www.crfs.com

RF SOLUTIONS FOR AIRPORTS

KEEPING AIRPORTS SAFE

- RF interference hunting
- VHF and ILS compliance
- GNSS jamming
- Drone detection

CRFS

EXTRAORDINARY
RF TECHNOLOGY

CR-005727-WP

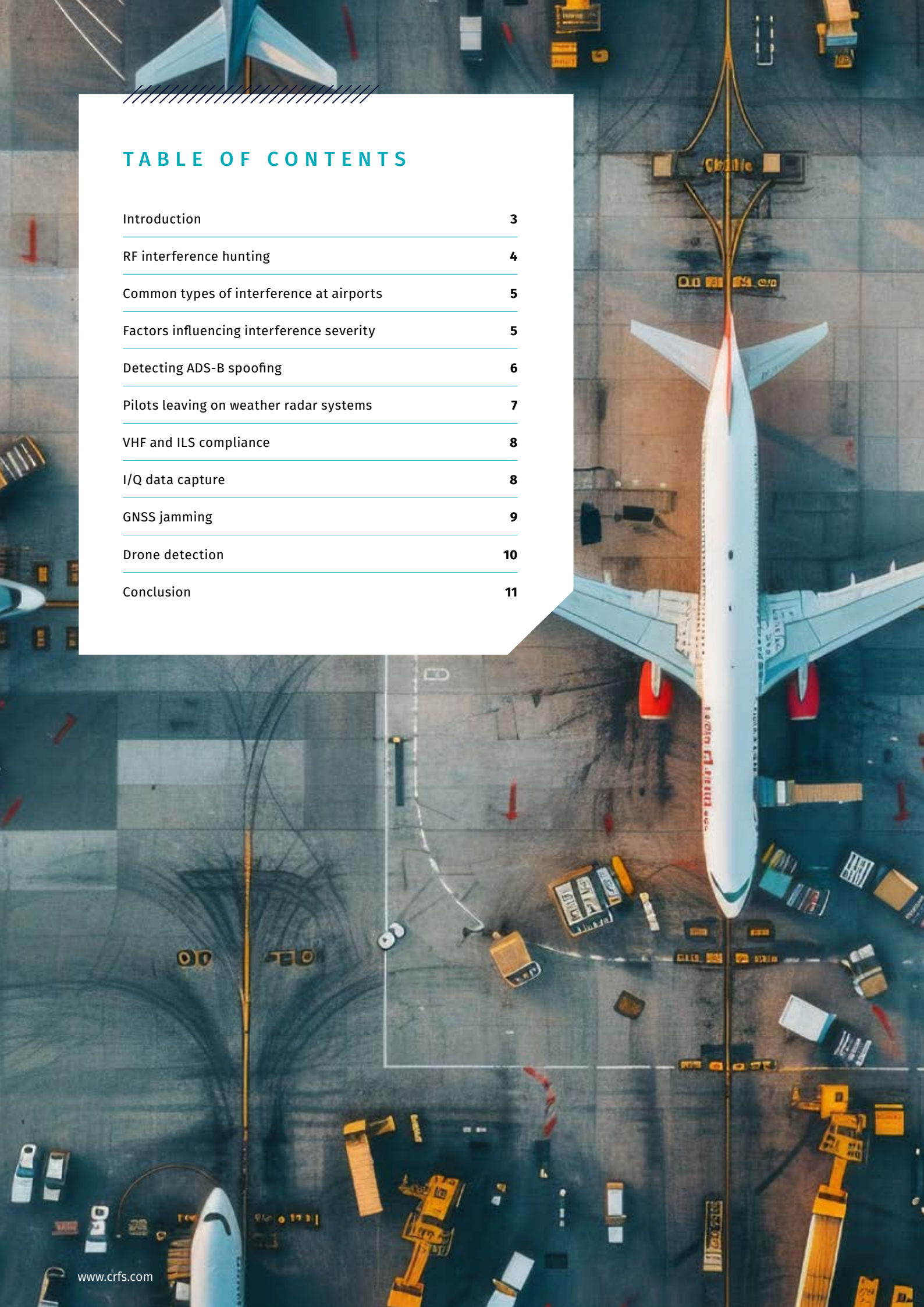

TABLE OF CONTENTS

Introduction	3
RF interference hunting	4
Common types of interference at airports	5
Factors influencing interference severity	5
Detecting ADS-B spoofing	6
Pilots leaving on weather radar systems	7
VHF and ILS compliance	8
I/Q data capture	8
GNSS jamming	9
Drone detection	10
Conclusion	11

INTRODUCTION

The air transport industry's forecasted growth is impressive, and the International Civil Aviation Organization anticipates that both passenger and cargo traffic will continue to enjoy continued growth over the coming years.

However, growth brings challenges for airports: it amplifies vulnerabilities, increases pressures, and heightens complexities. These challenges add to a situation that already requires careful management.

Due to the density of radio frequency (RF) emitting devices at airports, some of the most severe threats are the invisible ones lurking in the spectrum. From two-way radiocommunications systems to Instrument Landing Systems and Voice Communication Control Systems (VCCS), airport spectrum is awash with signals across a wide frequency range.

A congested spectrum increases the chance of unintentional interference, potentially having a negative impact on safety and operations.

For example, if the fire service's radios or communication systems are not working correctly, the whole airport must be temporarily shut down. Any interference must be searched for proactively and dealt with swiftly.

However, the most significant threats will likely come from outside the airport. The illegal flying of drones within flight restriction zones (FRZs) and intentional or unintentional jamming of critical frequencies are severe security risks. These threats must be immediately geolocated and mitigated.

Keeping the spectrum safe and operational requires a mix of procedures and standards, supported by continuous monitoring and management to help ensure compliance. Using RF technology to proactively monitor the spectrum allows security teams to detect, locate, and address any threat—ensuring safety and security at airports.

61 AIRPORTS
passenger volume 25 million + per year

8.6 BILLION
global passenger traffic in 2023

100,000+
commercial flights every day

400
departures per hour

10 MILLION
passengers transported every day

3.5%
is the aviation industry's annual contribution to GDP (US$ 2.7 trillion)

US$ 18 BILLION
worth of goods transported every day

65 MILLION
jobs globally created by the air transport industry

97.8 MILLION
jobs and US$5.7 trillion in GDPE - expected growth by 2036

RF INTERFERENCE HUNTING

RF interference can degrade the quality of essential navigation, communication, surveillance, runway overrun prevention, and traffic collision avoidance systems. It can be intentional or unintentional, internal or external, in-band or out-of-band. Regardless of where it comes from, interference must be swiftly identified and addressed at airports to avoid disruption, financial loss, and serious accidents.

The ITU (International Telecommunication Union) guidelines for managing RF interference at airports highlight the importance of strictly adhering to allocated frequencies, using spectrum management tools, and actively monitoring for interference—especially in critical navigation and communication systems that rely on GNSS.

CRFS provides airport security the tools to comply with ITU and ICAO (International Civil Aviation Organization) recommendations and actively hunt interference.

PROACTIVE SPECTRUM MONITORING

Establishing a network of **RFeye Nodes**, highly sensitive wideband software-defined RF sensors (9 kHz to 40 GHz), around an airport enables comprehensive, real-time monitoring of RF activity across airport facilities. These sensors detect RF energy and measure signal characteristics, including frequency, amplitude, and duration, which are crucial for identifying interference and unauthorized transmissions.

Using **RFeye Site**, a spectrum monitoring software, RF sensors detect signals based on predefined parameters, distinguishing between regular communication signals and those potentially causing interference. Once an interfering signal is detected, the software can geolocate the emitter using techniques like Power on Arrival (PoA), Angle of Arrival (AoA) and 2D/3D Time Difference of Arrival (TDoA). This capability helps security teams pinpoint interference and address it swiftly.

ADHERENCE TO ALLOCATED FREQUENCIES

The frequency allocation table in RFeye Site provides airport security with a clear visual of all allocated frequencies. If the power level of these allocations exceeds the permitted levels, the mask is broken, and security will receive an instant alert.

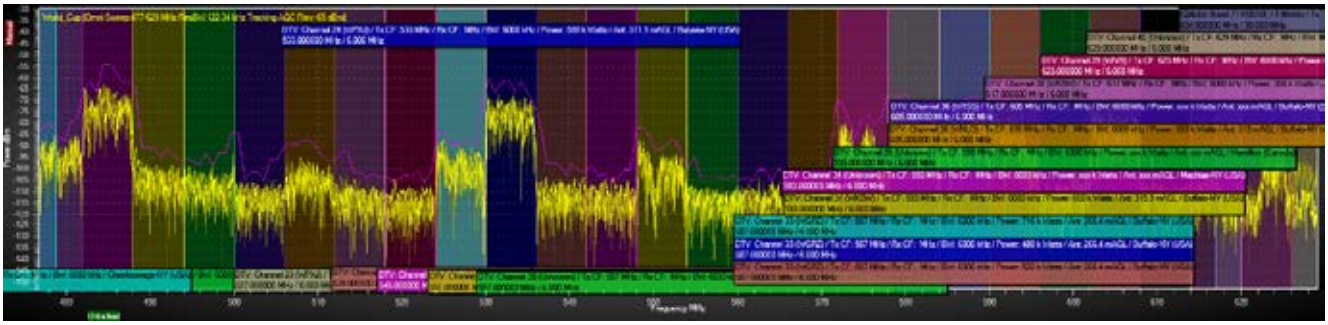

Image 1: Frequency allocation table showing all license holders in a given band.

COMMON TYPES OF INTERFERENCE AT AIRPORTS

The large number and close proximity of antennas at airports means interference is common. The bigger the airport, the more frequencies are used, and the higher the chance of interference.

The following are the most common types of interference at airports:

- Off-channel or adjacent channel interference occurs when receivers tuned to one frequency pick up transmissions from nearby frequencies.
- Simultaneous transmitter interference happens when multiple off-channel transmitters are operating at once, causing intermittent interference.
- Receiver desensitization happens when other transmitters nearby reduce a receiver's sensitivity. This can take place even if they are not transmitting on the same frequency.
- Spurious response frequencies are unintended signals inadvertently detected by receivers at frequencies other than the one it is tuned to. This unintended detection can cause interference if a transmitter is operating near the spurious frequency.

FACTORS INFLUENCING INTERFERENCE SEVERITY

Antenna proximity: If antennas are placed in close proximity, there is a higher likelihood of interference. The greater the distance between antennas, the lower the risk of interference.

Frequency proximity: Frequencies close in range to one another are more prone to interference. Listing all frequency allocations and forecasting potential causes of interference can be beneficial.

Transmitter power: High power in transmitters can increase the likelihood of interference.

Receiver and transmitter design: The specific design of receivers and transmitters also influences susceptibility to interference.

DETECTING ADS-B SPOOFING

Automatic Dependent Surveillance–Broadcast (ADS-B) is used to track aircraft. It relies on GNSS data to establish an aircraft's precise location, which is then broadcast automatically on 1090 MHz and 978 MHz to ATC and other aircraft. It is designed to enhance aircraft safety.

However, bad actors can intentionally transmit false ADS-B signals to provide incorrect data regarding an aircraft's location, speed, altitude, or identification. In August 2024, a United Airlines flight from New Delhi to New York reported a case of suspected ADS-B spoofing, which affected its navigation systems, causing the aircraft's GPS coordinates to increasingly deviate from its actual location.

As spoofing can negatively impact aviation safety, it is important to implement as many mitigation strategies as possible.

One strategy includes cross-checking ADS-B data transmitted by aircraft with data from other sensors, such as ground-based RF sensors to verify the accuracy of received signals. By building a sensor network and measuring the 3D Time Difference of Arrival (3D TDoA) of signals emitted from an aircraft at each RFeye Node, RFeye Site can triangulate the aircraft's location, which independently verifies ADS-B data.

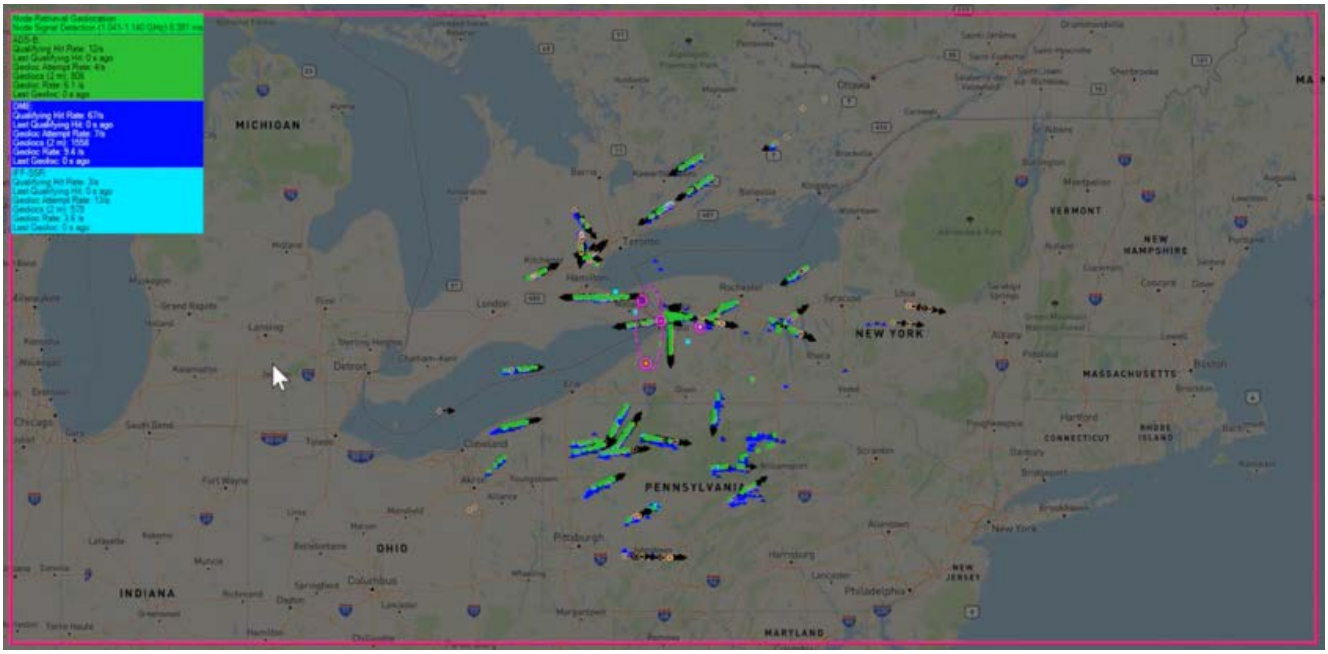

Image 2: Geolocations of ADS-B and DME signals from commercial aircraft.

PILOTS LEAVING ON WEATHER RADAR SYSTEMS

Located in the aircraft's radome, weather radars have a high-directional flat plate antenna, which transmits high-frequency radio pulses in the 9GHz to 10GHz range. These systems are essential to avoid turbulence during flight; however, if left on after landing, they may cause interference with other critical airport equipment operating within the same frequency range.

For example, ATC often use X-Band radars to precisely track aircraft positions, specifically in congested airspace, which improves the safety of airspace management. ATC also use X-band radars to monitor weather conditions.

Interference caused by pilots leaving on the weather radar can lead to challenges in managing ground operations and maintaining clear communication. Any interference may result in delays and affect the safety of aircraft taking off and landing.

While regulatory bodies, including the FAA and FCC, have created guidance to mitigate interference from any source, the only way to ensure problems are addressed quickly is to actively monitor the spectrum and identify and geolocate interference caused by active weather radar systems before they affect other systems.

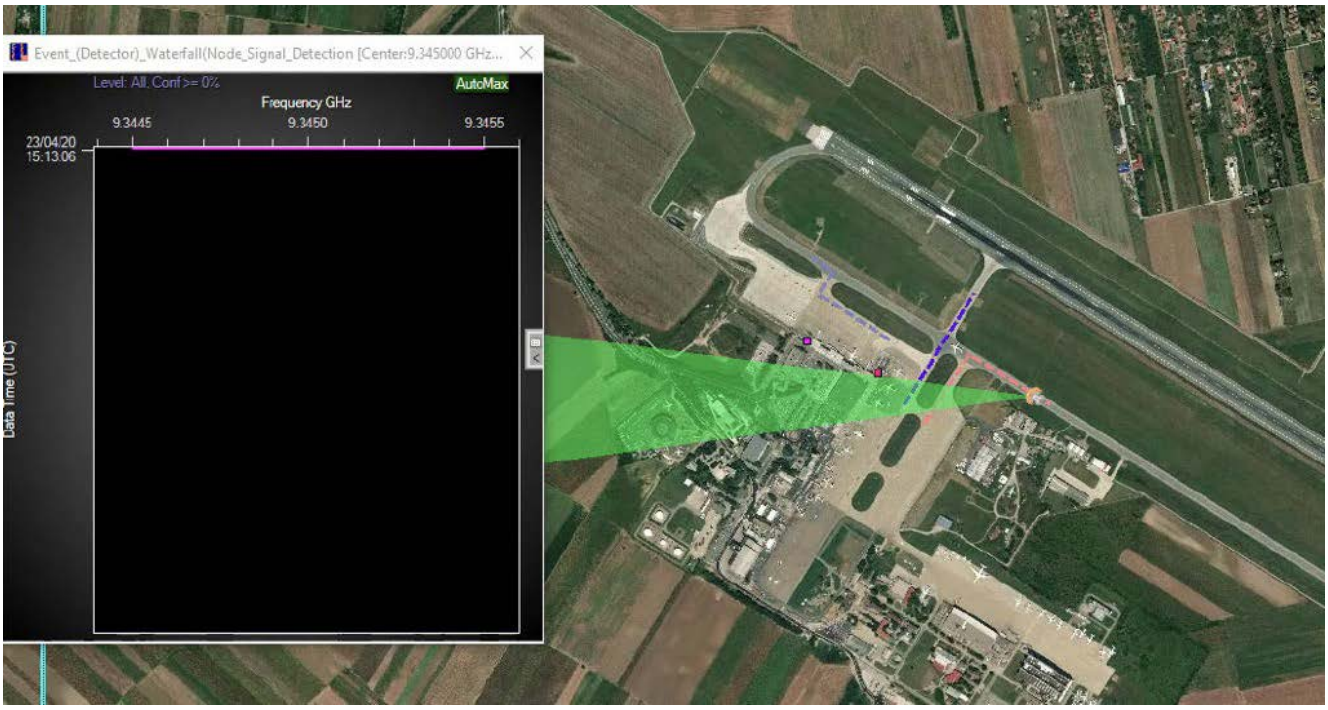

Image 3: Geolocating a weather radar, which continues to transmit after the aircraft has landed

VHF AND ILS COMPLIANCE

Very high frequency (VHF) communications, typically between 118.000 MHz to 137.000 MHz, are the backbone of air traffic control (ATC) operations. These radio links provide channels for controllers and pilots to communicate during multiple phases, including taxi, takeoff, approach, and landing.

Voice Communication Control Systems (VCCS) allow ATC to provide pilots with updates and instructions, and air-to-ground communications provide pilots with a way of problem solving. Both require clear, interference-free channels to prevent miscommunication that could compromise safety.

Ensuring VHF frequencies have been allocated and are managed according to national and international regulations can only be achieved through careful spectrum monitoring and management. This will ensure that the channels are correctly adhered to, preventing interference between airports and neighbouring areas.

Instrument Landing Systems (ILS) uses highly directional radio transmitters transmitting on VHF and UHF frequencies to ensure a precise aircraft approach path during a descent. The main component of an ILS, the localizer, operates between 108.1 and 111.95 MHz; however, each runway uses a unique frequency to prevent interference.

Compliance with ILS regulations is required to guarantee no signal overlaps impede an aircraft's precise alignment with the runway in low visibility conditions.

For compliance and to reduce interference, airports enforce measures that prevent physical objects such as vehicles or aircraft from blocking antennas. However, spectrum monitoring and management play a crucial role in ensuring interference-free operations for ILS.

- Detect unauthorized or unintended transmissions within the VHF band that may interfere with the localizer or the glide slope
- Locate interference sources in real-time, whether it stems from nearby equipment, other transmitters, or unauthorized usage
- Coordinate the allocation of nearby frequencies and enforce usage guidelines to minimize the likelihood of overlapping frequencies
- Create geofenced areas to monitor all signal activities

I/Q DATA CAPTURE

It is common for sources of interference to originate from outside airports; for example, there have been many reported cases of ATC interference caused by FM radio stations. These cases cannot be resolved by airport security; the national regulator is the only competent authority to conduct an investigation.

Recording I/Q data over a long period (one week, for example) using an RFeye SenS Remote can help expedite the regulator's initial investigation.

The recorded data can be analyzed to identify patterns of interference and determine the interfering signals' frequency and power levels. If the airport has a network of RF sensors, geolocation software can be used retrospectively to geolocate the interfering signals so corrective actions can be taken.

Mass data storage for I/Q recording with an RFeye SenS Remote

- Store I/Q data with a bandwidth of up to 100MHz
- Data storage of up to 1.8 TB per hour
- Includes 2 servers: Linux server for RRH control and Windows server for DeepView and storage
- The Windows server can be supplied with a 30TB, 60TB, or 90TB SSD or higher
- The SSDs are mounted in the Windows server so that no extra equipment is needed

GNSS JAMMING

For critical national infrastructure, including airports, Global Navigation Satellite System (GNSS) is essential for enabling precise navigation, positioning, and timing. It supports a wide range of applications critical to airport operational efficiency and safety. GNSS provides reliable guidance for aircraft approaches and landings, ground vehicle tracking, and time synchronization across systems.

What relies on GNSS?

- Area Navigation (RNAV) and Required Navigation Performance (RNP) enable aircraft to navigate accurately without needing ground-based navigational aids
- Ground-Based Augmentation Systems (GBAS) can be used as an alternative to the Instrument Landing System (ILS) and provide multiple approaches to runways
- Surface Movement Guidance and Control Systems (SMGCS) and Advanced-Surface Movement Guidance and Control Systems (A-SMGCS) use GNSS to monitor and manage aircraft and vehicle positions on runways and taxiways

Although GNSS is essential, the system's vulnerability lies in the extremely weak signal received by GNSS receivers on or near the Earth's surface. This makes it very easy to intentionally or unintentionally jam GNSS signals.

Jamming happens when GNSS signals are interrupted, preventing GNSS receivers inside anything from a Ground-Based Augmentation System to a cellphone from receiving the signal. It can happen intentionally when illegal jamming devices emit strong signals that overwhelm GNSS frequencies or unintentionally as a result of devices that use the GNSS frequency range.

Truck driver accidentally jams Newark Airport

A truck driver using a GPS jammer to evade his employer's tracking system inadvertently disrupted the satellite-based navigation aids at Newark International Airport. The signals emanating from the vehicle blocked the reception of GPS signals used by the air traffic control system.

DETECTING JAMMING THROUGH CONTINUOUS SPECTRUM MONITORING

There is no way to detect jamming until it occurs, and determining if it is intentional or unintentional is not always straightforward. Additionally, it is not always clear if a perceived case of jamming is the result of another factor, such as a signal blockage or receiver fault.

The most failsafe way of rapidly detecting jamming is to carry out continuous RF monitoring and receive data in real-time that provides insight into potential interference and the probability of jamming.

RFeye Nodes contain a jamming indicator provided by the u-blox chipset, which outputs a value from 0 to 256. CRFS automated spectrum management software, RFeye Mission Manager, has a feature that converts the number to a percentage, which is visually represented on a chart (as a percentage of jamming probability over time).

Once a percentage threshold of jamming has been surpassed, operators can geolocate the source of the jamming to stop it from broadcasting.

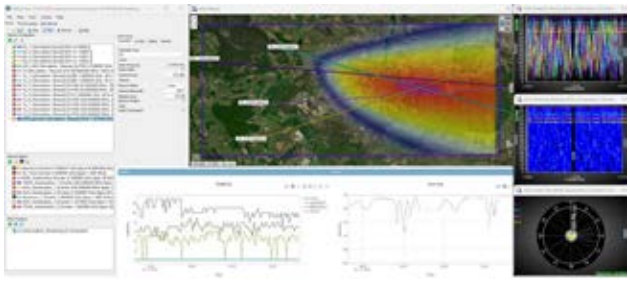

Image 4: The bottom left graph shows the percentage of jamming probability over time, and the map shows the geolocation of a jamming signal (where the lines intersect)

DRONE DETECTION

Globally in the first nine months of 2024, there were 17 ‘extremely serious’ reported incidents and thousands more less serious incidents involving unauthorized remote-controlled drones flying in restricted airspace. Although most drone operators have benign intentions, the threat to life and economic loss remains as significant as those posed by terrorist incidents.

Such serious safety risks require a multilayered defense approach involving radar, optical, and passive RF sensors, as each individual sensor has its own strengths and weaknesses.

DETECTING DRONES WITH RF SENSORS

Commercial off-the-shelf (COTS) drones are typically controlled remotely by an operator who uses a device to send command signals through a dedicated frequency. The operator also receives data from the drone (from video downlinks, for example) thanks to onboard data link transmitters (typically operating in the 2.4 GHz ISM band) for real-time data download.

The 4G and 5G frequency bands are also commonly used to control drones, as these networks increase the connectivity between the drone and the operator.

RF sensors have the unique benefit of being able to identify signals transmitted from the drone and the drone operator.

COTS drones can be detected using a network of at least four CRFS Nodes, which identify the time, frequency, and power characteristics of RF signals. Real-time spectrum monitoring software geolocates the signal 70 times a second using 3D TDoA (Time Difference on Arrival), which geolocates a signal based on its longitude, latitude, and altitude.

Although airport security may be actively monitoring the spectrum for unauthorized drones, RFeye Site allows spectrum managers to build custom detectors for any RF transmitters, including those on COTS drones, such as control transmitters, telemetry modules, GPS modules, and video transmitters.

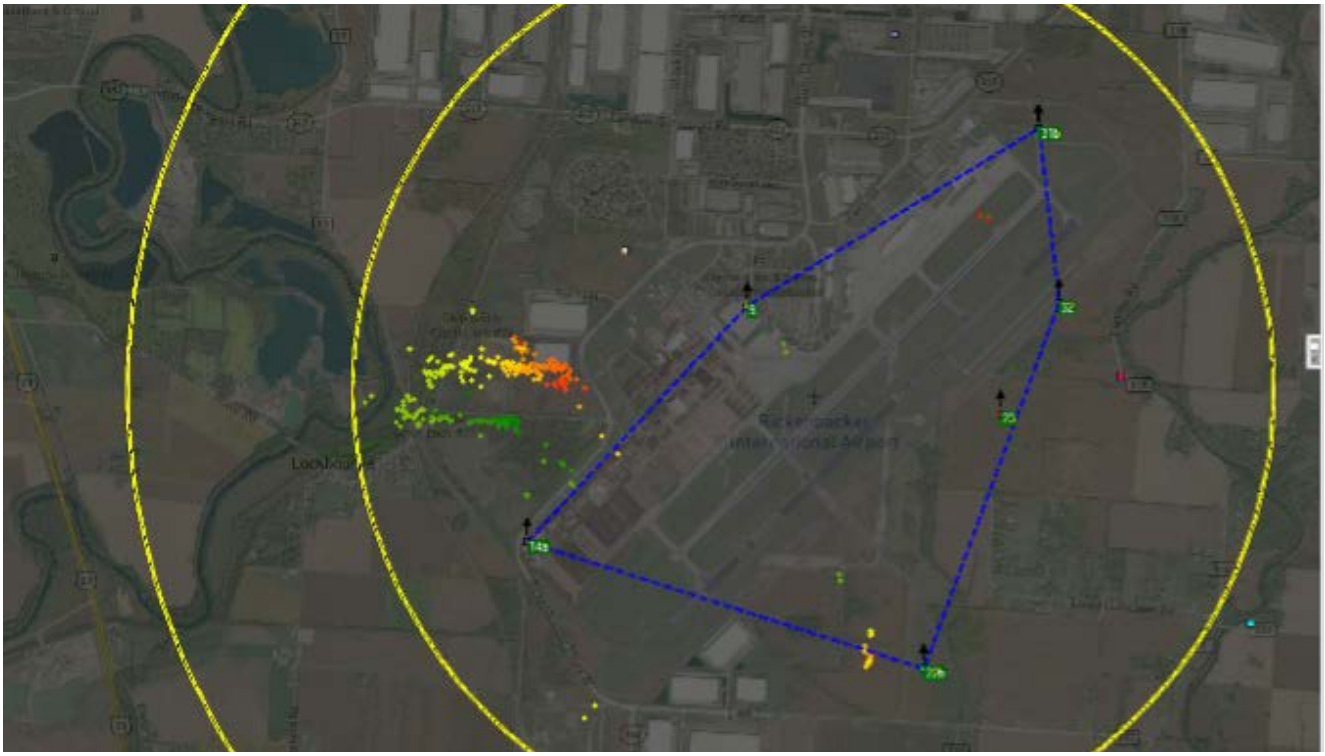

Image 2: RFeye Site geolocates a drone operating on 2.4 GHz outside a geofenced area at Rickenbacker International Airport. (Red indicates the most recent geolocation, and green the oldest.)

These signals can be detected up to approximately eight kilomotres outside the network, and the software sends an immediate alert to security personnel in real-time.

BENEFITS OF PASSIVE RF SENSORS

- Advanced detection: As RF sensors detect drones based on their RF emissions, they can identify even small or low-flying drones that radar may miss.
- Reduced false positives: Using RF sensors can reduce the number of false positive detections as radar may not always be able to differentiate between a drone and other low flying objects, such as birds.
- Early warning: Spectrum monitoring software can be used to geofence areas around airports. When a signal is transmitted from within this boundary, airport security will receive an immediate alert, and the signal will be automatically geolocated.
- No interference: Passive RF sensors do not emit any radio signals. Not generating additional interference is particularly important in sensitive airport settings, where reliable communications are crucial for safety.
- Real-time capabilities: RF sensors allow continuous monitoring of the spectrum and geolocation of signals of interest, which permits responses in real-time.
- Non-visual capabilities: RF sensors do not rely on visibility or daylight; they work effectively in poor weather, fog, rain, and low-light conditions, making them valuable for all-weather monitoring at airports.
- Easy integration with security systems: It is easy to physically install RF sensors into larger airport security systems, and **open APIs** allow CRFS software to be integrated into the airport's existing command and control system to provide enhanced situational awareness.

CONCLUSION

Proactive spectrum monitoring at airports with advanced RF technology can help protect critical communication and navigation systems from interference. With a network of RF sensors around the airport, spectrum managers can identify and geolocate interference before it has a negative impact on airport operations.

As airspace becomes more congested and RF-dependent technologies continue to expand, standards and compliance requirements for RF management at airports are likely to become more stringent.

In the future, large airports may be required to have enhanced spectrum monitoring systems and regular interference audits.

Integrating RF technology can not only help airports manage their complex RF environments today; it can allow them to face future challenges, ensuring clear communication and enhanced safety across all levels of airport operations.

RFeye® Receiver (Node)

High-performance spectrum sensor (receive / record) to 40GHz

RFeye® Site

Real-time spectrum monitoring & geolocation toolkit

RFeye® Mission Manager

Automated monitoring & mission management

RFeye® DeepView

Forensic signal analysis software with 100% probability of intercept

CRFS

EXTRAORDINARY
RF TECHNOLOGY

CRFS is an RF technology specialist for the defense industry, national security agencies, and systems integration partners. We provide advanced capabilities for real-time spectrum monitoring, situational awareness, and electronic warfare support to help our customers understand and exploit the electromagnetic environment.

CRFS Inc
Chantilly,
VA, USA
+1 571 321 5470

CRFS Ltd
Cambridge,
United Kingdom
+44 (0) 1223 859 500

bsi. ISO 9001:2015 Quality Management
UK Certificate number: FS576625