ONERA

THE FRENCH AEROSPACE LAB

www.onera.fr

Lessons learnt about MBSA for the safety analysis of drone designs

Pierre Bieber, Kevin Delmas, Sergio Pizziol
Tatiana Prosvirnova, *Christel Seguin*

01/06/2023

Prenom.nom@onera.fr

ONERA
THE FRENCH AEROSPACE LAB

Presentation context & objective

ONERA : the French Aerospace Lab

- ~1000 scientists who address major disciplines for aircraft design & operation
- Wind tunnels & various test benches

Works with DGAC in drone national projects since 2017

- Collaborative research projects with big and smaller aeronautics companies
- PHYDIAS project: exploration and application of methods for appraisal of drone design

Presentation objectives :

- Lessons learnt from the safety analysis of 6 actual drone systems used in BVLOS operations

Studied drone systems

4 fix wings (6 system versions)

- Medium/long range operations over sparsely populated are
- MTOW : from 2kg, 25kg
- Engines electrical and thermic

2 rotorcrafts

- Delivery of medical goods in populated area
- MTOW: 2,5kg and 100kg
- Engines electrical and thermic

1 aerostat

- Long range over sparsely populated area
- MTOW: 170 kg

Steps of safety analysis addressed in the presentation

Preliminary hazard analysis of the operation

- Can the drone be lethal? Who/what is at risk?

Specification of the safety policy

- When is the operation under control? How are mitigated the safety degradations?

Progressive safety review of the system design

- <u>Mitigation Procedures</u>: How human & systems share the operation supervision?
- <u>Functions</u>: How system functions implements the system tasks?
- <u>Physical resources</u>: How hard/soft component implements the functions ?

⇒ How these items fail? Are they robust enough ?

Preliminary hazard analysis of the operation

Goal: estimate the operation risks

- Primary safety risks: impact with ground or air collision
- Escalating safety risks : fire …
- Other risks: breach of privacy, noise, …

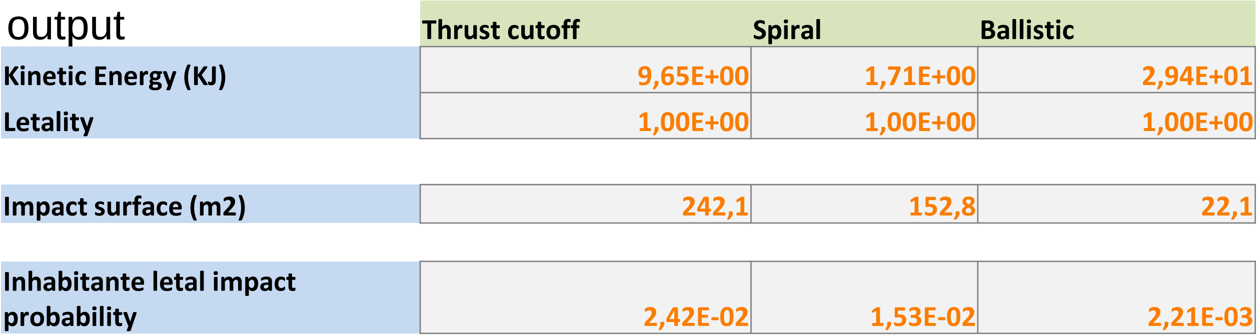
Guidance: excel check lists of influence factors for safety risks

- Impact mode : under parachute, spiral descent, ballistic descent …
- Kinetic energy at impact
- Impact surface
- Density of overflown populations
- Proximity with other traffic …

Preliminary hazard analysis of the operation

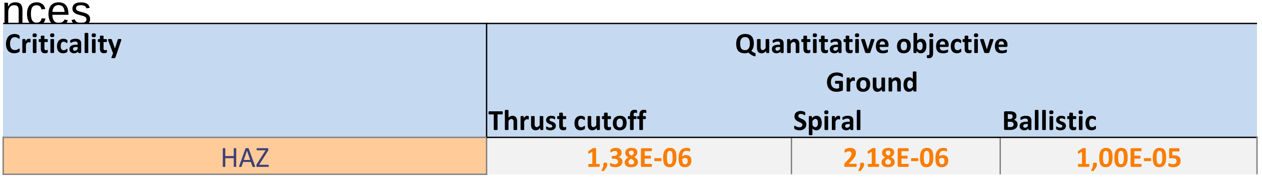
Example : fix wing of 25kg flying over population of 100 inhabitants / km2

- Analysis output



	Thrust cutoff	Spiral	Ballistic
Kinetic Energy (KJ)	9,65E+00	1,71E+00	2,94E+01
Letality	1,00E+00	1,00E+00	1,00E+00
Impact surface (m2)	242,1	152,8	22,1
Inhabitante letal impact probability	2,42E-02	1,53E-02	2,21E-03

- Impact of the safety objectives for the drone, assuming an equi-repartition of the crash mode occurrences



Criticality	Quantitative objective		
	Ground		
	Thrust cutoff	Spiral	Ballistic
HAZ	1,38E-06	2,18E-06	1,00E-05

Specification of a safety policy

Goal: specify rules to ensure safe flight and mitigate loss of operation control

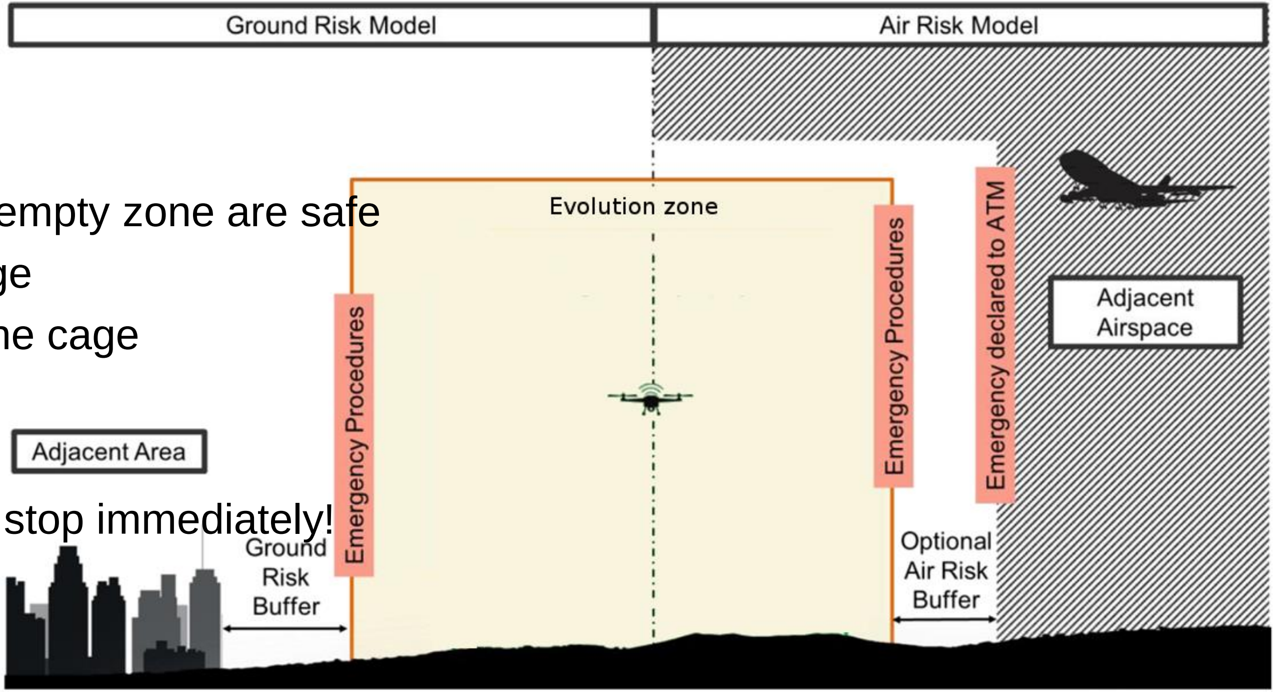
Examples:

- Flight and crash in an empty zone are safe

⇒Define a safe flight cage

⇒Stop any flight out of the cage

- Urban flight cannot be stop immediately!



Specification of a safety policy

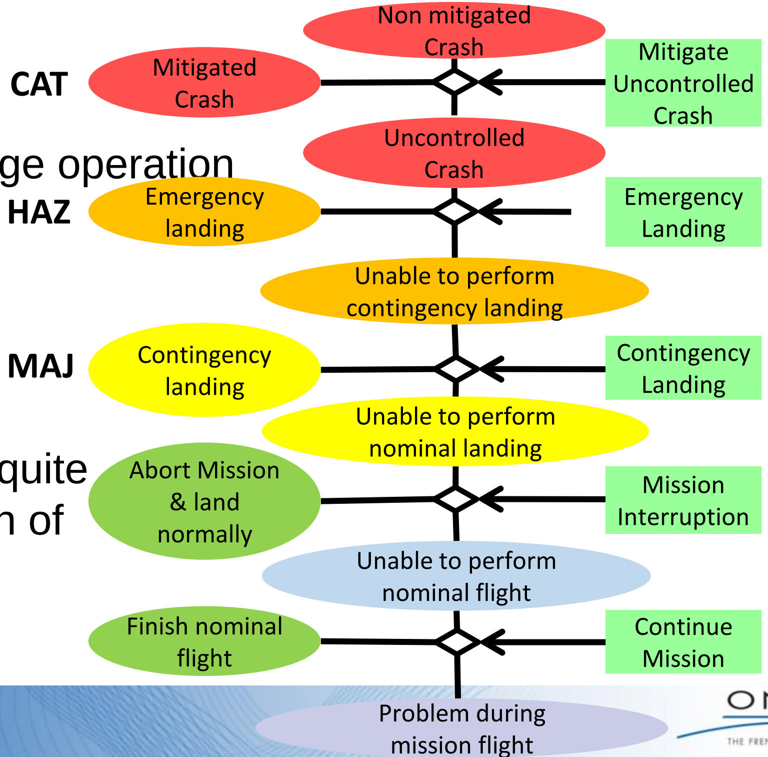
Guidance proposal : use diagram of safety barriers to state the policy

Example :

- Policy for the ground risk for long range operation

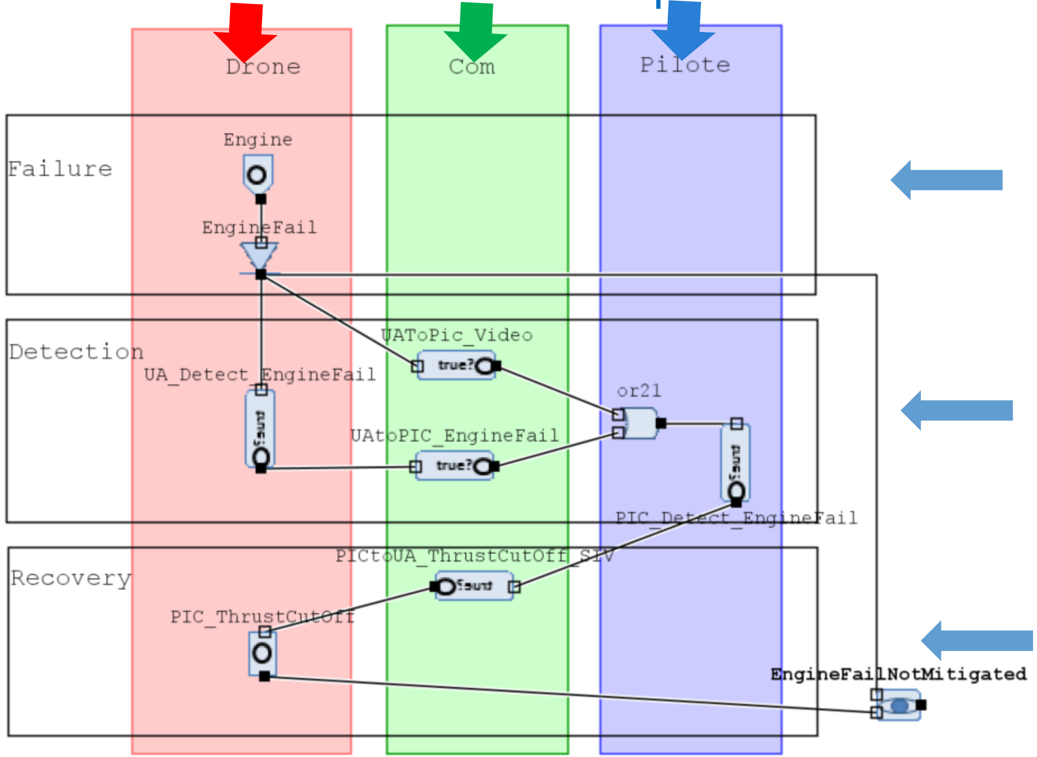
Lessons learned

- Explicit safety policy helps a lot: it focuses design choices & reviews
- Use of diagrams of safety barriers is quite accepted and sustain implementation of graceful degradation of safety



Example of mitigation procedure model

Actors : drone service tele-pilot



Hazard: engine failure

Hazard detection :

- By the drone
- By the pilote

Hazard management :

- Action : stop engine
- triggered by the tele-pilot

Safety review of the emergency procedures

Goals

- Specify how the tele-operator and the system manage the hazards
- Verify the compliance of the procedure with the safety policy
  - What are the consequences of successful procedures ?
  - What are the consequences of system failure or human error ?

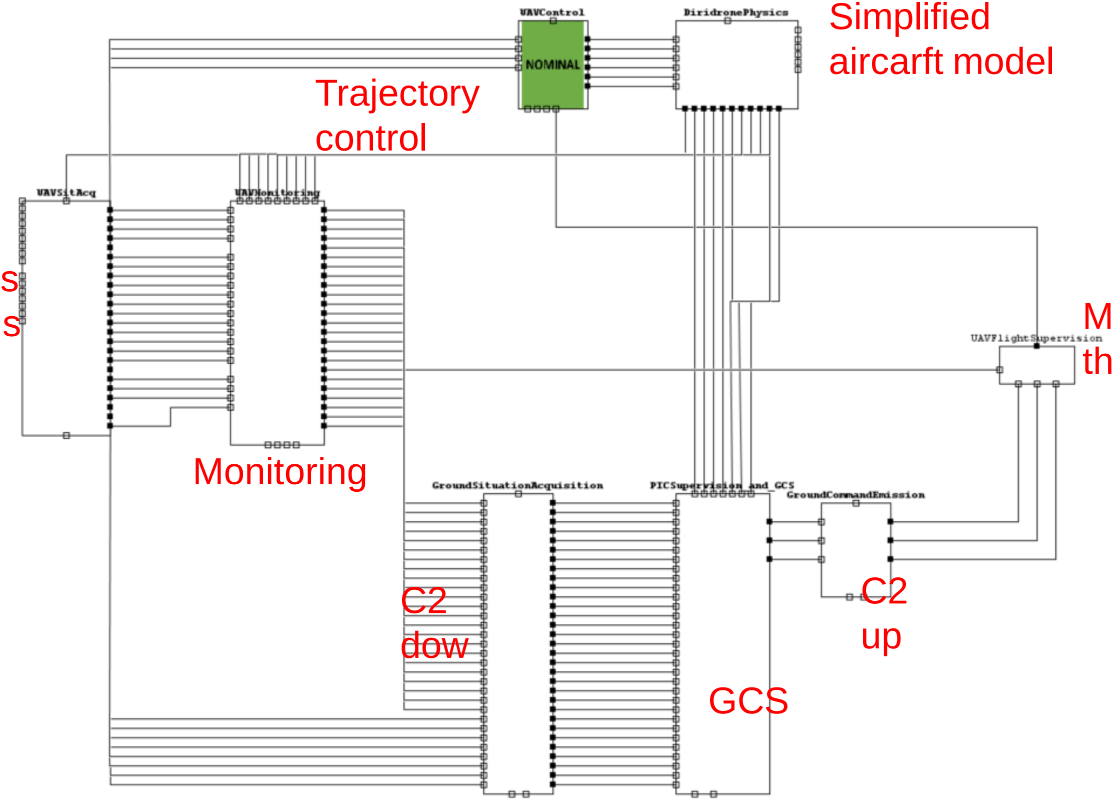
Guidance

- Link with the previous step : at least one procedure should be designed for each degraded situations identified by the safety policy
- Proposal of standard way of writing the procedure
- Tool available to quickly specify procedures and analyse the failure / error effects

Lessons learnt

- Procedures of the pilot manual are sometime too complex and some time inconsistent
- Quick feedback on the robustness to the loss of communication

Example of a functional architecture (level 1)



Simplified aircarft model

Trajectory control

Parameters acquisitions

Management of the drone modes

Monitoring

C2 dow

C2 up

GCS

Safety review of the drone functions

Goal

- Specify the system functions needed for a controlled / degraded flight
- Identify functional failure sets leading to CAT, HAZ, MAJ situations
- Verify safety functional requirements : FDAL, no single design error, …

Guidance

- Check list of usual functions
- Eurocae ED-125 – ARP 4761A recommended practices : Functional Hazard Analysis, Functional Fault tree, models …

Lessons learnt

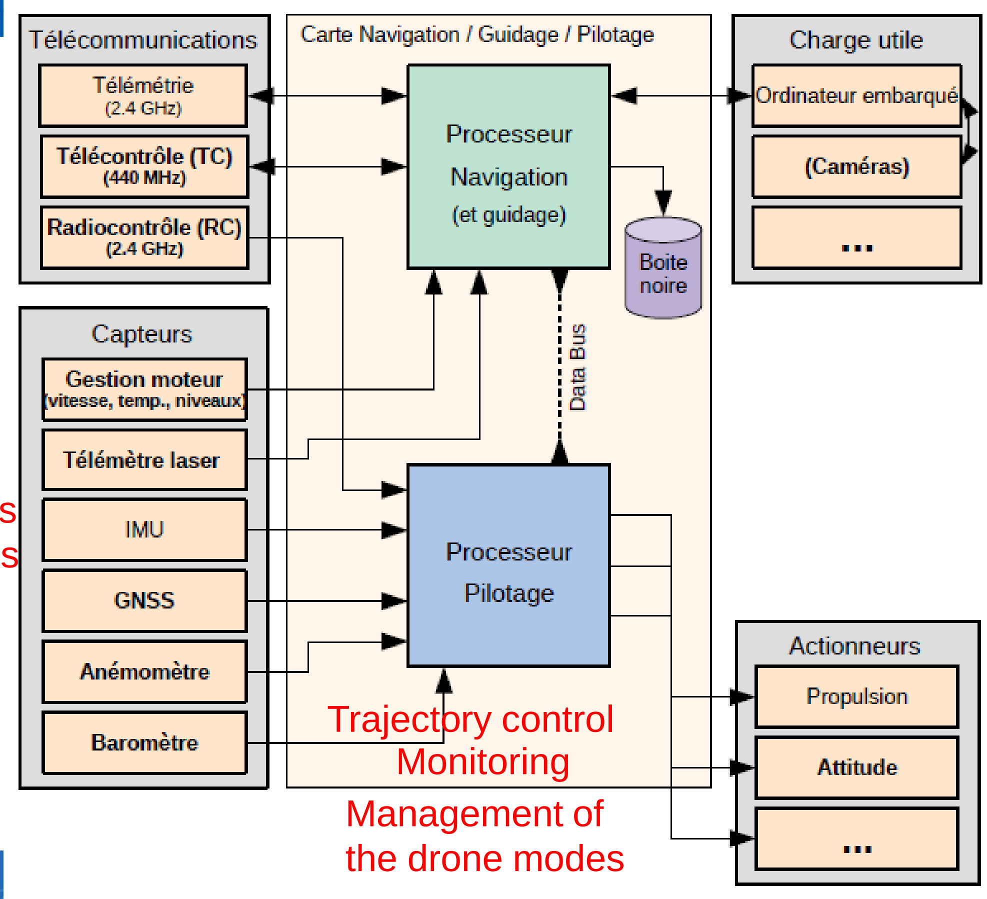
- Lack of logical details : connexions between functions, monitoring, engagement of flight control mode
- Similarity of flight modes between the 6 platforms

Example of a drone physical architecture (level 1)

C2
dow

C2
up

Parameters
acquisitions



Télécommunications

Télémétrie
(2.4 GHz)

Télécontrôle (TC)
(440 MHz)

Radiocontrôle (RC)
(2.4 GHz)

Carte Navigation / Guidage / Pilotage

Processeur
Navigation
(et guidage)

Boite
noire

Data Bus

Processeur
Pilotage

Charge utile

Ordinateur embarqué

(Caméras)

...

Capteurs

Gestion moteur
(vitesse, temp., niveaux)

Télémètre laser

IMU

GNSS

Anémomètre

Baromètre

Actionneurs

Propulsion

Attitude

...

Trajectory control
Monitoring

Management of
the drone modes

Safety review of the drone equipment

Goal

- Specify the drone equipment and their failure modes
- Specify the mapping functions - equipment
- Identify failure sets leading to CAT, HAZ, MAJ situations
- Verify safety physical requirements : probability of failure, IDAL, no CAT single failure...

Guidance

- Eurocae ED-125 – ARP 4761A recommended practices : FMEA, Fault tree, models …

Lessons learnt

- Architecture details available, lack of details about mapping between functions & equipment, lack failure rate for some components

Feedback on model validation/audit

Standard librairies of components

- Validation: review, reuse and documentation of components by at least 2 persons of the team
- Audit: short presentation of the generic components + detailed librairies guide available for interested readers

Specific components or system

- Validation: modelling hypothesis traced in the « comment » zone and overal model documentation generated by the person in charge of the study+

systematic simulation of sequences of failures+

review of sequences leading to observers

- Audit: review of pieces of code (especially monitoring and engagement logics), presentation of the model and simulation of scenario of interest