



S2C

System & Safety Continuity

- Method for consistency between MBSE and MBSA -

Table of Contents



Context of Project

Problem Positioning

Solutions Take Away

Proof of Concepts & Outcomes

Returns of experience

Appendixes

Project Definitions

Details on the Framing of Solutions

Details on Proposed Solutions

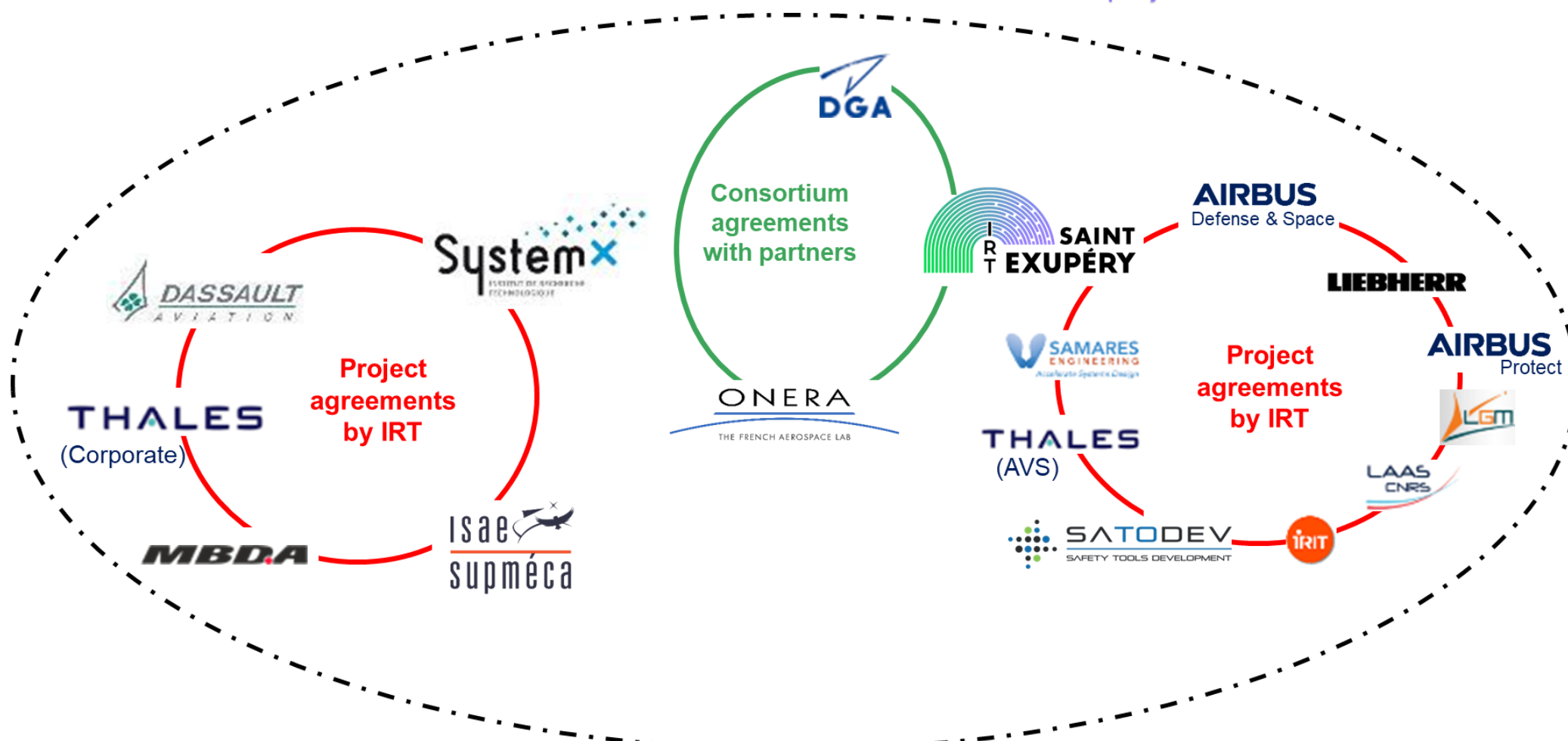


Context of Project


Project ecosystem

S2C

A same collaborative project



Key figures :

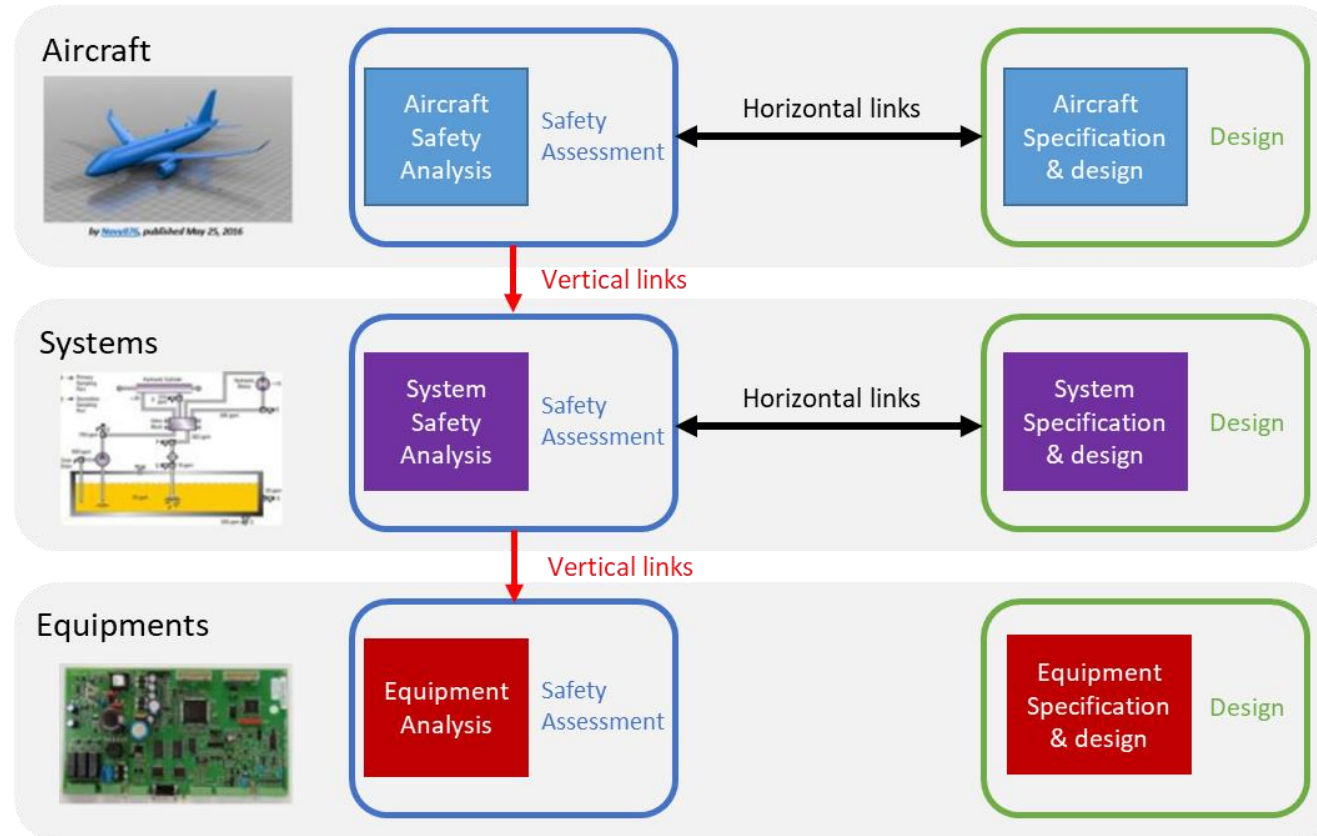
 17 partners	 6,5 people FTE	 2 thesis	 3,78 M€	 4 years [2019-2023]
--	---	---	--	--



**Method for consistency
between MBSE and MBSA**

Framing the Problem

Project breakdown

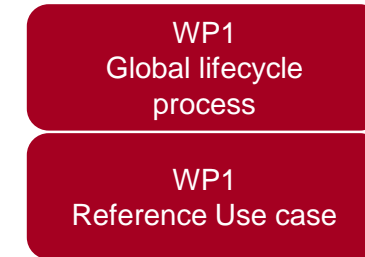
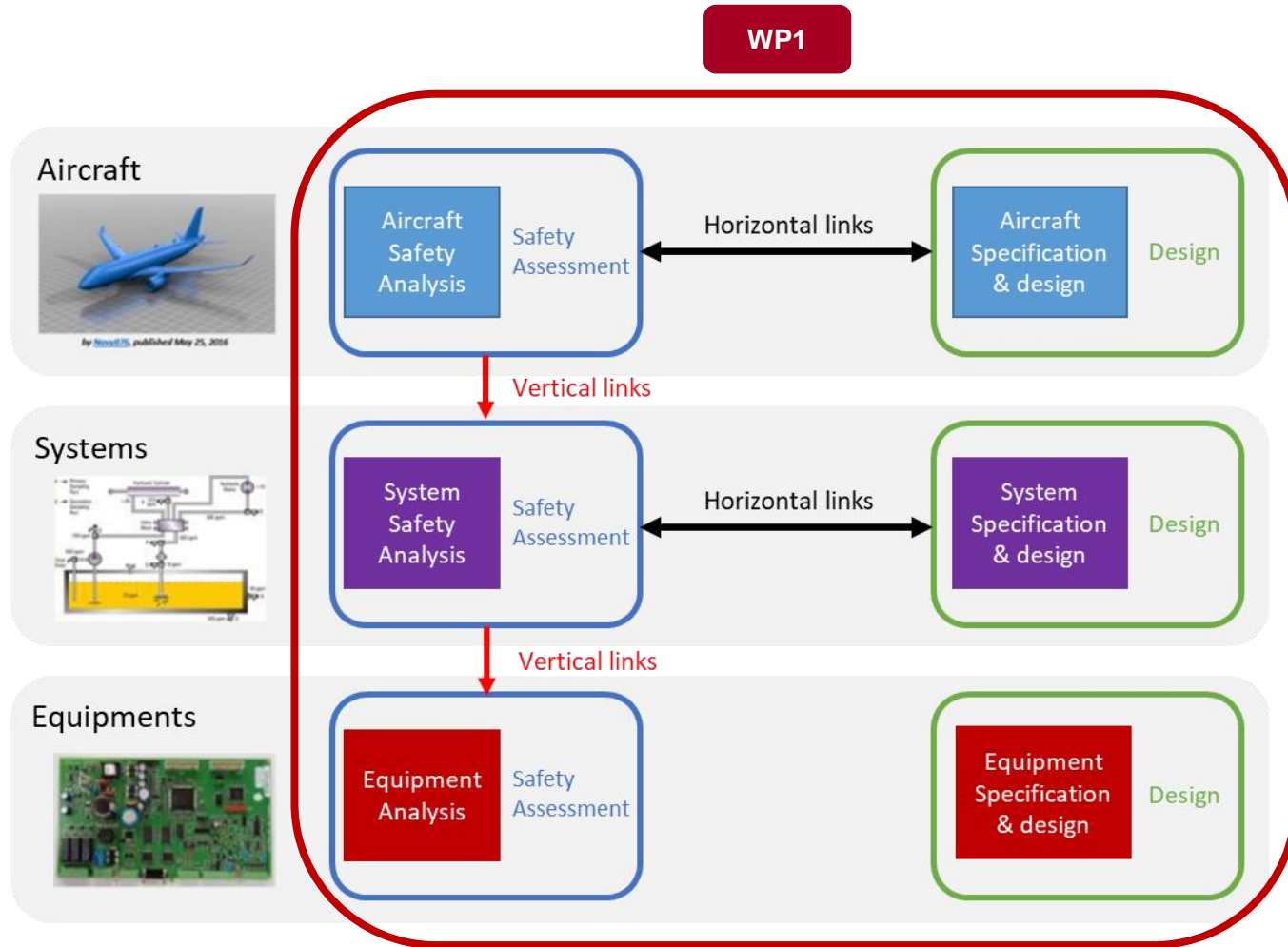


To define **processes, methods and tools** that allow to guarantee that **safety analyses** and system modelling done by system architect (**MBSE**) are **consistent**, in a context of numerical continuity, **during all iterative development cycles** of products and systems, and answering to **certification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

The project consists of **4 Workpackages** to address these objectives.

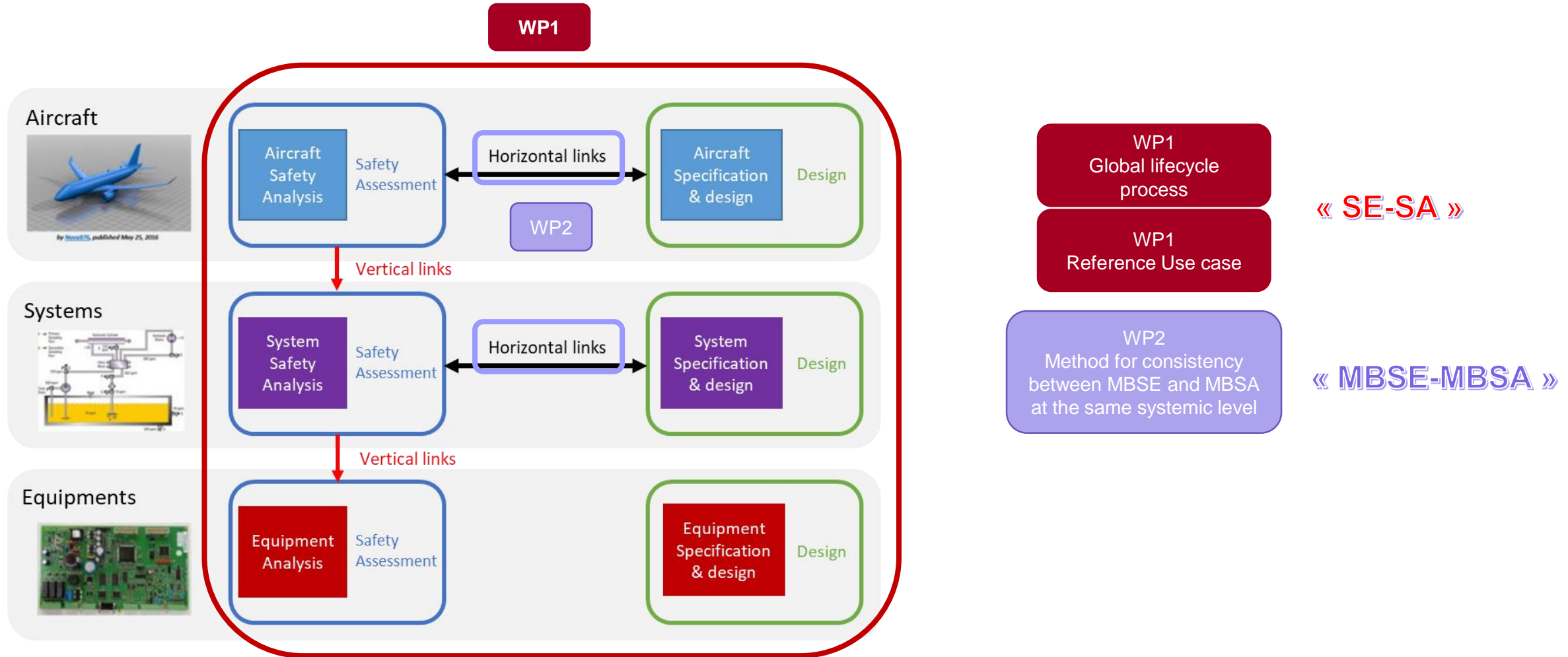
They **focus** either on **boxes** or **links**.

Project breakdown

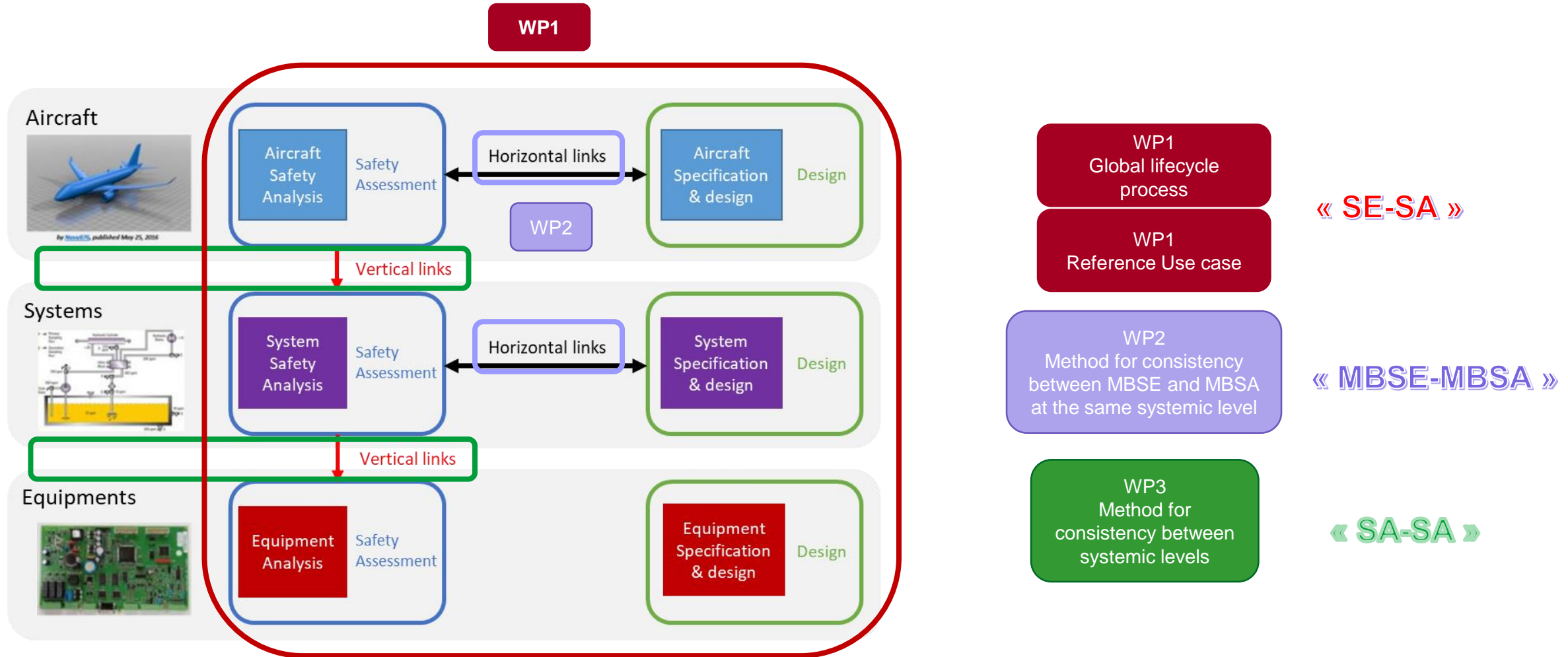


« SE-SA »

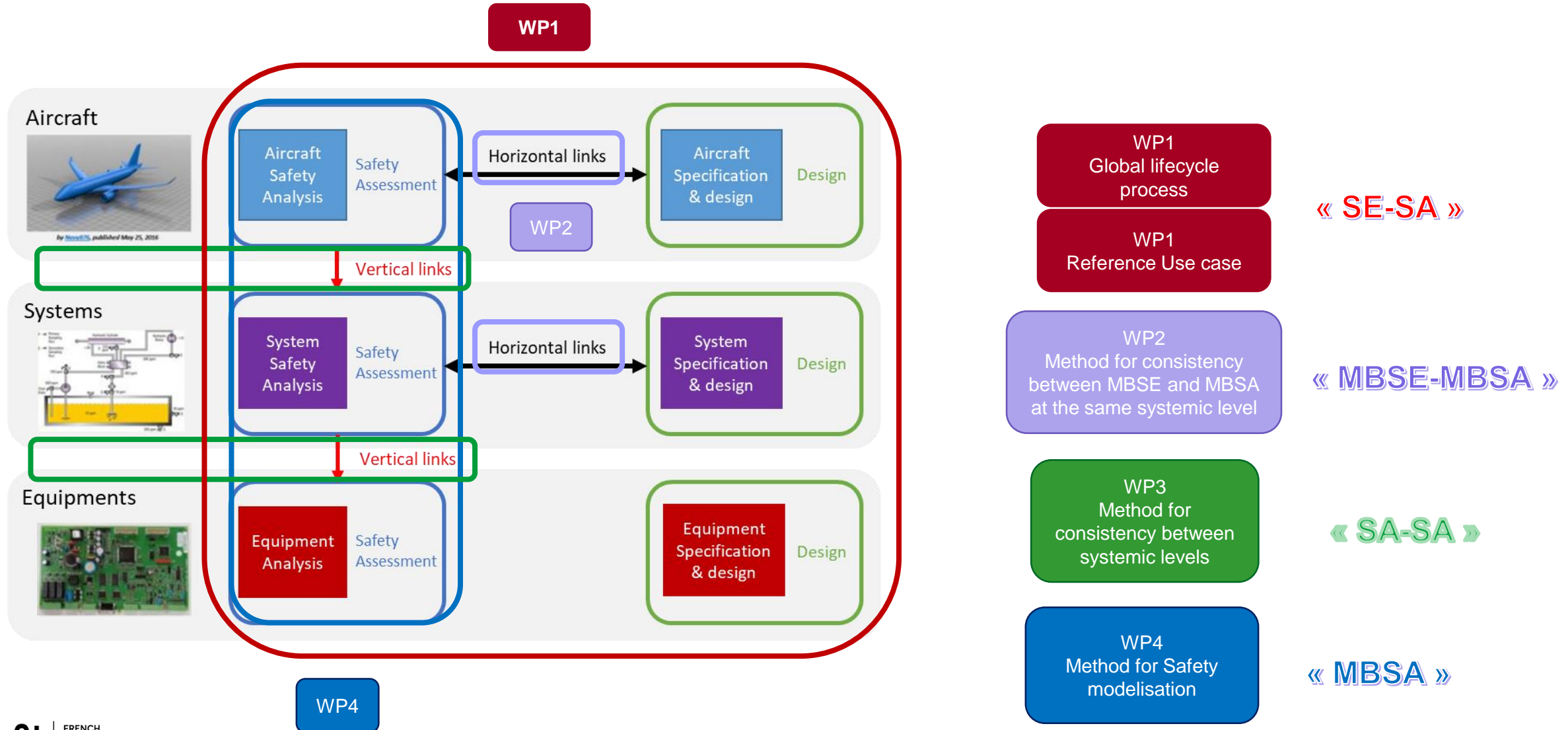
Project breakdown



Project breakdown



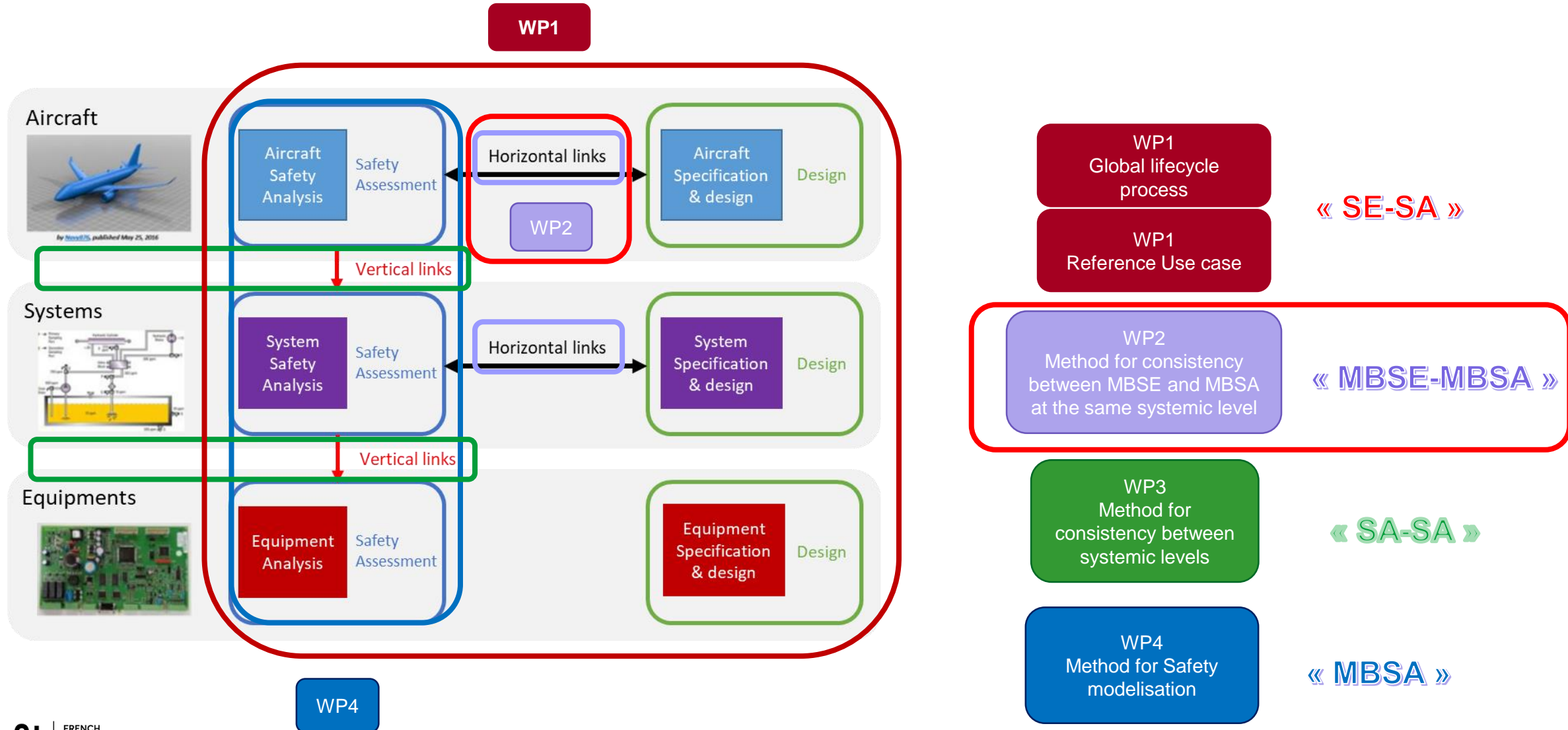
Project breakdown



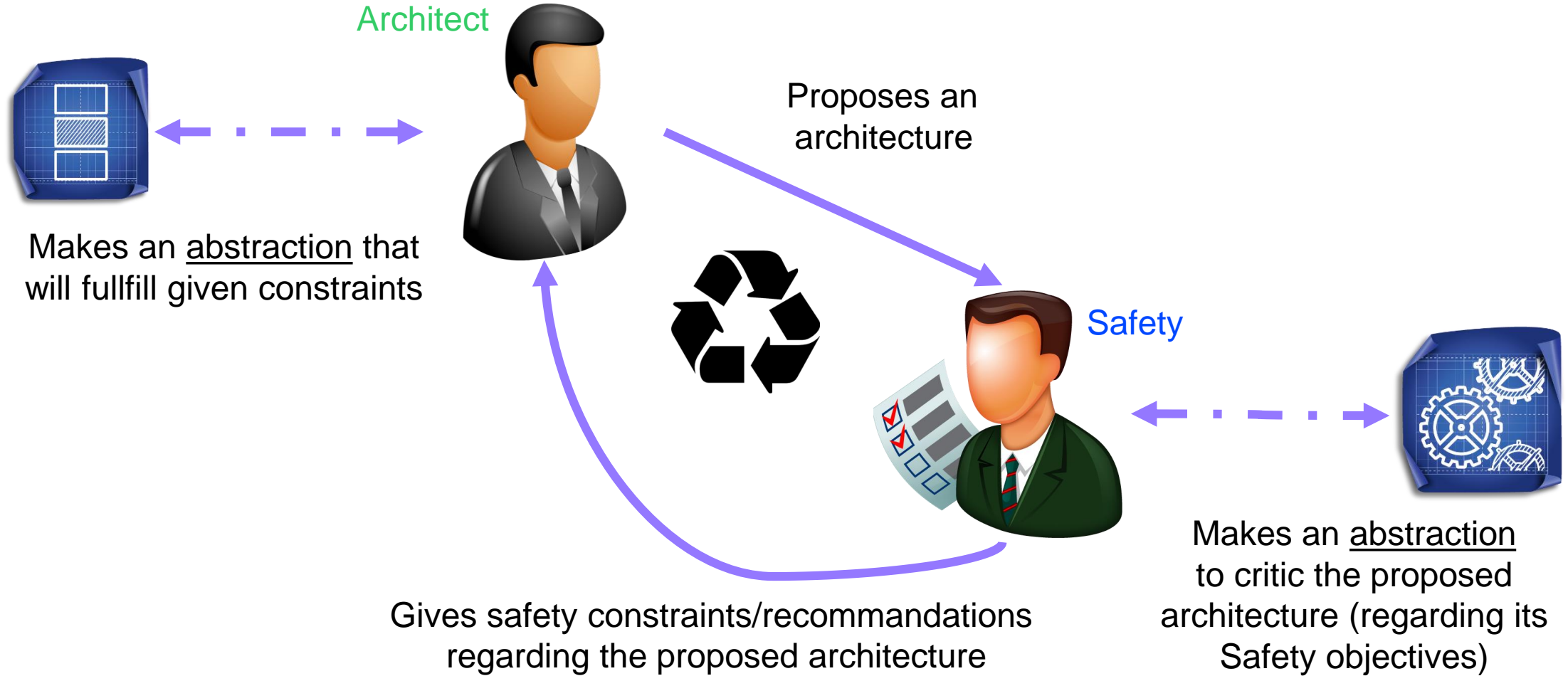
WP3

WP4

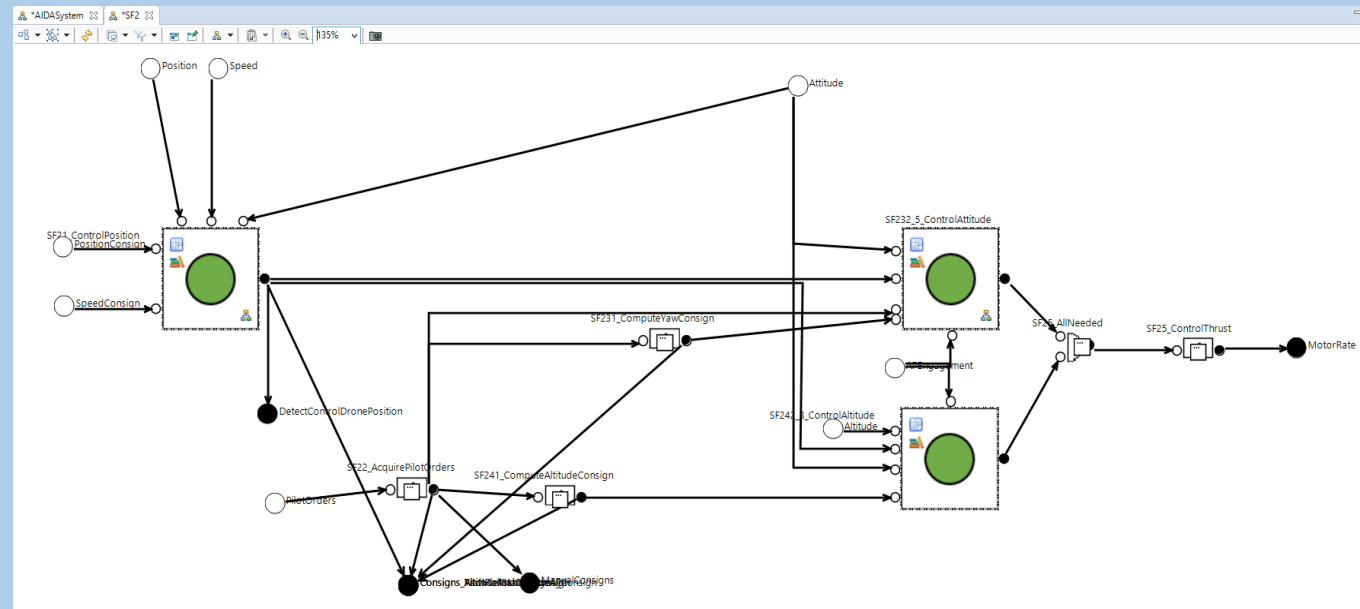
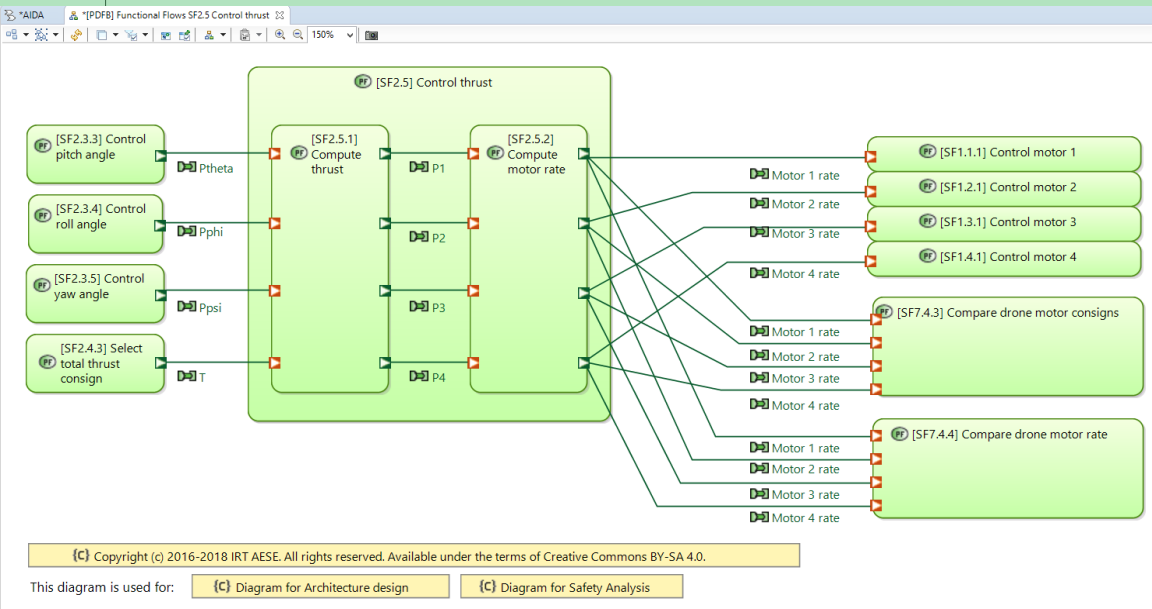
Project breakdown



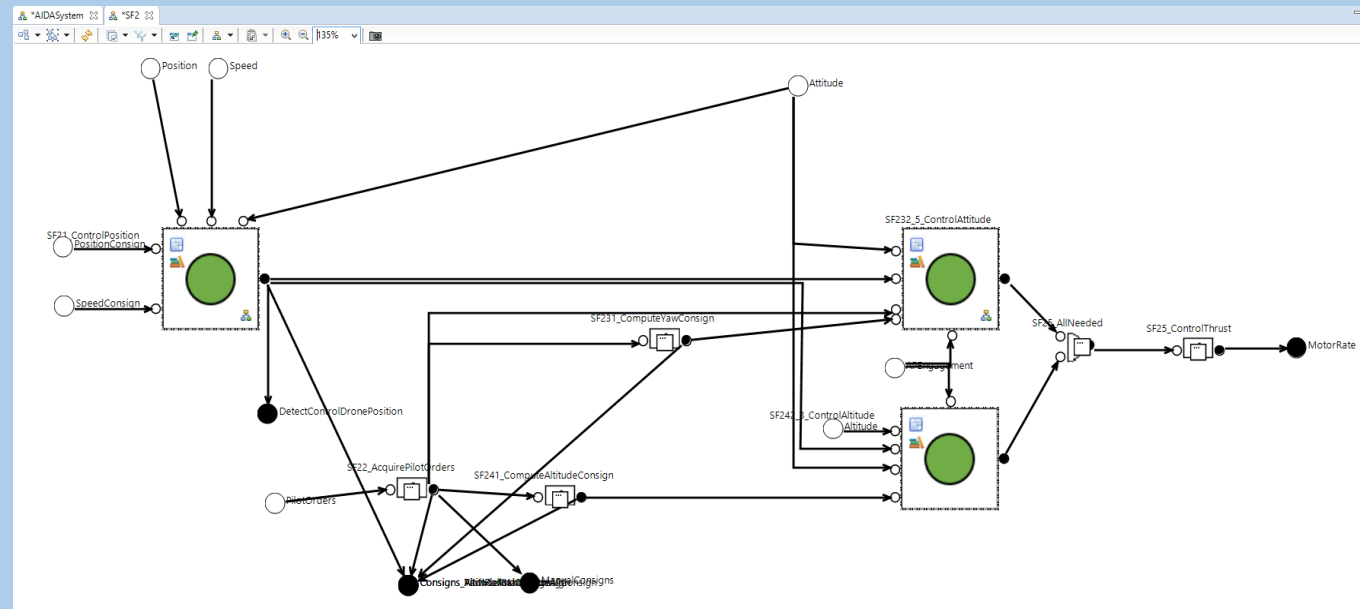
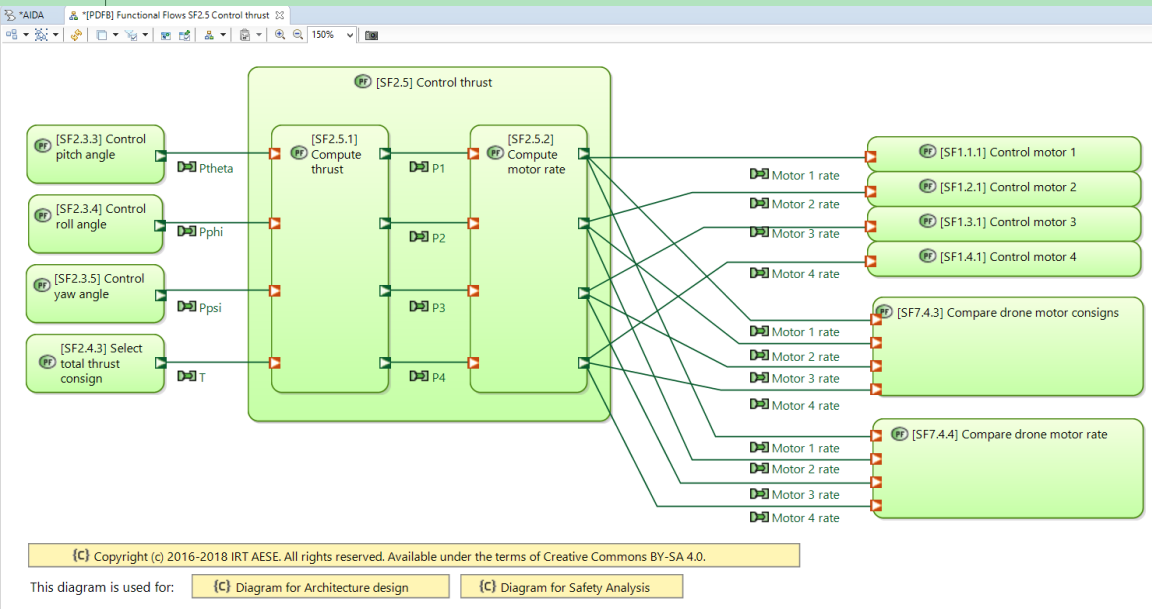
What occurs... at (very very) high level



What occurs ... at abstraction level

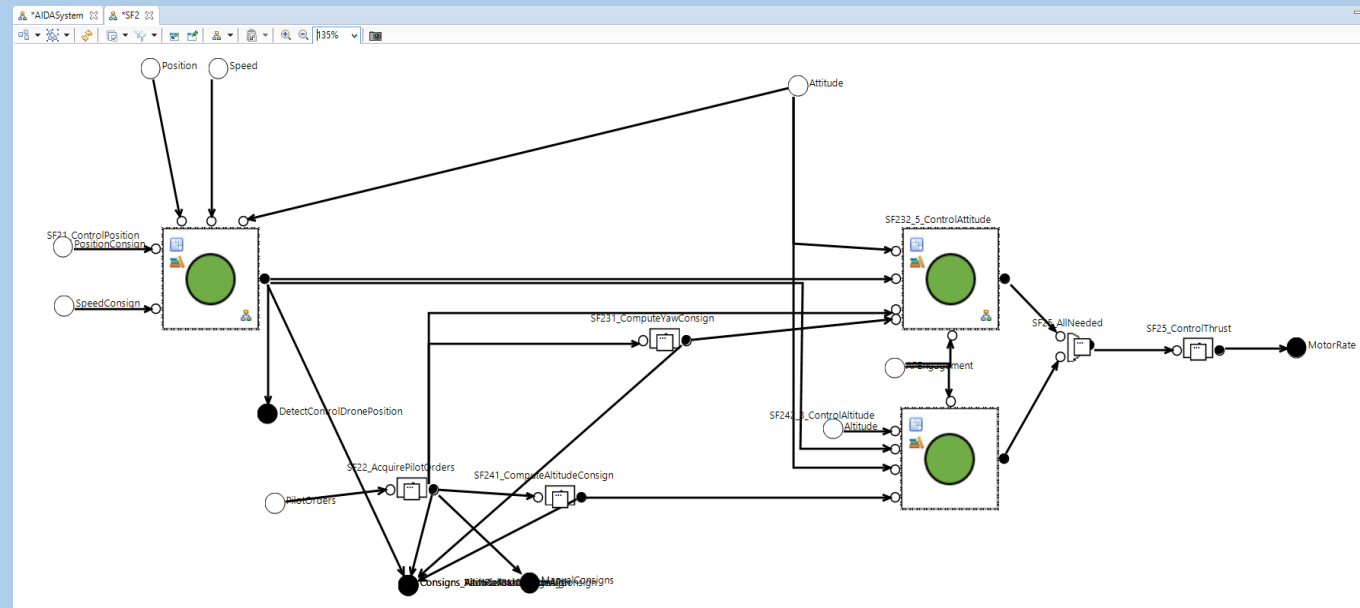
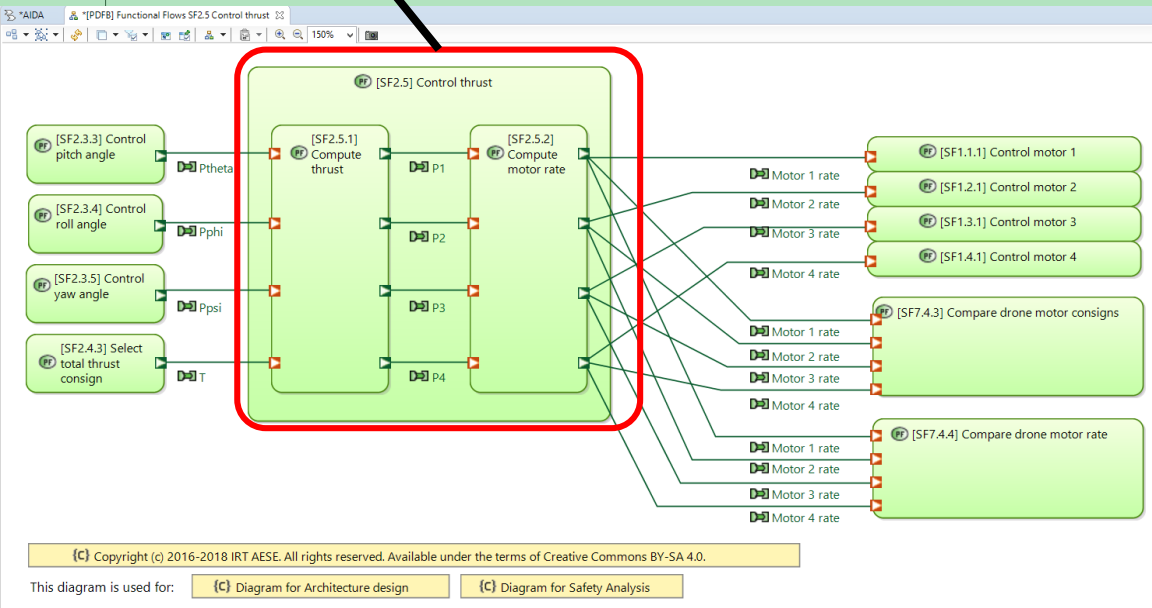


What occurs ... at abstraction level



SF2.5 and its context seen from SE

What occurs ... at abstraction level

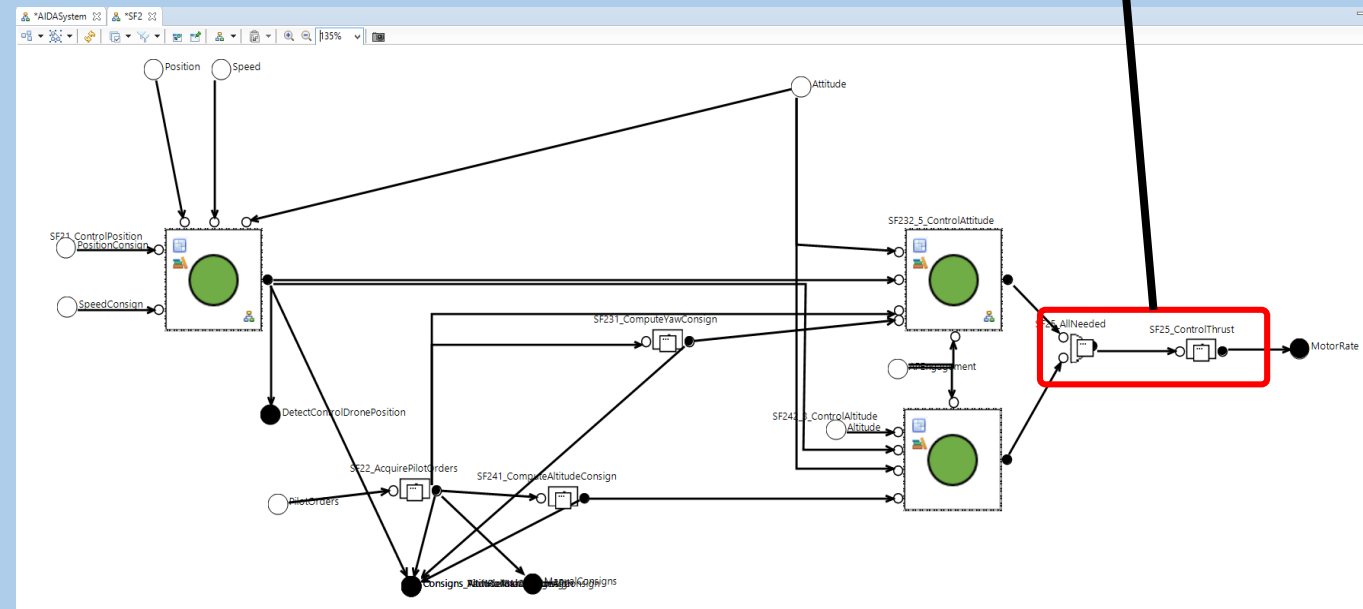
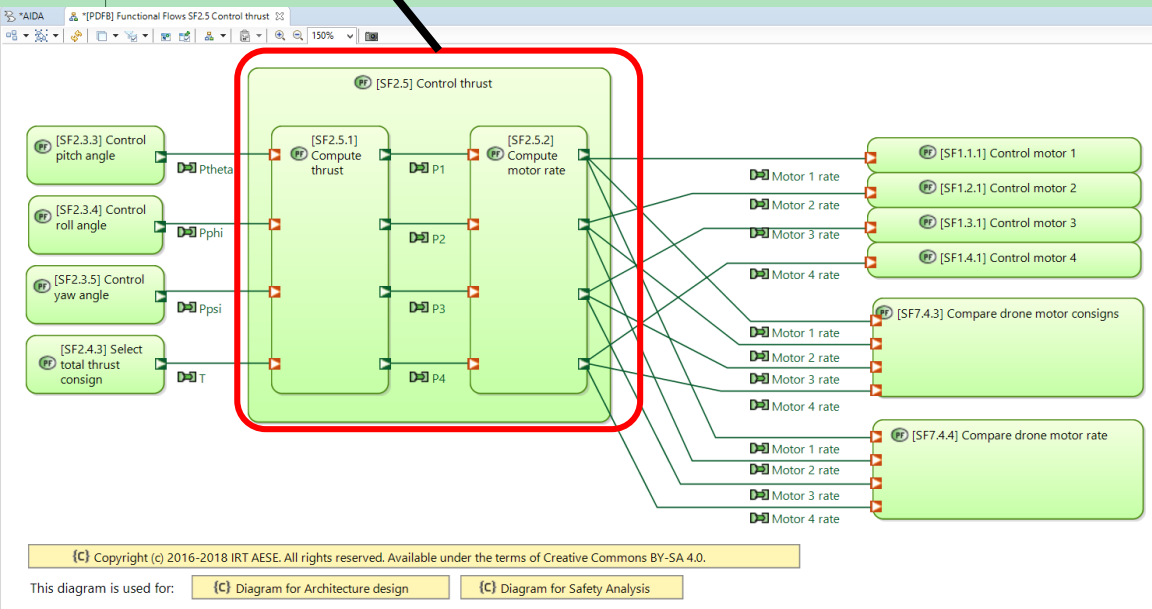


Representation differs

SF2.5 and its context seen from SE

What occurs ... at abstraction level

SF2.5 and its context seen from SA



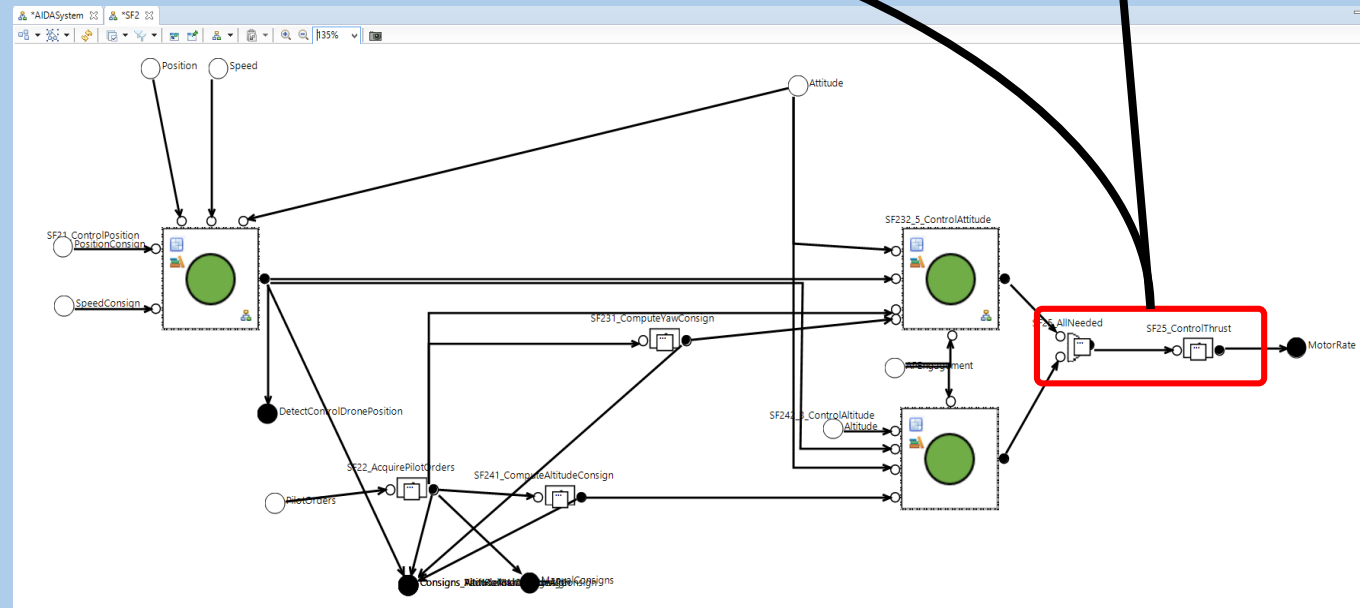
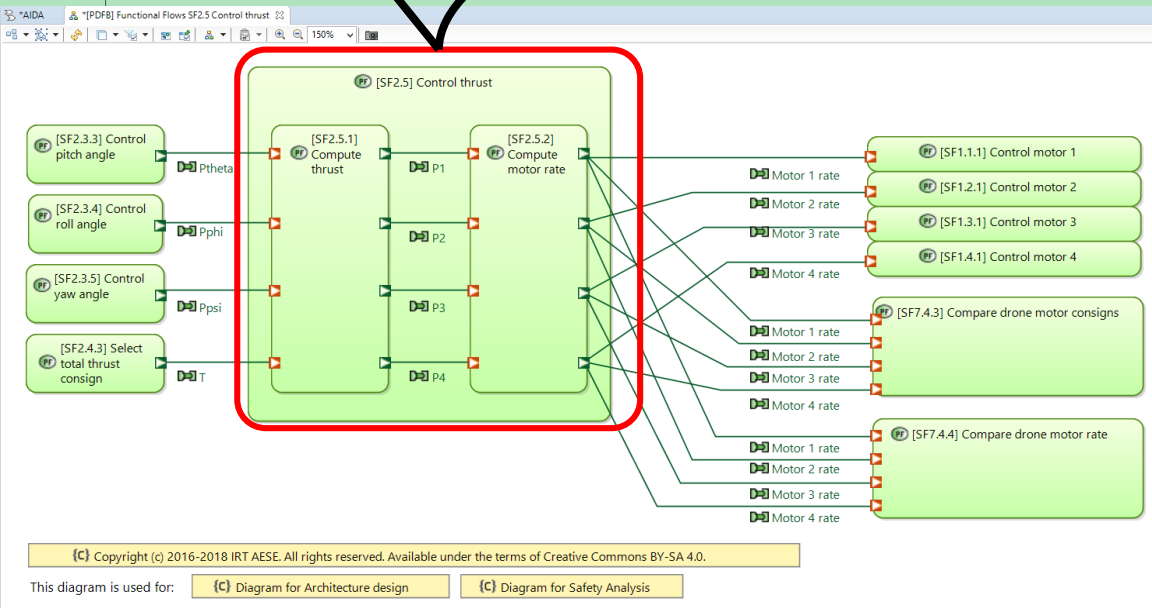
Representation differs

SF2.5 and its context seen from SE

What occurs ... at abstraction level

SF2.5 and its context seen from SA

Refinement and interface differ



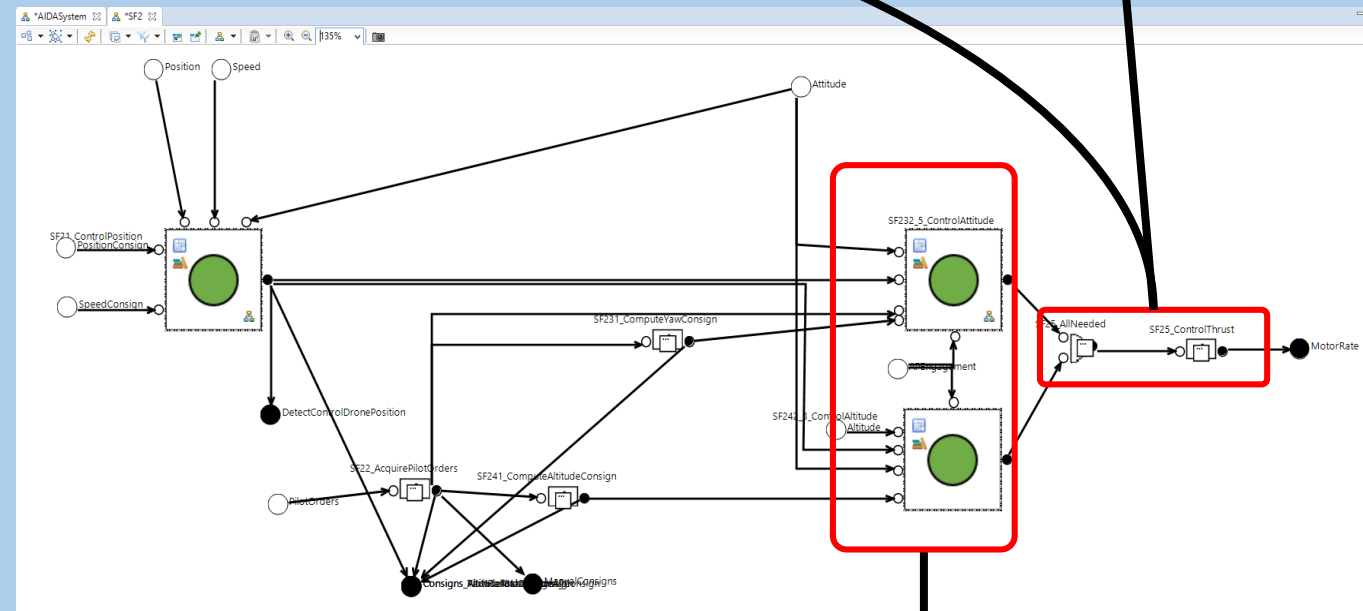
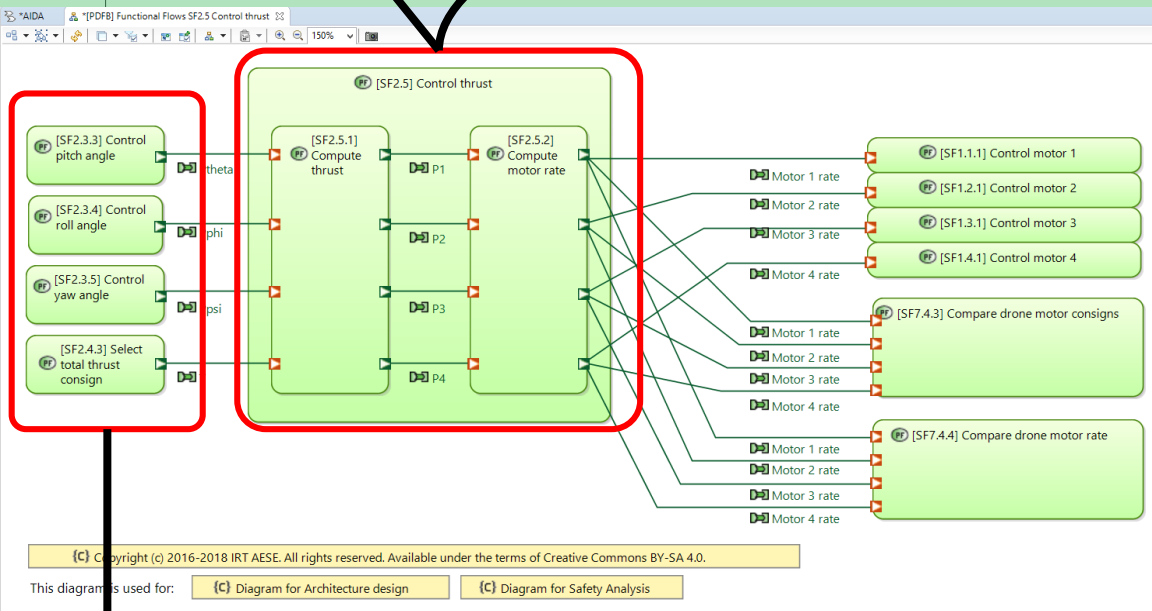
Representation differs

SF2.5 and its context seen from SE

What occurs ... at abstraction level

SF2.5 and its context seen from SA

Refinement and interface differ



Context differs

Representation differs

SF2.5 and its context seen from SE

What occurs ... at abstraction level

SF2.5 and its context seen from SA

Refinement and interface differ

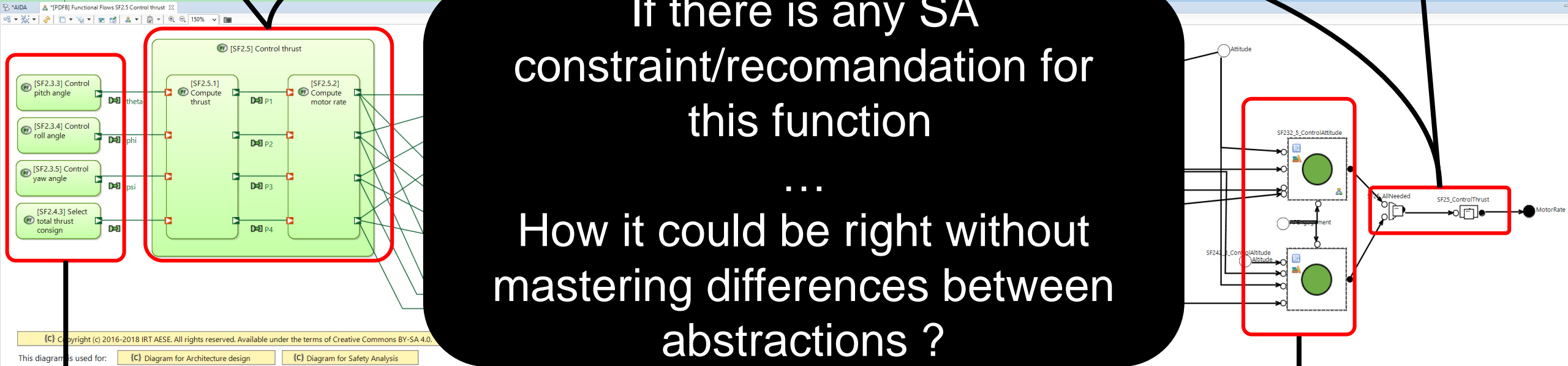
If there is any SA constraint/recomandation for this function

...

How it could be right without mastering differences between abstractions ?

Context differs

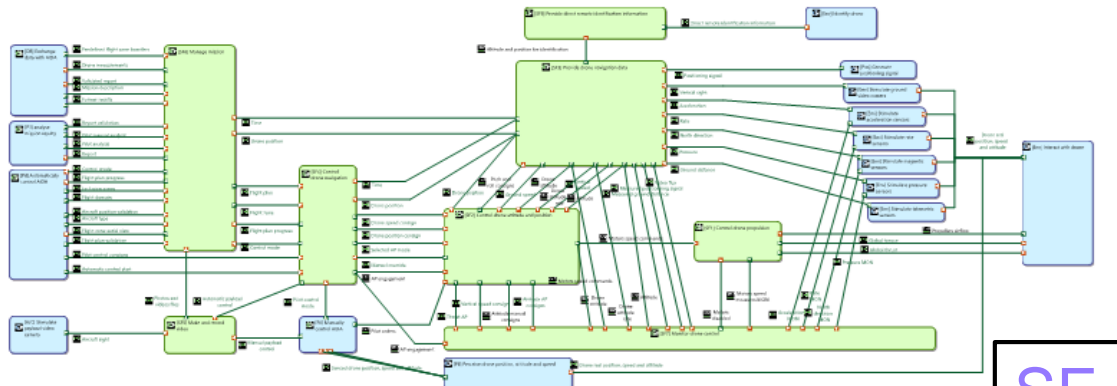
Representation differs



Problem Positioning

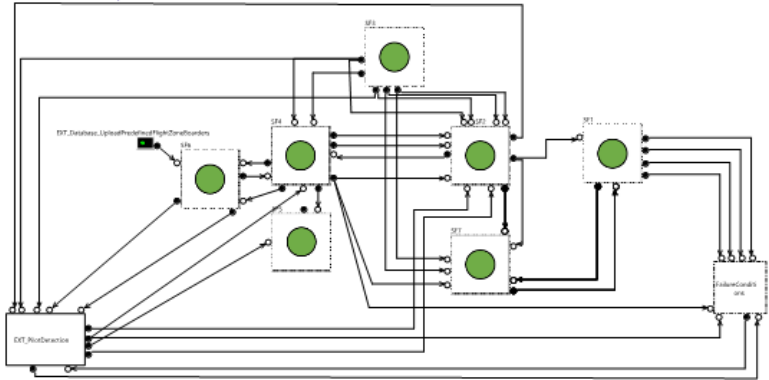
Statement

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



SE

Consistent ?



SA

When method shall be used ?

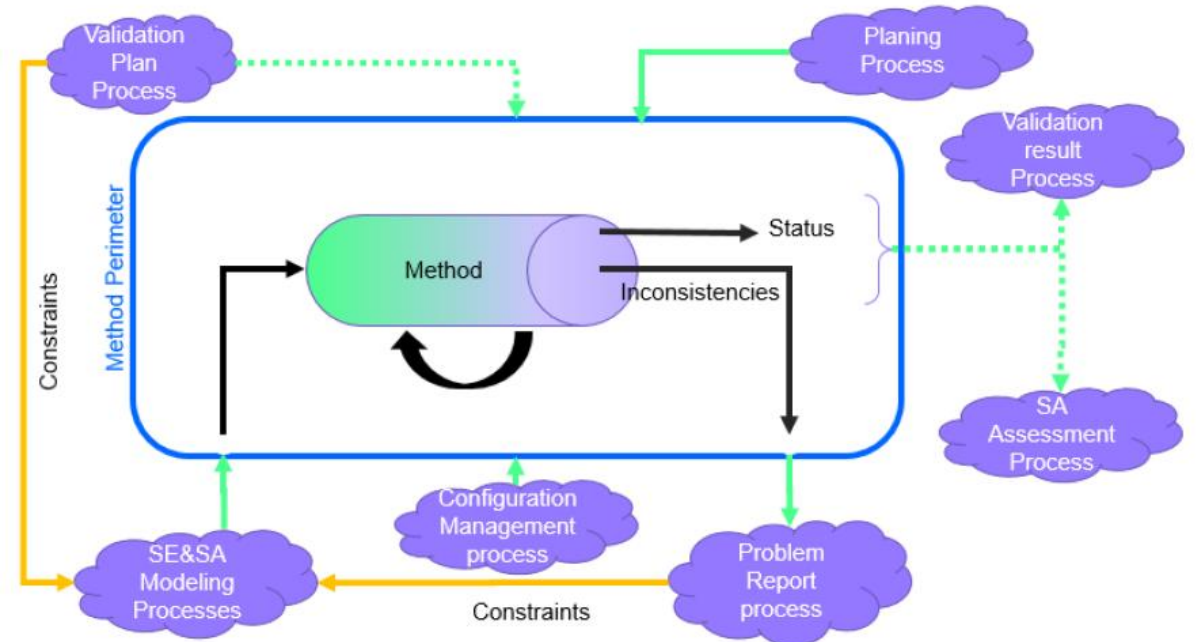


Both SE and SA models are available

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

page 28

Dimension : Coupling of Authoring

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

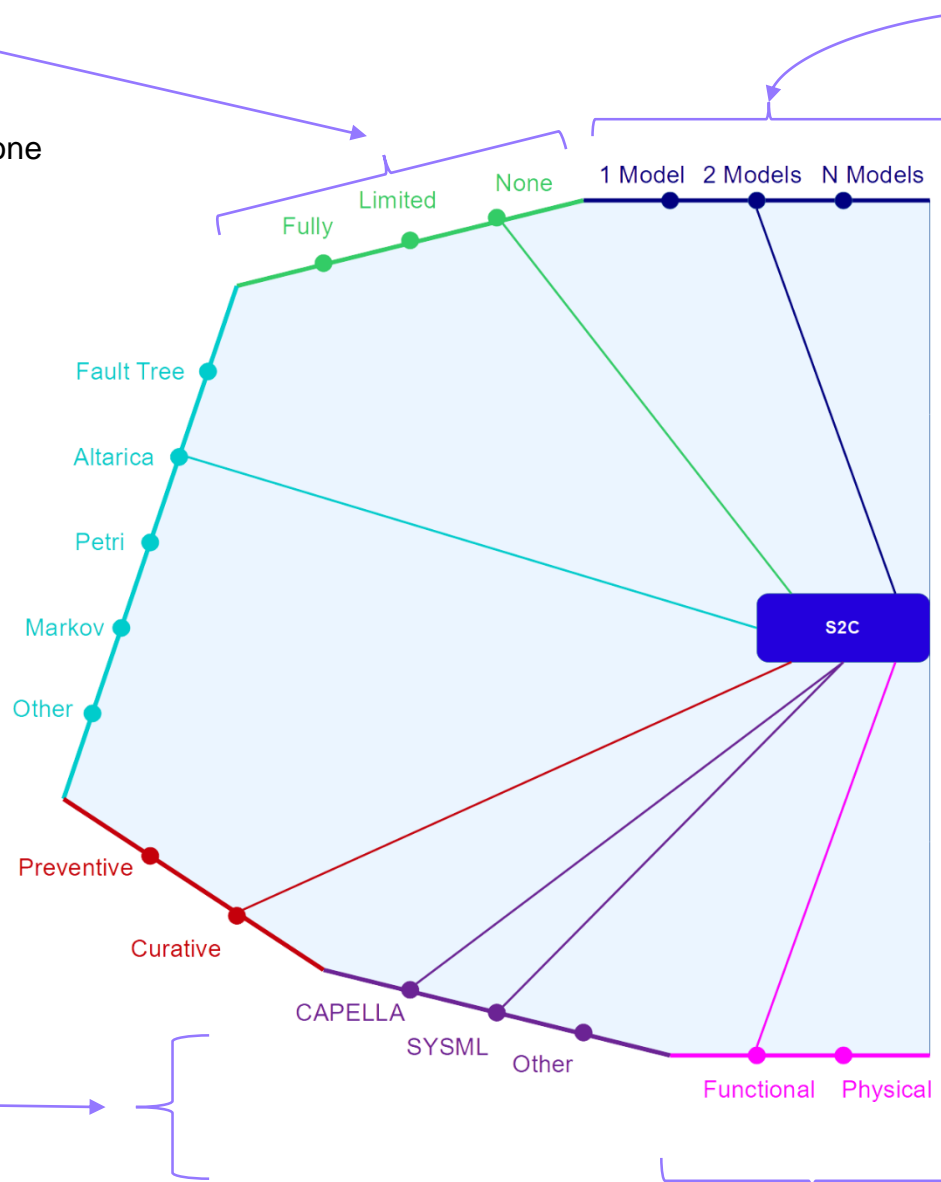
Dimension : SA model paradigm

- Underlying mathematic rules

Dimension : Method incursion on authoring

Dimension : SE model paradigm

- Underlying grammar and usage



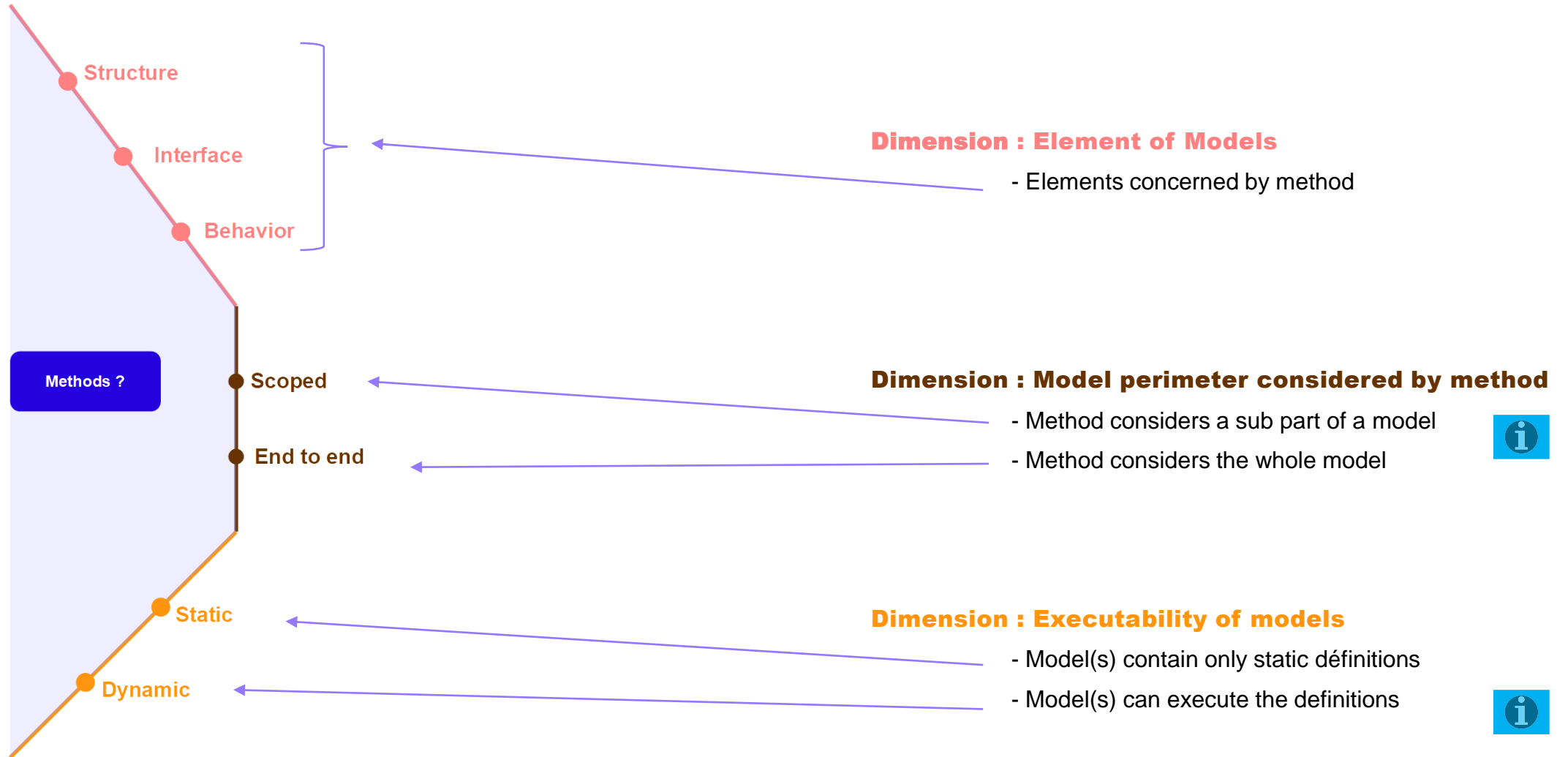
Dimension : Cardinality of Models

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

Dimension : Level of models

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

Problem Positioning : (exploratory) dimensions with their items





**Method for consistency
between MBSE and MBSA**

-

Solutions Take away

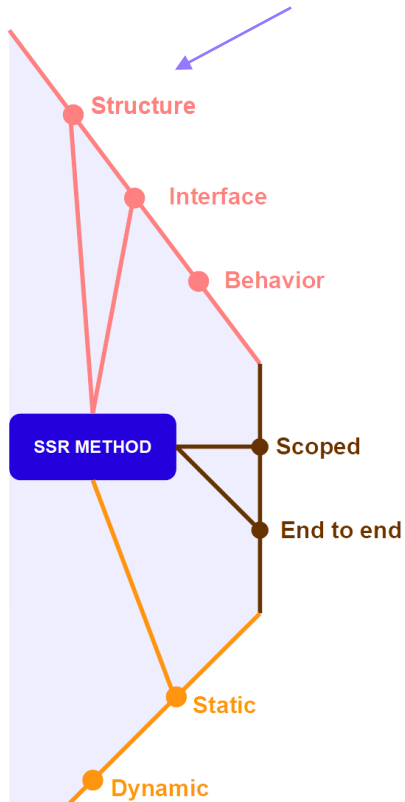
Take away : framing

Method cardinality : not 1 method but 3 ones

Structural Scope Review [SSR]

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

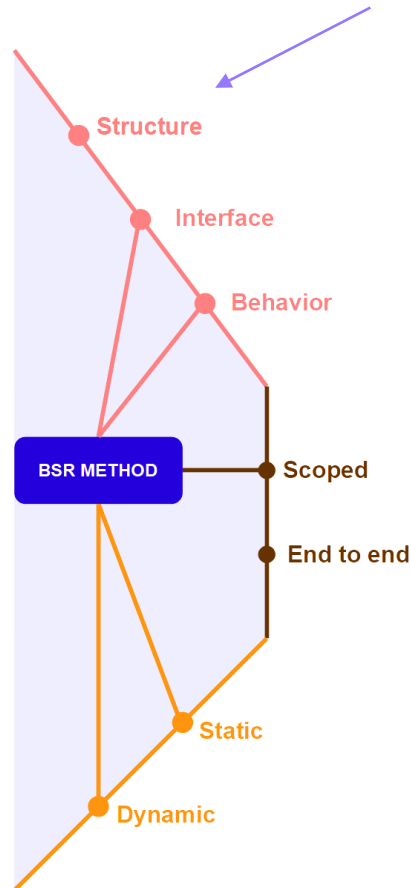
(Idea borrowed from process method)



Behavior Scope Review [BSR]

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

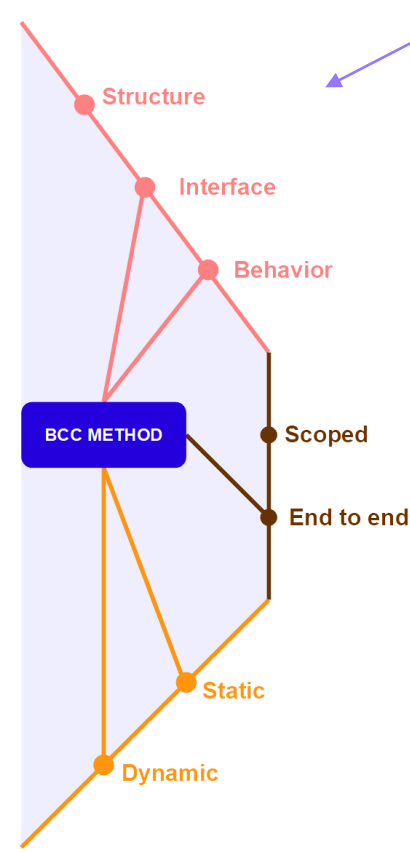
(Idea borrowed from software testing)



Behavior Cross Check [BCC]

kind of « model behavior comparison upon scenarios »

(Idea borrowed from Flight Testing for Performance model resynchronisation)



Methods inter-relationship

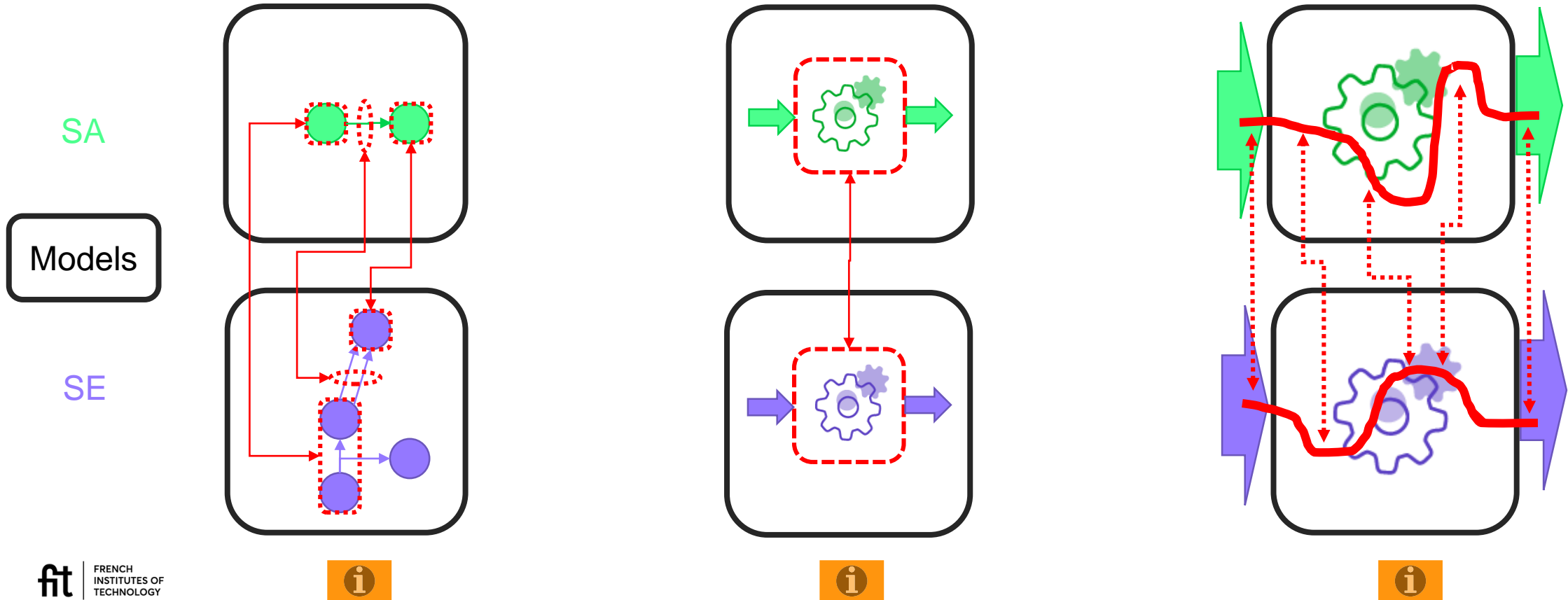
- Only one, (e.g. BSR only)
- Two amongst 3 (e.g. SSR and BCC)
- All the 3 (e.g. SSR and BSR and BCC)

Methods development

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

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





**Method for consistency
between MBSE and MBSA**

-

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 considers ?

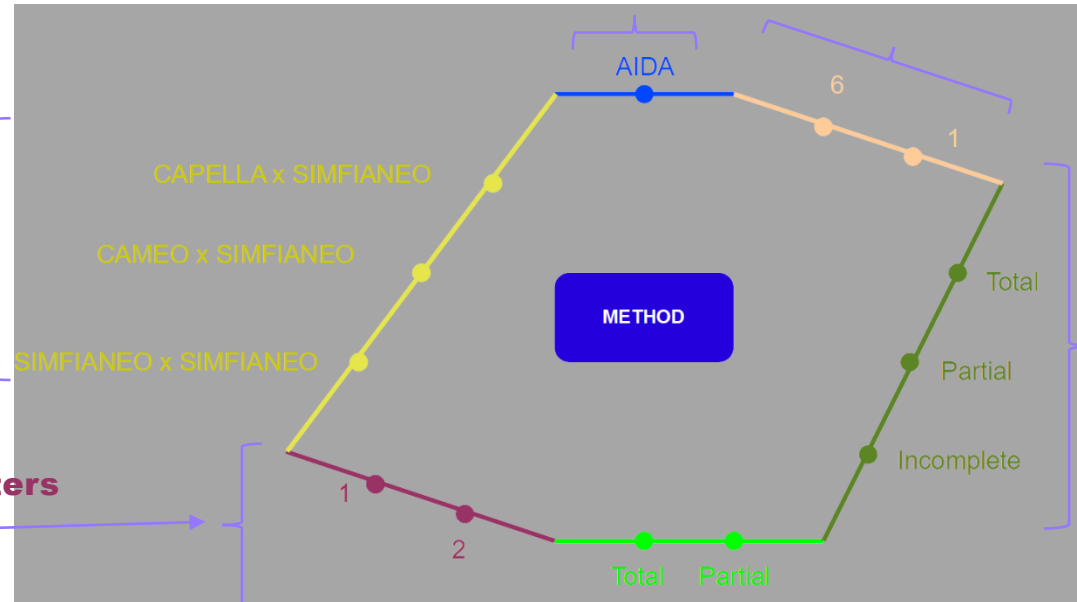


Dimension : sub perimeters vs Model

- How sub perimeters overlap the whole model ?

Dimension : Itérations done on sub perimeters

- Is there several iterations ?

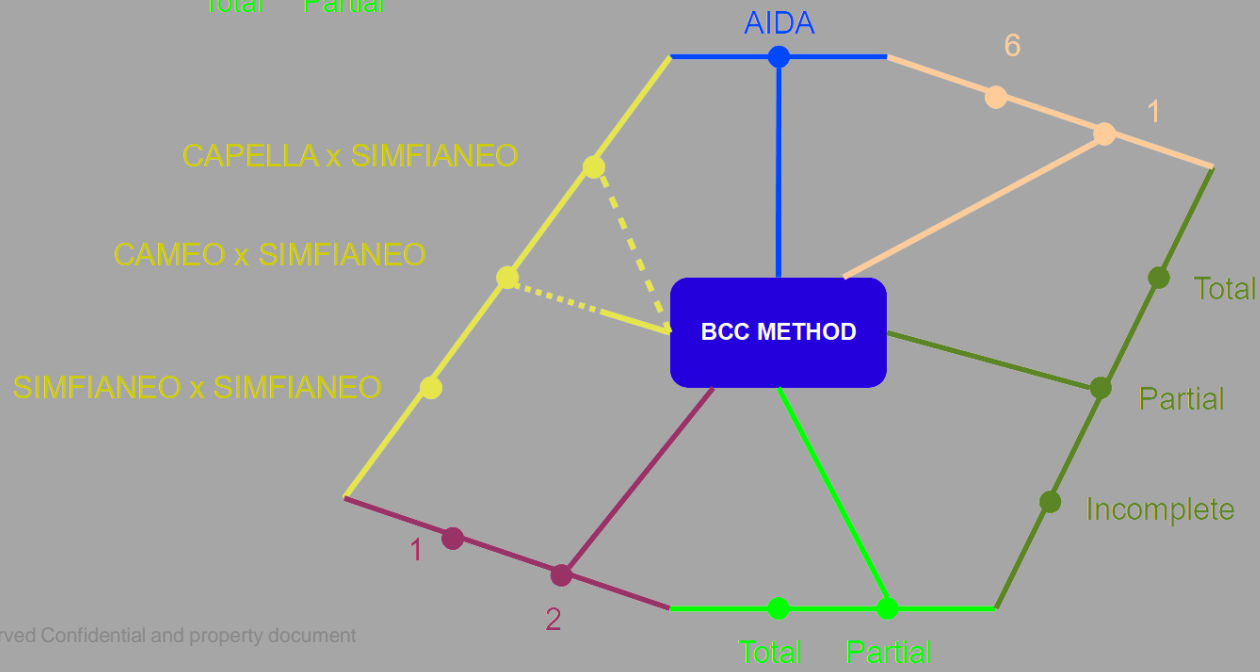
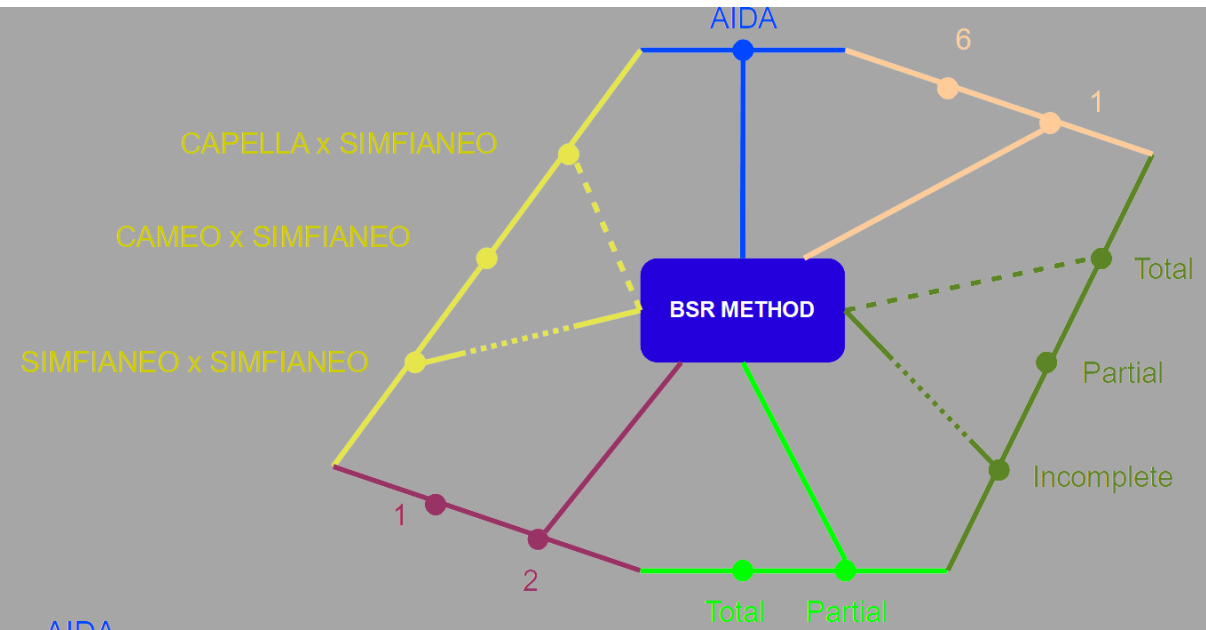
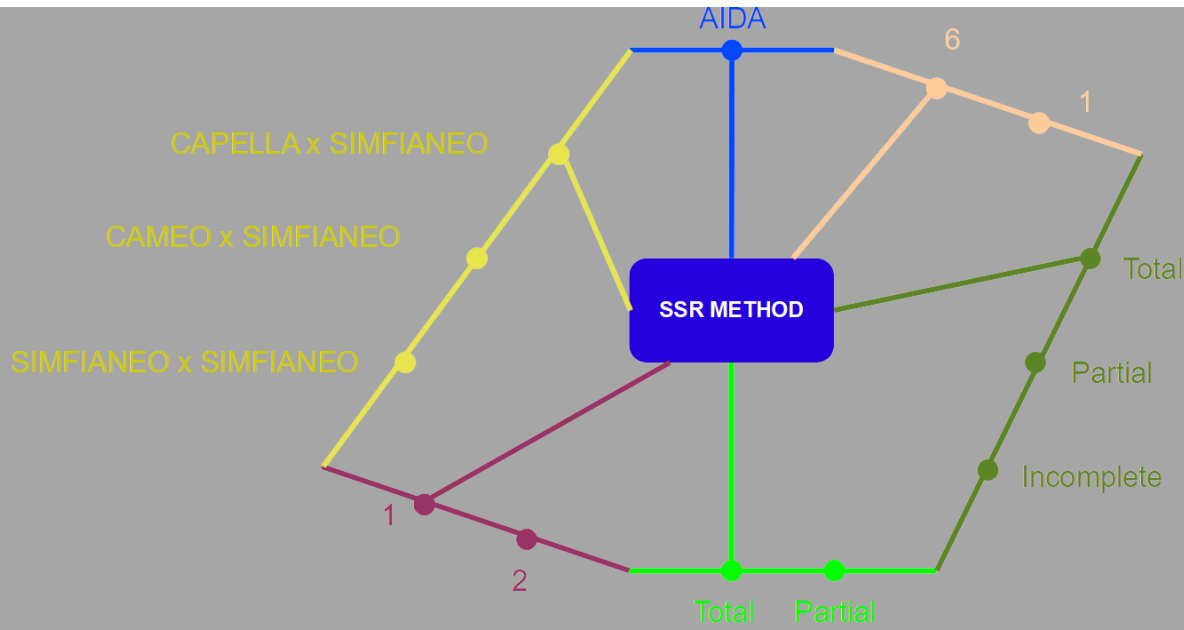


Dimension : Coverage of sub perimeters

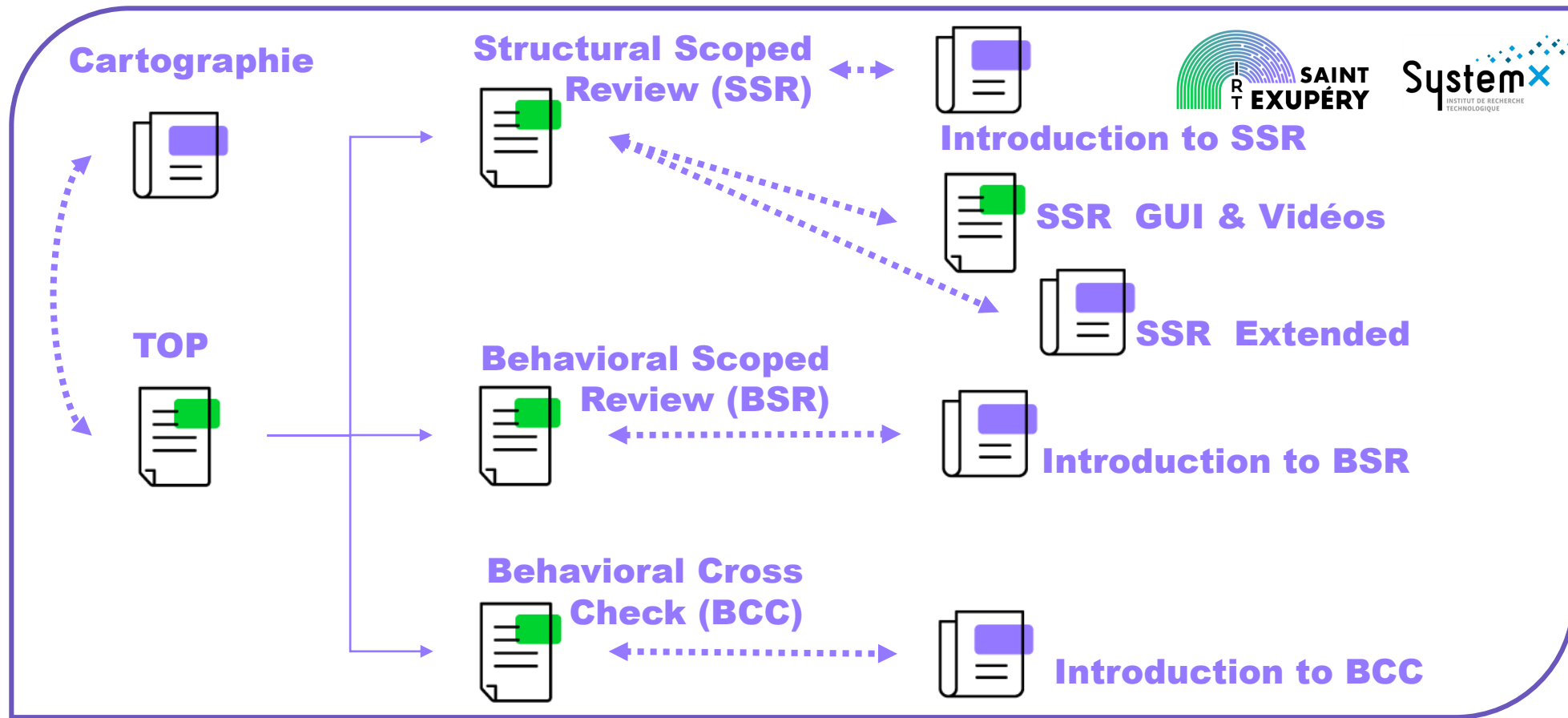
- Is all case into sub perimeters covered ?



PoC Dimensioning



Take away : Where to find informations



SHAREPOINT Projet

Accr.	Id.	Accr.	Id.
TOP	LIV-S085L02-007-V6 : MBSE-MBSA Consistency	Cartographie	NT-S085L02T00-034-V3
SSR	LIV-S085L02-023-V3 : Structural Scoped Review	Intro. SSR	NT-S085L02T00-040-V0
BSR	LIV-S085L02-024-V6 : Behavioral Scoped Review	Intro. BSR	NT-S085L02T00-041-V0
BCC	LIV-S085L02-025-V6 : Behavioral Cross Check	Intro. BCC	NT-S085L02T00-042-V0
SSR GUI	LIV-S085L00-017-V1	SSR étendu	NT-S085L02T00-031-DRAFT



**Method for consistency
between MBSE and MBSA**

Returns of Experience

Results after POCs

None-coupling hypothesis (i.e. full freedom from specialist when authoring)

Proving or stating the equivalent at **structural, interface and behavior**, costs a lot due to the fact that methods are curative because applied after “free” authoring, where changes over structure and interface are done to match each special needs but not traced/explained the other.

So This is the most difficult approach taken (it works but in a limited way against the possible gains)

Content of Models will progressively overlap ...

Initially models can overlap the « when no failure logic » only
 Progressively the SE model overlap more the SA one
 (e.g. monitoring added to SE after SA recommendations)

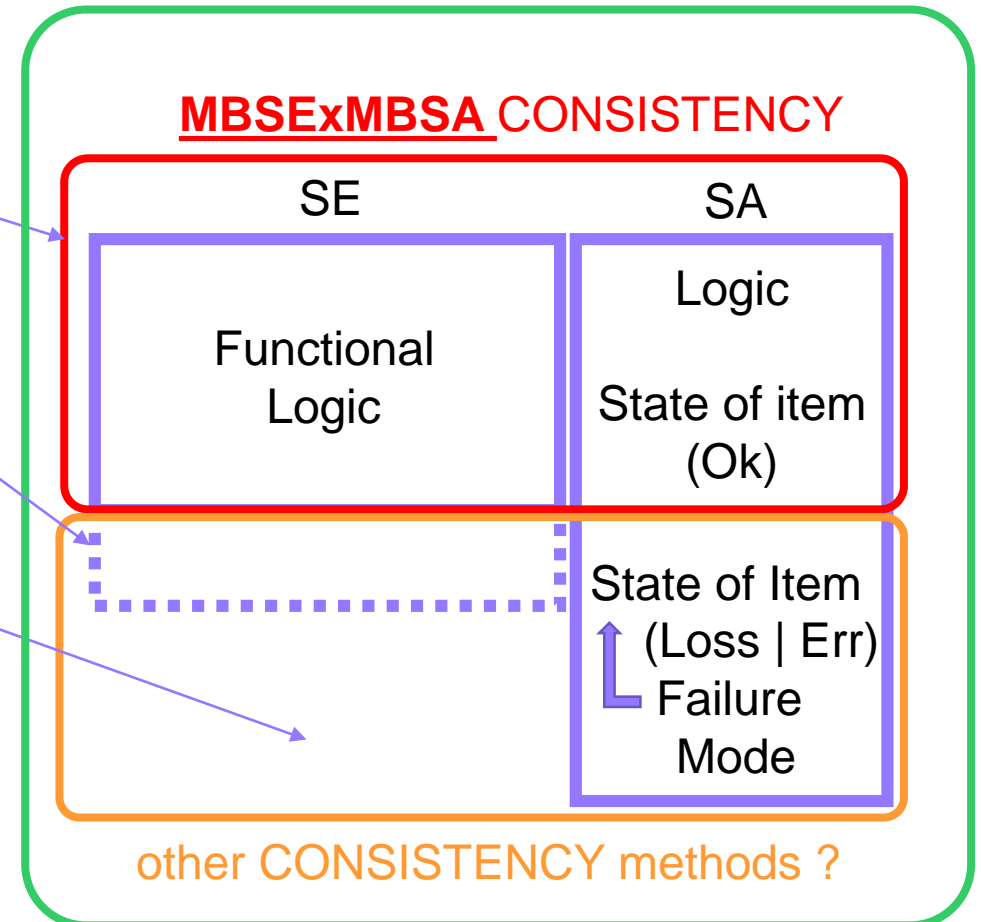
... **but on limited scope**

Some part remains a SExSA consistency problem (not cross 'MBSx')
 (e.g. what failure mode to consider is only in SA model ...)
 (e.g. not safety critical artefact exist only in SE model)

Coverage of model is not reached in some method

- BCC can not cover all the behaviors
- for BSR can not cover all the subparts

SExSA CONSISTENCY perimeter



Extend exploratory tracks

Explore the item called « limited » in coupling dimension to avoid current curative approaches

- What can be a minimal set of rules that each specialty shall apply when authoring its own model to foster consistency?
- What kind of tool can be used to populate SA model from SE model to ease consistency in the structure and interface facets (at least) ?
(without jeopardizing the independence criteria between specialities)

Explore item called « Dynamic » in executability of model dimension for SE

- Could Altarica computation engine be used to model SE logic and derisk some functional SE architecture points ?
(This may ease SA model review by SE, because he knows the tools and usage because he used it for its own modeling of logic.)

Explore item called « Physical » in level of model dimension to challenge given the methods

- What are the new concepts and their complexity carried on by physical models for SA and SE models against the methods?

Explore/Write scenarios driven dev models

- Can an anticipated usage of the scenarios, before modelling (and not after), foster mutual understanding before authoring?

Reinject RETEX into modelling methods (SE and SA) (to avoid the curative dimension)

- IMDR calls (GIFAS 2022/11/16) to start a guide for modelling may be RETEX of WP and WP4 can be a basis.

Focus on item 2 of Exploration of « coupling dimension » : a GATEWAY from SE to SA



The gains

- **For consistency:** Less variability introduced by the SA specialist when authoring its model regarding the SE one
- **For efficiency:** avoid structural actions done to 'redo' parts (structure and interface) of what exist in SE model.

Challenges : the robustness to iterations

- Rebasing the SA model against the SE new baseline shall be efficient for SA (leading to revise some way of working and doing model)

Challenges : the mind set change

- Accept partial loss of control of
 - the original model (SE shall not use 'model tricks' that gateway is desiged to handle, that will jeopardize therebase)
 - derivated model (SA will not change part of its model otherwise this may jeopardize the rebase activities as what he did will be erased)
- Accept to configure the gateway in place of doing manually some jobs.

Challenges : preparation to the factorisation of commonalities

- Revise the mono container approach so that common parts model may have a common repositories and isolate specializations.

Challenges : add/improve QoS of SA tools

- Modelling tools have to improve their interoperability and data allocation in repositories.

Unify experiences (from all presented at GIFAS 16/11/2022) to be beneficial for all

AIRBUS PROTECT (Automotive RETEX) / SYSTEM ANALYST (Import CAPELLA) / ALL4TECH (CAPELLA to SAFETY ARCHITECT)



Contact :

systems-engineering@irt-saintexupery.com



Appendixes

-

Project Definitions

Project Definitions

S2C : System & Safety Continuity

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 different, 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 independent
(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 different is using the same tool remains commonality?

⇒ 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.

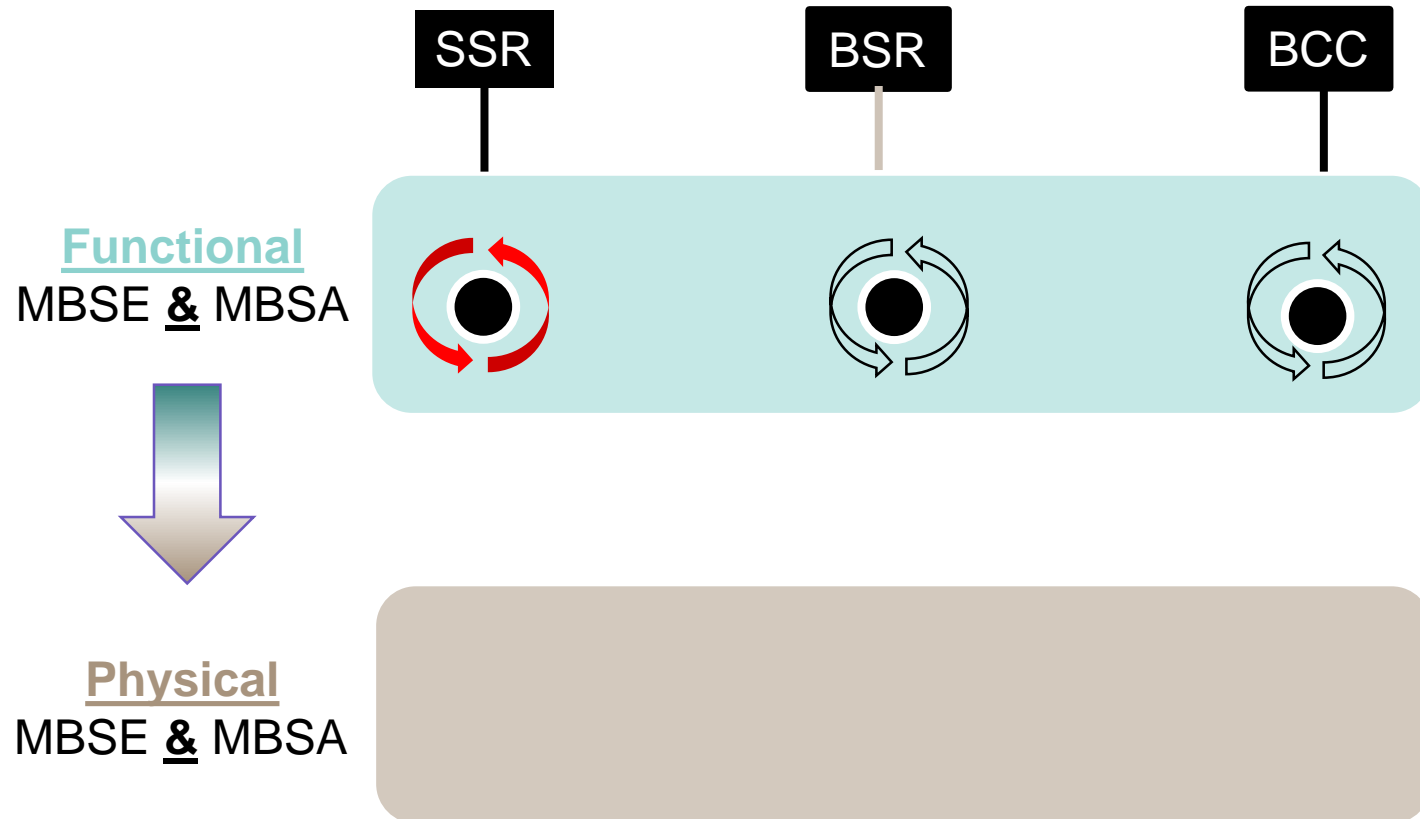
(frozen) dimensions : Why Functional only ?

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 announce
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 detachment 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 reasonable

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 differences between models without being 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 sequential 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 speciality but a trade off between both of them.

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



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 than from scratch



Farther usage for IRT

Comparison with other SE langage (SYSML)

Extended enterprise purpose.

Dimension : Couples of models

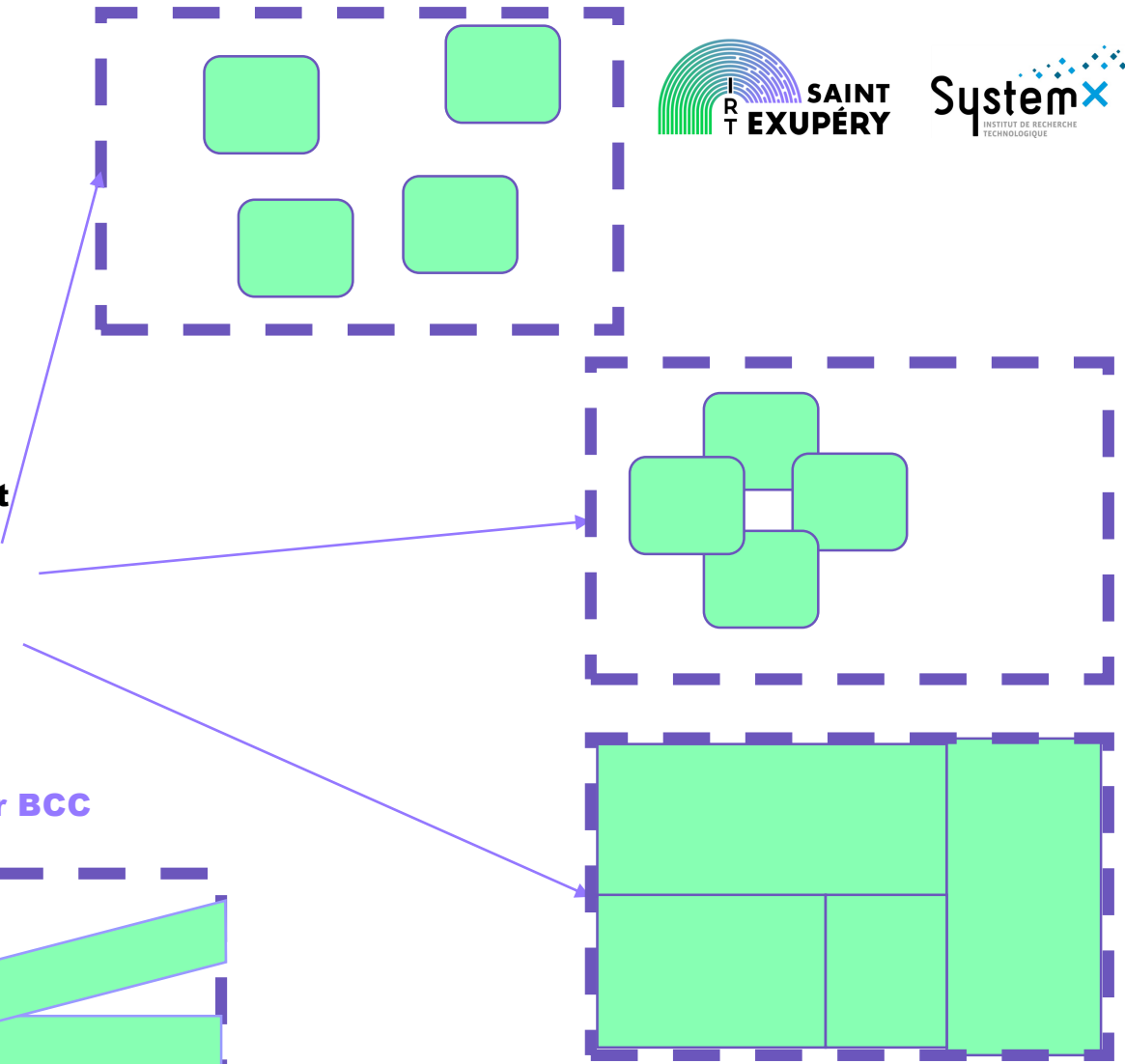
Expected and new track

SE Authoring tool	SE Authoring tool	Note
CAPELLA	SIMFIANE0	As expected by dimensions frozen dimensions  
CAMEO	SIMFIANE0	
SIMFIANE0	SIMFIANE0	New track using SIMFIANE0 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)

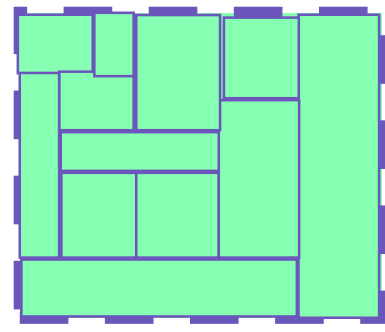
Dimension : Amount of sub perimeters and sub perimeters vs Model

Sub perimeters

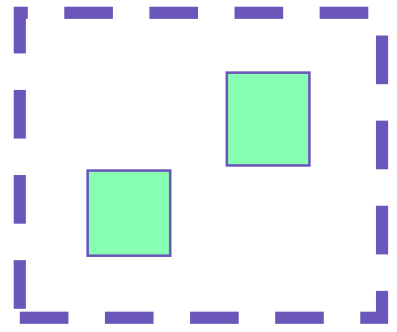
- If model is considered as a perimeter, PoC focused on sub part of it**
- One or several sub parts are possible**
- Overlapping of sub parts are possible**
- Union of all sub parts may cover the whole perimeter**



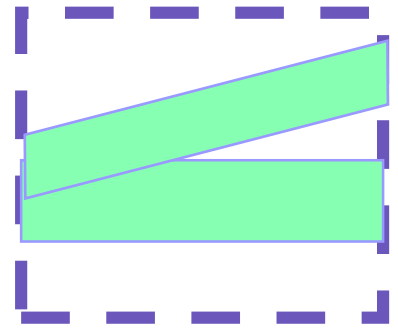
For SSR



For BSR



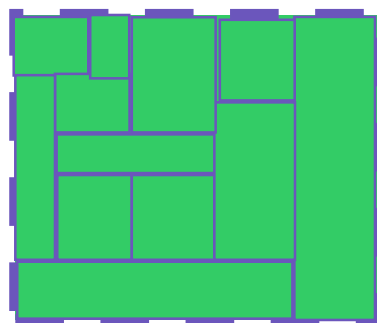
For BCC



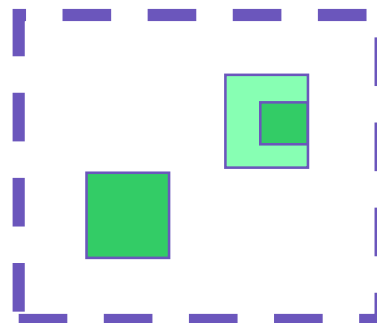
Dimension : Coverage of the sub perimeter

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

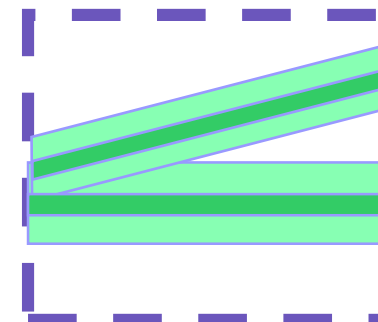
For SSR



For BSR



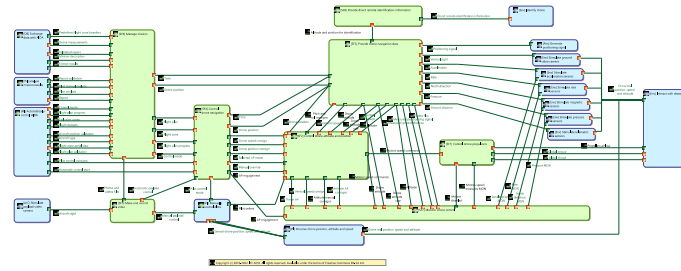
For BCC





Appendixes
-
**Details on
Proposed Solutions**

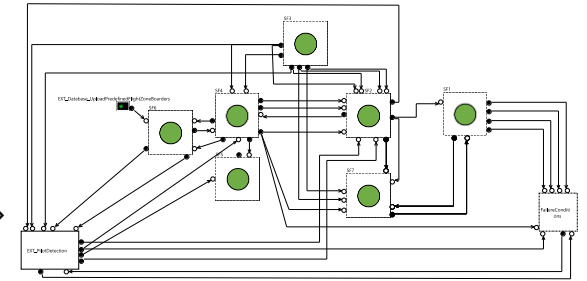
Remind the problem :



← SE one (CAPELLA)

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

SA one →

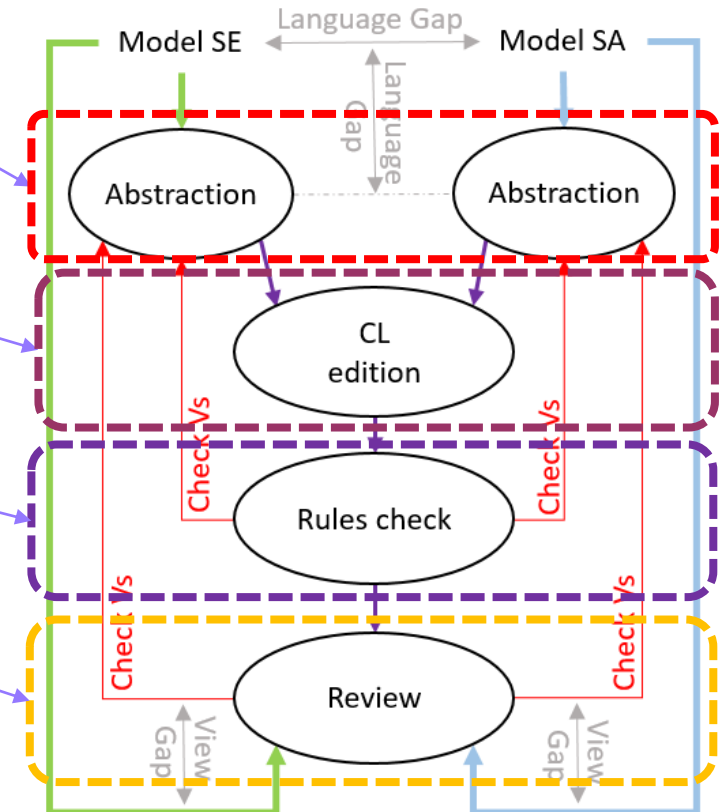


Method

- 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

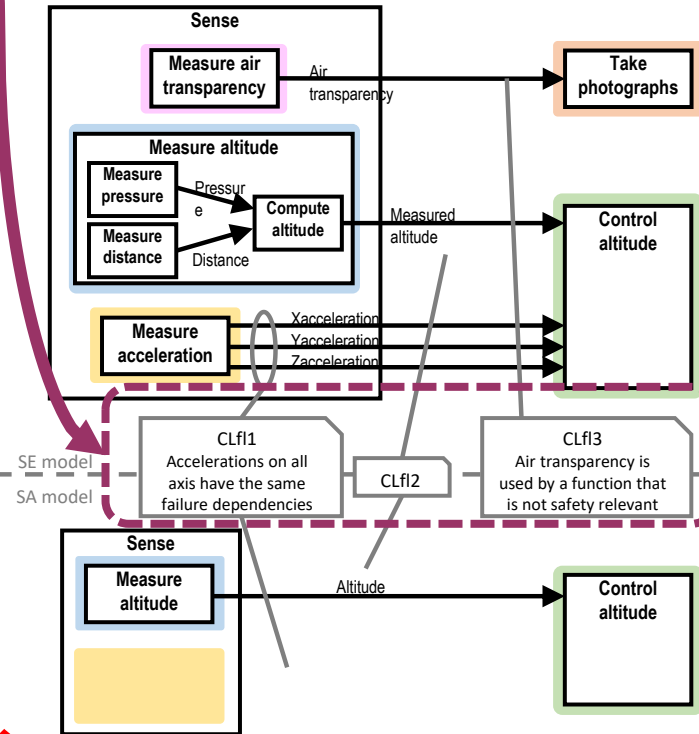
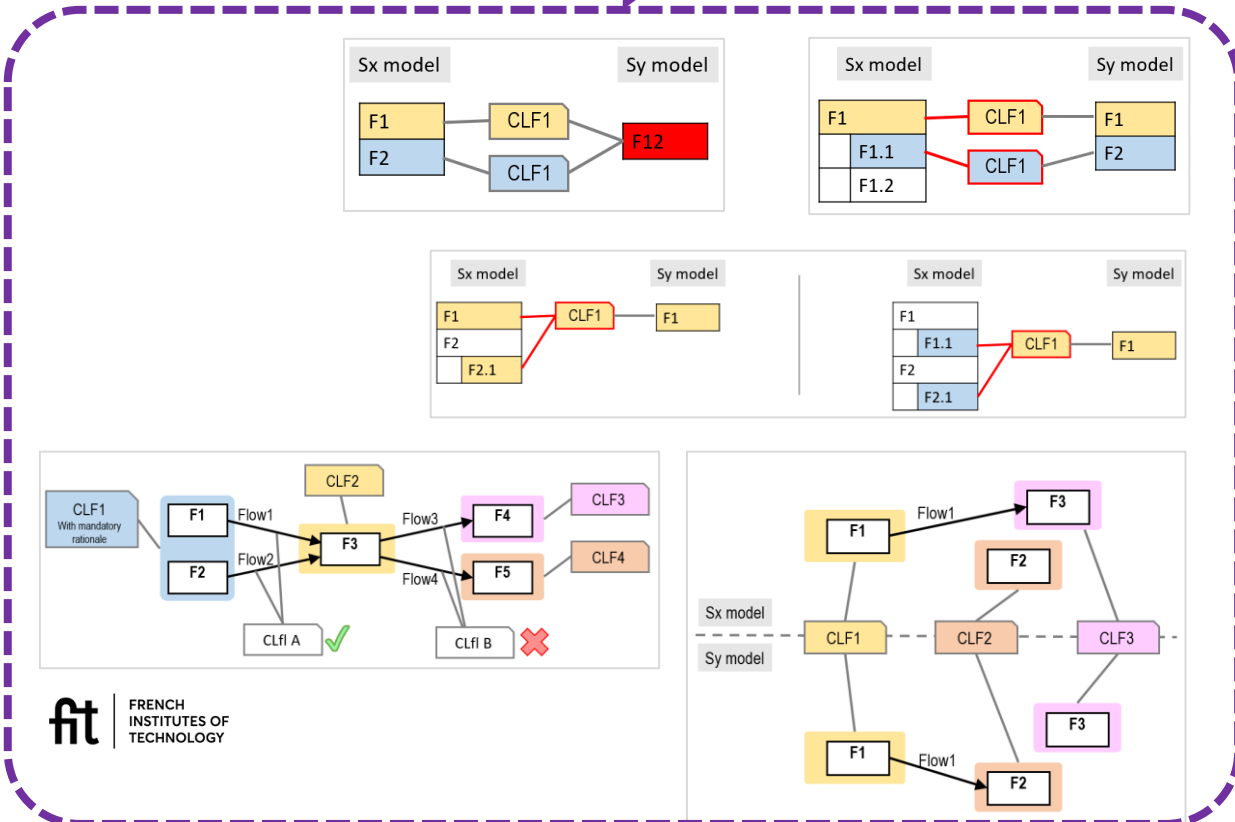
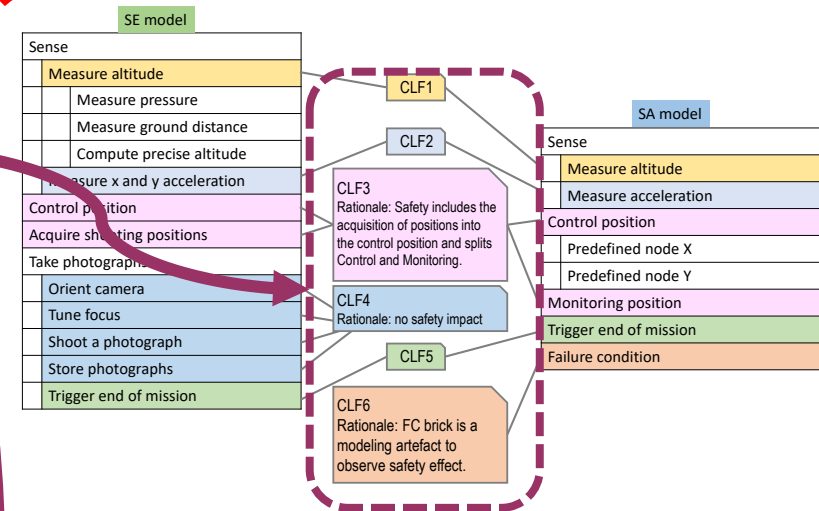
- Toolled process
- Coverage of the model



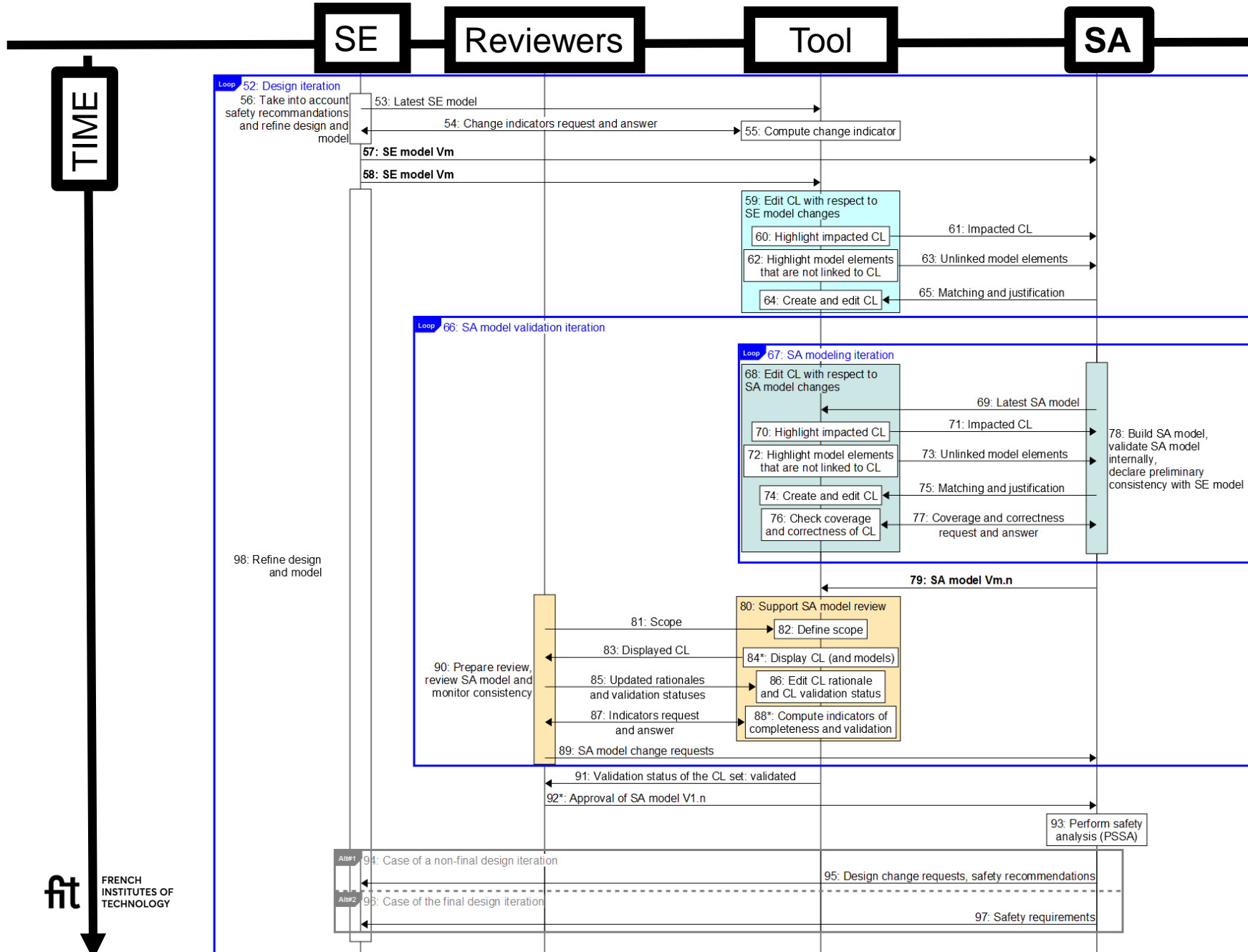
SSR : high level processus vs Examples

page 41

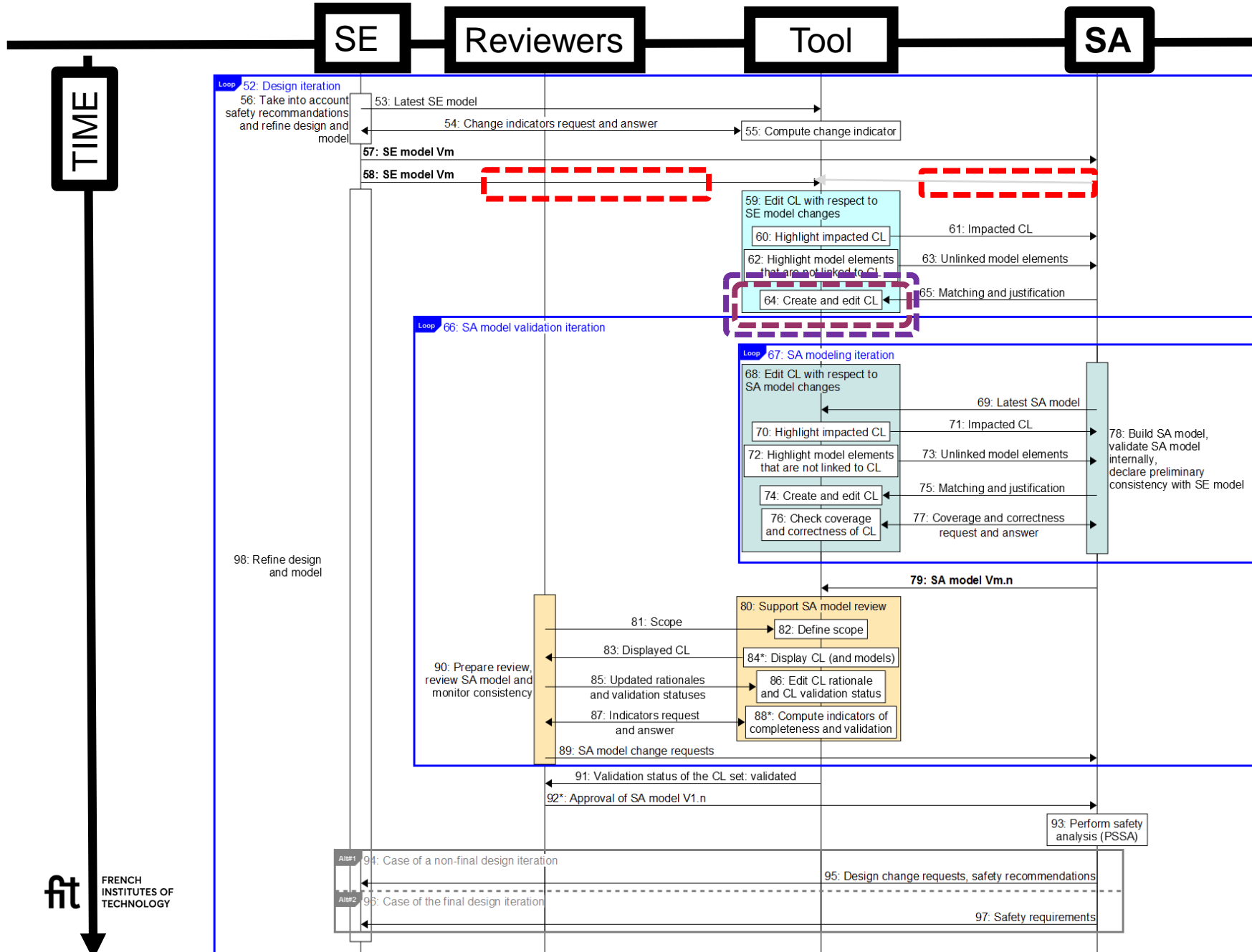
- Abstract both functional models to get their artefacts (structure and interfaces)
- Define structural link (CLFx) over functions (hierarchical or leaf) regarding method rules and capture: justifications, hypothesis etc.
- Define interfaces links (CLfly) regarding method rules and capture: justifications,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



SSR : Low level processus

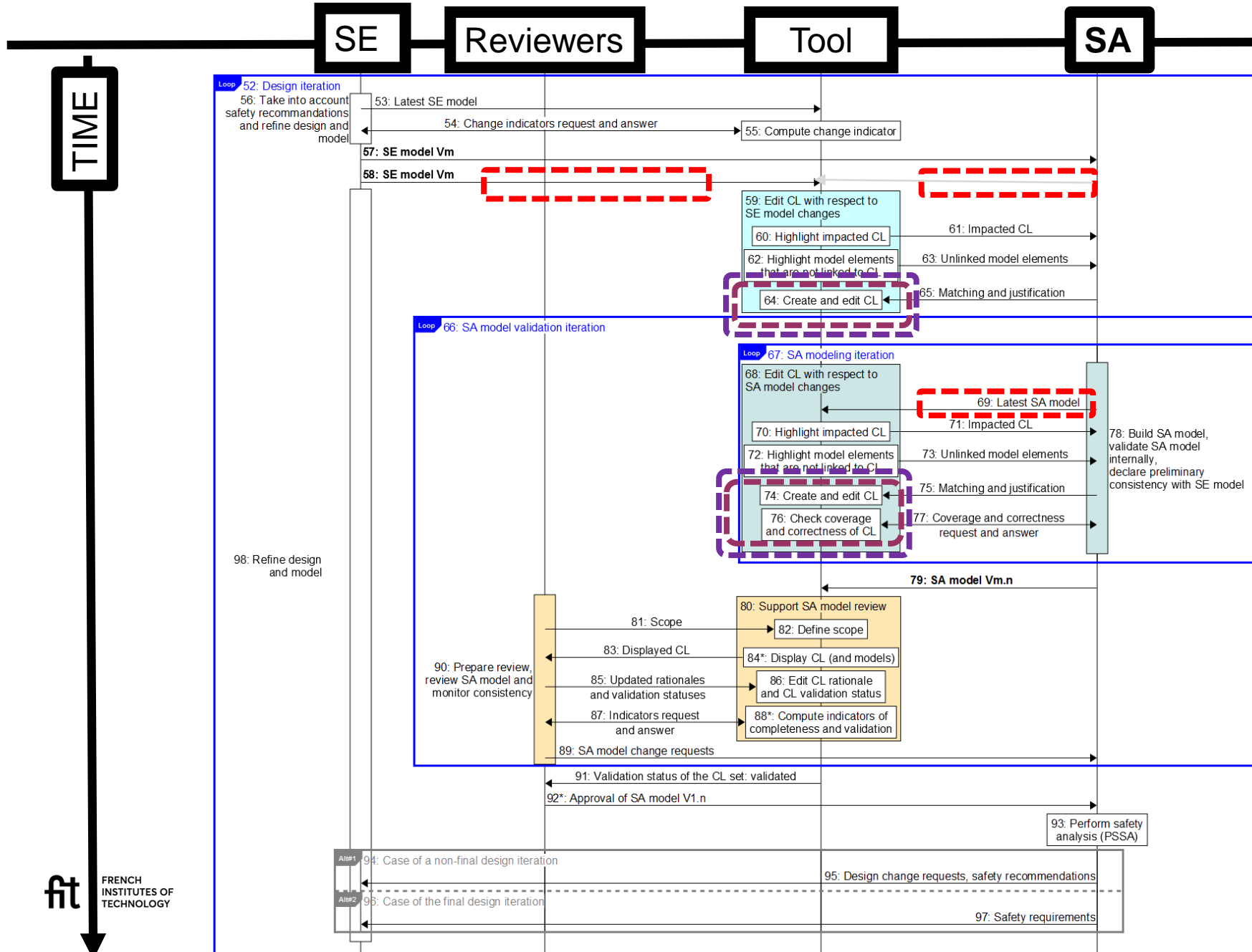


SSR : Low level processus



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

SSR : Low level processus

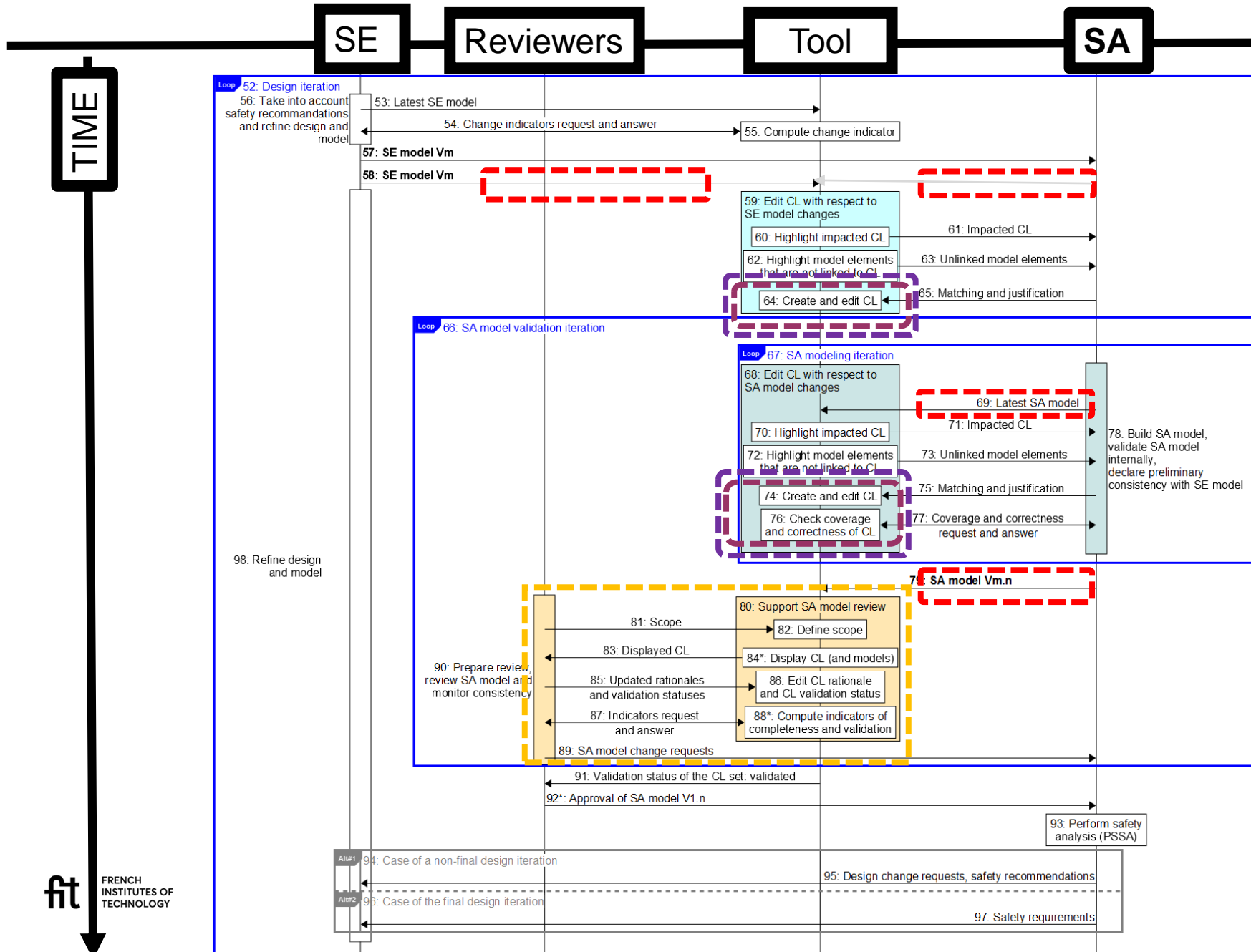


SE baseline changed, so ...
What's new ?
(SA realign concialiable CLs)

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



SSR : Low level processus



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

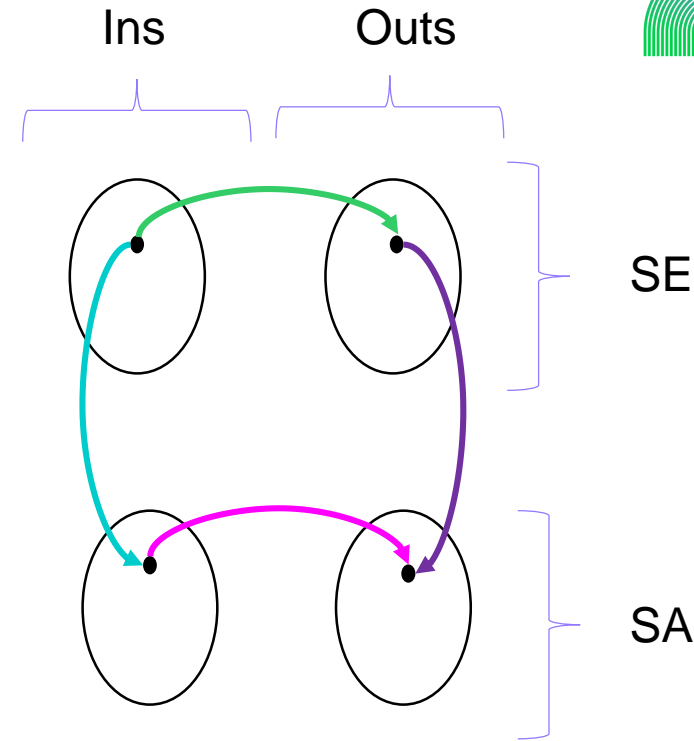
Method

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

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

PoC

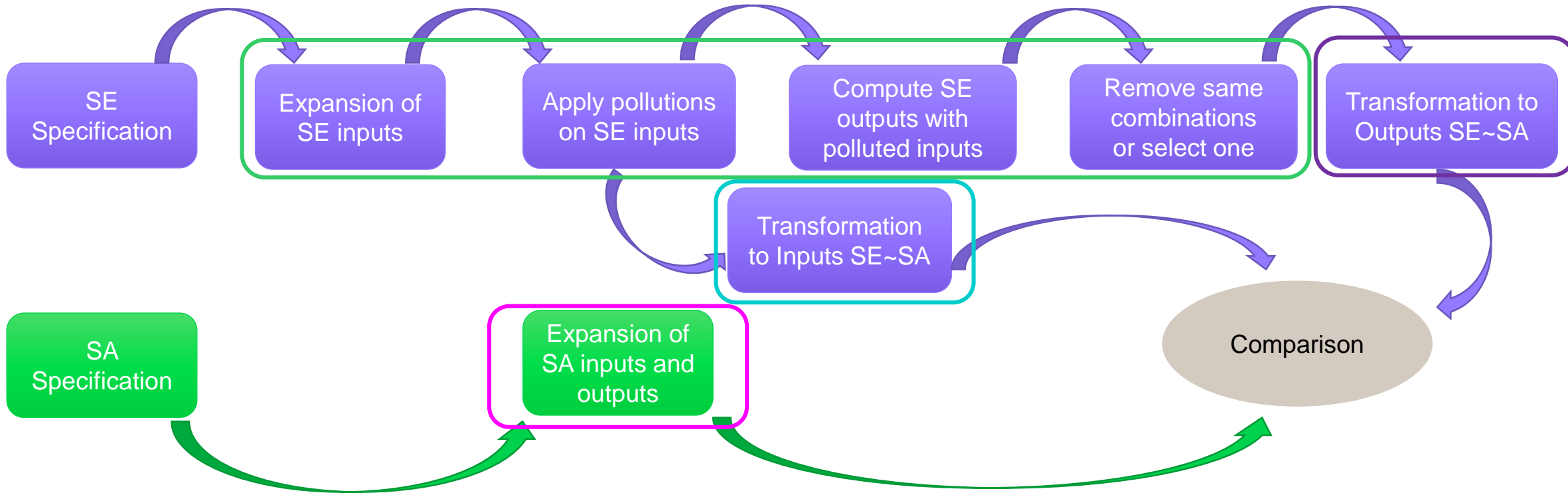
- Done on two scopes only and on logic exclusively (so very poor coverage and exploration too)
- Require tooling process because the amount of data can be huge.



Nota

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

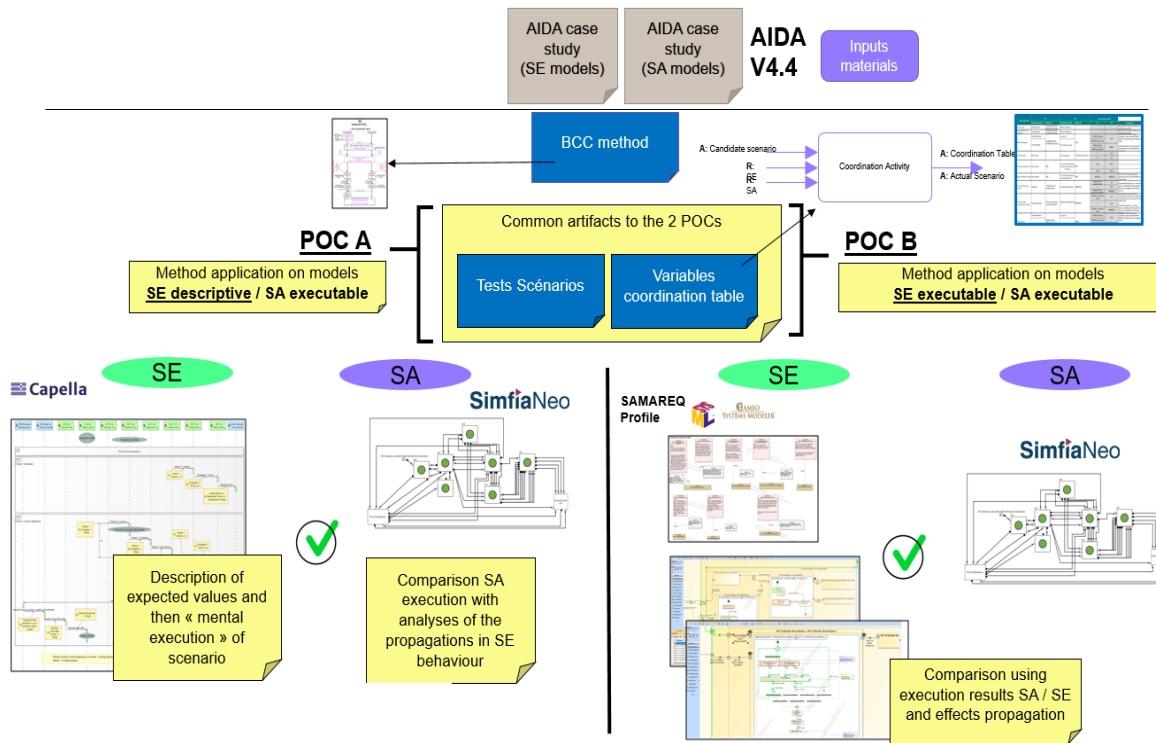
Over all process



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 and 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

SE&SA propose together...

... then specialists work

