L3 Technologies

Whitepaper:

Countering the drone threat to commercial airports

Introduction

Airports, Airlines and Air Navigation Service Providers (ANSP) can suffer significant financial losses when there is any disruption to operations, either intentionally or accidentally.

Drones reported flying in the approach, departure or ground operating areas will present a safety hazard and will likely force controllers to restrict operations or close the airport.

Drones seen flying in less critical areas of an airport or its surroundings may also disrupt routine business, given that airport security, police or border authorities will need to respond to those incidents.

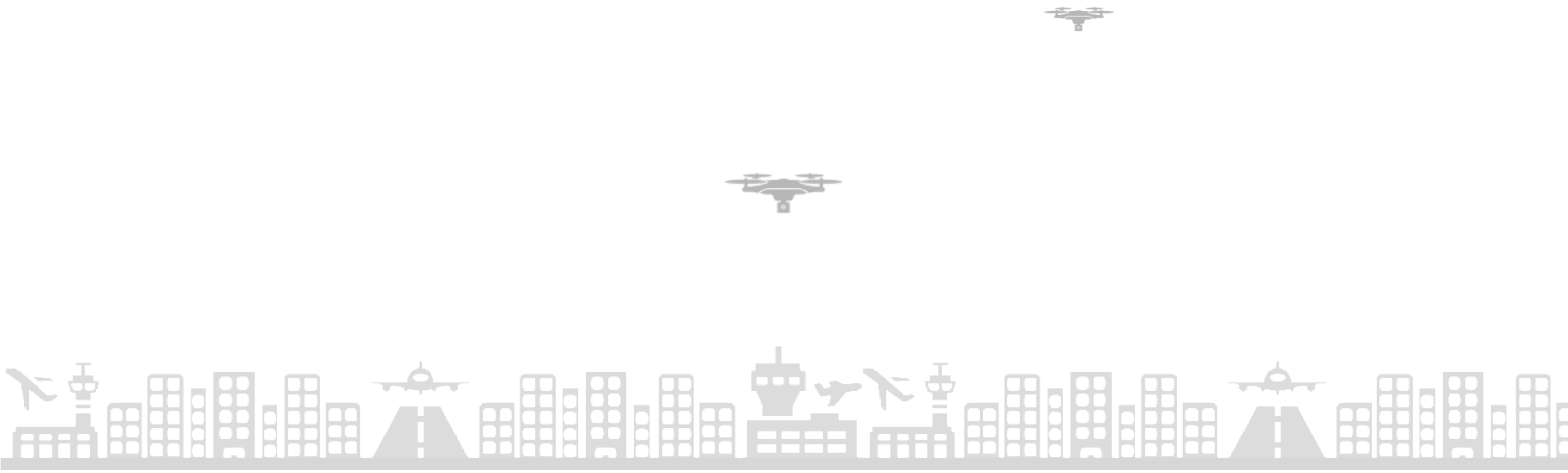
While regulation will deter a large proportion of illegal drone activities, and cooperative drone traffic management could provide further assurance, it is inevitable that airports will continue to be the target of deliberate or accidental disruption from drones.

The detection and disruption of illegal drone activity has previously been the task of military and national security specialists, with highly-specified system requirements. As drone use increases and technology develops, it will be necessary to provide reliable and permanent counter-drone systems at airports.

While the cost of disruption is likely to be significant, the cost of deterrence and/or prevention must also be reasonable, allowing operational authorities to reduce risks to as low as reasonably practical.

Each airport has unique characteristics and faces different level of risk from drone incursion, both in likelihood of event and the potential impact. Therefore, systems for the mitigation of that risk must be flexible, modular and scalable as the threat evolves.

Given the growing threat from illegal drone activity and the challenges of mitigating that threat, it is likely that military-grade capability will be required, but at a commercial price-point.



1. Deploying a Counter-Drone Solution

1.1. Key Factors

Airports have multiple operations, business and security stakeholders within one location, each with their own priorities and each looking for solutions to mitigate the threats of disruption. Furthermore, there are other external stakeholders who have a role in the protection of critical national infrastructure and who may require data for long term planning and immediate response. The threat from drones is just one threat among many, and the factors that should be considered in providing mitigation must take into account the need for integration across the airport enterprise.

Industry data has not previously been available to support an informed discussion on the drone threat and, until recently, disruption caused by drones at airports has been rare. However, the cost of closing runways at primary airports quickly runs into the millions, as recent events at Gatwick have highlighted. It is now highly likely that airport operators, airlines and ANSPs will need to have a clear view of the potential safety and business implications of drone disruption.

The development of a robust business case, aligned to risk management plans, will need to consider many factors. However, for cost-effective procurement of a counter-drone solution, airports should firstly consider deploying a solution that can be adapted over time, so that:

i) The system can grow to be used by the different airport stakeholders,
ii) can be enhanced to meet developing threats, and
iii) with hardware or software components that can be upgraded independently

To provide that flexibility for the future, airports should also consider building any counter-drone capability around a core command and control component which can accept any number of sensors from any supplier.

1.2. Making the response proportional to the risk

It is important to understand the full range of threats, along with the potential solutions that might be available. To build the most cost-effective response, an airport's key stakeholder team should be led and guided by drone security experts and supported by data gathered from observations and sensor equipment.

The aim of this combined team should be to define the risk which each stakeholder requires to be mitigated and how best to deploy sensors and software to gather the required data. The team should also start to formulate the response actions for drones reported in specific locations at specific times, with the overreaching aim to minimise disruption to airport operations.

The desired outcome of initial planning would be an agreed project timeline with milestones and budgets, along with a rolling plan to counter future developments in threat and drone technology.

1.3. Detecting drones

Data from drone events at airports will come predominantly from three sources:

- Visual sightings from aircrew, airport operations staff, security, police, public etc.
- System alerts from specialised drone detection sensors.
- Analysis of data from other existing sensors (CCTV, radar, etc.).

The coordination and integration of data from multiple sources is a complex challenge, and it is unlikely that data from a single source will be of sufficient quality to enable effective decisions to be made.

Sensors for the detection of drones will need to be placed in the most suitable locations to detect and track likely drone activity. It is possible that coverage may also be required in some cases beyond the airport perimeter. This can be accommodated using a network of sensors linked back to a central data integration node. Any real-time data gathered from counter-drone sensors will need to be analysed at this node and presented in a simple and intuitive manner to enable rapid response.

The likely counter-drone coverage required round an airport will depend on the level of risk, and the requirement for the operating authorities to mitigate that risk. Sensors deployed around an airport could provide overlapping and complementary coverage and would be sited based on several factors, including likely threat axes and available airport infrastructure.

Data from specialist counter-drone systems can be integrated with information from existing airport security and operations systems to present a comprehensive picture in an Airport Operations Centre (APOC) or equivalent. Where activities are managed separately (eg: CCTV monitoring in one centre and incident coordination in another), any drone alerts and tracks should be made available in each location in a simple interface on existing IT infrastructure. Existing airport sensors, such as bird detection radars and ground movement sensors, may also be useful in providing additional data sources to reduce false alarms. Integration with systems fitted to "cooperative" drones can also provide crucial information to differentiate threats from other traffic.

1.4. Proximity alerts, both real-time and historical

To be useful for airport operations, drone activity should initially be presented to stakeholders in real time, using a simple interface that allows intuitive interaction. This activity should not require specialist or dedicated operations team resource to monitor or manage. In real time, a flight operations stakeholder will need to make a rapid decision, with speed of detection and the mere presence of a drone being perhaps more important than its exact location. In this situation, it may be sufficient to see the general location of a drone within the airport perimeter. These initial alerts should be made available to all key stakeholders via SMS and/or email.

Other stakeholders may wish to identify the exact track of a drone, for example to help locate the drone's controller or to aid in post-event analysis. In this instance, the precise drone location and track should be capable of being displayed on existing control room screen(s), linked through a web-browser interface to other stakeholders and with alerts relayed to other security staff for a more precise response. Precise tracking and geo-location can also allow the cueing of CCTV and could in future be linked to active ATM systems to allow cooperative airspace management.

To understand the full range of threats, and to conduct detailed post-event analysis, any counter-drone system should have the capability to view and export historical event data, filtered via a time-selected report feature.

1.5. Countering drones – active and passive

Once a drone is detected, tracked and assessed as a threat, decisions can be made regarding the countering of the drone. Countering can be active or passive and there are many options available.

Active responses using "effectors" present many challenges, given the relatively unpredictable nature of a drone's likely flight once it has been disrupted.

- Radio Frequency (RF) jamming is a viable option to disrupt the command signals or the GPS navigation input for a drone. Jamming can be deployed at relatively long range and can be directional, zonal or in a "fence" around protected areas. There are challenges in deploying jamming capabilities in the UK, and airports present a complex RF environment. Given the potential for collateral interference, such countermeasures would be deployed on a case-by-case basis and activation clearly regulated.
- Other active measures, such as net guns, can be effective when a drone is within range, but will require both careful pre-positioning and dynamic coordination once a drone has been detected. This coordination can be achieved through the provision of accurate position and direction of flight of the target drone, to enable timely "intercept" from the ground.
- Using weapons such as shotguns will be a last resort in an airport environment and will always be the preserve of specialist response teams with appropriate authority and engagement criteria.

Passive responses will be dependent on the quality of the information available to the operations team and the perceived risks. For example, it might be possible to restrict aircraft

movements on the ground to certain areas if illegal drone activity is clearly confined to a specific location that can be avoided. In all cases, it is unlikely that a general alert to the mere presence of a drone on or around the airport will provide information of sufficient quality to make confident decisions.

1.6. Counter-drone Concept of Operations (CONOPS) and integration to airport operations

When a drone is detected, by machine or by man, it is virtually impossible to know its intent, or rather the intent of the pilot. Some deductions can be made from the flying location, nature of the flight track, frequency of event and time of day. Knowing the type of drone may not be relevant in the initial stages but can be useful in tailoring sensors and any response to incursions. Deductions can also be made about the general location of the pilot, and if the pilot is in range of sensors, that location can sometimes be usefully pinpointed by data analysis in real time.

At a high level, it is important that a clear path and hierarchy of communication is created to disseminate relevant information to key stakeholders both on and off the airport site so they may react to a drone event without delay. It is also critical to ensure that any counter-drone CONOPS is integrated into emergency response plans, security and ATM procedures. It is possible to deploy systems rapidly (within hours) to provide a level of immediate coverage. However, these systems invariably take time to “settle” into their operating environment and are rarely able to be deployed in the optimum location to meet a more general threat.

The CONOPS for the deployment of a counter-drone system at an airport can largely be pre-conceived and therefore automated, with counter-drone systems responding to pre-set rules. The associated security and operational workflows can also be tested and in many case automated.

1.7. Future evolution and growth

The integration of counter-drone CONOPS into the smooth operations of an airport demands a deeper dive than can be covered by this whitepaper. However, L3 has extensive knowledge of how best to integrate operational activity and can provide practical advice and support as part of any counter-drone solution.

L3 envisages that current methods for detecting and countering the majority of commercially available drones will remain relevant for the next 2-5 years, given the technology that is currently available and on the immediate horizon. It is likely that radar and camera technologies will always be relevant, while RF detection and jamming will need to evolve, as drone command technology changes. Fundamentally, as the threat evolves it will be essential to have a counter-drone system that is flexible and scalable to evolve with that threat.

2. Summary

The threat from illegal drone activity is likely to present a growing challenge to airports operators and key stakeholders, despite regulation and the deterrent effect of legislation. In countering the threat from drones, L3 understands this challenge and has the experience and expertise to provide support to mitigate the risks. As part of this support, L3 considers that the following key factors should inform any future decisions:

- The drone threat is continually evolving, and any mitigation solution must be capable of evolution with that threat.
- No single sensor will detect all drones, and no cooperative system will counter the most disruptive threat from a determined individual
- Systems should have a flexible architecture that allows the addition of new 3rd party sensors and effectors, and which allows networking of sensors from distributed locations.
- Drone activity information must be made immediately available with sufficient quality to allow critical safety and security decisions to be made in a cost-effective manner.
- It is essential to enable the integration of counter-drone systems with existing airport operations, including the use of stakeholders' own drones.
- Counter-drone systems should not be so complicated that they require specialist, dedicated resources to operate - they must be capable of seamless integration with existing security and safeguarding operations.

To learn about how L3's counter-drone solution, Drone Guardian, can overcome the threats and challenges outlined in this whitepaper visit:

https://www.l3-droneguardian.com/