

Facilitate STPA adoption through its integration to existing methods and tooling

Max Chopart
Czech Technical University in Prague
chopamax@cvut.cz

Julien Vidalie
Airbus Protect
julien.vidalie@airbus.com

CTU
CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF TRANSPORTATION SCIENCES
DEPARTMENT OF AIR TRANSPORT

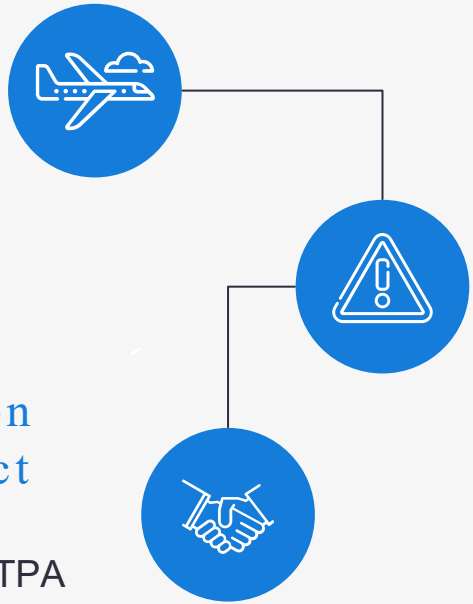
AIRBUS



01
Context

2023 - Internship at Airbus Protect

- Educating on STPA



First time I "hit the wall"

- "Isn't this just a big FHA?"
- "Can I certify with it?"
- "I already have a process to follow, and it **does not integrate** into it"

Since 2023 - Collaboration with Airbus Protect

- 2 publications on integrating STPA and MBSA
- Full guideline in preparation

- Performed full STPA (see "Hazard analysis of aircraft inspection by drone assistant system using STPA" **25.09.25**)



02

Model-Based Safety Analysis

Failure propagation models for RAMS

Model-Based Safety Analysis

Model-Based

Centralize data
Graphical tools
Share information

Safety

Avoid feared situation
Support certification

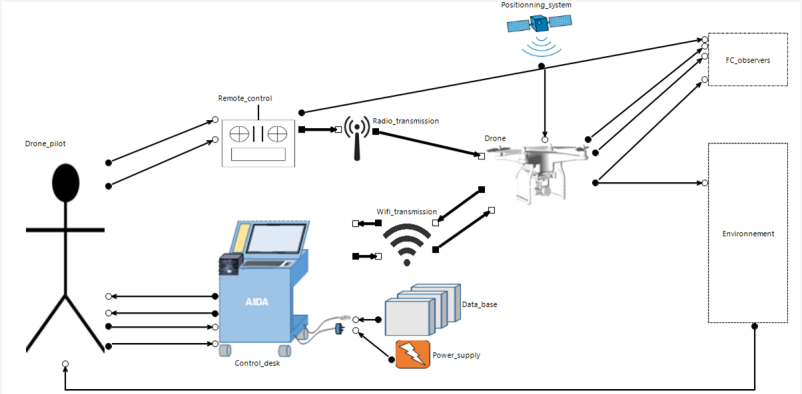
Analysis

Simulate failure propagation
Compute cutsets
Generate documentation

Feared Events (undesired states of the system) are modelled as **Observers** in MBSA.

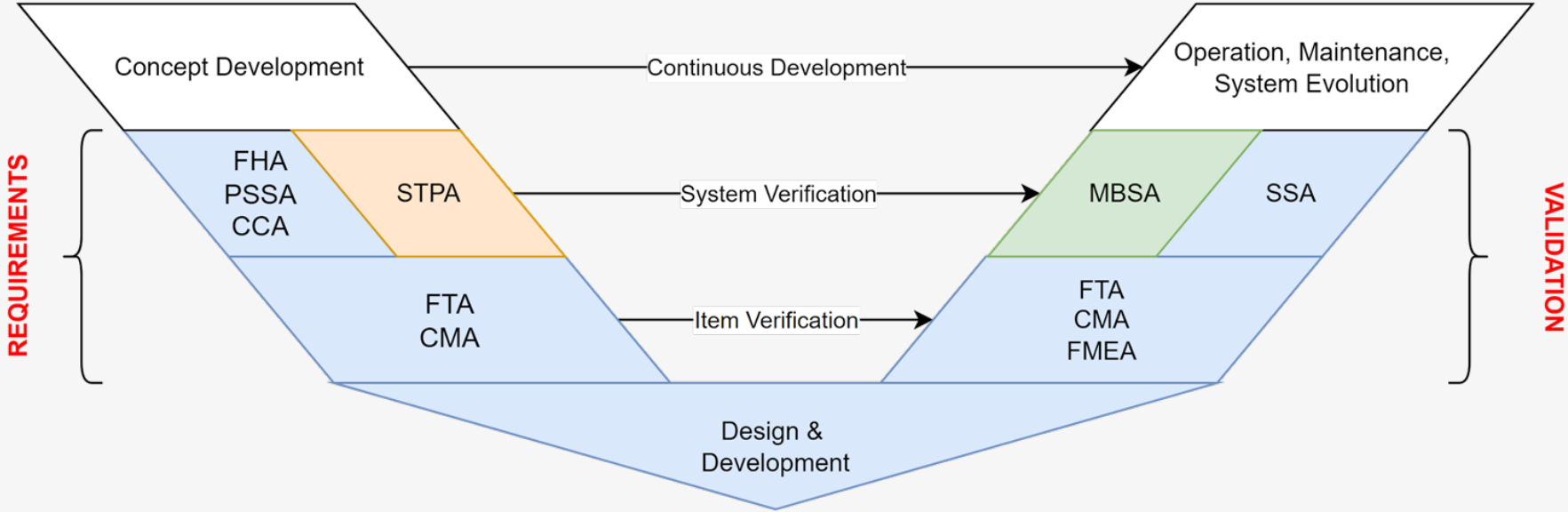
Observers are boolean formulae referring to variables of the model that allow the computation of RAMS indicators.

However, **what should be observed?**



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

Integrating STPA & MBSA- Our scope



STPA scenarios to MBSA observers

STPA Natural Language - Class 1 Scenario Archetype:

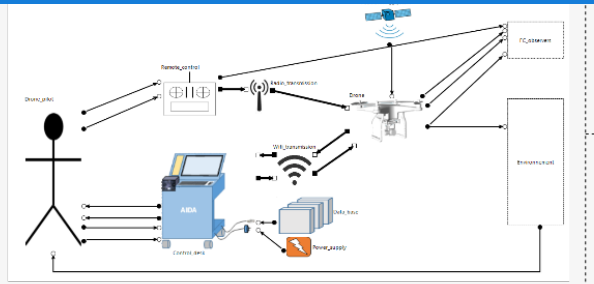
<Controller> does not provide <Control Action> when <Context> - <Input> to <Controller> correctly indicates <Context>

MBSA Formal Language (Altarica DataFlow) - Observer:

(Controller.Output = notProvided) and (Controller.Input = nominal) and (<Context> = <Value>)

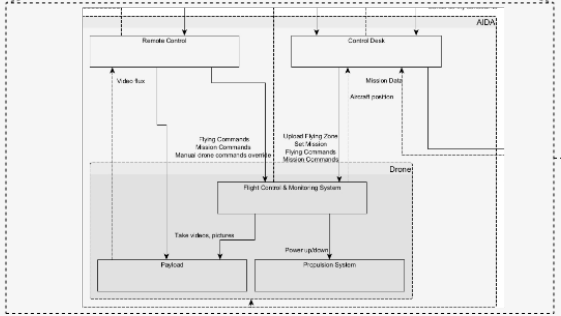


STPA scenarios to MBSA observers



Build the MBSA model

Build the Safety Control Structure



GraphDB

Construct MBSA system's Vocabulary

STPA - MBSA mapping

Generate the Loss Scenarios

GraphDB

```
observer LS-25 : boolean;
equation
LS-25 =
(Control_desk.Control_desk_common.
    Control_desk_common_state)
   = Nominal
AND (Control_desk.
WifiTransmissionUplink_FlightPlanAndZone)
   = Nominal
AND (Control_desk.iFlightPlanAndZone)
   = Erroneous;
```

Scenario to Observer

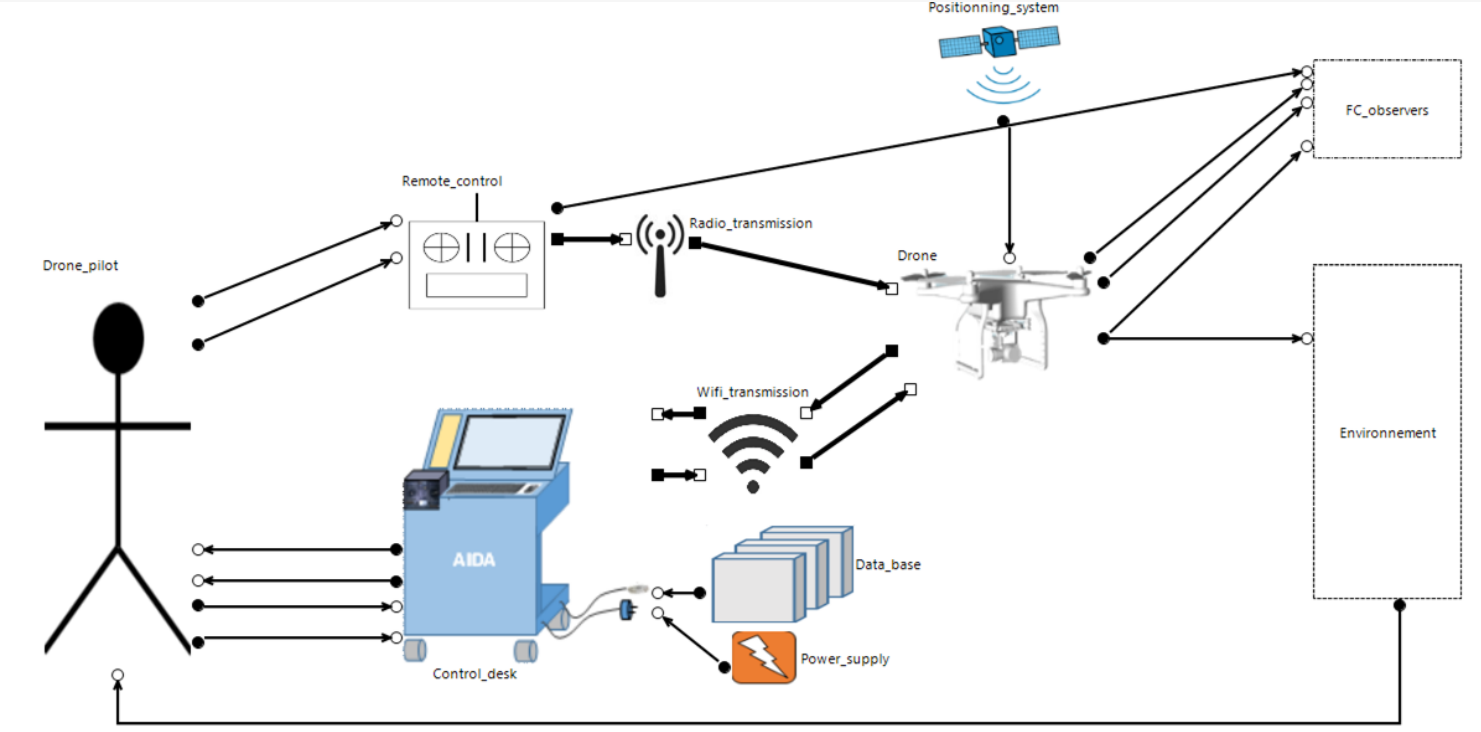
CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF TRANSPORTATION SCIENCES DEPARTMENT OF AIR TRANSPORT
AIRBUS

03

Case study: AIDA system

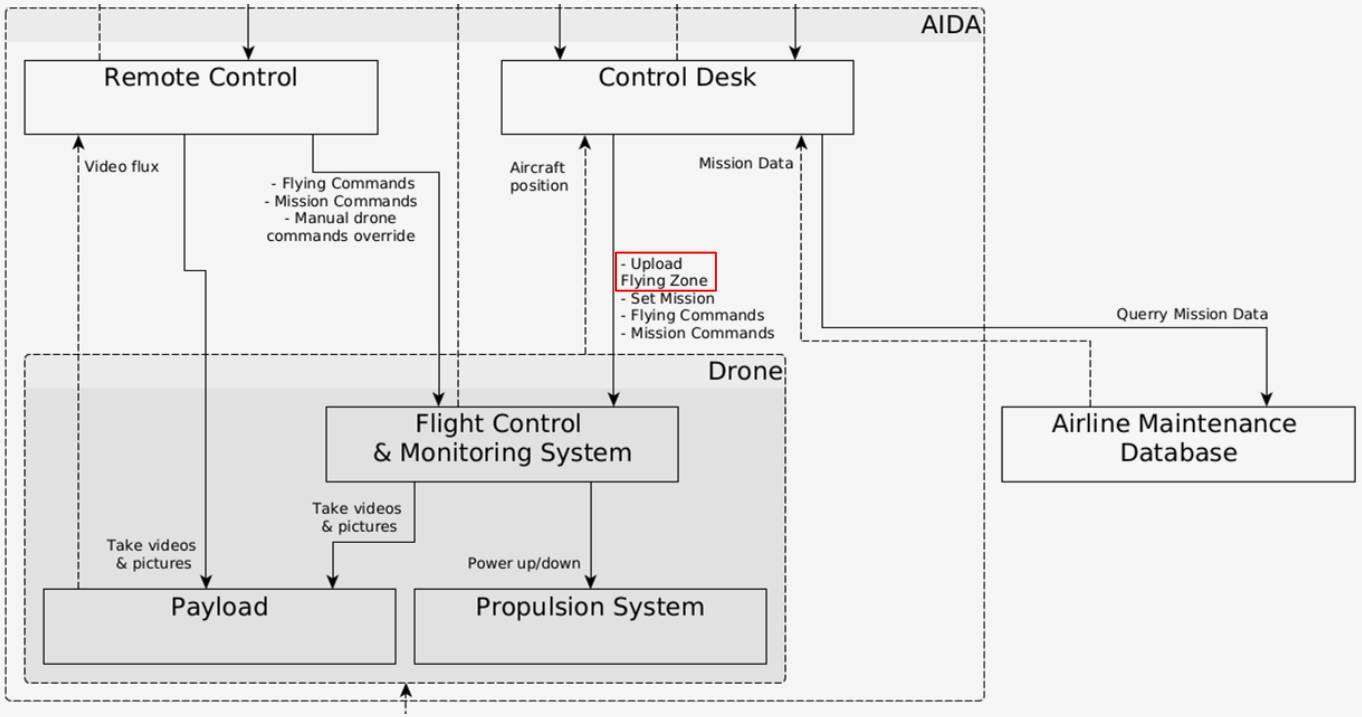


Architectural view of the MBSA Model



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

Safety Control Structure



STPA to MBSA artifacts

STPA Natural Language - Class 1: Scenario Archetype:

<Control Desk> does not provide <Controller> does not provide <Control Action> when <Context> - <Input> to <Controller> correctly indicates <Context>

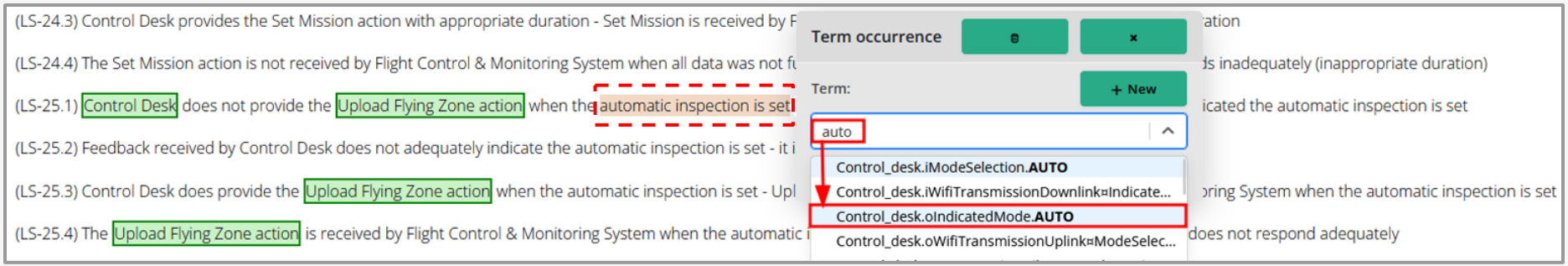
Upload Flying Zone Action when **Automatic Inspection is Set** - **Control Desk Feedback** to **Control Desk** correctly indicates that **Automatic Inspection is Set**

MBSA Formal Language (Altarica DataFlow) - Observer:

(Controller.Output = notProvided)
and (Controller.Input = nominal)
and (<Context> = <Value>)



Scenario Mapping



(LS-25.1) Control Desk does not provide the Upload Flying Zone action when the automatic inspection is set - Control Desk received feedback (or other input) that indicated the automatic inspection is set

(LS-25.2) Feedback received by Control Desk does not adequately indicate the automatic inspection is set - it is true that the automatic inspection is set

(LS-25.3) Control Desk does provide the Upload Flying Zone action when the automatic inspection is set - Upload Flying Zone is not received by Flight Control & Monitoring System when the automatic inspection is set

(LS-25.4) The Upload Flying Zone action is received by Flight Control & Monitoring System when the automatic inspection is set - Flight Control & Monitoring System does not respond adequately

AIDA system - Mapping Results

Scenario ID	Annotated text	Linked MBSA Item URI	MBSA model item
LS-25.1 - Controller	Control Desk	http://fd.cvut.cz/chopamax/mbsa/aida#Control_desk_Control_desk_common	Control_desk.Control_desk_common
LS-25.1 - Control Action	Does not provide the Upload Flying Zone action	http://fd.cvut.cz/chopamax/mbsa/aida#Control_desk_oWifiTransmissionUplinkFlightPlanAndZone_LOST	Control_desk.oWifiTransmissionUplink¤FlightPlanAndZone.LOST
LS-25.1 - Context	automatic inspection is set	http://fd.cvut.cz/chopamax/mbsa/aida#Control_desk_iModeSelection_AUTO	ControlDesk.oIndicatedMode.AUTO
LS-25.1 - Feedback	indicated the automatic inspection is set	http://fd.cvut.cz/chopamax/mbsa/aida#Control_desk_iModeSelection_AUTO	ControlDesk.iIndicatedMode.AUTO

AIDA system - Generated Observers

```
"bindings" : [
  {
    "scenarioName" : {
      "value" : "LS-25.1"
    },
    "allConditions" : {
      "value" : "(Control_desk.oWifiTransmissionUplink¤FlightPlanAndZone = LOST) and
(ControlDesk.oModeSelection.AUTO) and (Control_desk.iIndicatedMode = AUTO)"
    },
```

Feared situation	Phase	Max Order	Probability type	Calculated pro...
LS_25_1	Syste...	3	ARP4761	1.413E-5 /h

Elements	Order ▲	Probability ▼
Control_desk.Control_desk_common.Loss	1	1.09E-5
Control_desk.SF6_1_Compute_Flight_Zone_and_Flight_Plan.Loss	1	3.23E-6

04 Conclusion



Conclusion

Successful integration

- STPA & MBSA can be integrated together, within the same pipeline.
- Leads to further work to keep expanding the integration.

Failure Based Scenarios

For this specific use case, at the moment, only scenarios that are failure based are being processed, other ones are filtered out.

Non-Failure Based Scenarios

Non-failure based scenarios are simulable, but leads to new questions:

- Do we put probabilities?
- If yes, which ones?
- Is it actually representative?



Want to know more?

- M. Chopart, J. Vidalie, A. Lališ, and K. Grötschelová, “Harmonizing Safety Perspectives: Integrating STPA outputs into MBSA for Comprehensive Aircraft Safety Assessment,” in 2024 New Trends in Civil Aviation (NTCA), Apr. 2024, pp. 261–267. doi: 10.23919/NTCA60572.2024.10517833.

- M. Chopart, J. Vidalie, and X. Bossoreille, “Ontology-driven Integration of System-Theoretic Process Analysis and Model-Based Safety Analysis for Comprehensive Safety Assessment”, June 2025. doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P1191-cd.