SOLUTION SET-UP for AIRPORT PROTECTION from Intruder Drones

Angela Vozella
Centro Italiano Ricerche Aerospaziali S.C.p.A., a.vozella@cira.it

Francisco Muñoz Sanz
Instituto Nacional de Tecnica Aeroespacial Esteban Terradas, mugnozsf@inta.es

Mario Antonio Solazzo
Centro Italiano Ricerche Aerospaziali S.C.p.A., m.solazzo@cira.it

Edgar Martinavarro Armengol
Instituto Nacional de Tecnica Aeroespacial Esteban Terradas, martinavarro@inta.es

Pierre Bieber
Office National d'Etudes et de Recherches Aerospatials, pierre.bieber@onera.fr

Giancarlo Ferrara
Eurocontrol - European Organization for the Safety of Air Navigation, giancarlo.ferrara@eurocontrol.int

The trouble caused at the UK's Gatwick Airport by a malicious drone has highlighted the lack of safeguards in place for such events, even when it comes to key infrastructures such as international airports. 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. The focus of this paper is to exploit 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. Thus the analysis will consider a set of aircraft and airport operations, exploiting all their related attributes, to assess how they are vulnerable to different identified use cases of intruder attacks, how off nominal scenarios can evolve, performing a benchmarking to identify the best option to model (FMECA, FTA, ETA,…). A logic, service oriented architecture will be conceived involving all the impacted actors, exploiting interoperability of roles, procedures, data and systems. Such a research has been started within Garteur Aviation Security Group of Responsables and will go on within a project funded under SESAR 2020 EXPLORATORY RESEARCH.

Keywords: Airport, Operations, Safety, Security, FMECA, FTA, ETA, Drones.

1. Introduction

Application of drones or drone swarms and other related emerging technologies can increase the safety, security and overall efficiency of airports. Drones can enable pilot services, such as aircraft inspections, transport management (including emergencies), infrastructure condition monitoring and maintenance. Crucial services are monitoring of Airport runways for: obstruction analysis, pavement condition assessment and debris presence inspection, airfield light inspections, wild life management… Nevertheless, drones can represent a threat, intruding either by mistake or due to malicious activity.

Though prevention approaches are put in place at the airports to avoid intruders, they could access the airport areas. The problem with drones operating near airports is first the risk of collision between aircraft and drones and thus the fear of human and material losses, but also fear of terror attacks on airport infrastructure as well as financial losses due to periods of airport shutdown. The drastic solution to the arrival of an intruder at the airport is the closure of the airport itself.

However, on the one hand this solution is not always the most suitable one, because if an intruder arrives during a phase of a critical operation, the evolution of the specific critical

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

scenario must be managed in the best way before closing the airport. On the other hand, the closure of the airport leading to enormous impacts on all air traffic may not be convenient if the specific case of intruder does not have an impact on the safety of operations.

Airport environments due to different design features ranging from a single runway layout to large international airports with several runways and terminals, some located in dense urban areas and others in rural desolate areas, while have similar security requirements for detecting, can require different approaches for countering drones.

Since the risk of intruders at the airport cannot be eliminated, an approach to the management of this risk must be defined according to the impact on safety and efficiency of the specific airport. This paper sets up 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".

All these items will feed a decision support system (DSS) in charge of evaluating the best decision option according to a combination of previous conditions. Such conditions consist of a set of performance indicators preserving not only safety but reducing the impact of other key aspects such as efficiency. The outcome of the DSS, the provided solution, will contribute by means of an index of resilience joined with the concept of transparency and the traceability of artificial intelligence techniques to the overall evaluation of operation performance. Indeed the DSS is added with an AI layer assuring trust in its outcomes. Each option will trigger a drone neutralization procedure, characterized in terms of success rate estimation.

Paragraph 2 shows the overall approach which will be implemented while the focus of this paper is put on two enabling parts of such an approach: the definition of the drone danger weight model and the operation scenario evolution (vulnerable airport sub-areas). Paragraph 5 contains the conclusion.

2. The proposed approach

The proposed approach consists in defining a complete framework in charge of supporting decision making in case of intruders. Such a framework will provide a basis to verify and validate systems and procedures to manage the threat, developing knowledge about:

- The evolution over a time frame of vulnerable airport sub-areas at intervals of minutes,
- the possible intruders and their missions,
- the probability and the elapsed time in which the intruder will intersect a vulnerable airport sub-area,
- the mechanisms to manage the threats.

Generally speaking, the proposed approach will consist in "protecting" the intersected vulnerable airport sub-area impacted with a certain probability, by the intruder, to set up in that sub-area (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 will be conceived according to this logic flow, which will be fed by a complete event tree, which in turns contains all the possible scenarios generated by intruder attacks.

The scenarios will be based on the Protection Flow (PF) evolutions which characterize the actions to be performed. The PF will be activated when the intersection occurrence (between the drone and the vulnerable sub-area) overcomes a threshold value, according to the estimated Elapsed Time (ET) which will fix the protection flow Reaction Time (RT). The probability to bring the unsafe sub-area to a safe status depends on the magnitude of the ET vs RT.

According to the previous concept sketched in the following table:

Status of Sub-area(i) (SA)	ET(i)	RT(i)	PF(i)
SA#23	3'	1'	ACT#13 (i)
SA#27	2'	4'	ACT#00 (i)
…..	….	….	….

Each sequence of actions in the PF(i) will bring the vulnerable sub-areas to a new status, asking

for a further PF in case an occurrence of intersection still exists.

3. The Intruder risk patterns

Such a paragraph provides an approach to identify all the possible risk patterns related to intruders (single or fleet) according to their configuration and attributes. In recent years for drones, the possible altitude, range, endurance, air speed and precision of navigation have increased a lot. In addition, they can transport more mass and above all are cheap, easy to obtain and also available as a kit. Different classification criteria exist. They can be classified according to the propulsion system how described below.

Table 1. Drone Classification per Characteristics.

TYPE	CHARACTERISTIC
Multi-rotor helicopter	More than one power-driven engine (rotor) that rotate or turn vertically. It takes off, lands, flies and hovers like a traditional 'single rotor' helicopter but has more than one rotor.
Single-rotor helicopter	With one power-driven engine (rotor) and looks a bit like a traditional helicopter. It usually also has another rotor on the tail or end of the aircraft.
Aeroplane	looks and flies like a regular plane - it has fixed wings. It also takes off and lands horizontally and usually can't hover.
Powered lift	can take off and land vertically (straight up and down) like a helicopter, but can then move into forward flight like a traditional plane.
Airship	engine powered and is 'lighter than air' - it can be filled with a buoyant gas and usually 'floats' in the air. A blimp is a good example of an airship.

Source: https://www.casa.gov.au/drones/rules/drone-types

Another possible classification is based on their size or even on to the ranges they can travel and their endurance in the air.

Table 2. Drone Classification per Size.

Category	Weight [kg]	Operating Altitude [m]	Range [km]	Payload [kg]
Nano	<0.2	<90	0.09	<0.2
Micro	0.25-2	<90	5	0.2-0.5
Mini	2-20	<900	25	0.5-10
Small	<150	<1500	50-100	5-50
Tactical	>150	<3000	>200	25-200

Source: Ben Nassi, Asaf Shabtai (2019). SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. Ben-Gurion University of the Negev.

The previous properties are aerodynamic properties and are necessary to understand the possible path of intruder and the intrinsic risk related to a collision with such an obstacle: collision risk (intruder).

A collision with even a lightweight drone could result in serious problems. A small drone impacting an engine would be unlikely to cause a crash, but it could easily cause the failure of that engine and millions of dollars of damage.

According to tests carried on the potential damage to manned aircraft due to mid-air collisions with drones, they can cause more structural damage than birds of the same weight for a given impact speed, because they are made of heavy plastic or metal and often contain batteries and cameras. Furthermore, small drones could deliver chemical or biological or explosive agents in an attack.

The current generation of drones provides First-Person View (FPV) channel capabilities that allow operators to fly drones in areas located up to eight kilometres from the operator's location; this can be done both manually and automatically. In addition, modern drones are very small, and they can reach speeds of up to 65 kilometres per hour and carry up to six kilograms. Drones can cause much greater disasters in terms of the number of casualties by exploding into the airport.

Military-style drones are heavier, but can also carry a greater payload with more explosives. With the advent of machine learning and artificial intelligence, drones may soon become programmable and smart enough to be used without human guidance and for increasingly malevolent purposes.

Drone swarms also offer new means to improve offense having the advantage of being able to spread out broadly.

Dispersed attacks also allow for more careful targeting. Instead of spraying large masses of agent, drones could search for and target individuals or specific vulnerabilities such as air ventilation systems. This also means the drones would not need to carry as much agent.

Moreover, drone swarms enable the use of combined arms tactics. Some attack drones within the swarm could be equipped with chemical or biological payloads, while others could carry conventional weapons.

Each specific category can pose specific threats to security. There could be attacks to privacy, physical attacks, crime attacks or cyber-attacks. While, nano-drones can specifically be used for carrying surveillance, equipment for spying, micro drones equipped with a radio transceiver can pose MITM (man in the middle) attacks against cellular networks, tracking a person according to his/her devices or can pose a physical attack by carrying radioactive sand or chemical substances. Micro drones can also pose crime attacks by smuggling goods into restricted area. Mini drones can carry a bomb and collide with an airplane or release explosive on the ground.

4. Detecting, Identifying, Managing

Defence against drones asks for a three-step approach. The first step involves detecting the drone. Taking into account the high speed of the flying objects and the limited recognition radius of sensor technology, such objective is challenging and many factors, including ambient light, weather, false positive rates, ambient noise, cost, line of sight and detection range influence the effectiveness of each method. Each method's effectiveness at dealing with issues important for securing a restricted area from the presence of drones is summarized in the following, also whether the suggested method can be used for drone identification (i.e., detecting the drone type).

Detection and Tracking Systems are based on different features.

Radar detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters RF pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.

Radio-frequency (RF) identifies drones by scanning for the frequencies on which most drones are known to operate. Algorithms pick out and geo-locate RF-emitting devices in the area that are likely to be drones.

Electro-Optical (EO) detects drones based on their visual signature.

Infrared (IR) detects drones based on their heat signature.

Acoustic detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.

Combined Sensors integrating a variety of different sensor types will be used in order to provide a more robust detection capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements increases the probability of a successful detection, given that no individual detection method is entirely fail proof and every method has some limitations. For instance while RF detection can locate controller and drone, lending itself to signal jamming and intercept, it requires a RF signal which can pose problems to other equipment. Radars while detecting drones without RF control signal for long range, have problem to detect low flying drones and distinguish from other small objects. Acoustic sensors do not cause interferences but their operative range is limited and suffer from interferences in noisy environments. Infrared while detecting drones without RF control signal, do not work with most small drones which produce very little heat for a limited range. Visual-human based detection offering the possibility to detect drones without RF control signal, distinguishing between a drone or a bird at reasonable distance, they have a limited visual range and result not effective at night and in poor visibility conditions without image intensifying devices. Visual-automated systems, detecting drones without RF control signal, could not be reliable and accurate to detect odd-looking or disguised drones and of course have a limited range.

The second step involves identifying the type of drone and its related danger level. An analysis of the potential impact of malevolent intruders at the airport supports the possible scenario definition.

The potential impact on an airport has to be evaluated in terms of impacted assets.

They could be: other vehicles (air and ground), people, airport infrastructures, environment.

It consists in crashing, causing debris damaging the previous assets, releasing toxic or explosive substances.

Let I(T), the intruder detected at time step T, W(I(T)) represents the danger weight associated to I(T).

Such danger weight depends on the possible flight path the drone can perform in the next time intervals. Thus, it is strongly related to its aerodynamic performances and related spatial coordinates (4D).

In a further development of proposed approach the danger weight W(I(T)) will also encompass the probability of carrying explosive, chemical, biological, nuclear substances provided that the drone category is known.

At run time a forecasting of possible scenarios is implemented to support W(I(T)) estimation.

Thus summarizing the proposed framework related to the intruder, goes through the following steps:

1. Type identification (according to the previous classes), which, besides providing details about its specific features for implementing control (e.g. its specific radio frequency), supports next steps
2. Danger weight evaluation with a certain probability (considered in an evolution of the proposed approach)

According to the type identification step the intersection occurrence will be evaluated to activate the PF. Thus, the third step will be to bring the drone to the equipped zone. Interdiction will consist, as a first step, in identifying the closest zone where it can be quenched. Such a zone will not be affected by operations.

While from the operation point of view it will be necessary to possible interdict operations on unsafe sub-areas according to the impact evaluated by an event tree.

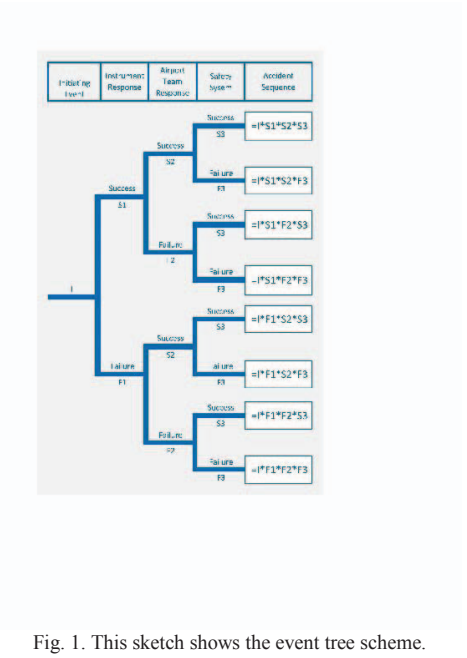

Fig. 1. This sketch shows the event tree scheme.

5. Operation management

When the drone I(T) is detected the corresponding operations in vulnerable sub-areas at time T will be analysed if they can be interrupted (postponed) or moved, while the drone threat will be managed according to PF.

The operation in next time frames (T+1, T+2, …T+n) will be analysed with an event tree for postponing or moving them to other places, if their current or next locations fall within the intruder's impacted sub-area.

Each operation is characterized in terms of: involved people (operators, crew, passengers), location of people (external environment, internal environment), involved vehicles, involved infrastructures and evolution of time of these parameters.

Such analysis will be aimed at allocating a vulnerability index to the operation itself to all the attack patterns.

6. Threats Minimization Methods

Several methods may be used to manage the intruders, like: jamming, net capturing, locating of the drone operator, spoofing, laser and projectile. Jamming, works on the communication

link and/or the 3D data tracking through GPS. The lost of such relevant info, typically forces the drone to switch to safety mode with very limited operational capacity. In other words, it will return to start lift-off point "Return to Home" or it will stays stand-by in the same zone.

The regulation for airport operation puts mandatory constraints referring to the jamming adoption, like to avoid any form of interference with the functionality of ground radio assistances and on-board devices.

Anti-intrusion systems take into account the possibility to use laser and projectiles. These systems obviously are extreme resources whose use is a practical option in the military infrastructures, but it is realistic to think that their adoption will soon be possible.

The intruder control by hijacking (protocol manipulation) together with the "Net Capturing" seem promising effective methods.

About the platforms, there are ground-based Systems designed to be used from either stationary or mobile positions on the ground. This category includes systems installed on fixed sites, mobile systems, and systems mounted on ground vehicles.

- Hand-held Systems that are designed to be operated by a single individual by hand. Many of these systems resemble rifles or other small arms.
- UAV-based Systems designed to be mounted on drones, which can come into proximity with the targeted unmanned aircraft in order to employ interdiction elements at close range.

7. Framework Modules

The list below describes the main functions of the proposed complete framework to provide a solution set-up for airport protection from intruders drones.

1. The Tracking systems continuously steer the intruder and collects its behaviour in terms of danger-weight system and trajectory (e.g. T[min], X[m], Y[m], Z[m], Lat[deg], Lng[deg], Alt[m];
2. The Module *estimation of danger weight* supports interdiction selection;
3. The Module *forecasting of the future drone trajectory evolution* with related uncertainty, in statistic terms (R2, Std.Dev.) based of tracking measures and accuracies;
4. The Module intersection path evaluation compares the expected drone trajectory and dispersions vs time to the location of the on-going operations inside the airport boundaries; thus it provides the occurrence of intersections and the elapsed time to the intersection.
5. The Module exposed critical asset assessment, identifies the critical assets (e.g. "Aircrafts", "Passengers", "Service personnel", "People", "Airport infrastructure", "Ground Service systems") related to affected operations.
6. The Module dynamical evaluation of the applicable threat level ("Critical", "Severe", "Substantial", "Moderate", "Low") will inform the airport security teams also supporting decisions for mitigation through User Graphic Interfaces
7. The Module Identification of clearance zone will generate a map of the airport safe and unsafe zones;
8. Periodic post analysis (Framework Performance) will be approached with DEA methodology in order to evaluate the mitigation action efficiency and to limit the operation risks for the ATS critical elements in airport and its surroundings.
9. The considered metrics is: Airport Efficiency = Sum of delays of all affected flights [min] / (number of affected flights * Average historical airport typical delay per flight) [min]. Such a module will be in charge of evaluating the performance of the Framework. there is a need to assess the benefits and the impact of any change to the overall system from a performance point of view. According to ICAO, performance can be categorized into "subjects related to high-level ambitions and expectations" [X]. These categories are often referred to as Key Performance Areas (KPAs). ICAO has identified eleven high-level KPAs: safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, interoperability. These areas are generally interrelated and usually include one or more focus areas that define more specific performance management needs.

The next sketch shows the process flow at top level.

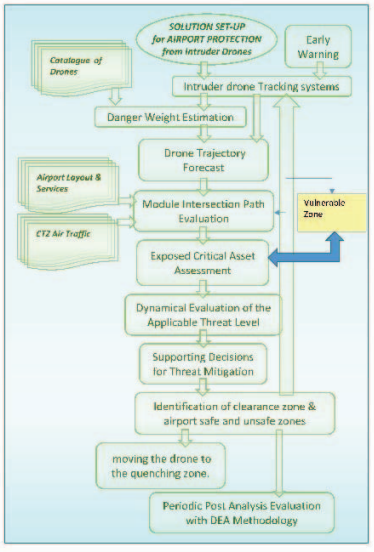

Fig. 2. This sketch shows the Airport protection process.

While the next sketch shows the reference FMECA methodology used.

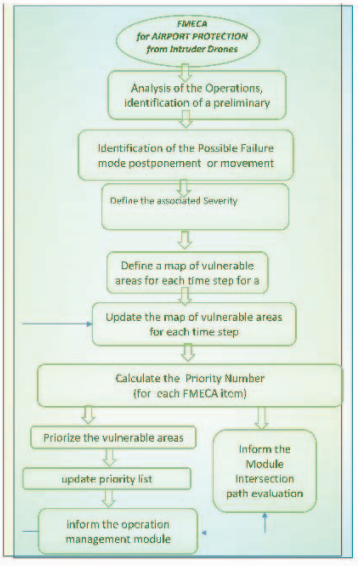

Fig. 3. This sketch shows the FMECA methodology.

8. Conclusion

Such a paper defines a framework to protect airports by intruders drones, identifying all the components which must be managed.

The concept of clearance zone identified at run time is new.

A multi-sensor approach will allow to distinguish drones from other objects, minimizing false alarms. Approach should be integrated into legacy systems and procedures, sending instant alerts and automatic or manually activate interdiction when a drone is detected also retaining for any subsequent legal scenario management. It will be tuned and experimented in a real scenario.

Acknowledgement

Such a research has been started within Garteur Aviation Security Group of Responsables

References

UAS ATM Integration Operational Concept, Vers. 1.0– 11.2018 EUROCONTROL & EASA Document (https://www.eurocontrol.int/sites/default/files/publication/files/uas-atm-integration-operational-concept-v1.0-release%2020181128.pdf)

UAS ATM Airspace Assessment, Vers. 1.2–11.2018 EUROCONTROL Document (https://www.eurocontrol.int/archive_download/all/node/10681)

Garteur Group for Aeronautical Research and Technology in Europe (http://www.garteur.org/Aviation_Security.html)

National Counter Terrorism Security Office (NaTCSO), Advice for security managers of crowded places following a change of threat level to critical., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/616572/Threat_Levels_advice.pdf

Subhash C.Ray (2004). Data Envelopment Analysis – Theory and Techniques for Economics and Operations Research, Press Syndicate of University of Cambridge.

Ben Nassi, Asaf Shabtai (2019). SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. Ben-Gurion University of the Negev.

Civil Aviation Safety Authority, Australian Government. Type of drones/Type classifications https://www.casa.gov.au/drones/rules/drone-types

Basic Statistics – Tools for Continuous Improvements – Fourth Edition, Mark J, Kiemele, Stephen R. Schmidt, Ronald J. Berdine

SESAR (2015). The Roadmap for Delivering High Performing Aviation for Europe, European ATM Master Plan, Executive View, Edition 2015

ICAO (2009). Manual on Global Performance of the Air Navigation System. Doc 9883

EUROCONTROL, "PJ19: Performance Framework (2017)," no. October, pp. 1–134, 2017.