FISSURE for Perimeter & Infrastructure Defense

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

1. EXECUTIVE SUMMARY

Critical facilities such as bases, airports, campuses, utilities, and data centers face mixed, fast-changing radio frequency (RF) and cyber-physical threats at their perimeters. Fixed, single-purpose systems often struggle to adapt, especially where links are intermittent, staffing rotates, and budgets favor incremental deployments. Teams need a way to sense, classify, and act across domains that fits existing workflows and keeps an evidentiary record tied to time, place, and configuration.

Assured Information Security, Inc. (AIS) offers the FISSURE Framework, an open-source, plugin-driven system built on commercial off-the-shelf (COTS) hardware and software-defined radios (SDRs). FISSURE scales from a single workstation to a distributed set of tactical nodes positioned at gates, rooftops, and standoff areas, and extends to nodes on vehicles and small unmanned aircraft when mobility is required. Nodes coordinate for tasking and synchronization, communicate over low- and high-throughput links, and can be tailored with compatible radios or adjunct sensors to match local threats and operating policies.

The framework fuses RF, protocol-level, acoustic, visual, motion, infrared (IR), and cellular cues to raise detection confidence, classifies activity to infer likely intent, and supports triggers that shift nodes between monitoring, verification, and response modes as policy allows. FISSURE integrates with Team Awareness Kit (TAK) for real-time awareness, chat, and geofenced tasking. It maintains PostgreSQL-backed logging with Global Positioning System (GPS) and configuration provenance so operators can trace alerts to system state. Because FISSURE is modular and community-driven, new detection methods, countermeasures, and hardware integrations can be added as they are developed, enabling organizations to improve capability without vendor lock-in. The result is a practical, low-cost foundation for perimeter and infrastructure defense that adapts to diverse threats, including counter-unmanned aircraft systems (counter-UAS), covert or rogue Wi-Fi, cellular anomalies, handheld radios near access points, GPS manipulation attempts, and other protocol-driven behaviors that require fast, coordinated sensing and response.

2. PROBLEM STATEMENT

Perimeter defense must operate in crowded radio frequency (RF) and sensor environments where malicious activity is weak, intermittent, or deliberately blended into routine traffic. Facilities need to recognize rogue access points, cellular anomalies, handset beacons, handheld radios, telemetry links, and small unmanned aircraft systems (sUAS) control channels without disrupting normal operations.

The picture is rarely just RF. Motion analytics, acoustic microphones, infrared (IR) cameras, and other site sensors add partial clues that only become useful when fused and tied to time, place, and configuration. Effective detection depends on combining several modest signals, classifying activity to infer likely intent, and presenting clear context for human review.

Edge realities complicate this work. Connectivity is uneven at fence lines and rooftops, staffing and experience levels vary, and policy limits what actions are allowed. Tools therefore need compact, store-and-forward messaging, low training overhead, and simple triggers that let nodes pivot between monitoring, verification, and response modes within policy. Approaches that assume steady networks and fixed signatures leave gaps when adversaries change bands, emit briefly, or avoid emissions altogether; the requirement is a modular approach that treats RF as one layer in a broader perimeter picture and accepts adjunct sensors as first-class inputs.

3. CURRENT STATE OF PRACTICE

Perimeter security at most facilities is a stitched set of systems assembled over time. Cameras and a video management system (VMS) watch gates and corridors. Badge and door controllers govern access. RF gets episodic attention through compliance scans, contractor surveys, or appliance boxes for Wi-Fi monitoring and occasional drone detection. During special events, sites rent extra gear and fold it into temporary command posts. This works for routine operations but falters when threats are irregular, distributed, or intentionally quiet.

Most offerings are closed and hardware-bound, tuned for known signals and fixed deployments. RF tools ship with static libraries and limited paths to add custom detections or drop new classifiers at the edge. Camera analytics and access control live in separate ecosystems with different vendors, data formats, and licenses. Interoperability often means CSV exports or proprietary APIs that are difficult to automate. Many systems assume reliable networks and centralized processing, which is not always true on rooftops, fence lines, or remote substations.

These constraints limit adaptation and context. Alerts frequently lack the GPS, configuration state, and timing needed for confident after-action review. Weak but meaningful cues are hard to correlate across domains when data is siloed. Field teams cannot easily script a new check, try a different radio, or reposition capability on a vehicle or small unmanned aircraft before the next shift. An open, plugin-driven framework can fill these gaps by enabling local customization, edge updates, and lightweight publishing to the common operating pictures teams already use.

4. SOLUTION: FISSURE FRAMEWORK

FISSURE is an open-source, modular framework that turns commercial off-the-shelf (COTS) hardware and SDRs into coordinated perimeter sensing and response. Tactical nodes can be driven by an operator through a dashboard or set to follow light

automation, with behaviors defined in readable playlists. Nodes scale from lightweight kits to full-compute edge boxes and can be placed at gates, rooftops, and standoff areas, or mounted on vehicles and small unmanned aircraft when mobility is required. Each node can be tailored for a specific role or target profile, so teams align sensors and radios to local conditions.

The framework is designed to fuse RF with adjunct sensors and protocol-level checks so modest cues become actionable when tied to time, place, and configuration. Nodes exchange compact, policy-aware messages that tolerate intermittent links and preserve provenance, with store-and-forward behavior so alerts and tasking survive real conditions. Flags help distinguish operator-initiated actions from automated checks, and simple triggers allow nodes to shift between monitoring, verification, and response modes within policy.

Networking options include on-site Wi-Fi, Wi-Fi HaLow, and mesh radios such as Meshtastic for multi-mile alert forwarding when backhaul is scarce, with higher-throughput paths over cellular or satellite communications (SATCOM) where available. Outputs publish to TAK for shared awareness, chat, and geofenced tasking, and logs are kept in a database such as PostgreSQL with GPS and configuration context so operators can reconstruct timelines and support training or investigations.

Because FISSURE is plugin-driven, teams can add radios, sensors, detection routines, and policy-controlled effects as they are developed without changing the core. The intent is a practical perimeter capability that adapts as threats and requirements change, supports both operator interaction and light automation, and fits within the systems that facilities already use.

5. DEPLOYMENT SCENARIOS

FISSURE can be configured for fixed, semi-fixed, and mobile use, with nodes ranging from small kits to full-compute edge boxes for classification and artificial intelligence (AI). The examples below span defense, public safety, transportation, utilities, and enterprise facilities, and emphasize multi-sensor fusion where modest cues become actionable when combined.

Gate and Entry Control: Sweep for unfamiliar infrastructure and cellular anomalies at gates. Fuse RF cues with motion analytics and license-plate or badge events to raise confidence. Publish compact alerts to TAK for rapid triage.

Rooftop and Overwatch Coverage: Watch approaches and rooftops with wideband scans and targeted verification. Cross-cue pan-tilt-zoom (PTZ) cameras or thermal imagers when signal patterns change. Use playlists to balance dwell time, power, and bandwidth.

Event Perimeters: Stand up pop-up kits for stadiums, ceremonies, and temporary security zones. Apply geofences for alert routing and TAK-based coordination among responders. Store and forward when backhaul is limited.

Parking Lots and Standoff Areas: Monitor adjacent roads and lots for push-to-talk, brief control-channel bursts, and telemetry. Cue patrols or cameras when thresholds are crossed. Keep context for after-action review.

Border Crossings and Ports of Entry: Watch inspection lanes and secondary areas for covert radios and atypical device behavior. Fuse RF indicators with camera and license-plate systems where available. Operate over low-throughput links when infrastructure is sparse.

Airports and Airfields: Pair counter-UAS playlists with acoustic and imagery inputs while scanning for uplink and downlink activity near flight lines. Coordinate alerts with airfield operations using TAK or existing common operating pictures (COPs). Preserve an evidentiary trail tied to time, place, and configuration.

Utilities, Substations, and Pipelines: Deploy weatherized nodes along fence lines and remote huts to spot unauthorized radios and telemetry. Use mesh radios to forward alerts over miles where fiber is unavailable. Sync data when cellular or SATCOM is present.

Rail Yards and Transit Hubs: Observe depots and platforms for illicit repeaters and command links that appear during movements. Correlate detections with yard cameras and access events. Surge coverage during peak operations.

Data Centers and Critical Rooms: Guard server rooms, labs, and comms closets for ad hoc links and atypical device presence. Maintain strict logging for audits and investigations. Integrate alerts with VMS and access control.

Hospitals and Campuses: Use gentle scanning profiles that respect operational constraints while watching for unsafe infrastructure changes. Fuse modest RF cues with motion analytics or infrared (IR). Route alerts to campus safety teams in TAK.

Correctional Facilities: Detect contraband cellular usage patterns and drone-drop activity near walls and yards. Combine acoustic, thermal, and RF cues to reduce false positives. Extend coverage to outer perimeters with long-distance mesh links.

Ports, Harbors, and Waterfronts: Extend sensing to piers and warehouses where backhaul is limited. Combine marine-band activity and imagery with site access systems to flag unusual behavior. Forward alerts across the waterfront using mesh links.

Disaster Response and Pop-Up Command Posts: Establish temporary perimeters when fixed infrastructure is unavailable. Share compact alerts with incident command in TAK. Shift nodes between monitoring and verification modes as the scene evolves.

Mobile Patrols and Rovers: Mount full-compute nodes on vehicles for on-edge classification, AI-assisted triage, and rapid repositioning. Backhaul over cellular where available, or relay via mesh when it is not. Use waypoints and geofences to automate survey patterns.

Drone-Borne Gap Fill: Fly lightweight nodes to map coverage holes, chase transient signals, or snapshot a sector during an incident. Cross-cue ground cameras or patrols when aerial detections meet a profile. Land and sync bulk data when higher-bandwidth links are available.

Cellular Watch and Profiled Targets: Observe activity in cellular bands near critical areas for anomalies that fit a site-defined profile, such as sudden small-cell beacons or unusual control-channel behavior. Correlate with motion or camera events for confirmation. Publish concise summaries to TAK for quick decision-making.

6. KEY BENEFITS

FISSURE provides practical advantages for perimeter and infrastructure defense while fitting into existing workflows.

Open-Source and Extensible: Community driven and fully modifiable, with radios, sensors, detections, and effects added as plugins.

Low Cost and Scalable: Built on COTS hardware; grow from one node to site-wide coverage without proprietary licensing.

Multi-Sensor Fusion: Combine RF, protocol-level, acoustic, visual, motion, and IR inputs to raise detection confidence.

Edge Processing and AI: Run classification and triage on full-compute nodes at the edge to reduce latency and bandwidth use.

Band- and Radio-Agnostic: Tailor node stacks to target profiles, including cellular bands and site-specific protocols.

Policy-Aware Messaging and TAK Interoperability: Send compact alerts and tasking to TAK over intermittent links.

Store-and-Forward Resilience: Preserve alerts during outages and sync automatically when connectivity returns.

Evidence and Provenance: Log to a database or filesystem with GPS, configuration, model versions, and timing for audit and after-action review.

Flexible Deployment and Mobility: Field fixed, semi-fixed, vehicle, and drone nodes, with weatherized kits and uninterruptible power supply (UPS) options.

Long-Distance Mesh Forwarding: Relay alerts across many miles with mesh radios (e.g., Meshtastic) when backhaul is limited.

Integration Ecosystem: Hook into VMS, access control, and security information and event management (SIEM) so RF cues can drive cameras, badge checks, and enterprise monitoring.

Operator Control and Light Automation: Support manual workflows plus simple triggers to switch modes within policy.

Continuous Improvement: Build datasets and retrain classifiers to adapt quickly without waiting on vendor releases.

7. RELEVANT EXPERIENCE

AIS has deep experience supporting defense and national security programs alongside commercial partners and prospective adopters, with a long history in cyber operations, offensive and defensive research, and penetration testing. Our teams have evaluated and red teamed commercial and government perimeter systems, characterizing how they detect, classify, and respond under stress. That work spans link-layer exploitation, GPS manipulation, protocol fuzzing, replay, and cross-domain sensor fusion, providing practical insight across airfields, ports, campuses, utilities, and data centers.

FISSURE builds on this background. We have flown FISSURE nodes on drones and participated in joint operations exercises, using those venues to refine playlist-driven workflows, TAK alerting in disconnected conditions, and provenance-aware logging. While perimeter defense is an emerging application area for FISSURE, these demonstrations have validated core concepts relevant to site security and informed next steps for defense and commercial deployments. AIS maintains labs and RF-safe spaces where we emulate adversary signaling, capture datasets, and prototype integrations with VMS, access control, and TAK/COPs, creating a clear path from demonstrations to pilot installations.

8. CONCLUSION

Perimeter and infrastructure defense needs tools that are adaptable, interoperable, and affordable. Fixed, monolithic systems struggle with mixed threats and uneven links; teams need practical ways to sense, classify, and act across RF and adjunct sensors while keeping an evidentiary record tied to time, place, and configuration.

The FISSURE Framework offers that path. It is an open-source, plugin-driven approach that places coordinated nodes at gates, rooftops, and standoff areas, and on vehicles or small unmanned aircraft when mobility is required. Nodes fuse RF with visual, acoustic, motion, IR, and cellular cues; run edge AI for faster triage; relay compact, store-and-forward alerts over mesh when backhaul is scarce; publish to TAK for shared awareness; and log to a database for audit and review.

Teams can start with focused pilots and scale as needs evolve, adding sensors, radios, and behaviors without vendor lock-in. Looking ahead, FISSURE will deepen sensor fusion, expand playbook-driven modes, and streamline integrations so facilities can maintain awareness and control in complex, real-world environments.