ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

ONERA
THE FRENCH AEROSPACE LAB

New approaches for the certification of AI based systems in civil aeronautics

Université Fédérale
Toulouse Midi-Pyrénées

Chair members

Claire Pagetti

Real-time systems, certification, safety

Kevin Delmas

Safety, SAT/SMT, design space exploration

Jérémie Guiochet

Safety, run-time verification, test

Charles Lesire-Cabaniols

Robotics, autonomous systems, AI-based planning

Aurélien Plyer

computer based vision, visual odometry, deep learning

Context: certification activities

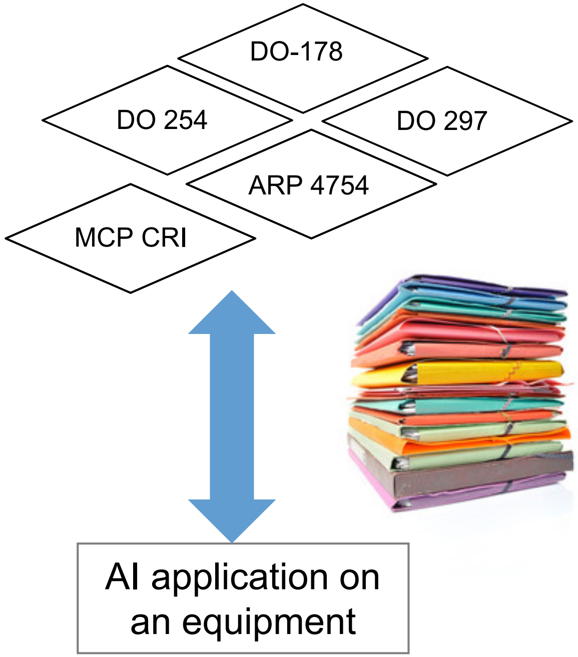
Certification:

- evaluation of an **argumentation**, to convince that a system (i.e., its architecture, its settings, including mitigation means. . .) satisfies **certification objectives** (expressed with AMC standards)

Difficulties :

- Existing standards are inapplicable [BCM+15]
- Importance of training/test/validation sets
- Confidence of an output
- How to provide redundancy
- etc.

[BCM+15] Siddhartha Bhattacharyya, Darren Cofer, David J.Musliner, Joseph Mueller, and Eric Engstrom. Certification considerations for adaptive systems. Technical Report NASA, 2015



DO-178

DO 254

DO 297

ARP 4754

MCP CRI

AI application on an equipment

Objectives

Research axes

- **Safety:**
  - Definition of hazards, dedicated safety methods
  - Run-time mechanisms
- **Programming framework (with real-time and certif in mind):**
  - Adequate low level programming
  - COTS hardware selection / assessment
- In the end: proposal for **certification objectives**
  - Participation to aeronautic standardization group at EUROCAE

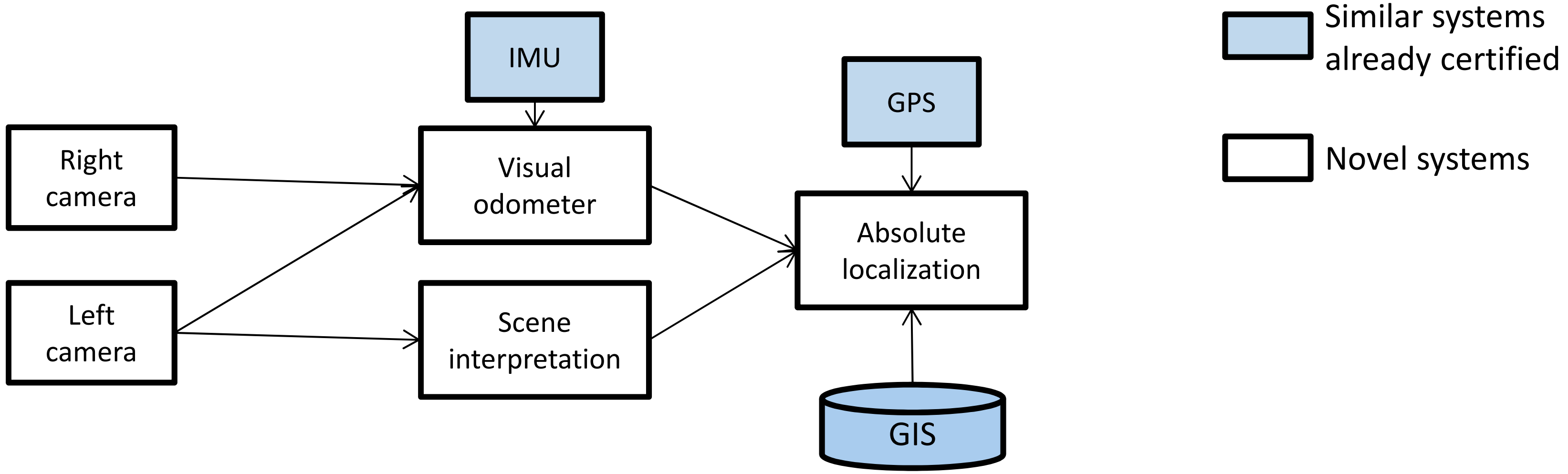
Supporting use case

- Computer vision-based

Outline

- General presentation
- Some results
  - Scientific results: SUPER / PHYDIAS projects
    - Use case
    - Beginning of safety assessment
  - Related works
  - Planned PhD / post doc proposals
- ANITI overview
  - Your vision of full ANITI project
  - Your vision of your interaction with other chairs
  - Your vision with your interaction with industrial

SUPER project



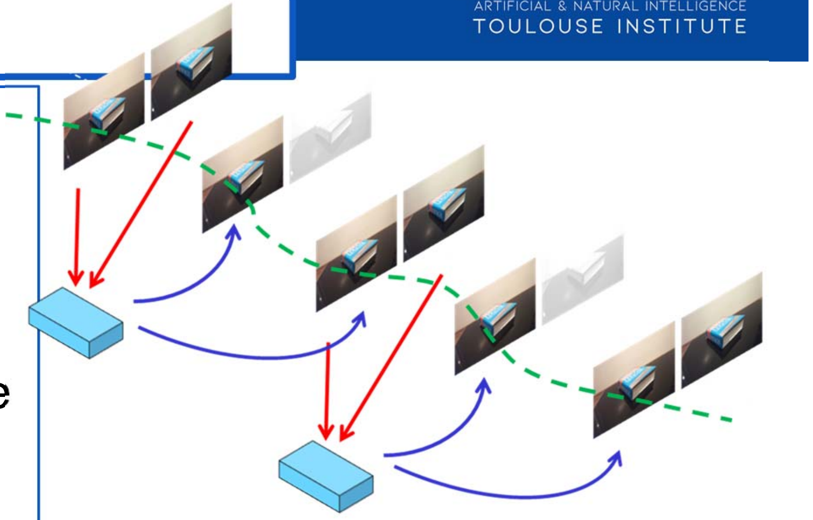
- **Geographic information system (GIS)**: certified data base with detailed airport maps
- **Visual Odometer (VO)**: estimate the trajectory (position and orientation) with respect to some relative reference coordinate system.
- **Scene Interpretation (SI)**: build a description of the scene
- **Absolute localization (AL)**: estimate the absolute position in the airport by fusing several information

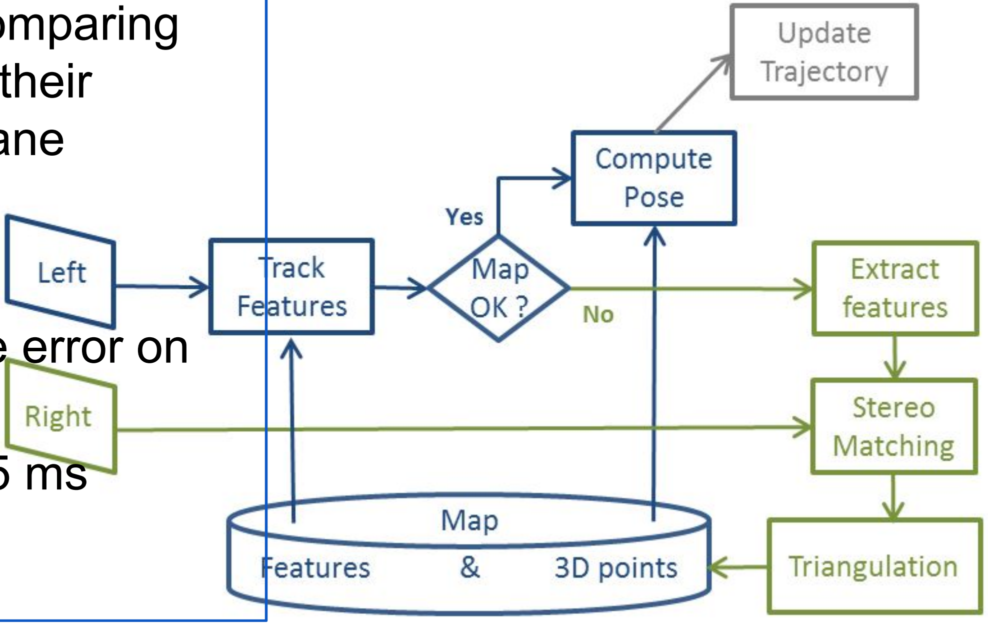
Visual Odometer (VO)

Ego-motion from the sequence of images

eVO (efficient Visual Odometer)

- Extraction of landmarks (not necessarily the same as GIS)
- Tracking of landmarks during motion (they are assumed to be fixed)
- Pose (position and orientation) of the current left camera can be computed by comparing the 3D positions of landmarks and their current localization in the image plane
- Features:
  - Covariance estimation of the error on the computed pose
  - pose computation 20 Hz / 15 ms
  - map building 1Hz / 55 ms

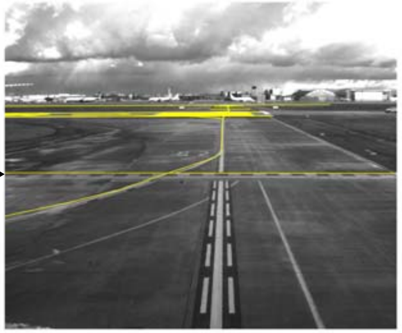




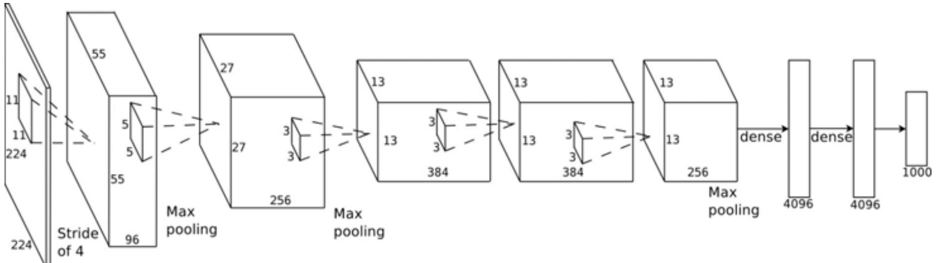
Scene Interpretation (SI)

(image Airbus)

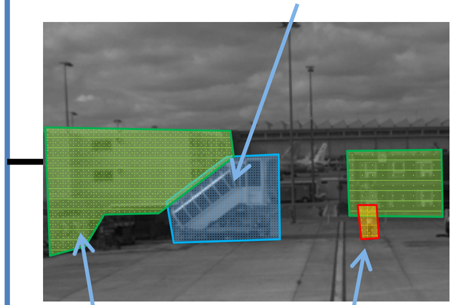
Machine Learning for detection of lane, horizontal marking, signposts, etc



(image Airbus)



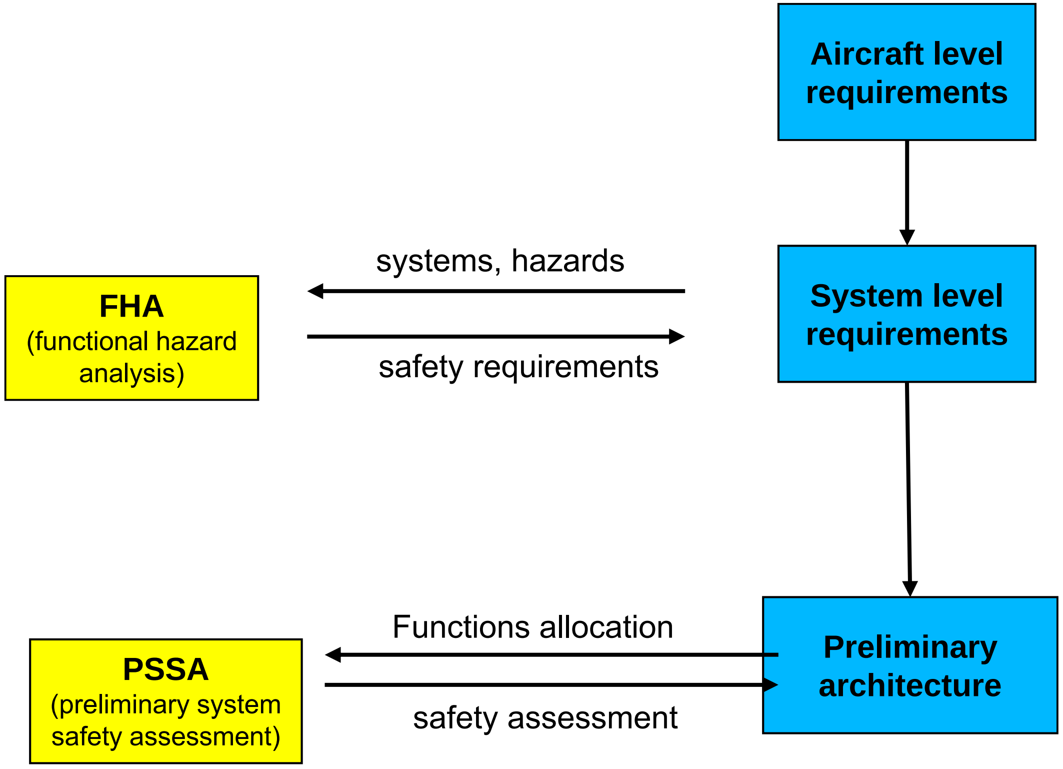
Deep Convolutional Neural Network for scene interpretation



Same landmarks as GIS

Reminder

ARP 4754 defines a safety process to run in parallel with the development process



Aircraft level requirements

System level requirements

Preliminary architecture

FHA (functional hazard analysis)

PSSA (preliminary system safety assessment)

Example

FHA analysis on Absolute Localization

- FC = "the function provides a wrong position without the error being detected".
- Hazardous (FC occurs → collision with other vehicles or people)
  - No single failure should lead to FC
  - Proba FC ≤ 10^{-7} FH

PSSA: Dysfunctional model:

- Identification of components
- Identification for each component of failure modes, failure events and associated probability
- Definition of failure propagations
- MBSA, e.g. with AltaRica

Hypothesis:

- Hardware failures and systematic failure (i.e. software bugs) are covered by existing safety process

VO

- **2 failures modes**
  - Loss: no pose estimation or error covariance high
  - Err: wrong pose estimation with low error covariance

- **External events / hazards**
  - Vision hazards [ZMH+17]: Illumination (low illumination ➔ low contrast); propagation conditions (e.g. smoke, haze); camera settings (e.g. aperture)…
  - unreliable contrasted edges between illuminated areas and shadows
  - reflections related to water surface
  - large sudden rotation motion of the camera
  - TBC

[ZMH+17] Oliver Zendel, Markus Murschitz, Martin Humenberger, and Wolfgang Herzner. How good is my test data? introducing safety analysis for computer vision. International Journal of Computer Vision, 125(1-3):95–109, 2017.

VO associated hazards

Even in the absence of adverse condition, VO may reach the erroneous failure mode ➔ new type of hazard

Algorithm associated hazards

- non deterministic divergence of internal random solvers
- confusing scene (e.g. when someone sees the train on the track next to his own that starts and feels like he’s going in the opposite direction)
- structural inconsistency related to the non linearity
- TBC

Next steps:

- Complete list
- Associate probability
- Link with failure modes

ANITI environment – DEEL Mission Certif

Contributors: Eric Jenn[1], Alexandre Albore[1], Franck Mamalet[1], Grégory Flandin[1], Christophe Gabreau[2], Hervé Delseny[2], Hugues Bonnin[3], Lucian Alecu[3], Jérémy Pirard [3], Baptiste Lefevre[4], Jean-Marc Gabriel[5], Adrien Gauffriau[2], Cyril Cappi[6], Laurent Gardès[6], Sylvaine Picard[7], Gilles Dulon[7], Brice Beltran[8], Jean-Christophe Bianic[9], Mathieu Damour[9], Claire Pagetti[10], Kevin Delmas[10]

[1] IRT Saint Exupéry, first.last@irt-saintexupery.com, [2] AIRBUS SAS, first.last@airbus.com,
[3] Continental, first.last@continental-corporation.com, [4] Thales, first.last@fr.thalesgroup.com,
[5] Renault Software Labs, first.last@renault.com, [6] SNCF, first.last@sncf.fr,
[7] SAFRAN, first.last@safrangroup.com, [8] DGA, first.last@intradef.gouv.fr,
[9] SCALIAN, first.last@scalian.com, [10] ONERA, first.last@onera.fr

Objective: identify the main challenges for placing a justifiable confidence on systems embedding ML and, eventually, certify such systems.

EUROCAE WG114

Kick off August 26 2019

Objective:

- **prepare technical standards, guides and any other material required to support the development of systems and the certification of aeronautical systems implementing AI-technologies.**

ANITI
ARTIFICIAL & NATURAL INTELLIGENCE
TOULOUSE INSTITUTE

« Chantier RTRA »: animation activities (workshops, seminars, master internship grants. Leader: Jérémie Guiochet

https://www.laas.fr/projects/trustmeia/

Topics

- Decision making under uncertainty and incompleteness : probabilistic and non-probabilistic approaches
- Validation and verification, confidence estimation and certification (formal methods for expression and verification of requirements, testing, simulation, assurance cases, etc.)
- New software architectures for safe autonomous systems (integrity levels, isolation in intelligence architectures, runtime verification, monitoring)
- Transparency and explainability of perception, inference, actions
- Security and autonomous systems
- Legal, ethical, societal aspects, superintelligence issues

ANITI overview

Your vision of full ANITI project

- « plateau » for collaboration
- Regular seminars and lectures between researchers / industrials / students

Interaction with other chairs:

- Theoretical results as inputs for certification and back for pushing towards particular research
- Works needing certification (R. Alami, F. Dehais, N. Mansard …)
- Leila Amgoud: assurance cases and argumentation
- Céline Castets-Renard: legal issues
- Bruno Jullien: common understanding approach
- Daniel Delahaye: fault tolerant drone