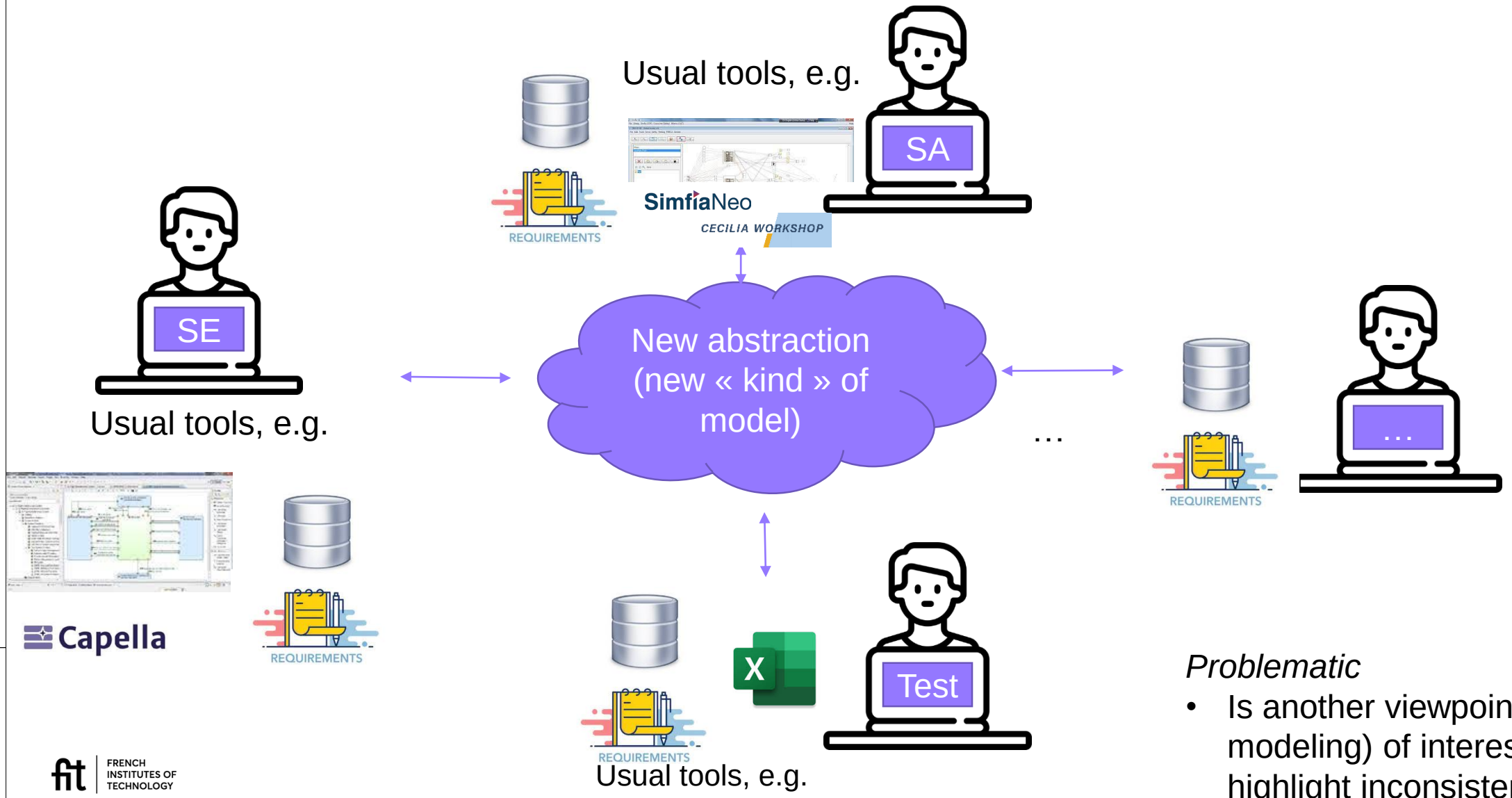
Compatibility : a new abstraction level that supports global consistency

Consistency *: are the data / points of view used by the different domains well aligned?*

vs

Compatibility *: are the different domains constraints or solutions compatible*

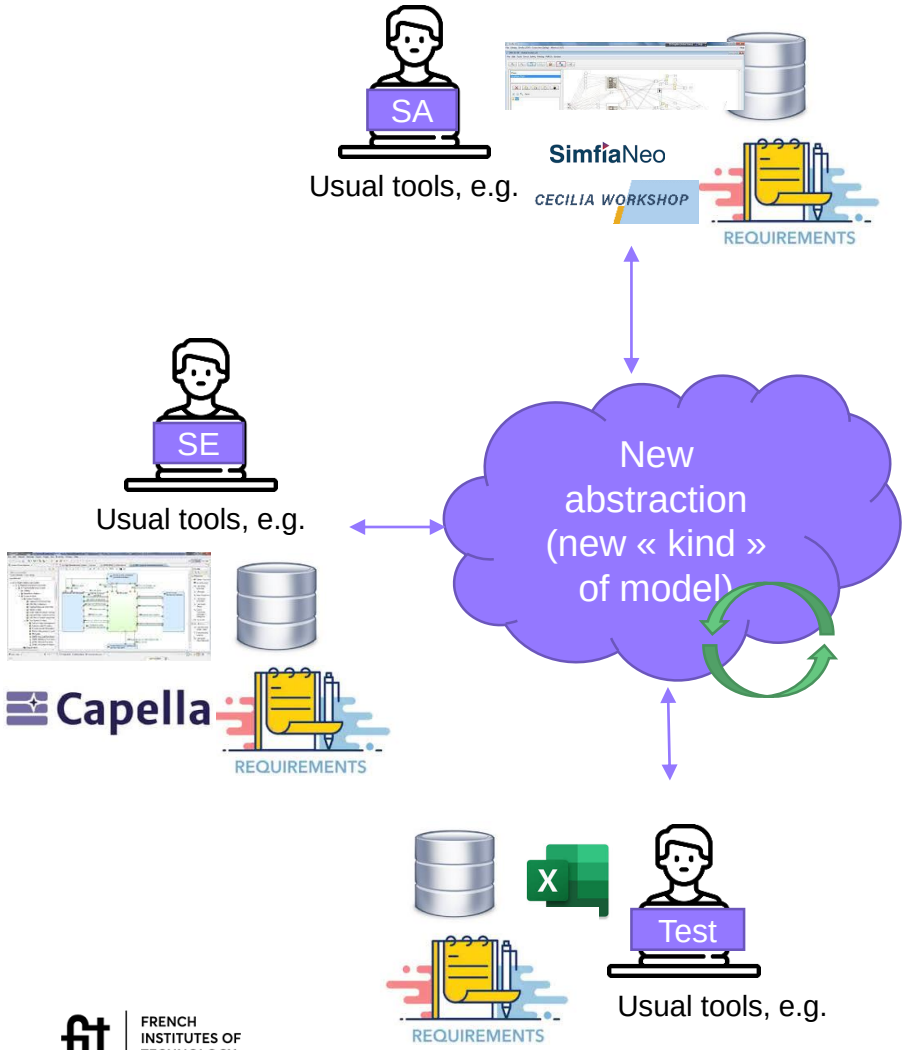
Goal: a new abstraction to facilitate the detection of incompatibilities



Problematic

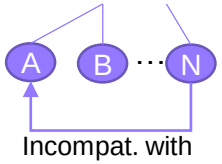
- Is another viewpoint (i.e. modeling) of interest to highlight inconsistencies?

Goal: a new abstraction to facilitate the detection of incompatibilities



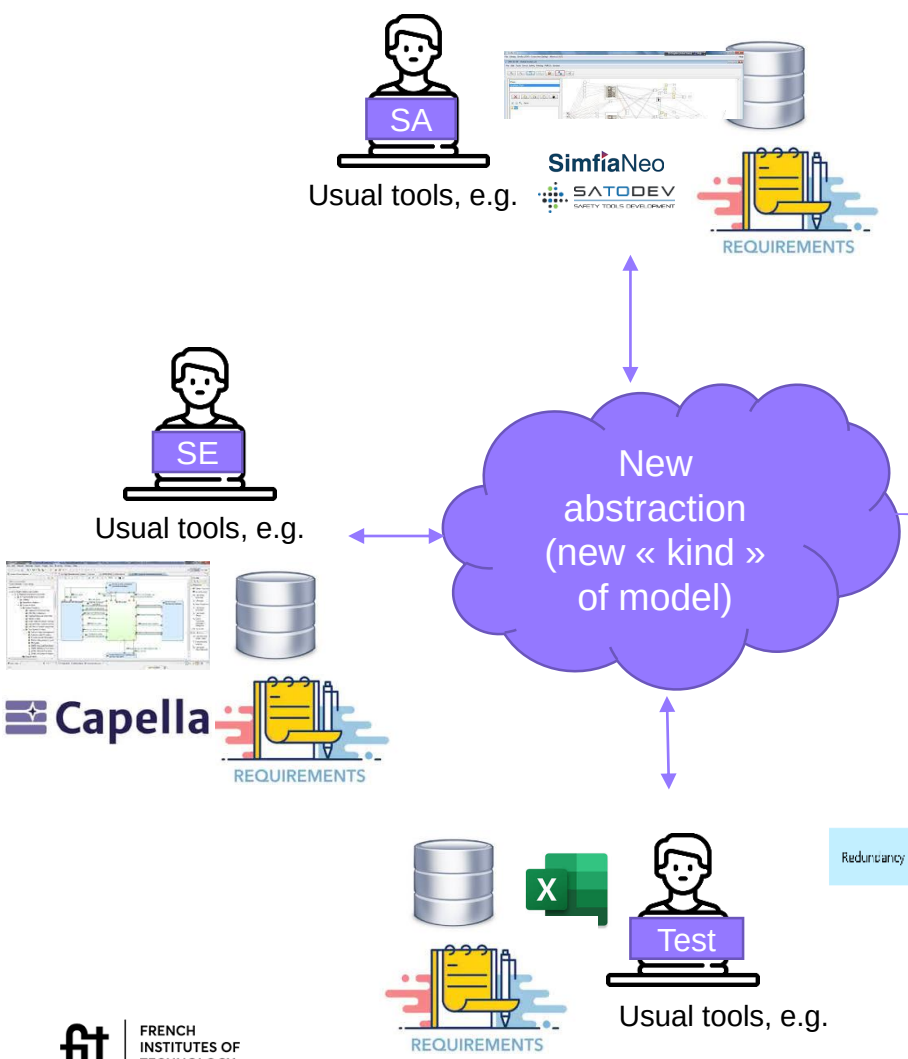
What to capture in this new abstraction?

- **For each concern** (SE, SA, Test, …)
  - Explain the **objectives / needs**, e.g.
    - SA: Increase reliability, increase robustness, …
    - Test: Increase testability
    - SE: Increase performance, reduce space requirement, …
  - Explain the **measures** applied, e.g.
    - SA: redundancy, diversity, quality of components, …
    - Test: add test links, …
    - SE: NF constraints…
  - **Related them to existing engineering artefacts** (instances), e.g.
    - Model elements in Capella, in SimfiaNeo, Requirements….
- **Between concerns** (architecting)
  - **Capture high level incompatibilities** between measures, e.g.
    - Redundancy != reduce space requirement,
    - Independence != testability
  - **Check if contradictory measures are applied** on a same set of artefacts (instance) to raise warnings!



➢ Capture a domain knowledge, that will be iteratively enhanced

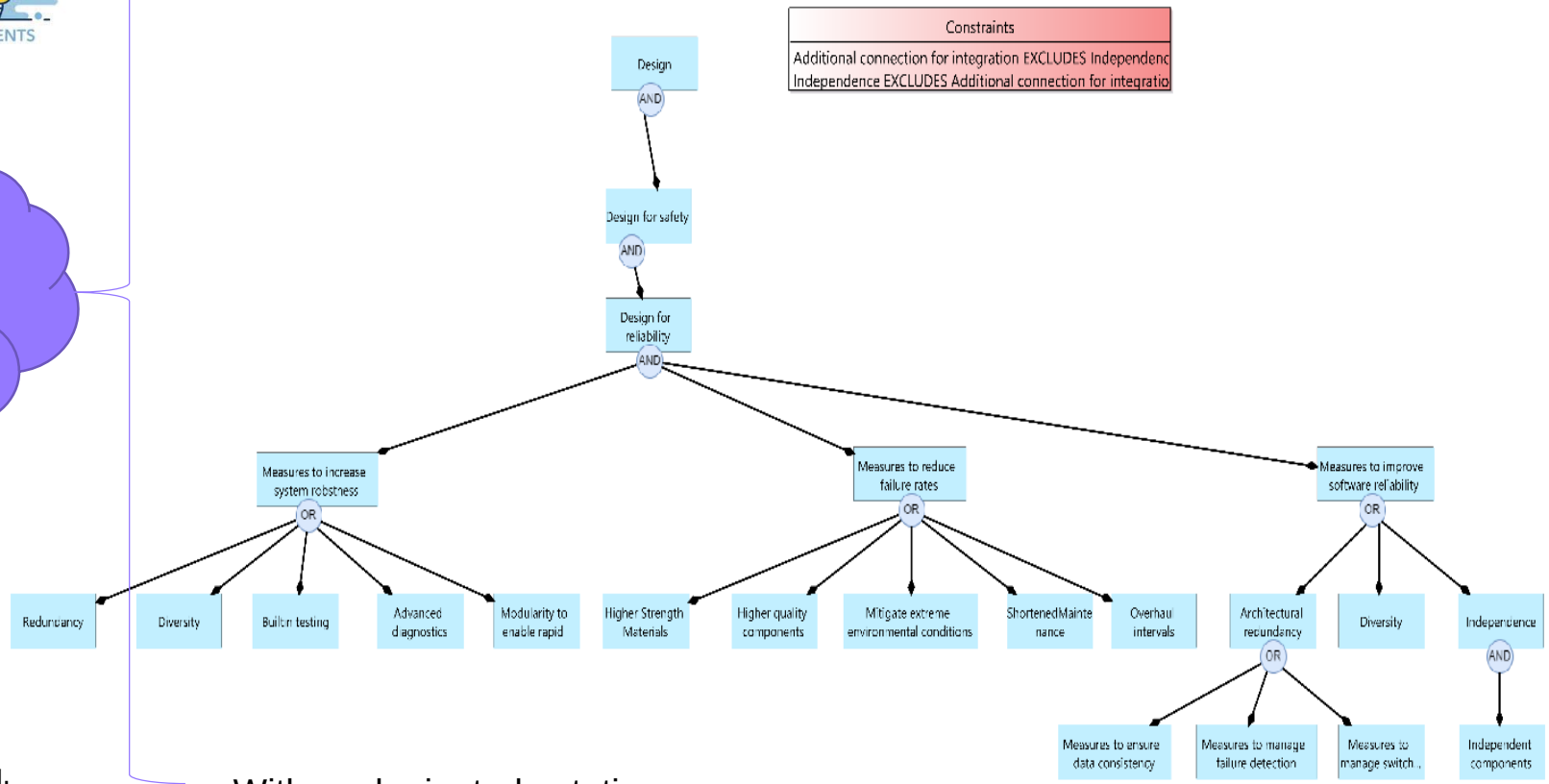
Goal: a new abstraction to facilitate the detection of incompatibilities



What to capture in this new abstraction?

Domain specific intentions: « Design for X »

e.g. Design for Safety (feature model representation)



With goal oriented notations:

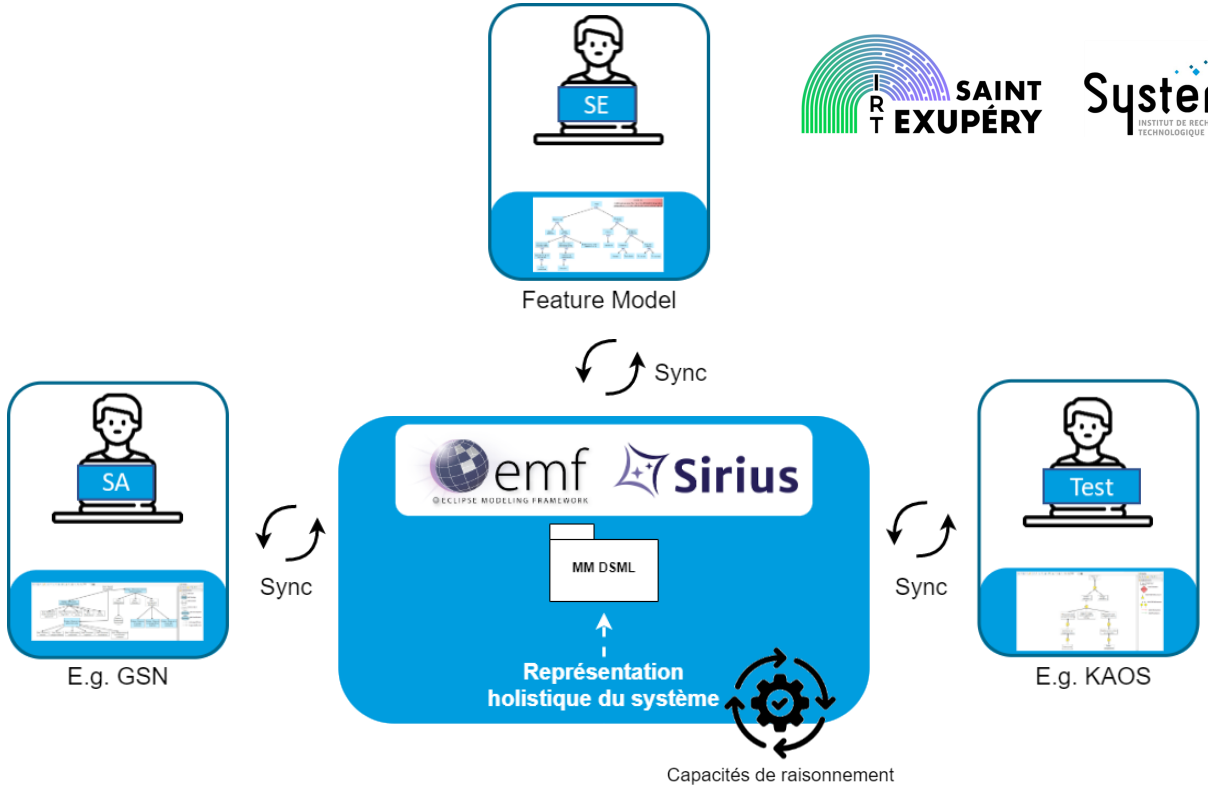
- GSN (Goal Structuring Notation), or KAOS for example

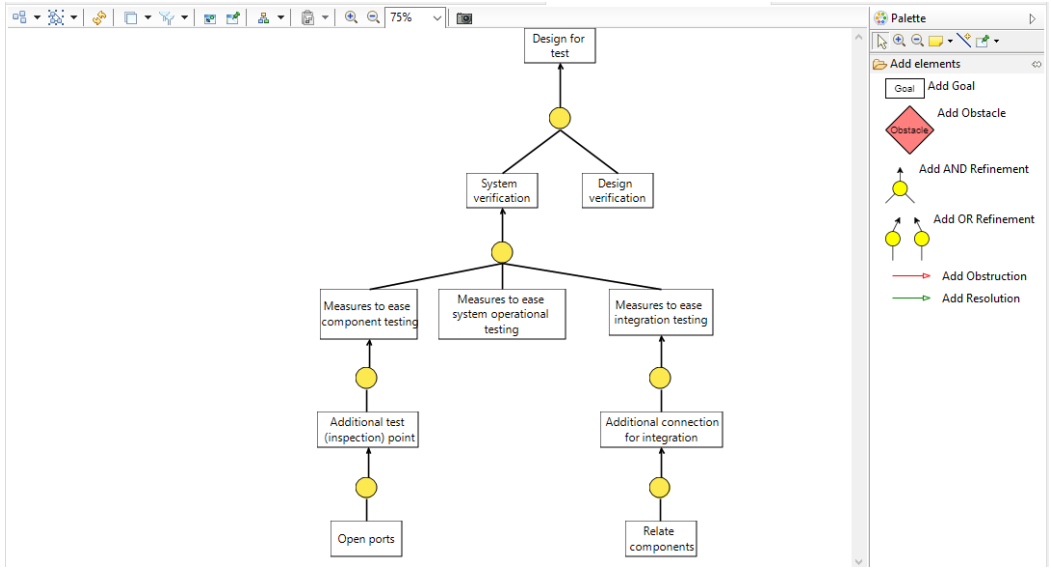
FRENCH INSTITUTES OF TECHNOLOGY

Incompatibility Pre-study results:

- **What has been produced:**
  - A framework based on Eclipse to
    - Model the domain
    - Represent synchronized viewpoints (feature model, GSN, KAOS),
    - Analyze incompatibilities between models, with a propositional logic (SAT solver).
  - An application on
    - An academic case study (e-shop)
    - A partial representation of 3 engineering domains (SE, SA, and Test)

- **What is missing:**
  - Connection to engineering domain tools
    - And more over Feature extraction from existing domain artifacts
  - Application to the AIDA case study





- Workshop presentation -

Today workshop presentation

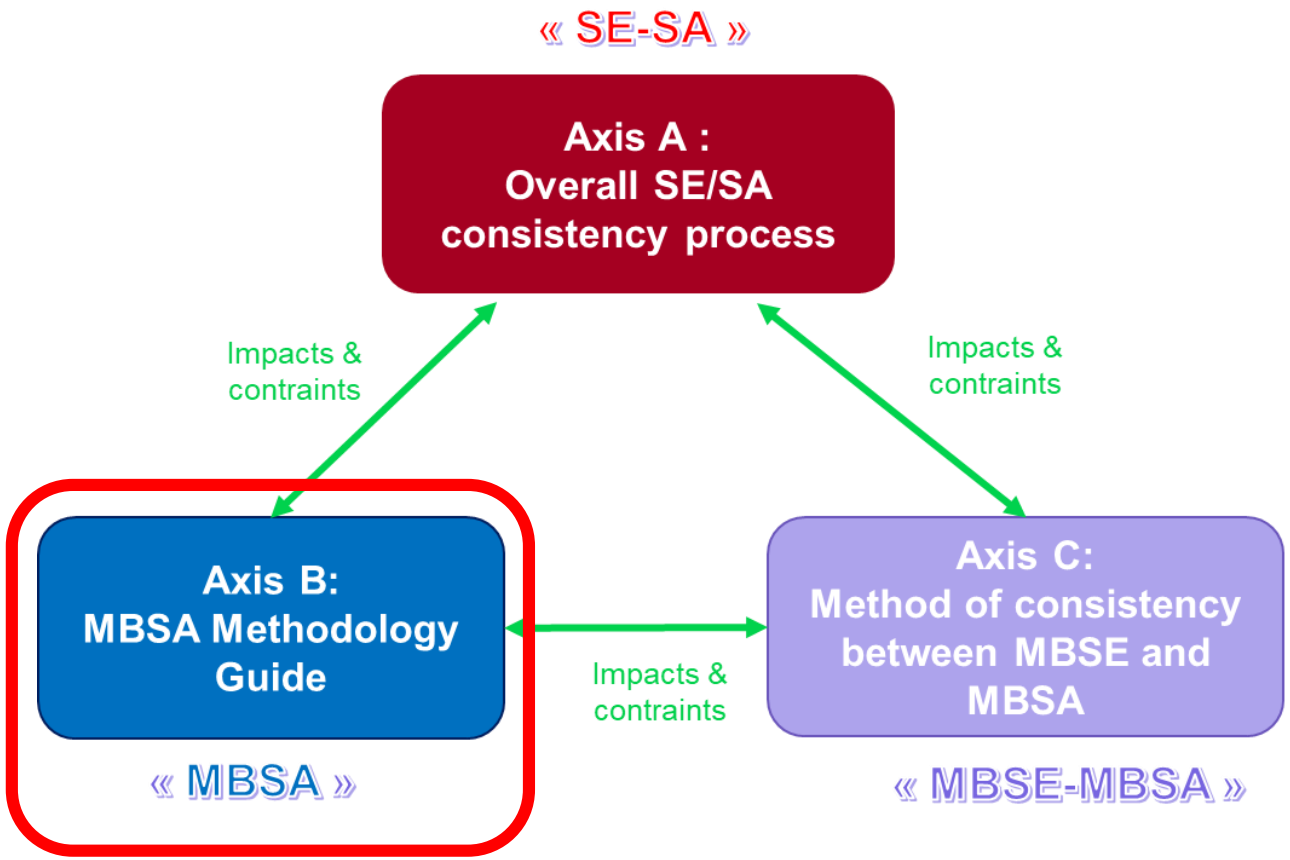
- **Deep Dive in the SE/SA consistency process [Stephen]**
  - Objectives view
  - Process view : illustration on some specific scenarii

- **Deep dive in the traceability activities [Sylvain]**
  - Traceability plan (data view)
  - Application on AIDA Use Case : what we learnt
  - Proposal for traceability plan Optimisation

- **POC « dynamic consistency management » demonstration [Stephen + Michel]**

Axis B : MBSA Modelling

Axis B – Overview



Objectives

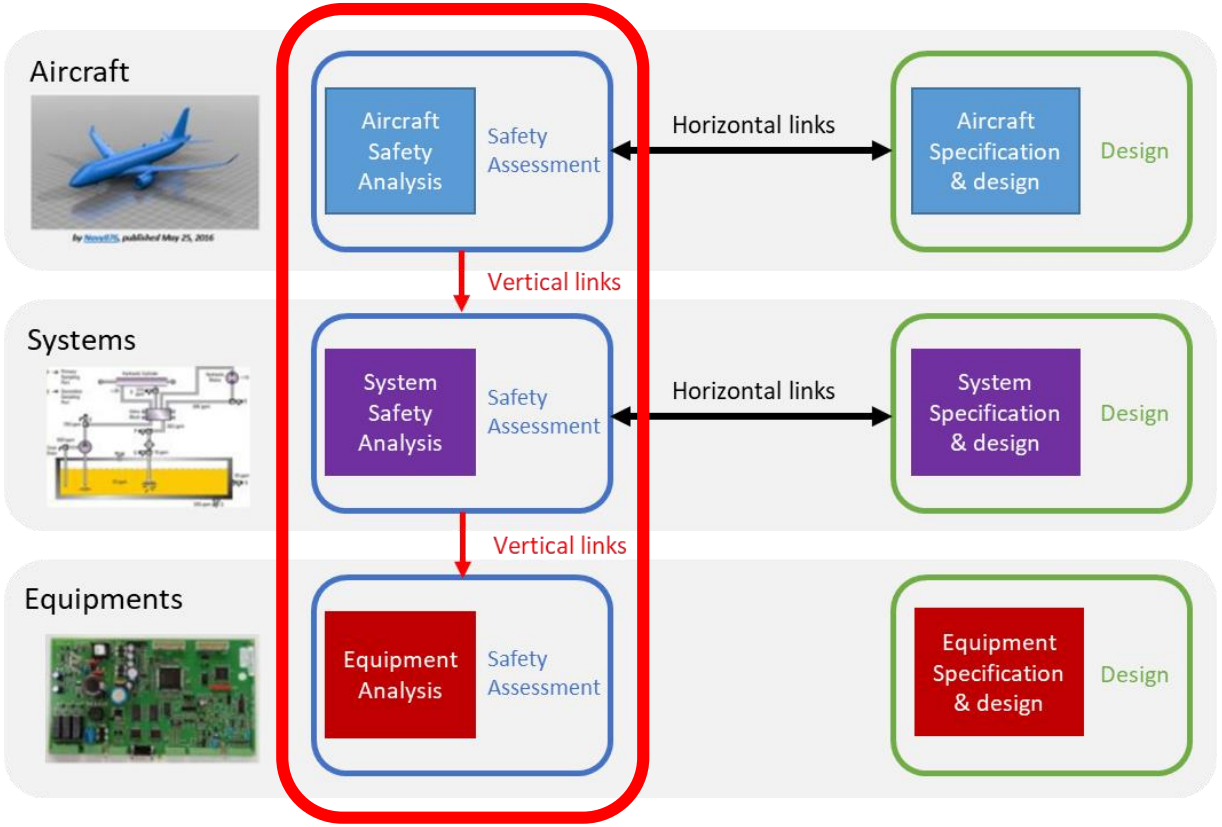
- ❑ Propose a MBSA generic method
- ❑ Contribute to MBSA promotion, specifically in aeronautical ecosystem

Objectives of Axis B

Objectives

MBSA methodology and promotion of MBSA

- MBSA methodology
  - Provide guidance for modeling choices to support the safety analyzes carried out in the project
  - In line with the constraints of industrial developments
  - To support MBSE / MBSA consistency activity
- Promotion of MBSA
  - Guidance for use and appropriation by the industrial safety specialists
  - Integration into an industrial process
  - Provide elements of RETEX for MBSA industrial deployment when possible give elements such as time spent in modeling, level of precision of the necessary models, reuse capacities, usability over time, etc ...



Working axes that drove our work

4 working axes

- Easy to read
- Standalone guideline
- Verification and Validation oriented
- Learn by practice

A methodology suitable for aeronautical developments.

A methodology that can be integrated in already existing company process

- Two deliverables:
  - The methodology guide
  - The GetStarted kit

The guide

- **The guide: MBSA Modelling guide and validation report**

Based on AltaRica Dataflow

RAMS engineer MBSA full method

120 pages

Means

To develop and validate a shared MBSA methodology suitable for aeronautical developments.

This document provides methodological guidance for MBSA modelling. It presents some general principles as well as main identified difficulties modelers can encounter.

Our intent is to support classical ARP4761A PSSAs and SSAs analyses with MBSA.

Offers

- Beginner level: to give the basics to RAMS Engineer without specific knowledge of the MBSA
- Intermediate level: for user who whish to go further in the theory and the calculation behing the MBSA
- Advanced level: for user who wish to understand the mathematics behind the analysis

The Get Started Kit

The Get Started Kit offers a quick way to begin without reading the full guide

Based on AltaRica Dataflow

The minimum to start MBSA

72 slides

Means

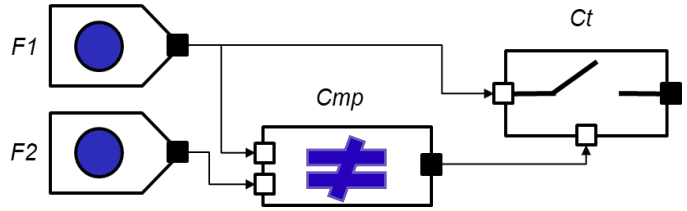
To allow anyone to start quickly with or without knowlegde of the MBSA activities

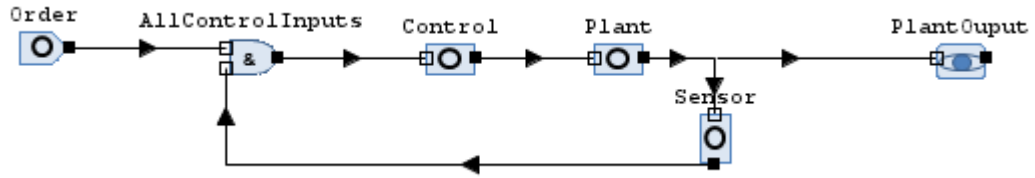
Offers

- All the basics to start modelling
- The tips to know
- An example fully commented in Cecilia and SimfiaNeo and AltaRica 3.0

What are the main issues we address?

- How to begin modelling in MBSA without preliminary experience ?
- How to deal with equation loops in AltaRica (control loop)?
- How to solve an event cycle?





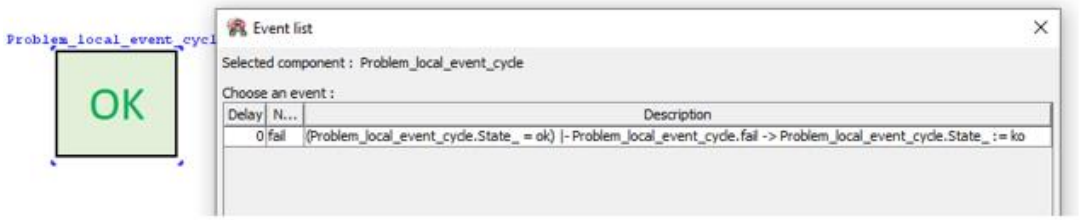


Figure 56: Event cycle illustration - OK state

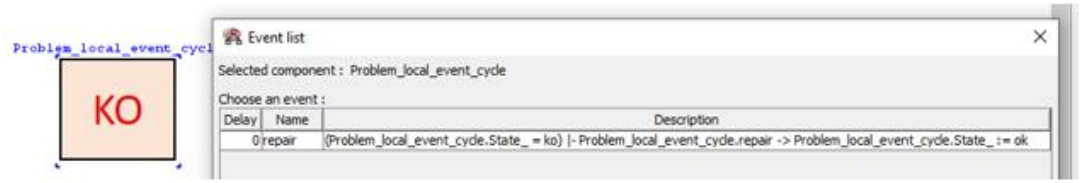


Figure 57: Event cycle illustration – KO state

- Method -

Methodology context

- This method aims is to provide **validated recommended practices** built on the experience of the S2C projects members who are amongst the main actors of the MBSA in aeronautics. We will provide support and illustration of the proposed methods using **AltaRica Data Flow** language

- This document targets the safety specialists with **no MBSA background** as well as **MBSA advanced users**. We expect readers discovering the MBSA to have a set of mind opened to programming, new reasoning and tools.

- This document offers in particular methods to deal with control loops in AltaRica Dataflow

Why AltaRica ?

Members

Two members are AltaRica (language data flow) tool vendor and one member has done its own language (Open Altarica 3.0)

Experts on projects

AltaRica Experts (on detachement and consulting) available for project

New mean of compliance in ARP

ARP4761A adds an Annex to describe the use of MBSA. Industrial members are interested to see if it is applicable to their respective systems and what is missing in the Annex.

Limited ressource forced to focus

We can not assess all way of doing thing so take one humbly then be ambitious…

AltaRica GUI concepts are close to SE ones

Evident proximity between the GUI ecosystem that reduce the friction.

A complete description of what is necessary

❑ B- Beginner

To understand the basics of MBSA based on AltaRica Dataflow

❑ -I- Intermediate

To integer in a an aeronautical process and to master the tools

❑ -A- Advanced

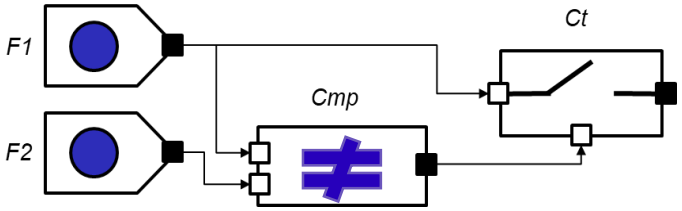
To go further to the maths and beyond

Easy to follow

Lead by example

The COM / MON pattern example

A simple example common to the guide and the Get Started kit to guide you through MBSA learning.



- General description: The purpose of the system is to send a command order F1 consolidated from two input commands. The system monitors the two orders F1 and F2. When F1 and F2 are different, an opening command is sent to the Contactor, the Contactor opens and the command is lost. When the Contactor does not receive the opening command, F1 is transmitted.
- Interfaces: Two input command F1 and F2 and one output command F1.
- The system is composed of:
  - A comparator (Cmp)
  - A contactor (Ct)
- Safety requirement:
  - FC1: erroneous output (Catastrophic)
  - FC2: loss of output (Minor)

A simple kit to start quickly

- The GetStarted presentation embeds all necessary information to quick start modelling.
- Self standing presentation

A summary of the guide to start modelling for beginner

The intermediate and advanced parts are not in the GetStarted

Modelling examples

- User guide to model the COM / MON example in:
  - Dassault Aviation Cecilia Workshop
  - Airbus Protect SimfiaNeo
  - AltaRica 3.0

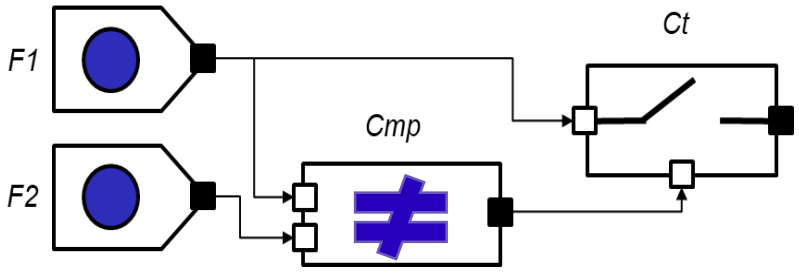
A simple kit to start quickly

- How to get started with MBSA ?
  - Main principles
  - Questions to address before starting
  - The different steps to follow
- Modelling the example
  - Go Through the tool
  - How do I do in practice to model ?
  - How do I do in practice to simulate?
  - How do I do in practice to compute?

Lead by the example

The COM / MON pattern example

A simple example common to the guide and the Get Started kit to guide you through MBSA learning.



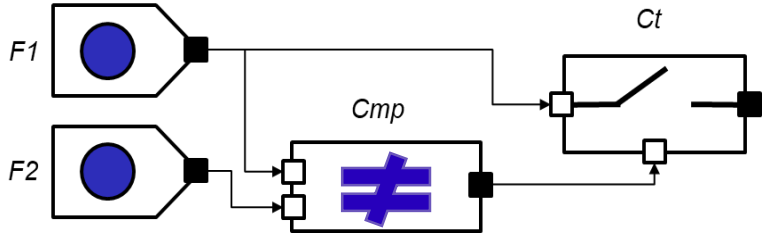
- The examples -

The examples

To model the COM / MON

In Cecilia Workshop, SimfiaNeo and AltaRica 3.0

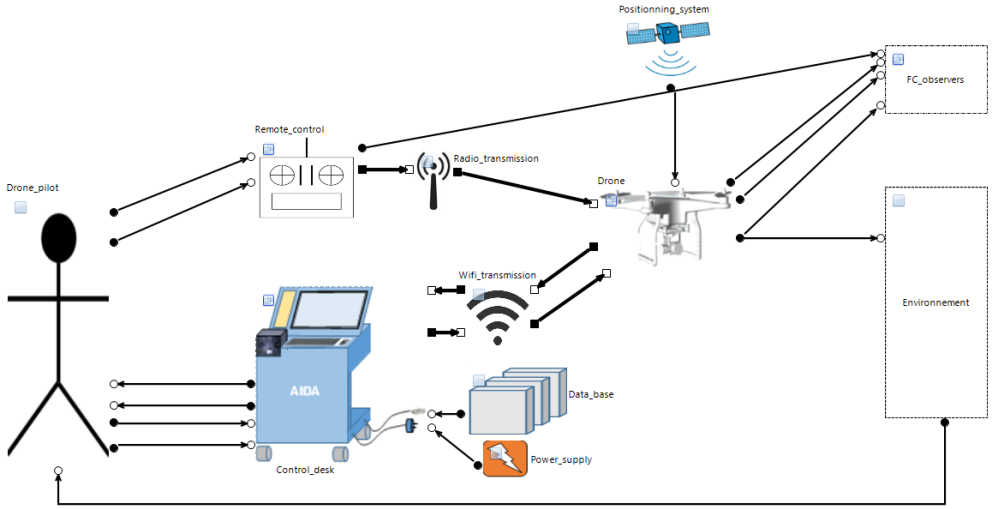
A quick and complete user guidance to model the example within the tool.



To apply the method thru a use case

In SimfiaNeo and AltaRica 3.0

A use case modeled with the giude methodology an the return of experience from the method: the AIDA (Aircraft Inspection by Drone Assistant) Use Case



A return of experience of modeler in open AR

Summary

This document provides complements and recommendations to the MBSA modelling guide “MBSA Modelling guide and validation report”,

It highlights questions, comments and recommendations made by the people in charge of modelling the "AIDA" safety case in the S2C project. Our intention is to provide answers and frequently asked questions during MBSA modelling.

2 topics addressed:

- **Modelling Activities: Remarks and recommendations**
- **Modelling strategy: Remarks and recommendations**

This note is based on AIDA Use Case modeling whith the method proposed by S2C

- Workshop presentation -

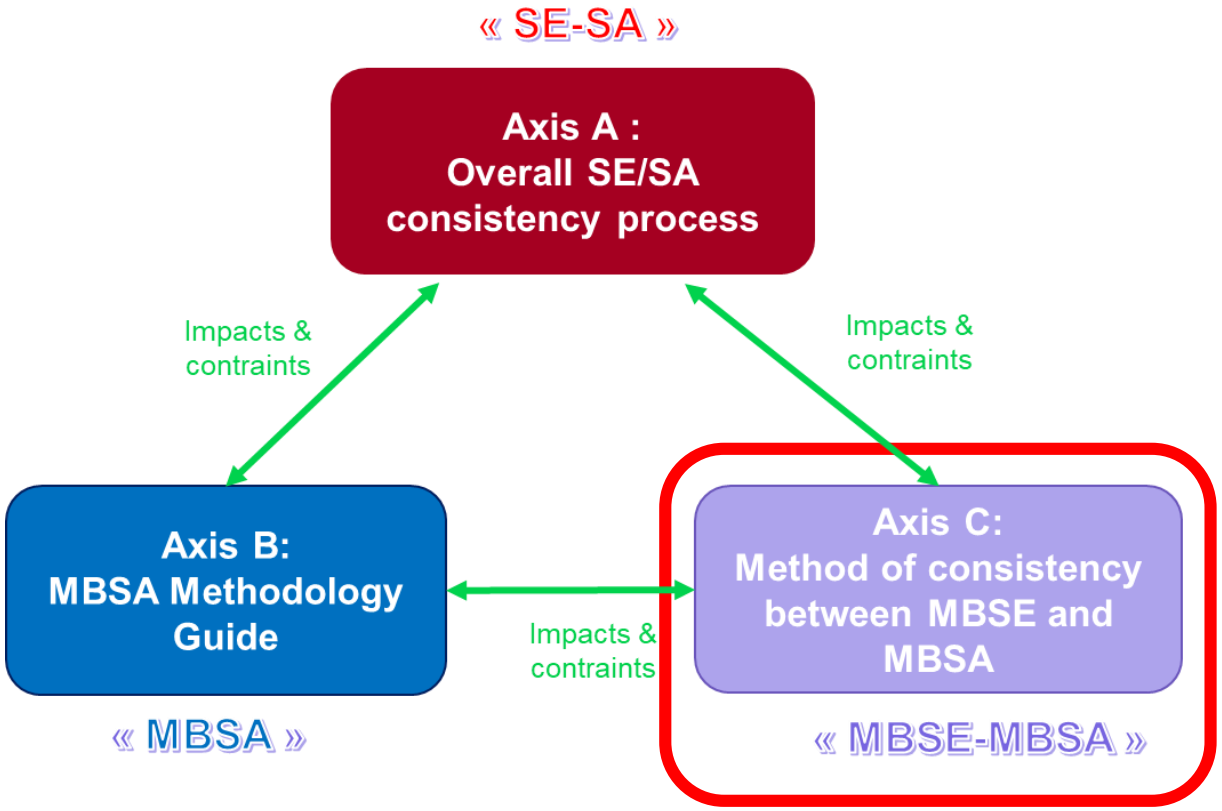
Today workshop presentation

- **Return of experience from modelers when modeling in AltaRica**
  - AIDA model in SimfiaNeo
  - AIDA model in open AltaRica
  - ARP4761A model in Cecilia WS
- **Discussion about the methods used to deal with the loops**
- **Open discussion on usage of MBSA in the future aeronautics projects**

- Axis C -

Method for consistency between MBSE and MBSA

Axis C - Objectives

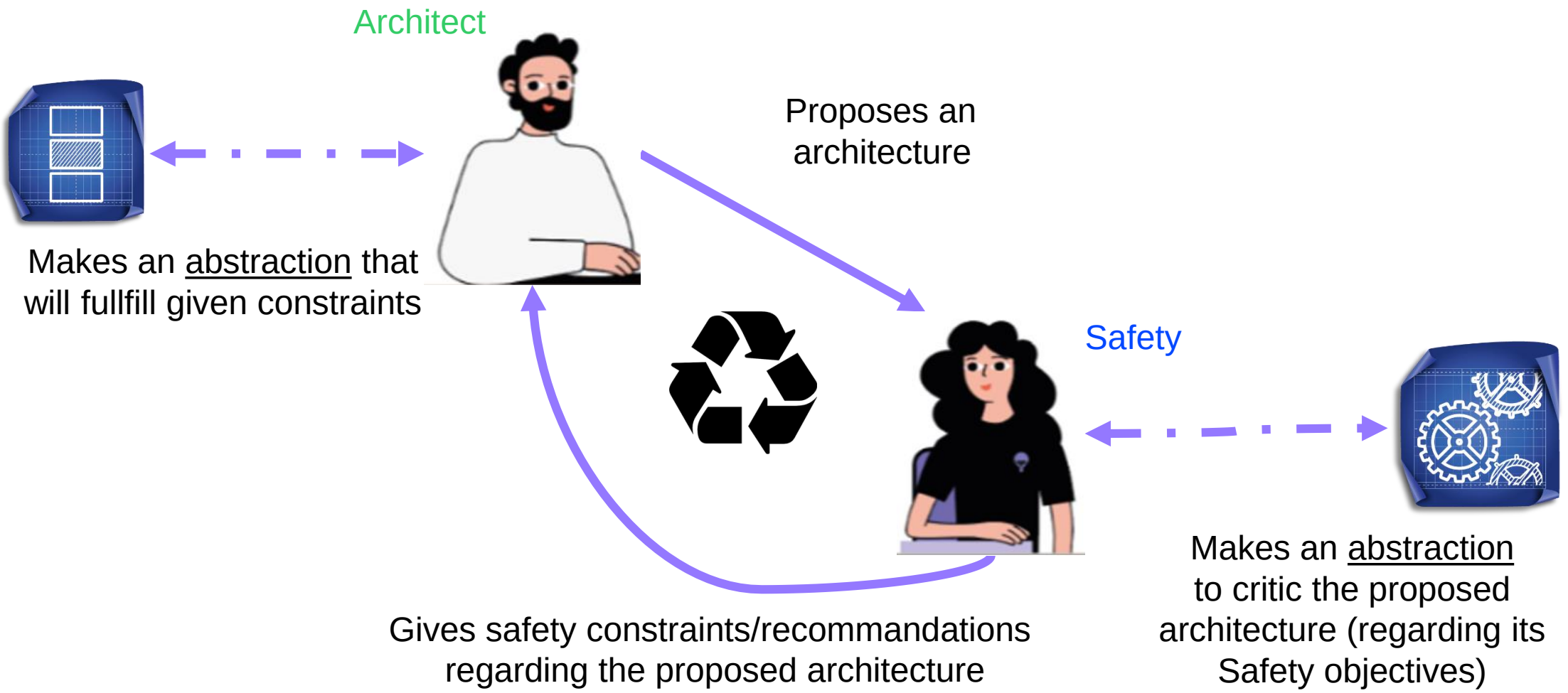


Objectives

- Methodology to **improve confidence** between a model based SE (MBSE) and a model based SA (MBSA) considering:
  - At the same systemic level (Functional or physical)
  - Maintenance over iteration of each the model

- Framing the Problem -

What occurs... at (very very) high level



What occurs ... at abstraction level

SF2.5 and its context seen from SE

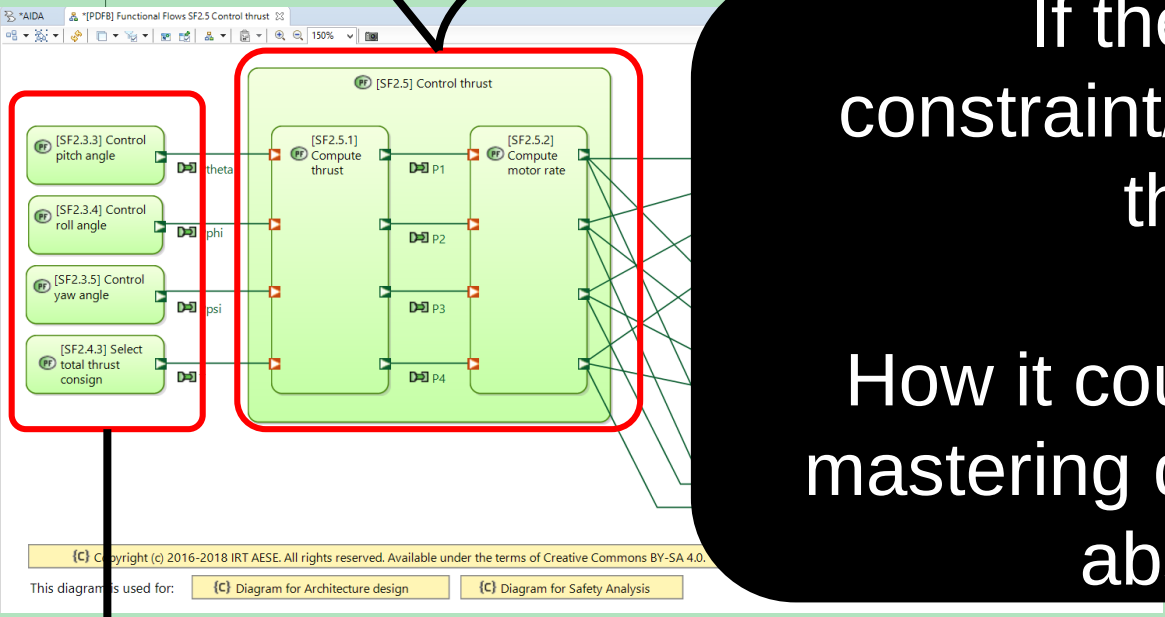
SF2.5 and its context seen from SA

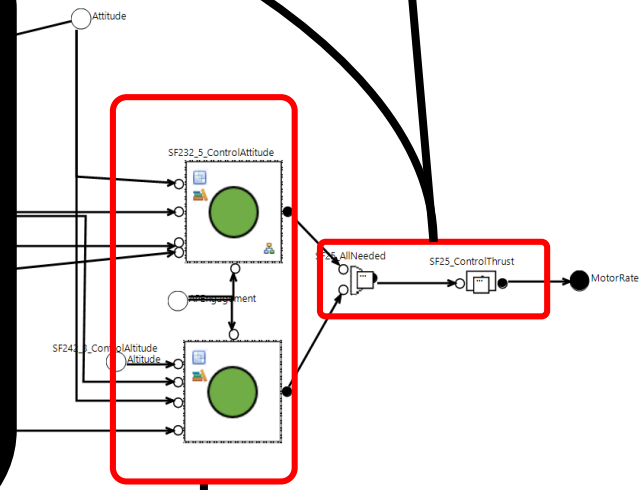
Refinement and interface differ

If there is any SA constraint/recomandation for this function

...

How it could be right without mastering differences between abstractions ?





Context differs

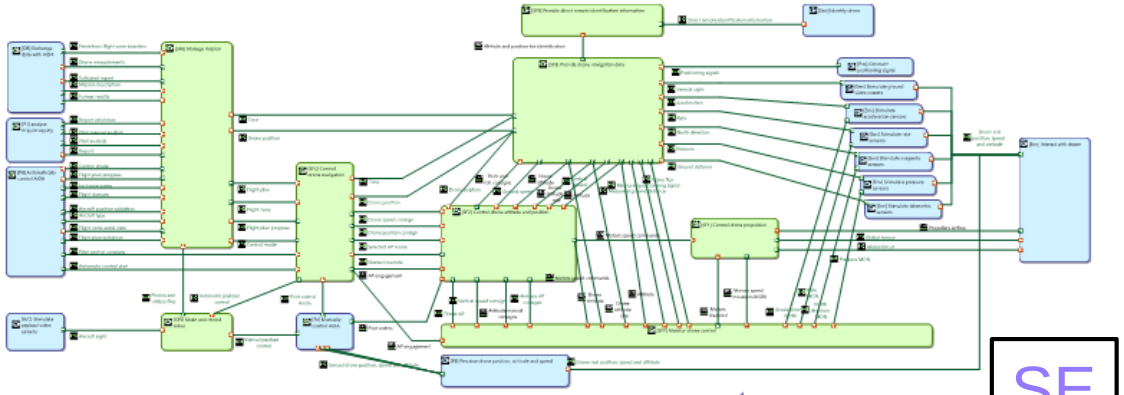
Representation differs

FRENCH INSTITUTES OF TECHNOLOGY

Problem Positioning

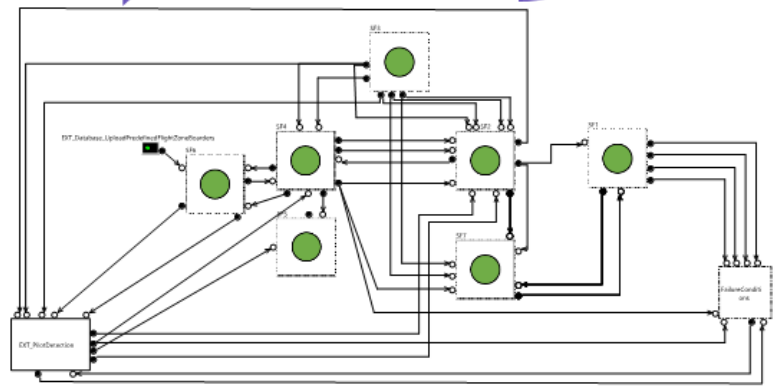
Statement

How to <u>improve confidence</u> in the results of safety assessment from SA models, knowing they are <u>based upon</u> a <u>distinct abstraction</u> and a <u>distinct realization from SE model</u>



SE

Consistent ?



SA

fit FRENCH INSTITUTES OF TECHNOLOGY

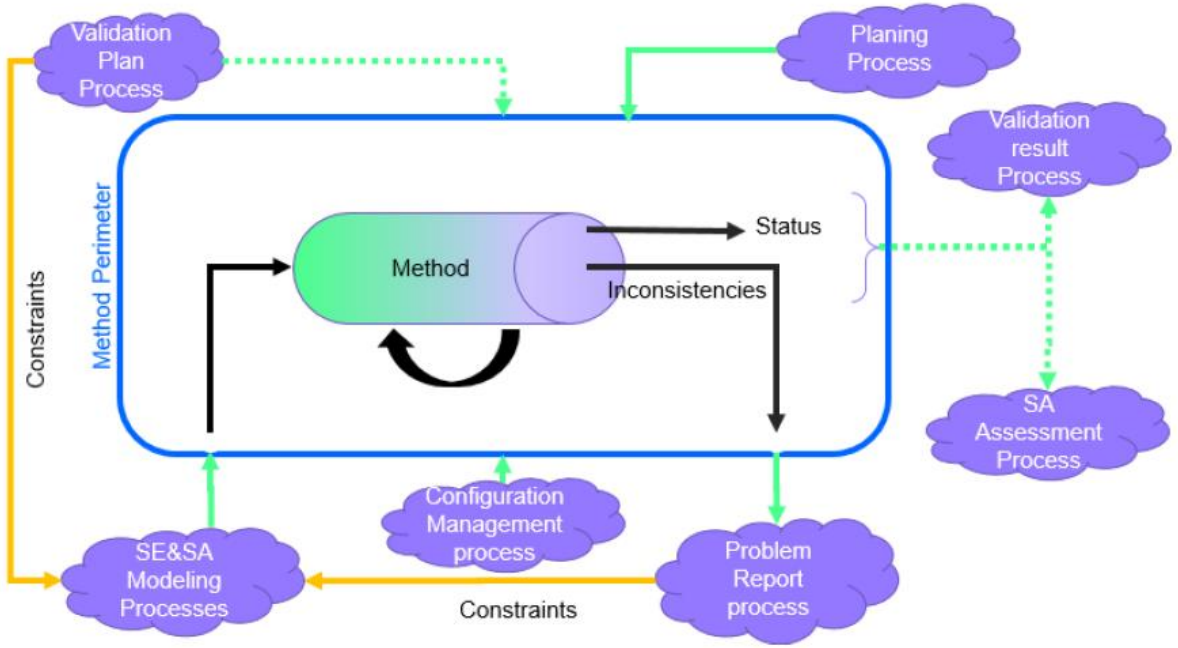
When method shall be used ?

Both SE and SA models are available

Am I confident to launch safety assessment and other depending processes ?

What is the positioning against company's processes

What are other methods around ?



Problem Positioning : (frozen) dimensions with their items

Dimension : Coupling of Authoring

- Each model authored on their own
- One model derived partially from the other one
- Authoring encompass both specialities

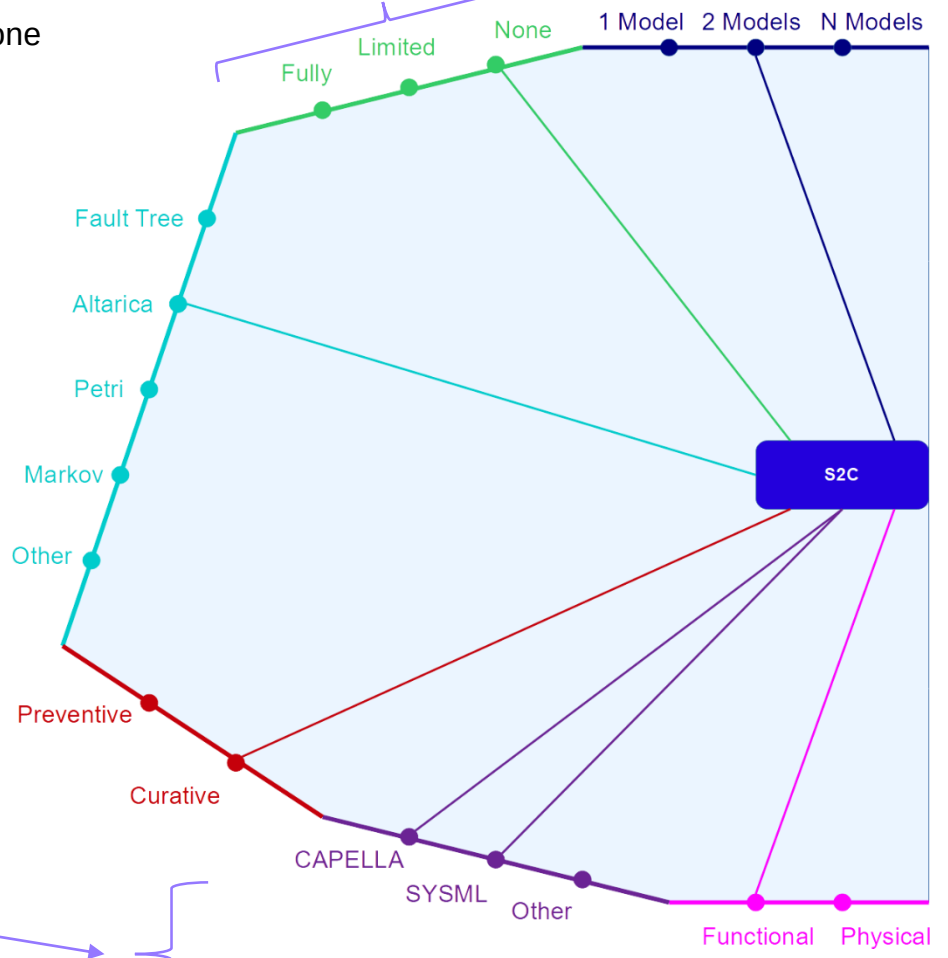
Dimension : SA model paradigm

- Underlying mathematic rules

Dimension : authoring Incursion

Dimension : SE model paradigm

- Underlying grammar and usage



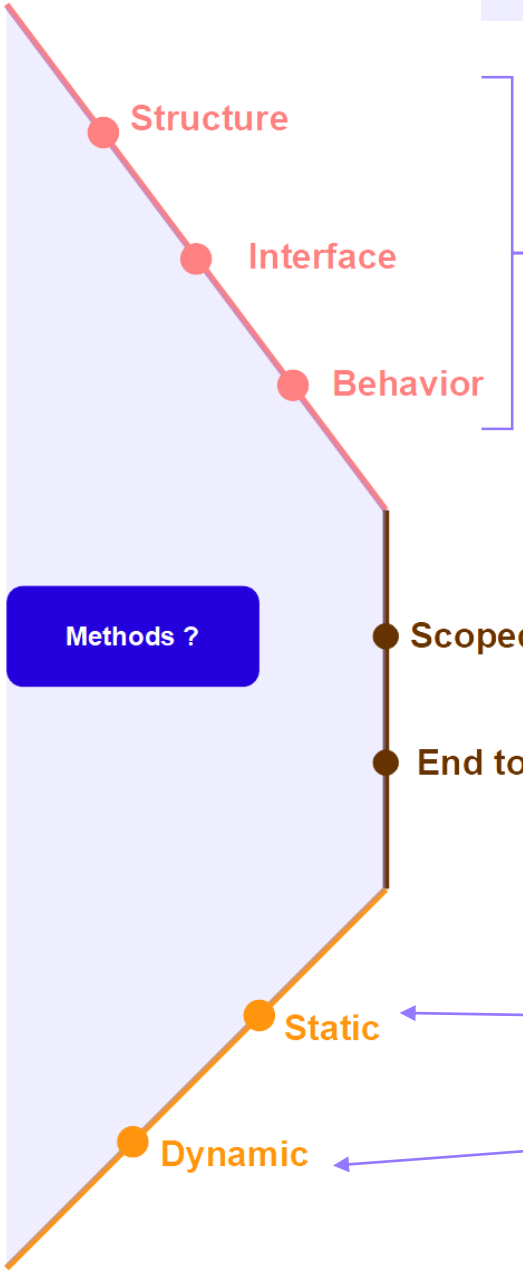
Dimension : Cardinality of Models

- all in one model
- each specialty has its own model
- specialties are spread on several agregated models

Dimension : Level of models

- Model(s) represent(s) physical parts
- Model(s) represent(s) functional blocks

Problem Positioning : (exploratory) dimensions with their items



Dimension :

Element of Models

- Elements concerned by method

Dimension :

Model perimeter considered by method

- Method considers a sub part of a model
- Method considers the whole model

Dimension :

Executability of models

- Model(s) contain only static définitions
- Model(s) can execute the definitions

FRENCH INSTITUTES OF TECHNOLOGY

- Solutions Take away -

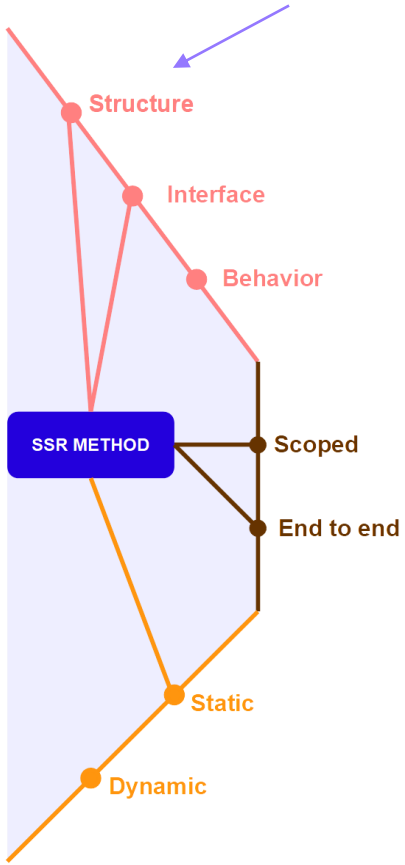
Take away : framing

not 1 method but 3 ones

Structural Scope Review **[SSR]**

kind of « tracability between 'N' SE model artefacts against 'M' SA model artefacts»

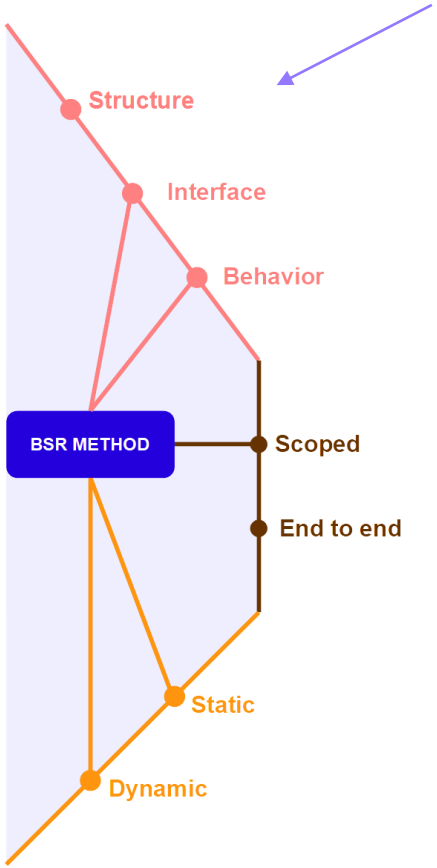
(Idea borrowed from process method)



Behavior Scope Review **[BSR]**

kind of « Unitary test » between SE spec. and SA model execution on same perimeter»

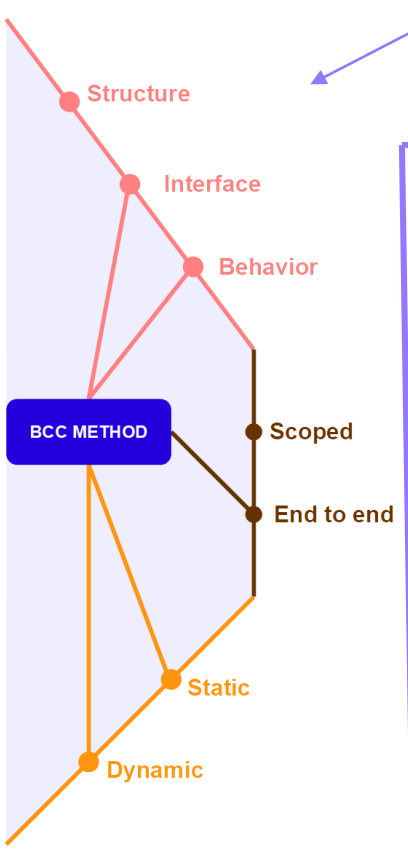
(Idea borrowed from software testing)



Behavior Cross Check **[BCC]**

kind of « model behavior comparison upon scenarios»

(Idea borrowed from Flight Testing for Performance model resynchronisation)



Methods inter-relationship

- Only one, (e.g. BSR only)
- Two amongst 3 (e.g. SSR and BCC
- All the 3 (e.g. SSR and BSR and BCC)

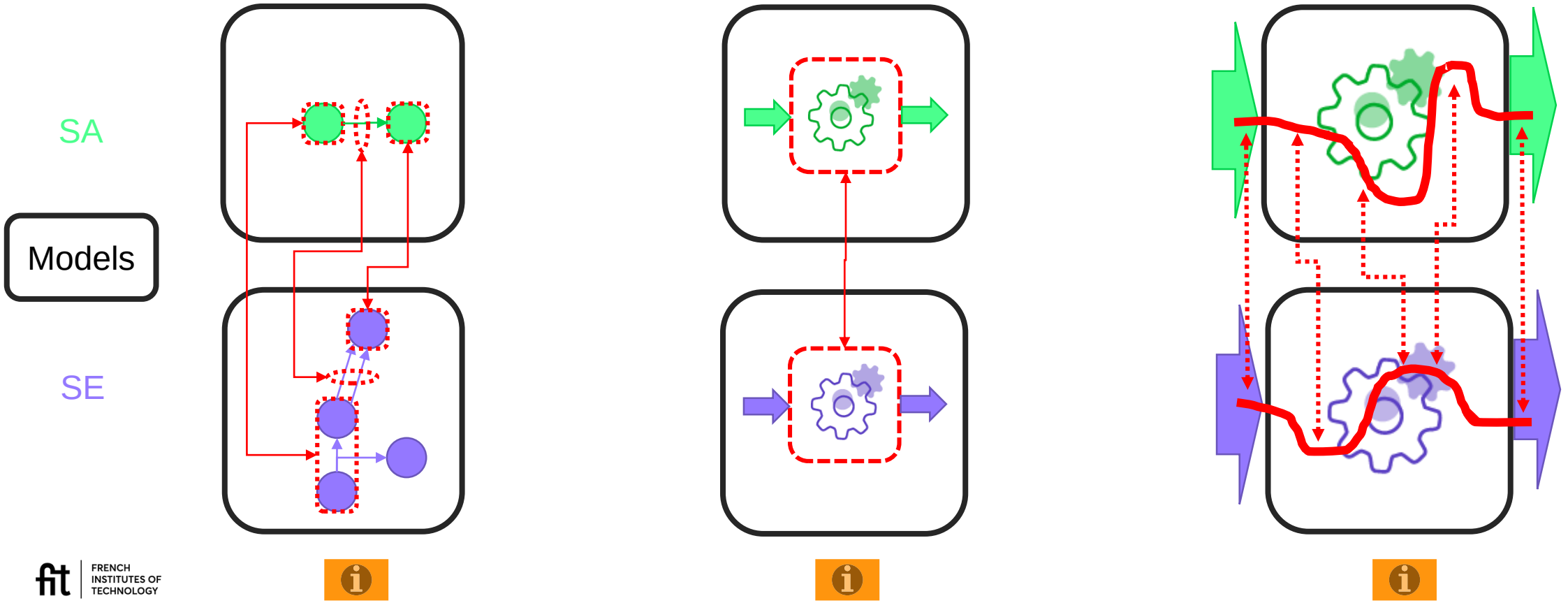
Methods development

- **Designed to be applicable** to different project dimensions
- **Assessed** via a Proofs of Concept [PoCs] having the previous frozen dimensions.

FRENCH INSTITUTES OF TECHNOLOGY

Take away : overview

Structural Scoped Review	Behavioral Scope Review	Behavioral Cross Checks
Structure and IO	Behavior and IO	Behavior and IO
Scoped	Scoped	End to end
Static analysis	Static analysis	Dynamic Observation



- PoC & Outcomes -

Proof of Concept [PoC] Positioning :

Dimension : Case Study

- How many Cse study used ?

Dimension : Couples of models

- which SE tool Vs SA tools

Dimension : Amount of sub perimeters

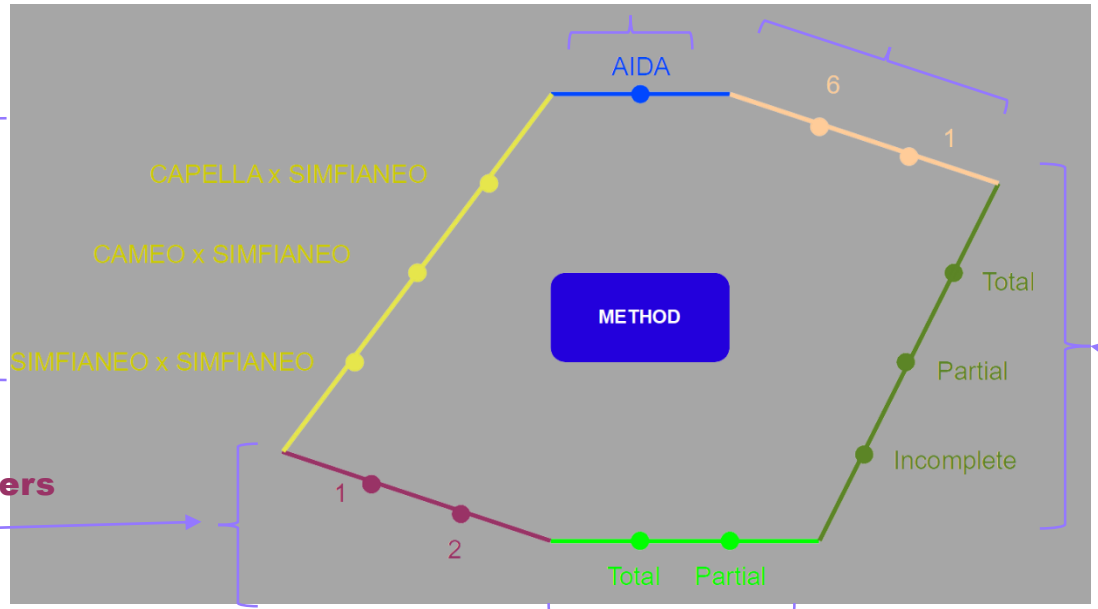
- How many sub perimeters consideres ?

Dimension : sub perimeters vs Model

- How sub perimeters overlap the whole model ?

Dimension : Itérations done on sub perimeters

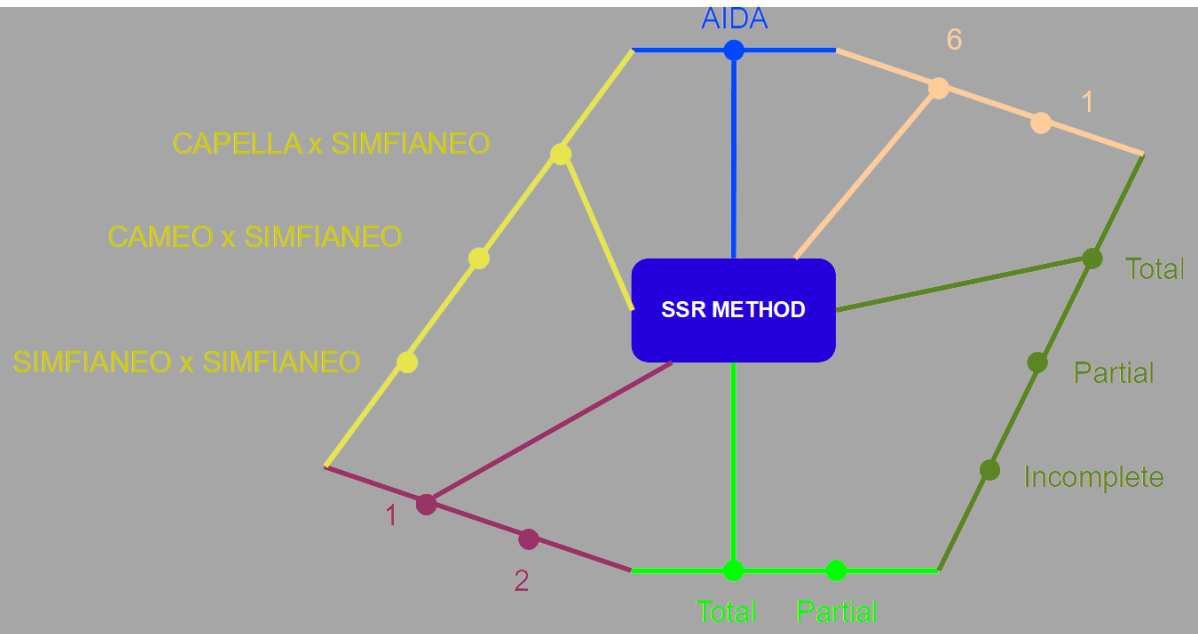
- Is there several iterations ?

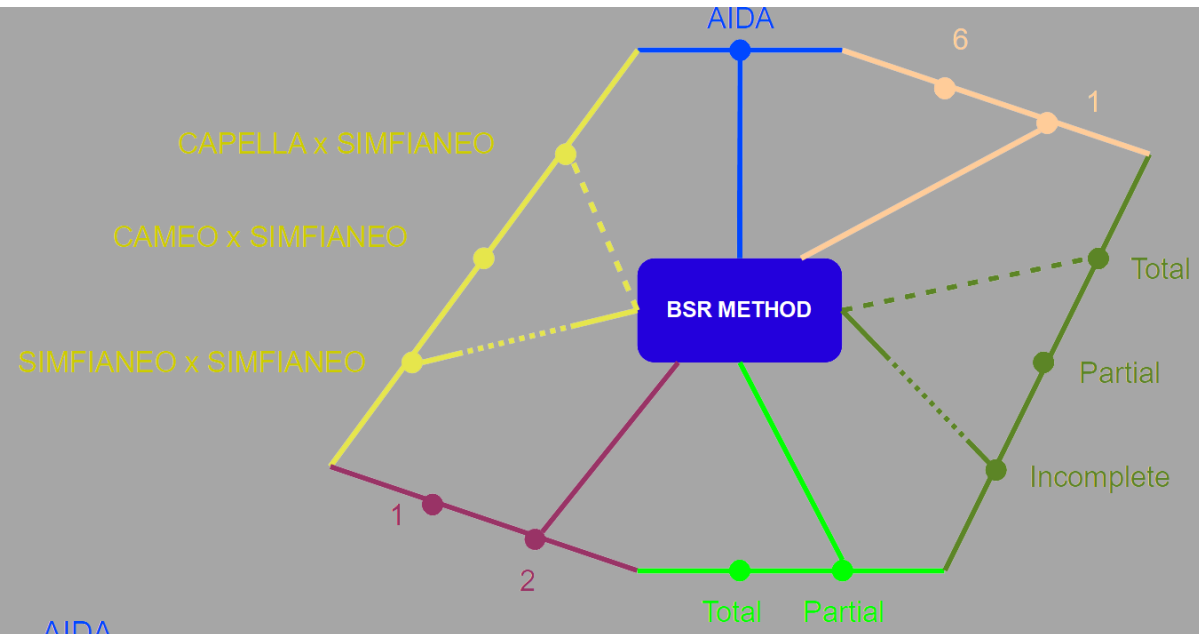


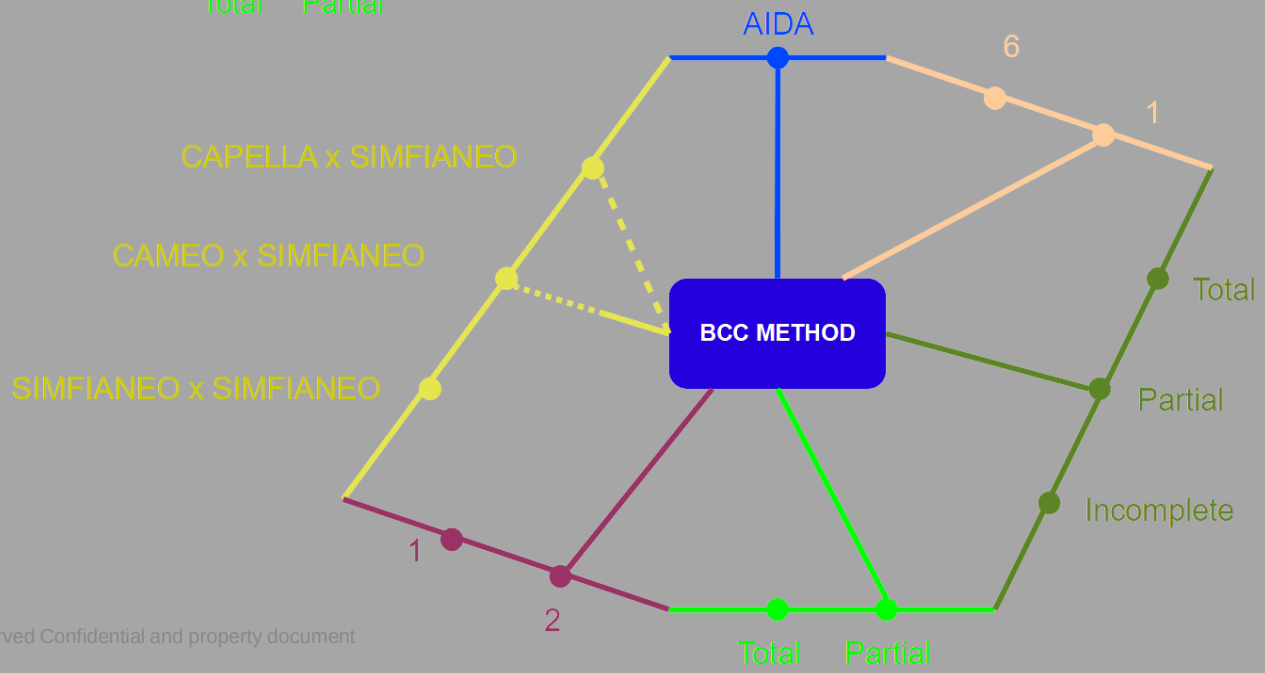
Dimension : Coverage of sub perimeters

- Is all case into sub perimeters covered ?

PoC Dimensioning







- Conclusion -

Limits

Dimensions limitations

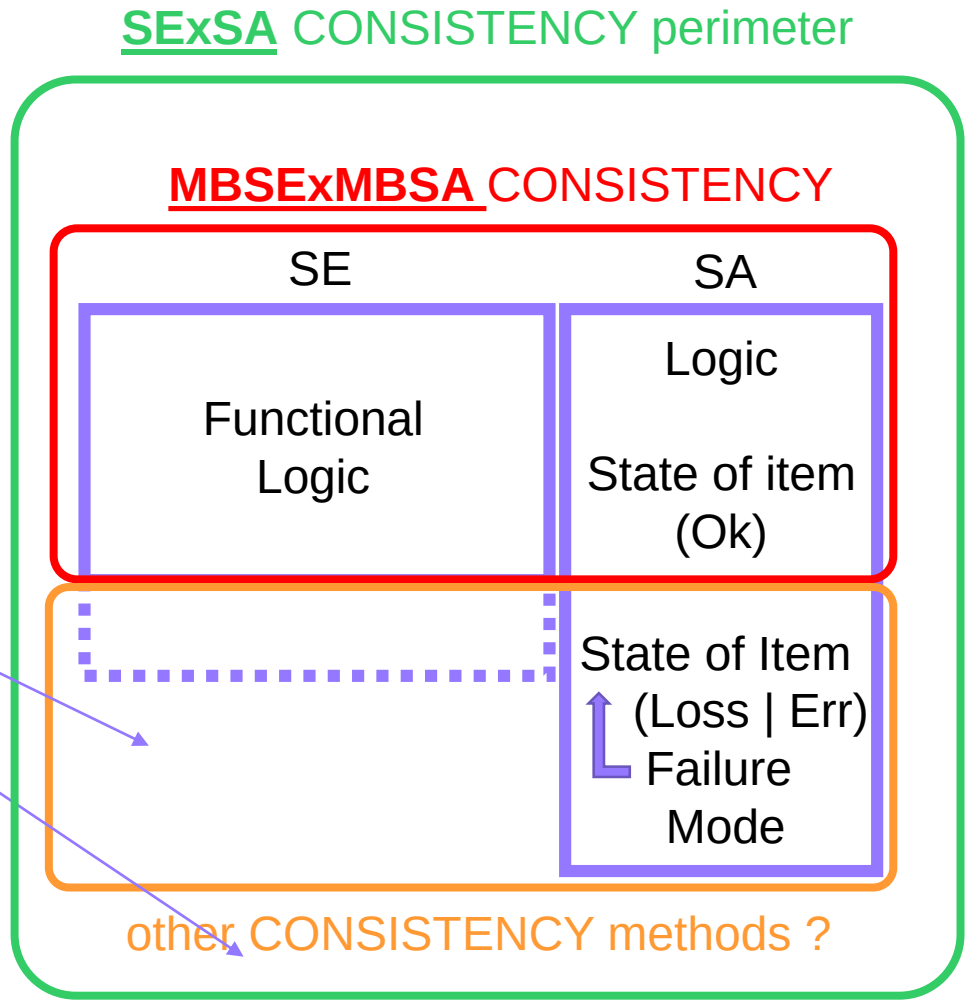
- As described with the polygons previously, frozen dimension and item are de facto “sky”.
- Free authoring induce encompassing case that can be handle by modelling rules

Time and workforce limitations

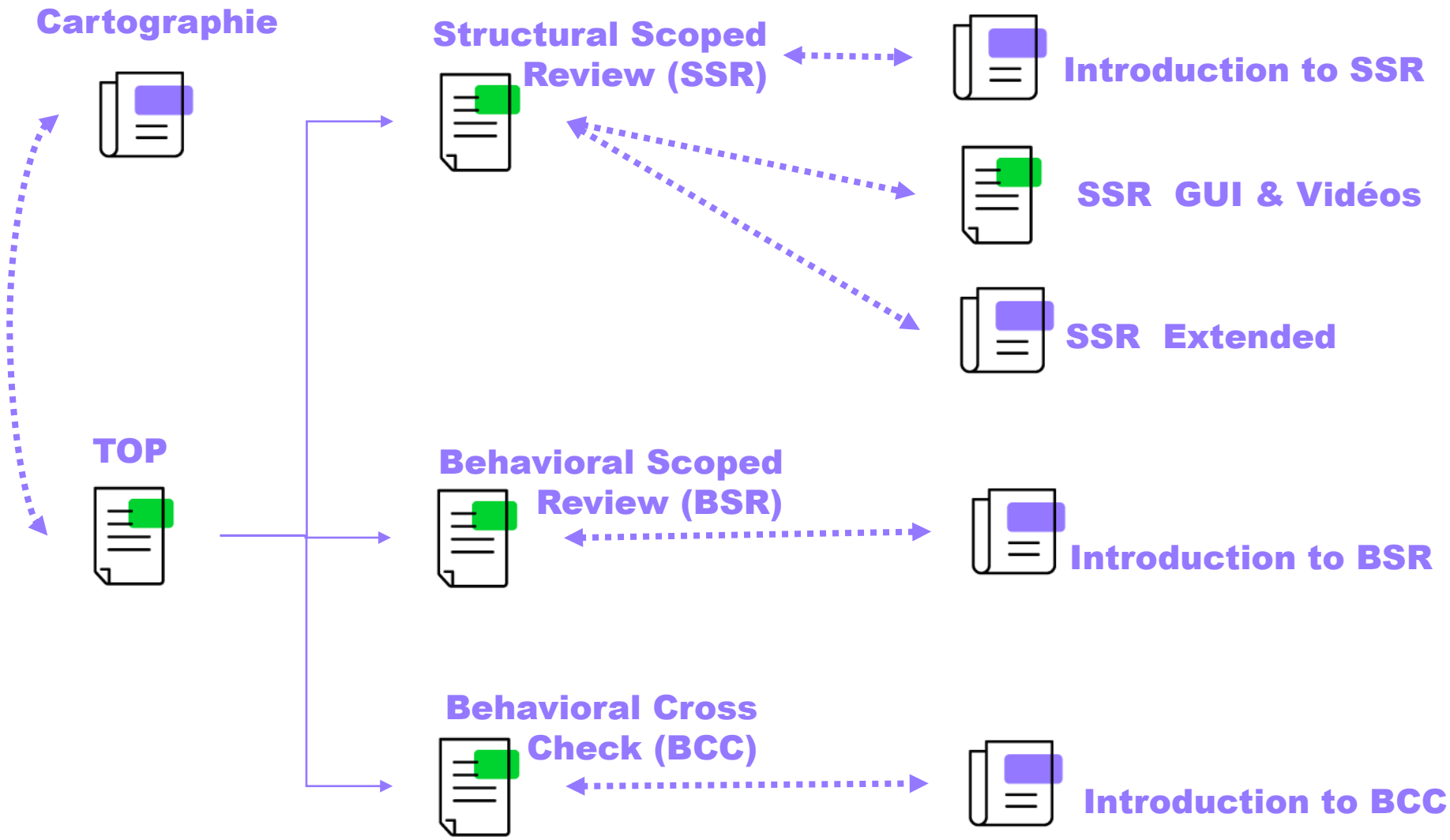
- reduce iteration of BCC and BSR
- reduce BSR deep analyse
- reduce SSR extension to physical part

Intrinsic limitations …

- Matching can neither be 1 to 1
- Matching can neither be strictly 1 to 1
- Not all the reality can be set into model



Where to find informations



- Workshop presentation -

Workshop

Presentation of SSR then BCC only (time constraint) with

- More Details
- Interaction with public
- Retex of methods

- 10 minutes -

Organisation Projet
& Synthèse des résultats

en présence de :

Vincent Marcatté - Président de la **FIT**
Pierre Moller - Responsable de l'action IRT à l'**ANR**
Magali Vaissière – Présidente de l'IRT Saint Exupéry
Denis Descheemaeker - Directeur Général de l'IRT Saint Exupéry

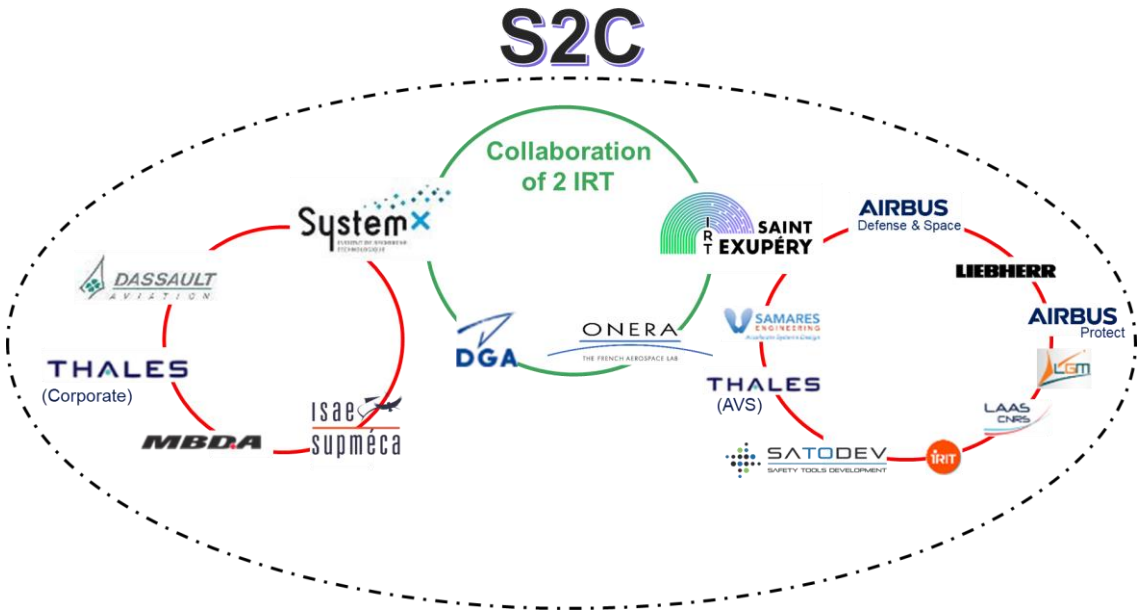
- Rappel de la problématique -

- En Vidéo -

Organisation du projet S2C

Les Chiffres clés du projet

- 17 partenaires (industriels et académiques)
- 3,78 M€ de budget
- 4 années [2019-2023]
- 6,5 ETP (Equivalent Temps Plein)
- > 50 contributeurs
- 2 thèses et 12 publications



Les membres et partenaires S2C

Airbus D&S

Airbus Protect

Dassault Aviation

DGA-TA (Partenaire)

IRIT/INPT (Acc. Thèse)

LAAS/CNRS (Dir. Thèse)

Liebherr

LGM

MBDA

ONERA (Partenaire & Acc. Thèse)

Supméca (Dir. Thèse, Partenaire)

Samares Engineering

SATODEV

Thales AVS

Thales R&T

Les acteurs du projet

L'équipe projet actuelle :

- Michel BATTEUX - IRT SystemX
- Xavier de BOSSOREILLE - AIRBUS Protect
- Jean-Patrick BRUNET – IRT SystemX
- Sylvain CHAMPION – MBDA
- Stephen CREFF - IRT SystemX
- Simon DELAVAULT - LIEBHERR
- Frédéric DESCHAMPS - LGM
- Sébastien DUBE – SAMARES
- Anouk DUBOIS - IRT SystemX
- Christophe FRAZZA – SATODEV
- Sébastien GUILMEAU - THALES AVS
- Anthony LEGENDRE – FRACTUS (Ss traitance)
- Jérémy PERRIN - LGM

- Nikolena CHRISTOFI - IRT St Exupéry
- Julien VIDALIE - IRT SystemX

Les anciens :

- *Patrick FARAIL – IRT Saint Exupéry*
- *Mathilde MACHIN - AIRBUS Protect*
- *Albert GUILLEN-B. - AIRBUS Protect*
- *Romaric DEMACHY – IRT Saint Exupéry*
- *Julien BACLET – IRT Saint Exupéry*
- *François LACRAMPE - LGM*
- *Alain RUAUDEL – LGM*
- *Sophie HUMBERT – SAFRAN*
- *Estelle SAEZ – LIEBHERR*
- *Hanane FADIAW - IRT SystemX*
- *Ismaïl CHEMAM - IRT SystemX*
- *Afef AWADID - IRT SystemX*
- *Colin POUBEL - IRT SystemX*
- *Nicolas HILI - IRT Saint Exupéry*
- *Lucas MASCARO - IRT Saint Exupéry*
- *Julie DE SOUZA - SAMARES*
- *Mihir JOSHI - SAMARES*
- *Mirna OJEDA - SAMARES*
- *Yann MORTIER - AIRBUS Protect*
- *Salvatore INFANTINO - AIRBUS Protect*
- *Hiba EL OUNI - AIRBUS Protect*

Avec la contribution de :

- Laurent BERRY - DGA TA
- Julien CHAOU - LIEBHERR
- Raphaël FAUDOUX - SAMARES
- Jean Luc GARNIER - THALES
- Jean GAUTHIER - DASSAULT
- Emmanuel LEDINOT - THALES
- Xavier LE ROUX - THALES
- Tatiana PROSVIRNOVA - ONERA
- Christel SEGUIN - ONERA

- Claude BARON - *LAAS*
- David CANUT - *Airbus DS*
- Jean-Yves CHOLEY - *ISAE-SUPMECA*
- Christophe DUCAMPS - *Airbus DS*
- Stéphane DUGOWSON - *ISAE-SUPMECA*
- Faida MHENNI - *ISAE-SUPMECA*
- Marc PANTEL - *ENSEEIHT*
- Xavier PUCEL - *ONERA*

Les modalités du travail collaboratif

Réunions équipe hebdomadaires

- Tous les mardi matin sur chaque site IRT et 1 mardi sur 2 entre les CdP IRT St Exupéry et SystemX.
- Point(s) Technique(s) dédié(s) en équipe complète IRT St Exupéry et SysemX entre les instances COPIL/COTECH.

Outils disponibles pour l'équipe

- SimfiaNeo - Cecilia Workshop - OpenAltaRica

Espace de stockage et de collaboration

- Webex, Teams et SharePoint.
- Espace de travail et d'échange entre IRT et Participants sur un espace Sharepoint dédié au projet
- Synthèse des livrables sur Sharepoint

Des points de rencontre avec les membres

- **Jalon Jx** (date anniversaire projet) – *pour un point de situation.*
- **COPIL** tous les 6 mois – *pour la gouvernance projet.*
- **COTECH** tous les 6 mois – *pour les orientations techniques.*

Des groupes de travail ouverts aux membres

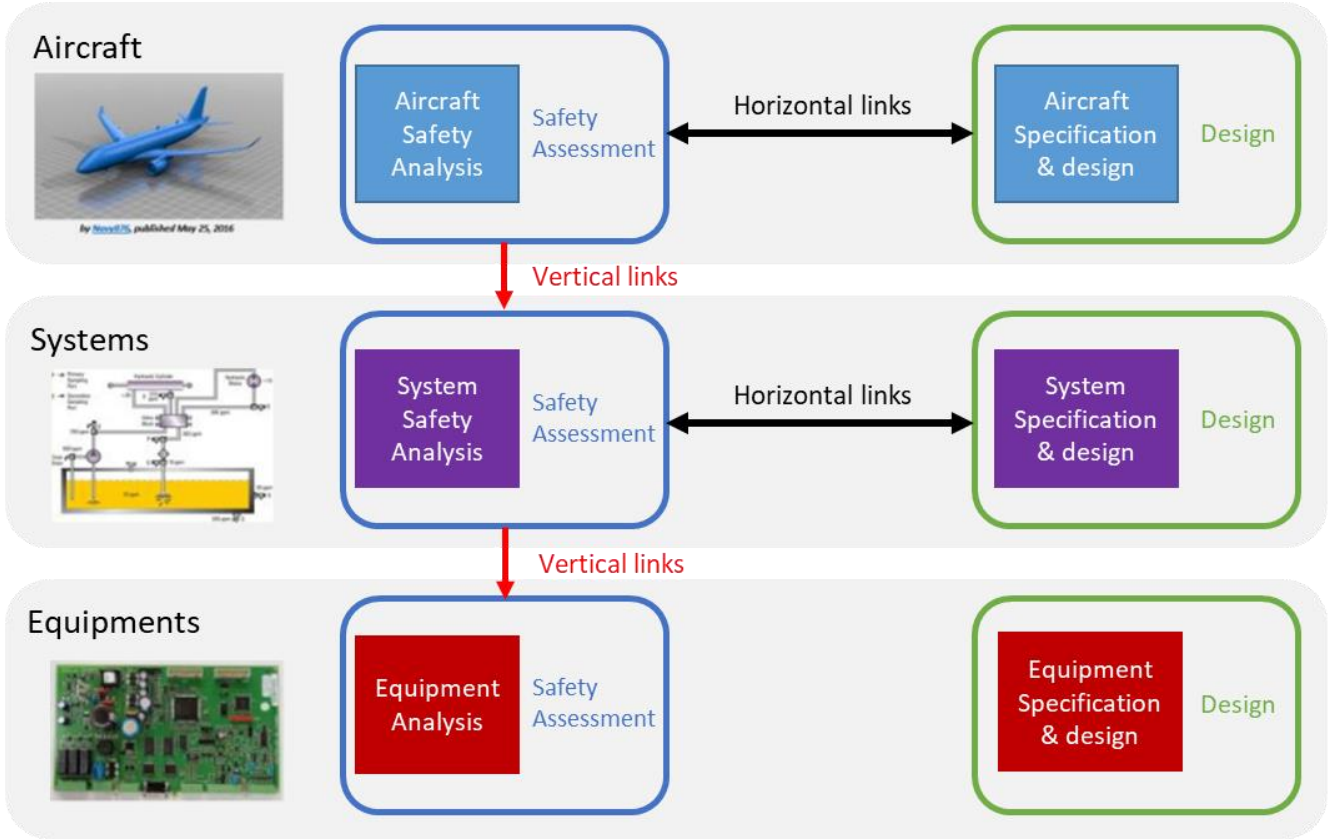
- Ouverts à tous les intéressés.
- Par sujets de réflexion (intrinsèques aux lots).
- Berceau des idées et orientations des travaux.

Le partage des résultats

- Par la relecture des livrables.
- Par disponibilité des travaux et CR des groupes de travail.
- Par la mise à disposition de la mise à jour du Use Case AIDA.

Structure du projet et travaux

L'objectif du projet S2C

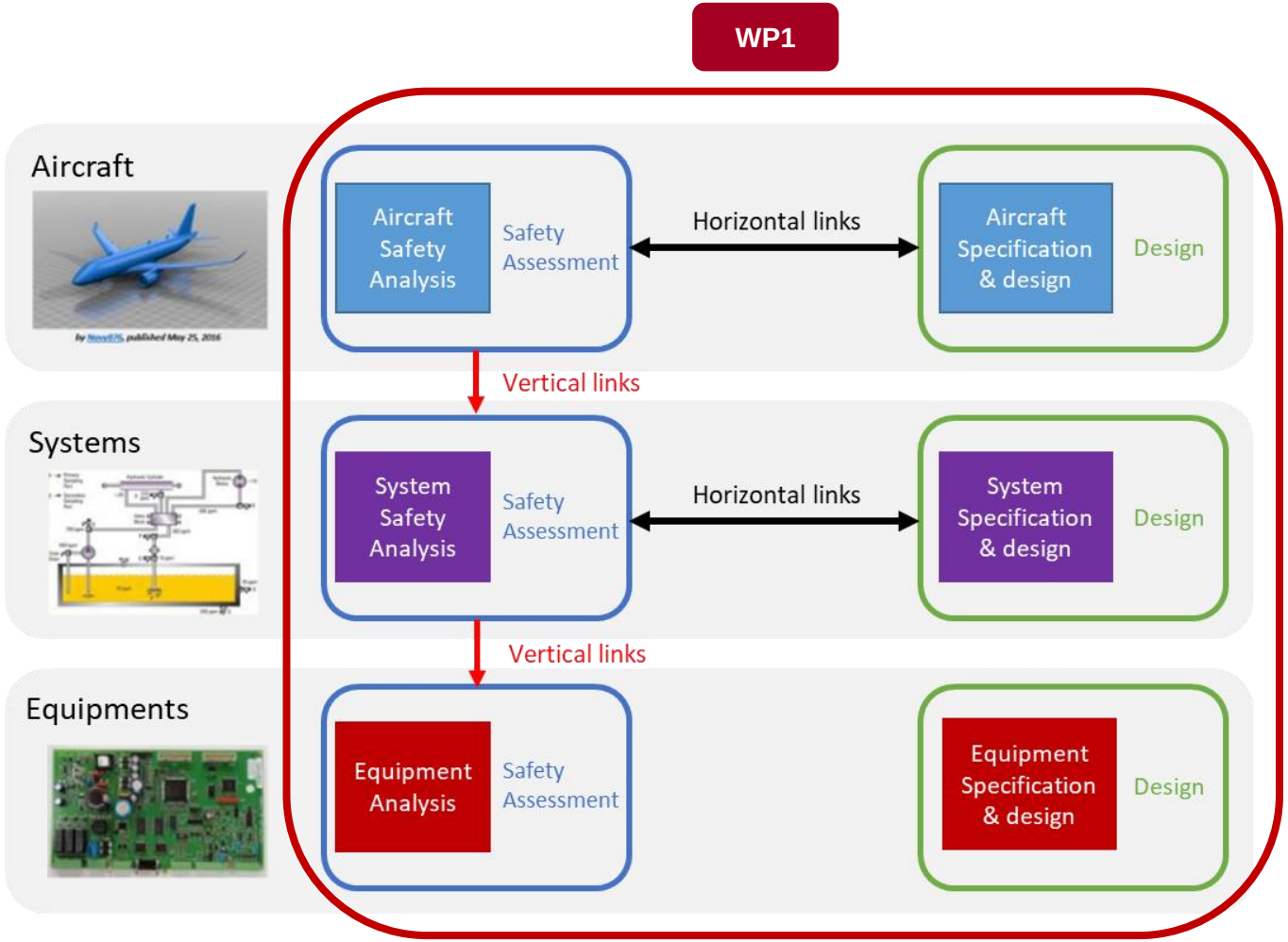


Définir des **processus, méthodes et outils** permettant de garantir que les **analyses de sûreté** et de la modélisation système réalisées par l'architecte système **(MBSE)** sont **cohérentes**, dans un contexte de continuité numérique, sur l'ensemble des **cycles itératifs de développement** des produits et systèmes, et répondant aux **contraintes de certification**.

Le projet se compose de 4 Axes de recherche (Lot de travail) pour atteindre ces objectifs.

Ils se concentrent soit sur des boîtes de ce schéma, soit sur des liens.

L'objectif du projet S2C

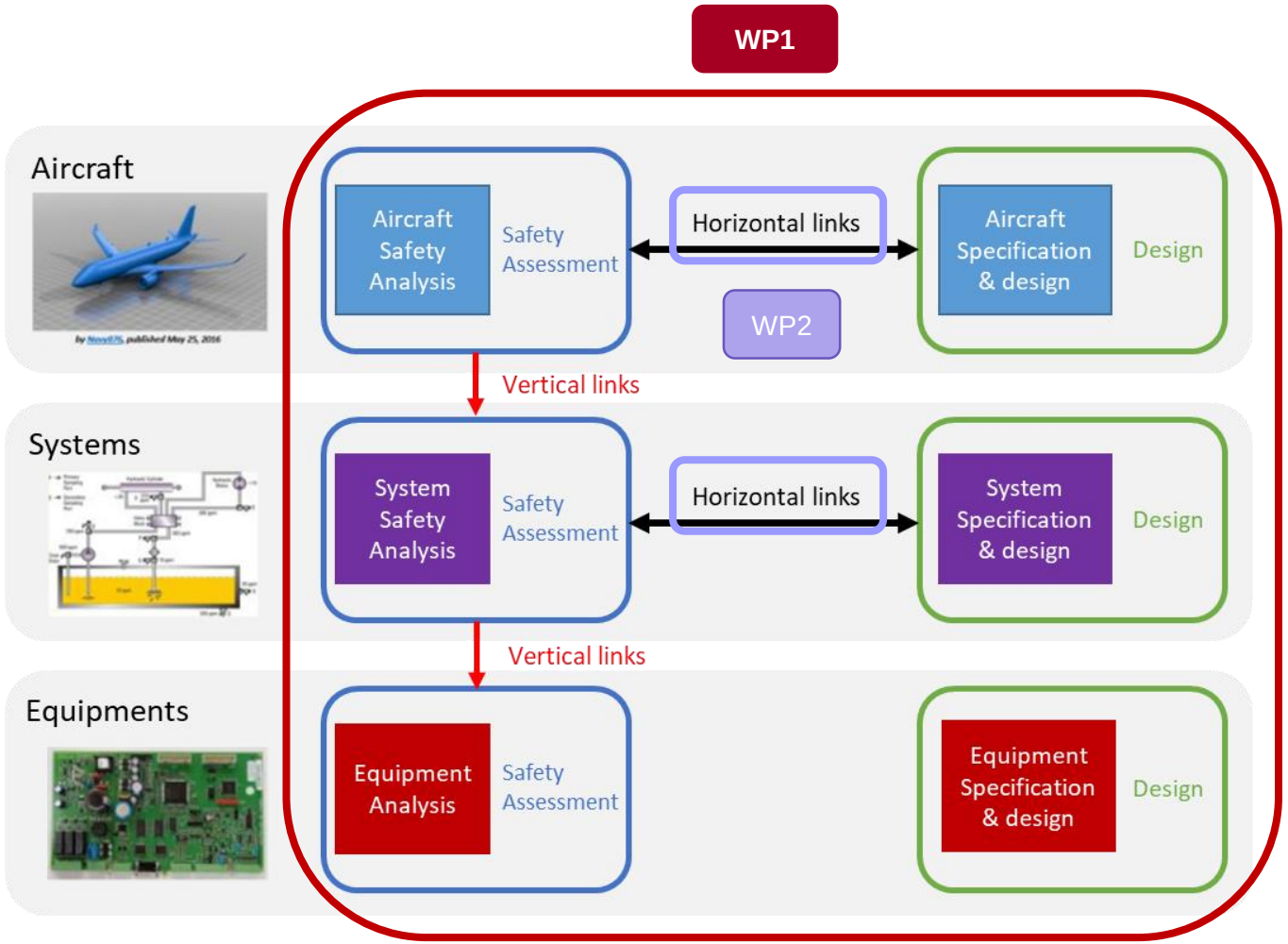


WP1
Processus global de développement

Cas d'utilisation commun

« SE-SA »

L'objectif du projet S2C



WP1
Processus global de développement

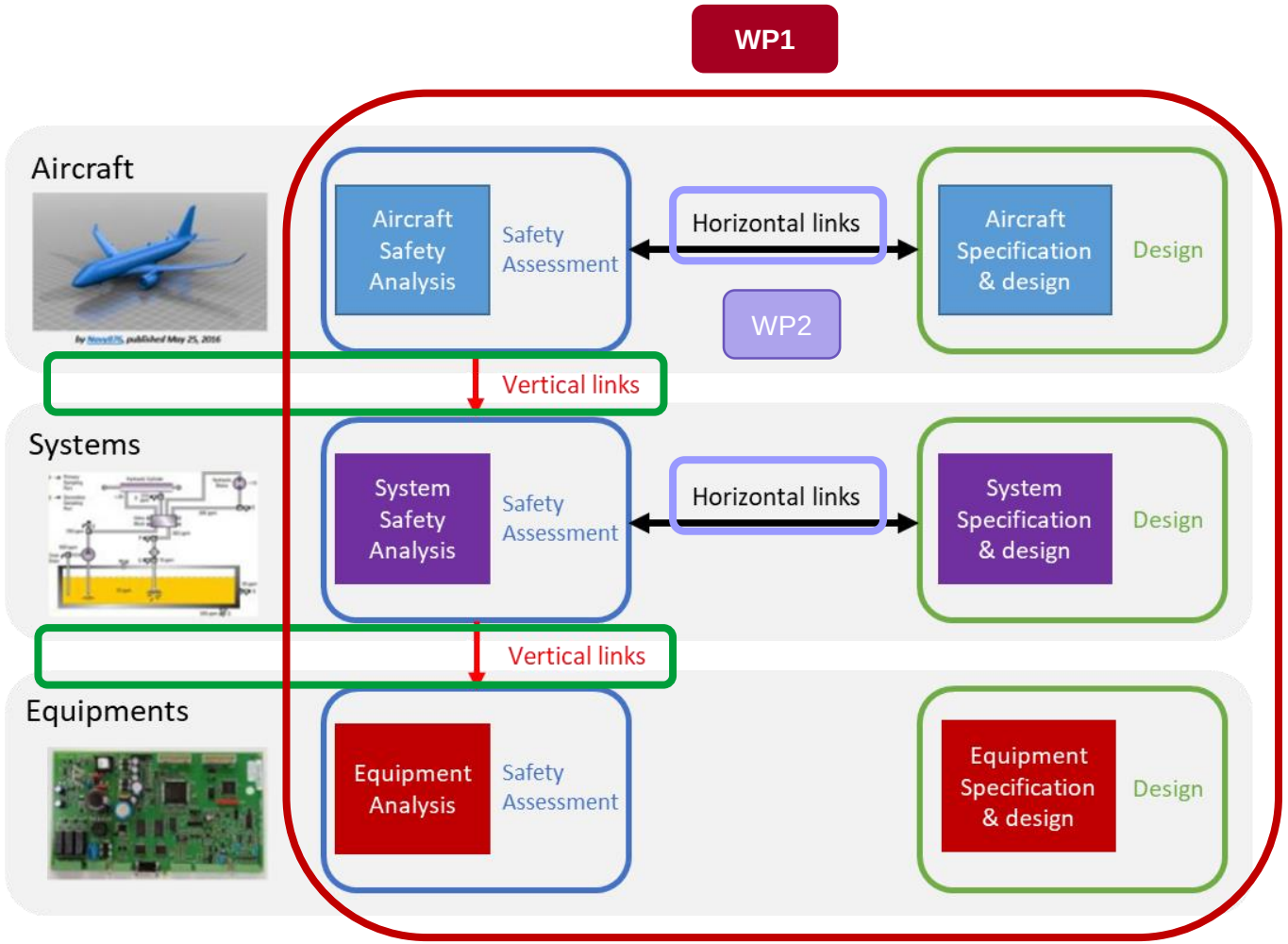
Cas d'utilisation commun

« SE-SA »

WP2
Méthode de cohérence entre MBSE et MBSA au même niveau systémique

« MBSE-MBSA »

L'objectif du projet S2C



WP3

WP1
Processus global de développement

Cas d'utilisation commun

« SE-SA »

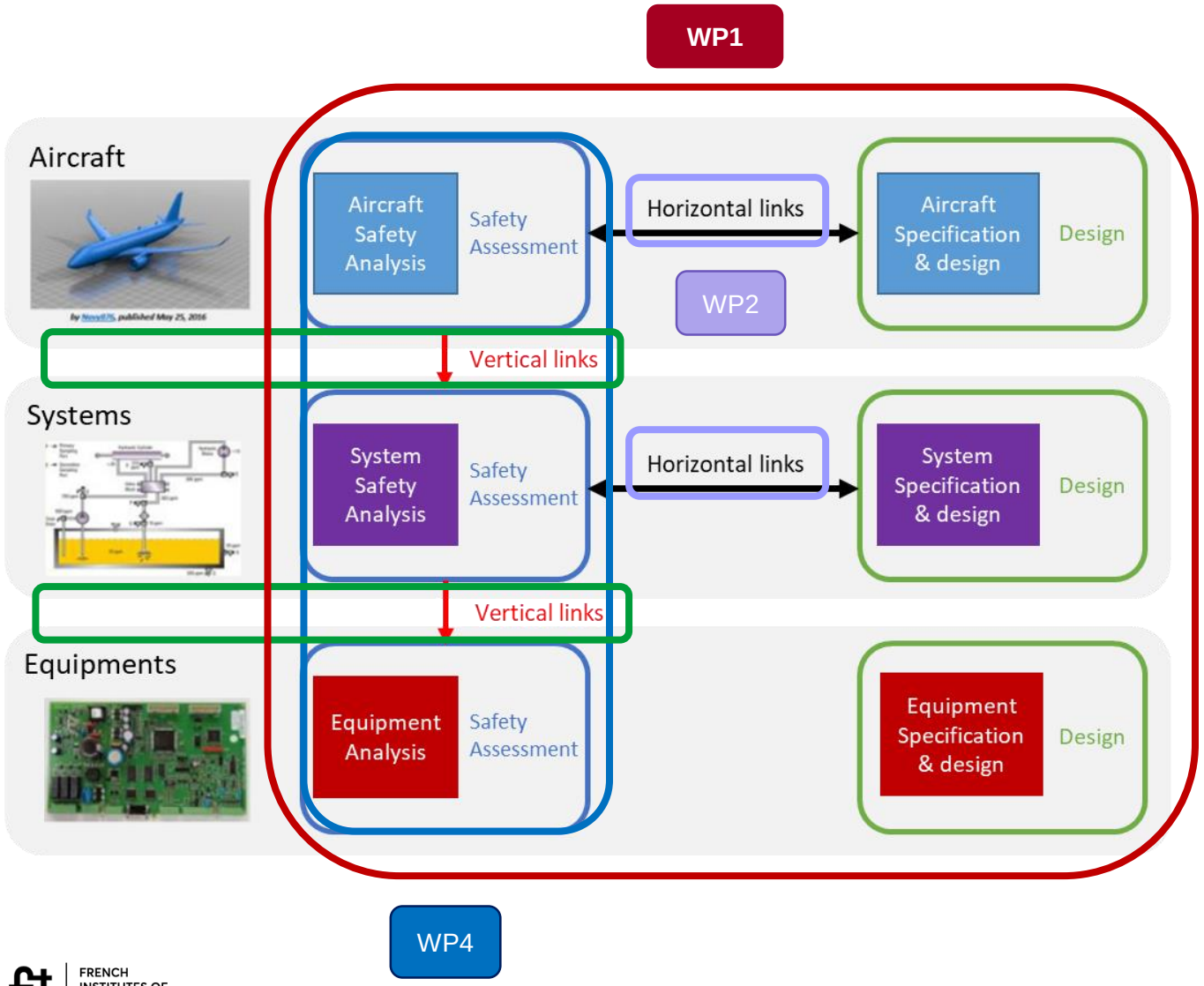
WP2
Méthode de cohérence entre MBSE et MBSA au même niveau systémique

« MBSE-MBSA »

WP3
Méthode de cohérence SA entre les niveaux systémiques

« SA-SA »

L'objectif du projet S2C



WP1
Processus global de développement

Cas d'utilisation commun

« SE-SA »

WP2
Méthode de cohérence entre MBSE et MBSA au même niveau systémique

« MBSE-MBSA »

WP3
Méthode de cohérence SA entre les niveaux systémiques

« SA-SA »

WP4
Méthode de modélisation MBSA

« MBSA »

FRENCH INSTITUTES OF TECHNOLOGY

S2C Project Objectives

- ## Rappel de l'objectif :

  Définir des **processus, méthodes et outils** permettant de garantir que les **analyses de sûreté** et la modélisation système réalisées par l'architecte système **(MBSE)** sont **cohérentes**, dans un contexte de continuité numérique, sur l'ensemble des **cycles itératifs de développement** des produits et systèmes, et répondant aux **contraintes de certification**.

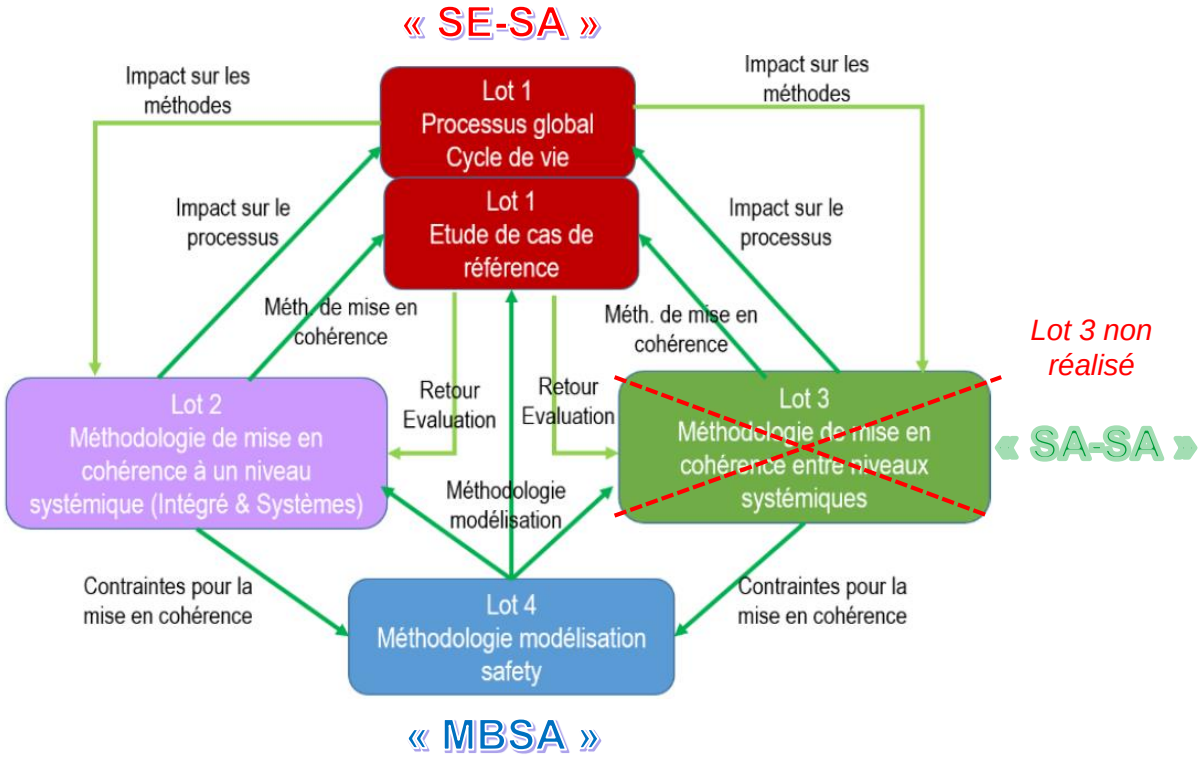
- ## Livrables cibles :

  - Méthodes de mise en cohérence SE/SA
  - Méthodes et lignes directrices pour le MBSA
  - Méthode/processus de synchronisation MBSE/MBSA
  - Spécification d'évolution d'outils existants
  - Prototype d'outils
  - Cas d'utilisation pour illustrer les propositions
  - Transfert de compétences vers les membres et la communauté

- ## Cas d'utilisation :

  - **AIDA** (drone d'inspection préalable au vol) - Open Source issu du projet MOISE (IRT Saint Exupéry)
  - Cas d'utilisation de référence pour tous les travaux

  https://sahara.irt-saintexupery.com/AIDA/



Bilan des travaux

Niveau Projet

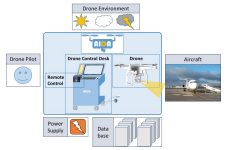
Rapport état de l'art

Publications et actions de Dissémination

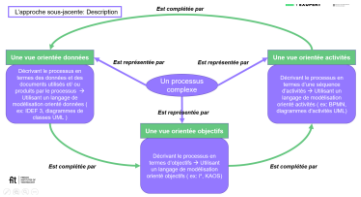
Axe A « SE-SA »

Processus global et traçabilité

Cas d'utilisation AIDA
- Modèles & documents disponibles

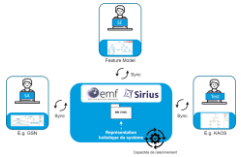


Processus multi-vues
- Orientée Objectifs
- Orientée Activités
- Orientée Données



POC traçabilité & impacts
- Plan de traçabilité générique
- Instancié sur AIDA & REX

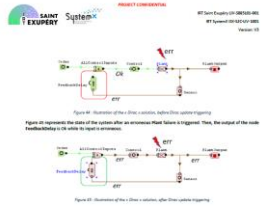
Compatibilité
- Exploration modèle de compatibilité
- Nouvelle abstraction



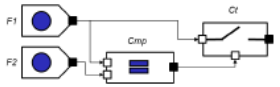
Axe B « MBSA »

Guide méthodologique MBSA

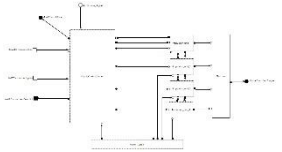
Guide méthodologique (AltaRica)
- Plusieurs niveaux de lecture
- Illustré par un cas simple
- Aborde les problématiques concrètes de modélisation



Get Started
- Basé sur le guide
- Format présentation pour débuter



Modélisations AIDA
- Basé sur le guide
- Format présentation pour débuter

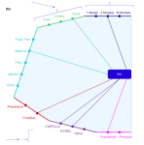


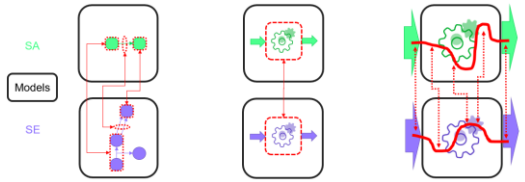
Note Technique de REX modélisation AIDA
- Les questions posées
- Les hypothèses et arbitrages

Axe C « MBSE-MBSA »

Méthode de cohérence entre MBSE et MBSA au même niveau systémique

Méthodes
- Cartographie de la problématique
- Introduction aux 3 méthodes
- Description de 3 méthodes :
  - Structural Scoped Review (SSR)
  - Behavioral Scoped Review (BSR)
  - Behavioral Cross Check (BCC)



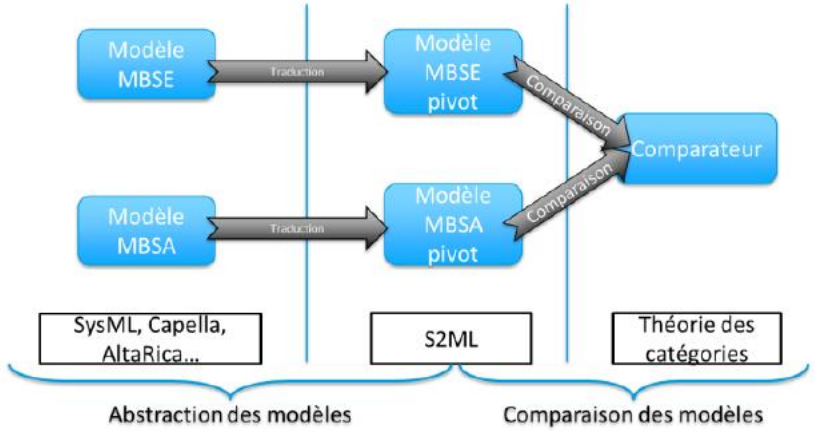


POC & Outils au service de la cohérence
- Cohérence structurelle SSR
- Cohérence comportementale BCC

Les Thèses

Théorie des catégories pour la cohérence des modèles multi-niveaux système (MBSE) et sûreté de fonctionnement (MBSA)

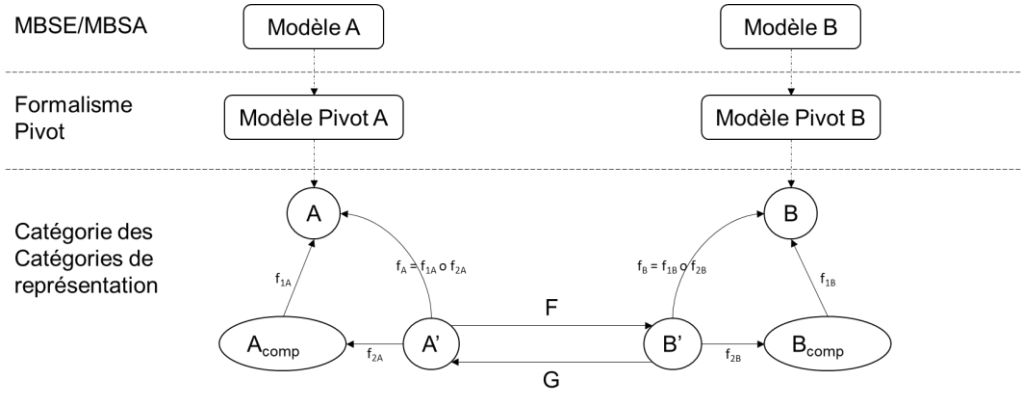
Par Julien Vidalie



Objectif : formaliser, au moyen de la théorie mathématique des catégories, la comparaison de modèles S2ML (System Structure Modeling Langage), issus de la traduction d'un modèle MBSE et d'un modèle MBSA (via l'approche SmartSync).

Résultats :

- Proposition d'un cadre mathématique (théorie des catégories) qui traduit la relation de cohérence
- Démonstration du cadre mathématique sur le drone Zipline Flyer (Modèles AltaRica 3.0, SysML et Modelica)



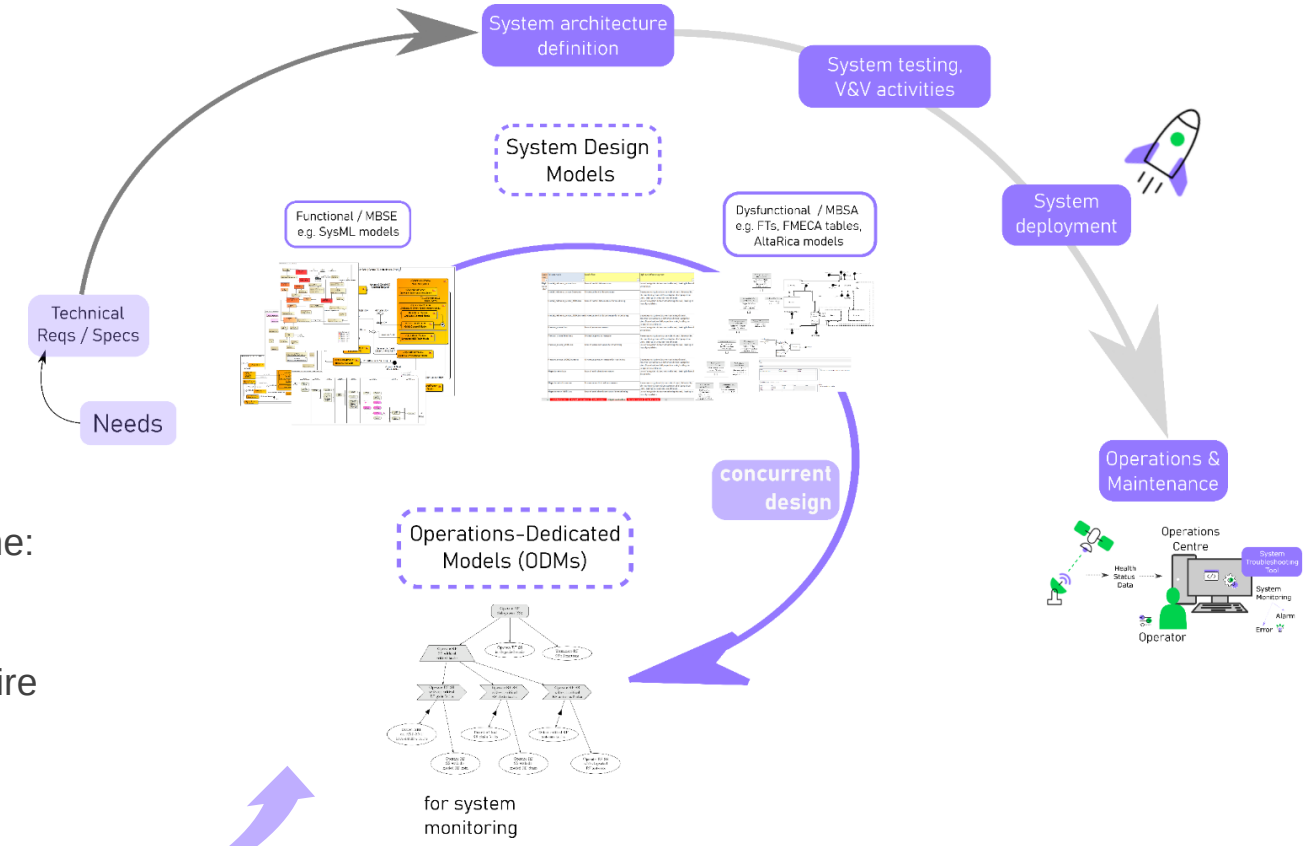
Les Thèses

Améliorer le diagnostic en opération par une approche de modélisation interdisciplinaire.

Par Nikolena Christofi

Co-création de modèles dédiés à la surveillance système avec des modèles de conception système (fonctionnels et dysfonctionnels), en utilisant des Arbres de Comportement.

- Introduire des objectifs liés au diagnostique opérationnel (maintenance opérationnelle) dès le début du cycle de développement système.
- Amélioration continue de l'architecture système (retour aux équipes MBSE & MBSA par des opérateurs).
- Améliorer le diagnostique opérationnel en accompagnant les opérateurs dans leurs activités de recherches de panne:
  - meilleure vue d'ensemble de l'architecture système
  - accès facile et rapide aux données pertinentes pour faire le diagnostique
  - orienter une diagnostique (pinpoint fault candidates)



Développement agile de systèmes complexes

FRENCH INSTITUTES OF TECHNOLOGY

Bilan des travaux

Un objectif fort de communiquer et diffuser les résultats pour la montée en compétences et en maturité dans l'utilisation des modèles

Un site internet accessible et des livrables à large diffusion

www.irt-saintexupery.com/s2c

Une boîte à outils méthodologique

- Processus, méthodes et recommandations
- Guides méthodologiques
- Use Case d'application partagé
- Outils de mise en œuvre (POC)

- Les livrables -

Liste détaillée des livrables

Contrat	Réf.	v.	Titre
L-0	LIV-S085L01-001 ISX-S2C-LIV-1001	V2	State of the Art of the S2C Project
L1.1	LIV-S085L01-003 ISX-S2C-LIV-1235	V2	Méthodes de mise et de maintien en cohérence SE/SA (livrable chapeau)
	NT-S085L01-055 ISX-S2C-DOC-464	V2	Modèle multi vues
	NT-S085L01-056 ISX-S2C-DOC-465	V1	Vulgarisation du process SE/SA
	NT-S085L01-057 ISX-S2C-DOC-466	V1	Vulgarisation du plan de traçabilité
	NT-S085L01-058 ISX-S2C-DOC-467	V1	Plan de traça instancié à AIDA
	NT-S085L01-059 ISX-S2C-DOC-468	V1	Retex plan de traçabilité appliqué à AIDA
	NT-S085L01-060 ISX-S2C-DOC-469	V1	Plan de traça optimisé avec recommandations
	NT-S085L01-061 ISX-S2C-DOC-470	V1	Checklists SE & SA support aux revues
L1.2	LIV-S085L01-004 ISX-S2C-LIV-1444	V3	Cas d'étude complet AIDA
L1.3	LIV-S085L01-005 ISX-S2C-LIV-1626	V1	POC Dynamic Consistency Management (Doc chapeau)
	NT-S085L01-047 ISX-S2C-DOC-471	V1	POC Dynamic Consistency Management
	NT-S085L01-048 ISX-S2C-DOC-472	V1	Stage « cohérence dynamique » (pré étude du POC)
	NT-S085L01-049 ISX-S2C-DOC-473	V1	Arbres de décision pour l'aide à la cotation de la sévérité d'un impact SE->SA (critique, majeur, mineur)
	NT-S085L01-050 ISX-S2C-DOC-474	V1	Notice d'utilisation du POC
L1	LIV-S085L01-002 ISX-S2C-LIV-1627	V1	Analyse Outils COTS et Spec de besoins (Doc chapeau)
	NT-S085L01-051 ISX-S2C-DOC-475	V1	Document de spécification des évolutions des outils COTS (synthèse des nouveaux besoins)

Contrat	Réf.	v.	Titre
L1	NT-S085L01-052 ISX-S2C-DOC-476	V1	Cartographie des outils de traçabilité
	NT-S085L01-053 ISX-S2C-DOC-477	V1	Illustration de l'instanciation du plan de traça AIDA dans SECOLLAB
new	NT-S085L01-054 ISX-S2C-DOC-478	V1	Pré-étude Compatibilité : Pré-étude, Modèle, résultat Stage compatibilité
L2.3	NT-S085L02-015 ISX-S2C-DOC-351	V1	Assesment of 3D Exerience to implement a method for MBSE/MBSA consistency
	NT-S085L02-034 ISX S2C DOC-455	V3	Cartography
	LIV-S085L02-007 ISX-S2C-LIV-1037	V6	Method to ensure and to maintain consistency of systemic levels & Validation report
L2.3 & L2.2	LIV-S085L02-023 ISX-S2C-DOC-436	V3	Structural Scoped Review method
	NT-S085L02-040 ISX S2C DOC 458	V0	Introduction to SSR
	NT-S085L02-031 ISX S2C DOC-454	V1	Technical Note – Extended SSR
	LIV- S085L02-024 ISX-S2C-DOC-437	V6	Behavioural Scoped Review method
	NT-S085L02-041 ISX S2C DOC-459	V0	Introduction to BSR
	LIV- S085L02-025 ISX-S2C-DOC-438	V6	Behavioural Cross Check method
	NT-S085L02-042 ISX S2C DOC-460	V0	Introduction to BCC
L2.4	LIV- S085L02-008 ISX-S2C-LIV-1628	V1	POC SSR - S2C structural consistency tool Installation & User Manual
L4.1	LIV-S085L01-001 ISX-S2C-LIV-1285	V4	MBSA Modelling guide and validation report
			The Get Started
L4.2	NT-S085L01-046 ISX-S2C-DOC-480	V1	Complements and recommendations of the MBSA modelling guide

- La dissémination -

Disséminations internes

Partenaires	Date	Sujet
AIRBUS PROTECT	05/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
LIEBHERR	11/2022	Méthodologie MBSA – Présentation détaillée du guide et du Get Started pour utilisation sur nouveaux projets.
	06/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
LGM	01/2023	Méthodologie MBSA – Présentation détaillée du guide et du Get Started.
THALES	06/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
	01/2023	Présentation d'ensemble du projet & Discussions.
MBDA	05/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
	01/2023	Présentation détaillée des Proof Of Concept (POC) des méthodologies de cohérence MBSE et MBSA.
AIRBUS DS	06/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
SAMARES	06/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
DASSAULT AVIATION	07/2022	Présentation processus SE-SA en BPMN et plan de traçabilité
Tous	[2019 – 2023]	- 7 COTECH - 10 COPIL - 4 Jalons -

Disséminations externes (conférences)

Dates	Conférence	Lieu	Sujet
19 juin 2019	**Journée AFIS**	Paris	Présentation du projet
16 au 18 octobre 2019	**IMBSA 2019**	Thessaloniki	Lot 2
12 novembre 2020	**MOSIM**	Agadir	Thèse NC
24 novembre 2020	**Lambda MU 22**	*distanciel*	Thèse JV
1 et 2 juin 2022	**ERTS**	Toulouse	Lot 2 et Thèse NC
5 au 7 septembre 2022	**IMBSA 2022**	Munich	Lot 4
12 au 16 septembre 2022	**EUROCAE**	Lindenberg	Lots 2 et 4
14 au 16 septembre 2022	**DX 2022**	Toulouse	Thèse NC
5 et 6 octobre 2022	**ISCLP**	Toulouse	Lot 1
10 au 13 octobre 2022	**Lambda MU 23**	Paris Saclay	Lot 4
23 au 28 octobre 2022	**MODELS 2022**	Montréal	Thèse NC
24 au 26 octobre 2022	**ISSE 2022**	Vienne	Thèse JV
16 novembre 2022	**GIFAS SDF 2022**	Paris	Lot 2
22 au 24 novembre 2022	**ESA MBSE 2022**	Toulouse	Thèse NC (Poster)
6 au 8 décembre 2022	**Forum Académie Industrie AFIS**	Toulouse	Thèse NC (Poster)
6 au 10 mars 2023	**SpaceOps 2023**	Dubaï	Thèse NC

Bilan des publications

Titre	Auteurs	Date	
Article : Modeling Functional Allocation in AltaRica to Support MBSE/MBSA Consistency – **IMBSA 2019**	Mathilde Machin, Estelle Saez, Pierre Virelizier, Xavier de Bossoreille	16/10/2019	
Article : Typology of the differences Between Model-Based System Engineering (MBSE) and Safety Assessment (MBSA) models: Analysis of a Reference System – **Lambda Mu 2020**	Julien Vidalie	Présenté le 10/11/2020	
Article : State Machines Consistency between Model Based System Engineering and Safety Assessment Models – conference **IEE ISSE 2021**	Julien Vidalie	Présenté en oct 2021	
Article : Short paper – Structural consistency of MBSE and MBSA models using Consistency Links – **ERTS 2022**	Romaric Demachy et Sébastien Guilmeau	Présenté en juin 2022	
Article : Towards an agile, model-based multidisciplinary process to improve operational diagnosis in complex systems – **ERTS 2022**	Nikolena Christofi	Présenté en juin 2022	
Article : Category Theory Framework for System Engineering and Safety Assessment Model Synchronization Methodologies – **journal MDPI**	Julien Vidalie	Article paru en juin 2022	
Article : Strategies for modelling failure propagation in dynamic systems with AltaRica – **IMBSA 2022**	Xavier de Bossoreille, Frédéric Deschamps, Christophe Frazza, Jean Gauthier, Tatiana Prosvirnova, Christel Seguin Estelle Saez	Présenté en sept 2022	
Article : Consistency of multiple system engineering models of a fixed wing drone – **IEE ISSE 2022**	Julien Vidalie	Présenté en oct 2022	
Article : Stratégies de modélisation AltaRica de la propagation de défaillances dans les systèmes dynamiques – conférence - **Lambda Mu 2022**	Tatiana Prosvirnova, Christel Seguin, Christophe Frazza, Estelle Saez, Mathilde Machin, Xavier de Bossoreille, Jean Gauthier, Pierre Darfeuil, Frédéric Deschamps	Présenté en oct 2022	
Article : A Digital Twins Modelling Methodology for System Operations using Fault Trees and Behaviour Trees – conference - **MODELS 2022**	Nikolena Christofi	Présenté en oct 2022	
Article : Introducing Operational Diagnosis Models for Ground Station Architectures using Behaviour Trees, 17th International Conference on Space Operations - **SpaceOps 2023**	Nikolena Christofi, Xavier Pucel, Claude Baron, Marc Pantel, David Canu, Jerome Golenzer, Christophe Ducamp.	Présenté en mars 2023	
Article : Towards an Operations-Dedicated Model for Space Systems – **journal JAIS** (Journal of Aerospace Information Systems - AIAA Aerospace Research Central (ARC))	N. Christofi, X. Pucel, C. Baron, M. Pantel, S. Guilmeau, C. Ducamp.	article paru en mars 2023	

Témoignages de Partenaires

« S2C a abordé avec pragmatisme et sens du retour sur investissement à court terme le difficile problème de la cohérence de modèles entre ingénierie système et évaluation de la sûreté de fonctionnement. Des avancées significatives également en méthodologie de modélisation de la propagation des modes de défaillance. » - ***E. Ledinot - THALES***

« La collaboration avec les équipes de l'IRT Saint Exupéry durant les 4 années du projets S2C nous aura permis d'enrichir notre compréhension de l'état de l'art de l'ingénierie basée sur les modèles et de faciliter son déploiement au sein de notre organisation. La diversité des parties prenantes du projet et leur expérience ont permis des échanges riches basés sur des résultats d'études pratiques. Enfin, les équipes de l'IRT Saint Exupéry se sont toujours montrées disponibles, créatives et à l'écoute des problématiques que les contributeurs au projet pouvaient rencontrer. » - ***J. Chaou - LIEBHERR***

« Le projet S2C a mis en évidence le résultat positif de ce travail collaboratif grâce à l'apport et pertinence des parties prenantes. Les résultats livrés ont permis de répondre aux exigences attendues et d'aller même au delà en ouvrant de futures perspectives dans la continuité du projet S2C. Par exemple la thèse de Nikolena Christofi, qui avec modestie a permis de mettre en évidence des relations formelles entre le monde fonctionnel et dysfonctionnel par une approche méthodologique novatrice et pleine de promesses pour améliorer le traitement de la complexité de nos univers de demain. » - ***Ch. Ducamp - AIRBUS D&S***

« Le projet S2C a été un fructueux support d'échanges entre les différents acteurs du MBSE et MBSA, aussi bien académiques qu'industriels. Il a permis à l'autorité et client DGA d'observer et de challenger les tendances dans ces domaines. La DGA est fière d'avoir contribué au projet S2C dont la qualité des livrables réalisés va au-delà des objectifs initiaux du projet. Ces livrables vont permettre d'initier de futurs projets aussi bien orientés sur la recherche que sur des applications chez les industriels en interaction avec la DGA. » ***L. Berry - DGA***

Merci de votre attention

23 mars 2023

Contact :

systems-engineering@irt-saintexupery.com

Appendixes

Appendixes
-
Project Definitions

Project Definitions

S2C : System & **S**afety **C**ontinuity

Consistency : Alignment between understanding of Safety analyst and System Engineer. Ensure Data Consistency consists in verifying that SE Data inputs are well and right taken into account by the Safety Analyst so that System Engineer and Safety Analyst share the same vision of the system.

MBSA : Technique which models system content and behaviour in order to provide safety analysis results. MBSA employs an analytical model called a Failure Propagation Model **(FPM) – [ARP4761A]**

Note: in literature, the MBSA acronym also stands for "Model-Based Safety Assessment". In this case, it refers to the safety analyses results.

MBSE : The formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases. [**INCOSE Vision 2020**]

Appendixes

-

Details on the Framing of Solutions

(frozen) dimensions : Why two models ?

SA specialist's needs vs SE specialist's needs are differents, are the tools ready for the union of both?

- SA needs to « **implement** the **dysfunctionnal** behavior of a block » (internal perspective)
  while SE needs to « **shape** the **functional** behavior of an allocated block » (external perspective)

- SA needs a tight integration of their engine (to debug dysfunctionnal behavior and compute cut-set, sequence etc) with the model editor
  not all SE modelers offer this and the ones remaining needs lot of investments (it is not Out Of the Box and also authoring method dependant)

Some members already explore single model on their side

- No concurrency between company internal R&D and IRT,
  better explore what is left apart than redo what is already explore outside.

Previous project at IRT (MOISE) explored multi-model agregation in Extended-Enterprise

- Return of experience on mono-model vs poly-model question has influenced the decision for this project.

(In)Dependance from Authoring dimension ?

- The coupling of authoring and models is often considered (due to tool development convenience) but they are indepdendent
  (i.e. one UI can dispatch and assemble data from different models, each one responsible of its own perimeter)

(frozen) dimensions : Why none-coupled authoring ?

Independancy of artefact

How is influenced the SA specialist's assessment if he/she reuses fully or partially SE's artefacts ?

But SE and SA team (so their brains) are differents is using the same tool remains commonalty?

⇒ The question is raised with no answer currently

⇒ so projet choose to be conservative having 2 models

Model Specialities does not have same life time, are the tools ready ?

SA specialist does their assesment on a baselined architecture (not a rolling release one)

But tools for monolithic model are not all able to freeze the SE subpart while the SA will evolve on versionning

⇒ The conservative approach was to consider the freedom of versionning regarding its life time

(this is easy doable with a two model approach)

Authoring shall be considered decoupled from model cardinality (1 or 2)?

This dimension is independant from the cardinality because authored data can be filled into several models e.g. a breakdown can be reproduced in 2 model applying authoring rules of each model.

(frozen) dimensions : Why Functional only ?

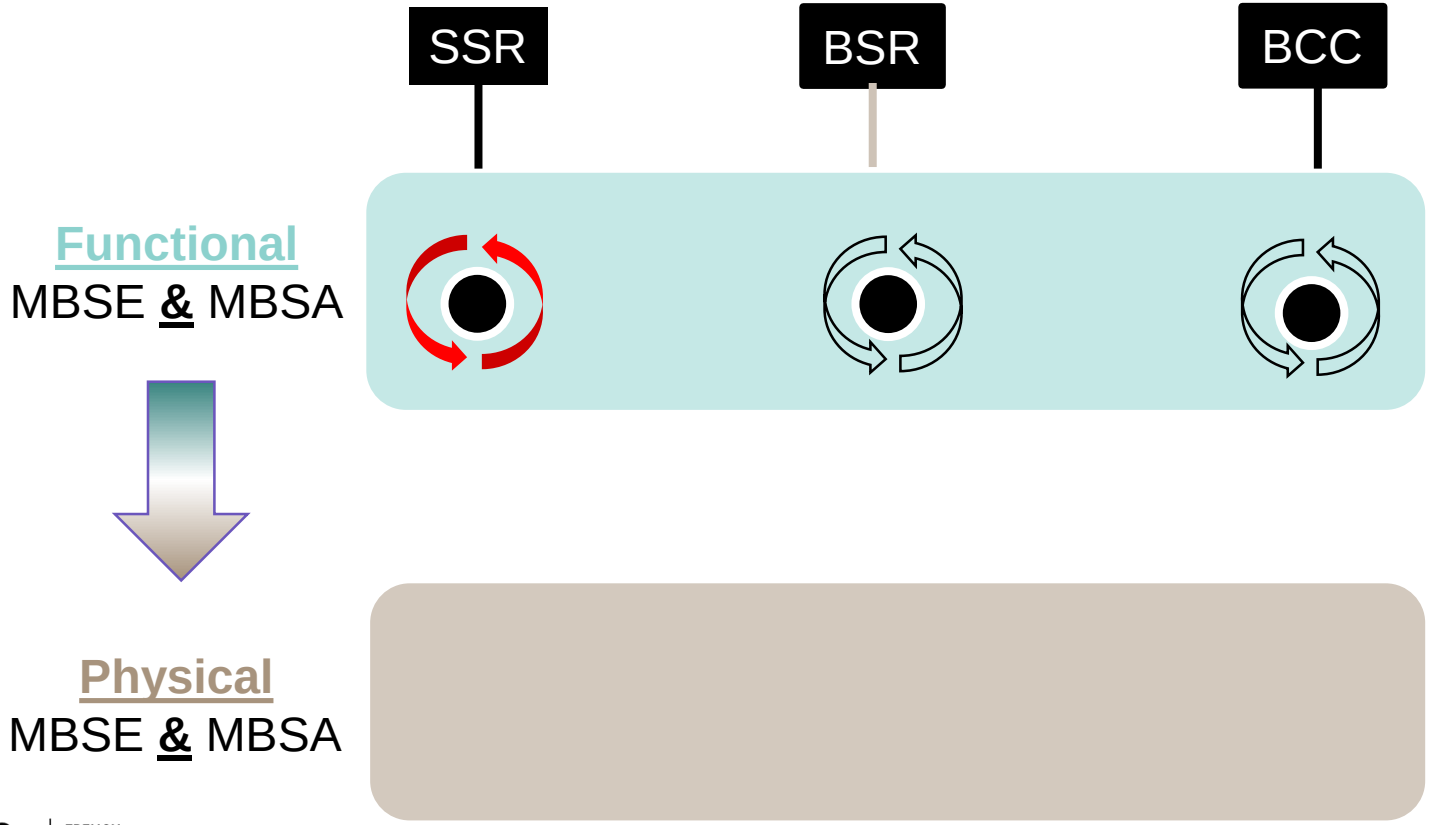
State of the art from WP2 of MOISE

Former IRT project had materials to avoid redoing part of the work

Humble first, ambitious after … if time allows it :

Models Iterations treated

Models Iterations not treated



Methods' set up on a narrower and more reduced concepts basis

Blocking there

Will anounce A failure here

Methods' set up on a wider and more complex concepts basis

(frozen) dimensions : Why Altarica ?

Members

Two members are AR tool vendors and one member has done its own dialect (Open Altarica 3.0)

Experts on projects

AR Experts (on detachement and consulting) available for project

New mean of compliance in ARP

ARP4761A adds an Annex to describe the use of AR. Industrial members are interested to see if it is applicable to their respective systems and what is missing in the Annex.

Limited ressource forced to focus

We can not assess all way of doing thing so take one we can master seems reasonnable

AR GUI concepts are close to SE ones

Evident proximity between model representation that reduces the gap between specialties but not solve it.

(frozen) dimensions : Why CAPELLA or SYSML ?

Members

Our members use or evaluate both of them

Impacts on methods

For SSR : SC2 project reuse MOISE materials on structure and interfaces which reduce the differencies between models withoutbeing identical.

For BSR : As method requires an exact linking between ins and outs, the behavior defined (textually in CAPELLA or semi-formally in CAMEO) does not jeopardize the method.

For BCC : CAPELLA has no executable behavioral semantic contrarily to CAMEO (based upon SYSML) so method was experienced on both models.

(Exploratory) Dimension : Scoped Vs End-to-End ?

Summary

	SSR	BSR	BCC
Method Authoring	Scoped	Scoped	End-to-End
Method Check	End-to-End	Scoped	End-To-End

(Exploratory) Dimension : Static Vs Dynamic ?

Static means definition only that can be…

… the ones of the structure and interface

… the ones of the behavior (e.g. to this inputs vector i have that output vector)

Dynamic means execution (that need to be defined previously) and can be…

… the order of blocks (ahead of runtime), independently from their content (like a sequence diagram)

… the order of blocks (at runtime), dependantly of the execution of active block content (like any simulation).

(frozen) dimensions : Why no incursion on authoring?

Legacy Models

Members of projects have already models (done without any consistency method considerations) such models will not be changed to integrate rules issued from the method.

S2C/LOT4 : modelling guide in parallel

Each working group (on consistency and on modelling) follows its own agenda and target not conciliable from the other one

A sequencial order would have been preferable (not the case in fact)

So consistency retex on modelling where available when guide activities were dispatch earlier.

No SE modelling guide

The project was not mandated to elaborate rules on SE authoring.
But ideally, consistency is not only a problem of one specilaty but a trade off between bith of them.

So SE specialty would have to author its models with some rules to ease the consistency with others specilaties.

Dimension : Case study

A single one which match needs

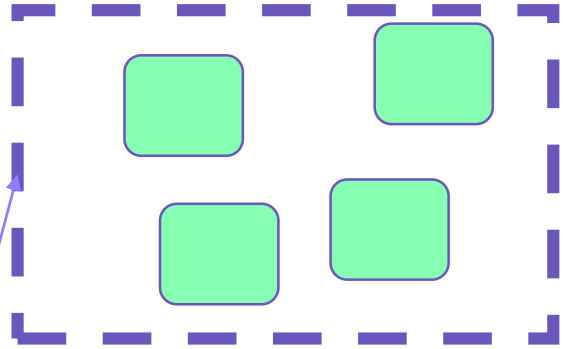
- **Aeronautical subject (drone for inspection)**
- **SE model already available**
  - **from reuse of MOISE/WP1 and extension done between MOISE and S2C**
- **SA model partially available**
  - **from MOISE/WP2 but baseline on MOISE/WP1 definition**
  - **Update less significant thant from scratch**
- **Farther usage for IRT**
  - **Comparison with other SE langage (SYSML)**
  - **Extended enterprise purpose.**

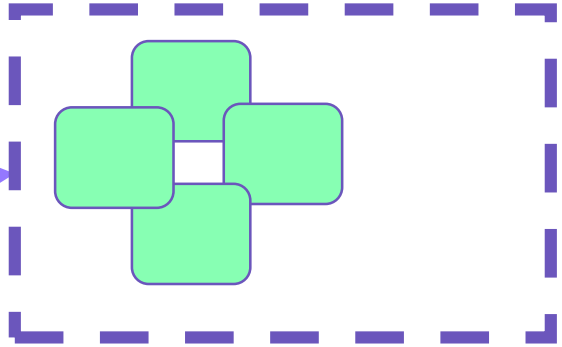
Dimension : Couples of models

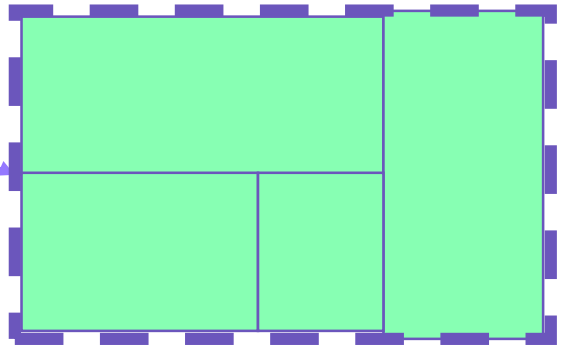
Expected and new track

SE Authonring tool	SE Authonring tool	Note
CAPELLA	SIMFIANEO	As expected by dimensions frozen dimensions
CAMEO	SIMFIANEO	
SIMFIANEO	SIMFIANEO	New track using SIMFIANEO as SE tool for authoring due to QoS available (i.e. truth table of SE logics) But limitation because not all SE QoS available (e.g. allocation from one layer to another)

Dimension :
Amount of sub perimeters and sub perimeters vs Model





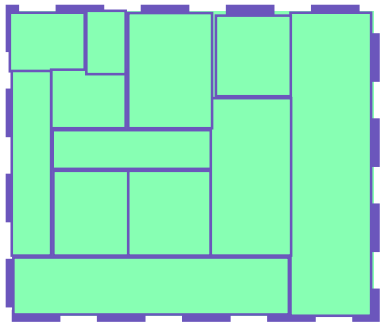


Sub perimeters

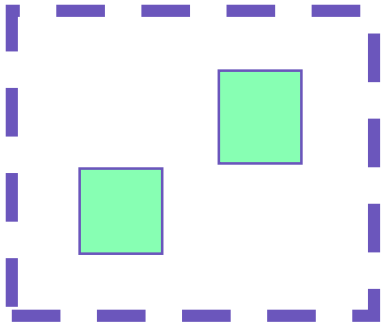
If model is considered as a perimeter, PoC focused on sub part of it

- **One or several sub parts are possible**
- **Overlapping of sub parts are possible**
- **Union of all sub parts may cover the whole perimeter**

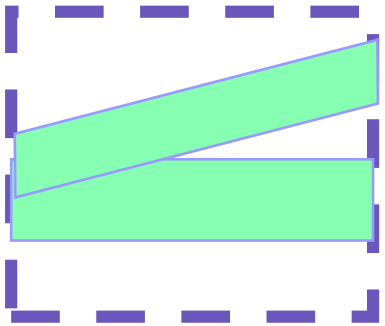
For SSR



For BSR



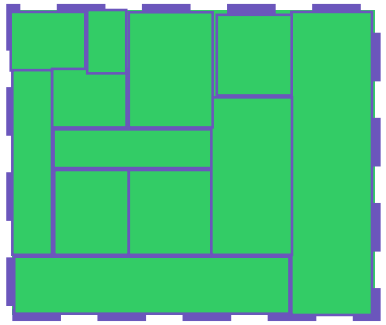
For BCC



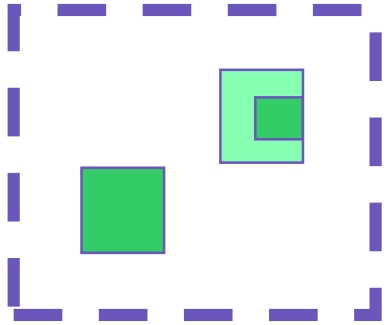
Dimension : Coverage of the sub perimeter

In a perimeter many different cases can occurs do we cover them all ?

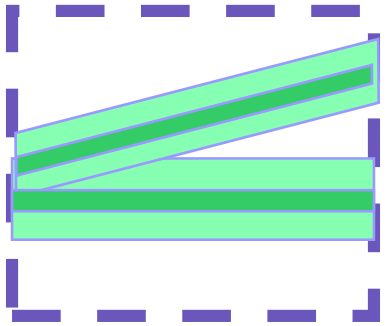
For SSR



For BSR



For BCC



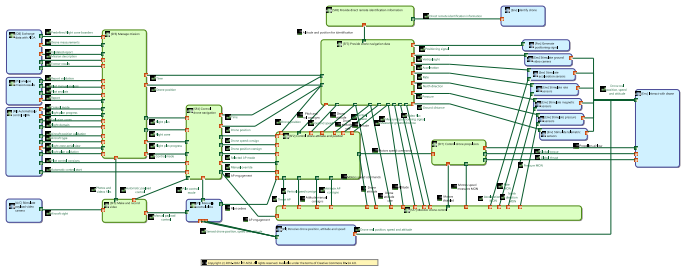
IRT SAINT EXUPÉRY

SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE

Appendixes
-
Details on Proposed Solutions

SSR

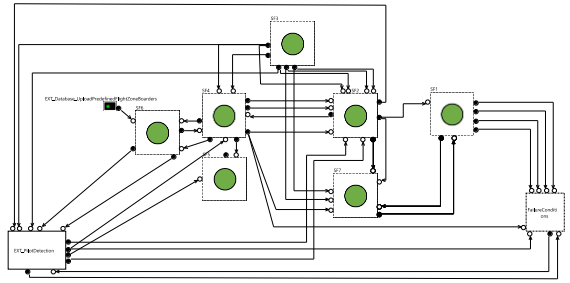
Remind the problem :



Are both models consistent at structure and interface levels with a scoped perspective?

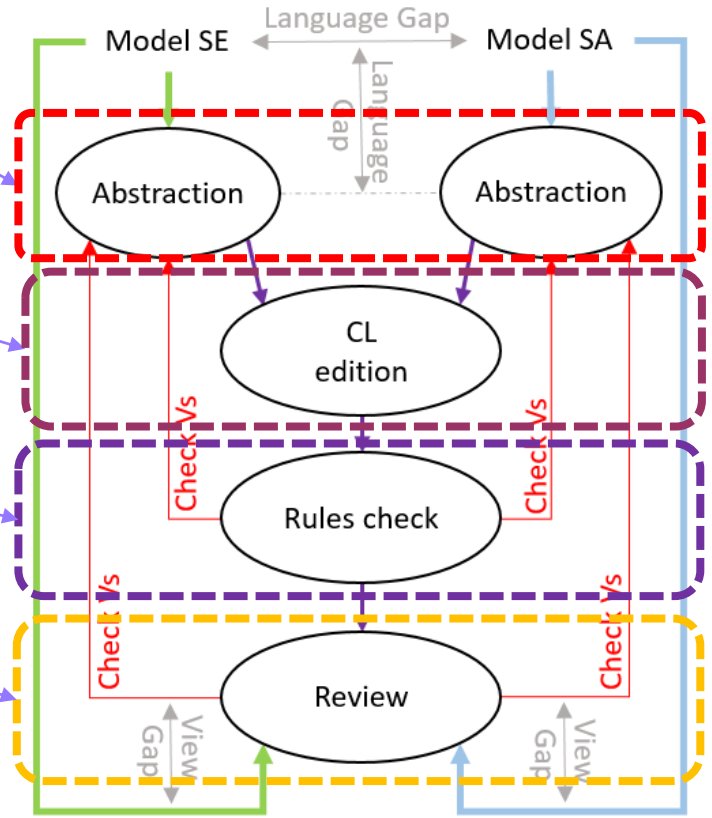
⇦SE one (CAPELLA)

SA one ⇨ (AR)



Method

- Abstract both functional models to get their artefacts
- Define structural link (**CLFx**) over functions regarding method rules and capture: justifications, hypothesis etc.
- Define links interfaces (**CLfly**) flow regarding method rules and capture: justifications, hypothesis etc
- Check inconsistency between previous definitions
- Feed SExSA review about captures

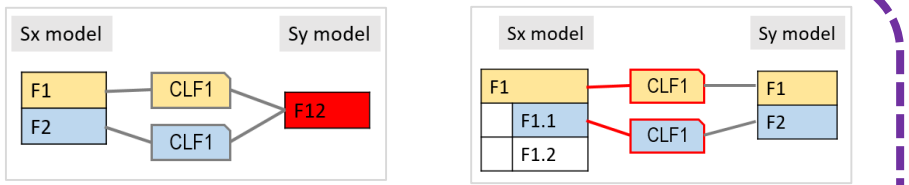


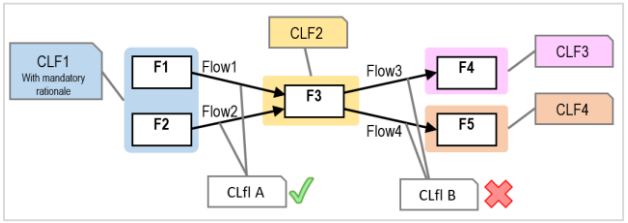
PoC

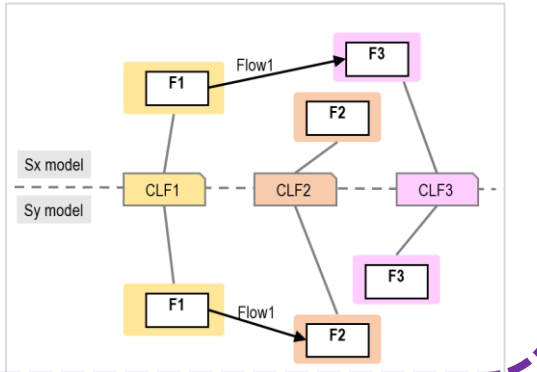
- Tooled process
- Coverage of the model

SSR : high level processus vs Examples

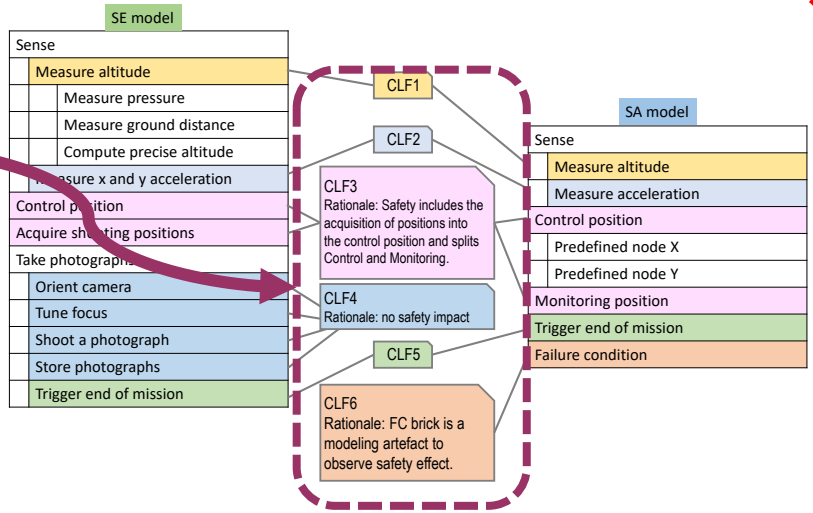
- Abstract both functional models to get their artefacts (structure and interfaces)
- Define structural link (**CLFx**) over functions (hierarchical or leaf) regarding method rules and capture: justifications, hypothesis etc.
- Define interfaces links (**CLfly**) regarding method rules and capture: justifications, hypothesis etc
- Check gaps between previous definitions
- Feed SExSA review about captures

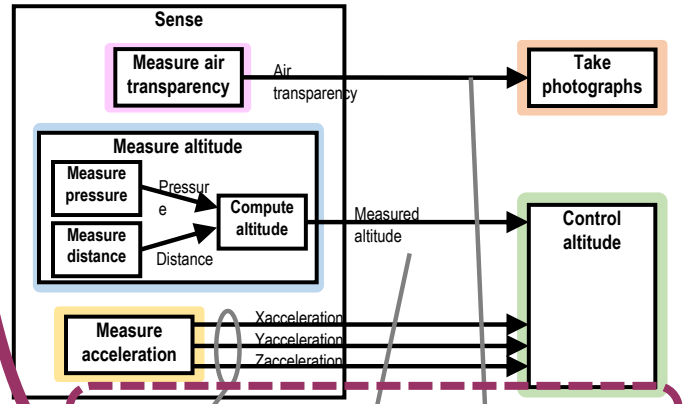


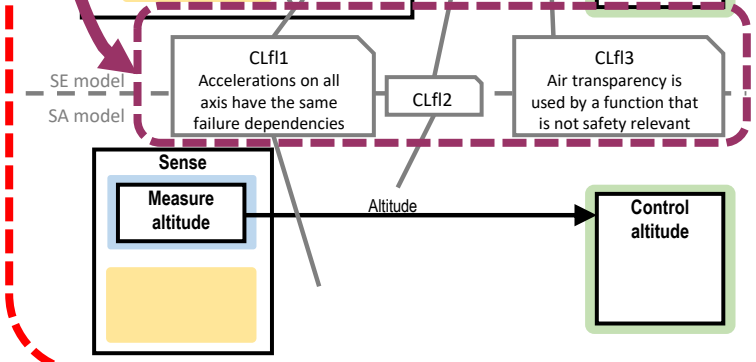




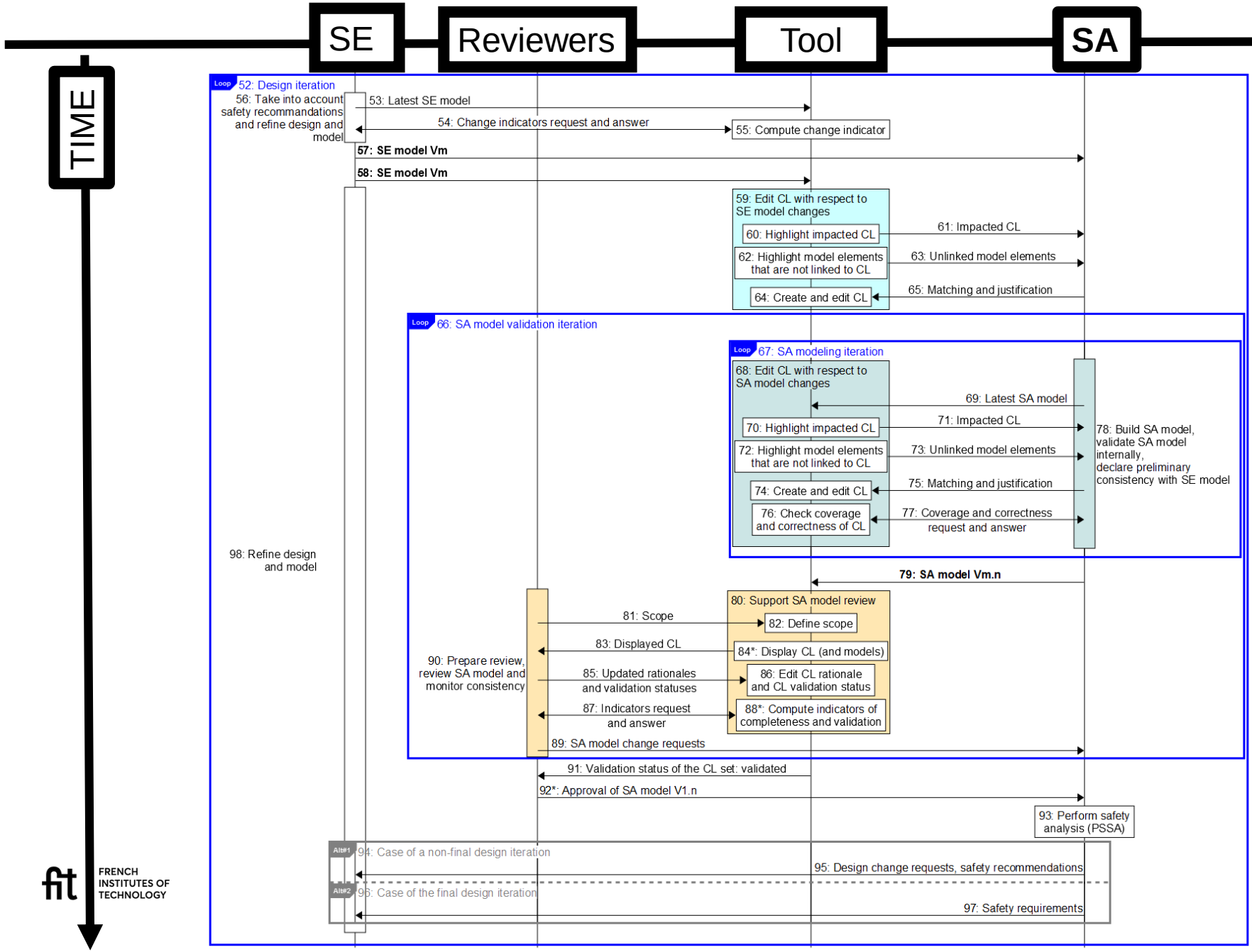
FRENCH INSTITUTES OF TECHNOLOGY





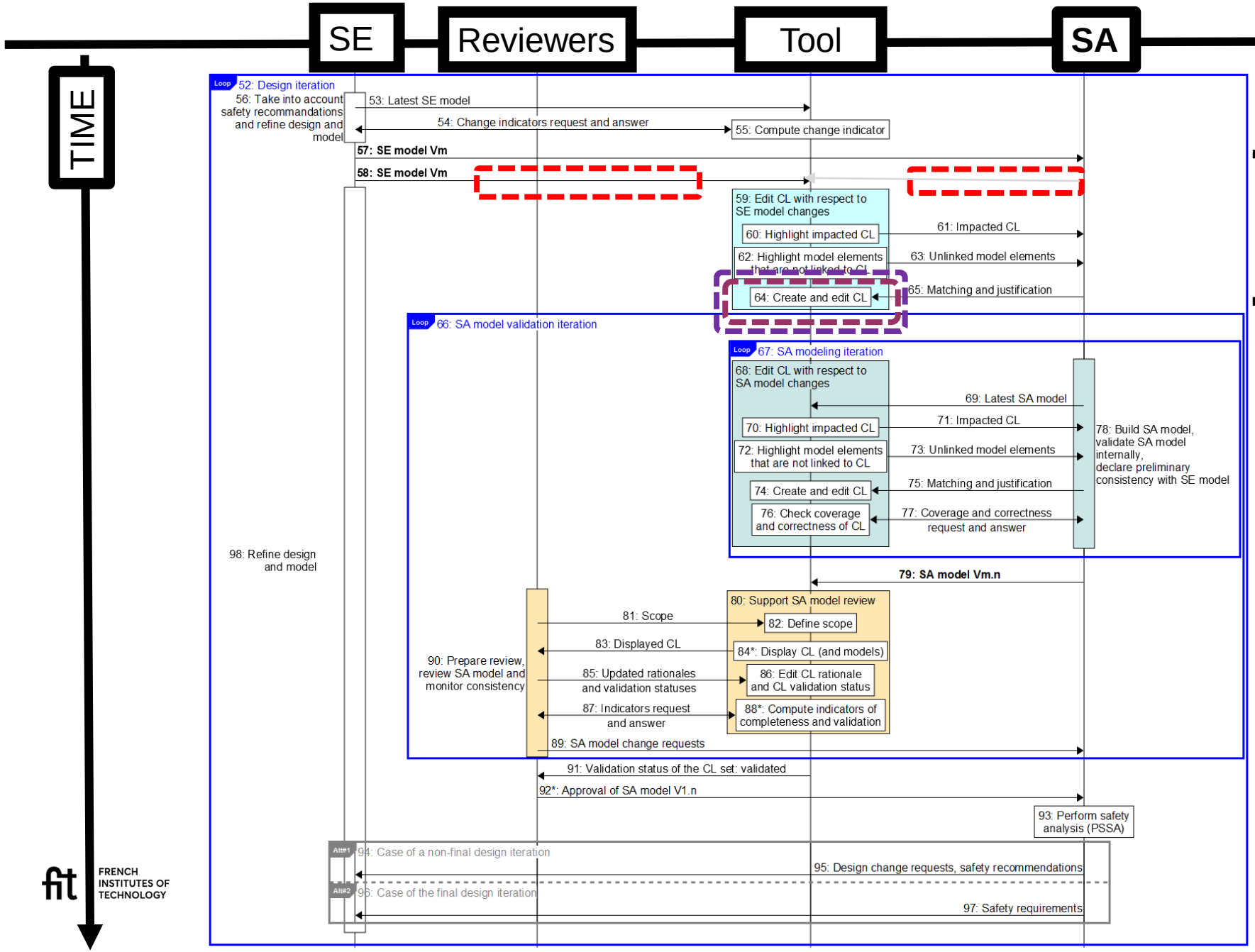


SSR : Low level processus



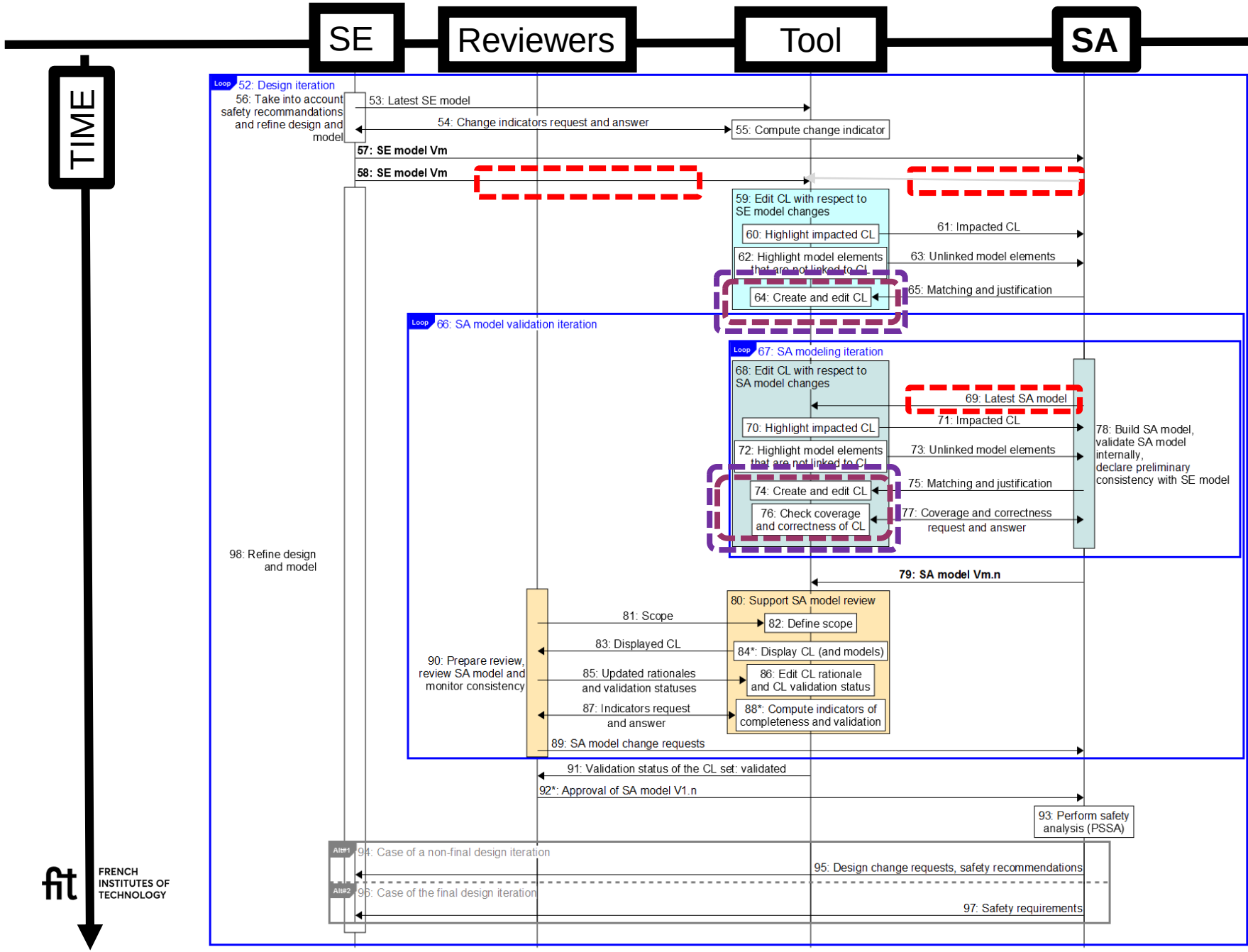
FRENCH INSTITUTES OF TECHNOLOGY

SSR : Low level processus



SE baseline changed, so …
What's new ?
(SA realign concialiable CLs)

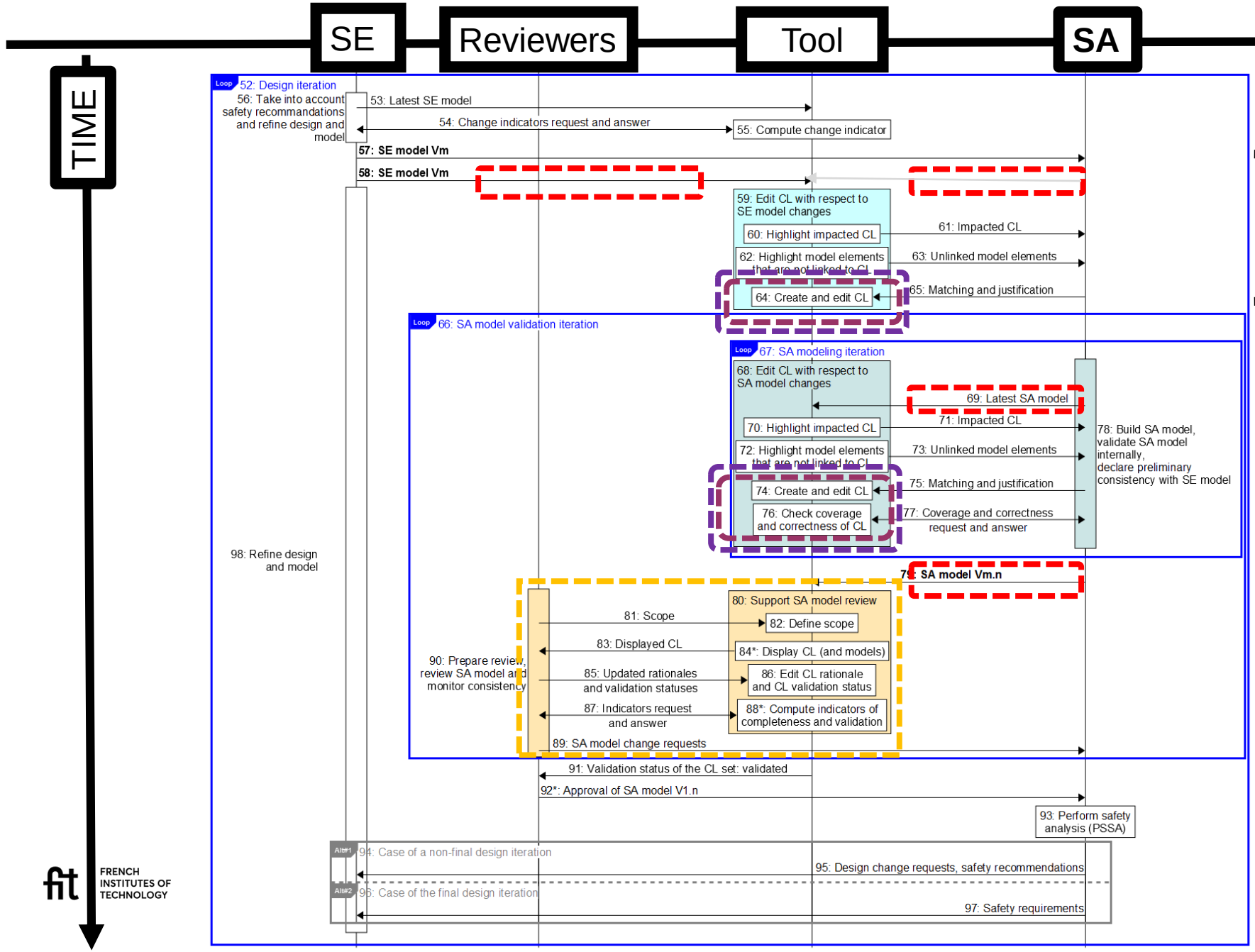
SSR : Low level processus



SE baseline changed, so …
What's new ?
(SA realign concialiable CLs)

Unconciliable CLs means
a SA model realignment,
so, its recommandations too
(SA creates/corrects CL too)

SSR : Low level processus



SE baseline changed, so …
What's new ?
(SA realign concialiable CLs)

Unconciliable CLs means a SA model realignment, so, its recommandations too (SA creates/corrects CL too)

SExSA review abstractions to agreed that recommandations are right (CI rationnale ans status updated)

FRENCH INSTITUTES OF TECHNOLOGY

BSR

Remind the problem : Are both models consistent at structure, interface and behavior level with a scoped perspective ?

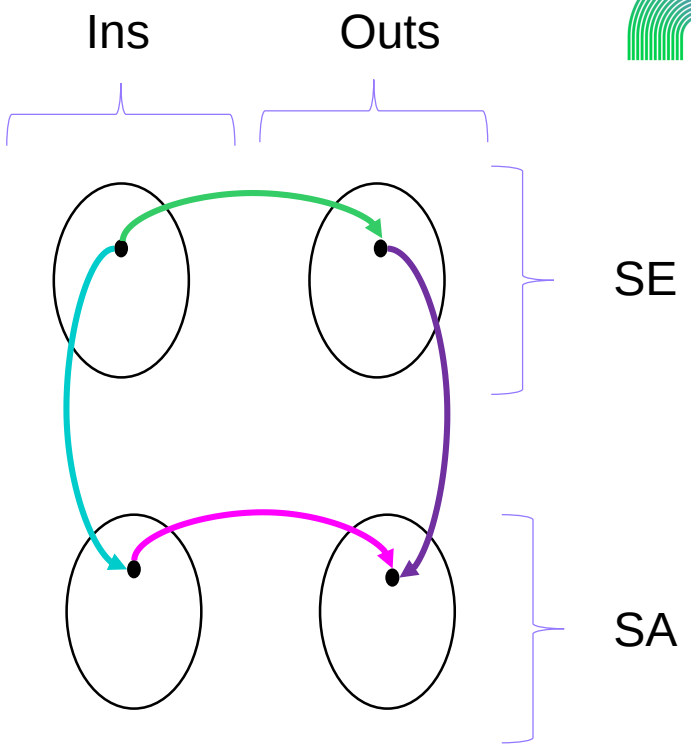
Method

- On reputed same perimeter (Scope)
  - A SE static specification is transformed into a table that links ins and associated outs →
  - A SA behavior is transformed into a table that links ins and associated outs →
- A transformation shall be defined to process
  - SE(ins) into SA(Ins) →
  - SE(Outs) into SA(Outs) →
- Check for every SE(Ins) :

The path → then → leads to the same SA(Outs) from path → then →

PoC

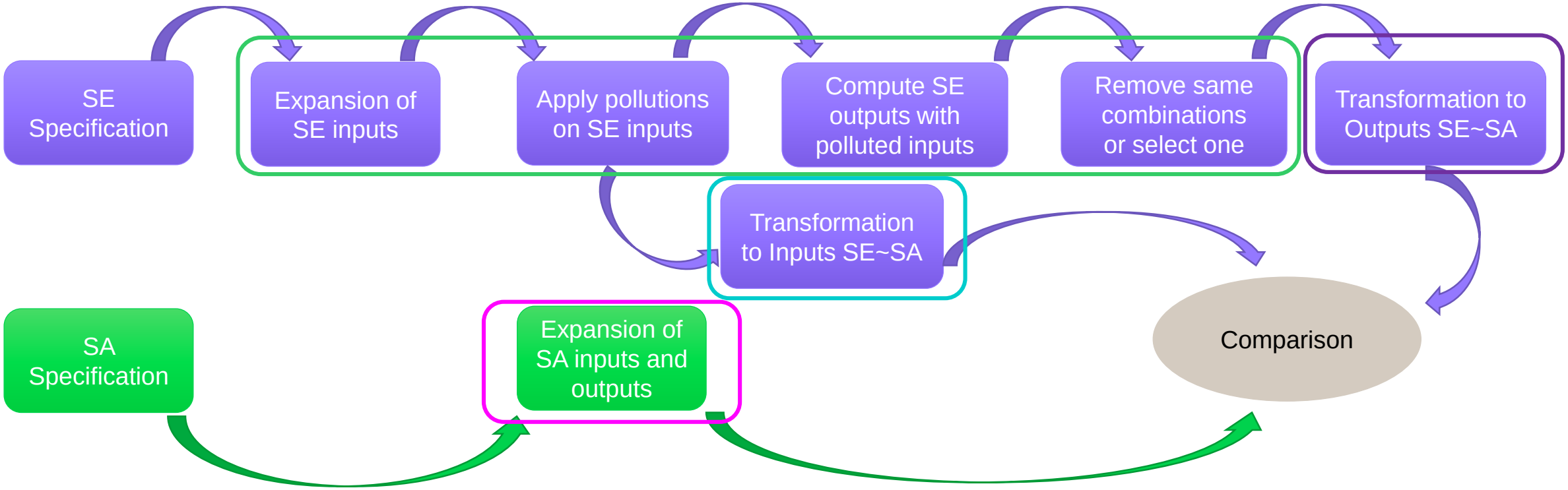
- Done on two scopes only and on logic exclusively (so very poor coverage and exploration too)
- Require tooling process because the amount of data can be huge.



Nota

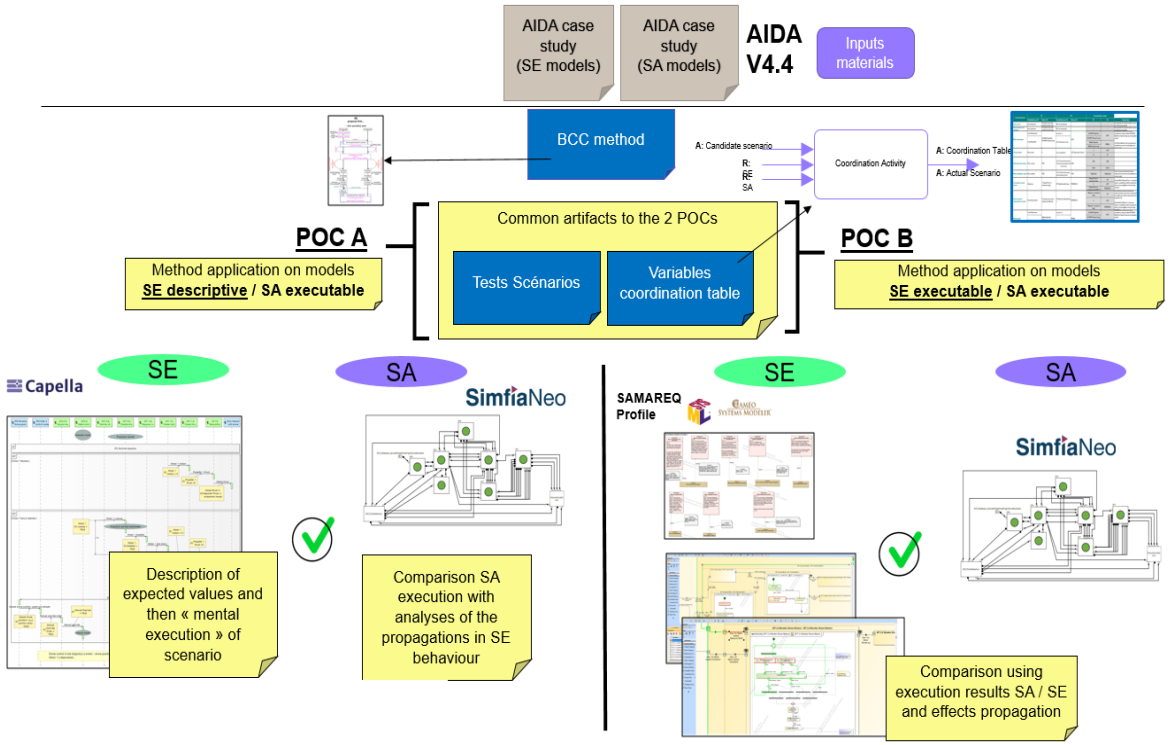
- Transformations → → are what SA specilialist's do in its mind when he creates its model from SE informations (like tranformation of SE values into a nominal value or considerering pollution of SE values as erroneous one, or considering SE invalidity status as lost one etc)
- Transformation → is the transfert function of SE
- Transformation → is the implementation of failure propagation in a component of SA.

Over all process



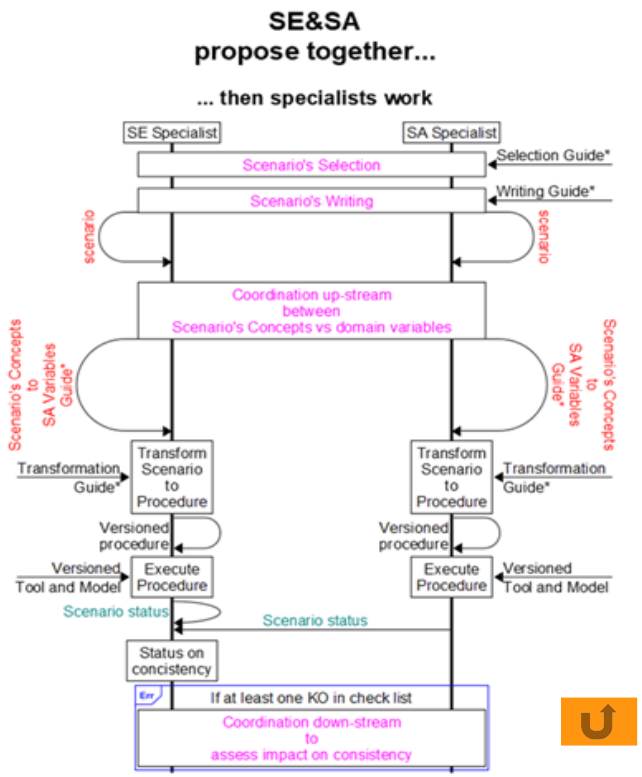
BCC

Remind the problem : Are both models consistent at structure, interface and behavior level with a end-to-end perspective ?



Method

- Force the sharing of common test scenarios between SE and SA
- Coordinate SE observations with SA observation along these scenarios
- Each specialty applies the scenarios regarding its models ans associated QoS
- Check that coordinated observations match or not expectations
- Feed SExSA exchanges all along the process and on derivations from it



PoC

- Done on two couples

CAPELLA (Sta), AR (Dyn)

SYSML (Dyn), AR (Dyn)

- Coverage is function of the reduced set of scenarios used