WHITE PAPER

Countering Drones at Airports

What to keep in mind when evaluating solutions

R1: Jan 2019

robin
radar systems

Executive Summary

The growth in drone use has caused an upsurge in near-miss reports and increased the risk of drones disrupting or even colliding with air traffic.

Consumer and commercial drones typically weigh under 10kg and mostly less than 2kg. Quadcopters with four horizontal rotor blades are most common but there are also small fixed-wing drones.

Drones are able to stay in the air for up to 30mins at a time, with quick battery changes and/or multiple drones able to cause persistent disruption. Regulations notwithstanding, drones are certainly capable of flight up to 6000m altitude and up to 8km from their operator and controller, which easily brings them into the same airspace as passenger aircraft approaching or taking-off at airports.

Studies have shown that a drone collision with an aircraft is more damaging than an equivalent energy bird strike, and that drones colliding with aircraft can damage the structure to cause a crash.

Besides the unintentional disruption or collisions caused by drone operators who either don't know, or choose to ignore, drone safety regulations around airports, there is another risk. From those who intentionally choose to cause disruption.

Consumer drones are capable of lifting small payloads of 500g and commercial drones can carry upwards of 6kg. If a terrorist wants to blow up a passenger plane, delivering the explosives by drone is probably more likely than through airport security on the ground.

There are different technologies available for both monitoring and countering-drones. Monitoring is allowed and recommended. Neutralising drones is still (in most countries) not legally permitted.

Typical monitoring technologies include Radio Frequency (RF) Analysers, Acoustic Systems, Cameras, and Radar. Each has their individual pros and cons and it is recommended that systems purchased for airport drone monitoring are an integration of:

- RF, for identification and triangulation of both drone and controller (if radio signals present);
- Cameras, for visual identification and understanding of threat and intent; and
- Radar, for long range detection, accurate localisation and tracking (also from drone swarms), and drone classification even from autonomous drones not sending any radio signals.

When using radar for drone detection, be it stand-alone or part of an integrated system, it should be micro-doppler radar. Specially designed micro-doppler radars are available that can differentiate birds from drones. This avoids drone alarms caused by birds; a common issue with radar.

Typical countermeasure technologies include, RF Jammers, GPS Spoofers, High Power Microwave (HPM) Devices, Nets and Net Guns, High Energy Lasers, and Birds of Prey. None are allowed due to regulations, but should an exemption be approved, Net Guns have a low collateral damage risk at an airport.

RF jamming, GPS spoofing and Electromagnetic Pulses (EMPs) generated by HPM Devices have an increased electronic collateral damage risk at airports but could be used successfully if coordinated and managed correctly.

What's the Problem (with drones at airports)?

Use of drones both recreationally and commercially has grown explosively over the last few years. They've become affordable, easy to obtain and simple to fly. This creates new opportunities, but also poses new threats. Especially at airports.

The growth in drone use has caused an upsurge in near-miss reports and increased the risk of drones disrupting or even colliding with air traffic. Both of which have already occurred world-wide on several occasions.

Besides the unintentional disruption or collisions caused by drone operators who either don't know, or choose to ignore, drone safety regulations around airports, there is another risk. From those who intentionally choose to cause disruption.

That could be simply by flying a drone over an airport or deliberately maneuvering a drone into the flight path of approaching or departing aircraft in an attempt to cause a collision.

It could also be from a terrorist aiming to deliver and detonate a small explosive on the wing of an aircraft sitting at the gate. An aircraft fully loaded with passengers and fuel...

What Type of Drones are a Problem?

The word drone covers many different aircraft. When it comes to the risk of drones at airports, we're not talking about the ones which carried out drone strikes in Afghanistan and Pakistan during the War on Terror.

We're talking about consumer and commercial drones, typically weighing under 10kg and mostly weighing less than 2kg. Most often these are quadcopters with four horizontal rotor blades. But the term drone also includes small fixed-wing aircraft as well.

Other names for drones are Small Unmanned Air Vehicles (SUAVs) and Small Unmanned Air Systems (SUAS). These terms are more typically used in the defence industry.

Some of the most popular and capable drones on the market currently come from a company called DJI. Their most popular models and relevant specifications are provided below:

	Spark	Mavic	Phantom	Inspire	Matrice 600
					
Dimensions	14x14x6cm	31x24x9cm	29x29x20cm	48x47x32cm	167x152x73cm
Weight	300g	700g	1.4kg	3.4kg	10kg
Max. Flight Time	16 mins	31 mins	30 mins	27 mins	18 mins
Max. Speed	50km/h	72km/h	72km/h	94km/h	65km/h
Max. Altitude	4km	6km	6km		4.5km
Max. Transmission Distance	2km	8km	7km	7km	5km
Max. Recommended Payload	n/a	n/a	n/a	810g	6kg
Autonomous Flight Capable?	Yes	Yes	Yes	Yes	Yes

Source: dji.com

INTENTIONAL AND PERSISTENT AIRPORT DISRUPTION

Flight times for drones are relatively limited - between 15 and 30 minutes. Fresh batteries can be exchanged quickly though (within a matter of seconds). This means flight times can be significantly extended with very short, but frequent, interruptions for battery swaps.

If the drone operator's goal is intentional and persistent disruption at your airport, this could easily be achieved with a set of spare batteries or even multiple drones.

AIRCRAFT CAN EASILY ENCOUNTER A DRONE DURING TAKE-OFF OR APPROACH

Most often drones are operated close to the ground, and in most countries the law requires that drones stay below set altitudes. Typically, around 120m. This ensures they stay far below most manned aircraft. It should be noted though that most drones are capable of flying significantly higher than that. Up to 6km in some instances. Not a danger to most aircraft at cruising altitude but certainly a danger within the take-off and approach funnels at airports.

THE OPERATOR OF THE DRONE MAY NOT EVEN BE AT YOUR AIRPORT

Another drone regulation, current in most countries, is that drones may only be operated within line-of-sight (LOS). To give this a value it means that the drone operator should be within at least 500m of the drone. As you'll see from the table, again, the capability far outstrips the regulation, with drones capable of being controlled from up to 7 or 8km away.

This means that the operator could be controlling their drone at your airport from several kilometres away. Which makes apprehension and subsequent prosecution harder.

WHAT HAPPENS WHEN A DRONE AND A PASSENGER AIRCRAFT COLLIDE?

As you can see from the above table consumer drones are typically around 30cm across and weigh less than 2kg. The professional drones are between 50cm and 1.5m and weigh upwards of 3kg all the way up to 10kg. Batteries take up most of the weight.

In a study conducted by the University of Dayton Research Institute (DRI), a DJI Phantom drone (measuring 30cm across and weighing 1.4kg) was fired at a speed 383km/h toward the wing of a general aviation (GA) aircraft. The test conducted in a laboratory simulated the conditions of an aircraft hitting a drone on approach to the runway. The drone punctured a hole through the leading edge of the wing, and carried on deep into the structure, hitting and deforming a spar.

According to Kevin Poorman, Group Leader of Impact Physics for DRI:

> ***"All the weight of the aircraft is suspended on the spars... If you damage the spar enough on that side, you would not survive. The aircraft would crash."***

While that test was on a GA structure, the UK Civil Aviation Authority (CAA) has downplayed the risk of damage, at least to large passenger aircraft, given they are built to higher specifications. They have though said that:

> ***"Drone collisions cause greater structural damage than bird strikes for equivalent impact energy levels."***

IS THAT DRONE CARRYING A CAMERA, A PIZZA, OR A BOMB?

As you can see above, some drones are designed for carrying payloads. The DJI Inspire can carry almost a kilogram. The DJI Matrice 600 can move 6kg. And those are just the recommended payload weights - they are capable of more.

The DJI Phantom for example, which is not designed for carrying additional payloads has been modified by ISIS to carry and deploy 40mm grenades (weighing around 400g). Hundreds of deadly attacks like this have been carried out in Iraq and Syria.

Two DJI Matrice 600's were used in the assassination attempt on President Maduro of Venezuela in 2018. Although ultimately unsuccessful, these drones, capable of lifting at least 6kg, carried and detonated explosives in the air, near to the President.

Although no Drone Borne Improvised Explosive Device (DBIED) has been signalled at an airport yet, the barrier to entry is low. Far lower than trying to get a bomb onto an aircraft through traditional means.

Additional Drone Challenges

Most drones are controlled using radio. And more often than not, they're controlled using Wi-Fi. The typical Wi-Fi frequencies used are 2.400 to 2.483 GHz or 5.725 to 5.825 GHz. Data is usually sent both ways; from controller to drone and from drone to controller. Both act as radio transmitters and receivers.

Drone-to-controller data often contains the drone's position, speed, heading, and altitude, as well as a live video feed. The live video feed and all the telemetry is normally displayed on a tablet or smartphone, which is connected with, and mounted on, the operator's controller. This provides the operator with remarkable situational awareness allowing them to control and manoeuvre their drone with high precision.

AUTONOMOUS FLIGHT

Used out-of-the-box, a drone operator typically controls the drone in real-time. But it's also possible to set way points up so the drone flies autonomously to pre-set locations.

A safety feature which many drones employ is to have a home location setup so if something goes wrong, like when the controller signal is lost, the drone can automatically fly to that pre-set home location again.

Drones can also be modified so they don't transmit any data at all. This technique can be used if the operator wants their drone to avoid radio detection systems.

SWARMS

While we mostly talk about single drones, swarms of drones are a very real possibility. Intel has put on drone shows with up to 1000 synchronised drones, all pre-programmed and controlled from a single source. And a Russian Airbase in Syria was attacked with 13 pre-programmed drones armed with explosives. That drone swarm was reportedly launched from 50km away.

FRIEND OR FOE

With drones being used more and more for commercial activities and by the emergency services, it's realistic to already think about how to determine which drones are being used legitimately at your airport (like for aircraft inspections) and which are unauthorised.

For example, during the Gatwick Airport disruption in December 2018, there were reports that some of the drone sightings may have actually been of police drones. The resulting confusion may have caused the airport being closed for longer than necessary.

What's Solutions are Available for Countering Drones at Airports?

Currently, most airports rely on visual sightings and alerts from pilots, ground staff, and the public. This passive approach has one major benefit of course; it's free. At least until an incident occurs like at Gatwick Airport in December 2018. That was expensive. Estimates range from tens to hundreds of millions of pounds lost due to closure of the airport.

Not having a robust drone monitoring system in place means you don't have the information you need to make decisions. And the information you do receive will be unpredictable, unreliable and erratic.

> ***"Question: Do you want to be informed about drone near-misses by airliner pilots or do you want to inform the airliner pilots about the drones – before it's a near-miss?"***

Safety and uncertainty don't mix well in an airport environment. The result is that runways, or entire airports, will be closed for far longer than is necessary. And that translates into unnecessary costs and potentially negative PR.

Many forms of equipment for countering drones have come onto the market in the last few years. These can be roughly divided into two categories: Monitoring Equipment; and Countermeasures.

Drone Monitoring Equipment

Monitoring equipment can be passive (simply looking or listening) or active (sending a signal out and analysing what comes back) and can perform several functions, including:

- Detection
- Classification or Identification
- Locating and Tracking
- Alerting

Not all equipment performs all of the above functionality at the same time.

There are four main types of drone monitoring equipment:

- Radio Frequency (RF) Analysers
- Acoustic Sensors (Microphones)
- Optical Sensors (Cameras)
- Radar

RADIO FREQUENCY (RF) ANALYSERS

RF Analysers consist of one or more antennas to receive radio waves and a processor to analyse the RF spectrum. They are used to try to detect the radio communication between a drone and its controller. Some systems are able to identify the more common drone makes and models, and some can even identify the MAC addresses of the drone and controller (if the drone uses Wi-Fi for communication). This is especially useful for prosecution purposes – proving that a particular drone and controller were active. Some high-end systems can also triangulate the drone and its controller when using multiple radio units spread far apart.

Pros: Can be low cost, detects (and sometimes identifies) multiple drones and controllers, passive so no licence required, some can triangulate drone and controller position.

Cons: Doesn't always locate and track drones, can't detect autonomous drones, less effective in crowded RF areas, typically short range.

ACOUSTIC SENSORS (MICROPHONES)

Usually, a microphone, or microphone array (lots of microphones), which detect the sound made by a drone and calculate a direction. More sets of microphone arrays can be used for rough triangulation.

Pros: Medium cost, doesn't normally locate but can provide drone direction

Cons: Doesn't work as well in noisy environments, very short range (max. 300-500m)

OPTICAL SENSORS (CAMERAS)

Essentially a video camera. As well as standard daylight cameras, optical sensors can be infrared or thermal imaging.

Pros: Provides visuals on the drone and it's (potential) payload, can record images as forensic evidence for use in eventual prosecution.

Cons: Difficult to use for detection by itself, high false-alarm rates, mostly poor performance in dark, fog, etc.

RADAR

Device using radio energy to detect an object. A radar sends out a signal and receives the reflection, measuring direction and distance (position). Most radars send their radio signal as a burst, then listen for the 'echo'. And almost all radars are designed to not pick up small targets. They are designed for large object tracking, like passenger aircraft.

Pros: Long range, constant tracking, highly accurate localisation, can handle hundreds of targets simultaneously, can track all drones regardless of autonomous flight, independent of visual conditions (day, night, fog, etc.)

Cons: Detection range dependant on drone size, most do not distinguish birds from drones, requires transmission license and frequency check to prevent interference.

Drone Countermeasures Equipment

Countermeasures can be grouped as either:

- Physically destroying the drone;
- Neutralising the drone; or
- Taking control of the drone.

You should also be aware that, although the technology is available, current regulations in most countries forbid the use of any of the following technologies to be used for neutralising drones. Exceptions are sometimes made for military or law enforcement agencies.

LOCATING AND PHYSICALLY APRHENDING THE DRONE OPERATOR

One method which is allowed is for security or law enforcement personnel to simply locate and apprehend the drone operator, forcing them to land the drone. But you need to find them first.

RF JAMMERS

An RF Jammer is a static, mobile, or handheld device which transmits a large amount of RF energy towards the drone, masking the controller signal. This results in one of four scenarios, depending on the drone:

1. Drone makes a controlled landing in its current position
2. Drone returns to user-set home location (which could be set to a target position instead of home)
3. Drone falls uncontrolled to the ground
4. Drone flies off in a random uncontrolled direction.

Pros: Medium cost, non-kinetic neutralisation.

Cons: Short range, can affect (and jam) other radio communications, can result in unpredictable drone behaviour, could unintentionally send drone to its target.

GPS SPOOFERS

This device sends a new signal to the drone, replacing the communication with GPS satellites it uses for navigation. In this way the drone is ‘spoofed’ into thinking it’s somewhere else. By dynamically altering the GPS coordinates in real-time, the drone’s position can be controlled by the spoofer. Once control is gained the drone can be directed to a ‘safe zone’, for example.

Pros: Medium cost, non-kinetic neutralisation.

Cons: Short range, can affect (and jam) other radio communications.

HIGH POWER MICROWAVE (HPM) DEVICES

High Power Microwave (HPM) devices generate an Electromagnetic Pulse (EMP) capable of disrupting electronic devices. The EMP interferes with radio links and disrupts or even destroys the electronic circuitry in drones (plus any other electronic device within range) due to the damaging voltage and currents it creates. HPM devices may include an antenna to focus the EMP in a certain direction, reducing the potential collateral damage.

Pros: Within range the drone can be stopped effectively, non-kinetic.

Cons: High cost, risk of unintentionally disrupting communications or destroying other electronic devices in the area, drone effectively switches off instantly falling uncontrolled to the ground.

NETS & NET GUNS

Firing a net at a drone, or otherwise bringing a net into contact with a drone stops the drone by prohibiting the rotor blades. There are three main types:

- Net Cannon fired from the ground: can be hand-held, shoulder-launched, or turret-mounted. Anywhere from 20m to 300m effectiveness. Can be used with or without a parachute for controlled descent of the captured drone.
- Net cannon fired from another drone: overcomes the limited range of a net cannon on the ground. Can be difficult to capture another moving drone. Normally used with a parachute for controlled descent of the captured drone.
- Hanging net deployed from a 'net drone'. The drone is captured by manoeuvring the friendly net carrying drone towards the rogue drone. The 'net drone' will normally be capable of either carrying the rogue drone to a safe zone, or if it is too heavy, can release the captured drone with or without a parachute for controlled descent.

Pros: Physically captures drone – good for forensics and prosecution, ground-launched net cannons are semi-automatic with high accuracy, drone deployed nets have long range, low risk of collateral damage.

Cons: Kinetic solution could result in debris depending on parachute options, drone deployed nets imprecise and long reload time, ground-launched nets have short range.

HIGH-ENERGY LASERS

A high-powered optical device which produces an extremely focused beam of light, or laser beam. The laser defeats the drone by destroying the structure and/or the electronics.

Pros: Physically stops the drone.

Cons: High cost, risk of collateral damage, large system, mostly experimental technology.

BIRDS OF PREY

Eagles have been trained to capture small drones. This can be a low-tech solution but requires a lot of man-power for training (at least 1 year per bird) and maintaining the birds of prey. The counter-drone team within the Dutch police, who were the original users, disbanded the service due to the birds not always capturing drones on command.

Pros: If the birds are available at your location, interception of the drone can be quick and accurate with low risk of collateral damage.

Cons: Difficult to operationalise, birds don't always listen to capture command, man-power intensive training and maintenance, birds could be a hazard themselves at airport.

Recommendation

AIRPORTS NEED AN INTEGRATED SYSTEM

None of the solutions discussed earlier in this white paper are considered to be a 'silver bullet'.

The most effective counter-drone system is a combination of all, or some, of the above; a system of systems.

And you should decide if you want, or are able (operationally and legally), to combine monitoring solutions with countermeasures.

BUT WHAT'S THE POINT IN MONITORING IF WE CAN'T USE COUNTERMEASURES?

Here's another question: does your smoke alarm at home put out the fire as well?

But you still have a smoke alarm. Right? It would be irresponsible and dangerous to remove it even.

It's a cliché, but it's true; what you don't measure you can't manage.

The first step in countering the problem is understanding the problem; how often it occurs, where does it happen, what kind of drones are appearing, and what is their intent?

You should also have a process in place for what to do when it does happen. The outcome based on the answers to the above questions.

And to do that, you're going to need an effective drone monitoring system. For airports we recommend a mixture of at least a drone radar and an RF device, preferably with a camera.

This gives you the long range, early warning, and high-accuracy tracking of the radar, the identification of the drones and controllers by the RF device, and the visual confirmation of the camera.

Each individual module in such an integrated system could be prone to false alarms by itself. But having the different technologies working together provides reconfirmation and adds redundancy.

YOU NEED MICRO-DOPPLER RADAR AT THE HEART OF YOUR INTEGRATED SYSTEM

While we wrote about the pros and cons of radar earlier, they mostly apply to traditional radars. Traditional target tracking radars are not good at detecting and tracking drones. At Robin Radar Systems, we work with micro-doppler radar, a special radar technology which *is* suited for detecting, tracking and most importantly, classifying, drones.

In the case of a drone, micro-doppler radar can identify if there are propellers present within a small moving target – by detecting the speed differences in the spinning rotor blades. Some blades are moving towards the radar and some are moving away.

Using this method, birds can easily be ignored, as they don't have propellers. And the technique works for both quadcopters (horizontal propellers) and fixed-wing aircraft (vertical propellers).

Our micro-doppler radar was designed specifically for detecting, classifying and tracking drones, and it counters some of the cons we mentioned earlier.

In particular:

- Low-cost alternative to traditional target tracking radars
- Automatically classifies drones apart from birds, so no false alarms from birds
- Low power, so safe to operate and easy to gain transmission permits

In addition, it can:

- Provide early warning with long-range detection
- Detect and track autonomous drones which can't be identified by RF systems
- Provide 360-degree coverage with a single radar unit

Micro-Doppler Radar 'ELVIRA®' at Berlin Airport During ILA 2018

Photo Credit: ESG

Conclusion

Studies have shown that a drone collision with an aircraft is more damaging than an equivalent energy bird strike, and that drones colliding with aircraft can damage the structure to cause a crash.

Besides the unintentional disruption or collisions caused by drone operators who either don't know, or choose to ignore, drone safety regulations around airports, there is another risk. From those who intentionally choose to cause disruption.

There are different technologies available for both monitoring and countering-drones. Monitoring is allowed and recommended. Neutralising drones is still (in most countries) not legally permitted.

Typical monitoring technologies include Radio Frequency (RF) Analysers, Acoustic Systems, Cameras, and Radar. Each has their individual pros and cons and it is recommended that systems purchased for airport drone monitoring are an integration of:

- RF, for identification and triangulation of both drone and controller (if radio signals present);
- Cameras, for visual identification and understanding of threat and intent; and
- Radar, for long range detection, accurate localisation and tracking (also from drone swarms), and drone classification even from autonomous drones not sending any radio signals.

When using radar for drone detection, be it stand-alone or part of an integrated system, it should be micro-doppler radar. Specially designed micro-doppler radars are available that can differentiate birds from drones. This avoids drone alarms caused by birds; a common issue with radar.

Typical countermeasure technologies include, RF Jammers, GPS Spoofers, High Power Microwave (HPM) Devices, Nets and Net Guns, High Energy Lasers, and Birds of Prey. None are allowed due to regulations, but should an exemption be approved, Net Guns have a low collateral damage risk at an airport.

RF jamming, GPS spoofing and Electromagnetic Pulses (EMPs) generated by HPM Devices have an increased electronic collateral damage risk at airports but could be used successfully if coordinated and managed correctly.

To find out more about how your airport can counter drones with an integrated micro-doppler radar, visit www.robinradar.com/markets/drone-detection/ or get in touch with our counter-drone team at info@robinradar.com.

About Robin Radar Systems

Our mission is to provide actionable information that increases safety and security for both humans and birds. We do that by combining purpose-built radars with unique software algorithms.

Our bird radars are installed at numerous civil and military airports around Europe, including Amsterdam, Frankfurt, Berlin and Copenhagen. There we track birds to prevent birds striking aircraft.

We also protect birds themselves and help to reduce the environmental impact of wind turbines with our bird radars at wind farms.

Our counter-drone radars have regularly been used to protect infrastructure, events and VIPS from rogue drones, sine 2016.

Listed in the top three most innovative Dutch companies, we continue to research, develop, manufacture, and above all, innovate.