Drone alert!

The market for small commercial drones is booming. However, these inexpensive and easy-to-fly devices also pose security problems. The R&S®ARDRONIS drone monitoring system helps businesses, government authorities and critical infrastructures to protect personnel and goods.

Commercial drones: the next big thing

Incidents with commercially available drones appear almost daily in the media: drones in the vicinity of airports or even in the flight paths of aircraft (e.g. Heathrow, Munich, Warsaw, Taipei), drones above power plants and governmental buildings (the Japanese Prime Minister's office, the White House South Lawn), drones at political events (German Chancellor Dr. Angela Merkel's election rally in Dresden), drones above automotive test tracks or in the skies over Paris.

Currently, more than 300,000 drones are sold per month through online shops or brick-and-mortar stores around the world. In the USA alone, about one million devices were sold in the weeks leading up to Christmas 2015. It is estimated that by 2025 the commercial drone market will reach a volume of more than 8.5 billion euros. The explosion of relatively inexpensive and easily operated flying drones represents a new type of challenge for the protection of public and private spaces. The devices – which are both readily available and easy to fly – provide ample opportunity for misuse. Difficult to detect and capable of carrying payloads up to a few kilograms, drones increasingly represent a threat to critical infrastructures and public figures and at public events. Security agencies, government authorities as well as private organizations and facilities that require protection must have the technological approach to counter this threat.

The first challenge is to detect these small flying objects, and a number of methods are available to accomplish this. Once detected, the intruder must be classified in order to determine whether countermeasures are necessary. Instead of visual detection or radar monitoring, the Rohde&Schwarz solution identifies, finds the direction of and disrupts radio control links to and from the drone. The R&S®ARDRONIS automatic radio-controlled drone identification solution from Rohde&Schwarz has already proven itself in operations requiring the highest level of security, such as the June 2015 G7 summit held at Elmau Castle in Bavaria, Germany, and US President Barack Obama's trip to Germany for the Hanover Trade Fair in 2016 (Fig. 2).

A few facts about commercial drones

Unmanned aerial vehicles (UAV) – alternately known as small drones, minidrones or micro UAVs – are remotely controlled from the ground, although higher-end models often additionally provide navigation technology so that they can independently fly predefined routes. UAVs are typically grouped into the following categories: drones for private use (toy and hobby), drones for commercial applications (aerial views, logistics, etc.) and drones for military applications (artificial targets, reconnaissance, combat). R&S®ARDRONIS is intended exclusively for commercial use. The rapid increase in the intelligence of commercial drones, (e.g. automated target recognition by logistic drones), the cost savings achieved through the use of drones in general and the intense interest from the private sector have all combined to cause the number of commercial drones to skyrocket exponentially. There are two basic types of drones: multicopters and fixed-wing drones. Fixed-wing drones are used in only limited numbers. Their greater range and altitude make them primarily suited to special tasks such as cartography and ground mapping. Reports in the media about drones almost always refer to multicopters. Additional criteria for the classification of drones include size, payload, speed, endurance, range, altitude – and the type of control. The last criterion is of particular interest for R&S®ARDRONIS, which is designed to detect the control signals.

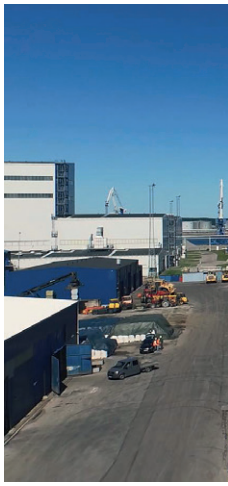
Proprietary FHSS/DHSS control systems	WLAN	Bluetooth®
▮ Most common (> 80 %) ▮ Range: < 1 km at up to 100 mW transmit power 3 km with power amplifier ▮ Some standards include telemetry data in the downlink (e.g. Jeti, Graupner)	▮ Range: up to 100 m (standard) up to 2 km with power amplifier ▮ Some models can be controlled via first person view (FPV) and/or GPS navigation	▮ Low-cost models ▮ Range up to 60 m

Fig. 1: Typical drone remote control systems.

Fig. 1 provides an overview of the various types of controls available on the market. More than 90 % of all drones communicate over the commercially available industrial, science and medical (ISM) bands, which are also used for telecommunications, e. g. for WLAN and Bluetooth® radio systems. The 2.4 GHz and 5.8 GHz bands see the most use, while use of the 433 MHz band is rare.

By far the most commonly used (> 80 %) radio technologies for remote drone control are proprietary implementations of frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). In order to increase immunity to interference, both methods use a broader spectrum than is actually required to transmit the wanted signal. FHSS alternates the carrier frequency in a pseudorandom hopping sequence. The transmitter and receiver must be synchronized and use the same hopping algorithm in order to maintain the connection. In contrast, DSSS occupies a fixed, very large bandwidth, although it decreases the spectral power density to such an extent that the wanted signal is barely above the noise floor and can only be retrieved by using a precisely matching demodulator. The two methods, which are sometimes also used in combination, are perfect for the heavily used ISM bands, where many users and radio technologies must coexist. FHSS/DSSS is therefore considered to be a quasi-standard for drone control and is used by most manufacturers. However, the game of hide and seek being played with FHSS/DSSS radio links within the spectrum make them difficult to detect and disrupt. R&S®ARDRONIS is up to the challenge with its powerful online hopper analysis. It analyzes the technical radio parameters such as hop lengths, symbol rate and modulation type and is able to unerringly classify the transmission system, e. g. HOTT (Graupner), FASST (Futaba), M-Link (Multiplex) or DSMX (Spektrum) (Fig. 4).

Fig. 2: Typical applications for drone monitoring and countermeasure systems: high-ranking events (for example, R&S®ARDRONIS guarded the G7 governmental heads in 2015 at Elmau Castle), test tracks for secret prototypes, critical infrastructures, sporting events, public rallies.



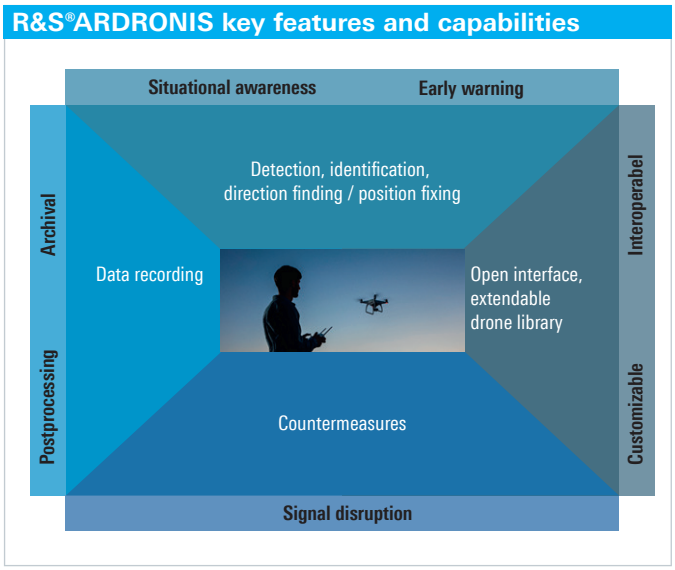


Fig. 3: R&S®ARDRONIS is a reliable, comprehensive system.

Advantages of a radiomonitoring solution

The interception of drone control signals provides certain advantages over alternative methods such as radar, optical or acoustical detection.

Reliable detection without false alarms

The system is not confused by other flying objects, such as birds, balloons or kites.

Earliest possible detection

R&S®ARDRONIS issues an alert as soon as a remote control unit begins transmitting, i.e. even before the drone takes off. This allows countermeasures to be deployed without delay.

Direction finding / position fixing of drone operators

Because R&S®ARDRONIS detects both the drone via its downlink signals and the remote control unit via its uplink signals, it can immediately determine the bearing of the drone

operator. By using multiple direction finders, it is even possible to fix the operator's precise position (in preparation).

Situational awareness

R&S®ARDRONIS not only detects all drones over a large monitored area, but in many cases can also indicate the type of drone by analyzing its radio signature, thus allowing an assessment of its threat potential. The downlink activities of the drones are additionally registered, for example whether video transmissions are taking place.

Signal disruption

The R&S®ARDRONIS system can be upgraded with a jammer that can effectively disrupt the radio link to a drone. This forces the drone into failsafe mode so that it will either land immediately or return to its point of origin. The jamming is so selective that it does not affect other radio activities. R&S®ARDRONIS creates radio parameter sets for all detected drones, making it possible to intercede at any time, e. g. to respond automatically when a protected area is breached. The setting speed of the R&S®WSE follower jammer is so fast that even rapid FHSS frequency hoppers do not pose any problem.

Reliable protection, easy operation

R&S®ARDRONIS uses antennas, direction finders and signal analysis solutions from Rohde&Schwarz. These tried and tested high-tech components, combined with a powerful detection algorithm, permit reliable interception of short-duration signals with a signal duration as low as 350 microseconds, even – and most especially – in the densely occupied ISM frequency bands. Under optimal conditions, the range is from one to three kilometers, depending on the drone and remote control transmit power and on the environment. To prevent unnecessary alarms, the alerts can be linked to an intrusion into a protected area (Fig. 5). The technical parameters for each transmission are compared against defined profiles and the matching drones are sorted into three categories: black list (e. g. potential threats), white list (e. g. own drones) and unnamed (e. g. unknown drones). A user-friendly operator interface lists the detected drones and their critical parameters (Fig. 4). If direction finding or position fixing functionality is implemented (R&S®ARDRONIS-D/P), DF beams or location markers are used to display the detection results on a map. An expert view with detailed information about detected signals is available for radio analysts (Fig. 6).

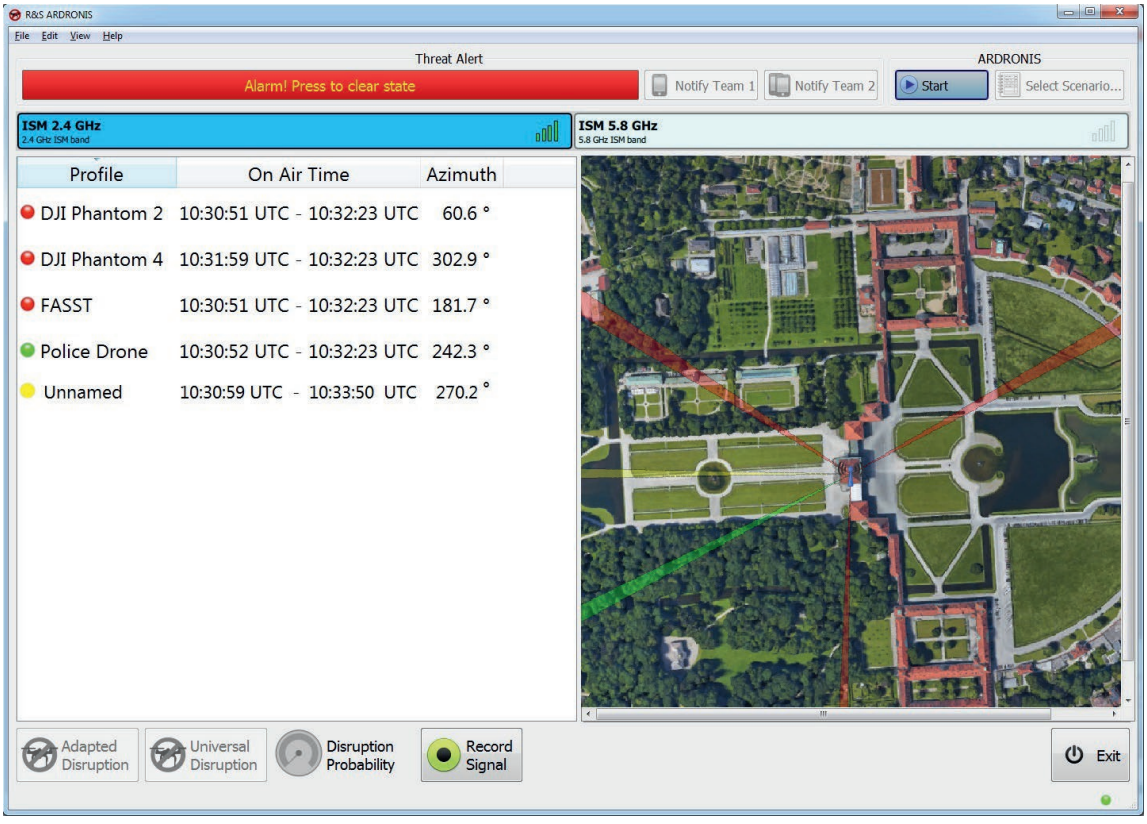


Fig. 4: Speed is of the essence in critical situations. The standard user interface therefore offers only the most important information and control buttons.

Protected area and detection range of R&S®ARDRONIS

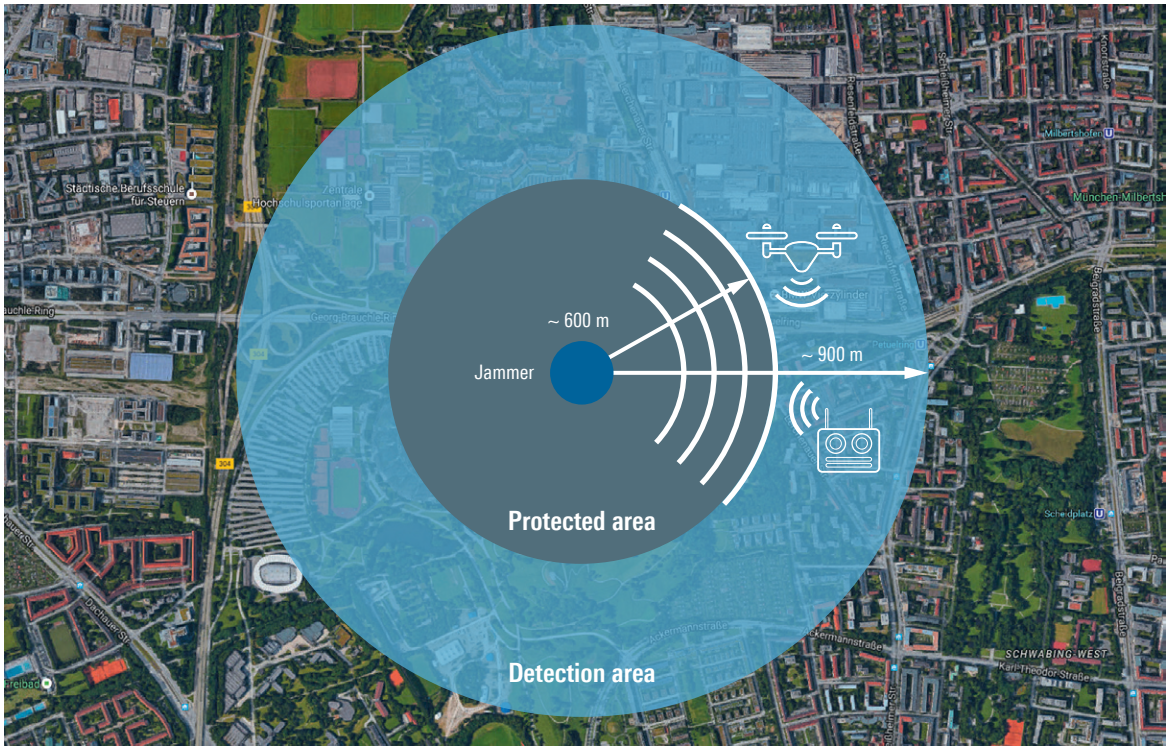


Fig. 5: R&S®ARDRONIS permits the definition of protected areas. If a drone flies into the defined area, the remote control radio link is automatically disrupted.

Fig. 6: The expert view is a treasure trove for radio experts. The uplink and downlink signals of the detected drones can be analyzed in full detail.

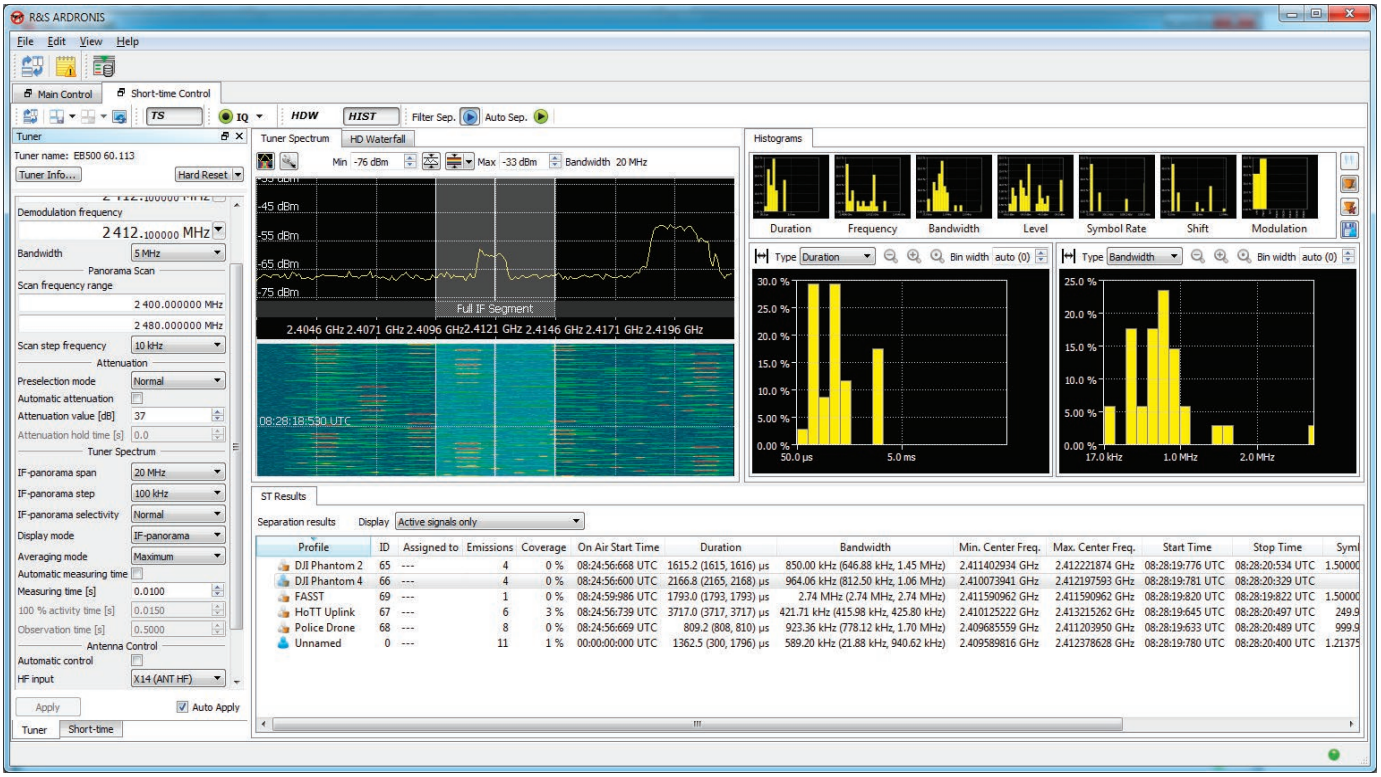
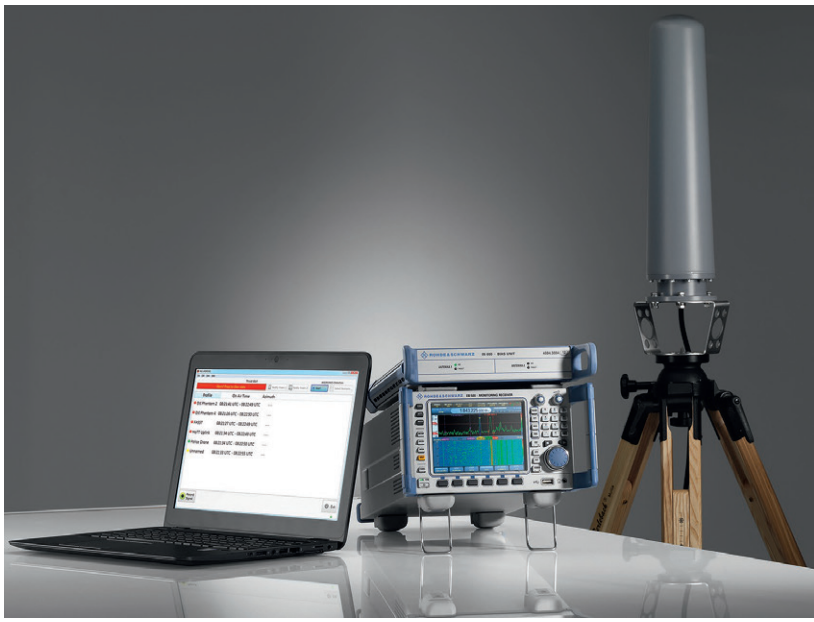


Fig. 7: R&S®ARDRONIS is made up of only a few components and can be easily transported to different sites. The photo at the bottom shows R&S®ARDRONIS-D; all others show R&S®ARDRONIS-I.



Package	Designation	Functionality		
		Identification	Direction finding / position fixing	Countermeasures
R&S®ARDRONIS Detection	R&S®ARDRONIS-I	•	–	–
R&S®ARDRONIS Direction	R&S®ARDRONIS-D	•	•	–
R&S®ARDRONIS Disruption	R&S®ARDRONIS-R	•	–	•
R&S®ARDRONIS Protection	R&S®ARDRONIS-P	•	•	•

Fig. 8: R&S®ARDRONIS – the right configuration for every application (contact us for availability).

As a reliable, comprehensive automated monitoring system, R&S®ARDRONIS also permits data recording. Everything that the system "sees" can be archived, both individual detection results and entire RF scenarios.

R&S®ARDRONIS is suited to stationary or mobile applications. Security agencies in particular must provide protection for events at a variety of venues. The turnkey system is therefore preconfigured as an easily transported plug&play solution (Fig. 7).

The right configuration for every application

Four different R&S®ARDRONIS packages with differing functionality are available for ordering (Fig. 8). R&S®ARDRONIS-I is the right solution for customers wanting to detect drone activity within a defined area, for example over a sports stadium or a commercial facility. R&S®ARDRONIS-R is suited for permanent monitoring and protection of an entire zone, such as a government district. Countermeasures are deployed automatically when an intrusion is detected within the protected area. If there is a valid need to track down or even apprehend the drone operator, the R&S®ARDRONIS-D or R&S®ARDRONIS-P packages should be used.

Inclusion in integrated drone monitoring and countermeasure systems

As described above, a drone identification system based on radio signal interception has several advantages and even unique selling points over other methods, most particularly the ability to provide very early alerts, to prevent false alarms and to identify the perpetrator. However, there are situations in which R&S®ARDRONIS will not show the way to the target in the truest sense of the word. If a drone remains "mute" and does not emit any radio signals, it will not be detectable. Nor will disruption of radiocommunications force the drone to turn back or land if it has been programmed with a fixed flight path. Customers requiring comprehensive protection, including these types of situations, can integrate R&S®ARDRONIS into a system that includes other position fixing and protection components, such as radar. R&S®ARDRONIS includes an open interface for this purpose. The product is continually updated with new functions. Regular maintenance includes a refresh of the profile database to add new drone models. One planned new capability is position fixing by means of a cross-bearing fix.

Summary

The rapid proliferation of commercial drones is equally problematic for both security agencies and private organizations. The possibilities for misuse of drones range from invasion of privacy to white-collar crimes such as corporate espionage all the way to the endangerment of public personalities and capital offenses such as terrorist attacks. With R&S®ARDRONIS, Rohde&Schwarz is introducing a system that provides early detection of threats. R&S®ARDRONIS intercepts radio links between a remote control unit and a drone and uses it to find both the drone and its pilot, something no other method can do. Detection occurs immediately after the remote control is turned on, before the drone is in the air, making early countermeasures possible. An open interface allows integration of R&S®ARDRONIS into complex drone defense systems that can include other position fixing methods such as radar as well as effective countermeasures.

YingSin Phuan