Unmanned Aircraft System Detection - Technical Considerations

DISCLAIMER: The following are technical considerations generally known to the C-UAS industry and relevant government stakeholders. They are provided as a courtesy and are not requirements or officially-accepted processes.

Counter-Unmanned Aircraft System (C-UAS) technologies are broken into two primary categories—detection and mitigation. Such technologies range from Commercial off the Shelf (COTS) systems to made-to-order systems developed by system integrators. The systems and sensors share similar characteristics and methods for detecting Unmanned Aircraft Systems (UAS), colloquially known as "drones."

Some detection systems are based on existing technologies, re-purposed for C-UAS efforts. For example, radar technology has been adapted for UAS detection purposes from uses such as anti-missile and anti-mortar detection applications for the military to weather, low-level wind shear, and avian wildlife monitoring for civilian use. Some UAS detection products have a very low technical maturity and may not be ready for steady-state use in domestic civil airport environments.

There are no nationally-recognized standards for detection or classifying items of interest at this time; detection systems do not have the ability to determine intent or a level of threat posed by the UAS.

The following selected technical questions and supporting materials may assist organizations that are reviewing the capabilities and limitations of UAS detection systems. They suggest some fundamental questions and concepts that an organization might choose to consider when examining and deploying UAS detection systems. Comparison of products and services from competing manufacturers and vendors might also be helpful. The challenges of UAS detection are complex and cannot be fully addressed by these questions alone. The questions included here are not exhaustive or all-inclusive.

UAS Mitigation

UAS mitigation or countermeasures include the capability to disrupt, disable, destroy, take control of, and/or provide alternate flight instructions to a UAS. Some UAS detection systems may have countermeasure capabilities built-in, which can be disabled, while others may offer them as an optional modular capability.

Does the UAS mitigation system have any capability to conduct countermeasure activities? If so, how is it disabled?
Which category of countermeasures is the system capable of?
Kinetic Non-Kinetic Hybrid Kinetic (Non-Kinetic with Kinetic Effect)
Which technologies or methods of countermeasures does the system employ?

Kinetic	Non-Kinetic	Hybrid Kinetic
Projectile	*RF C2 Jamming*	*Microwave*
Net / Open Containment	*RF C2 Intercept and Control*	*Acoustic*
Closed / Sealed Containment	*RF C2 Intercept and Control*	*Laser*
Predatory Animal	*GPS Jamming*	*NNEMP*

UAS Detection: General

A key factor in determining the feasibility of installing a detection system at or around an airport is the number of sensors needed to achieve the desired airspace coverage. Because the coverage volume depends on the unique characteristics and requirements of each airport and the type of system, the number of sensors will vary. The coverage distance for many types of detection technologies also constrains the efficacy of such systems in determining the locations of the unmanned aircraft (UA) and the ground control station (GCS). An additional critical factor is that technology can quickly become obsolete, as UAS technology is rapidly changing. Further, areas of coverage may need to span wider angles since the GCS and pilot in command (PIC) may not be collocated with or near the drone.

Primary detection sources are those sensors that have a greater level of system autonomy, providing alerts to be generated upon a detection, prompting further investigation by the detection system operator. Radar and Radio Frequency (RF) are the most common; however, Electro Optic (EO) and acoustic sensors do not typically have the capability to be a primary detection source. EO and acoustic might typically be considered validation tools or secondary sensors to the primary systems (radar and RF).

What are the coverage areas, critical site locations, and volumes of airspace that must be monitored?

What are the technologies or sensors used as a primary means for detection?

Radar RF EO/IR Acoustic Other

What are the technologies or sensors used as secondary or supportive means for validating activity detected by primary sensors?

Radar RF EO/IR Acoustic Other

Has an RF analysis been conducted for this site? Who conducted the analysis? Were the RF emissions simulated or actual?

Certain aircraft operational states (e.g., hovering) and the degree of flight autonomy may limit detection.

What types of UA can the system detect?

Multirotor Fixed-wing Hybrid Inflated Envelope Glider Other

How long does it take the system to detect a UA that is within range?

Dedicated manpower and specialized training is likely needed to operate equipment and help to discern false positives, such as when a detection system may incorrectly identify another moving object as a UAS.

How does the system make a determination between the sensing of a potential item of interest, and classifying it as a UAS?

Does the system detect semi-autonomous UAS (i.e. UAS that use pre-programmed navigation, but are capable of RF transmission)? If so, how?

Does the system detect fully autonomous UAS (i.e. UAS without RF capabilities that can navigate without in-flight commands)? If so, how?

Can the system detect UAS powered-on, but prior to flight?

Can the system detect and geolocate the ground control station (GCS)? If so, how does it accomplish this?

Does the system have only line of sight (LOS) capability, i.e. will trees and buildings inhibit the system's capabilities?

Which personnel should operate the system?

What kind of training is necessary to use the system?

What training is included?

What support is included?

Does support include software updates to address evolving UAS technology?

Is the system a fixed installation or is it readily deployable?

Is the system easily installed by personnel who are not affiliated with the system manufacturer or vendor?

Is the system readily portable to a civil environment?

What are the system specifications or requirements for the following at each point of installation:

Specifications / Requirements

Size (incl. antenna/sensor heights) Physical Storage

Deployment/Set-up Communications

Power Input Electrical Grounding

Calibration Physical Storage

Airport environments have numerous sources of potential interference – often more than anticipated which can impact performance of systems. Unintentional emitters of electromagnetic interference (e.g., power lines, breakers, bunched power cables, LED and florescent fixtures), as well as intentional emissions (e.g., digital and analog antennae, cellular services, 2-way radios, telemetry systems) could affect the accuracy of RF-based UAS detection sensors.

Frequently, multipath interference occurs as a result of unintentional reflections from large objects. This type of interference can be caused by large passenger planes inside a sensor area, skewing the location accuracy of the detection system. Similarly, equipment such as heating ventilation and air-conditioning units and electric motors co-located with a sensor can cause interference with the sensor's directional orientation, in addition to background electromagnetic interference and multipath reflections. Interference can also diminish the detection range of some systems.

Natural impediments such as trees, terrain, moisture and wind also impact sensors.

RF Detection

Manufacturers or vendors may identify RF systems as not emitting (often using the term "passive") although the product could include and regularly employ such emitting capabilities. In a steady state, a system may not appear to emit. This same system, however, may have embedded emitting capabilities that are deactivated through software that could be reversible. Further, some systems may emit during software upgrades, site installation, scheduled intervals or ad-hoc calibration. For these reasons, organizations would not be able to categorically assume any detection system does emit RF energy, which may impact the National Airspace System.

What is the coverage area per sensor? Azimuth? Altitude? Distance?

How many of each sensor type is required for the required area for this installation?

What are the filtering capabilities the system uses in order to reduce background RF and reduce multipath interference?

Does the detection system depend on a library of known RF signatures? If yes, how often is the library updated? What is the process to update the library? Is there an ongoing cost for library updates?

Can the system detect and geolocate the UAS pilot-in-command (using RF)?

Is the system able to detect a UAS operator who is intentionally hopping or changing frequencies at a random and/or rapid rate in order to evade detection?

Does the system intercept the live video streaming of the UA?

Does the system differentiate and track multiple simultaneous targets? If so what is the upper limit on the number of targets it can track?

What are the FCC licensing requirements for this system? Do you have proper approval from the FCC, if needed?

For this installation, have there been evaluations of RF frequency propagation during day and night to account for any potential electromagnetic interference high levels of DC power or other power sources used for airport lighting, etc. that might not be prevalent during daylight operation?

Radar Detection

Radar-based UAS detection systems can be used as a primary means of detection; however, they are typically challenged by a lack of automation and are highly dependent on a trained operator to become aware of new or changing detections, plot and track geolocations, and to choose the appropriate system settings. Radar-based detection systems also face difficulties when presented with UAS that only move vertically or hover in place. Some radar systems can trigger a secondary electro-optical system to “slew to cue,” which automatically points the optics in the direction of the detected target of interest. This feature can be challenged at times if the system inadvertently determines a larger, manned aircraft in the distance as a new target. Radar sensors are specially tuned for identifying small targets at short, medium or long ranges; therefore, multiple radars with different detection ranges may be necessary to cover the areas of detection.

Radar systems cannot have national spectrum licensing approval, as approvals are site specific. Licensing through FCC approval and in coordination with FAA's Spectrum Office are required for each site.

What types of UA can the system detect?

Multirotor Fixed-wing Hybrid Inflated Envelope Glider Other

How long does it take the system to detect a UA that is within range?

What is the transmit power of the radar?

What are the frequency band(s) of the radar? (Note: L-Band has been reallocated by the FCC)

What is the scanning type of the radar?

What are the radar cross section (RCS) the system can detect and classify at specific distances?

What is the coverage area per sensor? Azimuth? Altitude? Distance?

How do different types of weather affect this radar?

How many of each sensor type is required for the required area?

What are the filtering capabilities the system uses in order to reduce background radar clutter?

Does the detection system depend on a library of known radar signatures? If yes, how often is the library updated? What is the process to update the library? Is there an ongoing cost for library updates?

Electro-Optical Detection

Electro-Optical (EO) and EO/IR sensor suites do not typically serve as a primary detection sensor for detecting and tracking a UAS. They can be important secondary visual validation tools for targets detected by primary sensors. Enhanced EO systems can provide valuable capabilities, including automatic image tracking of potential targets detected by primary sensors; however, they can be challenged by being redirected to false targets, such as birds or manned aircraft crossing the field of view. EO sensors do not, absent human assistance, have the ability to begin tracking an object detected by a primary sensor.

EO specifications are similar to any modern digital camera; the quality of the lens, field of view, varifocal capabilities, pixel size, and pixel density all have a role in the overall image quality and usefulness for validating items of interest. Some metrics, such as pixel density, once exclusively used to determine image quality are no longer accurate – "more megapixels" does not mean a better picture. Performance in low-light conditions, lens quality and the sensitivity of electronic circuits are better indicators of image quality. When used for visual verification of suspicious activity, such as UAS detected by primary sensors, the image quality is critically important. The video surveillance industry uses a commonly accepted metric, Pixels Per Foot (PPF), as a more predictable level of image quality. Though it is not perfect, PPF is a single number conveying important information about the projected quality that a camera can provide. PPF is based on the size of the area that the image is capturing and depends on the distance from the camera, the focal length of the camera lens and the resolution of the camera.

What are the pan, tilt, and zoom (PTZ) capabilities of the EO/IR device(s)?

How are any PTZ capabilities automated in coordination with primary detection sensors?

What is the field of view of the EO/IR device?

What types and levels of image stabilization, if any, are used for EO/IR device(s)

What is the number of Pixels Per Foot (PPF) provided by the EO device?

How are any Artificial Intelligence (AI) or Machine Learning (ML) capabilities employed to assist in detection or classification of UAS?

Is the IR device cooled?

What is the life expectancy of the cooled IR device?

What wavelengths does the IR device detect?

What are the network bandwidth requirements of each EO/IR node?

What are the processing requirements of each EO/IR node?

What compression algorithms are used for EO? For IR?

Data and Information

Data and information management plays a crucial role in UAS detection systems. In addition to common "best practices" for information technology management and data security, some other factors might be considered. Clearly demonstrated tools and features such as statistical dashboards, historical information, and data portability may have greater value than amorphous buzzwords like artificial intelligence (AI) and machine learning (ML).

How will the system distinguish or deconflict between authorized and unauthorized UAS?

How does the system handle duplicate targets from multiple or overlapping sensors?

How is suspicious activity data verified or validated?

How is suspicious activity data generated, reported, and distributed?

How does the system store and retrieve historical information or provide for statistical analysis and data mining?

How will the federal, state, local and/or tribal retention and disposition requirements for the data that is captured, derived, transmitted, or stored be met?

Does the system employ a digital chain of custody procedure for producing evidence in a court of law?

What is the update rate of the sensors to the system and the system to the interface?

What are the alert and alarm features of the interface?

Does the manufacturer, vendor, or system integrator have access to data that is captured, derived, transmitted, or stored?

Does the manufacturer, vendor, or system integrator have a fix (geolocation) of the detection system?

Does the manufacturer, vendor, or system integrator have the ability initiate software updates (with or without consent)?

Does the system, components, or software have the capability to implement or maintain a whitelist of UAS without the knowledge of the operator or governing organization?

Integrated Solutions

Some systems might be referred to as an integrated solution, which employs multiple types of sensor technologies and provides their data into a single user interface. Other systems may provide capabilities to incorporate an organization's existing hardware and software elements.

These capabilities are still faced with the technical challenges of applying UAS detection systems in the absence of automation aids to help an operator better differentiate legitimate UAS activity from UAS detections that warrant further investigation.

If multiple systems, does the system provide a fused graphical interface to the user with an authoritative source?

How might the system be integrated along with existing security operations centers and infrastructure, such as security cameras, data connectivity, and display systems?

How can external information – such as ground personnel reports or photos - be integrated with the system information?