ROKE

Effective Counter-UAS

Neutralising drone risk for safer skies

William Oxford

Roke Futures

Abstract

In this paper we explore the risks posed by drones, with a focus on public spaces, the considerations when selecting systems to mitigate these risks and the pros and cons of counter-drone sensing technologies. We then introduce Roke's counter-drone system, RapidEO, and open-architecture fusion and autonomy engine, Roke Robotics and Autonomous Systems (RRAS).

Introduction

The rise of drone technology has brought about significant advancements and conveniences across various sectors such as agriculture, delivery services, and surveillance. However, alongside these benefits, there has been a corresponding increase in security concerns. Drones, also known as unmanned aerial vehicles (UAVs) or unmanned aircraft system (UAS), pose a broad range of threats to national security, public safety, and personal privacy.

The level of threat is increasing as drone technology becomes cheaper, more capable and ever more accessible. Understanding these threats and implementing effective counter-drone solutions is crucial for safeguarding against potential risks.

Here, Roke offers a world class product (RapidEO) to detect, track and identify small UAV swarms out to 2km.

Threats from drones

Drones have become tools for various malicious activities due to their accessibility and technological capabilities. The primary security threats posed by drones include:

- **Airspace violations:** Drones straying into restricted airspace near airports can cause significant safety concerns and operational delays. For venues, the simple presence of a drone can cause disruption and delay to events and may cause distress and panic amongst attendees
- **Property damage and personal injury:** Inexperienced operators or technical malfunctions can cause drones to crash, possibly resulting in property damage and injury to attendees
- **Unauthorised surveillance and "social auditing":** Drones can capture proprietary images and videos without consent, gathering sensitive information from government and industrial facilities, private properties, and commercial entities
- **Data theft:** Advanced drones can intercept wireless communications and gather private data, compromising personal and corporate privacy
- **Contraband delivery:** Criminal organisations use drones to transport illegal goods such as drugs, weapons, and other contraband across into prisons or across borders
- **Terrorism:** Drones themselves can be used as high-speed weapons and can be readily modified to drop chemicals or explosives, offering a low-cost, low-risk method for terrorists to execute attacks
- **In military conflicts:** Current conflicts, especially in the Ukraine, are demonstrating the operational effectiveness of drone technologies. Off-the-shelf drones can not only be used effectively for reconnaissance and targeting of static and mobile targets, but can also be cheaply modified to carry explosive payloads to cause destruction

The impact of these activities can range from reputational damage and loss of revenue through to political repercussions and, in the very worst cases, injury and loss of life, irrespective of the motivations and intentions of the drone operator.

Threats from drones

The National Protective Security Authority (NPSA) provides advice and guidance to operators[1] regarding the selection of counter-drone technologies. This journey begins with the development of the Operational Requirements (OR) which will inform the selection of the appropriate physical, operational and technical security solutions, which may include counter-drone systems. A well designed and deployed counter-drone system should provide benefits including:

- **Deterrence:** The presence of a counter-drone system, potentially able to locate the operator, may be sufficient to deter nuisance incursions
- **Indicators and warnings:** Early warning of a drone approaching the venue, providing alerts when designated perimeters are compromised
- **Inform response and/or effect[2]:** Provide sufficient detail of the threat to decide upon the appropriate operational and technical actions
- **Support investigations:** Securely record data to support the identification and prosecution of the offender and historical analysis of system performance

1 https://www.npsa.gov.uk/counter-uncrewed-aerial-systems-c-uas
2 Effect refers to employment of a system to degrade, deny or destroy the threat.

Selection of Counter-Drone Systems

Counter-drone systems can be categorised into systems designed to detect, track and identify (DTI) the Unmanned Air System (UAS), and systems that prevent or disrupt the ability of the UAS to operate. In this paper, we focus on the systems designed to DTI the UAS and potentially locate its associated Ground Control Station (GCS).

A Counter-UAS (C-UAS) DTI system will be comprised of one or more sensing nodes, each with one or more sensor type. Nodes will often report to, and be operated from, a security control room (SCR), which need not be co-located within the protected site. Key considerations driven by the OR include:

Vulnerability analysis

- An analysis of vulnerabilities will assess likely launch sites and flight paths and the types of threat. This will inform the range performance, and concurrent sectors required to be covered by the C-UAS DTI system
- ***Protected area:*** A sensing system may be designed to cover 360° or may focus on one or more sectors. For all systems, performance will be limited by range
- ***Threat types and numbers:*** Drones can be used maliciously in a number of ways: they can be used for surveillance, they can be used to transport illicit and illegal items (such as drugs and cell phones into prisons), they can be used to disrupt events and proceedings and, of course, they can be weaponised for use in warfare and terrorism. Swarm attacks are designed to overwhelm defences. C-UAS systems will be limited by the number of concurrent threats that can be detected and tracked from single or multiple directions
- ***Local environment:*** The environment in which the C-UAS DTI system is to operate will influence on the selection of C-UAS DTI solutions, e.g. terrain, obstacles, weather, radio interference, night-time

Response plan

- The possible technical and operational responses to a threat and the characteristics of the C-UAS DTI system are interdependent
- ***Detection and false alarm rates:*** The OR should consider the impact of "missing" a real threat and the consequences of declaring a false threat. A reality of any sensing system is that the probability of detecting real threats is constantly being balanced against the probability of declaring a false threat
- ***Threat localisation:*** The OR should consider the fidelity of information required to inform the response plan. Sensors can be differentiated by the type of location information provided: an indication of the presence of a threat; a 1-d bearing (azimuth) only; a 2-d bearing (azimuth and elevation) only; a 3-d location (azimuth, elevation and range)

Operational costs

- The C-UAS DTI system should offer low through-life operational costs, including procurement, training, manning and maintenance. The C-UAS DTI system should have a simple, intuitive interface, be usable by a single operator and require minimal operator interaction under normal non-alarm conditions. It should also be able to be easily updated to address new threats

C-UAS DTI Sensing Technologies

Many C-UAS DTI systems are commercially available for both military and civilian applications. These span a wide range of performance and price. Here, we will summarise the main capabilities and constraints of the dominant sensing technologies; Radar, Radio Frequency (RF), Acoustic and Electro-optical (EO) sensors.

Acoustic sensors

Radar sensors

Electro-optical sensors

Radio frequency sensors

Acoustic sensors

Acoustics sensors detect drones by capturing the sounds produced by their engines/motors and rotors. Acoustic detection systems recognise the distinct frequency signatures which vary based on the type of drone, number of rotors, and rotor speed.

Detection range performance and false alarm rates are impaired by background noise such as traffic, wind, rain, and industrial sounds. Multiple microphone sensors can be networked to provide an indication of the direction of a drone but will have limited range performance.

Counter-drone sensors are typically comprised of arrays of microphones, which, as well as improving range performance, allow one or more drones to be detected and tracked in 2-d. Nevertheless, these sensors typically have a detection range lower than that of, for example, radar sensors. However, microphone arrays have a significantly wider "field-of-view" than most other sensors considered here.

Acoustic sensors are best deployed around the perimeter of a protected area or to complement other sensors, for example, to fill in areas with no line of sight for radar or camera sensors. To address the potential of false alarms, an electro-optic sensor (see below) can be cued to provide an image of sufficient quality to provide confirmation.

Radar sensors

Radars operate by emitting electromagnetic waves, typically in the radio frequency spectrum, and detecting the signals reflected from objects in the field of view. Processing of the received signals enables detection of moving targets, such as drones, against the stationary background targets. Radars can operate day and night, and in all weather conditions.

A radar system is comprised of transmitters and receivers. In most C-UAS DTI systems, these are co-located; multiple transmit and receive antennas are integrated into an array, referred to as a phased array. A phased array radar can provide the azimuth, elevation and range (i.e. 3-d position) as well as radial velocity (i.e. towards or away from the radar) of multiple targets with high update rates. However, a rotating array or multiple radars would typically be needed to cover a full 360° in azimuth.

Radars can have ranges of many kilometres depending upon the radar power and reflectivity (radar cross section) of the drone, although heavy rain may impact range performance. Radars also need a clear line of sight to the target. In practice, there may be zones that are obscured by terrain or buildings.

Similar to acoustic sensing, the high-frequency motion of the drone rotors imparts a modulation onto the reflected radar energy. The track (bulk motion) of the target, as well as these small modulations, can be analysed by the sensor to filter out potential false alarms such as birds and vehicles (e.g. micro-Doppler processing).

Deployment and commissioning of a radar systems should consider avoiding or mitigating any interfering sources operating in overlapping frequency bands; in urban settings, multiple reflections from nearby buildings (i.e. multi-path) may generate ghost targets and limit tracking accuracy, and areas of high ground clutter (e.g. main roads) may be a source of false alarms as well as masking targets of interest.

Transmitting at radio frequencies in the UK requires prior permission from Ofcom. These can be approved in advance on a long-term basis.

The long-range, wide-area detection and tracking capability of radars, day and night in all weather conditions, make them an ideal sensor to provide early warning, allowing sufficient time for response measures. However, radars will be susceptible to generating false alarms and have relatively limited resolution; many systems therefore will cross-cue an electro-optic sensor to provide an image of sufficient quality to provide visual threat confirmation.

Electro-optic sensors

Electro-optic sensors (cameras) can be divided into two broad categories; visual sensors operating in wavelengths similar to those of the human eye, which detect ambient light reflected off of objects; thermal sensors which detect light emitted by objects (hotter objects emit more light than colder objects) in wavelengths not visible by the human eye.

Visible sensors operate in day-time conditions only (although may perform adequately in low-light) whereas thermal sensors can operate both day and night.

Detection range performance in both cases will be impacted by fog, haze, snow and rain.

Both sensors can acquire images at high rates (e.g. 30 Hz+). Drones can be detected by virtue of a combination of their size, shape, contrast and motion. Detection is strongly influenced by the number of pixels presented by the drone in the image. In this sense, visible sensors, which are available in formats over 65Mpix, are superior to thermal sensors, which are typically available in formats of around 1Mpix.

Due to their relatively small field of view, EO sensors are more commonly used to confirm detections from other sensors, for example radar. Here, an EO sensor is mounted on a gimble able to rapidly slew in the direction of the initial detection (so called "slew-to-cue", see example below). We note that Roke's RapidEO system slews incredibly quickly; this allows image capture of all detected airborne targets in sequence, effectively simultaneously imaging all potential threats. Note that multiple EO sensors could be cued by a single radar.

Once cued, acquiring one or more small, rapidly moving drones in the image, and further differentiating a drone from a bird or other confusers, is extremely challenging. Manual acquisition needs a skilled operator to be available at a moment's notice and limits the number of concurrent targets that can be tracked. Unsurprisingly, this an area where automated artificial intelligence algorithms are increasingly being applied. Roke's Rapid EO system takes such an approach; artificial intelligence processing is applied to very large format imagery to simultaneously locate and classify drones in near real time. This approach robustly acquires targets with no user interaction required.

Once acquired, the operator or automated software can assign a unique identifier and threat priority, and optionally engage auto-tracking of the highest priority threat .

The bearing accuracy of the initial detection and speed at which the confirmatory EO sensor can slew, will determine the minimum field of view to ensure that the detection is captured in the image. The camera format (e.g. 4K) and minimum number of pixels across the drone for confirmation (along with image quality considerations) will dictate the maximum practical range of the EO sensor; for small drones this may be less than 1km.

If it is not feasible to deploy a radar (e.g. transmission restrictions), an EO sensor may also be used to conduct the initial detection. In order to obtain a useful field of view at a sufficiently high resolution, either multiple cameras can be arranged in an array or a single camera can be rapidly rotated on a scanning platform. Systems of this type may use thermal cameras to detect the hot spots generated by the drone motors and batteries, or may use very high-speed cameras (this necessitates sacrificing spatial resolution) to detect the small variations in pixel intensity caused by the motion of the drone's rotors.

EO sensors provide the opportunity to confirm a detection, the make/model of drone (including never-before seen drones) and, uniquely, presence of payload which significantly contributes to the assessment of the threat. Although limited in range (compared with radars), their relatively low cost (again, compared to radars) means that multiple sensors could be strategically located to maximise coverage.

Radio frequency sensors

Radio frequency (RF) sensors can detect and track of drones and their associated ground control station (GCS) by leveraging the radio signals used for communication. These communication links are used for command and control, data transmission and telemetry.

In common with radar sensors, RF sensors can operate in all weathers, day and night but can be hindered by terrain and other physical obstacles (since the communication links sought operate along a line-of-sight). Unlike radar sensors, RF sensors operate passively, and do not emit any signals themselves.

RF sensors (e.g. Roke's PERCEIVE Multi-Role®[3]) intercept the emissions to/from the drone from all directions simultaneously. Systems with multiple antenna arrays are able to provide a 1-d or 2-d bearing (of both drone and GCS), and potentially some indication of range from the received signal strength. In some cases, the presence of an emission in a known or unusual frequency band or an emission from a certain direction may be sufficient to declare a detection.

Most commercial UAS use WiFi protocols with frequencies in the 2.4 GHz and 5.8 GHz bands as these can be operated licence free; more advanced UAS may use frequencies assigned for cellular communications. Analysis of signals using pre-trained algorithms, or the extraction WiFi data packets can enable the make and model of the drone to be determined.

A congested RF environment may introduce interference. However, advanced systems can separate multiple co-channel signals to provide direction finding unhindered.

RF sensors are vulnerable to autonomous UAS operation or so-called "dark UAS". These are drones pre-programmed to fly to way-points, or those that make use of autonomous navigation technology, with little or no communication with the GCS post-launch.

RF sensors offer advantages of passive, omnidirectional, long-range detection and bearing of drones and are the only sensor considered here able to also detect and provide the bearing of the GCS, which may provide early warning of the UAS prior to launch.

3 Roke's Perceive (https://www.roke.co.uk/products/perceive-multi-role-mr) can separate multiple co-channel signals and give bearings on to multiple targets.

Emerging Technologies

Passive Radar: As the name suggest, a Passive Radar does not transmit. Instead, it relies on signals of opportunity (SOOP), typically terrestrial digital television transmissions, to illuminate the target with electromagnetic energy. Passive Radar may be attractive to use in scenarios where RF transmissions may be prohibited or subject to too much interference, or where the size, weight, power or cost (SWAP-C) of a dedicated transmitted is undesirable.

However, detection range and resolution are typically inferior when compared to active radar systems. Roke has expertise in this approach and has demonstrated the detection and tracking of a small drone using this technique.

3-d LiDAR (Light Detection and Ranging): A LiDAR is conceptually similar to a radar, in that it measures the range to an object, but emits radiation in the non-visible light spectrum rather than the RF spectrum.

A 3-d LiDAR uses multiple simultaneous (and typically rotating) beams to build a 3-d representation (a "point cloud") of the environment. Such systems remain experimental in the C-UAS domain, with very limited range. However, as the capabilities of these systems improves, driven by the automotive industry, 3-d LiDAR may become a viable option for drone detection and tracking.

Fusion for "Layered Sensing"

It is generally accepted that most C-UAS DTI problems require a layered sensing solution. Each sensor node (which itself may be comprised of one or more sensors) will apply local "at-the-edge" processing to reduce false alarms. The details of this process will vary between sensors and vendors but the node will invariably report a timestamped detection or track. In a system comprised of multiple sensor nodes, threats may be reported by more than one node, in 1-d, 2-d or 3-d, at varying reporting rates.

When multiple detections or tracks are reported, the operator will need to quickly determine if some, or all, of the reports are associated with the same threat or multiple threats. This will inherently involve a qualitative assessment of the "credibility" of each separate report, including perceptions of accuracy, latency and false alarm rate. This is both time consuming and will almost certainly lead to non-optimal outcomes. Despite this, some multi-sensors solutions on the market only apply simple layering to sensor data.

A solution to this is the deployment of a data fusion capability able to merge all reports into an uncluttered, actionable output. A well implemented fusion capability should account for node specific characteristics in a mathematically robust (probabilistic) manner. The outcome is reduced operator burden, increased probability of detection, reduced false alarms, improved localisation and reduced response times.

Fusing reports from different types of nodes is made possible via the use of a common reporting standard. One example is the SAPIENT/BSI Flex 335 specification[4], generated by the UK Ministry of Defence; a key principle of SAPIENT is to reduce operator workload during monitoring activities. SAPIENT has been widely adopted by industry and incorporated into C-UAS products.

A fusion capability should be seamlessly integrated into a command-and-control system, enabling fused outputs to be made available in near-real time for display, e.g. overlaid onto mapping, and potentially distributed over secure communication links.

4 https://knowledge.bsigroup.com/products/bsi-flex-335-v2-0-2023-sapient-network-of-autonomous-sensors-and-effectors-interface-control-document-specification-specification?version=standard

Adoption of C-UAS DTI Systems

There are many circumstances in which the NPSA process cannot be followed in full and/or in depth for reasons of lack of time and/or cost effectiveness. One important category is the protection of one-off or non-permanent locations e.g. festivals, rallies, protests, VIP visits, first responders to incidents. In these cases, as well as low operational costs, rapid deployment is an important consideration.

Roke's RapidEO C-UAS DTI solution is particularly well suited to these circumstances.

Roke's **RapidEO** C-UAS DTI system is a stand-alone sensing node which combines the benefits of all-weather radar sensors and a visual confirmation sensor. The highly agile EO sensor interrogates each radar track and provides high-quality real-time imagery, with threats immediately acquired and classified using state-of-the-art AI models. Unlike other "slew to cue" systems, RapidEO, over 50 times faster than standard pan-tilt units, can track up to 10 threats simultaneously making it ideal for pairing with lower cost radars that tend to generate more noise.

RapidEO is designed for low burden operations. The system is compact, lightweight and simple to deploy, for example on a mast or vehicle. The system tracks and identifies threats autonomously, reporting via a clean, intuitive interface which can be deployed on any networked device (e.g. a wireless tablet).

The speed with which the system operates provides confidence that swarms and multi-axis threats can be effectively detected; rapid detection means more time to respond. Real-time imagery of each potential threat may be critical to taking appropriate action e.g. to determine if the UAV is carrying a payload. We believe that RapidEO is the world's best multi-UAS imaging capability.

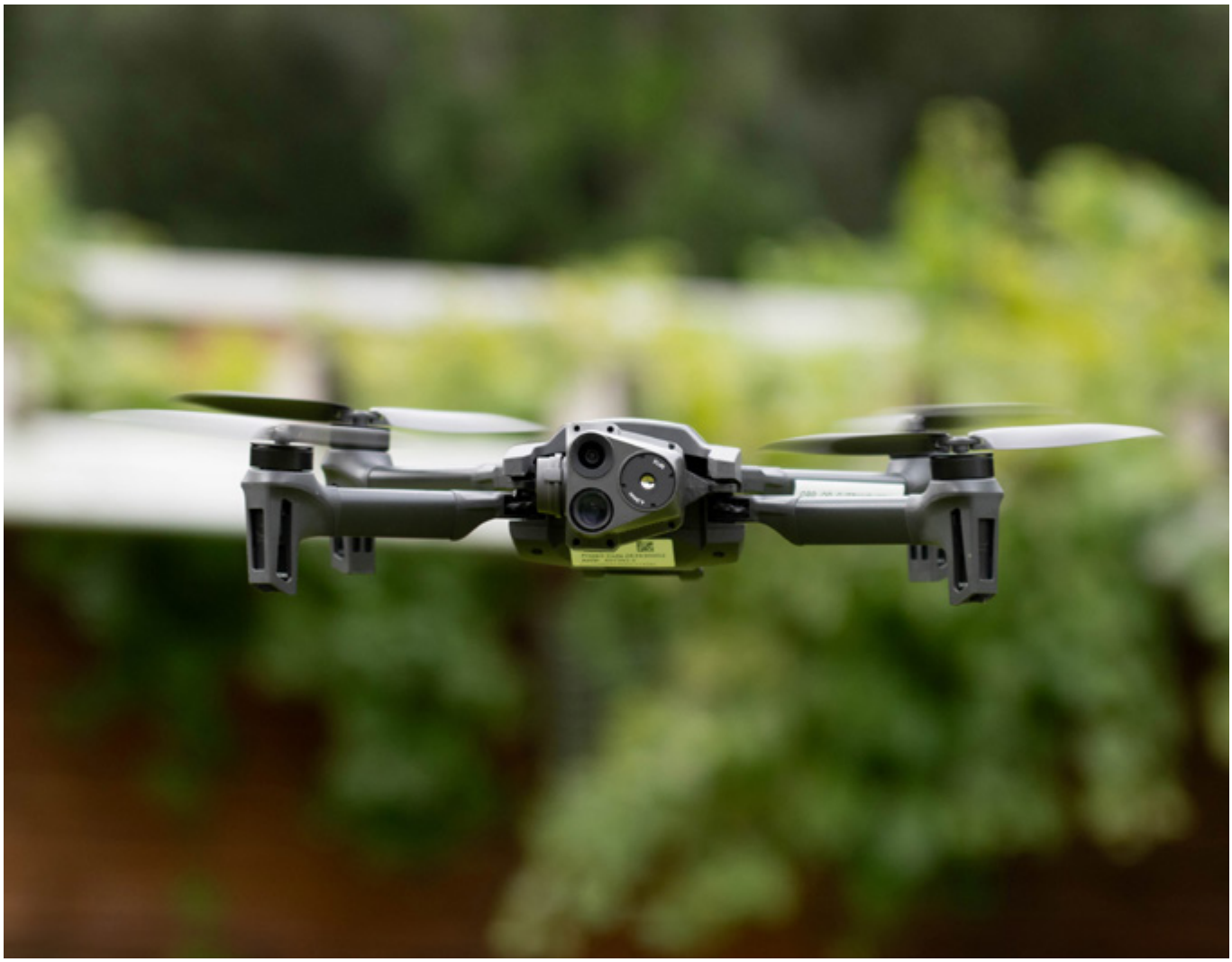
RapidEO is SAPIENT/BSI Flex 335 compliant, meaning it is scalable and interoperable out-of-the-box.

Roke Robotics and Autonomous Systems (RRAS) delivers a clearer and easier to manage situational awareness picture to operators by fusing reports from multiple nodes protecting one or more venues. RRAS is SAPIENT/BSI Flex 335 compliant which allows users to integrate their choice of sensor mix to best address a specific challenge.

RRAS integrates sensor information using deep probabilistic algorithms and supports all C-UAS sensor types. A critical discriminator is that RRAS not only fuses reports from sensors, it can also manage sensors, dynamically adapting to feedback, to maximise user-defined criteria in real time.

Examples of sensor management include changing sensing parameters, pointing a sensor in a particular direction or even moving mobile sensors (or recommending movement to a human operator). In a C-UAS context examples include cueing EO sensors to look at detections and thereby handling multiple targets, without requiring human interaction.

RRAS is easy setup and configure, provides a geo-spatial interface and, if required manual controls over sensor configuration. We believe that RAAS at the heart of a multi-sensor system provides levels of performance unmatched by human operators.



Can we help you?

The UAS threat is growing rapidly. It poses risks to people, assets, and infrastructure. This threat challenges both civilian and military organisations. Countering this threat effectively requires a scalable and flexible solution set that can be deployed quickly and adapted to different applications. This often utilises layered sensing technology.

Our systems are built to meet this developing threat head-on, delivering flexibility, resilience and the ability to futureproof your operation while deploying solutions at speed and scale.

Contact us now on **info@roke.co.uk** to find out more and set up a demo with our team.

ROKE

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk