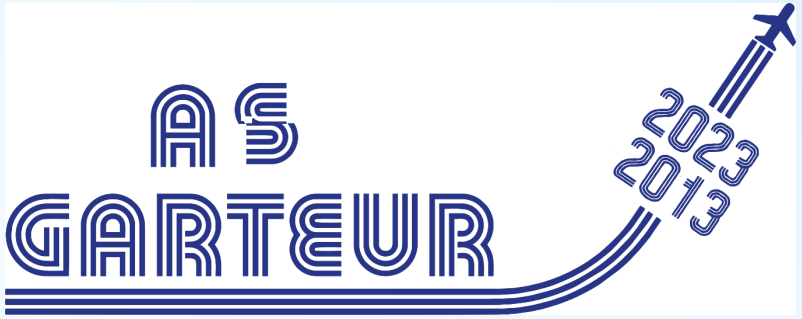
Aviation Security

Highlights of Key Themes and Impact

Pierre BIEBER, ONERA

Aviation Security GoR 10th Anniversary (*almost*)



- 2013 : Activities discussed
- March 2014 : AS GoR launched
- 2015-17 : Aviation Security White Paper & Engagement with Stakeholders
- 2019-22 : Action Group & SESAR project on the Protection of Aiports against unauthorized drones

4 Themes

Aviation Security = Safeguarding civil aviation against acts of unlawful interference (ICAO)

Laser Dazzling

Chemical, Biological & Explosive detection

Cybersecurity

Malevolent use of drones

Both Physical and Digital interferences are considered

Innovative Detection and Mitigation means are investigated

Partners

Participants

- CIRA
- DLR
- FOI
- Fraunhofer
- INTA
- NLR
- ONERA

If you wish to contribute to the group do not hesitate to contact one of us !

Angela Vozella, CIRA A.Vozella@cira.it

Pierre Bieber, ONERA Pierre.Bieber@onera.fr

Tim Stelkens-Kobsch, DLR Tim.Stelkens-Kobsch@dlr.de

White Paper & Stakeholder Engagement

Aviation Security White Paper

- Definition of Research Priorities for the 4 themes

Consistent with other initiatives

- ACARE Strategic Research & Innovation Agenda – WG 4 on Safety & Security
- EREA Security for Aviation White Paper

Workshops

Two GARTEUR AS GoR workshops

- 2016 : Toulouse, 2017 : Rome
- 15 stakeholders participated

OPTICS2 Workshops :

- 2018 @EASA : Cybersecurity, Data Analysis

Action Group

Top priorities

- **Malevolent drones near the airport** (Gatwick drone incident, 2018)
- **AI and Aviation Security**

Action Group on Drones and cybersecurity

- Technical work on the identification of cyber-threats applicable to drones
- Several joint proposals to EU calls
- SESAR Exploratory Research 2019 call : **ASPRID** selected !

  GARTEUR Partners : CIRA, INTA & ONERA + AENA, ENAIRE, ALI, SOUL software

ASPRID Project – Context & Goal

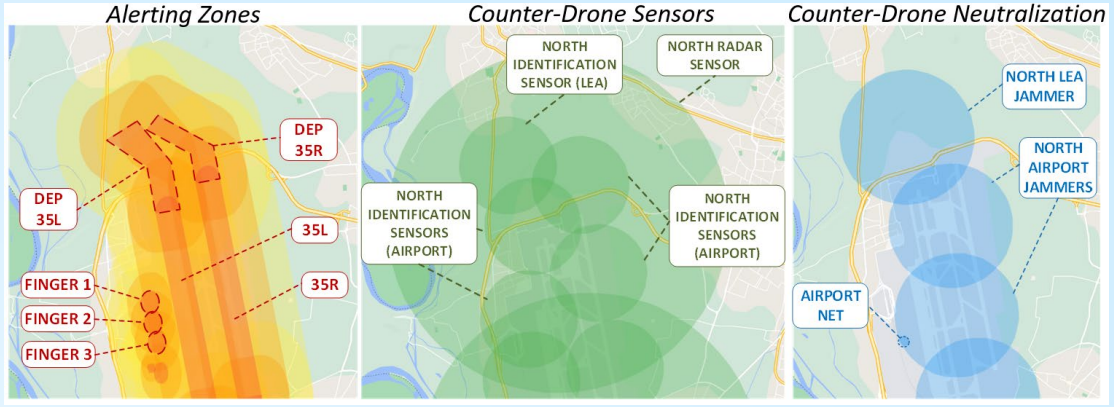
- Drone intrusions in airports are incrementing and causing major disruptions
- EASA has published a *counter-drone action plan* advocating the development of Drone Intrusion Management.

- ASPRID investigated a **Drone Intrusion Management System**
  - situational awareness about drone intrusions
  - dynamic assessment of their risks
  - new procedures and protocols to manage the intrusions

  in order to ensure the resilience of airport operations

ASPRID Project – Main Achievements -1

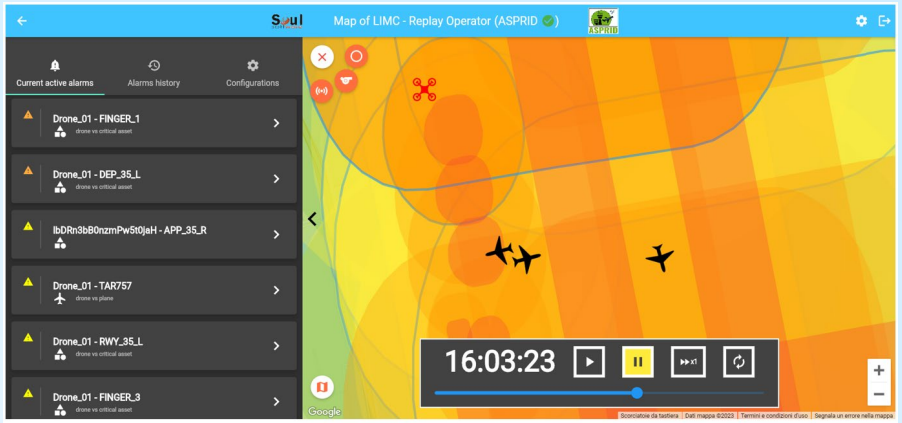
- Risk Assessment
  - Airport Vulnerability Index for Drone Intrusions
  - Drone Intrusion Management Evaluation
- Operational Concept
  - Roles of Air Traffic Controllers, Airport ASPRID Operator, Law Enforcement Agency



Triggering Condition	ASPRID Operator Action	Controller Action
White infringement of unauthorized drone	① Monitor the object (periodic monitoring) ② Keep the controller updated about the evolution of object's trajectory (significant updates)	No actions
Yellow infringement of unauthorized drone	① Inform the controller ② Monitor the object (continuous monitoring) ③ Keep the controller updated about drone's trajectory and features, e.g., speed, model, etc. (continuous update)	① Move/redirect aircraft to keep them far from the infringed zone (e.g., use another runway for taxiing or take-off)
Orange infringement of unauthorized drone	As above	① Stop aircraft in nearby zones
Red infringement of unauthorized drone	As above	① Stop all airport operations
Available countermeasure to neutralize an unauthorized drone	① Ask the controller to confirm the neutralization action ② If the controller confirms the neutralization action, issue neutralization command ③ Inform the controller about the neutralization result ④ Repeat in case of failed neutralization	① Check that there are no moving aircraft close to the neutralization area (close to the drone) ② Inform ASPRID operator about the previous check

ASPRID Project -Main Achievements -2

- Resilience Assessment
  - Real-Time Simulation Platform
  - Applied to Malpensa Airport
  - Gaming Exercise with Air Traffic Controllers, Airport Managers and Guardia Civil Officers.



- 5 scientific publications were written by the ASPRID team.

Conclusions

- Participation to GARTEUR Exploratory/Action Group is a nice way to progress scientifically and build funded projects.

- Ideas for new Action Groups :
  - Follow-up activities : AI and cybersecurity, coordinated security threats
  - New ideas, especially in the dazzling and CBE detection topics, are welcome !