IDS
INGEGNERIA DEI SISTEMI

WHITE PAPER

Amsterdam Drone Week 2018

Aerodrome security and safety for air traffic: new technological means to protect airports

OVERVIEW

Introduction

RPAS a new threat paradigm

The presence of Remotely piloted Systems (Drones) in the civil market is booming with technological development making entry to market easily accessible, with greater capability, higher performance and increasingly lower price point.. The episodes of improper, when not directly hostile, use of Mini or Micro UAV systems is more and more frequent. This is because drones can easily overcome traditional security systems such as fences and security barriers thanks to the possibility of performing autonomous missions on predefined waypoints with a range of 2-3 km.

Drones and aerodromes

Incursions are mostly known as an airport runway incursion, which will be presented in this document. If considering the "incorrect presence of an aircraft, a vehicle, or person on the protected area of a surface designated for the landing and take-off of an aircraft[1]". Drones are aircrafts (of a specific category) and their unwanted presence in and around airports, are considered as a real problem regarding safety

Access to Airspace by (RPAS), in particular small aircraft systems (sUAS, still referred to as "drones"), given its small size acquisition cost and ease of operation, is becoming an increasing concern for the entire aeronautical segment because of the risks inherent, due to the irresponsible use and impacts on manned aviation.

On the other side, it has to be considered the commercial implications of an airspace restriction for those applications of interest for the society, such as (but not limited to) aerial mapping, photogrammetry, infrastructure inspections, emergency support, law enforcement and recreational activities, they all have opened new perspectives in the field of transport and services, suggesting a different use of the airspace, thus allowing, a large number of sectors to consider important benefits, including those of an economic nature.

The lack of preparation for aeronautical knowledge of many RPAS operators, combined with recklessness and transgressing mentality is also present in this segment, as depicted by international statistics. Unfortunately, we have to take note that these new platforms can also be a serious threat, because drones can easily overcome traditional security systems as mentioned above and consequently, they can be used for illegal purposes related to various types of activities, including spying, smuggling, privacy invasion, military and terrorist attacks.

[1] ICAP Doc 4444 – PANS-ATM

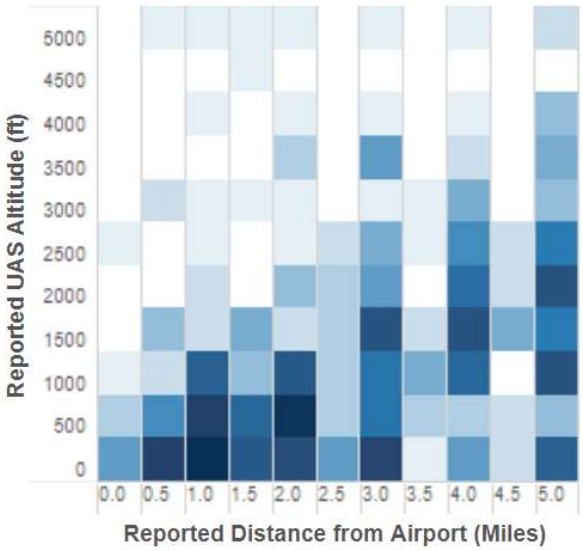
← Islamic State affiliated propaganda group released a digital leaflet threatening France with weaponized UAS

Iranian aligned Houthi rebels are claiming a UAS attack on the → Dubai airport, specifically against an Emirates flight. Some reports indicate their Qasef armed drone was responsible. However, the media being shared is actually of a crash landing of Emirates flight 521 in 2016 caused by mechanical failures and no fatalities reported. Dubai airport officials have said the airport is operating as normal and no events have occurred.

This paper provides an overview of the different types of RPAS involved in unauthorized airport incursions and proposes an effective solution for both monitoring and counter measure possible RPAS threat's. The reader, will also enjoy discovering the possible (and feasible) extension of the use of existing monitoring capability to a well-known category of *raiders.* IDS is going to further develop the radar for being capable of distinguishing birds from drones. This means that we're going to have a dual use system bird strike prevention and drone detector

Highlights

More broadly, it must also be considered that the number of incidents where drones are involved is increasing.i.e. overflights of critical and sensitive sites or approaching manned aircraft flight paths is now not uncommon. The possible reasons why this happens is, drone users are unaware of the rules or pilot their drone in an irresponsible manner or are a potential threat (terrorism). According to the *UAS sightings report* published by the FAA[2], relevant to available data from 11/13/14 to 3/31/2018, only in the United States the monthly average of sightings in airports' surroundings was higher than 200.



The RPAS Sighting report were first released by the FAA beginning in November 2014 and each successive reporting period has continued to show a significant increase in the number of encounters between manned and unmanned aircraft in the US national airspace.

Looking at those statistics[3], with focus on the period from 11/14/2014 to 1/31/2016, there were 491 sightings in the airspaces included in the volume of 5 miles distance and 5,000 ft. altitude from airports.

Drones that collide with planes cause more damage than birds of the same size because of their solid motors, batteries and other parts, a study[4] released by the Federal Aviation Administration. The study's researchers say aircraft-manufacturing standards designed for bird strikes aren't appropriate for ensuring planes can withstand collisions with drones. A team of researchers from four universities simulated collisions between drones weighing 2.7 to 8 pounds and common airliners and business jets. In some cases, drones would have penetrated the plane's skin. The researchers said the drone collisions inflict more damage than striking a bird of the same size and speed because drone components are much stiffer — birds are composed mostly of water.

[2] https://www.faa.gov/uas/resources/uas_sightings_report/

[3] http://www.forthillgroup.com/uas-sightings/

[4] https://www.seattletimes.com/business/boeing-aerospace/faa-warns-drones-more-damaging-than-bird-strikes-to-planes/

With the increasing use of drones of various types and technologies, plus the various purposes for which they are used, especially with the invasion of the airspace near the airports, causing risks to the safety of aircraft and their users, it is necessary to educate and equip the airport operators and stakeholders in order to deal with unmanned aircraft, operated remotely, with or without specific authorizations, which in any case will impact the running of Air Operations.

Challenges

Considering technological developments related to the drone market, it is envisioned the adoption of a system (, known as Anti-Drone Systems)that allows the detection, identification and (possibly) blocking of the aerial activities of these small unmanned aircraft in specific areas that are designated to other air traffic users are implemented to safe guard the airport and surrounding airspace..

The implementation of a system that allows the identification and monitoring of a drone's flight position in the areas of prohibited or restricted flight in the vicinity of airports, will represent a significant improvement in the safety and security of routine air operations.

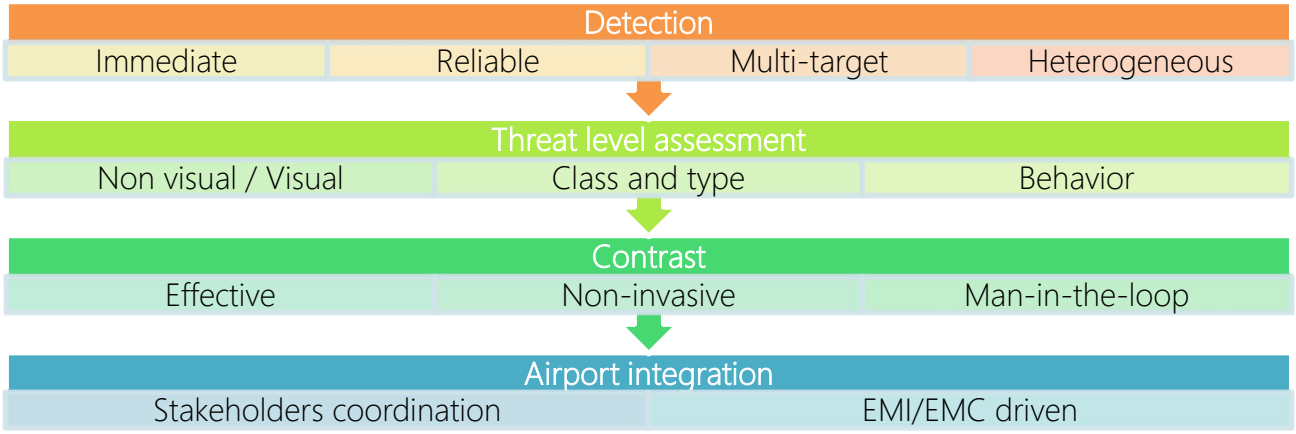
CONCEPTUAL SOLUTION

Objective

The main objective in the field of drone monitoring and countermeasure is *response time*. It is essential to detect, identify, locate and, eventually, counter the targets (threats)in the shortest possible time, before potential risks become true interferences with impact on the airport’s capacity or, rather, turn into accidents.

Required capabilities

IDS recommends that airports use multiple integrated technologies in a layered approach to detect, track, identify and interdict sUASs, with limited impact on the airport environment or operational procedures.



The key features for the definitive solution are:

- "Detection" domain
  - Immediate: time is critical for approaching threats. Any detection capability must be implemented as far as possible from the airport fences and the confirmation of a real target is a task that has to be completed quickly.
  - Reliable: most of the scenarios do not allow false alarms, operator's workload must be reduced to minimum, but not avoided, since full (or quasi-full) automation is not accepted when dealing with the implementation of time-critical response and ultimate decision making. Only man-in the loop operations with properly trained personnel guarantee both reliable detections, fast analysis and situational awareness.
  - Multi-target: scenarios are evolving together with technology and enemy tactics. Any protection system has, therefore, to implement a fundamental requirement of being capable to detect and track more than one target, providing situational awareness as it evolves
  - Heterogeneous: no matter how small it is, nor if it is a fast-fixed wing rather than a hovering multirotor. Some of the drones fly radio-controlled, some other follow a pre-determined sequence of waypoints. As long as it is something flying in the interdicted or controlled volume of airspace, it has to generate a warning to the operator
- "Threat level assessment" domain
  - Visual and non-visual: a multi-sensor technology is recommended in order to allow the operator to understand the situation and configure the best response for it.
  - Class and type: depending on the target characteristics, different responses may be implemented according to technics, tactics and procedures
  - Behavior: analysis of kinematics supports the response team in the decision making. Some target, tough verified, can result to be not offensive by their position or speed vector, with respect to the aerodrome and relevant surroundings to be protected
- "Contrast" domain
  - Effective: more than 75% of the micro and mini class drones in commerce use the communication link produced by the same company. Out of it, there are a few more companies on the market. Jamming is an effective solution as long as it covers all the known systems of above.
  - Non-invasive: the impact of jamming action on the air traffic can be disruptive, unless some action is put in place, like directionality, power balancing, selectivity.

- Man-in-the-loop: air traffic has to be timely informed about the presence of drones in aerodromes, especially approaching and taking-off airplanes. Vice-versa, anti-drone system operators should be aware of their presence and have visual support to decision about possible impact of jamming action over the plane onboard equipment. The operator will always activate the jammer independently from the level of automation of the system, but having a full situational awareness on the air traffic

- "Airport integration" domain
  - Stakeholders coordination: there are several actors involved in airport operations which, for different reasons, have to be informed on the ongoing events, or involved into the decision making process. This requires real-time structured data dissemination capability
  - EMI/EMC driven: passive elements can be interfered by airport equipment, existing CNS[5] infrastructure. As well, active subsystems may interfere with airport's technology and services. As a result, systems might operate differently from design and, especially, under-perform. Loss of performance is not an option when dealing with air navigation safety standards, not even with security levels. Any system deployed shall, therefore, be electro-magnetically compatible with the aerodrome environment.

Proposed system: working principle

An effective system is able to counter most common very-low-level flying threats spanning from small multirotor, to mini rotary-wing (classic helicopter configuration) and fixed wing systems. The detection capability cannot be affected by propulsion type (electric engines rather than petrol-fuelled engines), nor by the aerial asset dynamics (stationary, fast moving, hovering, loitering, other manoeuvres). It is also important to be able to detect and tract any UAS independently from the type of flight executed (RC controlled or autonomous) and the context and scenario of operation (urbanized area rather than open field). Therefore, a radar-based solution is of major interest, with respect to RF[6] detectors, which are lacking of robustness in metropolitan airports. The radar unit controls the surrounding portion of airspace and detects the energy reflected by any aerial asset generating a warning to the operator. In case of detection (coherent plots), the system has to automatically perform the verification activity in order to reduce any false alarm. If the verification confirms the presence of a target, the radar subsystem start tracking and collecting data in order to produce estimations of position and vector of velocity. Usually radar technology embeds specific algorithms which make real time analyses of the various tracks and comparison against elements in their libraries, opportunely prepared. Classifiers are, therefore, to be considered a must in order to reduce FA rate, workload for the operators and increase overall situational awareness.

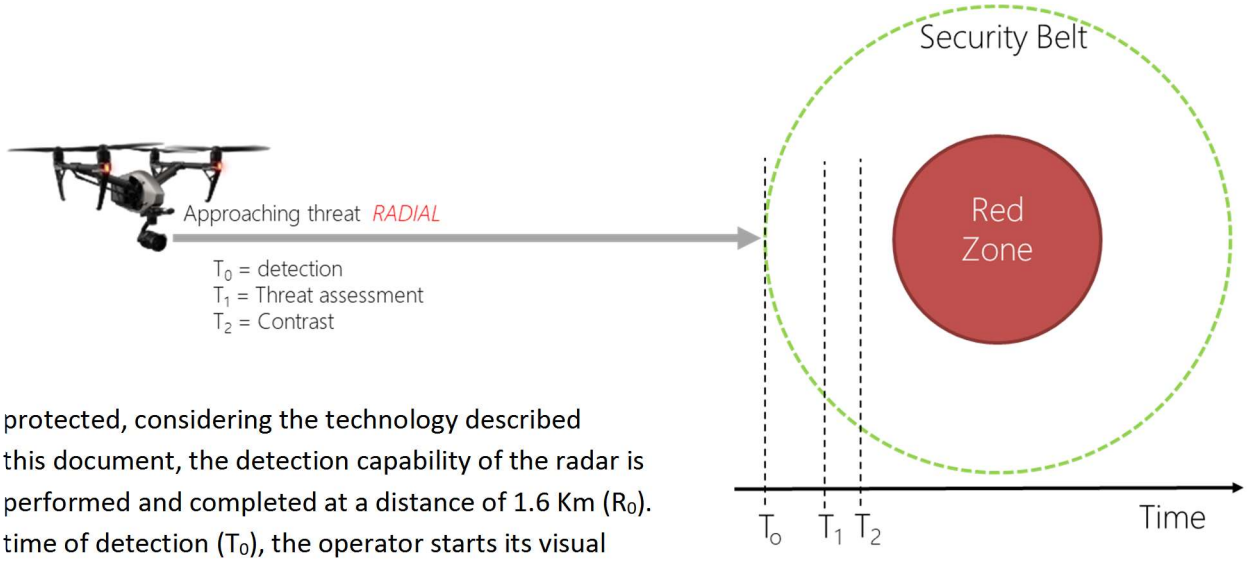
So, detection, tracking and classification of the target are accomplished by implementing radar technology, but the drone is still there, performing a mission or executing the assigned task. Before engaging it, the operator has to be sure of the real existence of a target, rather than an errant (non-malicious) drone. Once the potential target is acquired, the operator needs to investigate and assess, in the shortest time possible, the occurrence. There is generally on a few hundred meters between the drone and the area to be protected and so, success is time-dependent. The system will automatically cue the camera on the position of the target, constantly updating orientation according to target's movements, reducing the time taken by the operator, who has to prepare for the next counter measure. Once the target is visualized and locked (visual confirmation and lock-on), an automatic video

[5] Communication, Navigation, Surveillance
[6] Radio Frequency

tracking feature has to be used. In the case of multiple targets detected by the radar subsystem, the operator will select which threat has to be locked by the camera subsystem. The presence of effectors can be used to definitely contrast the threat.

The presented system is conceived for providing the operator with a warning about the verified presence of RPAS approaching, in order to enable institutional staff to mount a response. With reference to the following picture, the approach is to organize a tailored deployment of a number of different technologies opportunely dimensioned in order to protect a "Red Zone". "Protect" has to be intended as the creation of a *security belt* around the site which guarantees appropriate response to be set in time.

Assuming a possible threat (DJI Phantom 3 class) approaching radially at his maximum horizontal speed (16 m/s in ATTI mode) the Red Zone to be protected, considering the technology described later in this document, the detection capability of the radar is performed and completed at a distance of 1.6 Km (R_0). From the time of detection (T_0), the operator starts its visual engagement with the target, with the scope of assessing the real threat level and preparing the response, if needed. The presented architecture and the technology allow the accomplishment of the task in less than 15 seconds (therefore T_1=T_0+15 seconds), therefore:



- Cameras have to be dimensioned in order to guarantee tracking activity to be accomplished at R_0
- $R_1=R_0-V_{target} \times (T_1-T_0)$=1.6 km – (16 m/s x 15 sec) = 1600 m - 240 m = 1360 mt

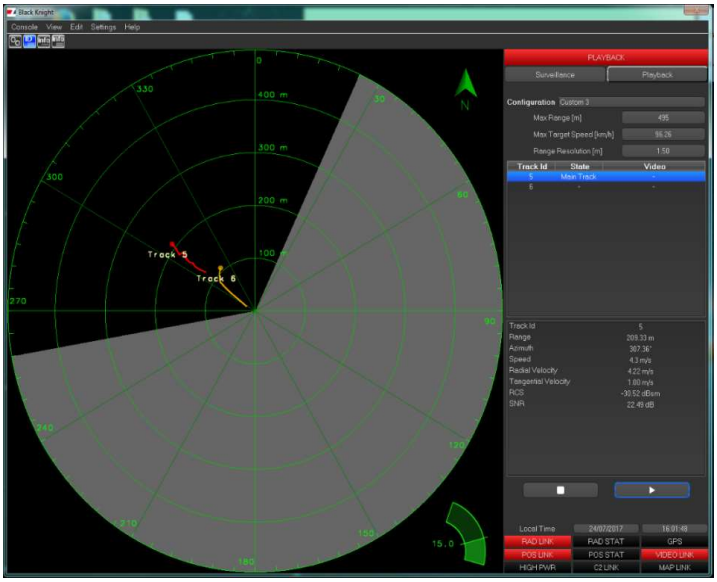
The selected effector will have the capability to jam the identified frequency range at a distance greater than R_0, ensuring a complete coverage of the monitored area. The time required for completing the jamming activity on a DJI Phantom 3 has to be less than 10".

Detection and track-while-scan

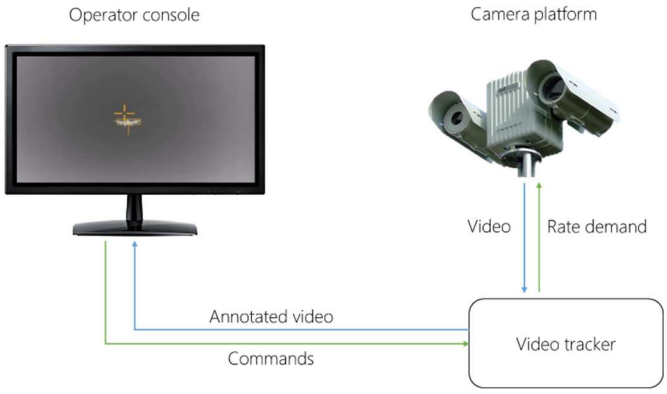
The Radar subsystem is the component that performs detection, tracking and target classification by exploring the surrounding environment with an electromagnetic signal continuously transmitted by a radar sensor with a rotating antenna on a 360° angle. The Radar subsystem will uninterruptedly scan the airspace and report in real time to the operator the possible presence of targets. The Detection console has to have a graphical interface through which the operator can do the followings:

- Configure surveillance parameters (maximum detection distance, distance resolution, maximum measurable speed, non-irradiating areas)

- Visualize in real time the airspace traffic, analyze warnings
- Manage acquired data, recording and storage
- Designating the pointing of video subsystem on the desired target



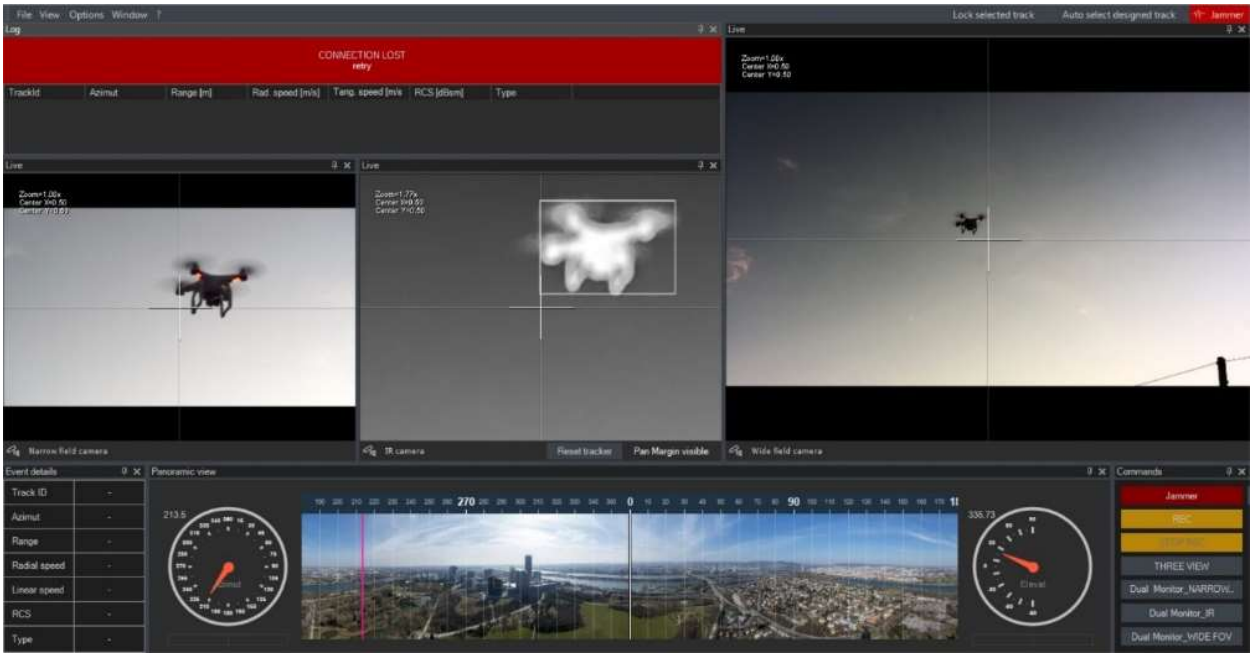
Recognition and video-tracking



The recognition capability is due to imaging sensors, independently from the other sensors, as this activity includes man in the loop. Typically, both EO and IR cameras are used and bore sighted together with the additional provision of a special mounting which allows the installation of an effector, according to the applicable CONOPS. Tracking is performed by both the radar subsystem and the cued camera. Being a TWS[7] system, it can continue monitoring concurrent threats (multi-target) operating in its FoV while designating the cued camera for video tracking. The proposed imaging subsystem integrates a hardware-based video tracking system with robust detection and target tracking software for complex image processing applications. The video tracker analyzes video image sequences from the imaging sensor, mounted on a servo controlled pedestal to keep the camera pointing at the nominated object. In this context, the tracker has two primary processing functions:

- Detecting and locating objects of interest in the video image (object location).
- Controlling the platform (Pan and Tilt) position and rate such that the camera locks and follows the designated object (Pan and Tilt Control).

[7] Track While Scan



Classification

The combined use of the above mentioned subsystems allow a precise classification of the monitored threat. The classification activity populates a local library which can be enriched along with mission performance.

This evolving dataset enriches intelligence and forensic activity with coherent data on intruders or unwanted airspace users. The classification capability collects and stores the following threat data:

- Type of drone
- Cinematics (Radial speed, etc…)
- Radar cross section
- Dimensions
- Segment of mission tracked

The main advantage of radar technology is, if present, an embedded Radar Classificator, which supports operator's task of threat detection and assessment by using:

1. RCS and Kinematics
2. Micro-Doppler Signature, extracted by "micro-observations" of the target

The result of this classificatory activity is a reduced FA rate and increased recognition capabilities, of utmost importance in the threat level assessment. All the collected data are opportunely stored in a mission database which, through a machine learning algorithm, populates the internal threat library, contributing therefore to an increase of performance for the consecutive mission.

Long term, operators will enjoy a substantial reduction of the workload and concurrent reduced time for decision making.

Risk mitigation and signal disruption

The jammer unit performs the functionality of communication channels disruption. This unit allows the jamming on ISM and, optionally, GNSS frequencies in order to inhibit navigation and control systems. The output power has to be adjustable in order to avoid disturbing beyond the distance of the threat. The antennas are highly directive and aligned with the video unit, in order to allow for accurate pointing and reduce the effects of the disturbance outside the area of interest.

Non-kinetic effector of various type can be integrated to the system in order to provide a defense capability to the operating force. Different frequencies can be disturbed and disrupted.

Airport integration

When implemented into the airport environment, the anti-drone solution can be stand alone or integrated in to existing airport infrastructure. Two factors for successful implementation are:

- EMI/EMC prediction
- Integration with airport systems

The possibility to predict EM behavior of RF elements (passive/active) in a complex scenario such as airport environment is of utmost importance. A professional tool providing advanced simulation techniques to perform airport electromagnetic environment analysis as well as airport and en-route electromagnetic site verification is a requirement. This includes performance assessment of any existing Communication, Navigation and Surveillance (CNS) equipment, prediction of the effects on navigational aids by the placement of a new equipment. The SW tool has to include a set of validating, 3D modeling and simulation tools, which are modular and capable of tackling the electromagnetic compatibility (EMC) and electromagnetic interference (EMI) issues that occur within the complex environments of airports and air navigation sites. It also allows the user to create a numerical model of the equipment under analysis, either current or proposed, and an electromagnetic model of the environment surrounding it. It then performs a numerical analysis on the data provided and generates a visual representation of the computed electromagnetic field and the associated air navigation qualities (e.g. DDM, coverage limits). The SW tool also has built-in parameter tools to simulate the behavior of on-board aircraft receivers.

Airport integration also means to disseminate available information, in real time, to the various entities entitled to receive information about occurrences and/or to participate to the response. ATC controllers should be informed and updated about any target flying in ATZs, as well as security officers could be interested in obtaining useful data for the threat level assessment, decision making on the actions to be put in place, and post-event forensics. This is the reason why the anti-drone system will implement an open architecture allowing data to be exchanged (radar tracks, video streams, warning levels, etc…) in various formats and over a wide number of protocols (JSON, XML, DDS and Asterix CAT21).

Anti-Drone dual use for bird strike prevention

Bird strike prevention calls for birds' incursion monitoring. Traditionally implemented by BCUs[8], professionals in charge of inspecting periodically the aerodrome, the task can be optimized with complimentary features by leveraging the radar technology presented in the previous sections. A human observer is able to monitor up to a few hundreds of meters in a single direction per time, with a limited field of view given by physical characteristics of the human body, the daily hour and the meteorological conditions. Radars instead, can extend the capability over these physical constraints into continuous day/night observations, overcoming weather conditions in a 360° coverage at a greater distance, allowing automatic detection, tracking and recording of multiple birds flying on the area of interest. Having this capability implemented, the BCU can build up statistics and produce adequate reporting on:

- Migration paths
- Seasonal occurrences
- Key areas (nests, recoveries, …)
- Habits
- Impact of specific weather conditions

Radars typically are conceived for a single task and, in most of the cases, do not support a dual task mode of operation simultaneously however, nowadays, the new generation of anti-drone radar systems are developed and designed with a set of requirements embracing the multiple capabilities required by aerodromes to detect both Bird and RPAS. In The radar is designed with, features that are embedded with a classifier which is optimized, allowing to implement a dual-use mode accomplishing the desired tasks.

It is also assumed that a complete integration of the system in airport operations allows the selective and accurate activation of countermeasures (e.g. WCS), where required, when really needed, a key capability to reduce the loss of effectiveness due to birds getting use to these devices.

CONCLUSIONS

The rapidly increasing use of civilian and commercial drones, calls for an urgent need for monitoring aerodrome surroundings, especially in the critical paths of landing and take-off. This paper proposes an end-to-end solution, matching present and future requirements of managing potential threats to air navigation safety and airport security. The solution encompasses detection, tracking, recognition, identification and counter measures of drones in a very effective approach, zeroing the impact on aerodrome environment while maintaining the minimum workload for operators but highest level of information sharing and widest coordination to all stakeholders. Finally, the same technological base, if selected opportunely, offers the unpaired capability of supporting the bird strike prevention maximizing the return on the investment.

[8] Bird Control Unit