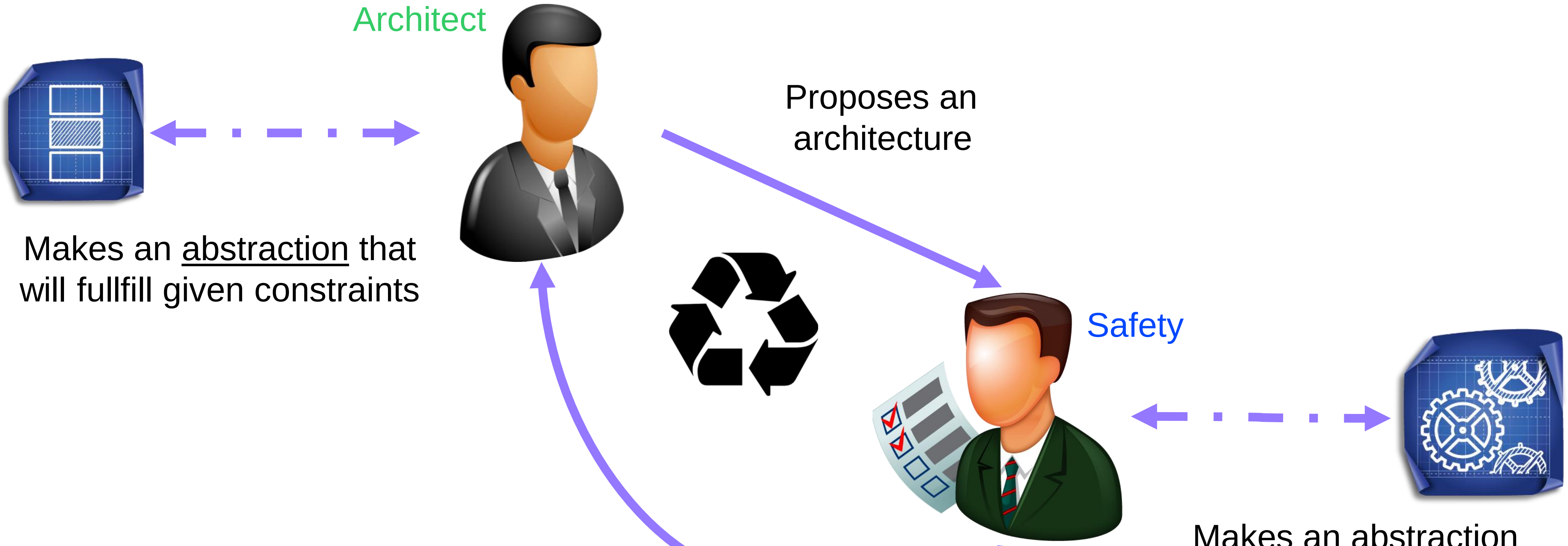
Référence IRT Saint Exupéry: NT-S085L02T00-041
Référence IRT System X : ISX-S2C-DOC-459
Version : V0
Date : 2023-01-19

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*

System & Safety Continuity

- Method for consistency between MBSE and MBSA –

- **Behaviroal Scope Review (BSR) -**



Architect

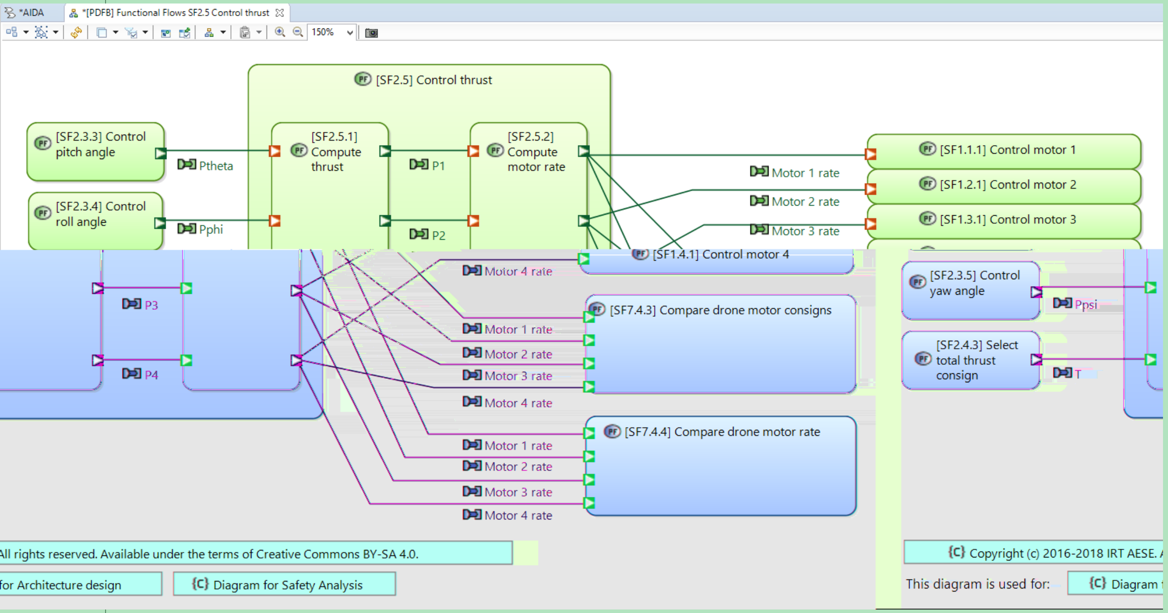
Makes an abstraction that will fullfill given constraints

Proposes an architecture

Safety

Makes an abstraction to critic the proposed architecture (regarding its Safety objectives)

Gives safety constraints/recommandations regarding the proposed architecture


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
Ptheta
Pphi
P1
P2
P3
P4
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
[SF7.4.3] Compare drone motor consigns
[SF7.4.4] Compare drone motor rate
[SF2.3.5] Control yaw angle
[SF2.4.3] Select total thrust consign
Ppsi
T

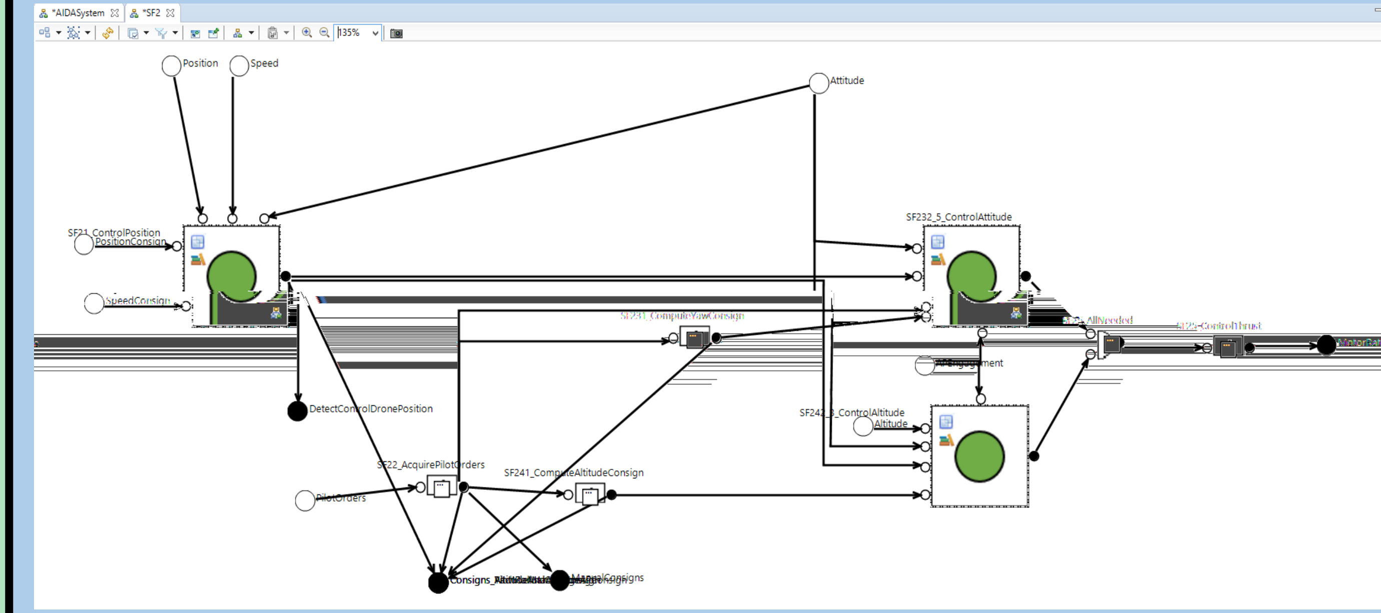
ll rights reserved. Available under the terms of Creative Commons BY-SA 4.0.

{C} Copyright (c) 2016-2018 IRT AESE. /

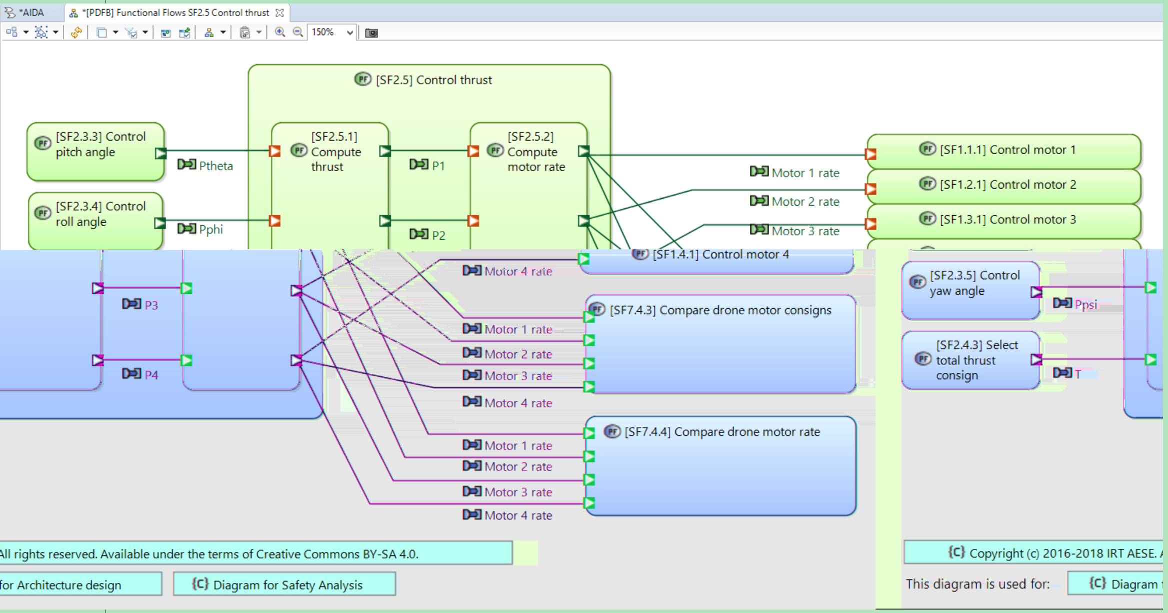
or Architecture design

{C} Diagram for Safety Analysis

This diagram is used for: {C} Diagram



FRENCH
INSTITUTES OF
TECHNOLOGY


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
Ptheta
Pphi
P1
P2
P3
P4
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
[SF7.4.3] Compare drone motor consigns
[SF7.4.4] Compare drone motor rate
[SF2.3.5] Control yaw angle
[SF2.4.3] Select total thrust consign
Ppsi
T

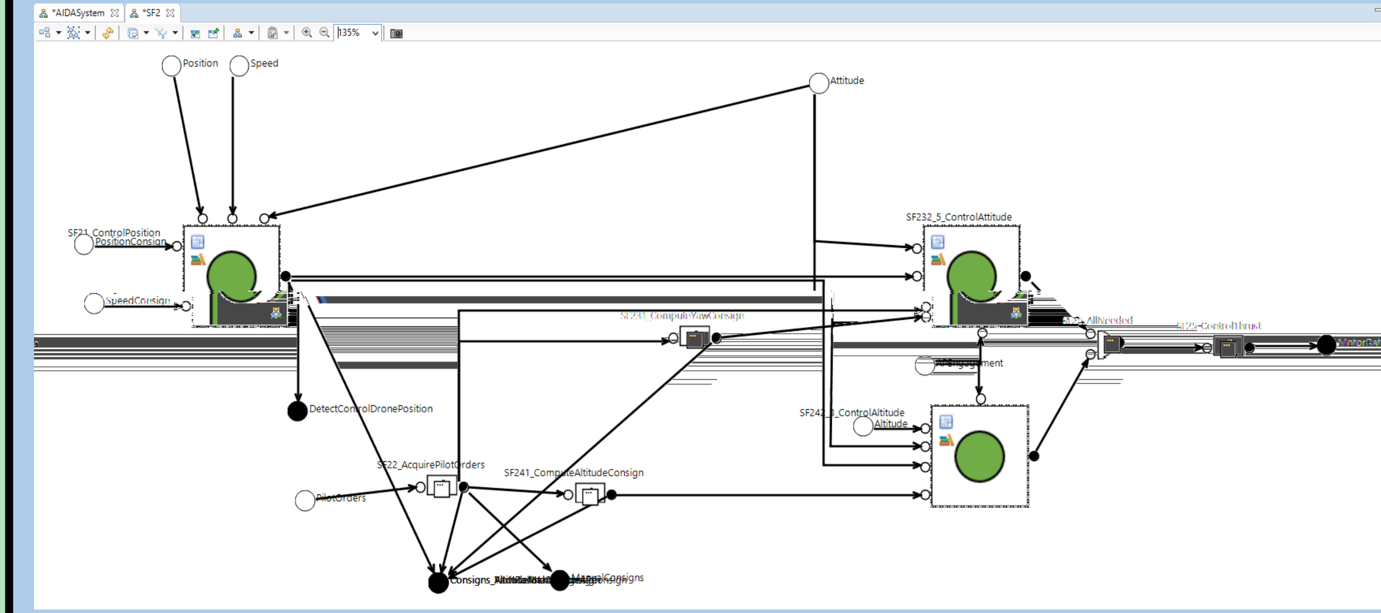
All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.

for Architecture design

{C} Diagram for Safety Analysis

{C} Copyright (c) 2016-2018 IRT AESE.

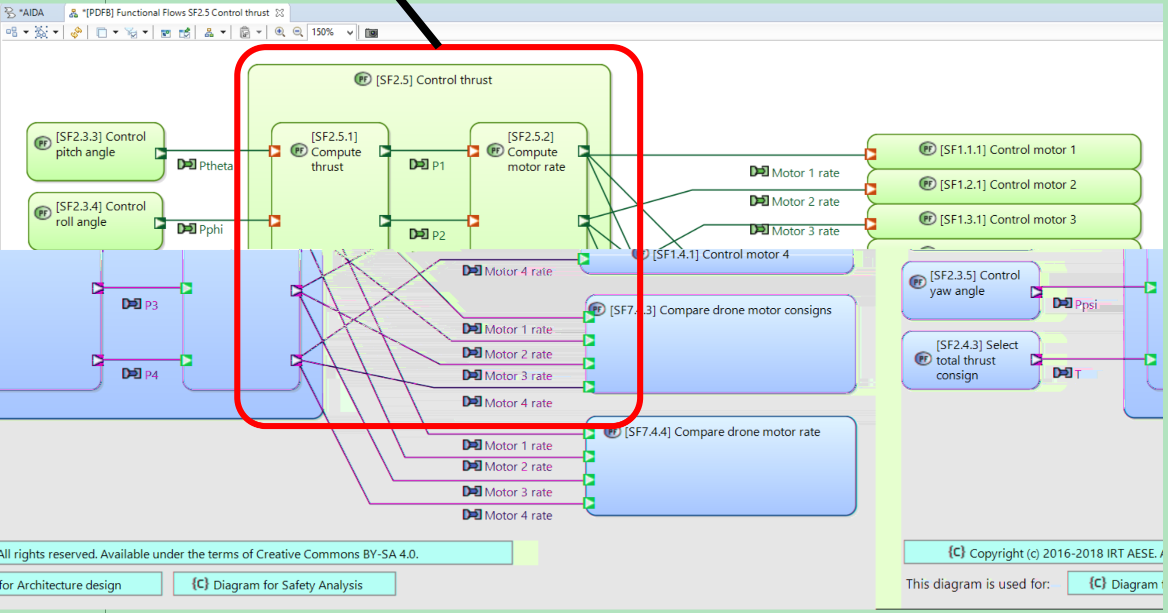
This diagram is used for: {C} Diagram



Representation differs

FRENCH
INSTITUTES OF
TECHNOLOGY

SF2.5 and its context seen from SE


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
Ptheta
Pphi
[SF2.5.1] Compute thrust
P1
P2
[SF2.5.2] Compute motor rate
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
P3
P4
[SF7.4.3] Compare drone motor consigns
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF7.4.4] Compare drone motor rate
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF2.3.5] Control yaw angle
Ppsi
[SF2.4.3] Select total thrust consign
T

All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.

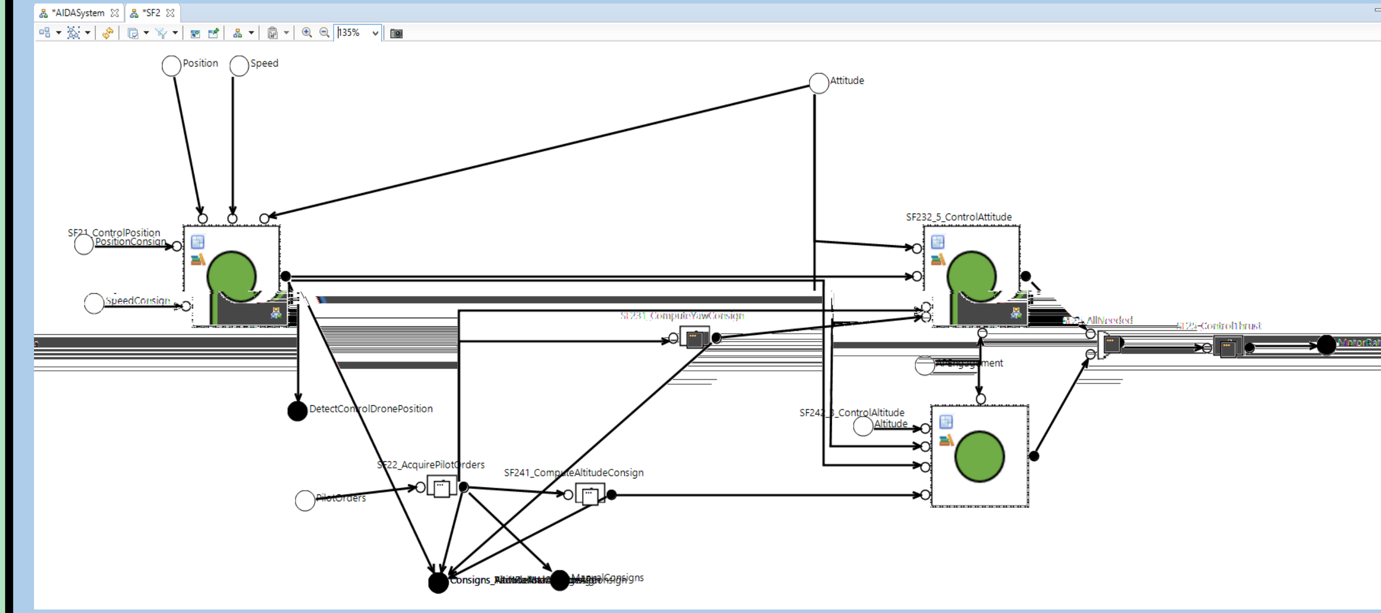
{C} Copyright (c) 2016-2018 IRT AESE.

for Architecture design

{C} Diagram for Safety Analysis

This diagram is used for:

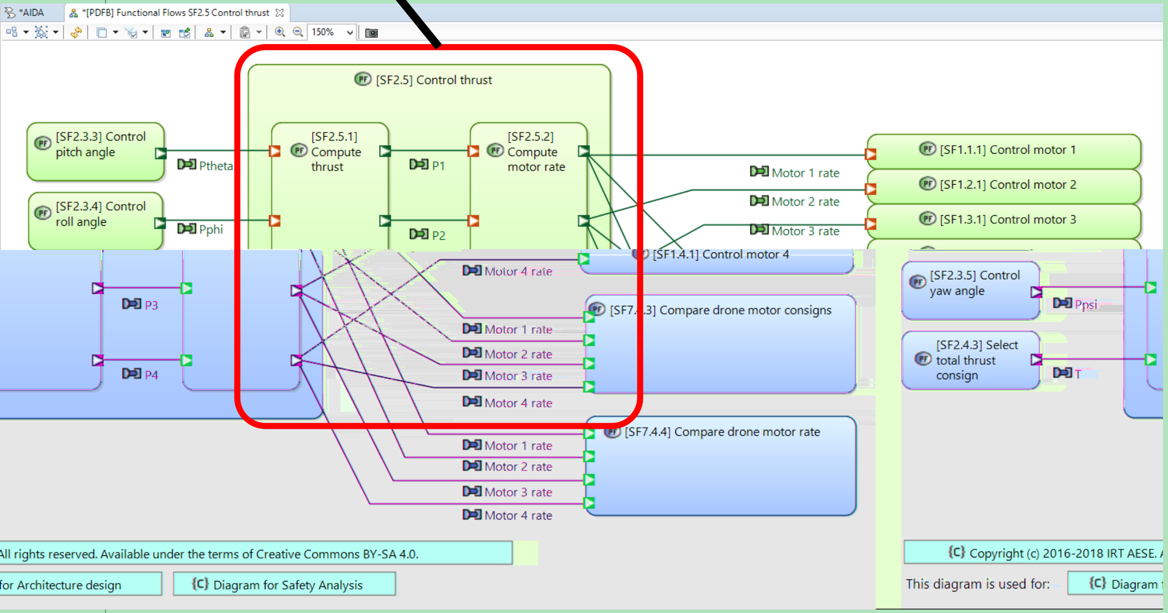
{C} Diagram

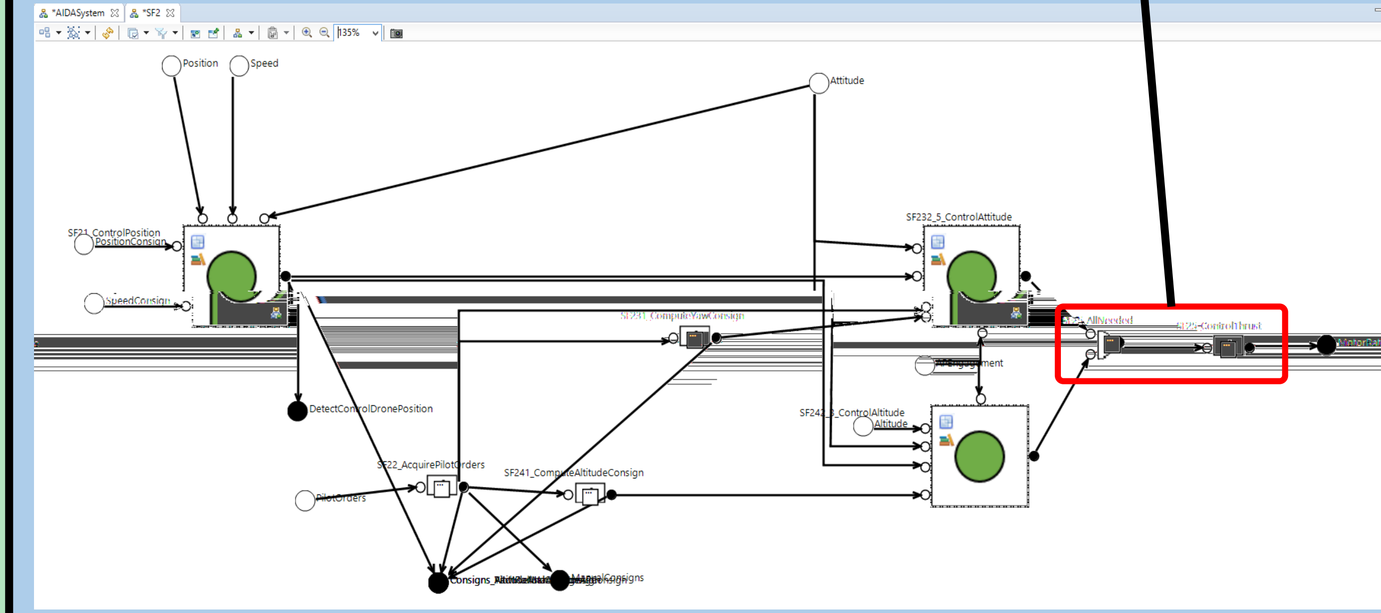


Representation differs

SF2.5 and its context seen from SE

SF2.5 and its context seen from SA


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
Ptheta
Pphi
P1
P2
P3
P4
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
[SF7.4.3] Compare drone motor consigns
[SF7.4.4] Compare drone motor rate
[SF2.3.5] Control yaw angle
[SF2.4.3] Select total thrust consign
Ppsi
T
All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.
{C} Copyright (c) 2016-2018 IRT AESE.
for Architecture design
{C} Diagram for Safety Analysis
This diagram is used for:
{C} Diagram



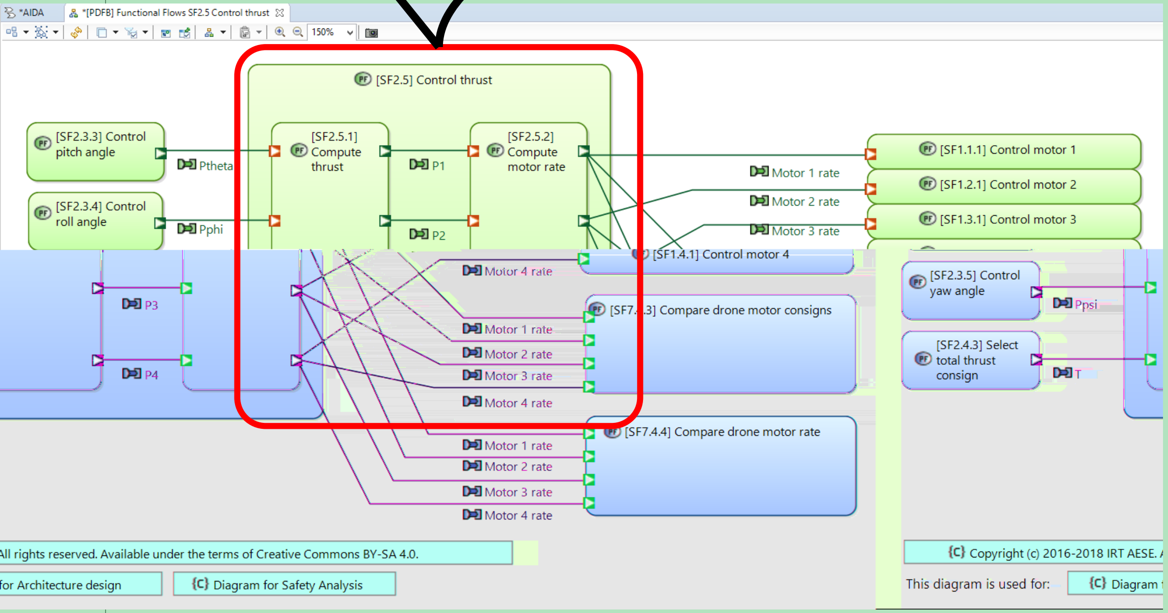
Representation differs

FRENCH INSTITUTES OF TECHNOLOGY

SF2.5 and its context
seen from SE

SF2.5 and its context
seen from SA

Refinement and interface differ


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
Ptheta
Pphi
P1
P2
P3
P4
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
[SF7.4.3] Compare drone motor consigns
[SF7.4.4] Compare drone motor rate
[SF2.3.5] Control yaw angle
[SF2.4.3] Select total thrust consign
Ppsi
T

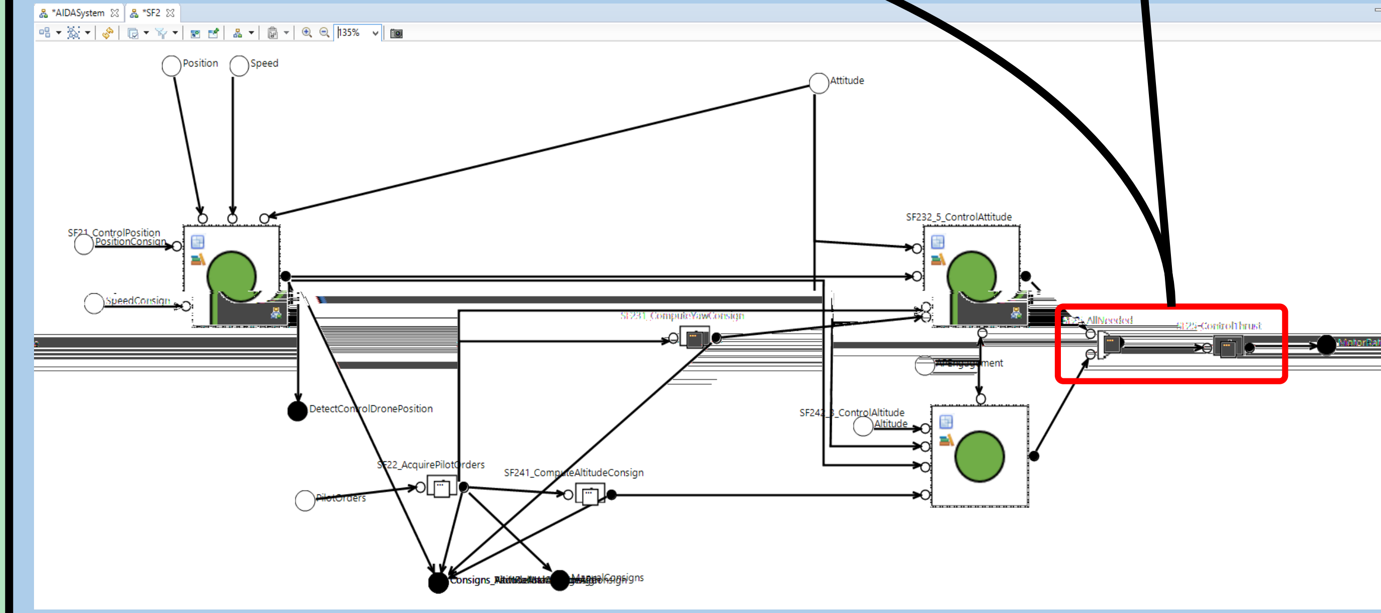
All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.

for Architecture design

{C} Diagram for Safety Analysis

{C} Copyright (c) 2016-2018 IRT AESE.

This diagram is used for: {C} Diagram

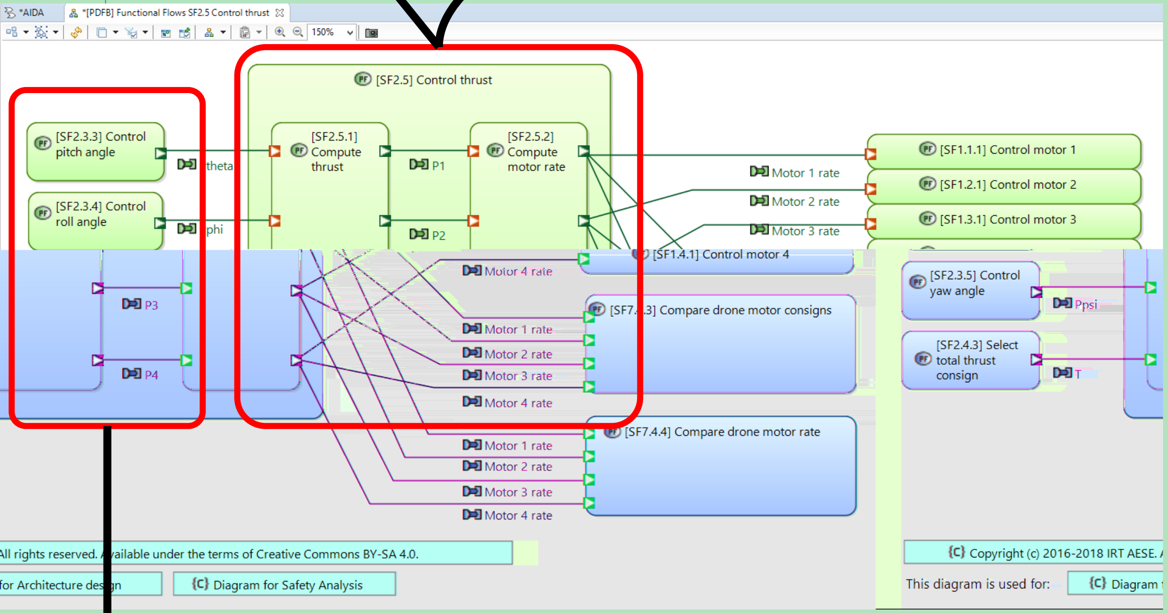


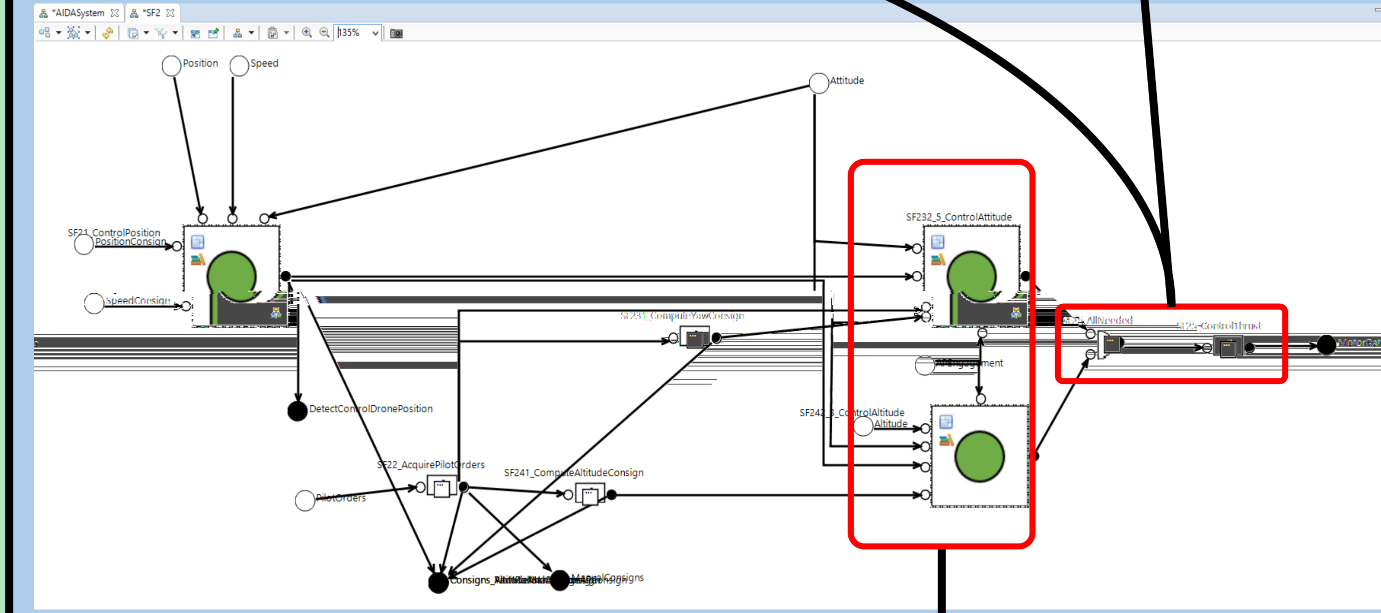
Representation differs

SF2.5 and its context
seen from SE

SF2.5 and its context
seen from SA

Refinement and interface differ


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
theta
phi
P1
P2
P3
P4
[SF1.1.1] Control motor 1
[SF1.2.1] Control motor 2
[SF1.3.1] Control motor 3
[SF1.4.1] Control motor 4
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
[SF7.4.3] Compare drone motor consigns
[SF7.4.4] Compare drone motor rate
[SF2.3.5] Control yaw angle
[SF2.4.3] Select total thrust consign
Ppsi
T
All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.
for Architecture design
{C} Diagram for Safety Analysis
{C} Copyright (c) 2016-2018 IRT AESE.
This diagram is used for:
{C} Diagram



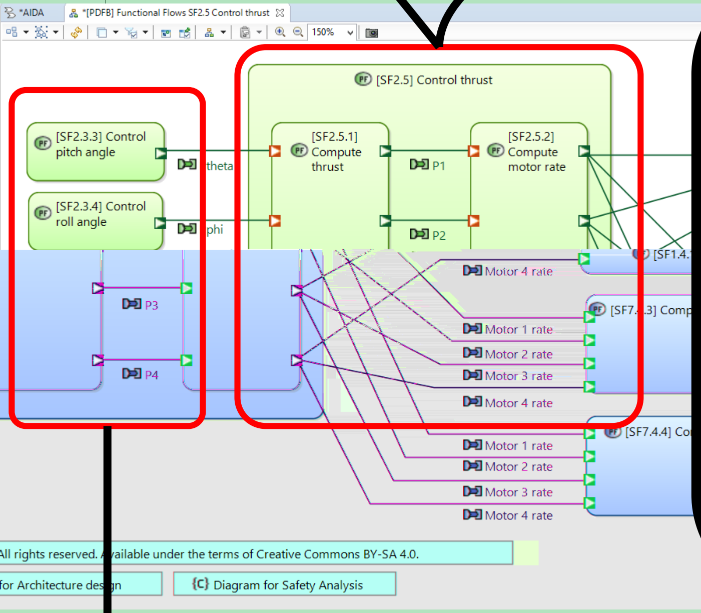
Context differs

Representation differs

SF2.5 and its context seen from SE

SF2.5 and its context seen from SA

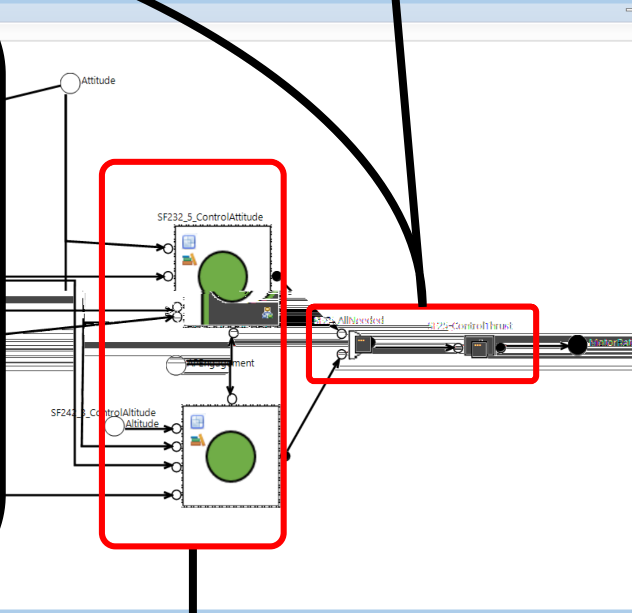
Refinement and interface differ


*AIDA
*[PDFB] Functional Flows SF2.5 Control thrust
150%
[SF2.5] Control thrust
[SF2.3.3] Control pitch angle
[SF2.3.4] Control roll angle
[SF2.5.1] Compute thrust
[SF2.5.2] Compute motor rate
theta
phi
P1
P2
P3
P4
[SF1.4.
[SF7.4.3] Comp
[SF7.4.4] Co
Motor 1 rate
Motor 2 rate
Motor 3 rate
Motor 4 rate
All rights reserved. Available under the terms of Creative Commons BY-SA 4.0.
for Architecture design
[C] Diagram for Safety Analysis

If there is any SA safety constraint/recomandation for this function

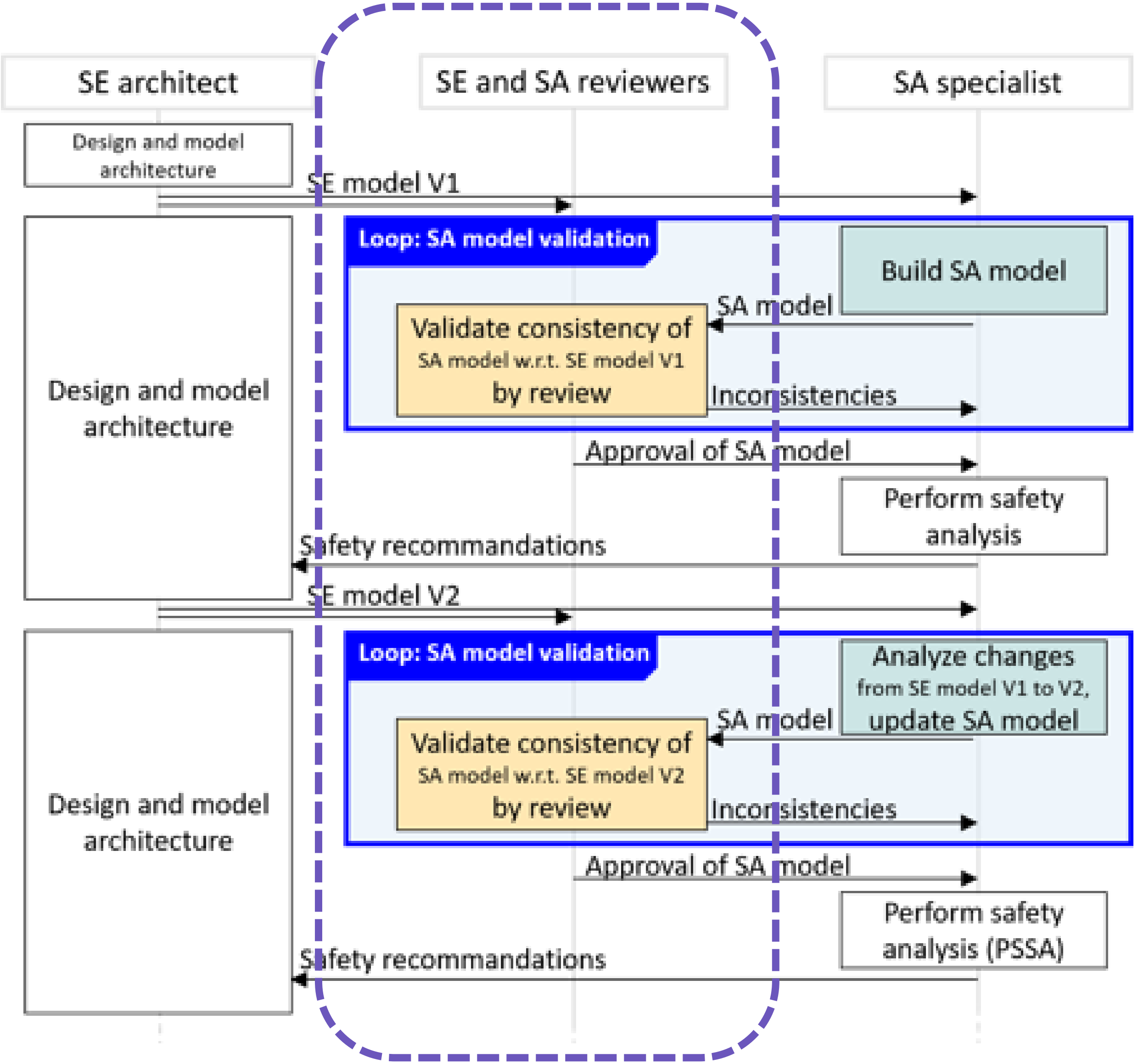
…

How it could be right without mastering differences between abstractions ?

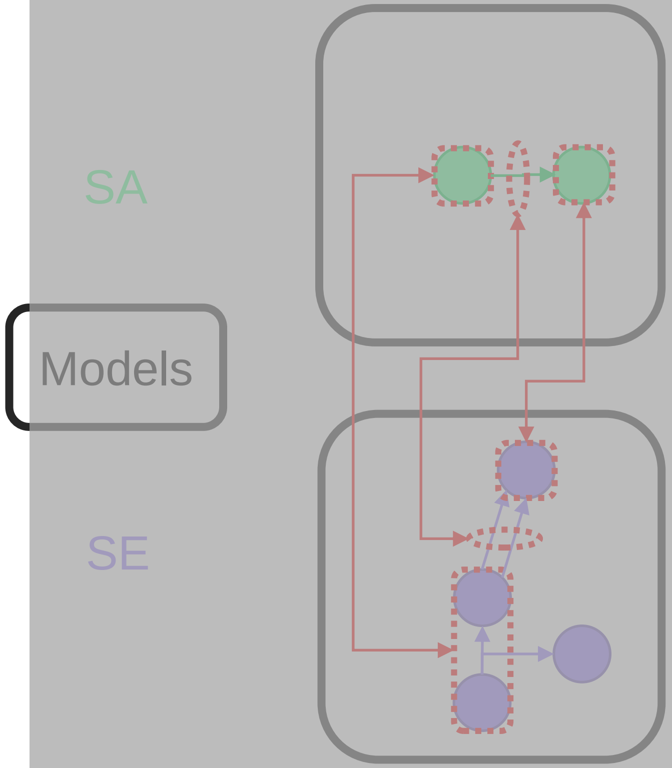


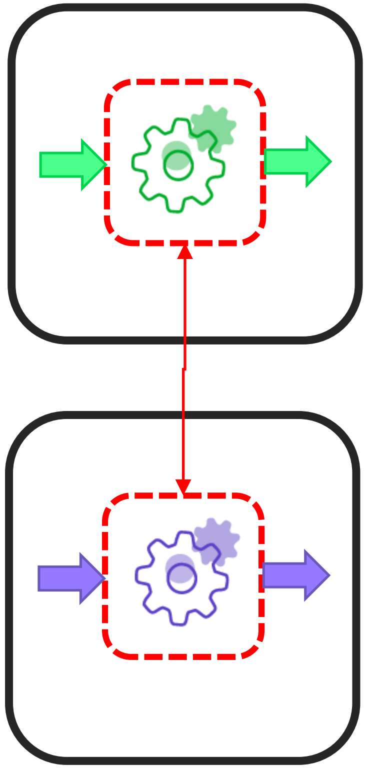
Context differs

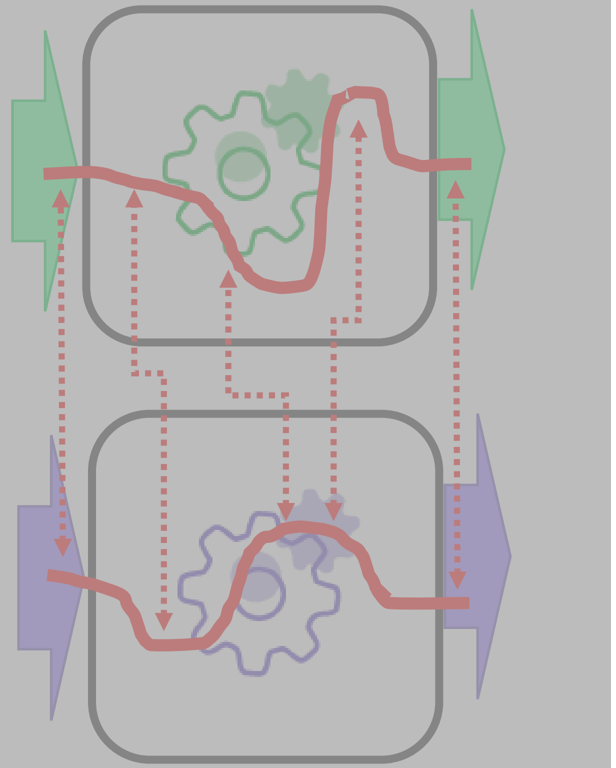
Representation differs


SE architect
SE and SA reviewers
SA specialist
Design and model architecture
SE model V1
Loop: SA model validation
Build SA model
SA model
Validate consistency of SA model w.r.t. SE model V1 by review
Inconsistencies
Design and model architecture
Approval of SA model
Perform safety analysis
Safety recommandations
SE model V2
Loop: SA model validation
Analyze changes from SE model V1 to V2, update SA model
SA model
Validate consistency of SA model w.r.t. SE model V2 by review
Inconsistencies
Design and model architecture
Approval of SA model
Perform safety analysis (PSSA)
Safety recommandations

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

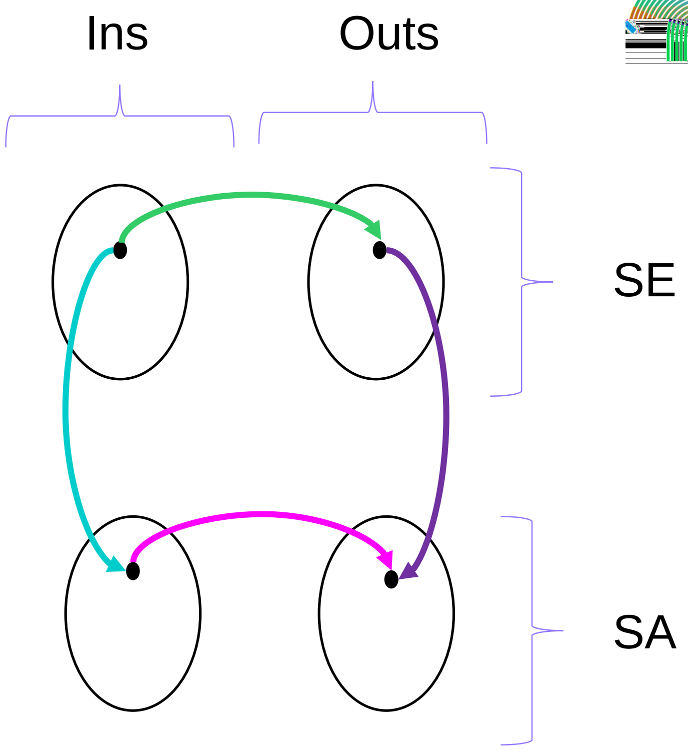




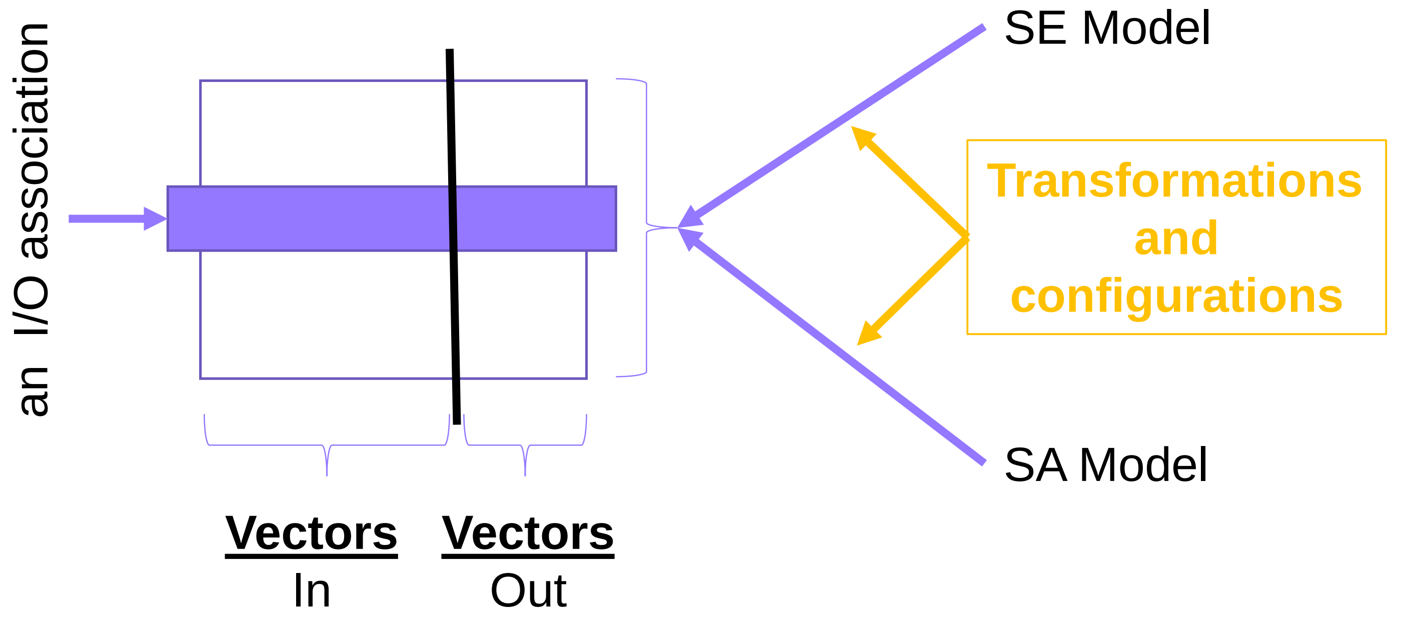


- On reputed same perimeter (Scope)
    - A SE static specification is transformed into a table that links ins and associated outs →
    - A SA behavior is transformed into a table that links ins and associated outs →
- A transformation shall be defined to process
    - SE(ins) into SA(Ins) →
    - SE(Outs)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

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



- 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.



an I/O association

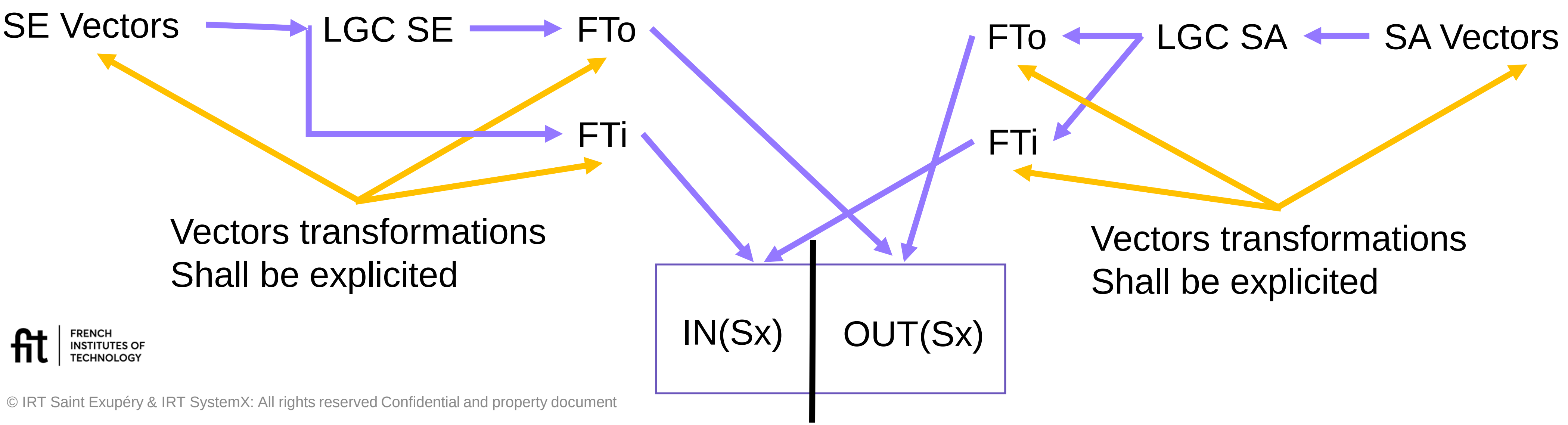
SE Model

Transformations and configurations

SA Model

Vectors In

Vectors Out



SE Vectors

LGC SE

FTo

FTi

FTo

LGC SA

SA Vectors

FTi

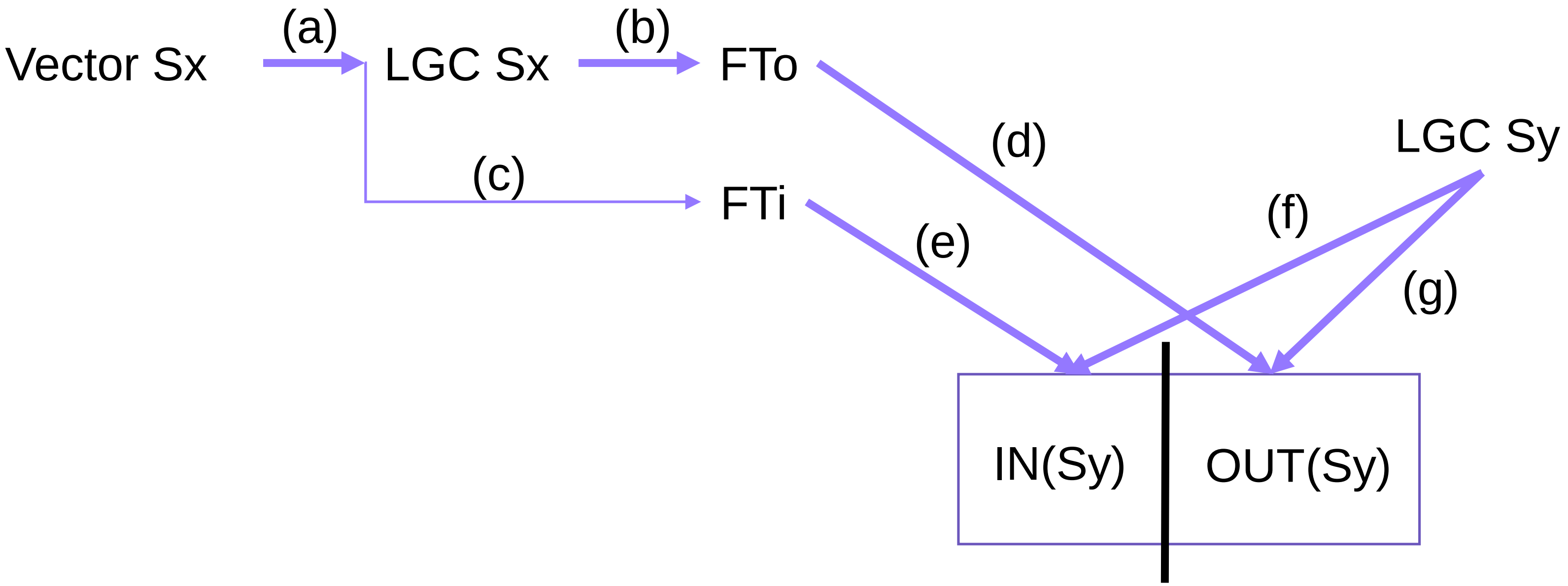
Vectors transformations
Shall be explicited

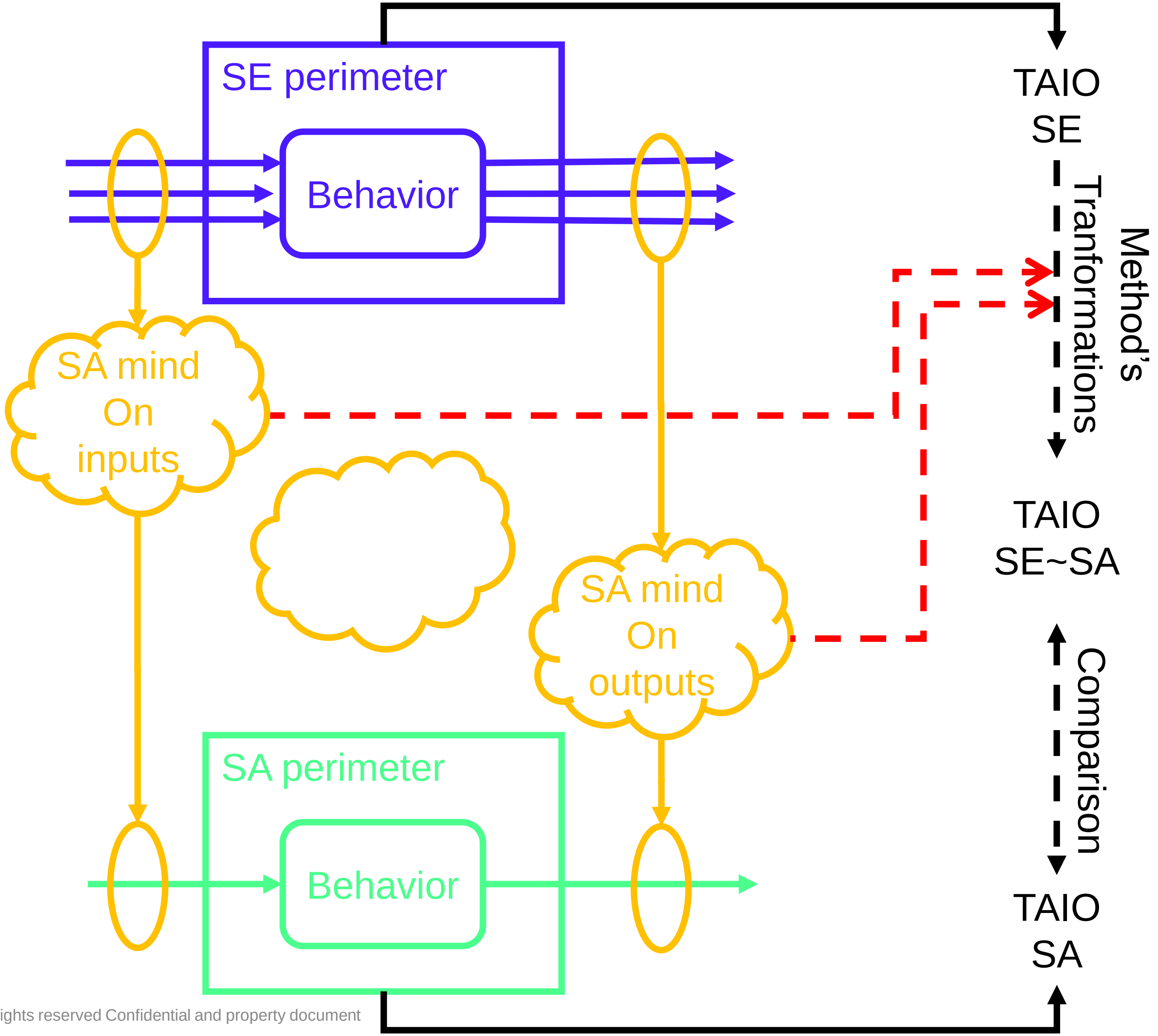
IN(Sx)

OUT(Sx)

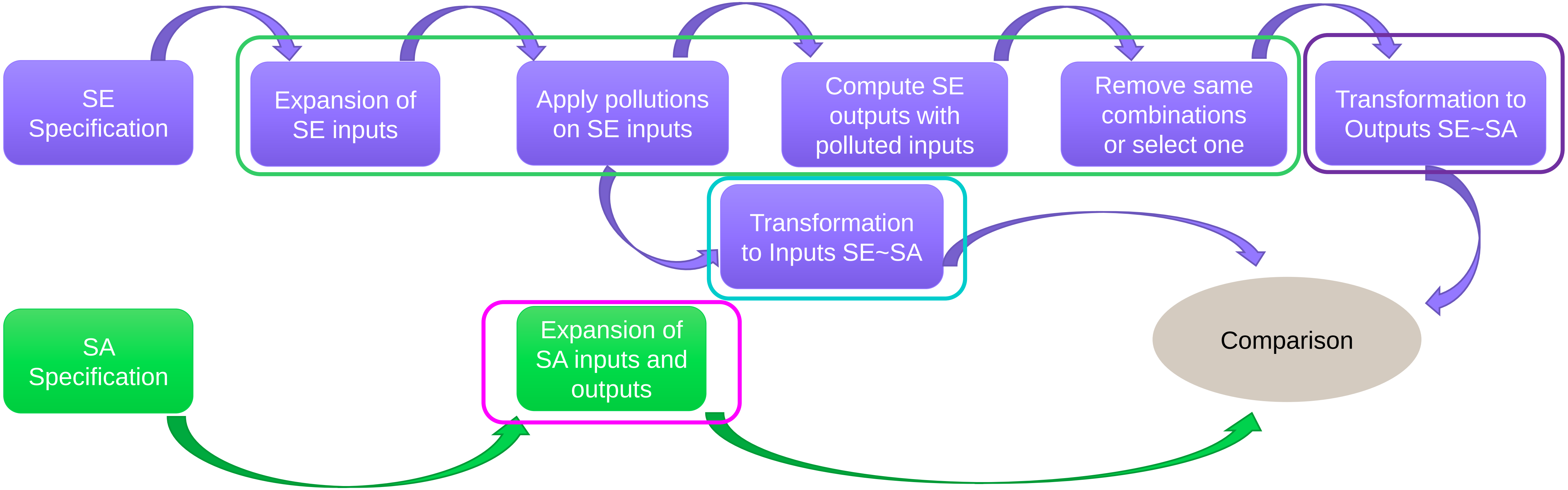
Vectors transformations
Shall be explicited

In our case SA is used as the reference of comparison :
So no transformation is done on its side




SE perimeter
Behavior
SA mind
On
inputs
SA mind
On
outputs
SA perimeter
Behavior
TAIO
SE
Method's
Tranformations
TAIO
SE~SA
Comparison
TAIO
SA

SA mind


SE Specification
Expansion of SE inputs
Apply pollutions on SE inputs
Compute SE outputs with polluted inputs
Remove same combinations or select one
Transformation to Outputs SE~SA
Transformation to Inputs SE~SA
SA Specification
Expansion of SA inputs and outputs
Comparison

We have to exercize the implemented behavior and transformation, this requires tooling that runs

A selected set of IN(SE) to get OUT(SE)

=> so SE specification shall be sufficiently formal ro be run

Selection can be exhautive is SE domain and cardinality allow it

Selection can be partial (if too much combinations)

Transform the IN(SE) into IN(SA) and OUT(SE) into OUT(SA)

=> the transformation shall be parametrized regarding the needs

Run the set of IN(SA) to get the OUT(SA)

=>so use the formalism of ALTARICA to get data

We have to make equivalent of FUZZY software algorithm on IN(SE)

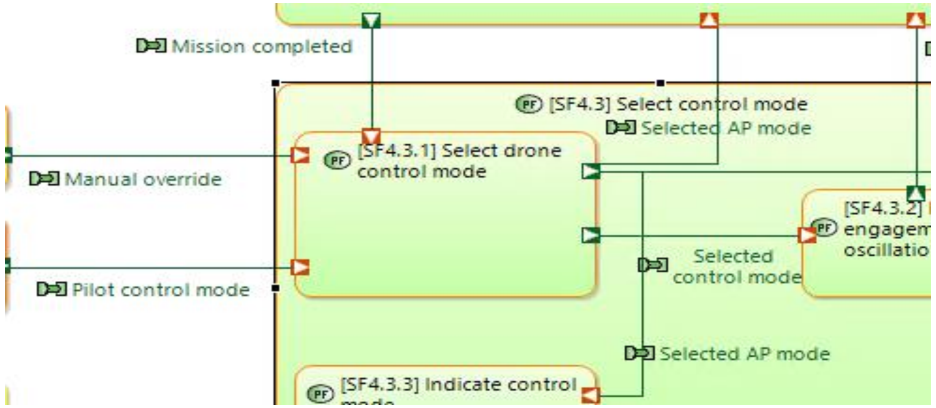
(to make an equivalent of SA ERRONEOUS domain enum)

We have to make equivalent validity of SE data

(to make an equivalent of SA LOST domain enum)

Perimeters

SE

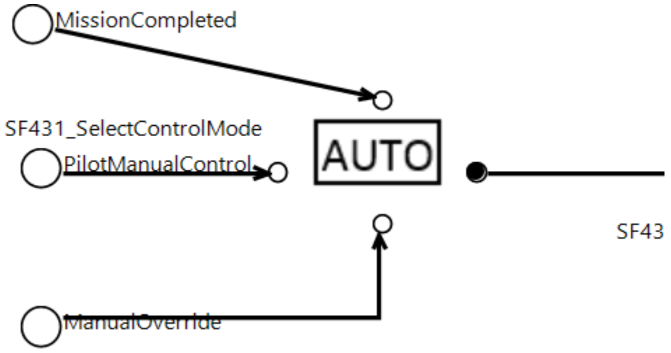

Mission completed
[SF4.3] Select control mode
Selected AP mode
[SF4.3.1] Select drone control mode
Manual override
[SF4.3.2] engagem oscillatio
Selected control mode
Pilot control mode
Selected AP mode
[SF4.3.3] Indicate control mode

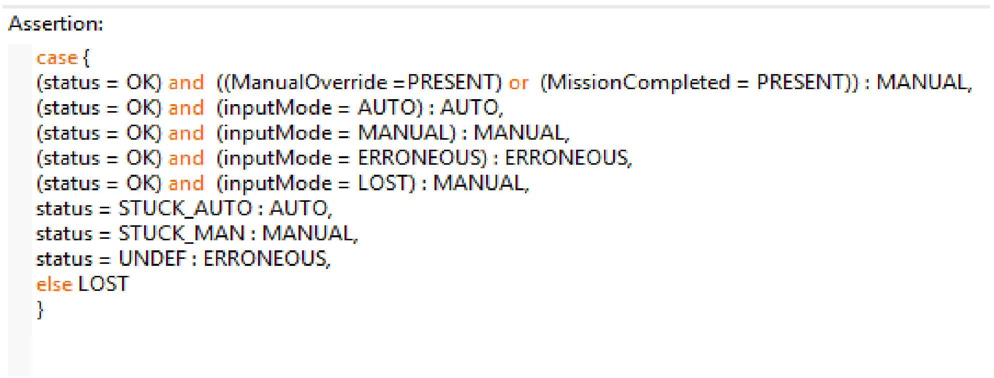
Pilot control mode		Manual override		Mission completed	Selected AP mode	Selected control mode
Value	Validity status	Value	Validity status	Value	Value	Value
N/A	N/A	OVERRIDE	VALID	N/A	Speed consign mode	MANUAL
N/A	N/A	N/A	INVALID	N/A	Speed consign mode	MANUAL
N/A	N/A	N/A	N/A	Completed	Speed consign mode	MANUAL
N/A	INVALID	N/A	N/A	N/A	Speed consign mode	MANUAL
MANUAL	VALID	N/A	N/A	N/A	Speed consign mode	MANUAL
Speed consign mode	VALID	NO OVERRIDE	VALID	N/A	Speed consign mode	AUTO
Flight plan mode	VALID	NO OVERRIDE	VALID	Not completed	Flight plan mode	AUTO

Interfaces

Behaviors

SA

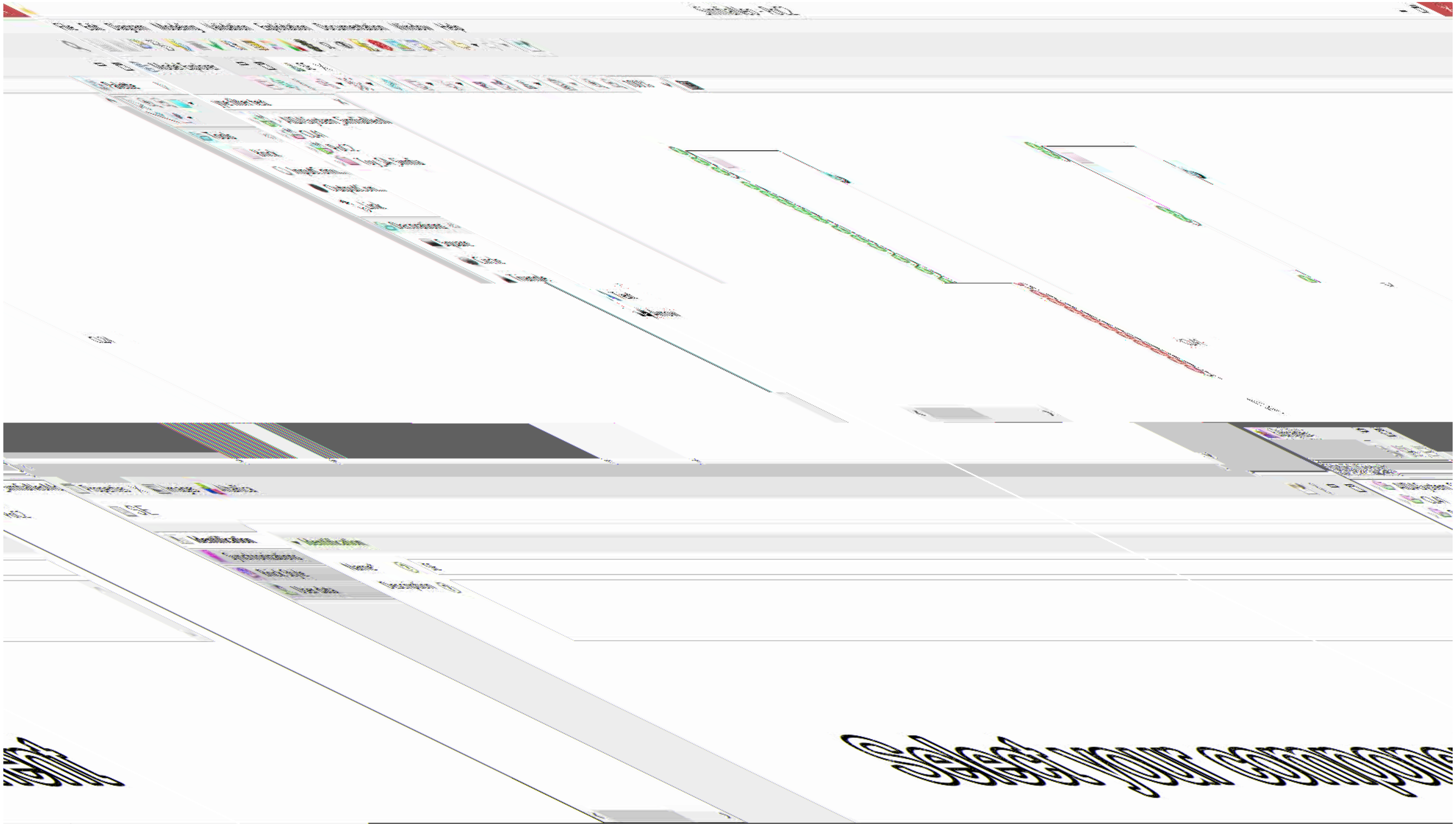




Assertion:

```
case {
(status = OK) and ((ManualOverride =PRESENT) or (MissionCompleted = PRESENT)) : MANUAL,
(status = OK) and (inputMode = AUTO) : AUTO,
(status = OK) and (inputMode = MANUAL) : MANUAL,
(status = OK) and (inputMode = ERRONEOUS) : ERRONEOUS,
(status = OK) and (inputMode = LOST) : MANUAL,
status = STUCK_AUTO : AUTO,
status = STUCK_MAN : MANUAL,
status = UNDEF : ERRONEOUS,
else LOST
}
```

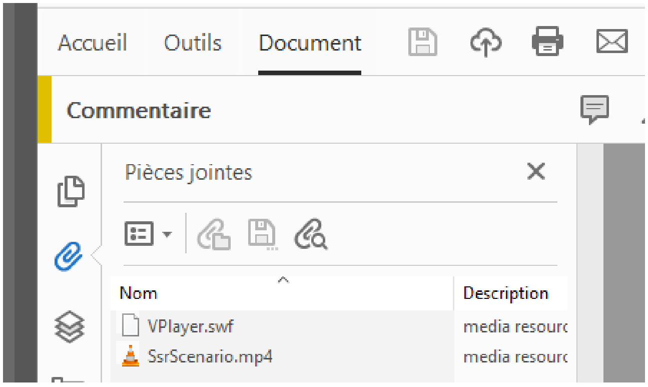
FRENCH INSTITUTES OF TECHNOLOGY



fit

Select your compone

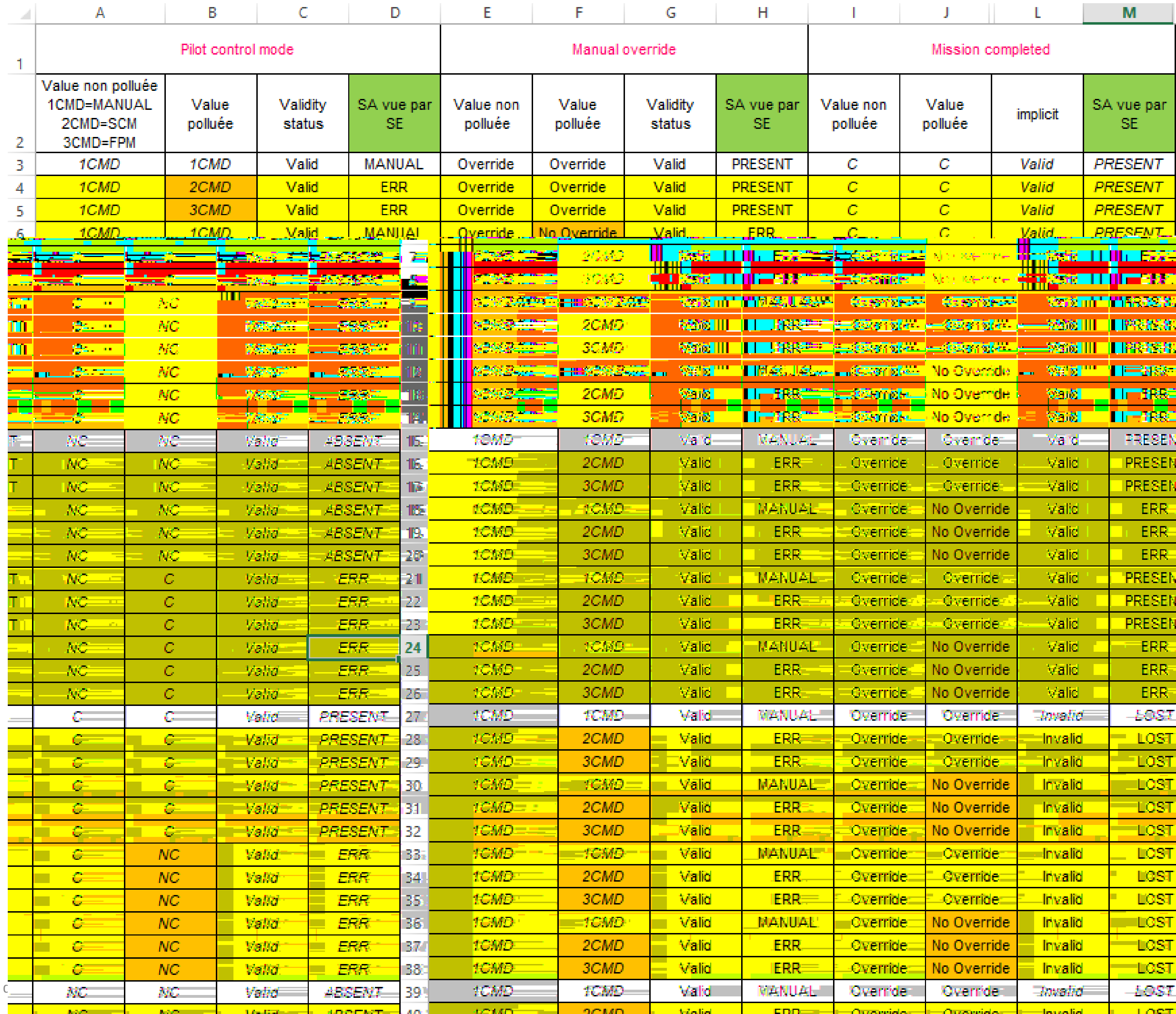
Get Video from PDF using attachement services of your reader (here above with Acrobat):



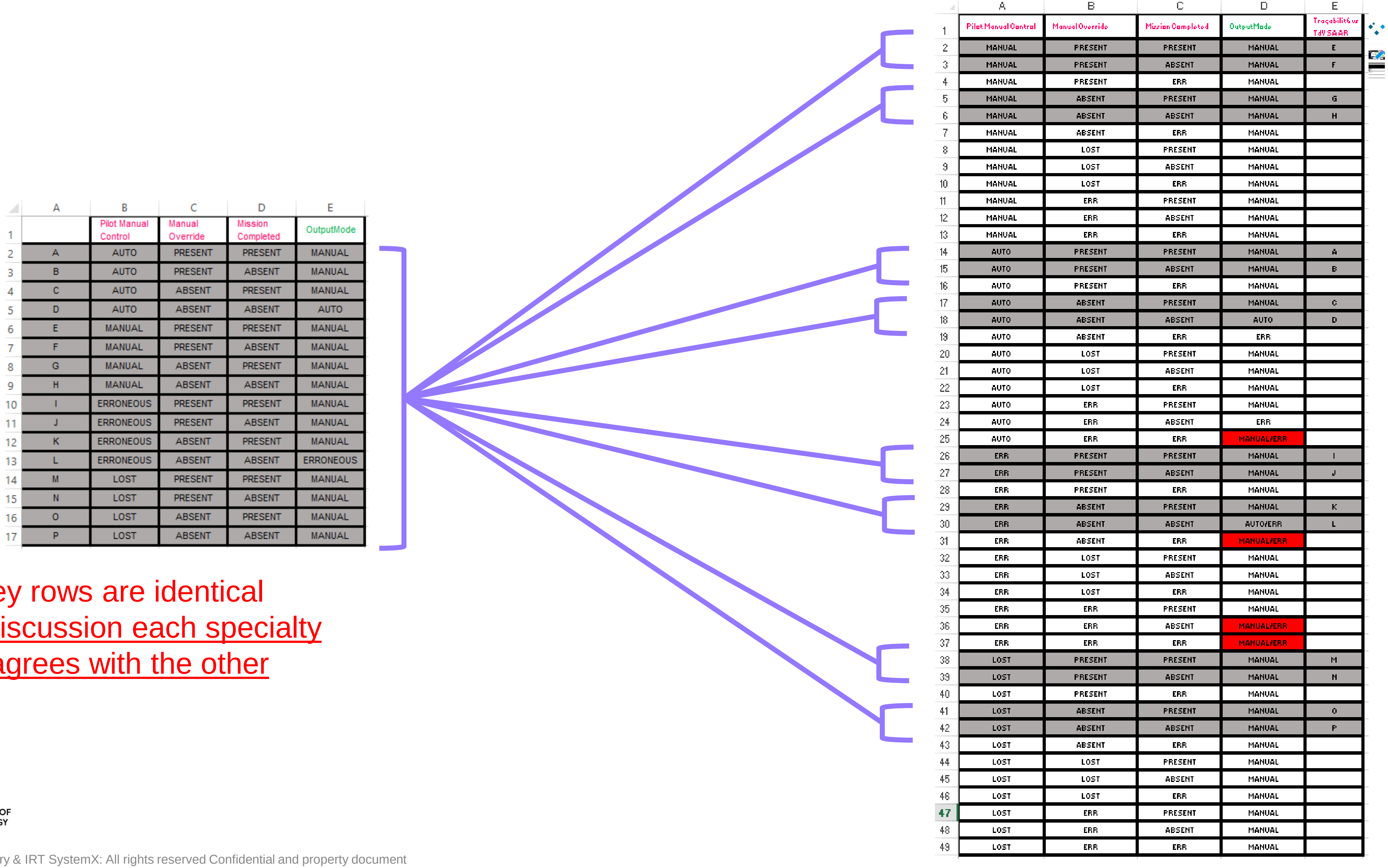
Nom	Description
VPlayer.swf	media resourc
SsrScenario.mp4	media resourc

- Transformation of
  - SE inputs and values to …
    … SA inputs and values
    (green header column)

- Remark
  - The pollution in orange cells
    (to be equivalent to an error)
  - The validity column added
    (to be equivalent to lost)
  - The volmetry
    (only a very little sub part of all combinaisons)



	A	B	C	D	E	F	G	H	I	J	L	M
1	Pilot control mode				Manual override				Mission completed			
2	Value non polluée 1CMD=MANUAL 2CMD=SCM 3CMD=FPM	Value polluée	Validity status	SA vue par SE	Value non polluée	Value polluée	Validity status	SA vue par SE	Value non polluée	Value polluée	implicit	SA vue par SE
3	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	Valid	PRESENT	*C*	*C*	*Valid*	*PRESENT*
4	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Valid	PRESENT	*C*	*C*	*Valid*	*PRESENT*
5	*1CMD*	*3CMD*	Valid	ERR	Override	Override	Valid	PRESENT	*C*	*C*	*Valid*	*PRESENT*
6	*1CMD*	*1CMD*	Valid	MANUAL	Override	No Override	Valid	ERR	*C*	*C*	*Valid*	*PRESENT*
7	[illegible]	2CMD	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8	[illegible]	3CMD	[illegible]	ERR	Override	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	*NC*	[illegible]	[illegible]
10	[illegible]	2CMD	[illegible]	ERR	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	*NC*	[illegible]	[illegible]
11	[illegible]	3CMD	[illegible]	ERR	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	*NC*	[illegible]	[illegible]
12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	No Override	[illegible]	[illegible]	[illegible]	*NC*	[illegible]	[illegible]
13	[illegible]	2CMD	Valid	ERR	[illegible]	No Override	Valid	ERR	*C*	*NC*	[illegible]	[illegible]
14	[illegible]	3CMD	Valid	ERR	[illegible]	No Override	Valid	ERR	*C*	*NC*	[illegible]	[illegible]
15	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	Valid	PRESEN	*NC*	*NC*	*Valid*	*ABSENT*
16	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Valid	PRESEN	*NC*	*NC*	*Valid*	*ABSENT*
17	*1CMD*	*3CMD*	Valid	ERR	Override	Override	Valid	PRESEN	*NC*	*NC*	*Valid*	*ABSENT*
18	*1CMD*	*1CMD*	Valid	MANUAL	Override	No Override	Valid	ERR	*NC*	*NC*	*Valid*	*ABSENT*
19	*1CMD*	*2CMD*	Valid	ERR	Override	No Override	Valid	ERR	*NC*	*NC*	*Valid*	*ABSENT*
20	*1CMD*	*3CMD*	Valid	ERR	Override	No Override	Valid	ERR	*NC*	*NC*	*Valid*	*ABSENT*
21	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	Valid	PRESEN	*NC*	*C*	*Valid*	*ERR*
22	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Valid	PRESEN	*NC*	*C*	*Valid*	*ERR*
23	*1CMD*	*3CMD*	Valid	ERR	Override	Override	Valid	PRESEN	*NC*	*C*	*Valid*	*ERR*
24	*1CMD*	*1CMD*	Valid	MANUAL	Override	No Override	Valid	ERR	*NC*	*C*	*Valid*	*ERR*
25	*1CMD*	*2CMD*	Valid	ERR	Override	No Override	Valid	ERR	*NC*	*C*	*Valid*	*ERR*
26	*1CMD*	*3CMD*	Valid	ERR	Override	No Override	Valid	ERR	*NC*	*C*	*Valid*	*ERR*
27	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	*Invalid*	*LOST*	*C*	*C*	*Valid*	*PRESENT*
28	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Invalid	LOST	*C*	*C*	*Valid*	*PRESENT*
29	*1CMD*	*3CMD*	Valid	ERR	Override	Override	Invalid	LOST	*C*	*C*	*Valid*	*PRESENT*
30	*1CMD*	*1CMD*	Valid	MANUAL	Override	No Override	Invalid	LOST	*C*	*C*	*Valid*	*PRESENT*
31	*1CMD*	*2CMD*	Valid	ERR	Override	No Override	Invalid	LOST	*C*	*C*	*Valid*	*PRESENT*
32	*1CMD*	*3CMD*	Valid	ERR	Override	No Override	Invalid	LOST	*C*	*C*	*Valid*	*PRESENT*
33	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
34	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
35	*1CMD*	*3CMD*	Valid	ERR	Override	Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
36	*1CMD*	*1CMD*	Valid	MANUAL	Override	No Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
37	*1CMD*	*2CMD*	Valid	ERR	Override	No Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
38	*1CMD*	*3CMD*	Valid	ERR	Override	No Override	Invalid	LOST	*C*	*NC*	*Valid*	*ERR*
39	*1CMD*	*1CMD*	Valid	MANUAL	Override	Override	*Invalid*	*LOST*	*NC*	*NC*	*Valid*	*ABSENT*
40	*1CMD*	*2CMD*	Valid	ERR	Override	Override	Invalid	LOST	*NC*	*NC*	*Valid*	*ABSENT*

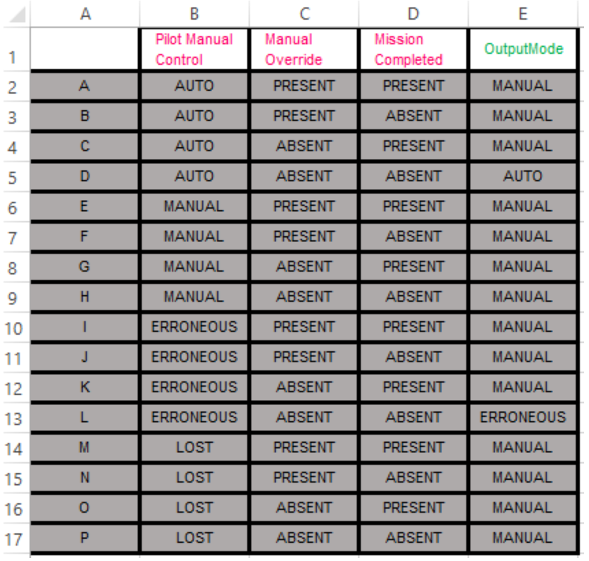


	A	B	C	D	E
1		Pilot Manual Control	Manual Override	Mission Completed	OutputMode
2	A	AUTO	PRESENT	PRESENT	MANUAL
3	B	AUTO	PRESENT	ABSENT	MANUAL
4	C	AUTO	ABSENT	PRESENT	MANUAL
5	D	AUTO	ABSENT	ABSENT	AUTO
6	E	MANUAL	PRESENT	PRESENT	MANUAL
7	F	MANUAL	PRESENT	ABSENT	MANUAL
8	G	MANUAL	ABSENT	PRESENT	MANUAL
9	H	MANUAL	ABSENT	ABSENT	MANUAL
10	I	ERRONEOUS	PRESENT	PRESENT	MANUAL
11	J	ERRONEOUS	PRESENT	ABSENT	MANUAL
12	K	ERRONEOUS	ABSENT	PRESENT	MANUAL
13	L	ERRONEOUS	ABSENT	ABSENT	ERRONEOUS
14	M	LOST	PRESENT	PRESENT	MANUAL
15	N	LOST	PRESENT	ABSENT	MANUAL
16	O	LOST	ABSENT	PRESENT	MANUAL
17	P	LOST	ABSENT	ABSENT	MANUAL

	A	B	C	D	E
1	Pilot Manual Control	Manual Override	Mission Completed	OutputMode	Traçabilité vers TdV SAAR
2	MANUAL	PRESENT	PRESENT	MANUAL	E
3	MANUAL	PRESENT	ABSENT	MANUAL	F
4	MANUAL	PRESENT	ERR	MANUAL	
5	MANUAL	ABSENT	PRESENT	MANUAL	G
6	MANUAL	ABSENT	ABSENT	MANUAL	H
7	MANUAL	ABSENT	ERR	MANUAL	
8	MANUAL	LOST	PRESENT	MANUAL	
9	MANUAL	LOST	ABSENT	MANUAL	
10	MANUAL	LOST	ERR	MANUAL	
11	MANUAL	ERR	PRESENT	MANUAL	
12	MANUAL	ERR	ABSENT	MANUAL	
13	MANUAL	ERR	ERR	MANUAL	
14	AUTO	PRESENT	PRESENT	MANUAL	A
15	AUTO	PRESENT	ABSENT	MANUAL	B
16	AUTO	PRESENT	ERR	MANUAL	
17	AUTO	ABSENT	PRESENT	MANUAL	C
18	AUTO	ABSENT	ABSENT	AUTO	D
19	AUTO	ABSENT	ERR	ERR	
20	AUTO	LOST	PRESENT	MANUAL	
21	AUTO	LOST	ABSENT	MANUAL	
22	AUTO	LOST	ERR	MANUAL	
23	AUTO	ERR	PRESENT	MANUAL	
24	AUTO	ERR	ABSENT	ERR	
25	AUTO	ERR	ERR	MANUAL/ERR	
26	ERR	PRESENT	PRESENT	MANUAL	I
27	ERR	PRESENT	ABSENT	MANUAL	J
28	ERR	PRESENT	ERR	MANUAL	
29	ERR	ABSENT	PRESENT	MANUAL	K
30	ERR	ABSENT	ABSENT	AUTO/ERR	L
31	ERR	ABSENT	ERR	MANUAL/ERR	
32	ERR	LOST	PRESENT	MANUAL	
33	ERR	LOST	ABSENT	MANUAL	
34	ERR	LOST	ERR	MANUAL	
35	ERR	ERR	PRESENT	MANUAL	
36	ERR	ERR	ABSENT	MANUAL/ERR	
37	ERR	ERR	ERR	MANUAL/ERR	
38	LOST	PRESENT	PRESENT	MANUAL	M
39	LOST	PRESENT	ABSENT	MANUAL	N
40	LOST	PRESENT	ERR	MANUAL	
41	LOST	ABSENT	PRESENT	MANUAL	O
42	LOST	ABSENT	ABSENT	MANUAL	P
43	LOST	ABSENT	ERR	MANUAL	
44	LOST	LOST	PRESENT	MANUAL	
45	LOST	LOST	ABSENT	MANUAL	
46	LOST	LOST	ERR	MANUAL	
47	LOST	ERR	PRESENT	MANUAL	
48	LOST	ERR	ABSENT	MANUAL	
49	LOST	ERR	ERR	MANUAL	

Grey rows are identical

⇒ No discussion each specialty agrees with the other

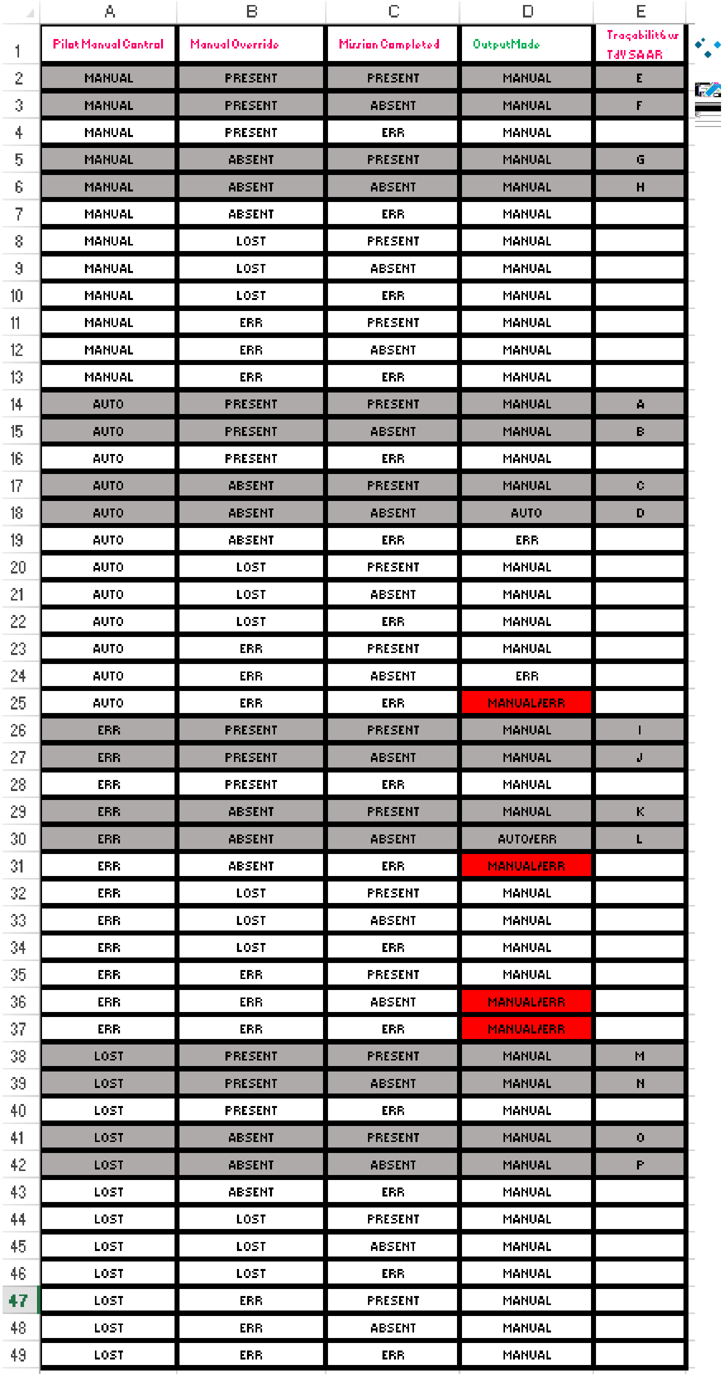


	A	B	C	D	E
1		Pilot Manual Control	Manual Override	Mission Completed	OutputMode
2	A	AUTO	PRESENT	PRESENT	MANUAL
3	B	AUTO	PRESENT	ABSENT	MANUAL
4	C	AUTO	ABSENT	PRESENT	MANUAL
5	D	AUTO	ABSENT	ABSENT	AUTO
6	E	MANUAL	PRESENT	PRESENT	MANUAL
7	F	MANUAL	PRESENT	ABSENT	MANUAL
8	G	MANUAL	ABSENT	PRESENT	MANUAL
9	H	MANUAL	ABSENT	ABSENT	MANUAL
10	I	ERRONEOUS	PRESENT	PRESENT	MANUAL
11	J	ERRONEOUS	PRESENT	ABSENT	MANUAL
12	K	ERRONEOUS	ABSENT	PRESENT	MANUAL
13	L	ERRONEOUS	ABSENT	ABSENT	ERRONEOUS
14	M	LOST	PRESENT	PRESENT	MANUAL
15	N	LOST	PRESENT	ABSENT	MANUAL
16	O	LOST	ABSENT	PRESENT	MANUAL
17	P	LOST	ABSENT	ABSENT	MANUAL

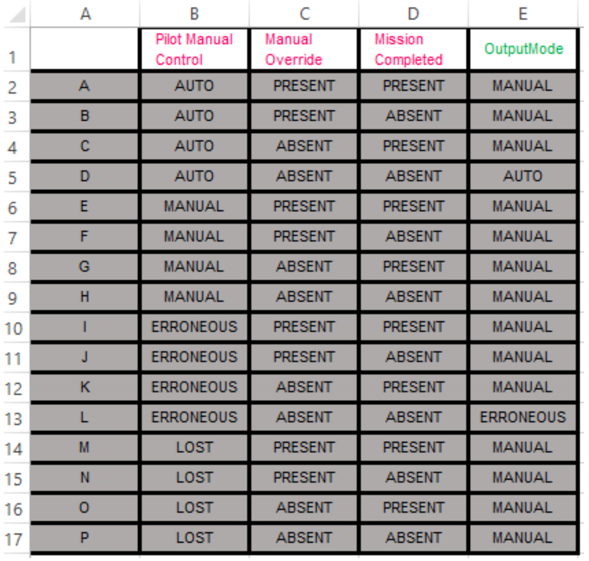
White rows have are absent in SA side

⇒ During transformation we consider control input can be wrong while SA consider it is not possible.

⇒ <u>This shall be discuss between specialities</u>



	A	B	C	D	E
1	Pilot Manual Control	Manual Override	Mission Completed	OutputMode	Traçabilité vs TdV SAAR
2	MANUAL	PRESENT	PRESENT	MANUAL	E
3	MANUAL	PRESENT	ABSENT	MANUAL	F
4	MANUAL	PRESENT	ERR	MANUAL	
5	MANUAL	ABSENT	PRESENT	MANUAL	G
6	MANUAL	ABSENT	ABSENT	MANUAL	H
7	MANUAL	ABSENT	ERR	MANUAL	
8	MANUAL	LOST	PRESENT	MANUAL	
9	MANUAL	LOST	ABSENT	MANUAL	
10	MANUAL	LOST	ERR	MANUAL	
11	MANUAL	ERR	PRESENT	MANUAL	
12	MANUAL	ERR	ABSENT	MANUAL	
13	MANUAL	ERR	ERR	MANUAL	
14	AUTO	PRESENT	PRESENT	MANUAL	A
15	AUTO	PRESENT	ABSENT	MANUAL	B
16	AUTO	PRESENT	ERR	MANUAL	
17	AUTO	ABSENT	PRESENT	MANUAL	C
18	AUTO	ABSENT	ABSENT	AUTO	D
19	AUTO	ABSENT	ERR	ERR	
20	AUTO	LOST	PRESENT	MANUAL	
21	AUTO	LOST	ABSENT	MANUAL	
22	AUTO	LOST	ERR	MANUAL	
23	AUTO	ERR	PRESENT	MANUAL	
24	AUTO	ERR	ABSENT	ERR	
25	AUTO	ERR	ERR	MANUAL/ERR	
26	ERR	PRESENT	PRESENT	MANUAL	I
27	ERR	PRESENT	ABSENT	MANUAL	J
28	ERR	PRESENT	ERR	MANUAL	
29	ERR	ABSENT	PRESENT	MANUAL	K
30	ERR	ABSENT	ABSENT	AUTO/ERR	L
31	ERR	ABSENT	ERR	MANUAL/ERR	
32	ERR	LOST	PRESENT	MANUAL	
33	ERR	LOST	ABSENT	MANUAL	
34	ERR	LOST	ERR	MANUAL	
35	ERR	ERR	PRESENT	MANUAL	
36	ERR	ERR	ABSENT	MANUAL/ERR	
37	ERR	ERR	ERR	MANUAL/ERR	
38	LOST	PRESENT	PRESENT	MANUAL	M
39	LOST	PRESENT	ABSENT	MANUAL	N
40	LOST	PRESENT	ERR	MANUAL	
41	LOST	ABSENT	PRESENT	MANUAL	O
42	LOST	ABSENT	ABSENT	MANUAL	P
43	LOST	ABSENT	ERR	MANUAL	
44	LOST	LOST	PRESENT	MANUAL	
45	LOST	LOST	ABSENT	MANUAL	
46	LOST	LOST	ERR	MANUAL	
47	LOST	ERR	PRESENT	MANUAL	
48	LOST	ERR	ABSENT	MANUAL	
49	LOST	ERR	ERR	MANUAL	

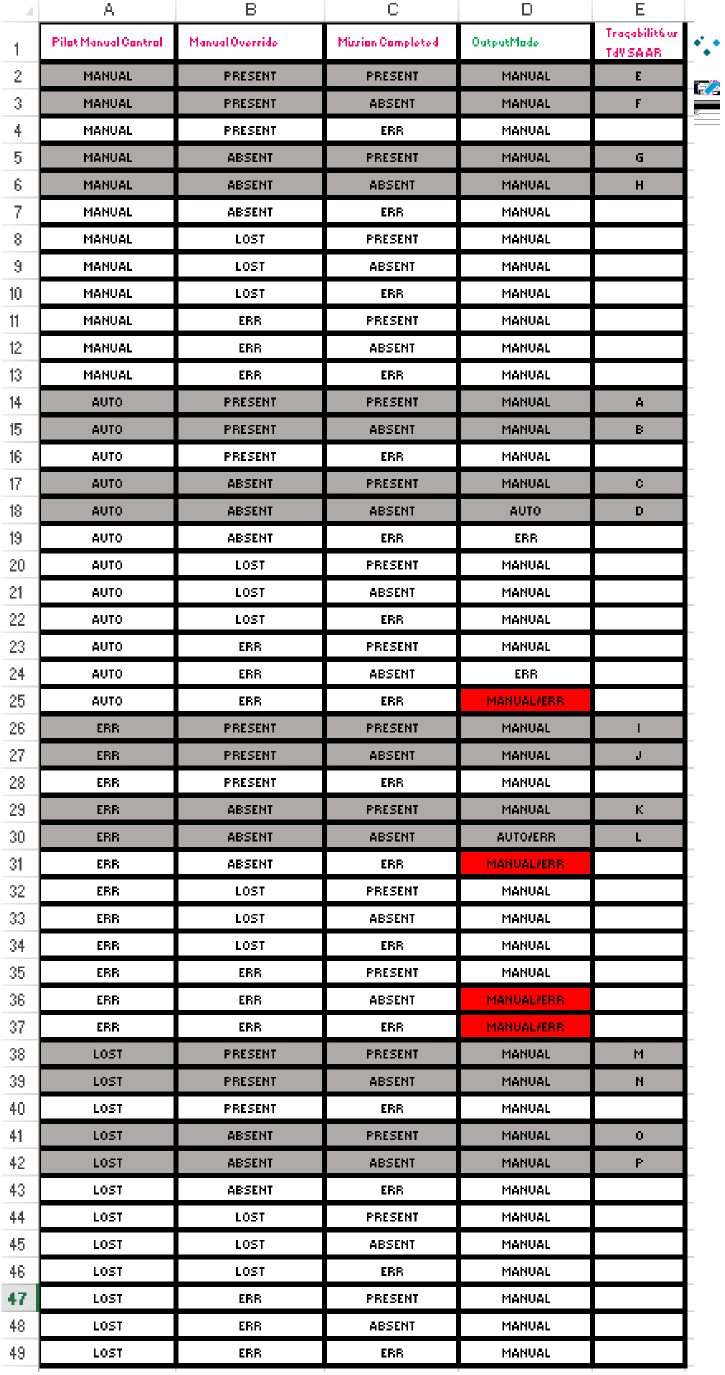


	A	B	C	D	E
1		Pilot Manual Control	Manual Override	Mission Completed	OutputMode
2	A	AUTO	PRESENT	PRESENT	MANUAL
3	B	AUTO	PRESENT	ABSENT	MANUAL
4	C	AUTO	ABSENT	PRESENT	MANUAL
5	D	AUTO	ABSENT	ABSENT	AUTO
6	E	MANUAL	PRESENT	PRESENT	MANUAL
7	F	MANUAL	PRESENT	ABSENT	MANUAL
8	G	MANUAL	ABSENT	PRESENT	MANUAL
9	H	MANUAL	ABSENT	ABSENT	MANUAL
10	I	ERRONEOUS	PRESENT	PRESENT	MANUAL
11	J	ERRONEOUS	PRESENT	ABSENT	MANUAL
12	K	ERRONEOUS	ABSENT	PRESENT	MANUAL
13	L	ERRONEOUS	ABSENT	ABSENT	ERRONEOUS
14	M	LOST	PRESENT	PRESENT	MANUAL
15	N	LOST	PRESENT	ABSENT	MANUAL
16	O	LOST	ABSENT	PRESENT	MANUAL
17	P	LOST	ABSENT	ABSENT	MANUAL

Red cells indicates maximisation During transformation

⇒ i.e. different IN(SE) transformed in IN(SA) leads to different OUT(SA)

=> This shall be discussed



	A	B	C	D	E
1	Pilot Manual Control	Manual Override	Mission Completed	OutputMode	Traçabilité vs TdV SAAR
2	MANUAL	PRESENT	PRESENT	MANUAL	E
3	MANUAL	PRESENT	ABSENT	MANUAL	F
4	MANUAL	PRESENT	ERR	MANUAL	
5	MANUAL	ABSENT	PRESENT	MANUAL	G
6	MANUAL	ABSENT	ABSENT	MANUAL	H
7	MANUAL	ABSENT	ERR	MANUAL	
8	MANUAL	LOST	PRESENT	MANUAL	
9	MANUAL	LOST	ABSENT	MANUAL	
10	MANUAL	LOST	ERR	MANUAL	
11	MANUAL	ERR	PRESENT	MANUAL	
12	MANUAL	ERR	ABSENT	MANUAL	
13	MANUAL	ERR	ERR	MANUAL	
14	AUTO	PRESENT	PRESENT	MANUAL	A
15	AUTO	PRESENT	ABSENT	MANUAL	B
16	AUTO	PRESENT	ERR	MANUAL	
17	AUTO	ABSENT	PRESENT	MANUAL	C
18	AUTO	ABSENT	ABSENT	AUTO	D
19	AUTO	ABSENT	ERR	ERR	
20	AUTO	LOST	PRESENT	MANUAL	
21	AUTO	LOST	ABSENT	MANUAL	
22	AUTO	LOST	ERR	MANUAL	
23	AUTO	ERR	PRESENT	MANUAL	
24	AUTO	ERR	ABSENT	ERR	
25	AUTO	ERR	ERR	🟥 MANUAL/ERR	
26	ERR	PRESENT	PRESENT	MANUAL	I
27	ERR	PRESENT	ABSENT	MANUAL	J
28	ERR	PRESENT	ERR	MANUAL	
29	ERR	ABSENT	PRESENT	MANUAL	K
30	ERR	ABSENT	ABSENT	AUTO/ERR	L
31	ERR	ABSENT	ERR	🟥 MANUAL/ERR	
32	ERR	LOST	PRESENT	MANUAL	
33	ERR	LOST	ABSENT	MANUAL	
34	ERR	LOST	ERR	MANUAL	
35	ERR	ERR	PRESENT	MANUAL	
36	ERR	ERR	ABSENT	🟥 MANUAL/ERR	
37	ERR	ERR	ERR	🟥 MANUAL/ERR	
38	LOST	PRESENT	PRESENT	MANUAL	M
39	LOST	PRESENT	ABSENT	MANUAL	N
40	LOST	PRESENT	ERR	MANUAL	
41	LOST	ABSENT	PRESENT	MANUAL	O
42	LOST	ABSENT	ABSENT	MANUAL	P
43	LOST	ABSENT	ERR	MANUAL	
44	LOST	LOST	PRESENT	MANUAL	
45	LOST	LOST	ABSENT	MANUAL	
46	LOST	LOST	ERR	MANUAL	
47	LOST	ERR	PRESENT	MANUAL	
48	LOST	ERR	ABSENT	MANUAL	
49	LOST	ERR	ERR	MANUAL	

FRENCH INSTITUTES OF TECHNOLOGY

It is hard in some case where speciality do regroup inputs and outputs
(e.g. grouping all flow by sources or grouping by similar treatment on flow)

Redoing transformations that proof the non destructive changes or the identification of maximisation done

The SE segmentation of range of data can be an help to think in state and reuse of SA tools.
E.g. simulations so SE can experiment their specification and avoid waiting Ivv level while they better understand SA model)

Memory effects beetween vectors (i.e. sequence in vector order) are hard to do.
We can pass from exhaustiveness to some case of vectors association only.

Create variations on inputs vectors to get corresponding outputs need fuzzying tools and automation.

When tests are echaustive, we can reduce the lambda of context of a failure.
(i.e. instead of maximizing for all the situation, isolate the risky situation and modulate effect regarding its failure rate occurence)