33RD CONGRESS
OF THE INTERNATIONAL COUNCIL
OF THE AERONAUTICAL SCIENCES
STOCKHOLM, SWEDEN, 4–9 SEPTEMBER, 2022

ICAS 2022 SWEDEN

# AVIATION SECURITY CONCERNS

Angela Vozella[1], Pierre Bieber[2]

[1]CIRA
[2]ONERA

## Abstract

This paper gives an overview of aviation security concerns which are of greater interest for future research activities. Since its creation, GARTEUR Aviation Security GoR has been investigating two important topics: cybersecurity and malevolent drones. More recently, two new high priority topics appeared: Artificial Intelligence/Machine Learning contribution to aviation security and Harmonization of security and safety risk assessment and management. These topics were identified thanks to a review of Aviation Strategic Research Agendas.

**Keywords:** security, cybersecurity, safety, certification, drone, counter-drone

## 1. Introduction

The Group for Aeronautical Research and Technology in Europe (GARTEUR) Group of Responsables (GoR) on Aviation Security (AS) was created during the GARTEUR Council meeting in March 2014. This GoR is composed of specialists from Research Establishments and Industry who have identified relevant topics to be studied in the Aviation Security area. GoR AS pursues to do research in the Aviation Security field dealing with both military and civil R&T.

Aviation security aims to prevent acts of unlawful interference, above all by keeping threatening items such as arms and explosives away from aircraft. It became a major cause for concern following the terrorist attacks of September 2001. Since then, the regulatory framework in this field has expanded worldwide, whether nationally, or via international cooperation/agreements, or through the International Civil Aviation Organization.

An important aviation security concern that was discussed by GARTEUR AS GoR is **aviation cybersecurity**. The latest aircraft rely on interconnected systems which extend off the aircraft to ground-based systems run by airlines, airports and Aviation Service providers of various types. With the fast and rapid integration of new technologies, the aviation assets keep changing and becoming interconnected. The introduction of new technologies and interconnection of systems introduce new vulnerabilities. Without the appropriate security measures in place, the air transport system may be at risk. Special attention is therefore due to this complex problem.

Another aviation security concern discussed by GARTEUR AS GoR is represented by **malevolent use of drones** (a.k.a Remotely Piloted Aircraft Systems (RPAS) and/or Unmanned Aerial Systems (UAS)). They represent a reality in the airspace thanks to their integration into non-segregated airspace (thanks, among others, to EU drone roadmap). This opens the airspace not only to security applications but also to a wide number of particular, private, leisure and commercial ones. Many small and low cost systems (some hundred Euros) such as autonomous model aircrafts or micro/mini RPAS/UAS are currently being flown in cities or in the surrounding of airports potentially increasing the risk of collisions with other aircraft, people or infrastructure on ground. Thus an important effort in risk management has to be put to face with this risky scenario.

More recently, thanks to the review of Strategic Research Agenda and of main findings of the OPTICS2 project new topics were identified.

The first new topic is related with the **harmonization of Security and Safety**. Though these two concerns have historically followed two different paths and dynamics, they are intrinsically interdependent and nowadays there is a common understanding about the need to harmonize them by design. Aviation is the safest form of long-distance transport. In 2018, the all accident rate (measured in accidents per 1 million flights) was 1.35, which was the equivalent of one accident for every 740,000 flights. This was an improvement over the all accident rate of 1.79 for the previous 5-year period (2013-2017). It is thus very important to that new security threats do not decrease aviation safety.

The second new topic is related with the **contribution of Artificial Intelligence/Machine Learning for security risk management**. This new technology combined with the capability to collect vast amount of aviation data is an enabler for advanced threat detection and mitigation means. But if the collected data is not properly protected, this could also be viewed as a new Aviation Security threat.

This paper gives an overview of these four areas which are of greater interest for future research. Specifically: paragraph 2.1 will introduce a summary of ACARE security goals and ACARE Strategic Research Agendas, paragraph 2.2 will deal with OPTICS2 main findings,;.Finally chapter 3 will describe some hot topics as derived by this analysis in terms of challenges and current development.

## 2. Review of Strategic Research and Innovation Agendas

### 2.1 ACARE Strategic Research and Innovations Agenda

In 2011 a European group of stakeholders from the aviation domain defined a vision of European aviation with the publication of Flightpath2050 which identifies ambitious goals [1]. Flightpath Security goals are:

- *Boarding and security checks allow seamless security for global travel, Passengers and cargo pass through security screening without intrusion,*
- *Air vehicles are resilient by design to aerial and ground security threats,*
- *The air transport system has a fully secured global high bandwidth data network, hardened and resilient by design to cyber-attacks*

To reach those goals, the Advisory Council for Aviation Research and Innovation in Europe, ACARE produced a first issue of the Strategic Research and Innovation Agenda (SRIA) in 2012 depicting the specific path with achievements over the reference time frame. Such a roadmap is periodically updated according to maturation of technology and external scenario changes affecting aviation directly and indirectly. A second updated issue of the SRIA was published in 2017 [2]. It has become a driver for the implementation of research and the evolution of work program for European aviation research. Safety and security research in aviation had a dedicated chapter of the SRIA with specific action areas.

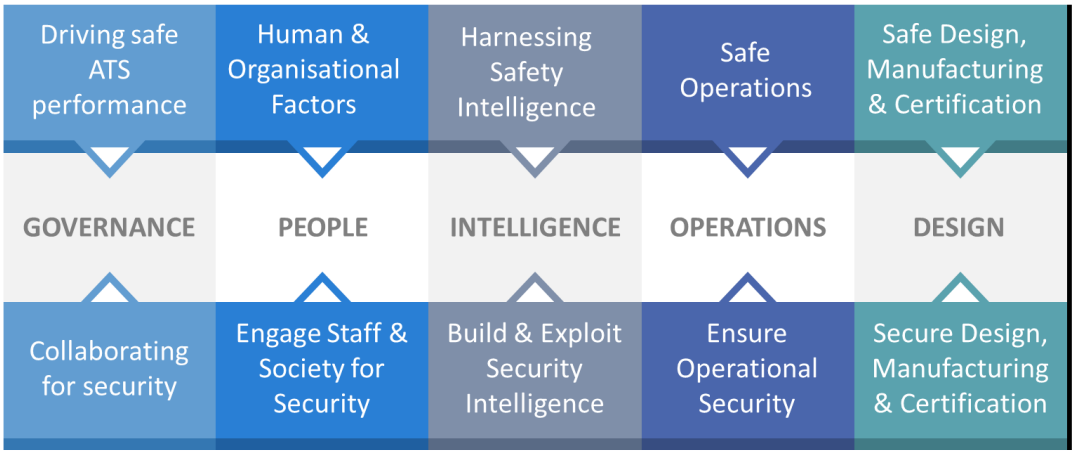


Figure 1 – ACARE Safety and Security Action Areas

The SRIA contains the five following action areas:

- *Collaborate for Security,* asks for a collaborative and harmonized approach for SMS, Risk management, security baseline, incident management among different actors and domains.
- *Engage aviation personnel and society for security,* focusses on the human/social issues of security from risk prevention to contingency management also considering the legal aspects.
- *Build and exploit security intelligence,* aims at building and exploiting security intelligence for forensic analysis, security radar, horizon scanning, information management and sharing by addressing methods, tools, procedures and systems.
- *Ensure operational security,* works on Security Management System, collaborative support, security baseline, efficiency of flows and on incident management, also ensuring the adaptability of the legal framework to operational requirements and promoting approaches to measure security performance in real-time.
- *Design, manufacture, and certify for security* targets the resilience by design, ensures the development of a performance framework for security allowing definition of KPIs, modelling, verification, validation, certification for security performance, ensuring detection and management of threats and interoperability also with other transport modes.

The SRIA contains five similar actions areas for safety, they are summarized in the first row of the table depicted in Figure 1. Furthermore, for each action area corresponding achievements for 2020, 2035, 2050 versus which to measure research results were also defined.

## 2.2 Review of OPTICS2 Research Priorities

To track the evolution of the roadmap a methodology has been defined in OPTICS2 [3] (H2020) a coordinated and support action (CSA), to analyse the research activities in safety and security for aviation. OPTICS2 aimed to provide oversight of progress in research and innovation (R&I) aiming to improve the safety and security of aviation in accordance with Flightpath 2050 challenges and goals, exploiting as far as possible the identified metrics, achievements, main topic areas and broad knowledge and expertise base established in the development of SRIA .Within this csa processes supporting stakeholders with strategic recommendations were implemented and a comprehensive vision of the safety and security - oriented research landscape was built. The action defined a reference base and methodologies to perform assessment of progress both from a technological perspective - are we doing the right research and the research right? and from the societal and economic perspective - is it delivering societal and market benefit? The surveys were performed on an annual basis, in close collaboration with expertise from the aviation industry through a series of workshops, fully exploiting the network developed by ACARE. Assessments were performed upon all on-going initiatives addressing safety research as well as security research in aviation. The assessments resulted in the provision of an annual report, identifying main performers, gaps and obstacles in the research landscape, formulating strategic recommendations, corrective actions and suggested priorities. The findings were presented and discussed with the aviation community at an annual safety conference, organised on the premises of EASA, EUROCONTROL, etc. The results of the annual state-of-the-art

review, together with relevant basic data and project information were made available on the OPTICS2 repository, accessible on a dedicated website.

The methodology developed in OPTICS2 combines:

- A bottom-up approach, in which the OPTICS2 team assesses in a structured way how individual R&I projects contribute to elements of the SRIA2;
- A top-down approach, in which experts are invited to contribute to the OPTICS2 work throughout workshops and roundtable consultations. The workshops are centered on specific aviation safety and/or security R&I fields and are aimed to identify gaps in research being performed as well as new research opportunities. The roundtable consultations are events on call aimed at discussing specific issues arisen during the project.

The results from the bottom-up and top-down processes were then reviewed by the OPTICS2 team and compiled to provide strategic recommendations to the EC and ACARE via an annual report, including suggested corrective actions and priorities.

In short, the overall process can be split up into three phases:

1. Selection of projects;
2. Assessment of projects, in turn subdivided into three steps:
   a. Mapping of projects and preliminary assessment,
   b. Moderation,
   c. Project coordinator review;
3. Synthesis of results and formulation of strategic recommendations.

The flow diagram of the OPTICS2 approach is shown in Figure 1. Each phase is further described in the following paragraphs.

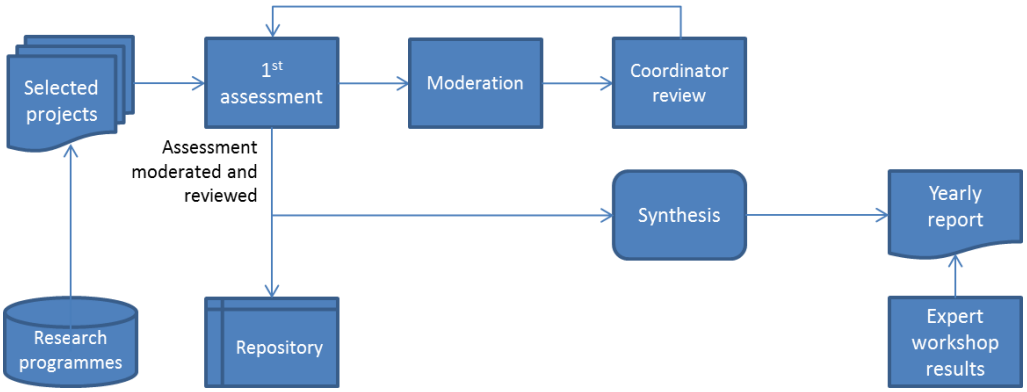


Figure 2: Flow diagram of the OPTICS2 methodology

The contribution of each project to the linked research areas is assessed with respect to the following metrics:

1. Contribution to achieving strategic goals: this metric assesses how the scope of a project contributes to the implementation of the SRIA2. More specifically, for security it identifies the targeted time-frame of the project (2020, 2025, 2035), identifies the aviation segments addressed, and evaluates to what extent the scope of a research area is addressed by the scope of the project.
2. Maturity: this metric evaluates the level of maturity of the project outcomes (expected for on-going projects, actual for finished ones) in order to understand how research and innovation projects make it into operational deployment. It also identifies the potential users of each project outcome in order to understand what is necessary to take the solutions produced to higher TRL levels. In summary, it provides an indication of the progress towards the targeted delivery to the aviation system, and what remains to be achieved.
3. Contribution to reducing current risks:
   a) Research coverage of top safety risks: this metric refers to the Annual Safety Reviews published by EASA and aims to assess the safety research coverage of current safety key risks. More specifically, it identifies the key risk areas and safety issues addressed by each project and evaluates the level of contribution.

b) Research coverage of security lifecycle: this metric assesses the contribution of security research and innovation to security improvements within the different phases of the security lifecycle: prevention and preparedness, detection and surveillance, response and recovery. It identifies the phase/s covered by each project, and evaluates the level of contribution.

4. Ease of adoption: this metric aims to represent the perceived complexity of the translation of research and innovation into solid steps towards achieving the SRIA2 goals. It identifies, for each project, the main risks and threats of adoption of the project outcomes.

5. Investment in research: this metric explores the financial resources invested in European aviation safety and security R&I, aiming at evaluating the magnitude of funds as well as identifying trends and dispersions.

6. Economic impact: this is a cluster of metrics aimed at exploring various industrial and regulatory aspects.

The Safety and Security Cross-Cutting Research Priorities

- [DESIGN] Ensure the safety and security of the future aviation 'skyscape', addressing the full future complexity of current and novel manned and unmanned vehicles, including drone fleets, personal vehicles and sky-taxis, as well as operations in Higher Airspace, including solar planes, supersonic and hypersonic aircraft, and new sustainable aviation fuels and aircraft configurations for Clean Aviation.
- [INTELLIGENCE] When it comes to safety and security intelligence and data analytics, cooperation matters, there is still insufficient sharing of data between the various stakeholders. Research is needed to determine how best to enable multiple actors to share their data confidentially, enabling benchmarking and insights that will lead to safer and more secure operations and designs of aircraft, airports and air traffic systems. Data-sharing and safety & security learning platforms must also include new entrants (drones, sky taxis, etc.). Additionally, this requires efficient automated look-up procedures and mechanisms across heterogeneous data sources.
- [OPERATIONS] Research is needed on the adoption into the cockpit of electronic devices with increasing automation capabilities and interactive modes, and the potential for safety /security compromise (e.g. tablets, electronic flight bags, etc.). This research needs to encompass conventional airliners as well as GA aircraft and new vehicles (personal aerial vehicles, sky taxis, etc.).
- [INTELLIGENCE] The 'promise' of Big Data and Machine Learning has yet to deliver in aviation safety and security. Research is needed on which related use-cases should be prioritised by advanced analytics and data-mining, providing compelling demonstrations of the utility of the approach for safety and security, as well as guidance on how to install data driven safety analytic processes into aviation businesses. This is particularly challenging for all current Machine Learning approaches as safety and security incidents are extremely rare.
- [GOVERNANCE] Research is needed to develop more agile and less fragmented certification methods (which are still fit-for-purpose) such as virtual certification, to maximise the implementation of safe and secure innovations in the aviation sector by means of model based tools and the adoption of shared and robust validation approaches, including Industry 4.0 technologies and new aerial systems. Moreover, there is a need for research that identifies obstacles in regulatory and/or certification requirements and that activelystimulates a dialogue between all stakeholders and regulators to overcome these obstacles.

The following recommendations for the cross-fertilisation between the aviation safety and security domains have been identified.

1. **Safety and Security Management System integration**: Whilst safety and security systems can be integrated, organisations should be given the flexibility to choose whether they have integrated or federated management systems. However, when it comes to Safety and Security Policy, Risk

Management, Assurance and Promotion, efficient information exchange is essential.
2. Safety and Physical Security: Security processes at airports involve many physical interactions so in the case of pandemics this presents a challenge to the safety of passengers and staff. It is recommended that there should be a better clarification of scope of what is covered by safety and what is covered by security, as the lines between safety and security and public health can become blurred.

3. **Safety and Information Security**

- Safety and Security Risk Assessments: Whilst the results of a Safety risk assessment will change slowly, the results of an information security risk assessment will change more rapidly due to the changing threat landscape. It is recommended that their there needs to be:
  - Acceptance that security risk assessments need to be performed more frequently than safety assessments, driven by changes to the threat landscape, and the occurrence of security incidents, as well as scheduled system changes.
  - Efficient risk assessment information exchange, and appropriate risk treatment between the safety and security development processes within a domain. This also allows potential conflicts between safety and security requirements to be addressed as early as possible, since a proposed security requirement (or control) may potentially have a negative impact on safety, or vice-versa.
  - Compatible safety and security information exchange and agreement of appropriate risk treatment between connected domains.
- Architecture development: Security measures are likely to need to be upgraded over the operational lifecycle. It is recommended that consideration should be given in the early architecture design to allow security measures to be able to be updated without causing a 'major' impact to the safety and the certification of the system in question.
- Certification question: currently, safety and security certification are disjointed processes/concepts. A system can be certified as "safe" although it may possess security vulnerabilities. Can an insecure system really be presumed to be safe? Coordination in safety/security certification is required in future2.
- Information Sharing: Mobility as a Service (MaaS) will support the optimisation of passenger multi-mode travel. This will require secure information sharing between transport modes, and for them to achieve similar levels of security. Failures in MaaS systems could lead to situations impacting the safety of passengers (e.g., exposure of personal data; stranding in remote locations; inability to complete journey; …)
- Operations: As the information security threat landscape will evolve and new vulnerabilities are discovered over time, it is recommended that there needs to be efficient incident, event and vulnerability information exchange, and appropriate risk treatment to mitigate new threats that would have a safety impact. A compatible approach across transport modes is a pre-requisite for the realisation of multi-mode transport.

**4. Safe and secure automation and human factors**

- Operations: To operate safely in future congested urban environments, automated drones and UAM vehicles will have to rely on robust communications, seamless integration of air and ground sensors, automated flight controls, and will increasingly use electric propulsion. This is going to provide another level of challenge for development and operation to ensure a seamless and integrated safe and secure urban environment system that integrates smart cities, vehicles and the Air Traffic management system.
- Warnings and alerts: Systems need to be designed, or the crew provided with better guidance, on how to react and respond to a variety of scenarios. A system could be operating normally, but still be presenting misleading information. The crew/operator needs to be provided with better guidance so that they can distinguish between a real safety alert and warning in the cockpit or workstation, and a false alert introduced by an information security attack. This also raises questions of trust, and could further be complicated when AI systems, such as those employing machine learning, are introduced into the flight-deck

**5. Resources and Skills:** Delivery of integrated safety and security can be an issue, predominantly because of the different approaches taken by the safety and security communities. It is recommended that there should be encouragement of cross-functional knowledge between the safety and security teams to promote better understanding and mutual collaboration.

**6. Aviation domain Fragmentation**: The current landscape of safety and security standards and policies for all the aviation domains and supply chain is fragmented, which is exacerbated when considering compatibility with the other transport and infrastructure systems that integrate with the air transport systems. It is recommended that there be better synergy and compatibility between the domains.

**Among the most demanding research priorities there are: safety and security harmonization, which starts from the harmonization of risk assessment to the safety and security assurance by design.**

There are several situations in which this harmonized approach is necessary. Safety and Security management could share concepts and approaches, nevertheless so far two different domains have grown up with different perspectives, communities and even capabilities. There is a communication problem between the two domains: each has developed its own glossary for similar –concepts, which could cause confusion and duplicate efforts.

The basic properties of safety and security are indeed not identical, but interdependent on each other. In both cases there is a "system" in an operating environment.

The system could cause an undesirable effect on its environment, but the environment could cause in turn an undesirable effect on the system itself.

Safety can be defined as the inability of the system to affect its environment in an undesirable, while the inability of the (external) environment to affect the system in an undesirable way is usually called security.

According to the type of system, its operational environment and the types of undesired effects one can have on the other, there could be different approaches for safety and security.

As an example, addressing security in a “safety critical scenario” possible protection measures for airport operations (runway and ground) from intruder drones, which may be either intruding by mistake or for malicious intent like terrorism or economical extortion will be described in paragraph 3. Most of the world’s airports remain vulnerable to such intruders coming by a rapidly expanding market. The drastic solution to the arrival of an intruder at the airport is the closure of the airport itself. However, this solution is not always the most suitable even for safety itself, as well as for performance and cost efficiency. Since the risk of intruders at the airport cannot be eliminated, an approach to the management of this risk must be defined, characterized and prioritized. Such approach has been developed within project ASPRID (SESAR 2020 EXPLORATORY RESEARCH).

**+ OPTICS2 Cybersecurity workshop**

OPTICS2 brought together more than 50 experts to EASA in June 2018 from all aviation domains to consider both existing and potential future cyber risks, and identify a top list of both urgent and mid-term research required to maintain a safe and secure air transport system today, and in the future.

The top ten aviation cybersecurity research priorities as identified by the expert participants.

1. Improving security culture and risk awareness
2. Security by design for the whole lifecycle
3. Safety and security integration
4. Maintaining security of the system throughout lifecycle
5. Improved anomaly & intrusion detection
6. Improved cybersecurity situational awareness for incident management
7. Artificial intelligence systems for improved cybersecurity
8. Dynamic and Integrated Safety-Security Risk Management
9. End-to-end authenticity supported by international regulations

10. Improved incident information sharing

The clear winner was the need to develop a security culture across the industry, with heightened security awareness of all staff, supported by robust security processes and techniques. This was seen as necessary due to perceived complacency and lack of preparedness in the industry, as well as a lack of validation of existing security measures.
The next four research priorities relate to learning how to be secure by design, moving safety and security closer together so they can learn and leverage from each other, determining how to maintain the security of a system throughout its entire life-cycle, and developing improved detection means for anomalies and intrusions

## 3. Concluding Remarks about Aviation Safety and Security hot research topics

### 3.1 Safety and Security Harmonization in Counter drone activities

Since the risk of intruders at the airport cannot be eliminated, an approach to the management of this risk has been defined according to the impact on safety and efficiency of the specific airport. A systemic approach to protect airport operations from intruders by mistake or malevolent intent by increasing situational awareness about: the intruder attack danger weight, the capability of re-scheduling the airport operations, the dynamic identification of free zones" where it is possible to "neutralize the threat" has been designed. The proposed approach consists in "protecting" the intersected vulnerable airport sub-area impacted with a certain probability, by the intruder, to set up in that subarea (SA) possible specific countermeasures
(change management of operations and countering the intruders). Such a condition will
make the sub-area to switch to unsafe status. The airport will be divided into vulnerable and no vulnerable sub-areas (dynamically changing over time) and the objective will be to maintain low the number of possible intersections between the drone and the vulnerable sub-area (avoid unsafety condition propagation) and to bring the unsafe zones to a safe status. At the same time, the intent will be to push the drone to an equipped zone where it can be quenched. A decision support system has been conceived according to this logic flow, which is fed by a complete event tree, which in turns contains all the possible scenarios generated by intruder attacks.


Artificial Intelligence is expected to support Security for Aviation in many situations specific of A.I. (training systems and operators to face with unknowns, enabling better awareness about the specific situation, to measure performance of countermeasures, to derive the best options among possible decisions.

### 3.2 The role of Artificial Intelligence

A.I. can also support modelling socio-complex systems, where humans interact with autonomous systems too and the allocation of tasks can be also dynamically performed according to risky evolving scenarios, in this case A.I. will also be in charge of reinforcing the human agent behavior. From simulating attack scenarios also evolving, to analyze large sets of data supporting decision making in real time, to learn by external attacks adversary behavior, applications of A.I. can solve security issues. An effective data sharing is necessary among different aviation stakeholders, to allow seamless interactions among different operators (e.g. OEM, suppliers in collaboration with drone operators/manufacturers, air traffic controllers and supervisors in the design of the U-space/UTM (Unmanned Aircraft System Traffic Management) human machine, national and local legislation data/rules). Data should also regard information access to operators on emerging hazards that in several cases are considered confidential or restricted at specific internal offices. One of the main challenges for A.I. is Trustworthiness which represents an enabler for acceptance

and the process to increase it must pass through explainability, the adoption of learning assurance approaches and the validated capability for A.I. application to control safety risks.

### 3.3 The trendy Digital Twin Concept

A digital twin has recently gained interest by many industries to increase their competitiveness, productivity, and efficiency. It links together physical and virtual worlds by exchanging real-world data. It is a dynamic cyber representation of a system, possible on different phases of its lifecycle. It uses real-world data, simulation or machine learning models, combined with data analysis, to enable awareness, learning, and decision support.

Digital Twin can be used for product prototyping to assess system behaviors facing with different external environment scenarios, to support the manufacturing processes and last but not least for decision making. It captures, aggregates and analyses data from real world systems to optimize operations. In case of external attacks, it can combine metadata and log information to reason on the possible attacks by using A.I. approaches.

## 4. Contact Author Email Address

Contact author email address, mailto: A.Vozella@cira.it, Pierre.Bieber@onera.fr

## 5. Copyright Statement



## 6. References

[1] ACARE, Flightpath2050 Goals, https://www.acare4europe.org/sria/flightpath-2050-goals

[2] ACARE, Strategic Research and Innovation Agenda – Volume 1, 2017, https://www.acare4europe.org/sites/acare4europe.org/files/attachment/acare-strategic-research-innovation-volume-1-v2.7-interactive-fin_0.pdf

[3] OPTICS$^2$ Consortium, OPTICS$^2$ 1st Workshop Report - Aviation Cybersecurity: what's around the corner and are we ready for it?, 2018, https://www.optics-project.eu/1308-2/

[4] OPTICS$^2$ Consortium, State-of-the-art in Safety and Security, August 2021, http://www.optics-project.eu/download-the-state-of-the-art-in-safety-and-security-2021/

[5] OPTICS$^2$ Consortium, OPTICS$^2$ Main Findings – Final Safety and Security Integrated Recommendations, August 2021, http://www.optics-project.eu/download-the-final-safety-security-integrated-recommendations/

[6] EASA AMC 20-42 Airworthiness information security risk assessment, in General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances (AMC-20), Amendment 23, 2022 https://www.easa.europa.eu/document-library/certification-specifications/amc-20-amendment-23

[7] EUROCAE ED-202A, Airworthiness Security Process Specification, dated June 2014 /RTCA DO-326A, dated August 2014;

[8] EUROCAE ED-203A, Airworthiness Security Methods and Considerations, dated June2018 / RTCA DO-356, dated June 2018;

[9] COMMISSION IMPLEMENTING REGULATION (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

[10] COMMISSION IMPLEMENTING REGULATION (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space

[11] EASA, Drone Incident Management Manual for Aerodromes, part 1, 2021, https://www.easa.europa.eu/drone-incident-management-aerodromes-part-1

[12] EUROCAE ED-286 - Operational Services and Environment Definition for Counter-UAS In Controlled Airspace, 2021.

[13] Vozella, A., Bieber, P,….Solution Set Up for Airport Protection from Intruder Drones, ESREL 2020

[14]Pascarella, D., Gigante, G., Nebula, Vozella. A., Redondo de la Mata, E., Roncero, F.J., and Olmo Criado, M. and Martinavarro E , Historical Data Analysis and Modelling for Drone Intrusions in Airport. In proceedings of 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) 2021

[15] Bieber P, Blanquart, JP, Descargues G,, Dulucq M, Fourastier Y, Hazane E, Julien M, Léonardon L, and Sarouille G, Security and Safety Assurance for Aerospace Embedded Systems, in proceedings of Embedded Real Time Software and Systems (ERTS2012), Toulouse, 2012

[16] Piètre-Cambacédès L and,Chaudet C.The SEMA referential framework:avoiding ambiguities in the terms ‘security’ and ‘safety’. International Journal of Critical Infrastructure Protection 2010;3(2):55–66.