L3HARRIS®
FAST. FORWARD.

COUNTERING THE UAV THREAT TO MILITARY AIRBASES

Ensuring freedom of action

COUNTERING THE UAV THREAT TO MILITARY AIRBASES

Ensuring freedom of action

INTRODUCTION AND OVERVIEW 4

UAV THREAT CHARACTERISTICS 5 - 7

C-SUAS CONCEPT OF OPERATIONS 8 - 10

SITE-SPECIFIC CONSIDERATIONS 11 - 13

MULTI-SENSOR DETECTION 14 - 15

OPEN STANDARDS AND EXTENSIBILITY 16

INTEGRATION WITH OTHER SECURITY SYSTEMS 17

DATA FUSION AND CORRELATION 18

SYSTEM OPERATORS AND TRAINING 19 - 20

C-SUAS REACTION AND EFFECTOR SYSTEMS 21

PARALLEL DEVELOPMENT 22 - 23

DRONE GUARDIAN 24 - 25

Note that the term UAV is used for brevity throughout this paper. However, sUAS is the more correct (although not widely-recognised) term for the relevant threat type to avoid confusion with larger, military specification UAVs.

INTRODUCTION

As the availability of sophisticated Unmanned Air Vehicles (UAVs) continues to grow, airbases are increasingly vulnerable to threats from unauthorised UAV flights. The nature of the associated threats these UAVs pose, their potential consequences and many resulting mitigation strategies are well-known to airbase stakeholders. This paper aims to identify and outline the specific considerations required for the planning, procurement and deployment of airbase Counter-Small Unmanned Aircraft System (C-sUAS) solutions to address these potential threats.

Ensuring freedom of action at airbases by mitigating UAV impacts on operational capability and risks to air safety requires intuitive C-sUAS solutions able to detect, track and identify potential threats. This combination helps to enable a suitably rapid and appropriate response to safeguard air traffic and secure the airbase.

KEY FACTORS FOR C-SUAS SOLUTION DEPLOYMENT AT AIRBASES

To help ensure the successful deployment of a C-sUAS solution at airbases, the following needs to be considered:

1. UAV Threat Characteristics
2. C-sUAS Concept of Operations (CONOPS)
3. Site-specific Considerations
4. Multi-sensor Detection
5. Open Standards and Extensibility
6. Integration with Other Security Systems
7. Data Fusion and Correlation
8. System Operators and Training
9. C-sUAS Reaction and Effector Systems
10. Parallel Development

1. UAV THREAT CHARACTERISTICS

As part of each site's security estimate, the UAV threat must be considered alongside all other force protection factors, with the vulnerability of high-value assets and the protection of personnel particularly critical. Denial of freedom of action such as runway closures and disruption of operations have both military and political impacts. These impacts need to be considered in order to align threat assessment and mitigation actions to resource allocation.

The following UAV-related incidents near airfields have been increasingly reported in recent years:

> Suspected or confirmed UAV sightings reported leading to runway closures (e.g. Gatwick Airport, UK in 2018)

> Targeted disruptive action involving UAVs leading to runway closures (e.g. Frankfurt Airport, Germany in 2020)

> Suspected or confirmed near misses between UAVs and aircraft (e.g. Manchester Airport, UK in 2020)

> Suspected or confirmed UAV to aircraft collisions (e.g. Buttonville Municipal Airport, Canada in 2021)

> Diversions of F-35 aircraft and military airfield suspension due to suspected UAV sightings (e.g. Williamtown RAAF Base, Australia in 2019)

Most publicly-reported incidents have involved commercial airports, however there are also a large number of incidents involving airbases not currently publicised. Safety is a primary concern at all airbases and as such all unauthorised UAV activity needs to be treated extremely seriously, regardless of the intention of the operator.

This follows a defined hierarchy of potential UAV threat actors:

Clueless and careless:
No intent to cause harm

Protestor or criminal:
Intent to cause disruption or commit other crimes but not serious damage or injury

Terrorist:
Intent to cause injury or serious damage using crude or improvised equipment and surveillance to plan future attacks

Military:
Intent to cause injury, serious damage and/or national security damage using military equipment as well as surveillance to plan future attacks

While there is some overlap between these categories of near surface events, the response from the airbase and relevant authorities will need to be proportionate in each case. This could range from a brief delay to flight operations in the case of a 'clueless and careless' incident to a retaliatory strike on an adversary in the case of a military attack.

It is therefore vital to ensure any deployed C-sUAS system can provide stakeholders with the ability to quickly assess the correct threat level and carry out an appropriate response.

In addition to the possibility of direct harm resulting from a UAV incursion, airbases are at risk of unauthorised UAV-based surveillance, compromising operational freedom and capturing details of assets or infrastructure. Even if performed by a 'clueless and careless' actor there is still the possibility of images, video or other intelligence falling into the wrong hands. This is of particular concern for airbases where high-value military assets such as F-35, strategic or ISTAR platforms are stationed, as adversaries could acquire key knowledge of the capabilities or movements of these assets. Pattern-of-life analysis may therefore be required to distinguish the important difference between 'clueless and careless' and nefarious surveillance activities.

Another key factor when considering intentional UAV actors is the asymmetric nature of the threat. UAVs are increasingly low cost (even military-grade models, when compared to other weapon types) and operating them generally presents low-risk to the operator. However, the impact, amount of damage and injury they can cause is potentially very large. Additionally, many high-value assets are not currently well-defended against UAV threats.

It is important to understand the full range of threats within these threat actor categories, along with the potential C-sUAS solutions available to defend against them. To build the most effective solution, an airbase's key stakeholder team should be guided by UAV security experts as well as data gathered from observations and sensor equipment. However, as the example of Chinese surveillance balloons shows, the absence of data about UAV usage in the vicinity of airbases doesn't necessarily mean lack of activity, it may demonstrate sub-optimal surveillance of near surface areas. This should enable mitigations to be identified that address specific risks and vulnerabilities while minimising disruption to base operations.

2. C-SUAS CONCEPT OF OPERATIONS (CONOPS)

The integration of C-sUAS capabilities into airbase defence is a complex challenge that needs detailed planning and exercising of multiple CONOPS options. At the most demanding level, C-sUAS operations will need to be conducted in a high-threat environment while flying operations and wider layered air defence activities are underway. It is important that a clear path and hierarchy of communication is created to disseminate relevant information to key stakeholders both on and off the airbase site so they can respond to a UAV event without delay.

It is critical to ensure that any C-sUAS CONOPS is integrated into emergency response plans and security/air traffic management procedures. It is possible to deploy systems rapidly (within hours) to provide a level of immediate coverage, however, systems deployed in this way invariably take time to be fully optimised and integrated and can rarely be deployed in the optimum location to meet a more generalised threat.

A C-sUAS system should form one part of a wider C-sUAS strategy developed to suit individual site requirements and risk levels. This includes understanding:

- How the C-sUAS strategy works alongside existing site security
- Regional laws regarding use of effectors
- Emergency response plans
- Air traffic management procedures

Planning should consider the following:

- What are you trying to protect?
- What is the likely threat and intent?

UAV characteristics:

- Size
- Shape
- Speed
- Manoeuvrability
- Likely ingress and egress routes
- Likely altitude

Physical constraints:

- Line-of-sight
- Environment – weather, wildlife, radio frequency environment
- Likely launch points surrounding the airbase

Non-Physical constraints:

- Legalities and permissions
- Risk – to people, property, reputation
- Cost

The wider C-sUAS strategy should include:

- Risk assessments
- Shielding or concealing sensitive assets
- Identifying potential launch sites and reducing their appeal
- Identifying potential ingress and egress routes and increasing difficulty of use
- Deterrents including local community engagement and communication e.g. signage

In response to a UAV threat it is important to have a planned, tested and rehearsed operational response that complies with the extant Rules of Engagement in force for air defence.

This may include:

- A dedicated drone incident management team(s)
- Security patrols on standby or roaming who are suitably trained, qualified and ready to respond to a drone incursion
- A standardised reporting process to enable rapid dissemination of information including appropriate levels of automation
- The ability to conduct dynamic risk assessments based on information provided
- Clear understanding of the approved escalation of response and the authority to implement this

The integration of C-sUAS CONOPS into the smooth operations of a airbase demands a deeper dive than can be covered by this paper. L3Harris' extensive knowledge of how best to integrate such operational activity means our technical experts are perfectly positioned to provide practical advice and support as part of any C-sUAS solution.

3. SITE-SPECIFIC CONSIDERATIONS

While many features are shared by most or all airbases (in terms of assets, layout and vulnerabilities), there are also important differences that mean that any C-sUAS solution needs to be carefully tailored in order to provide the appropriate level of protection.

Some examples of site-specific considerations and their influence on C-sUAS system design are as follows:

- Any airbase with existing radars in place will require selection of a C-sUAS radar model that can co-exist with existing radars without causing interference
- Some airbases will have restrictions on modifying infrastructure in certain areas, seeing C-sUAS sensors are sited elsewhere
- Some airbases require a higher level of protection in certain areas to protect critical assets necessitating additional sensors and/or effectors
- The characteristics of nearby terrain and location of airbase buildings will dictate the optimal placement of sensors due to line-of-sight factors
- The size and location of any Flight Restriction Zones (FRZ) around the airbase and approach paths will affect the optimal system coverage patterns
- The situation of local population centres and other factors influencing the likelihood of UAV launches will affect sensor placement and general system configuration

Differences in available budget and high-level customer requirements will have obvious influences on the choice of types, models and numbers of sensors. A C-sUAS system that readily supports open standards and can accommodate multiple sensor types through its architecture has clear advantages with regards to tailoring solutions, system longevity, modular replacement and cost competition for site-specific factors.

Sensors for UAV detection need to be placed in the most suitable location(s) possible to effectively detect and track UAV activity. It is very likely coverage will be required beyond the airbase perimeter, perhaps as far as the edge of the Military Aerodrome Traffic Zone (MATZ). Sensors deployed around an airbase would likely have to cover (at minimum) a volume of air space equivalent to the Flight Restriction Zone (FRZ) currently in place around each airbase in the UK.

To achieve the required range and quality of coverage (i.e. high probability of detection and low false alarm rate), a network of sensors in multiple locations linked back to a central data integration node is required.

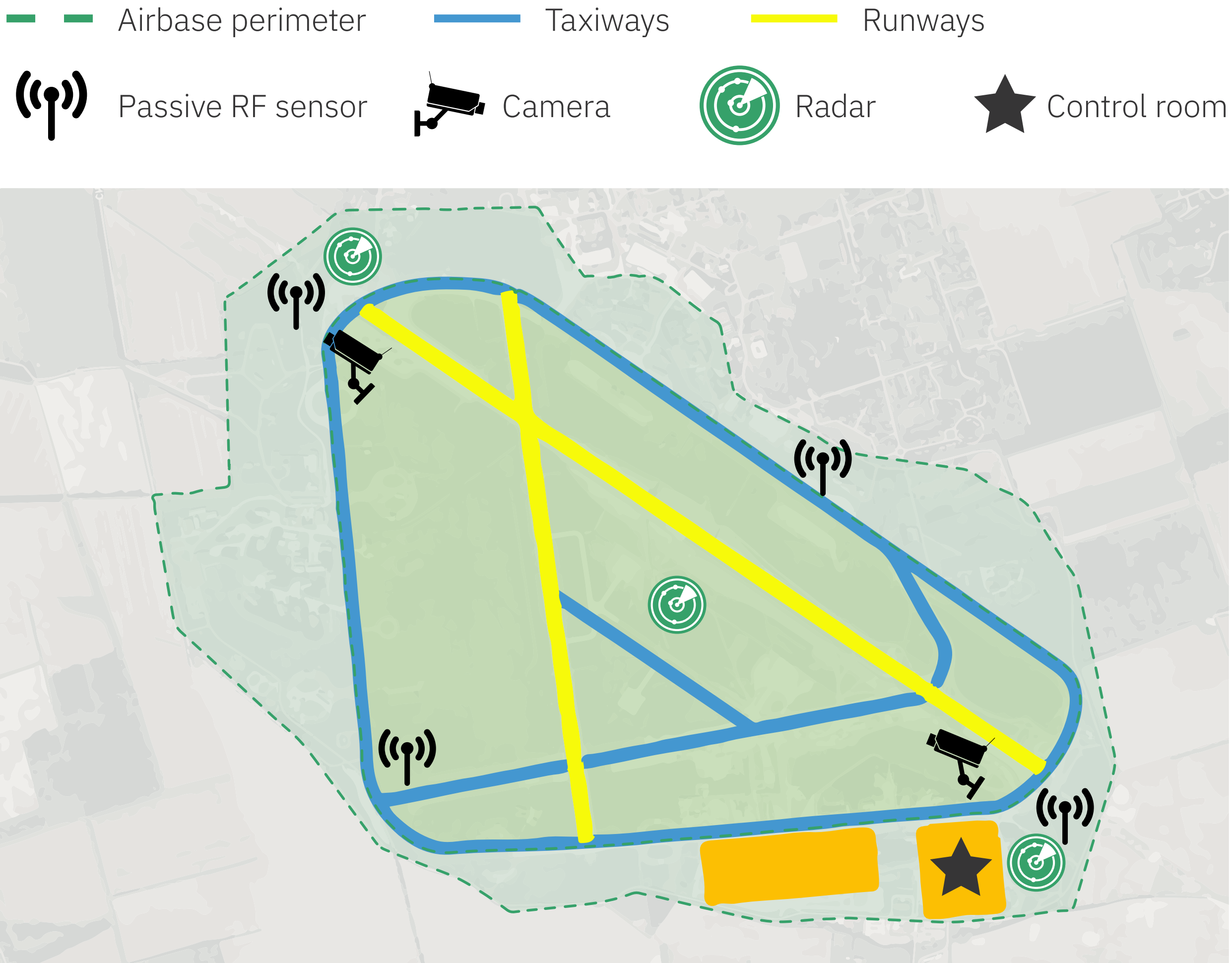


Figure 1: Potential sensor deployment within an airbase setting

Figure 2 shows an example of UAV detection coverage that could be provided by an airbase C-sUAS system with a suitable combination of sensors such as those shown in Figure 1.

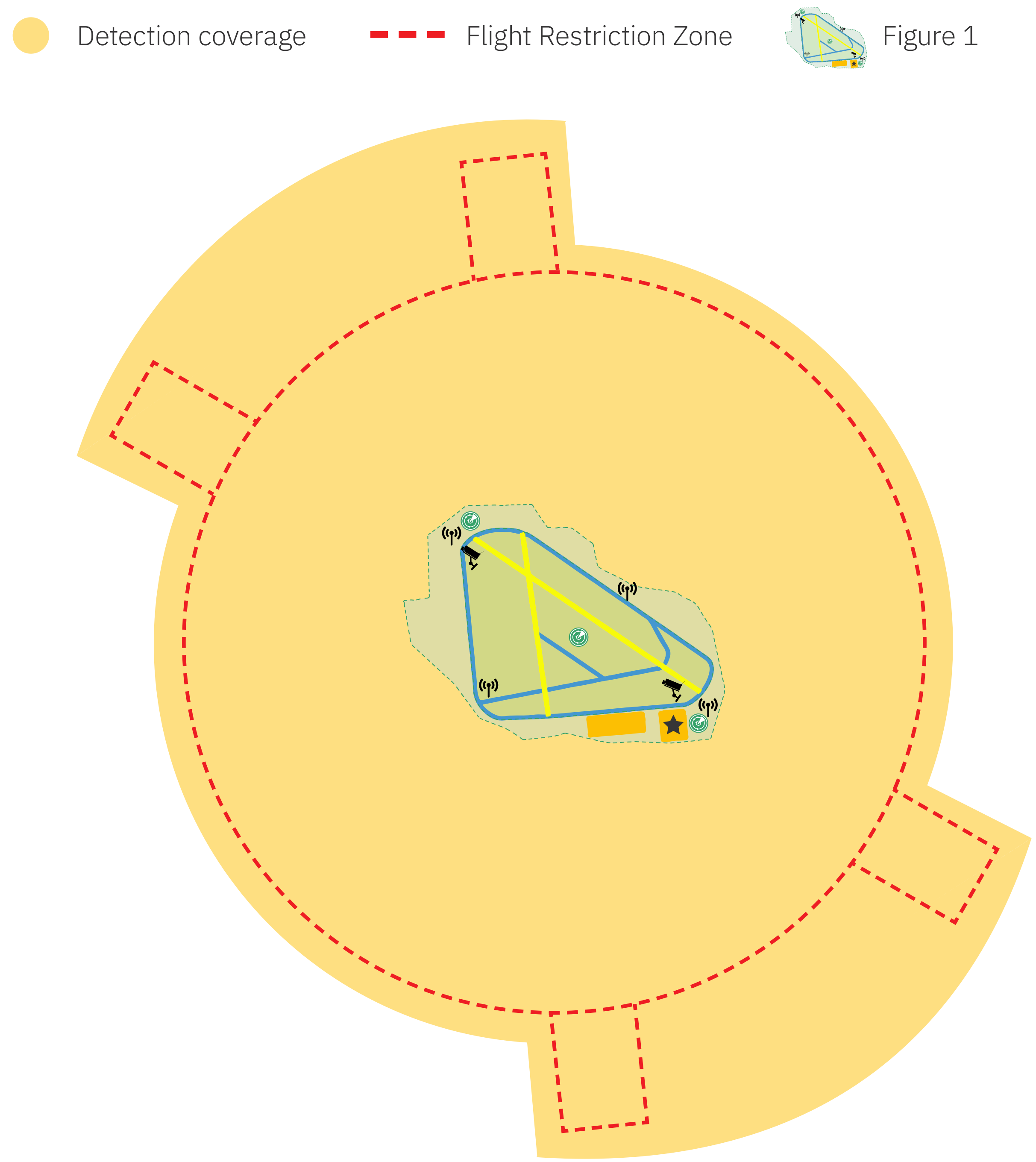


Figure 2: C-sUAS system detection coverage based on figure 1 sensor deployment

4. MULTI-SENSOR DETECTION

Data from UAV events at airbases will predominantly come from three types of sources:

Detections and alerts
from specialised UAV detection sensors of various types

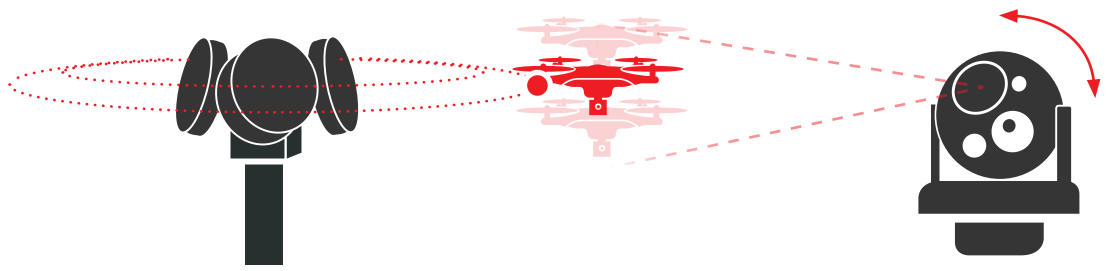
Visual sightings
from aircrew, operations staff, security, police, public etc

Outputs
from other systems and sensors such as CCTV, radar, etc

The coordination and integration of data from multiple sources is a complex challenge. It is unlikely that data from a single source will be of sufficient quality to enable timely and confident decisions to be made to counter the threat. Relying exclusively on a single type of UAV detection sensor will lead to unreliable and restricted threat coverage due to inherent limitations on each sensor technology. For example, passive RF detectors relying on library-based methods will not work for any UAVs that are not already in the library, and cameras of all types will be much less effective in bad weather. Additionally, radars can be easily confused by moving vehicles or rotating equipment such as air conditioning.

Multiple sensors can provide overlapping and complementary coverage that minimises the effects of individual sensor technology limitations and significantly increases the system's overall probability of threat detection.

In addition, a system with multiple sensor types can be used to provide tasking of one sensor based on detections made by a different sensor. This includes "slew to cue" techniques where detections from a radar (for example) can be used to point a camera in the direction of a target.



Incorporating multiple sensor types and locations also has the advantage of increased redundancy. In the event of a deliberate attack, natural disaster or infrastructure failure it is plausible that certain sensors will become temporarily or permanently unavailable. In these cases, a system that can offer resilience and survivability by continuing to provide UAV threat protection and detection for an airbase has great value.

5. OPEN STANDARDS AND EXTENSIBILITY

For an optimal C-sUAS solution, airbases should deploy a solution that can be evolved and scaled so that:

The system can be upgraded to keep pace with evolving threats

Through use of standard interfaces (such as SAPIENT and ASTERIX) the system is capable of integration with existing and future security systems

Individual system hardware or software components can be upgraded independently through a modular approach

To support cost-effective and flexible future development, incremental expansion should be possible around a core C2 component. For maximum flexibility and extensibility, the C2 component should be able to accept any number of sensors from any supplier.

This approach also reduces the risk of unacceptable delays when the system needs to be upgraded in future and reduces any re-training burden.

6. INTEGRATION WITH OTHER SECURITY SYSTEMS

There are likely to be substantial benefits from integrating specialist C-sUAS systems with existing systems already in place on an airbase. By sharing data between systems, a more comprehensive picture can be presented to control room personnel and operator burden can be reduced. The use of open standards can ease the process of integration of C-sUAS systems with other systems but proprietary or bespoke interfaces can also be used if necessary. In the latter two cases it is vital that the system integrator has the required knowledge and experience in building customised interfaces between systems.

Some examples of existing airbase systems that could potentially be integrated with a C-sUAS system (in an automated or semi-automated fashion as appropriate) are as follows:

> Existing airbase sensors, such as bird detection radars, ground movement sensors and Precision Approach Radars (PAR) which could assist in reducing false alarms

> Air Traffic Management (ATM) systems and systems providing the position of "cooperative" UAVs (e.g. the new "Remote ID" system being introduced in the US), which could provide crucial information for the C-sUAS system to differentiate threats

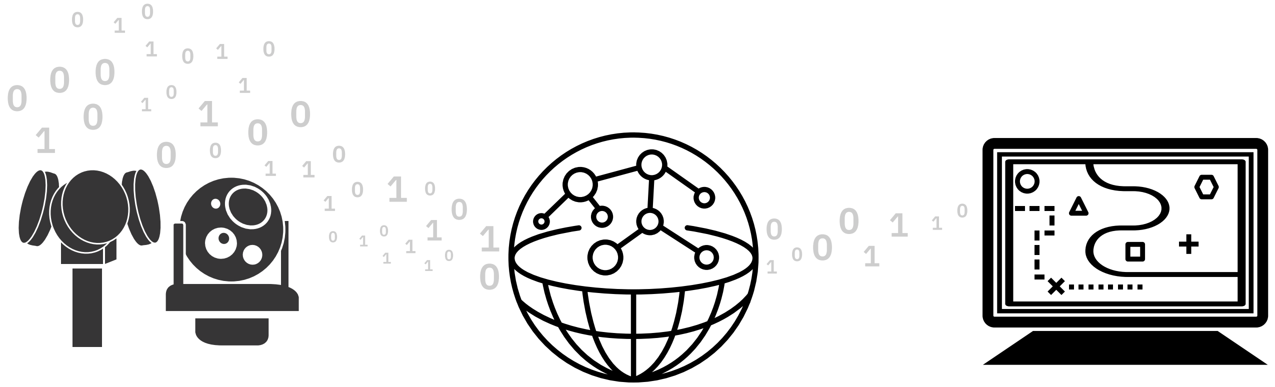
> Physical Security Information Management (PSIM) systems that could provide information on the location of suspected UAV activity, allowing the cueing of CCTV cameras to capture imagery of pilots or other ground-based activity linked to UAVs

> Base-wide alarm systems which could relay alerts on serious threats produced by the C-sUAS system to all personnel

C-sUAS systems can additionally be linked to a wide area computer network (WAN) to allow integration with centralised military and other Government systems.

7. DATA FUSION AND CORRELATION

A highly capable command and control (C2) component is essential to make full use of the threat detection coverage provided by multiple sensors. The C2 component needs to perform correlation and fusion between the data sources in order to create a single common operating picture (COP). A Human Machine Interface (HMI) is also needed that presents the information from the C2 component to the operator in a clear and coherent way.



A C-sUAS system using an appropriate multi-sensor approach with a suitable C2 component and HMI will provide operators and stakeholders with reliable and timely threat information. This threat information will then result in a rapid and proportionate response. Combining multiple sources into a single operational picture reduces operator burden and has the potential to reduce the overall false alarm rate by requiring multiple sensor types to detect a target before an alert is even generated in certain cases.

There are many challenges to producing a C2 component and HMI. In particular, integrating and presenting data from multiple diverse sources has the potential to lead to duplicate tracks and alerts on the same object. There is also the risk of data from sensors being inappropriately discarded, for example if tracks from two sensors on two different objects are erroneously correlated together. These challenges mean that it is critical the provider of the C2 component and HMI has a proven pedigree in data fusion and correlation.

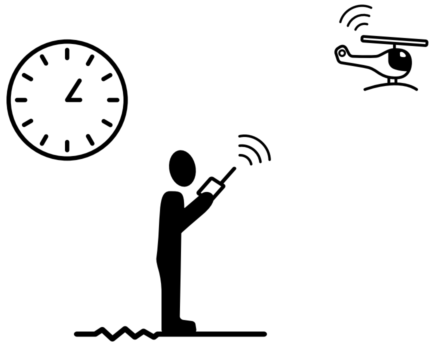
8.SYSTEM OPERATORS AND TRAINING

To be useful for airbase operations, operators should be notified of any UAV incursions in real-time so that continuous monitoring is not required. Details of UAV activity (including geographic location and any identity information) should then be presented using an HMI designed for a security control room environment. An HMI offers a simple interface that can be monitored alongside other airbase security systems without the need for any additional manpower, minimising the operational burden.

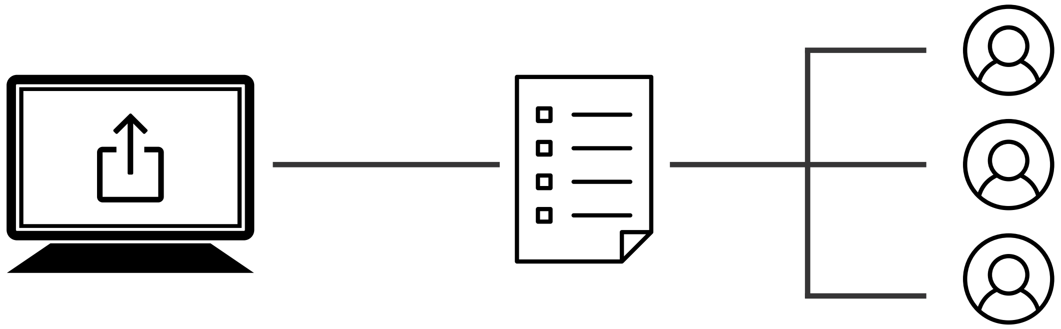
Operator training for a C-sUAS system with a well-designed HMI should not be onerous for control room personnel with experience of other security or similar systems. It is expected that a "train the trainer" approach would be appropriate and all required training topics could be covered within a single day. Training of the maintainers for the system is longer and more complicated but the same general approach can be taken in both cases.

In addition to the requirement for real-time UAV threat information, airbase stakeholders may require post-event analysis to be performed. This could be needed for evidential purposes as well as for general pattern of life reviews. Pattern of life reviews can determine typical UAV (and UAV-like) activity in the vicinity of an airbase and allow refinement of procedures for operators and general airbase operations.

For example, if a local model flying club was found to operate at the same time each week, operators could be trained to treat any alerts generated by the system at these times differently to those generated at other times.



To facilitate post-event analysis, any C-sUAS system HMI should enable operators to view events historically via a time-selected event review feature where full trajectory and identity data can be accessed. The C-sUAS system should also allow high-level information about each event of interest to be exported in the form of a report (e.g. PDF) for dissemination to relevant stakeholders.



9. C-SUAS REACTION AND EFFECTOR SYSTEMS

Once a UAV is detected, tracked and assessed as a threat, decisions can be made regarding the countering of the UAV, according to the relevant CONOPS. Countering can be active or passive; for example, in the UK, active responses would most likely involve RF jamming while a passive response might be to move vulnerable assets away from the UAV, suspend runway use or to mobilise security personnel to search for the pilot.

RF jamming at an airbase raises key concerns over the potential for collateral interference (e.g. GPS jamming would impact existing systems at the airbase and beyond), and such countermeasures cannot be deployed lightly. The broadcasting of RF is tightly controlled, but specialist jamming devices can be used at airbases without affecting other critical equipment if jammers are selected and configured correctly. Other active countermeasures may become more relevant at airbases in the future as technology improves and regulations change. These could potentially include use of high energy lasers, UAV capture devices (e.g. net guns) or specialised ballistic effectors.

The deployment of any active countermeasures would be on a case-by-case basis with activation clearly regulated and high confidence in the presence of a threat needed before an active response could be authorised. As such, deployment of active countermeasures would almost certainly be manually initiated, but this could potentially be done from the HMI of a C-sUAS system, or via an interface to an approved effector engagement system.

The primary response to a UAV threat should always be locally determined and controlled. However, an effective C-sUAS system should also be able to provide distributed real-time alerts and/or post-event information to remote stakeholders via suitable secure networks. This will allow coordination of a wider response to the threat if appropriate.

10. PARALLEL DEVELOPMENT

Within the UK Ministry of Defence (MOD), parallel development concepts within capability management are referred to as Defence Lines of Development (DLODs). Such mechanisms for coordinating different aspects of defence capability are universally required and have great relevance to the delivery of a C-sUAS solution. Examples of parallel development aspects applied to a C-sUAS system are as follows:

Training
Required training of system operators and maintainers will be delivered such that all personnel are appropriately trained. This will allow the system to be fully operated and maintained from the required operational start date and throughout the lifetime of the system

Equipment
Complementary and compatible sensors and effectors will be selected and procured for installation at the deployment site

Personnel
The training, support and procedures required by control room staff to operate the system with minimal additional demands need early assessment

Information
Relevant details of previous UAV incursion incidents (from multiple sites if possible) will be gathered and analysed to optimise sensor/effector siting and operator training through consideration of observed pattern-of-life characteristics

Concepts and Doctrine
The CONOPS of the system will be defined and refined based on discussion with relevant stakeholders, which will include procedures for taking specific actions when particular types of UAV threats are detected

Organisation
The relationship between all relevant stakeholders in the system will be documented, with identification of chains of command related to taking actions following detection of a UAV threat

Infrastructure
C-sUAS systems will typically require equipment sited at multiple locations which will involve appropriate physical installation as well as establishing connection to power and IT networks

Logistics
C-sUAS systems typically involve equipment from multiple different suppliers, with on-site storage of spare equipment in order to replace faulty units. In some cases, it may be cost-effective to share equipment between sites

Interoperability
Implementation of a C-sUAS system architecture that allows relevant data and information products (e.g. alerts and event evidence) to be shared securely with other systems (including those of other stakeholder organisations) if required

Each parallel development aspect needs to carefully accounted for during the planning phase of every C-sUAS deployment project and coordinated with the other aspects that will be occurring concurrently during delivery and beyond. This will allow a capability that fully meets the requirements of the customer to be delivered on time and within budget, as well as providing full benefits to the customer and other stakeholders over the operational lifetime of the C-sUAS system.

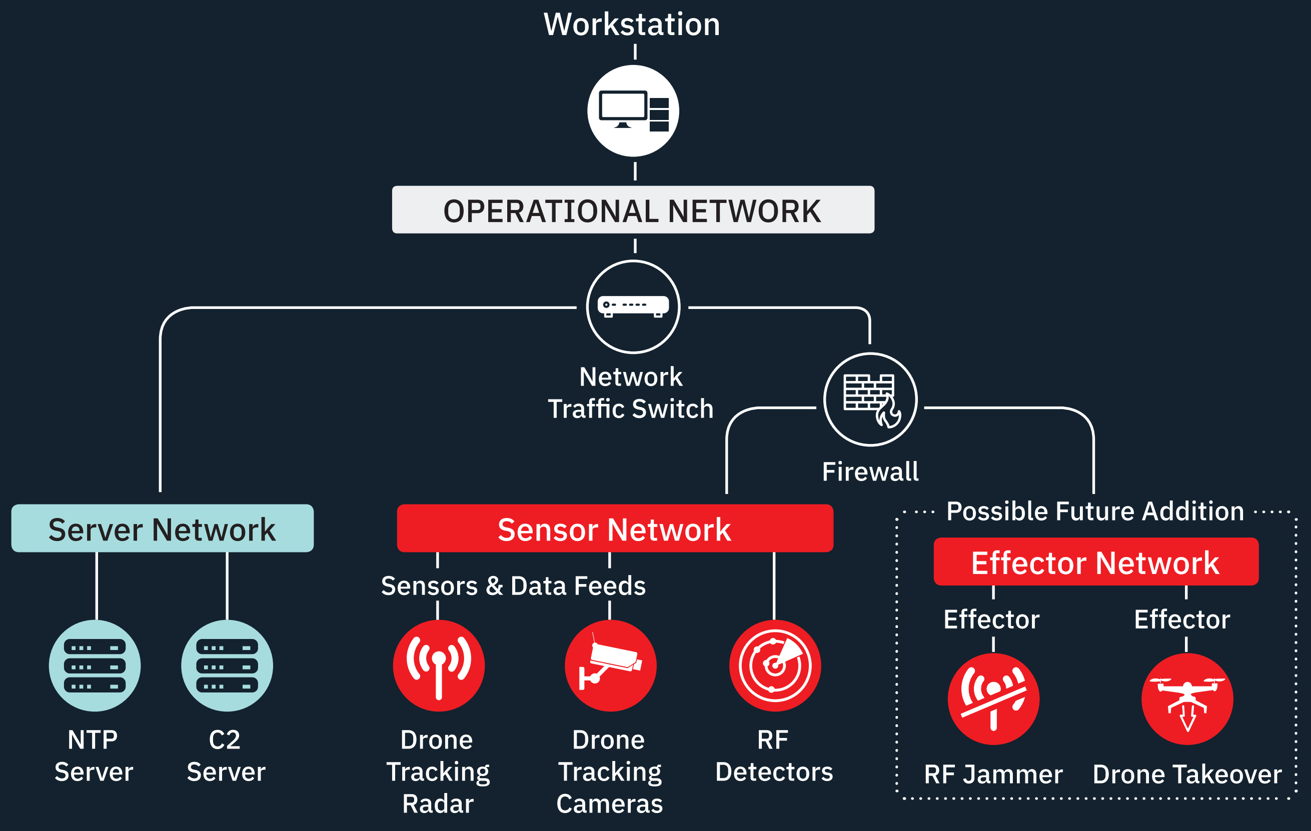
The planning process will need to involve the customer as well as contractors.

L3HARRIS DRONE GUARDIAN

Our sensor- and effector-agnostic C-sUAS solution, Drone Guardian, offers proven fixed site protection. Underpinned by intuitive C2 software, the system operates in the background and requires very low manpower, helping operators detect, track, identify and defeat sUAS threats in real-time. This multi-sensor approach combined with L3Harris' 35 years of heritage in data fusion and situational awareness delivers increased probability of drone detection, reduced false alarm rate and minimal operational burden. L3Harris has extensive experience in tailoring solutions to specific requirements, including mission-critical infrastructure protection, as well as a strong reputation for reliable and timely delivery.

Drone Guardian's open architecture has a proven pedigree of being able to integrate with diverse sensor solutions and technologies to meet the operational need, with L3Harris perfectly positioned to support in building customised software and hardware interfaces. Drone Guardian has already been successfully integrated with multiple radars, cameras, RF sensors, RF jammers and PSIM systems. The open architecture is also compatible with open standards for data exchange such as SAPIENT (including Version 7, the latest version as of 2022) and ASTERIX, allowing low risk and rapid integration of sensors and effectors compliant with these standards.

The system is designed for minimal or no constant monitoring by operators, with an HMI featuring customisable visual and audible alerting, as well as via email or text messages. This means no increase in security manpower while achieving immediate notification of threats. A representative Drone Guardian system architecture is shown in Figure 3.



Through non-kinetic L3Harris BROADSHIELD® and CORVUS® electronic warfare countermeasures as well as multiple kinetic effectors, Drone Guardian further enables the safe and reliable defeat of drones and drone swarms as needed. The power and frequency range of such jammers are configurable to allow compliance with any applicable regulations and to avoid interference with other equipment. Drone Guardian is ideally suited for deployment at any type of airbase requiring a C-sUAS capability.

EVOLUTION AND GROWTH

L3Harris envisages that current technologies and methods will remain relevant for detecting and countering the majority of readily available UAVs, at least for the foreseeable future. This said, it will be essential to have a C-sUAS system that is flexible and scalable to incrementally evolve with threats and regulations, as well as integrating new sensor and effector technologies as they emerge. L3Harris continues to invest in the development of Drone Guardian and will therefore be able to offer new and upgraded C-sUAS capability to customers as requirements change.

GLOSSARY OF TERMS

AD	Air Defence
ASTERIX	All Purpose Structured Eurocontrol Surveillance Information Exchange
ATC	Air Traffic Control
ATM	Air Traffic Management
C2	Command and Control
CCTV	Closed Circuit Television
CONOPS	Concept of Operations
C-sUAS	Counter-Small Unmanned Aircraft System (where small denotes NATO Class I or below)
DLOD	Defence Line of Development
FRZ	Flight Restriction Zone
HMI	Human Machine Interface
MATZ	Military Aerodrome Traffic Zone
PSIM	Physical Security Information Management
RAAF	Royal Australian Air Force
SAPIENT	Sensing for Asset Protection with Integrated Electronic Networked Technology

FURTHER INFORMATION:

To learn more about how L3Harris can help you stay ahead of the curve please get in touch:

Hello@L3Harris.com

FAST. FORWARD.

L3HARRIS®

THE COUNTERING THE UAV THREAT TO MILITARY AIRBASES

L3Harris Technologies is the Trusted Disruptor for the global aerospace and defence industry. With customers' mission-critical needs always in mind, our more than 50,000 employees deliver end-to-end technology solutions connecting the space, air, land, sea and cyber domains.