Safety assessment of the autonomous systems

DCSD

Christel.Seguin@onera.fr

ONERA

THE FRENCH AEROSPACE LAB

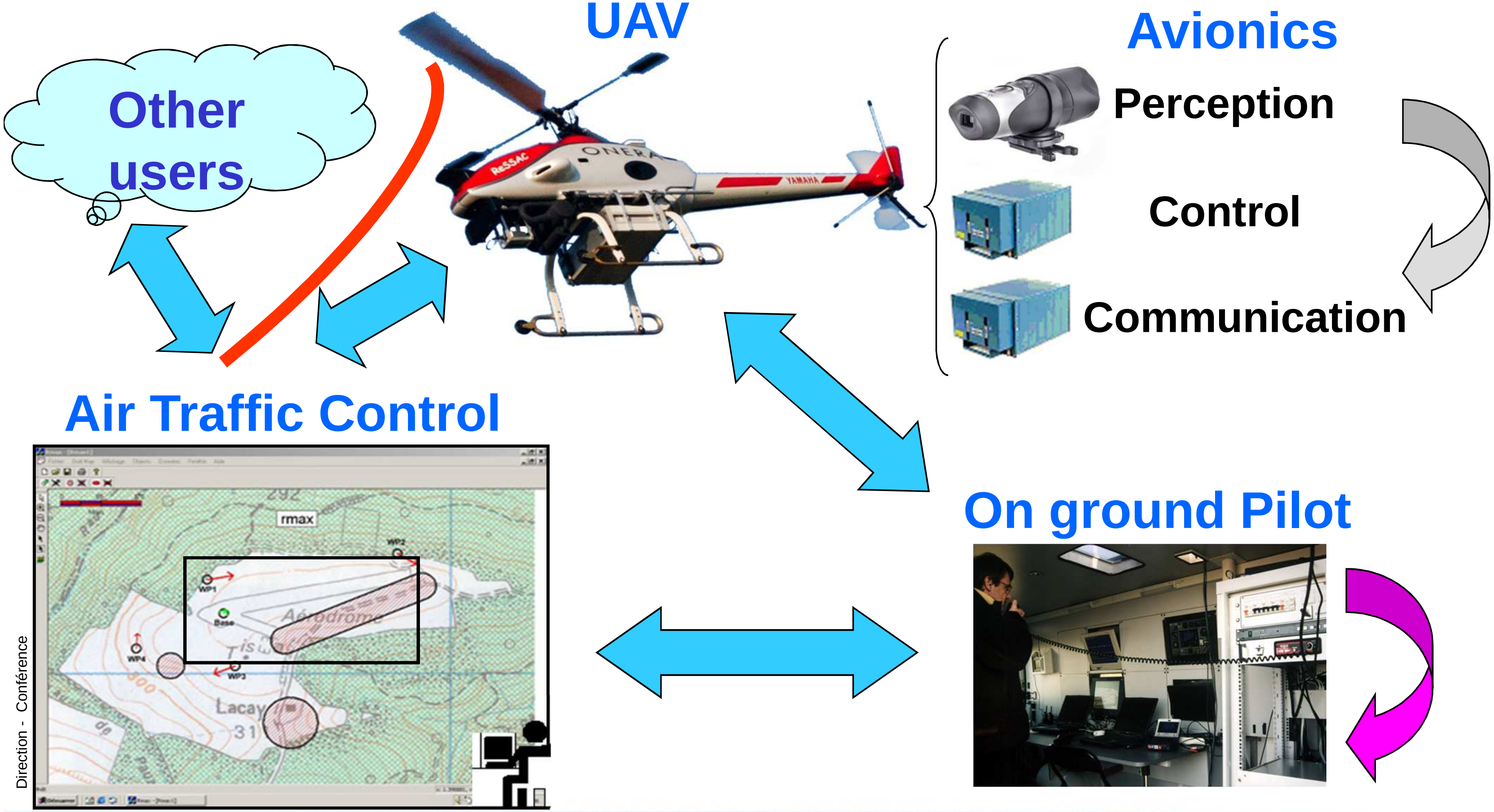
retour sur innovation

Presentation objectives

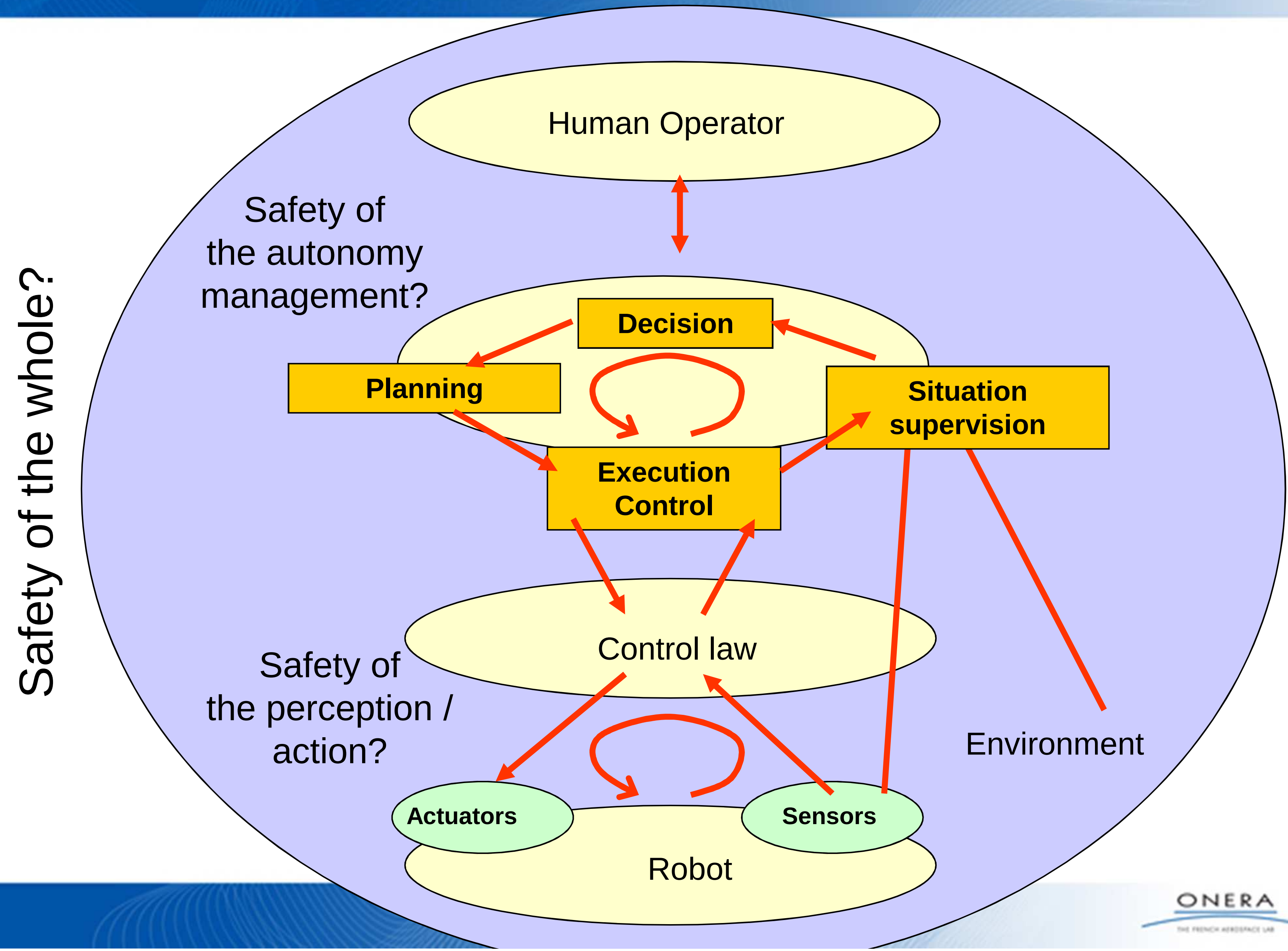
- Via an example addressed in the ONERA project IDEAS
  - UAV Insertion into General Air Traffic
- To identify the main classes of risks raised by the operation of autonomous systems
- To point out some engineering practices to limit the risks

IDEAS perimeter

- UAS : a challenging system mixing organizational, human and technical concerns



UAS: an autonomous system



Regulations impacting the insertion of UAV in General Air Traffic

- 3 pillars

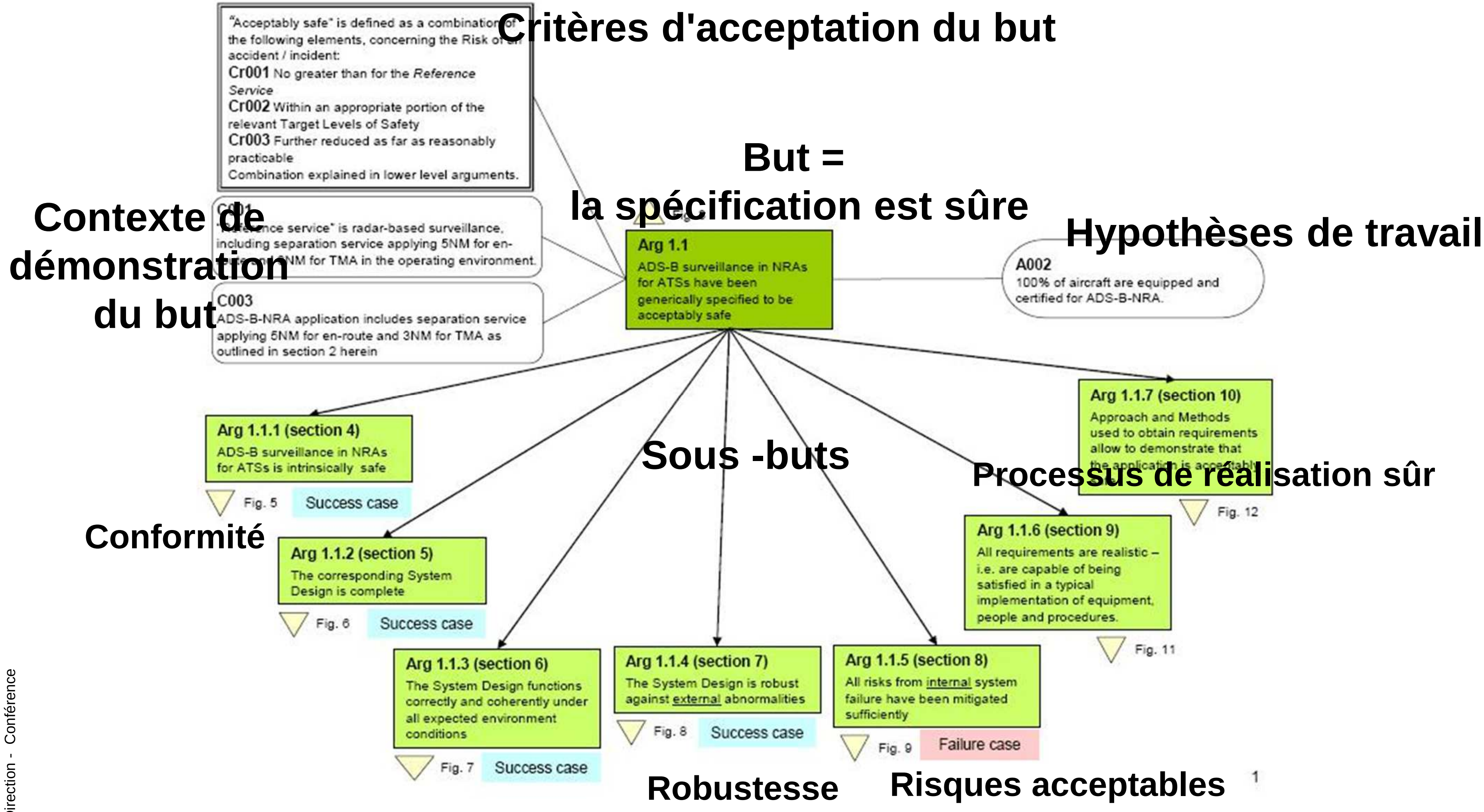
Rules of the air	Pilot licenses	Aircraft airworthiness

  - To be revisited for the insertion of UAV in General Air Traffic

Insertion scenario compatible with the rules of the air?	How to share the UAV control between ground and board ? Pilot skill?	certification of innovative avionics ?

- Difficulties:
  - A very wide scope of inter-related analyses needed to verify organizational, human and technical requirements
  - Heterogeneity of applicable certification standards
  - Instability of the regulations and wide spectrum of mission

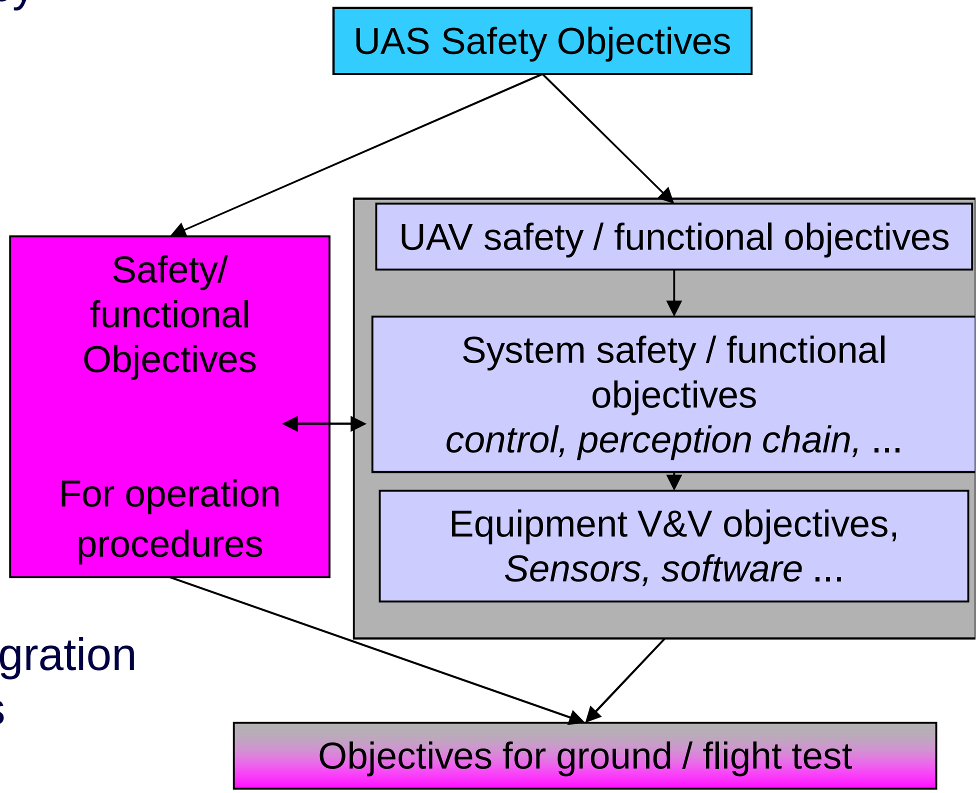
Safety Case of the A-DSB



System engineering approach to ease the safety assessment and the safety case building(1)

Idea 1 : Structure and link the safety case in the "GSN" style.

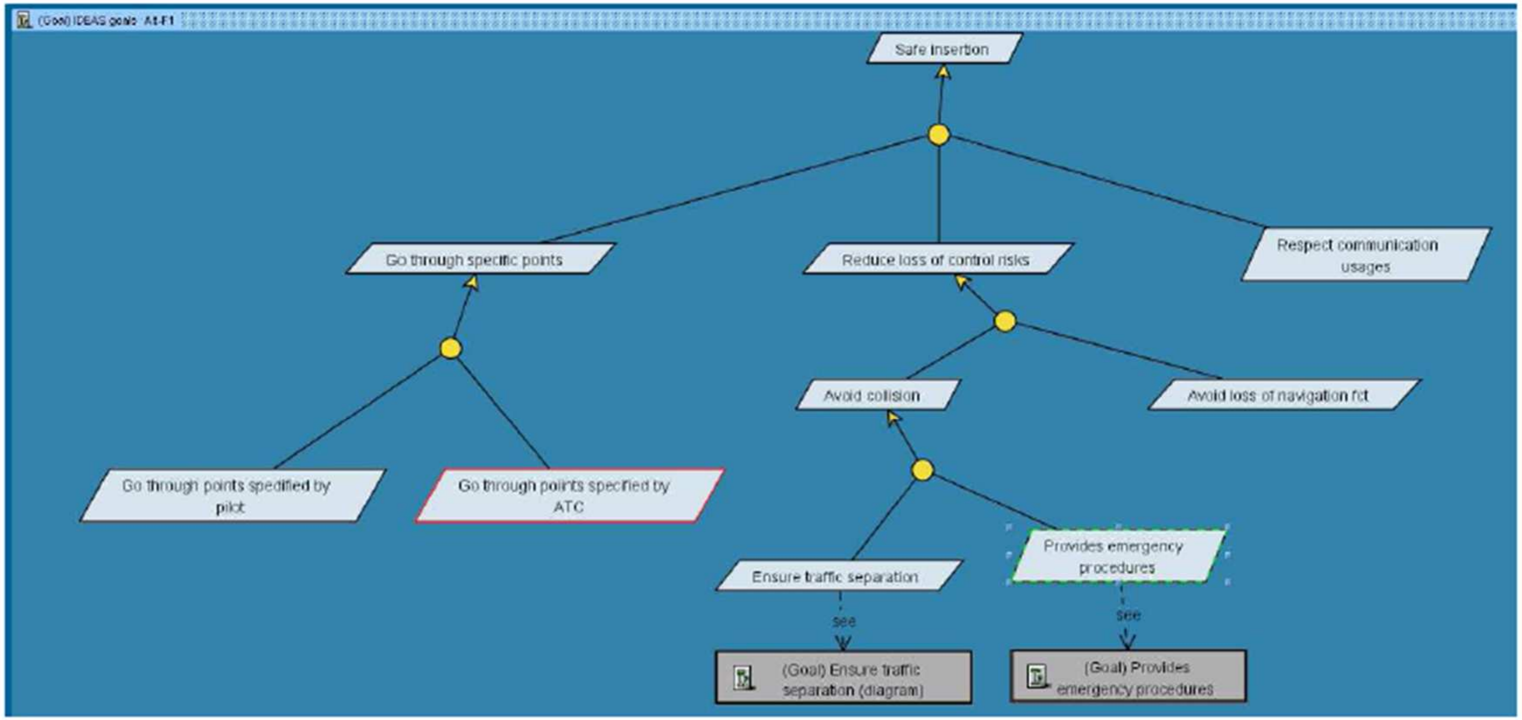
- Goal Structured Notation:
  - Defined by York University, applied by Eurocontrol
  - Safety case = a tree that
    - Decomposes the proof objectives
    - Accounting for
      - Regulations
      - System feature
- Expected Benefits = thanks to the tree like structure, master
  - Complexity by progressive decomposition of proof goal
  - Heterogeneity by homogeneous integration of proof goals extracted from various standard
  - Evolutivity by traceability tools



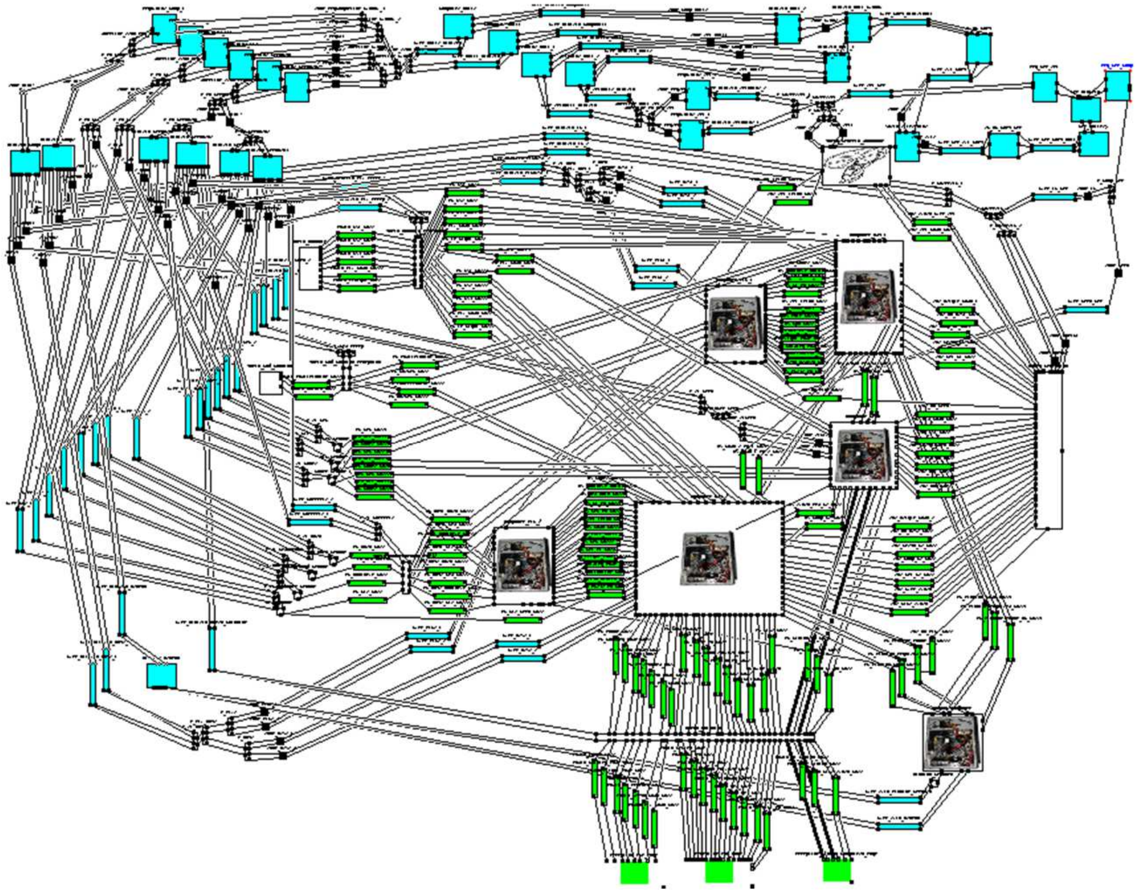
Example of goal for an UAS: reduce the risks of the loss of control

Exemple de modèle Kaos tiré d'IDEAS

Modèle des buts



On board architecture to control the Vario UAV



System engineering approach to ease the safety assessment and the safety case building (2)

Idea 2 : Use in a complementary way model driven engineering, formal proofs and (flight) tests to get the leaf of the safety case.

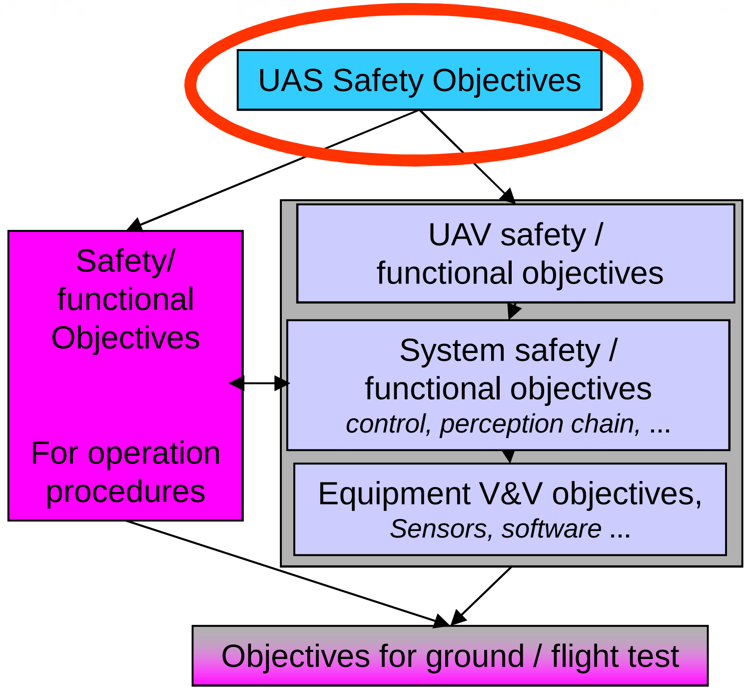
- Roles of formal models and proofs
  - Altarica models and supporting tools (ex: OCAS Dassault Aviation) for the system safety assessment :
    - UAS as a whole
    - Embedded system architecture
  - Simulink / Scade (Esterel) : V&V of the UAV flight control system and auto-pilot
  - Model-checking (probabilistic) (University of Trento / ONERA): V&V of on board planning function

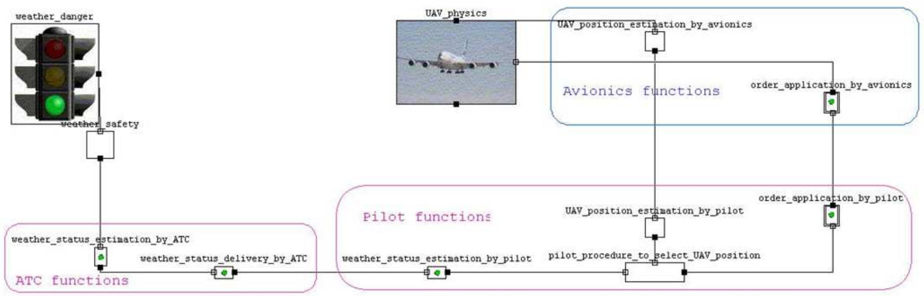
- Role of (flight) test
  - Calibration of models
  - Validation of the system performances

- Expected benefits
  - Find problems earlier in the design process thanks to rapid and formal prototyping
  - Update quickly the safety case after design change thanks to the automation of the analysis

Goal examples and formal assessment techniques: Preliminary Safety Assessment of the Role Sharing

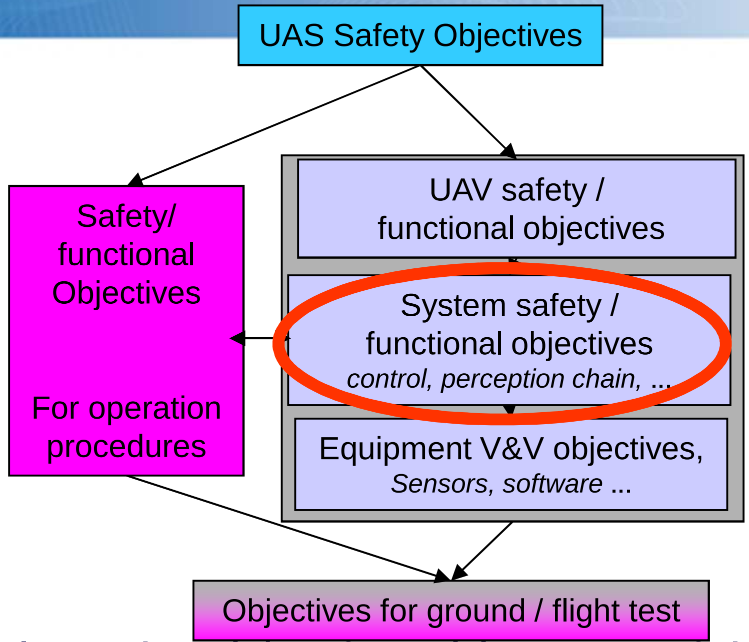
- Goal ex: proof the acceptability of the loss of the UAV control for all conditions of UAS operation
  - 1: No single failure shall lead to the UAV control loss in case of adverse weather
  - 2: The occurrence probability of the UAV control loss shall be less than 10^{-X} /F H



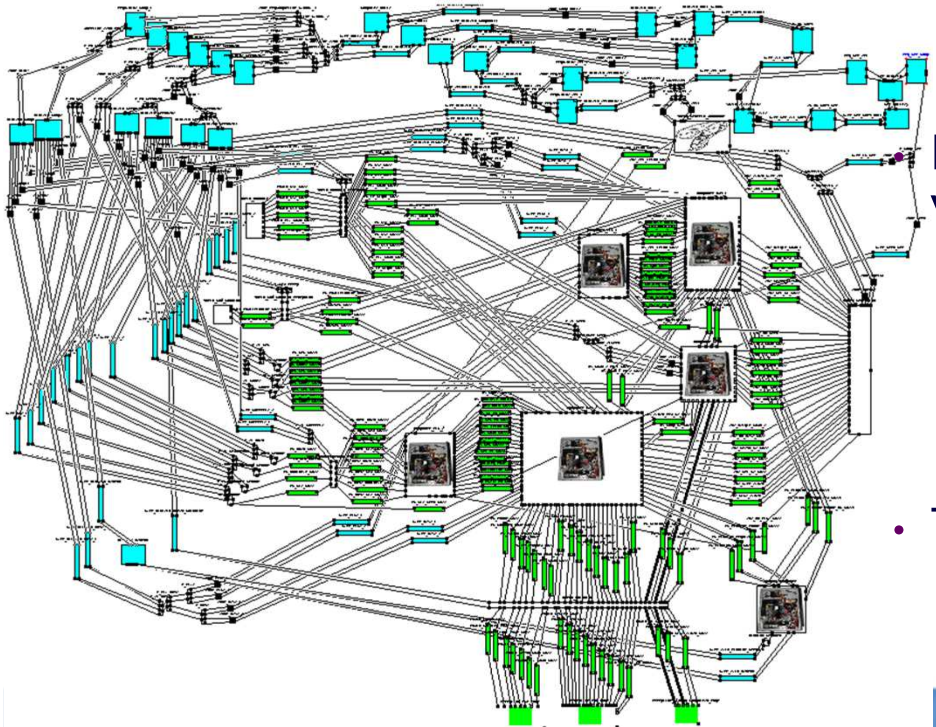


- Model ex : operation in adverse weather condition
  - discrete variables / discrete events model
  - to specify the communications between ATC, UAV pilot and the UAV
- Tool used: Cecilia OCAS (Dassault Aviation) for AltaRica models

Goal examples and formal assessment techniques: Preliminary Safety Assessment of the UAV architecture and supervisor

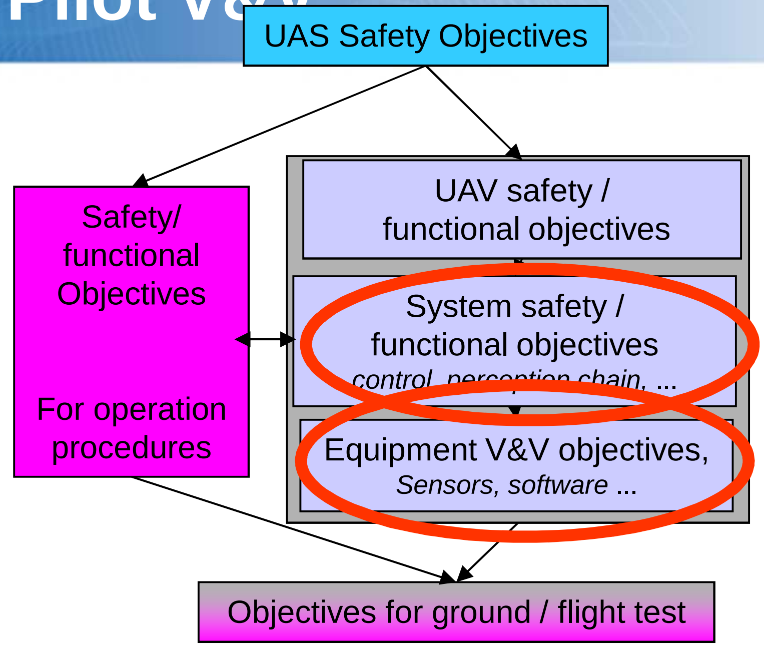


- Goal ex: proof the acceptability of the loss of the UAV control
  - 1: No single failure shall lead to the UAV control loss
  - 2: The occurrence probability of the UAV control loss shall be less than 10^{-X} /F H

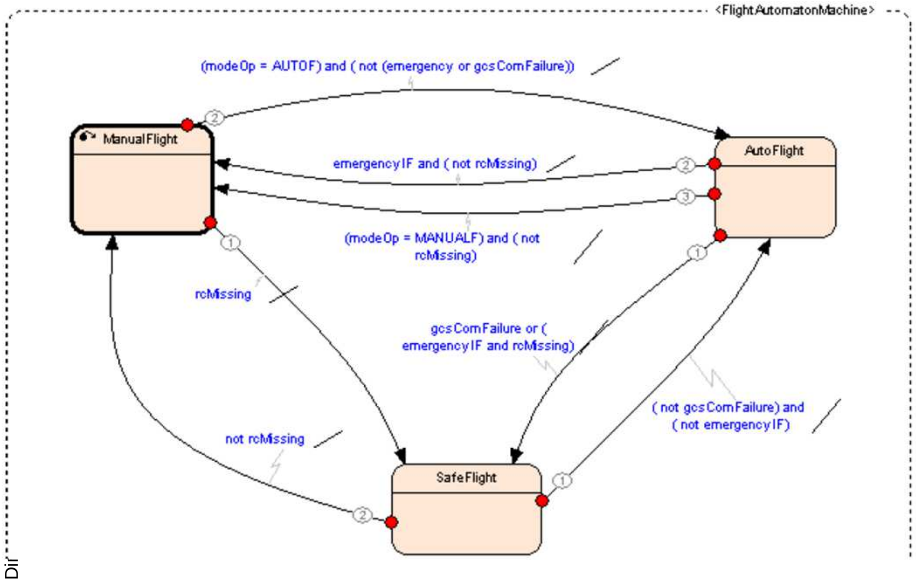


- Model ex : hard / soft architecture of the Vario UAV
  - High combination of discrete variables : ~ 1500 failures for 1000 components linked via 5500 variables
  - Discrete time detection and reconfiguration
- Tools used: for AltaRica models
  - Cecilia OCAS (Dassault Aviation)
  - + ONERA tools (MISSA, ATMOST projects)

Goal examples and formal assessment techniques: Supervision and Automated Pilot V&V



- Goal ex: verification of functional requirement
  - 1 The specification of the helicopter control law ensures that:
    - If the data link with the ground is loss then the control mode "Safe"
  - 2 The embedded software is compliant with this specification



Model ex: Vario Automated Pilot

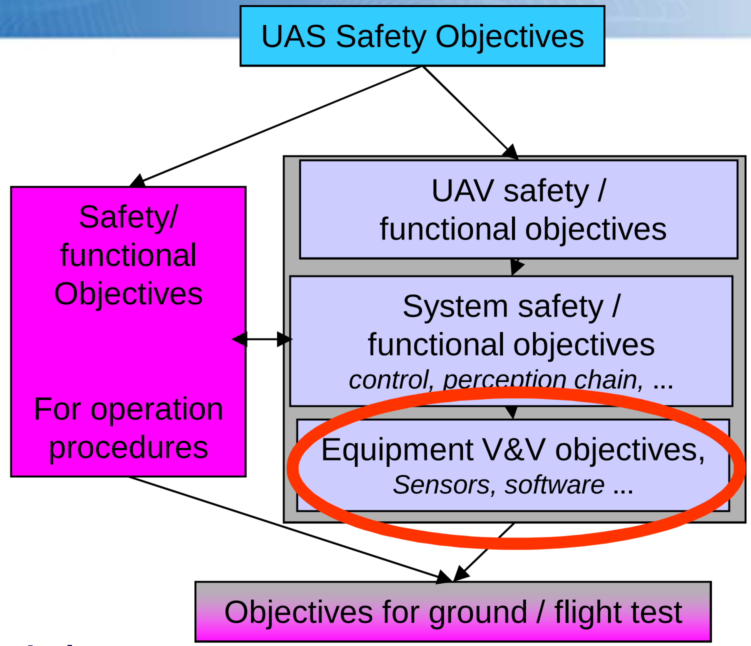
- Mode automata +
- Discretized control laws

Esterel tools used for Scade 6 models:

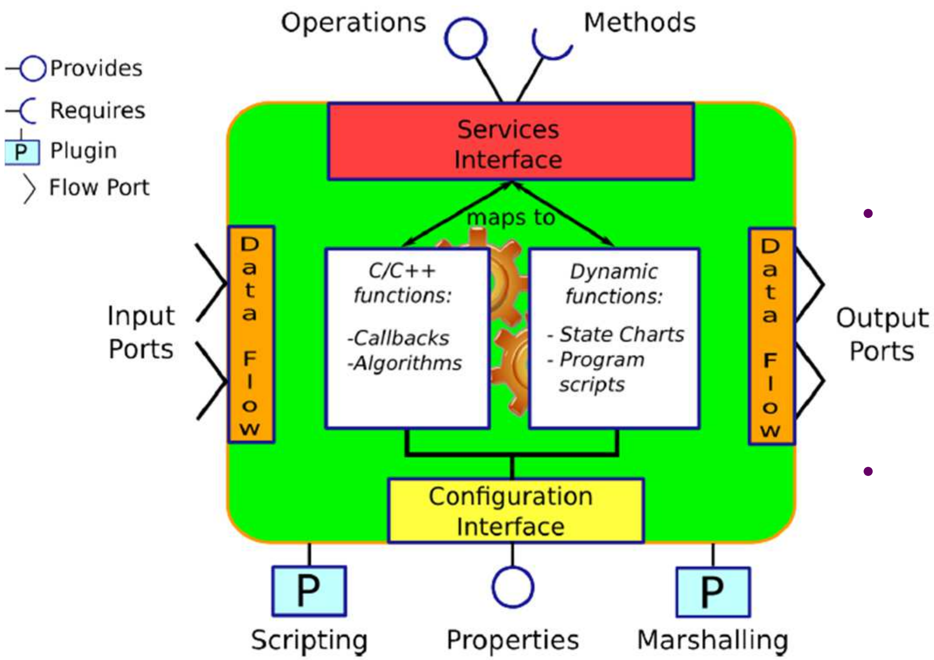
- Proof of the specification with the design verifier tool
- Code automatically generated from the specification

ONERA

Goal example and formal assessment techniques: Software schedulability and Real Time Verification

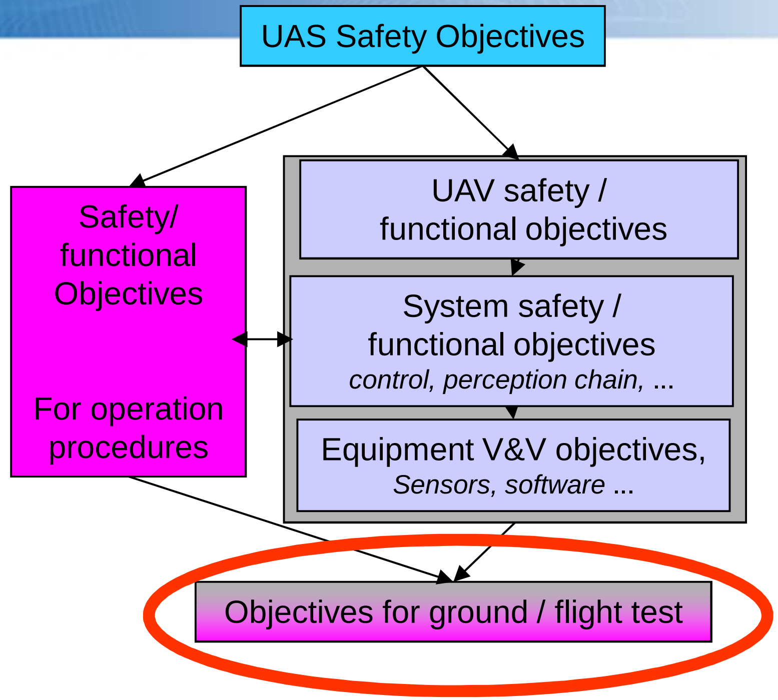


- Goal ex: verification of real time requirements
  - The execution of each atomic software task does not exceed a worst case time
  - All the tasks can be scheduled on the computer

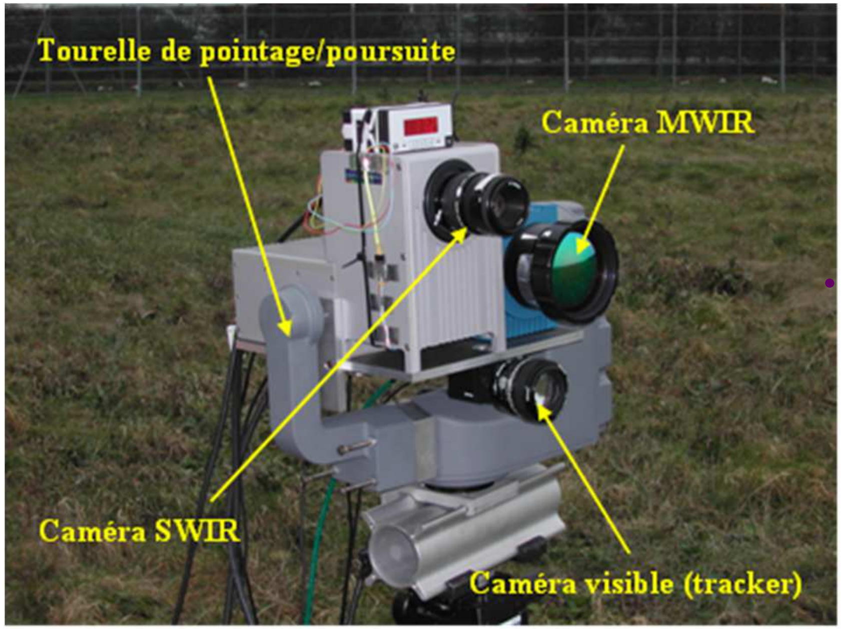


- Model ex: OROCOS component
  - C/C++ code / Finite state machines
  - + interfaces to manage accurately the software execution
- Tools used:
  - OROCOS Real Time Toolkit
  - MAUVE DSL for OROCOS
  - OTAWA for worst case time execution

Goal example and related test : Verification of the performances of the "sense and avoid"



- Goal ex :
  - The perception chain can detect any significant kind of intruder aircrafts in various atmospheric conditions
  - Characterize "significant intruders"



- Characterization approach
  - Method: phenomenological study
  - Mean: measures of IR signature of non cooperative targets with known background (sky) and environment (mountain)

Conclusion

- Presentation of a safety case
  - For an aeronautical system including a "flying robot" (the UAV)
  - Compatible with aeronautical standards (ARP 4754A 4761, DO 178C)
- Some key points
  - Accurate knowledge of the robot operation and environment is requested to start soundly the classification of the risks
  - The work sharing between human and robot shall be carefully analyzed
  - The criticality of each piece of the system depends on the piece function and the availability of means to mitigate the piece failures (redundancies, backup procedures or ressources...)
    - Planning is used in our case only for optimizing the trajectory
    - It can be integrated safely in a software architecture that masters rigoursly the run-time execution
  - Use of numerical simulation, formal methods ... helps to increase the confidence early during the design
    tests are also mandatory to characterize the system inputs
- Approach compatible for other domains ?
  - At least with other transport and space standards

Some ONERA related studies

- New air traffic control procedures and UAV:
  - European Project INOUI (2008-2012)
- Autonomous avionics
  - ONERA project ReSSAC (2002-2007)
  - DGA PEA Action (2006-2012)
  - ONERA project IDEAS (2009 – 2012)
  - ANR MAUVE
- Human factors studies
  - PAUSA project
- Safety assessment methods for complex systems
  - European project ISAAC (2004-2007)
  - European project MISSA (2008-2011)
- Safety critical software V&V
  - European project ES-PASS (2007-2009)
  - ANR SIESTA (2008–2010)