# FISSURE for C-UAS

Christopher Poore
Assured Information Security, Inc.
153 Brooks Road
Rome, NY 13441
315-336-3306 x1569
poorec@ainfosec.com

## 1. EXECUTIVE SUMMARY

Small unmanned aircraft systems (sUAS) have evolved into persistent and complex threats that are increasingly difficult to detect, classify, or counter with traditional systems. Many existing counter-UAS tools depend on fixed infrastructure, single-sensor inputs, and outdated assumptions that fail in contested and dynamic environments.

Assured Information Security, Inc. (AIS) offers the FISSURE Framework, an open-source, modular system designed for distributed RF and sensor operations at the tactical edge. FISSURE supports customizable tactical nodes built from commercial off-the-shelf (COTS) hardware that can detect, log, and respond to unconventional drone activity. It integrates across multiple sensing domains, enables operator-defined behaviors, and is interoperable with platforms such as TAK.

Backed by AIS' extensive experience in RF systems, drone exploitation, and counter-UAS research, FISSURE provides a scalable and adaptable foundation for addressing today's sUAS threats. Its open, extensible architecture, multi-domain capabilities, and low deployment overhead make it a strong fit for mission environments that demand rapid adaptation, operator control, and seamless integration with existing tools.

## 2. PROBLEM STATEMENT

The threat posed by sUAS has rapidly evolved from a limited nuisance into a persistent and complex challenge across many operating environments. Originally developed as COTS products for hobbyist use, these systems have been adapted into modular, low-cost tools now employed by both non-state actors and near-peer adversaries. They support intelligence, surveillance, reconnaissance (ISR), electronic warfare (EW), cyber operations, and kinetic effects.

Adversaries are increasingly fielding drones with greater endurance, advanced autonomy, hardened communications, and non-standard signaling methods. Many employ low-probability-of-intercept (LPI) waveforms, custom modulation schemes, and encrypted protocols that bypass traditional RF detection. Some avoid RF emissions entirely by using fiber-optic links for control and video relay during critical mission phases, reducing or eliminating detectable signatures and limiting the effectiveness of RF-based sensing.

Meanwhile, access to open-source tools and inexpensive hardware has enabled small, decentralized teams to assemble and deploy capable sUAS platforms quickly. These may feature mesh networking, GPS spoof resistance, onboard autonomy, and modular payloads. They often do not follow common assumptions about drone behavior. Many operate beyond visual line-of-sight (BVLOS), outside ISM bands, ignore Remote ID requirements, or remain passive during key stages of a mission. Communications may be brief, infrequent, or disguised through frequency hopping or custom waveforms.

This evolving landscape creates uncertainty and limits the effectiveness of static, rules-based defense systems. The RF spectrum is saturated, especially in contested or urban environments, and malicious signals may be weak, intermittent, or indistinguishable from background activity. Line-of-sight monitoring is no longer sufficient. Threat identification, characterization, and intent assessment must now occur under conditions of incomplete visibility and limited prior knowledge.

Most existing counter-UAS systems are not designed for this level of complexity. Many rely on fixed signal libraries, single-mode detection (such as radar or RF), or stovepiped sensor platforms that are difficult to update and slow to adapt. Proprietary architectures further limit transparency, interoperability, and operator control. Others are vulnerable to spoofing, signal injection, or cyber compromise. These limitations often force operators to make decisions with incomplete context, increasing the risk of false positives or delayed action.

There is a pressing need for operational tools that move beyond legacy assumptions and fixed infrastructure. These tools must detect, classify, and characterize unconventional threats across the RF spectrum and beyond, while remaining modular and scalable to incorporate visual, acoustic, and protocol-specific interfaces. They must support real-time decision-making without heavy backend support or lengthy training cycles. Closing this gap requires solutions that respond quickly, accurately, and with minimal overhead.

## 3. CURRENT STATE OF PRACTICE

The counter-UAS space is crowded with both commercial and government-developed solutions. These range from specialized sensing platforms to full-spectrum systems that include detection, identification, tracking, and interdiction. While this reflects greater awareness of the threat, the market remains fragmented, with most offerings designed around narrow use cases, proprietary technologies, and outdated assumptions about drone behavior.

Many current systems are built on assumptions that no longer hold true. They are often optimized to detect commercial drones operating in ISM frequency bands, following Remote ID protocols, and staying within visual line-of-sight (VLOS). As a result, they struggle against non-standard, modified, or deceptive platforms. Detection is usually limited to predefined libraries, fixed frequency ranges, or known protocols, leaving blind spots for drones using LPI waveforms, frequency hopping, or non-RF methods such as fiber-optic control.

Detection technologies span multiple domains, including:

- RF-based systems: Rohde & Schwarz ARDRONIS, CRFS RFeye, DedroneTactical, Aaronia AARTOS, AeroDefense AirWarden
- Radar systems: Robin Radar, ESG, CERBAIR, and various X-band and passive radar solutions
- Acoustic systems: Squarehead Technology and other low-frequency audio sensors for motor signatures
- Optical and EO/IR systems: perimeter defense setups for stadiums, airports, and government facilities

Multi-sensor or "layered" systems combine several of these modalities, often with cameras, RF sensors, and radar fused into one product line. Companies like SRC, Hidden Level, and Dedrone market such solutions, while large defense contractors (Lockheed Martin, Boeing, Raytheon, Northrop Grumman, Elbit, BAE Systems) integrate C-UAS packages into broader command and control systems.

Interdiction approaches vary widely and include:

- Kinetic methods such as net-equipped drones, munitions, or explosives
- Electronic countermeasures including handheld or vehicle-mounted jammers, GPS denial, and video spoofing
- Cyber techniques such as protocol exploitation or link takeover
- Directed energy systems such as high-powered microwaves or lasers
- Specialty solutions such as foam launchers for convoys or prisons
- Civilian tools such as Ukraine's "ePPO" drone reporting app

Despite this diversity, most systems share critical weaknesses:

- **Vendor Lock-In:** monolithic systems that are difficult to integrate or expand
- **High Cost:** radar, directed energy, and proprietary software suites are out of reach for many users
- **Slow Adaptability:** reliance on signature libraries and closed firmware limits updates against new tactics
- **Limited Interoperability:** many lack native integration with common platforms like ATAK, WebTAK, or existing sensor fusion frameworks
- **Detection Gaps:** single-modality systems are easily bypassed by drones that emit briefly, operate passively, or rely on non-RF control

Some initiatives, such as Edgesource's SPECTRE and the Dowding C-sUAS COP, attempt to create common operating pictures, but data sharing across platforms is still limited and often blocked by proprietary restrictions. Even widely deployed systems have shown mixed results. In Ukraine, tools such as Dedrone, Bukovel-AD, Typhon, Terrahawk Paladin, Smartshooter, and VAMPIRE have been used with varying success depending on integration, terrain, and threat profile. No system has proven universally effective across all environments.

Counter-UAS requirements are also expanding beyond the battlefield. Airports, prisons, stadiums, and government buildings all face drone-related risks. Yet many current solutions were never designed for mobility, rapid reconfiguration, or dynamic missions. They rely on fixed infrastructure, dedicated networks, or centralized processing, making them poorly suited for disconnected, denied, or low-resource environments.

In summary, today's counter-UAS market is broad but fragmented. Most systems remain expensive, inflexible, and tailored for known threats in controlled conditions. A clear capability gap remains for tools that can adapt in real time to unknown signals, operate across sensing domains, and integrate seamlessly into modern tactical workflows.

# 4. SOLUTION: FISSURE FRAMEWORK

FISSURE is an open-source, modular framework designed for distributed RF and tactical node operations in contested environments. It provides a flexible and scalable approach to counter-UAS missions, replacing rigid, vendor-locked systems with adaptable, field-ready tools built from COTS hardware and a plugin-based software architecture.

FISSURE tactical nodes can be deployed in a variety of configurations, including mounting to vehicles, carrying in backpacks, attaching to drones, or fixing in place. Each node can be equipped with mission-specific software that define behaviors such as RF monitoring, signal classification, protocol analysis, or countermeasure execution. Tactical nodes may operate independently or as part of a coordinated network, giving operators the ability to adapt coverage to mission needs.

The framework supports multi-domain detection, including RF sensing, protocol-level monitoring, acoustic detection, visual classification, and optional radar integration. This layered approach improves resilience against LPI signals, non-emitting drones, and deceptive tactics. Data can be stored locally, transmitted when connectivity is available, or integrated directly with platforms like ATAK for real-time alerts and visualization.

At the center of the system is a coordination hub that manages communication, tasking, and synchronization across tactical nodes. The hub distributes playlist updates, aggregates results, and ensures nodes remain aligned even in dynamic network conditions. Operators interact through the FISSURE Dashboard, a graphical interface designed for configuration, monitoring, and alerting. The dashboard provides real-time visualization of tactical node activity, integration with TAK for map-based awareness, and tools for defining or updating behaviors.

Countermeasure options include jamming, GPS disruption, replay of IQ data, and protocol-specific attacks such as Wi-Fi deauthentication. Responses can be automated through rules-based triggers or kept under operator control, allowing flexible alignment with mission rules of engagement.

One of FISSURE's most important features is its plugin architecture. New detection algorithms, countermeasures, or sensor integrations can be added without altering the core system. This reduces time to field, avoids vendor lock-in, and enables teams to continuously adapt as drone technology evolves.

# 5. KEY BENEFITS

The following features highlight how FISSURE supports a range of counter-UAS missions and deployment environments.

**Open Source and Extensible:** FISSURE is community-driven and fully modifiable. Users can create plugins, integrate new hardware, and extend functionality without vendor lock-in. Its

open design ensures rapid updates and continuous improvement as threats evolve.

**Low Cost:** Tactical nodes can be built from COTS hardware, reducing per-unit cost and enabling deployment at scale. Unlike many radar or directed energy systems, no single component is prohibitively expensive.

**Modular and Flexible:** The system supports a wide variety of radios, antennas, sensors, and network types. Users can tailor deployments to their environment, mission, or threat profile.

**Multi-Sensor Support:** FISSURE tactical nodes can integrate RF, acoustic, visual, and other sensing modalities. This enables cross-domain detection and characterization, improving resilience against unconventional threats and deceptive tactics.

**Scalable Deployment Options:** Tactical nodes can be deployed on UAVs, in convoys, mounted to buildings, concealed in terrain, or scattered across a wide area, all coordinated through a central hub and dashboard.

**Autonomous and Distributed Operation:** Nodes continue functioning even when disconnected, logging data locally and reporting results once connectivity is restored. Multiple nodes can be coordinated to cover broad areas or perform synchronized actions.

**Scriptable Behavior via Playlists:** Detection routines and countermeasures are defined in simple, readable playlist scripts. Operators can preload actions or define responses to triggers with minimal overhead.

**Flexible Countermeasure Execution:** FISSURE supports both passive monitoring and active effects, including RF jamming, GPS disruption, replay attacks, and protocol exploitation. Rulesets can be tailored to automate responses or keep operators in the loop based on mission requirements.

**Alerting and TAK Interoperability:** Alerts and messages can be pushed directly to TAK clients in real time. Operators can visualize alerts, review data, and issue commands from common operating pictures (COPs) such as ATAK.

**Data Logging and Offline Analysis:** Tactical nodes can store IQ or sensor data locally for replay, analysis, or use in developing cyber and RF capabilities. This enables collection in low-bandwidth environments without requiring continuous connectivity.

**Integration Ecosystem:** FISSURE can serve as a control interface for existing sensor suites and is compatible with a broad range of third-party open-source tools for RF, protocol, and signal analysis, enhancing post-processing and mission planning workflows.

**Future Growth:** FISSURE provides a testbed for experimentation, allowing new detection methods, countermeasures, or integrations to be developed and fielded quickly without vendor restrictions.

**Training and Ease of Use:** The operator burden is low. Tactical nodes can be configured with minimal training, and TAK integration leverages a platform that many operators already use and understand.

# 6. RELEVANT EXPERIENCE

AIS has extensive experience in RF systems, drone exploitation, and counter-UAS research, with a proven record supporting test, evaluation, and integration across C5ISR domains. Our work spans a wide range of commercial and modified small UAS platforms, including research into vulnerabilities in communications, navigation, and payload control.

We have conducted hands-on research in link-layer exploitation, GPS spoofing and denial, video feed manipulation, protocol fuzzing, denial-of-service attacks, and system-level disruption. This includes both red-team assessments and defensive evaluations, providing insight into how UAS platforms behave under stress and how countermeasures must adapt.

AIS regularly contributes to joint demonstrations, field events, and technology evaluations with government, academic, and industry partners. We help operate the ORION technology accelerator in Rome, NY, which includes a dedicated drone cage and hangar space that enable safe experimentation and demonstration of advanced capabilities. These facilities provide controlled environments for rapid prototyping, realistic testing, and collaborative evaluation.

In addition to UAS-focused research, AIS has deep expertise in RF signal processing, electronic warfare, and spectrum operations. This includes forensic analysis of commercial RF technologies, development of advanced digital signal processing (DSP) techniques, and evaluation of acoustic and optical sensor modalities. Our staff have supported integration efforts across a broad set of C5ISR systems, ensuring interoperability with existing workflows and platforms.

This background demonstrates AIS' ability to bridge research, experimentation, and operational deployment. It is the same philosophy that drives the FISSURE Framework as an adaptable, open-source solution for counter-UAS and related mission areas.

# 7. CONCLUSION

The small UAS threat is evolving faster than many defense tools can keep pace. Closed, monolithic counter-UAS systems remain costly, rigid, and narrowly scoped, leaving operators with limited options against unconventional tactics.

The FISSURE Framework provides a different path. Built for adaptability, it gives operators the ability to deploy tactical nodes quickly, integrate multiple sensing domains, and define responses in ways that legacy architectures cannot. Its open design encourages continuous improvement and rapid incorporation of new capabilities.

AIS combines deep expertise in RF systems, drone exploitation, and counter-UAS research with a proven record of test and integration. With FISSURE, we deliver a practical foundation that can scale from today’s missions to tomorrow’s challenges, enabling operators to respond at the speed of threat evolution.