WHITE PAPER:

Countering the drone threats to international airports

Introduction

Air Navigation Service Providers, (ANSP), Airlines, and Airports can suffer major financial losses in case there is a disruption of their operations, be it accidentally or intentionally.

Drones that are reported to be hovering near a flight's approach, departure and ground operating zones can present significant safety hazards and may cause controllers to impose operation restrictions or shut the airport down. If drones are observed flying near other non-critical airport zones or the surroundings, there is a good chance that they can disrupt the airport's routine operations, as airport security officers, border authorities or police officers may have to respond to such incidents.

Although regulations are capable of stopping most illegal drone-related activities with an effective drone traffic system providing further assurance, airports are always likely to remain targeted by drones, either accidentally or deliberately. The disruption and detection of unlawful drone activities used to be the domain of national security and military specialists, with extremely specific system requirements.

As the usage of drones increases & technology advancements are made, it'll become necessary to be able to provide permanent and reliable anti-drone solutions at airports. Although disruptions costs are significant, it is mandatory that prevention or/and deterrence systems be reasonably priced as well, which would enable authorities to minimize risks while remaining practical about the subject as well.

Every airport possesses unique characteristics & faces different risks due to drone incursion. Therefore, it is vital that systems meant to mitigate this risk be scalable, modular, and flexible in the face of evolving threats. As illegal drone activities and related challenges continue to grow at a steady pace, it is highly likely that military-level capabilities will be needed, but at commercial price points in order to be sustainable.

1. Deployment of Counter-Drone Solutions

1.1 Key Factors

All airports come with multiple security and business stakeholders, and multiple operations in a single location. Each member has their own primary priorities and they are all searching for solutions that can minimize disruption threats. Additionally, external stakeholders may be present too, who may play a serious role in protecting key national infrastructure and who may need data for immediate response and for making long-term plans.

The threat posed by drones happens to be just one among many. Factors and solutions that are meant to mitigate disruption risks must also consider that they have to be integrated across the entire airport enterprise as well.

Industry data hasn't been made publicly available yet, which would have supported informed discussions regarding drone threats. Up until recently, drone-related disruptions in airports have always been a rare occurrence. However, shutting down airport runways, especially in international airports, can cost millions, which has already been highlighted by the Gatwick airport incident. It is now quite likely that ANSPs, airlines, and airport operators will be able to come up with a clear understanding of the business implications and safety issues that come with drone-related disruption incidents.

Before developing a robust and sustainable business case that is in line with risk management strategies, one must first consider several factors. However, in order to deploy cost-effective counter-drone measures, airports must first consider deploying solutions, which can be adapted over time, ensuring that:

i. This system can be expanded for usage by various airport stakeholders,
ii. It can be thoroughly enhanced for meeting developing threats.
iii. It can be used along with software or hardware components, which can be updated independently.

In order to provide flexibility down the road, airports must also consider developing counter-drone solutions around core control and command components that can utilize additional sensors provided by suppliers.

1.2. Making the solution proportional to risks taken

It is important to fully understand the entire range of drone-related threats and potential solutions, which may be available for your usage. For building cost-effective responses, the key stakeholder group in an airport must be guided and led by qualified drone security professionals and supported by using data obtained from sensor equipment and observations.

This combined group must aim to define risks which the stakeholders would like to have mitigated immediately and find out optimal ways for the deployment of software and sensors for gathering required data and information. This team must also devise response actions in case drones are observed in specific locations at specific times and aim to mitigate the airport activity disruptions.

This initial desired outcome of planning phase would be to establish a project timeline along with budgets and milestones and devise a rolling strategy for countering upcoming threats and drone technology advancements.

1.3. Detection of drones

Drone event-related data at airports shall be predominantly obtained from 3 sources:

- Via the analysis of information obtained from existing sensors such as radar, CCTV, etc.
- Via system alerts sent from drone detection and alarm sensors
- Visual sightings obtained from the public, police, security, airport staff, and aircrew.

The integration and coordination of information from several sources are likely to be highly complex challenges. It is unlikely that information obtained from one, single source is going to be of the necessary quality required for enabling the making of effective decisions.

Drone detection sensors will have to be located in suitable locations for the tracking and detection of drone activity. It is possible that coverage might be necessitated in a few cases beyond an airport's perimeter. However, this can be ensured by utilizing a sensor network that is linked to central information integration nodes. Any kind of real-time information obtained from these anti-drone sensors will have to be thoroughly analyzed at the node and presented in an intuitive and simple manner in order to ensure a rapid response.

The required counter-drone solutions throughout an airport's surroundings are dependent on the risk levels and requirements of the airport authorities, who are tasked with mitigating these risks. Sensors that are deployed around airports can provide complementary coverage and overlapping, and will be placed based on many factors, which include airport infrastructure and threat axes.

Data obtained from these specialist anti-drone solutions may be integrated along with data obtained from pre-existing airport operation and security systems for presenting a comprehensive image of the entire situation in an APOC (Airport Operations Centre) or equivalent. When such activities are handled separately (For instance, CCTV monitoring could be in one place and incident coordination activities in another center), drone tracks and alerts must be provided in each center using an interface built on pre-existing IT capabilities. Airports sensors like ground movement trackers and bird radars can be useful for providing multiple data sources in order to minimize false alarms. System integration may also be enabled for cooperative drones that can provide vital information, which help in distinguishing between threats and other traffic sources.

1.4. Historical and real-time proximity alerts

In order to aid airport operations and activities, drone-related activity has to be initially presented to the stakeholders on a real-time basis, using simple interfaces, which allow intuitive interaction. These activities won't need a dedicated or

specialist operations team for managing or monitoring the whole deal. Flight operations stakeholders will have to make rapid decisions on a real-time basis with detection speeds and drone presence alerts being far more important compared to its location. In such situations, it could be enough to obtain a drone's general location within an airport's perimeter. Such initial alerts have to be provided to every key stakeholder via email or/and SMS.

Several other interested parties may also wish to track and identify a drone. This could aid in locating the controller of a drone or help during the analysis of an event. In this example, precise drone track and location must be displayed on control room screens, linked via web browser interfaces to other important stakeholders. Alerts could also be relayed to security staff members for obtaining precise responses. Geolocation and precise tracking can help cue CCTV and may even be connected to ATM systems in order to permit airspace management in a cooperative manner.

To gain a better understanding of all possible threats and for conducting a detailed analysis of the events, counter-drone systems must have the ability to export and view event data, which may use time-selected filter report features.

1.5. Passive and active counter-drone measures

Once a certain drone has been tracked, detected and assessed to be a threat, several decisions have to be made for countering this drone. These measures may be passive or active, and there happen to be multiple options available that can be used effectively.

Active responses include effectors, however, these come with many challenges, as it can be difficult to predict the drone's flight path after it's been successfully disrupted.

- RF or Radio Frequency jamming happens to be a useful option for disrupting GPS navigation drone inputs or command signals. Drone jamming measures may be deployed over a long-range and may be zonal, directional or placed in a certain "fence" around several protected areas. Several challenges remain for the deployment of jamming abilities in the United States, as airports can present an extremely complex RF environment. As there is a likelihood of great collateral damage, these countermeasures must only be deployed after due consideration has been given.

- Other measures including net guns may be effective in case drones happen to be within a certain range. However, this will need dynamic coordination and careful positioning after a drone has been detected. The coordination may be achieved via the discovery of the drone's flight direction and accurate position, which would enable ground-based efforts to intercept it in a timely manner.

- Utilizing weapons like shotguns is only to be allowed when no other options are viable in the airport's environment. This should only be handled by professional response teams that have the appropriate engagement criteria and authority. Passive responses may be based on the level of data available to an operations team and perceived risks. E.g. It may be viable to start restricting aircraft movement to specific areas alone in case illegal drone activities are confined to specific avoidable locations. In such cases, it is doubtful whether a mere drone presence alert near or on the airport is going to provide data that is comprehensive enough to come up with confident decisions and analysis.

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

When drones are detected by either man or machine, it is virtually impossible for understanding its intention or the intention of its pilot. A few deductions may be

possible, based on its flying location, flight track nature, event frequency, and timing. Although knowledge about the drone variant may not seem relevant, it can help tailor sensors and responses to incursions. Several deductions are also possible, which can help track the pilot's location. If the drone pilot happens to be within sensor range, the location can be traced out using data analysis methods working on a real-time basis.

At high levels, it is vital that an established path and communication hierarchy be created in order to disseminate information to all key stakeholders, off and on the

airport location, which allows them to react without a delay. It's critical to make sure than counter-drone CONOPS are integrated into ATM procedures, security, and emergency plans. It's possible to deploy certain systems rapidly, providing them with immediate coverage to a certain level. However, the systems will take time to operate effectively in their environment and can rarely be deployed at optimal locations for meeting general threats.

CONOPS regulations for counter-drone system deployments can be preprogrammed and automated beforehand, enabling counter-drone solutions to respond based on pre-existing rules. Associated operational and security workflows may also be properly tested and automated in many cases.

1.7. Future growth and evolution

Integrating counter-drone CONOPS strategies into an airport's smooth operations requires a greater dive that hasn't been covered in this whitepaper. But DGS possesses extensive knowledge about integrating operational activity and can give practical support and advice related to counter-drone solutions.

DGS predicts that the currently used methods for defending against and detecting commercially available drone technologies will remain useful for another two to five years, as they show significant promise against technology that is already in the pipeline. It is also likely that camera and radar technologies will remain relevant. However, RF jamming and detection will have to evolve further since drone

command technologies are constantly changing. On a fundamental level, with evolving threats, it is essential to maintain counter-drone systems that are scalable and flexible to keep up with evolving threats.

2. Summary

Illegal drone activity-related threats are only likely to present growing challenges to key stakeholders and airport operators, in spite of deterrent legislation and regulation. In order to counter the threat prosed by drone technologies, DGS understands the various challenges on the horizon and possesses the necessary expertise and experience for providing support to mitigate any risks. DGS considers these key factors to play an important role in future decisions such as:

Drone threats are continually evolving and mitigation solutions must be capable of evolving with these threats. No single sensor is capable of detecting all drones.

Systems must have flexible architecture built into them, which can add new third-party sensors and effectors. They must also allow sensor networking from several deployed locations.

Data related to drone activities have to be provided immediately with ample quality in order to make critical security and safety decisions that are cost-effective as well.

It is vital to integrate counter-drone solutions with pre-existing airport mechanisms, which may include using the drones of stakeholders as well.

Counter-drone solutions cannot be complex. They should not have to need dedicated, specialist resources to carry out operations – They have to be able to integrate seamlessly with existing safeguarding and security operations.

To find out more regarding Urban Dynamite, the counter-drone system offered by DGS, visit https://www.usdgs.com/ and discover how it overcomes the challenges and threats outlined in the whitepaper.