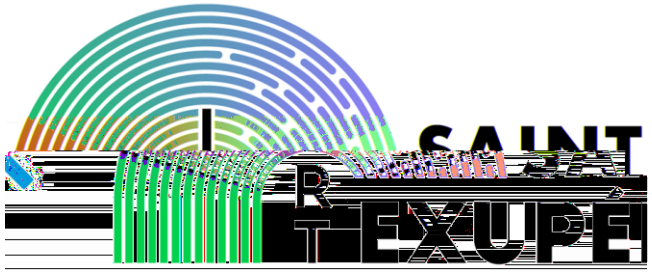
Référence IRT Saint Exupéry: NT-S085L02T00-042
Référence IRT System X : ISX-S2C-DOC-460
Version : V0
Date : 2023-01-12

Author(s)	*Function(s) & name(s)*	*IRTs Team*	*S. Guilmeau*
Checker(s)	*Function(s) & name(s)*	*Head Of project IRT Saint Exupéry*	*J. Perrin*
Approver	*Function & name*	*Head Of Disciplie*	*J. Baclet*



S2C

System & Safety Continuity

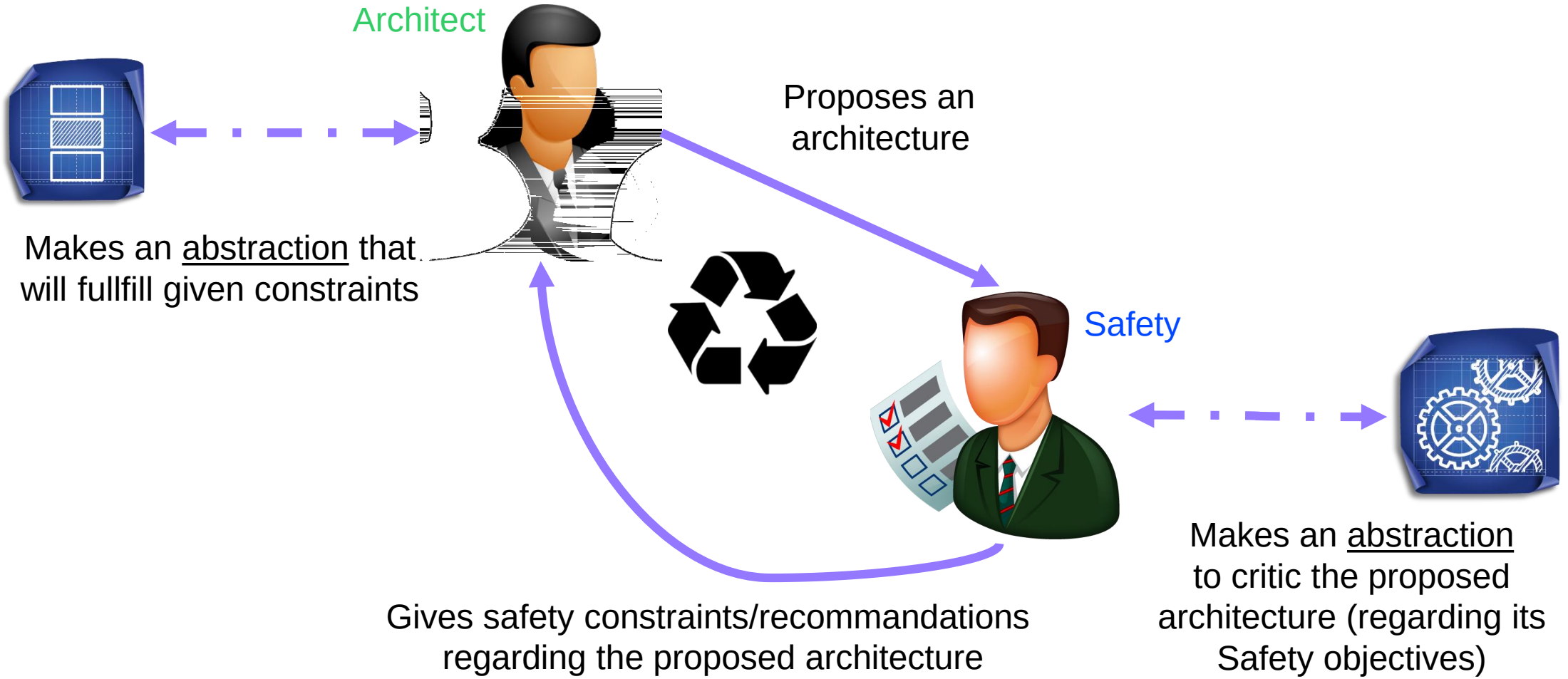
- Method for consistency between MBSE and MBSA
- **Behavioral Cross Check(BCC) -**

Table of Content

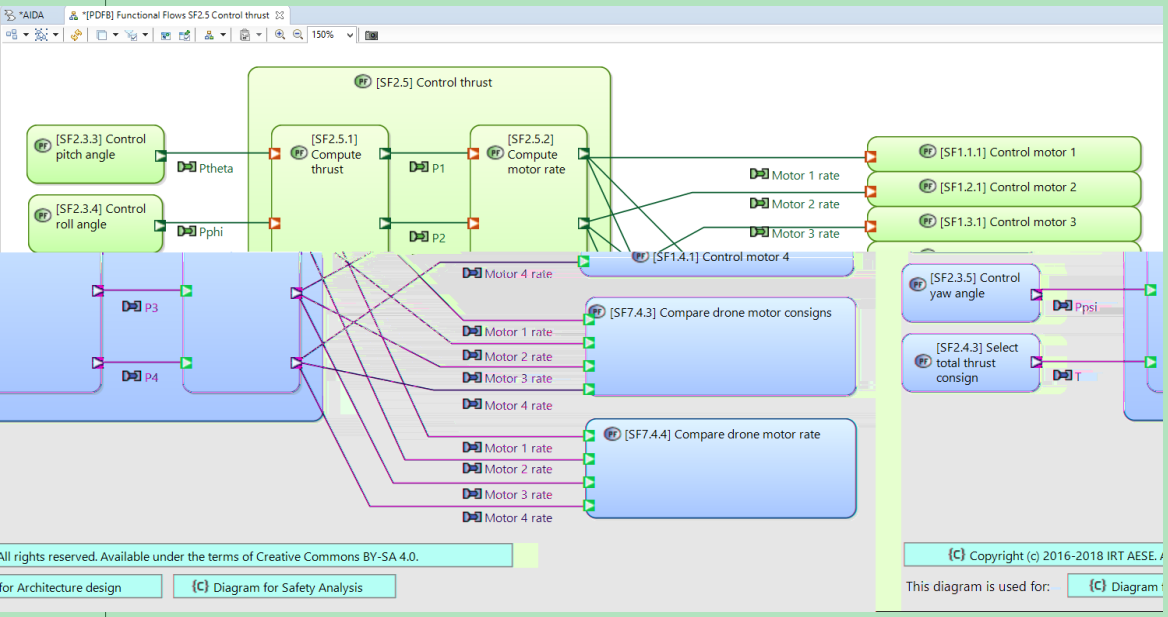
FRENCH INSTITUTES OF TECHNOLOGY

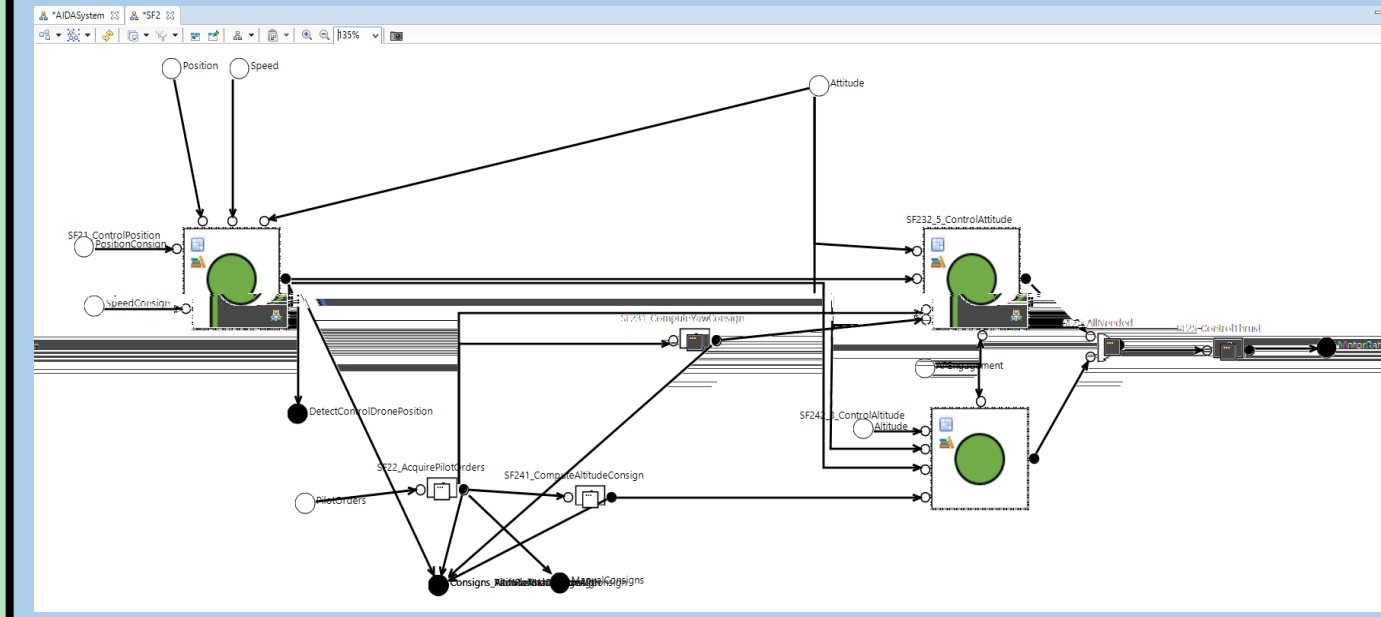
Method for consistency between MBSE and MBSA
-
Problem positionning by (very dummy) example

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



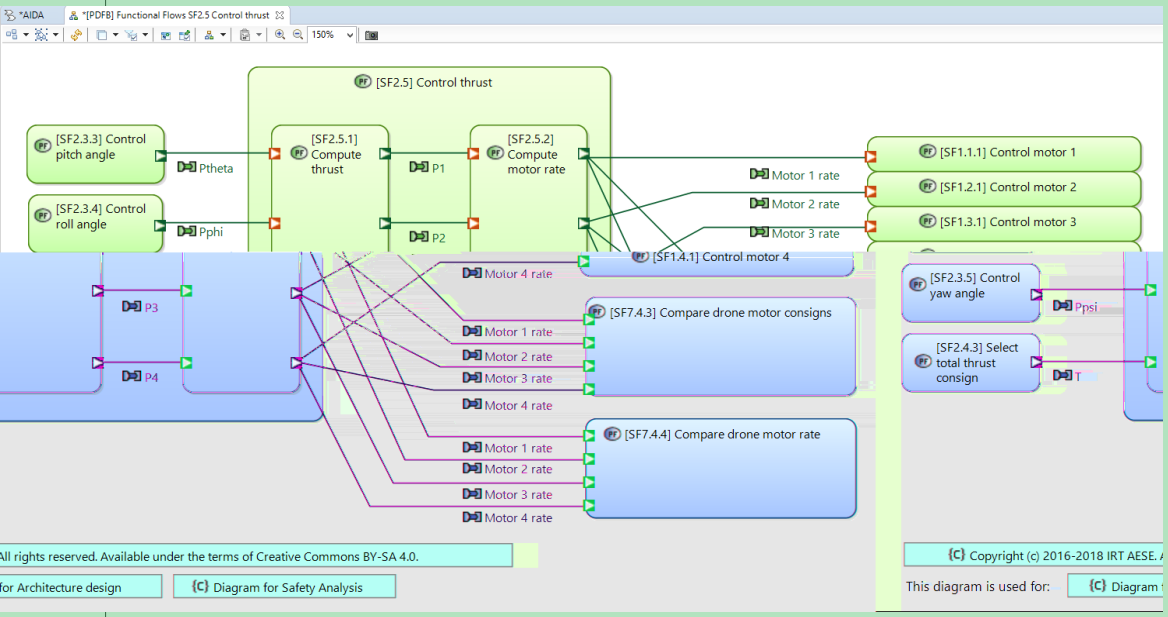
What occurs … at abstraction level

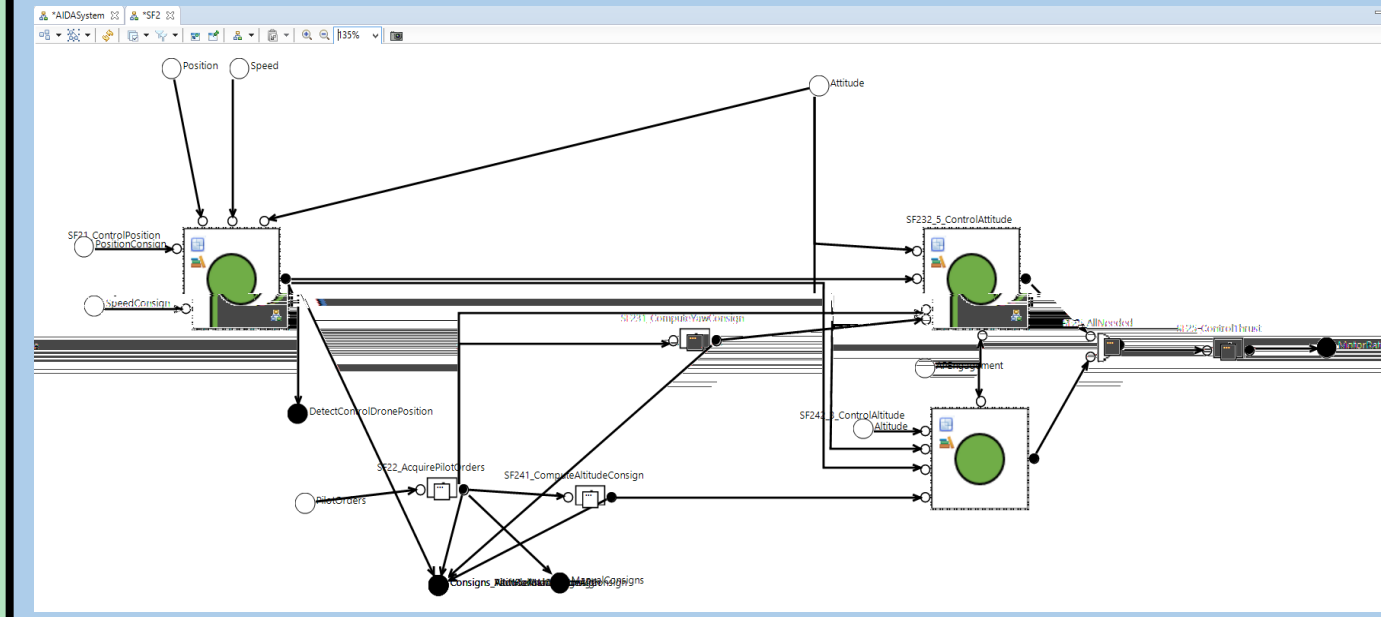




FRENCH INSTITUTES OF TECHNOLOGY

What occurs … at abstraction level



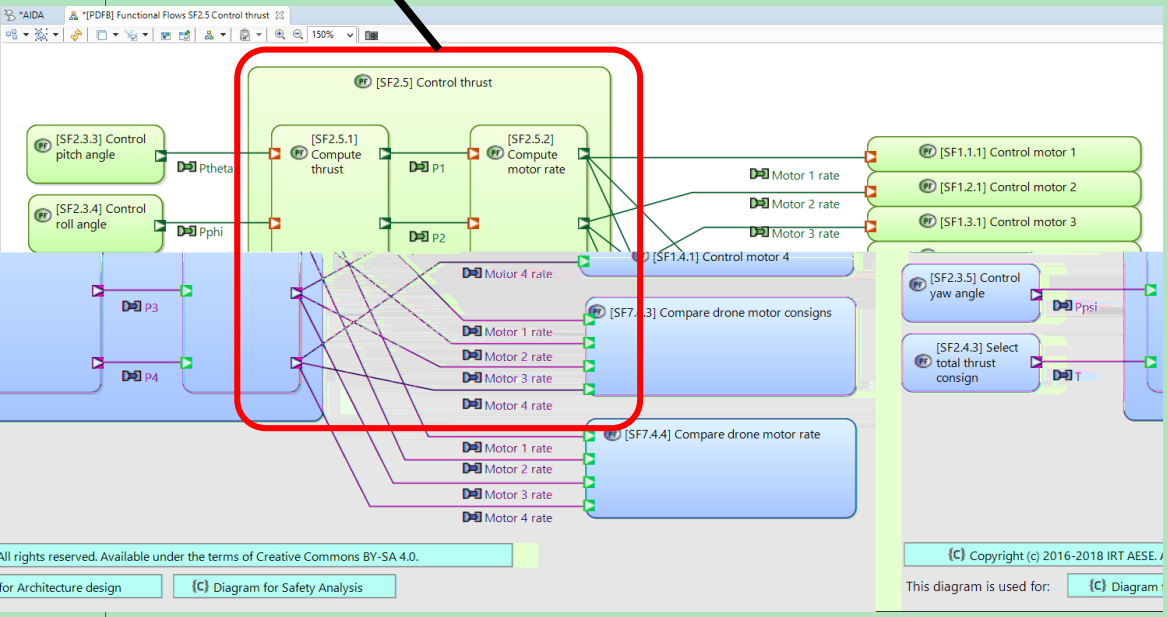


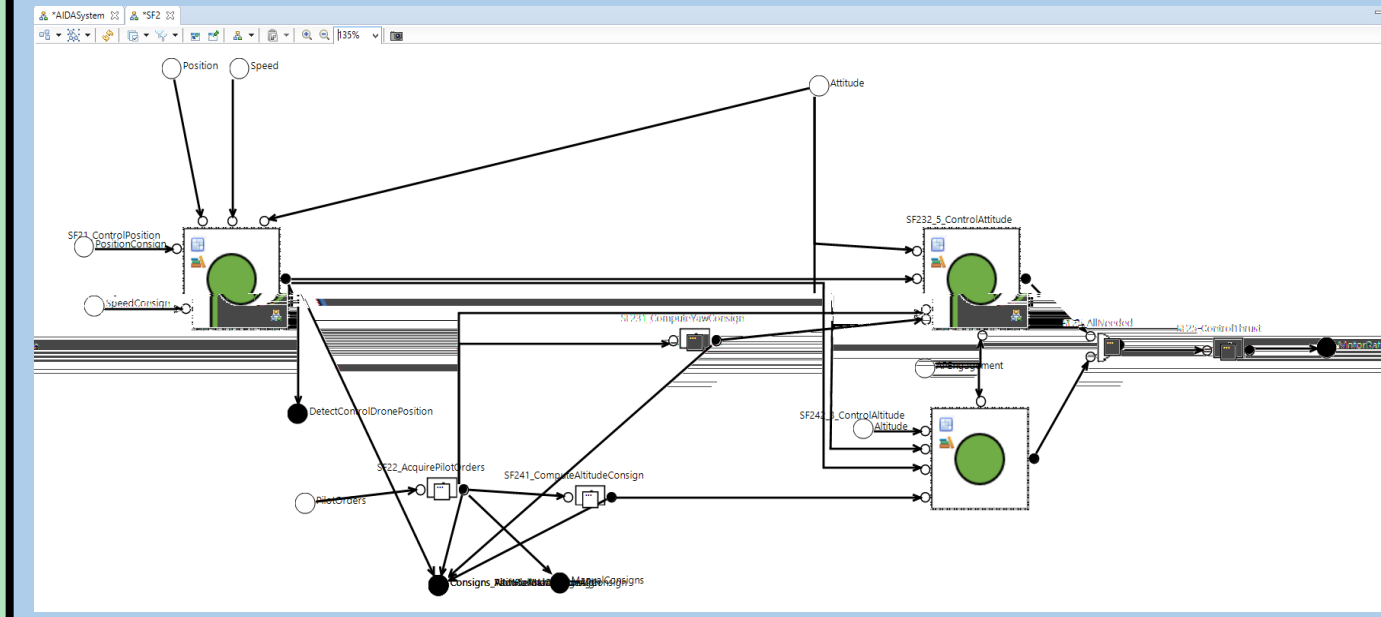
Representation differs

FRENCH INSTITUTES OF TECHNOLOGY

SF2.5 and its context seen from SE

What occurs ... at abstraction level



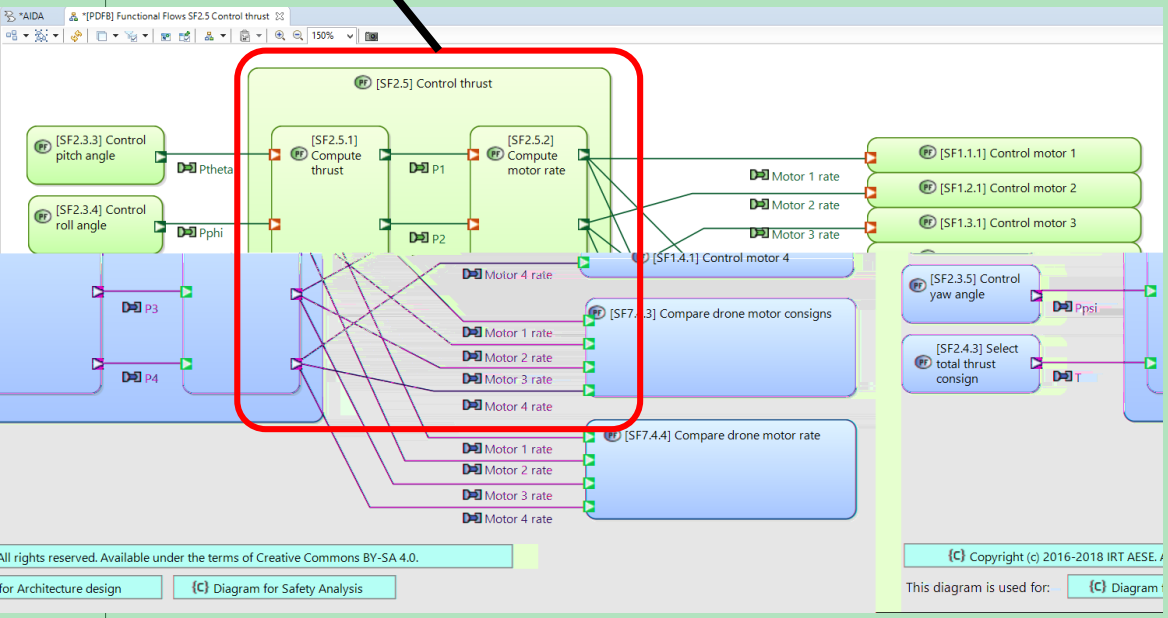


Representation differs

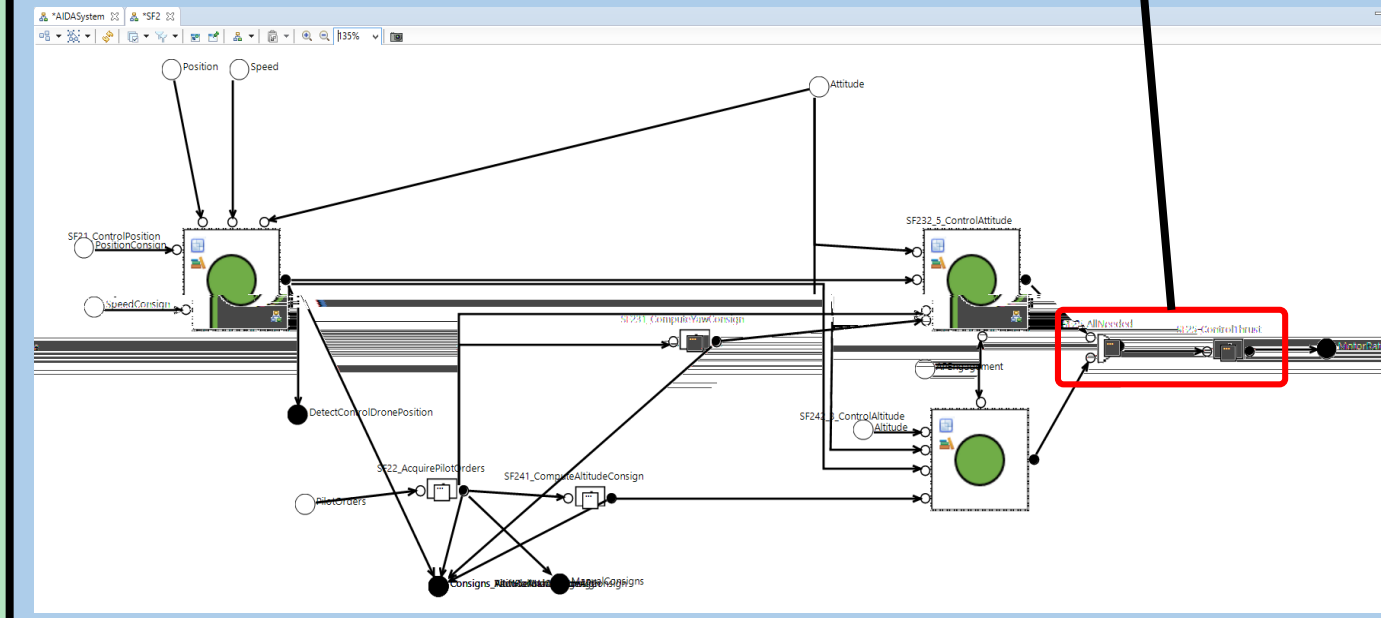
FRENCH INSTITUTES OF TECHNOLOGY

What occurs ... at abstraction level

SF2.5 and its context seen from SE



SF2.5 and its context seen from SA



Representation differs

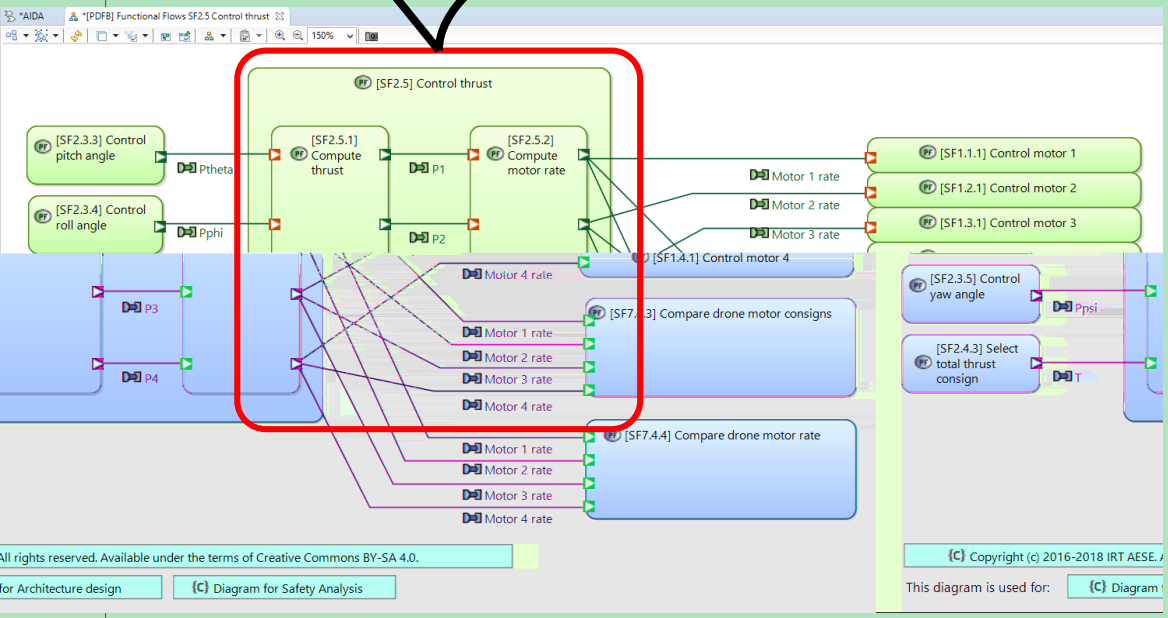
FRENCH INSTITUTES OF TECHNOLOGY

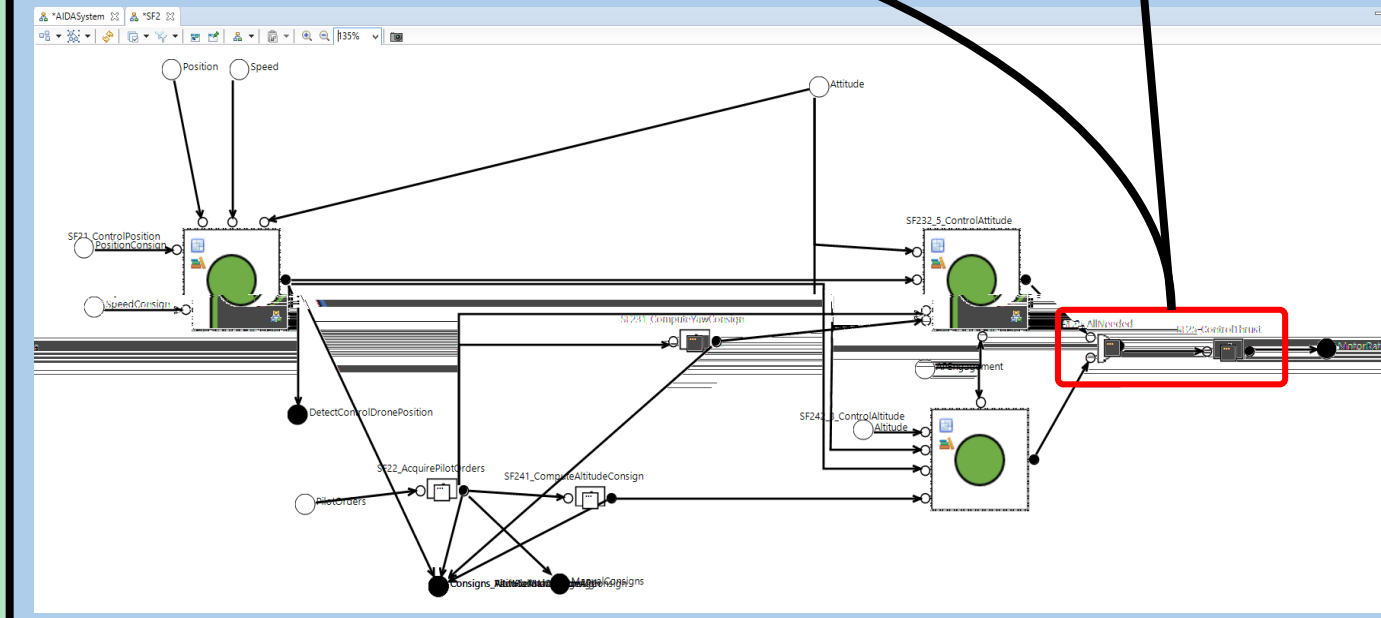
What occurs ... at abstraction level

SF2.5 and its context seen from SE

SF2.5 and its context seen from SA

Refinement and interface differ





Representation differs

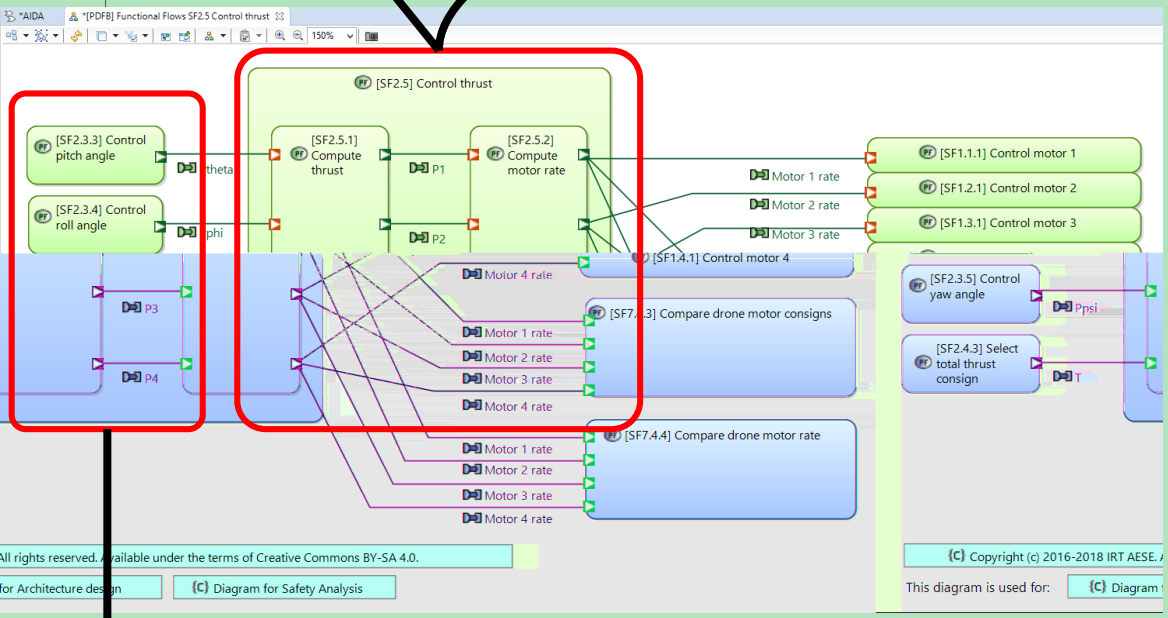
FRENCH INSTITUTES OF TECHNOLOGY

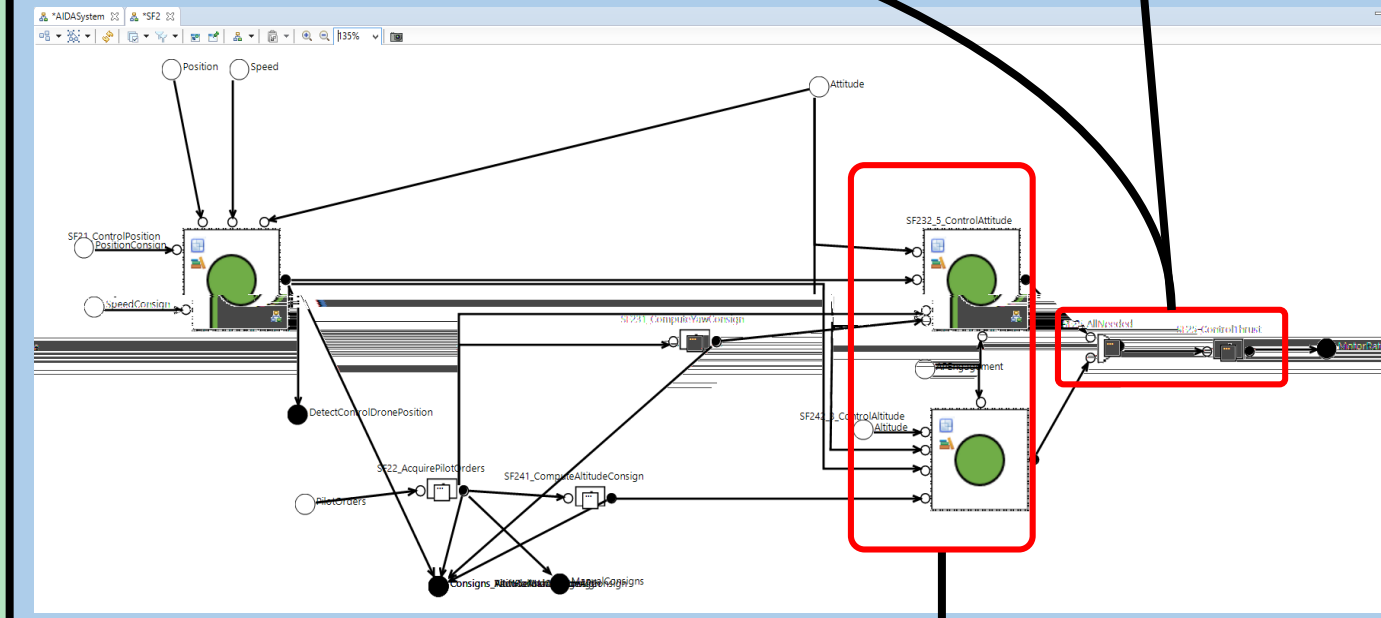
What occurs ... at abstraction level

SF2.5 and its context seen from SE

SF2.5 and its context seen from SA

Refinement and interface differ





Context differs

Representation differs

FRENCH INSTITUTES OF TECHNOLOGY

What occurs ... at abstraction level

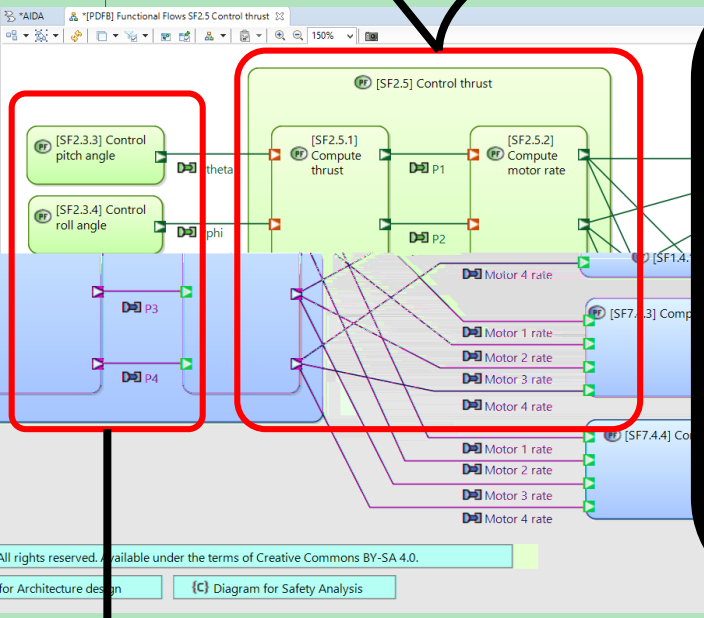
SF2.5 and its context seen from SE

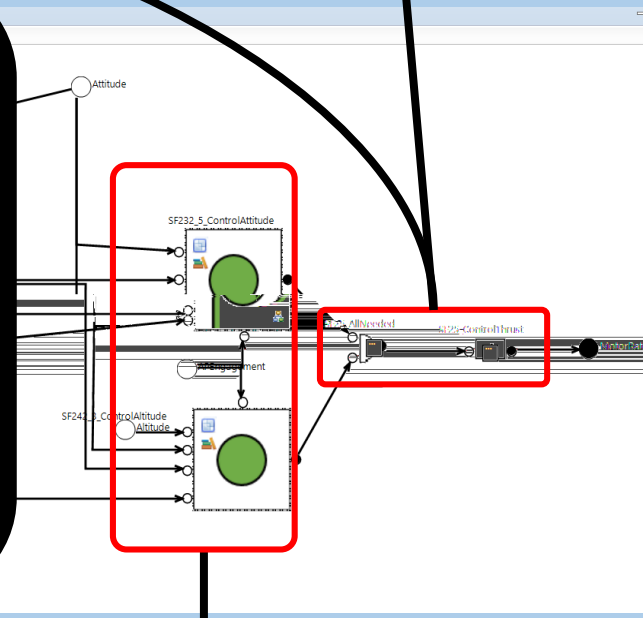
SF2.5 and its context seen from SA

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

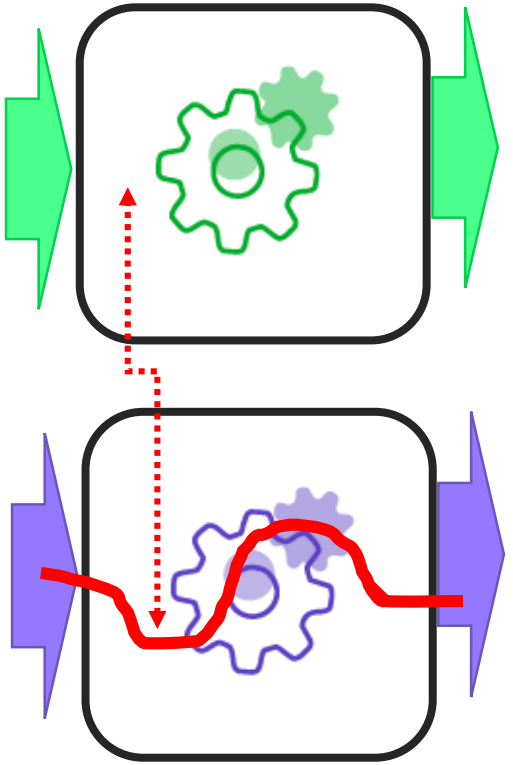
Representation differs

FRENCH INSTITUTES OF TECHNOLOGY

Method for consistency between MBSE and MBSA
-
Narrowing the situation

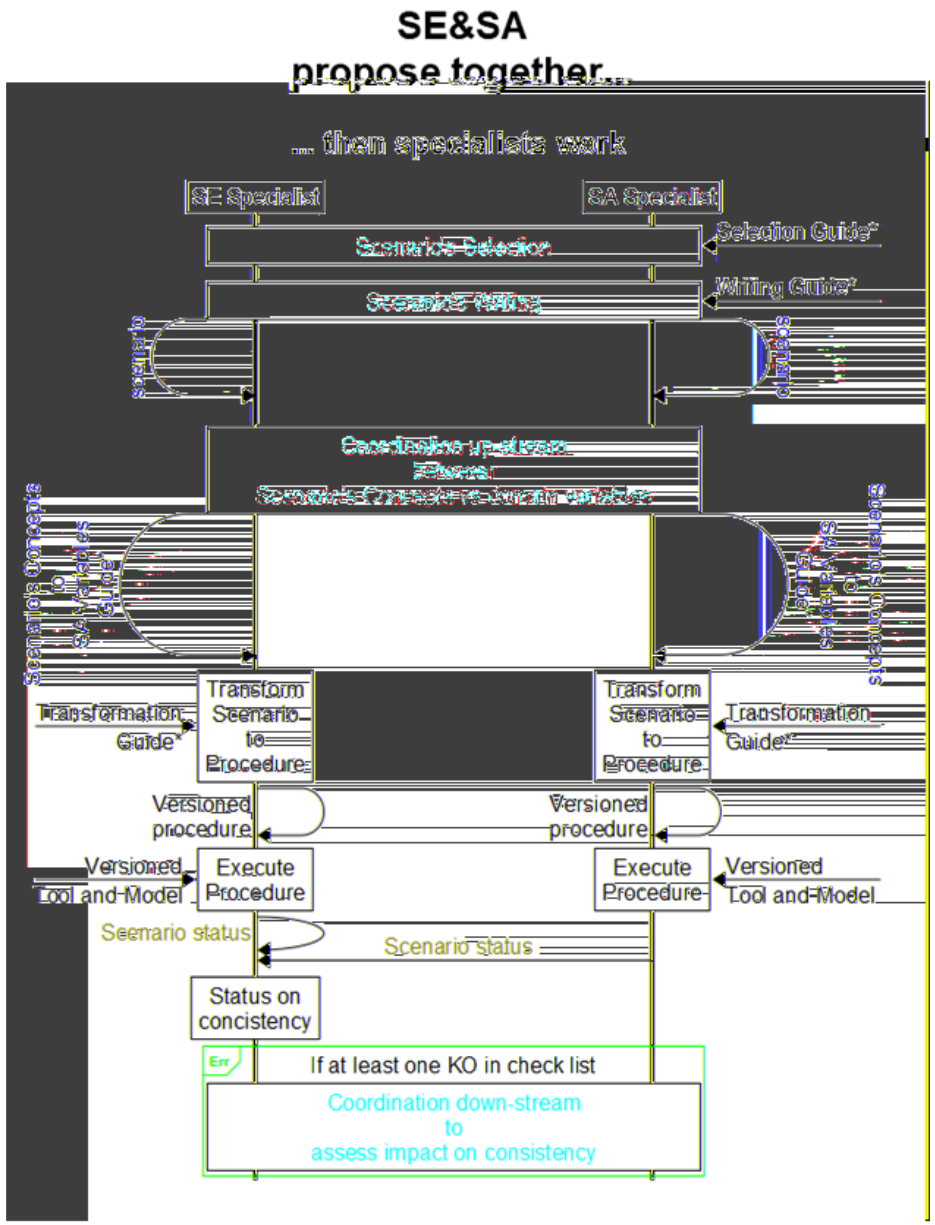
Proposed approach : high level view

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
-
M&T consequences

Method overview



Define End to End behavior for consistency review SE/SA

Identify mapping between « monitors » defined by SE / SA

Use the scenarios exécution results to check system compliance with SA requirements

PRODUCED ARTIFACTS

BCC Methodological guidelines

POC common artifacts

- **Variables coordination table SE/SA**
- **Verification procedures SE**
- **Verification procedures SA**
- **SIMFIANeo Model**

POC A

- **AIDA Capella Model extended with SE variables**

POC B

- **Cameo SYSML (19.0 SP4) model equivalent to AIDA V4.5**
  - **Functional Architecture model (structural)**
  - **Functional Behavioral models (Dynamic, Activity/StateCharts) for identified scenarios**
  - **SE Model execution report and videos**

Other result

- **Usage of SE/SA consistency review tool for consistency review between Capella and Cameo SYSML Models (different SE languages)**

POC Overview

FRENCH INSTITUTES OF TECHNOLOGY

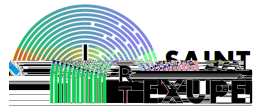
POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data



FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

SE/SA Variables coordination table

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

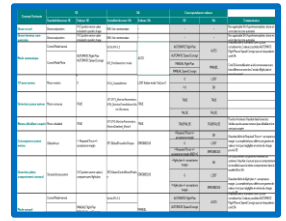
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



SE/SA Variables coordination table

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

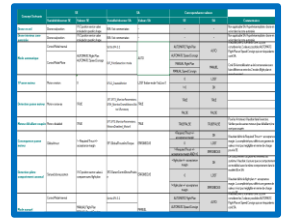
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



Tests Plan/ Scenarios

SE/SA Variables coordination table

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

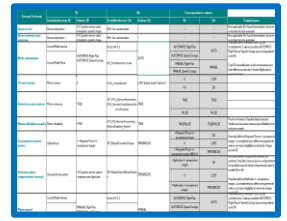
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



Common artifacts for both POCs

Tests Plan/ Scenarios

SE/SA Variables coordination table

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

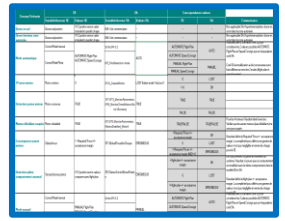
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models
SE descriptive / SA executable

Common artifacts for both POCs

Tests Plan/ Scenarios

SE/SA Variables coordination table

POC B

Method application on models
SE executable / SA executable

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

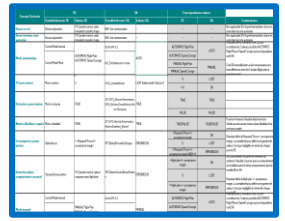
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models **SE descriptive / SA executable**

Common artifacts for both POCs

Tests Plan/ Scenarios

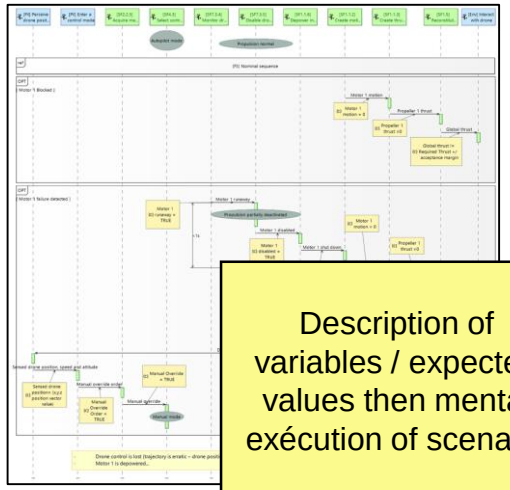
SE/SA Variables coordination table

POC B

Method application on models **SE executable / SA executable**

SE

Capella



Description of variables / expected values then mental exécution of scenario

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

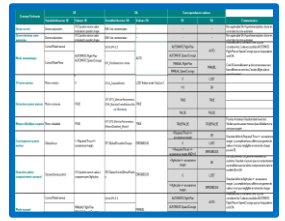
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models
SE descriptive / SA executable

Common artifacts for both POCs

Tests Plan/ Scenarios

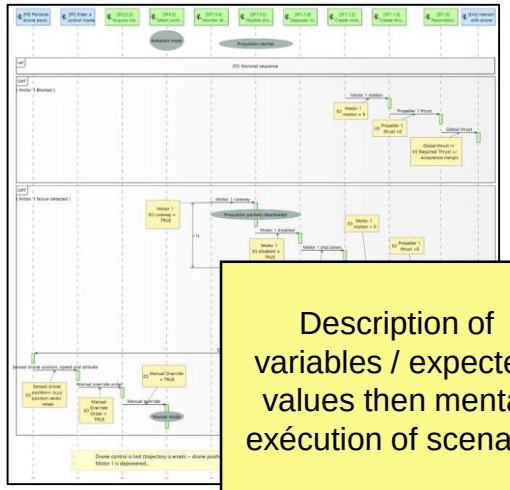
SE/SA Variables coordination table

POC B

Method application on models
SE executable / SA executable

SE

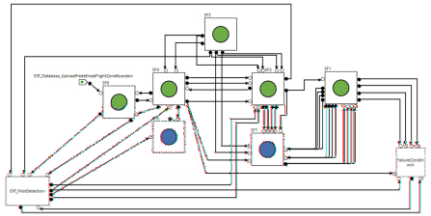
Capella



Description of variables / expected values then mental exécution of scenario

SA

SimfiaNeo



FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

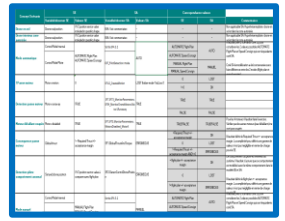
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models **SE descriptive / SA executable**

Common artifacts for both POCs

Tests Plan/ Scenarios

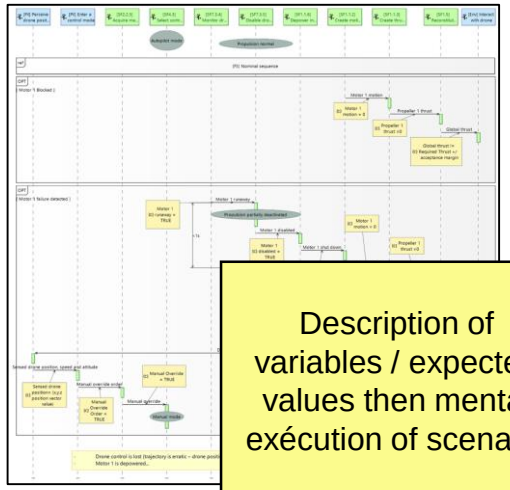
SE/SA Variables coordination table

POC B

Method application on models **SE executable / SA executable**

SE

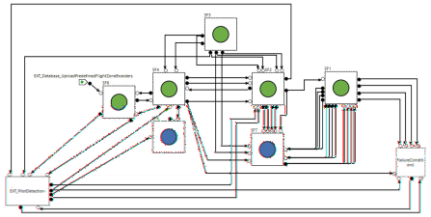
Capella



Description of variables / expected values then mental exécution of scenario

SA

SimfiaNeo



Compare with SA exécution and then analyse SE behavior on effects propagation

FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

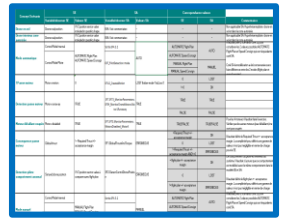
Inputs data

BCC Method

A: Scénario candidat
R: SE
R: SA

Activité coordination

A: Table de coordination
A: Scénario agréé



POC A

Method application on models
SE descriptive / SA executable

Common artifacts for both POCs

Tests Plan/ Scenarios

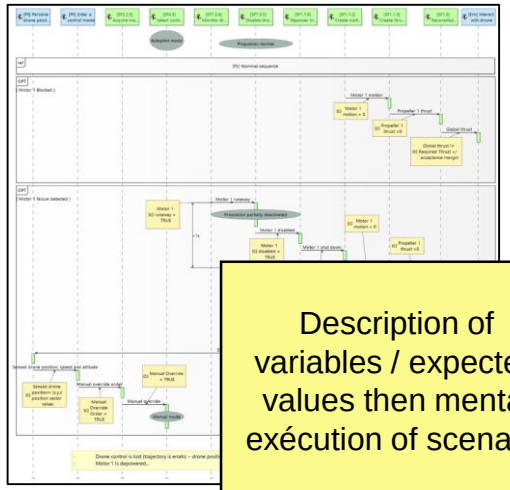
SE/SA Variables coordination table

POC B

Method application on models
SE executable / SA executable

SE

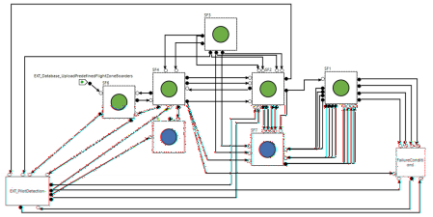
Capella



Description of variables / expected values then mental exécution of scenario

SA

SimfiaNeo

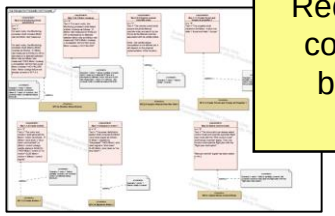


Compare with SA exécution and then analyse SE behavior on effects propagation

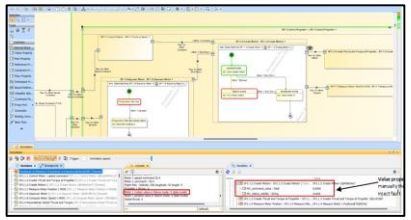
SE

SAMAREQ Profile

Cameo Systems Modeler



Requirements coverage by behavioral models



FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

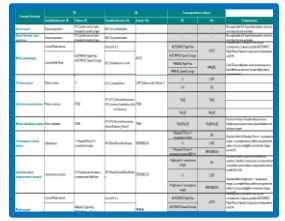
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models
SE descriptive / SA executable

Common artifacts for both POCs

Tests Plan/ Scenarios

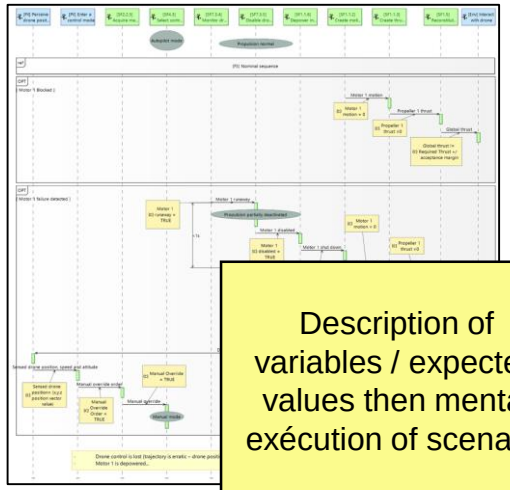
SE/SA Variables coordination table

POC B

Method application on models
SE executable / SA executable

SE

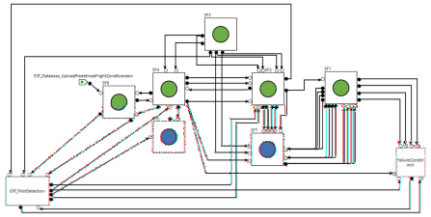
Capella



Description of variables / expected values then mental exécution of scenario

SA

SimfiaNeo

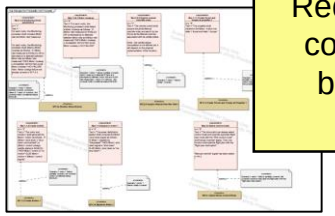


Compare with SA exécution and then analyse SE behavior on effects propagation

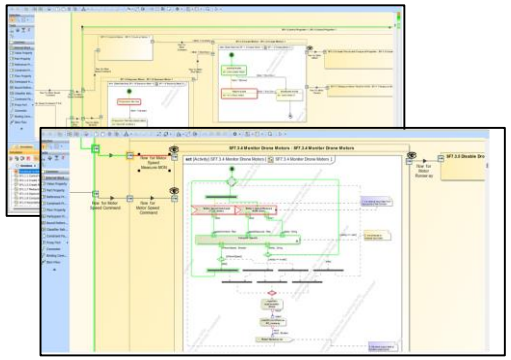
SE

SAMAREQ Profile

Cameo Systems Modeler



Requirements coverage by behavioral models



FRENCH INSTITUTES OF TECHNOLOGY

POC Overview

AIDA Case Study (SE model)

AIDA Case Study (SA model)

AIDA V4.5

Inputs data

BCC Method

A: Scénario candidat

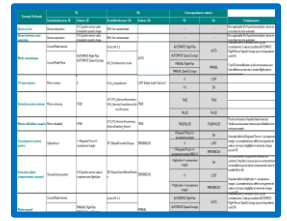
R: SE

R: SA

Activité coordination

A: Table de coordination

A: Scénario agréé



POC A

Method application on models
SE descriptive / SA executable

Common artifacts for both POCs

Tests Plan/ Scenarios

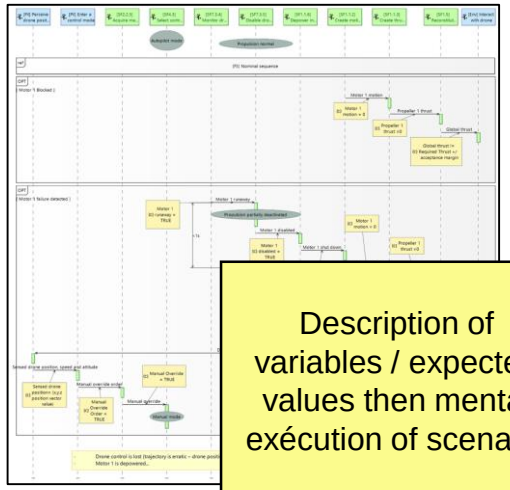
SE/SA Variables coordination table

POC B

Method application on models
SE executable / SA executable

SE

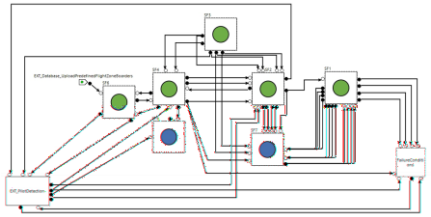
Capella



Description of variables / expected values then mental exécution of scenario

SA

SimfiaNeo

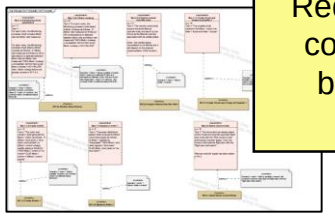


Compare with SA exécution and then analyse SE behavior on effects propagation

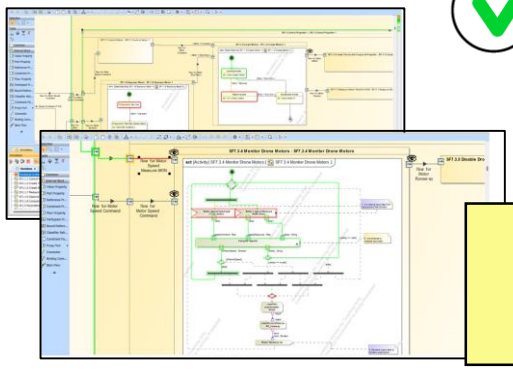
SE

SAMAREQ Profile

Cameo Systems Modeler



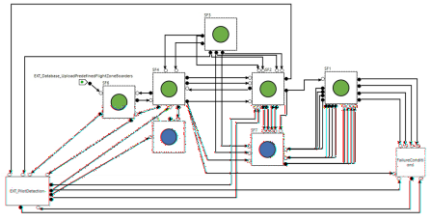
Requirements coverage by behavioral models



Compare models execution results between SE and SA

SA

SimfiaNeo



FRENCH INSTITUTES OF TECHNOLOGY

Method for consistency between MBSE and MBSA

-

Example

Procedure Report results and consistency – Example

Step of Procedure

Action to prepare the step
Or
Action triggering the event

Observations expected
During or ad end of step

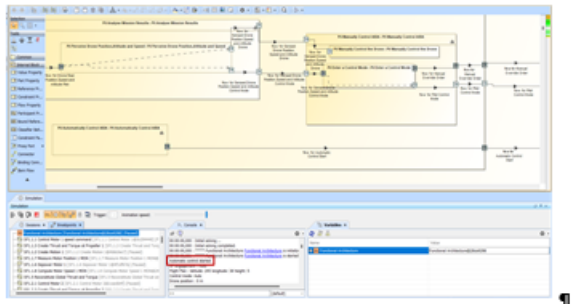
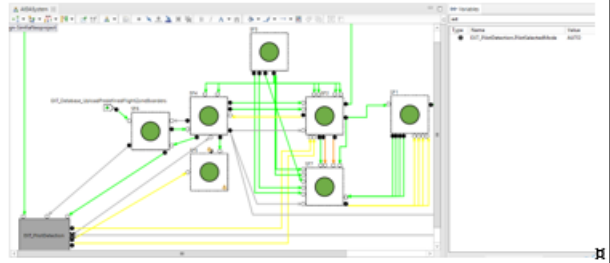
Proof of observation
(for audit / debug)

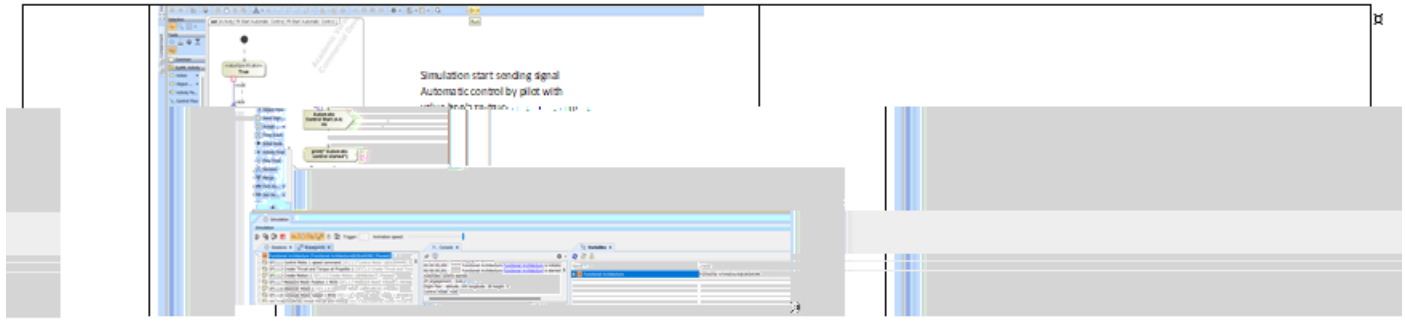
Another step of Procedure

SE activites

SA activites

a.→AIDA-XX.YYY-SA-001¶

¤	SE¤	SA¤
Action:¤	Open·MBSE·tool·and·start·standard·simulation·until·UAV·is·around·the·aircraft·in·the·allowed·area¤	Open·SimfiaNeo·1.3.2·and·load·model·AIDA·V4.4.3.·Launch·a·*Step·by·step·simulation*·and·check·initial·conditions·are·as·expected.¤
Expectation:¤	**Drone·real·position**·is·included·in·the·allowed·area¶ Drone·follows·the·flight·plan¶ **Control·Mode·=·AUTOMATIC**¤	**EXT_PilotDetection.PilotSelectedMode·=·AUTO**¤
Result:¤	¶  ¶	**EXT_PilotDetection.PilotSelectedMode·=·AUTO**¶ ¶  ¤



b.→AIDA-XX.YYY-SA-002¶

¤	SE¤	SA¤
Action¤	the·thrust·should·be·equal·to·required·thrust·so·that·we·can·verify·that·all·equipments·are·behaving·normally.¤	Check·the·thrust·is·equal·to·required·thrust·so·that·we·can·verify·that·all·equipments·are·behaving·normally.¤
Expectation:¤	Global·Thrust·=·Required·thrust·+/-·acceptance·margin¤	SFL.GlobalThrustAndTorque·=·OK¤
Result:¤	¶	SFL.GlobalThrustAndTorque·=·OK¶

FRENCH INSTITUTES OF TECHNOLOGY

Coordination Table

Scenario Concept	SE		SA		Value's domain correspondance		Commentaires
	Variable/observer SE	SE Values	Variable/observer SA	SA Values	SE	SA	
Drone in fligh	Drone real position	XYZ position vector value included in specific shape	N/A: Voir commentaires	-	-	-	Non applicable SA. Hypothèse implicite: drone en vol et dans la zone autorisée
Drone insied authorized area	Drone real position	XYZ position vector value included in specific shape	N/A: Voir commentaires	-	-	-	Non applicable SA. Hypothèse implicite: drone en vol et dans la zone autorisée
Automatic Mode	Control Mode Internal	AUTOMATIC Flight Plan AUTOMATIC Speed Consign	Sortie SF4.3.2	AUTO	AUTOMATIC Flight Plan AUTOMATIC Speed Consign	AUTO	Il faudrait jouer 2 scénarios coté SE pour considérer les 2 valeurs possibles AUTOMATIC Flight Plan et Speed Consign qui sont équivalents coté SA.
	Control Mode Pilote		EXT_PilotDetection.PilotSelectedMode		MANUAL	MANUAL	Coté SA la momdélisation a été conservative sans faire différence entre les 2 modes (flight plan et speed consign)
Loss of motor	Motor x motion	0	SF1i2_CreateMotion	LOST (failure mode "fail_loss")	0	LOST	
					!=0	OK / ERRONEOUS	
Motor loss detection	Motor x runaway	TRUE	SF7.SF3_MonitorParameters.SF734_MonitorDroneMotors.Motro1Runaway	TRUE	TRUE	TRUE	
					FALSE	FALSE	

Assuming that SE and SA may focus on different aspects but try to establish mapping between 2 domains.

SE&SA notes on mapping done

Var domaine (related to SA model implementation)

Var name used in procedure (related to SA model implementation)

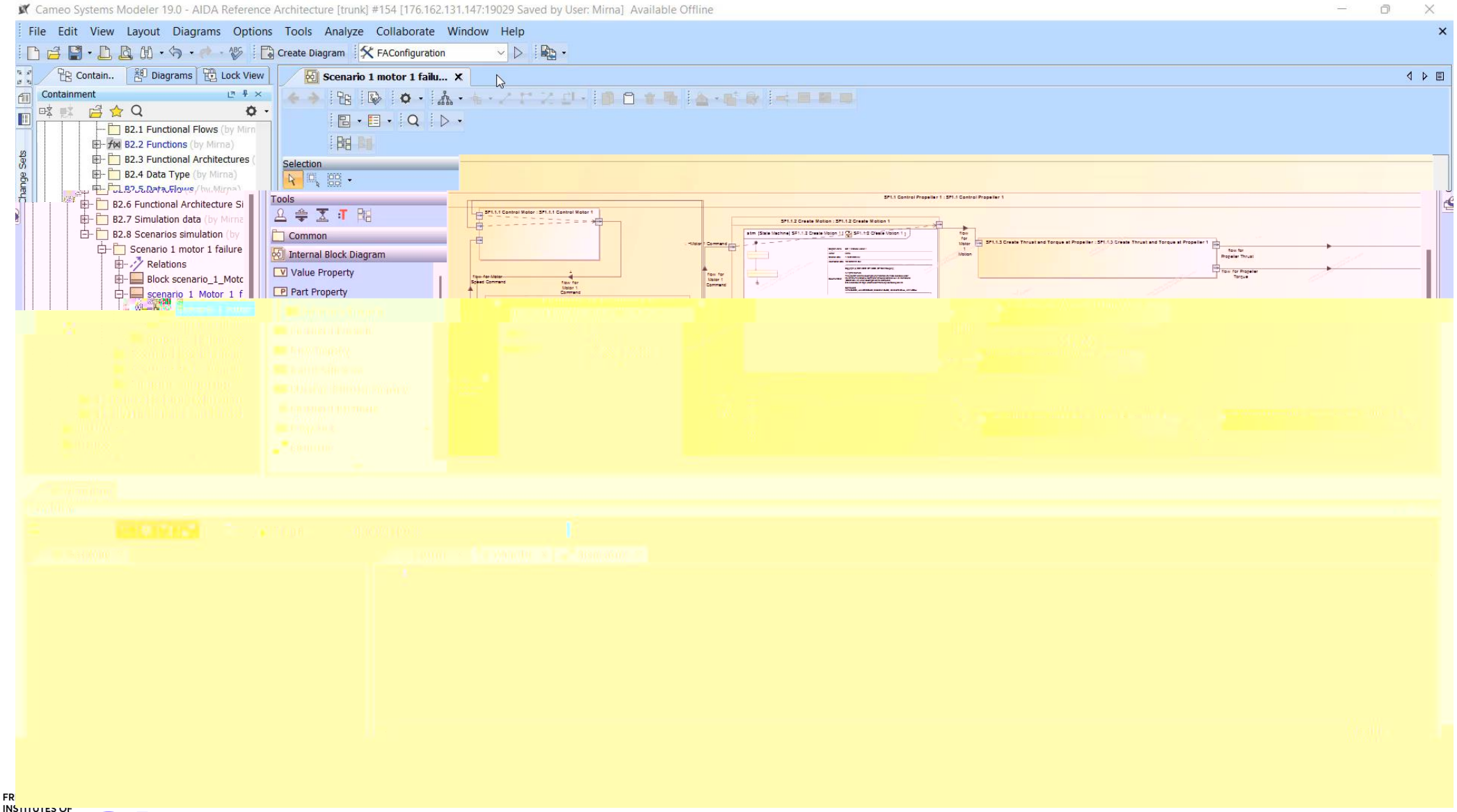
Var domaine (related to SE model implementation)

Var name used in procedure (related to SE model implementation)

Var name used in scenario (agnostic from models implementation)

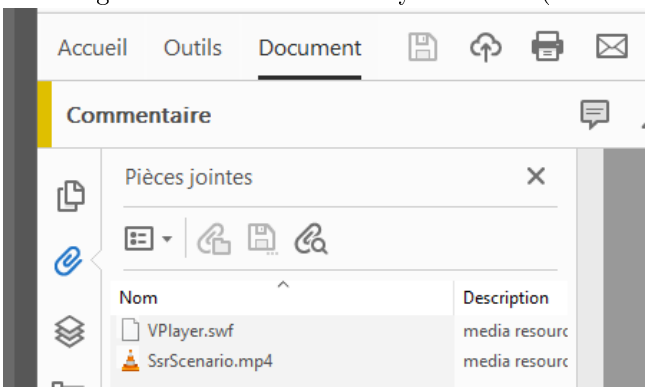
Executions

SE : Video



SA : no video (similar to SE but with SA simulation QoS tools)

Get Video from PDF using attachement services of your reader (here above with Acrobat):



Method for consistency between MBSE and MBSA
-
Returns of experience

Retrun of Expérience

Simplify the global behavior consistency review between SE and SA

Behavioral exécution (End To End) based on identified scenarios

Failure cases defined by SA may be executed on SE models to visualize effects and consequences in defined system execution

SE Behavioral modelling with exécution has to focus on the appropriate fidelity level for simulation models.

FRENCH INSTITUTES OF TECHNOLOGY

METHOD Limits

POCs have limited the study on functional architecture level

Behavioral Consistency may be difficult/complex if SE/SA models are very different

Method consider some differences between the 2 models

SE/SA représentations are different viewpoints even if linked to the same system

Using the SSR method in previous step ease the building of variables coordination table

Executable Behavior Modelling effort to adjust according to the need

Considering Models fidelity to appropriate need (ROI) to represent effects propagation in the system and identify effects of safety mechanisms defined in the system (redundancies, monitors, …)

Identify relevant scenarios is a key activity for SE/SA coordination activity

The method is to measure efficiency/consistency of defined system

To build SA model differently from the system definition may ease the consistency review work

The scalling effect when targeteing better precision

It rely on underlying tool chosen to implement the method (i.e. simulation tools/frameworks may be more accurate than coarse grain model)

FRENCH INSTITUTES OF TECHNOLOGY