FISSURE Overview

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

1. EXECUTIVE SUMMARY

Modern spectrum operations face a rapidly shifting landscape. The rise of unconventional waveforms, encrypted protocols, drones, and low-cost emitters has outpaced many proprietary and closed solutions. At the same time, most available tools remain fragmented, single-use, or locked behind costly systems that are inaccessible to many researchers, trainers, and operational teams. This forces organizations to reinvent capabilities in isolation, slowing progress and limiting knowledge sharing.

Assured Information Security, Inc. (AIS) offers the FISSURE Framework, an open-source, plugin-driven system for RF, intelligence, surveillance, and reconnaissance (ISR), electronic warfare (EW), and cyber experimentation. Built on commercial off-the-shelf (COTS) hardware, software-defined radios (SDRs), and a modular architecture, FISSURE scales from a single workstation to fleets of coordinated sensor nodes.

FISSURE enables RF reverse engineering, signal and data analysis, feature extraction, artificial intelligence (AI)-driven classification, packet crafting, fuzzing, and vulnerability exploration, all within one framework. Users can capture and archive signals, build protocol libraries, and log traffic for long-term study, while also deploying nodes on drones, vehicles, or fixed stations. Integrated PostgreSQL data management, Global Positioning System (GPS) support, and interoperability with Tactical Assault Kit (TAK) allow outputs to feed directly into familiar operational tools.

FISSURE is more than a research toolkit. It is a scalable, adaptable framework for spectrum operations that combines deep analysis with deployable sensing and countermeasure capabilities. Its open-source foundation, extensible design, and proven use in academic, research, and operational settings make it an ideal solution for users who require rapid innovation, interoperability, and real-world applicability across ISR, EW, and cyber domains.

2. PROBLEM STATEMENT

Spectrum operations are essential for reconnaissance, ISR, and countermeasure development. They rely on the ability to detect transmissions, capture traffic, analyze behavior, and build knowledge of both known and unknown devices. This understanding is critical for identifying new emitters, assessing capabilities, and anticipating potential threats.

Although advanced systems exist, they are often expensive, closed, and available only to specialized organizations. These tools provide strong capabilities but remain inaccessible to most researchers, trainers, and smaller operational teams. Outside of these environments, communities are left with fragmented or single-use tools that do not transition easily into practice. The sensitive nature of spectrum operations further limits collaboration, slowing progress in understanding new devices and behaviors.

As a result, many groups reinvent the same skills and build narrow solutions in isolation. Capabilities are duplicated across organizations, and knowledge is seldom shared or extended. The field has produced countless variations of the same tools, but little that is open, modular, and reusable.

At the same time, the economics of defense and security are shifting. Government spending increasingly emphasizes efficiency and low-cost solutions, while adversaries prove that inexpensive, distributed hardware combined with flexible software can deliver real operational effects. Future conflicts will rely not only on large, fixed systems but also on small, adaptable, and distributed capabilities that can be deployed quickly and scaled affordably.

This creates a persistent gap between what is possible and what is available. Many organizations cannot afford or access advanced proprietary systems, yet they still face the challenge of detecting activity, logging communications, and identifying patterns in a rapidly changing spectrum environment. Without accessible and adaptable tools built on affordable and distributed hardware, it remains difficult to build skills, explore new signals, or prepare for emerging threats.

3. CURRENT STATE OF PRACTICE

A wide range of tools exist for spectrum monitoring, RF analysis, and electronic warfare experimentation. Open-source ecosystems such as GNU Radio, Scapy, and Wireshark provide powerful building blocks for signal processing and protocol inspection. Commercial SDR vendors supply their own software suites optimized for specific hardware. At the other end of the spectrum, government and defense programs field large proprietary systems that integrate multiple sensing domains with advanced analytics.

These approaches each have value, but they remain fragmented. Open-source tools are flexible and inexpensive, yet they often require deep expertise and extensive customization to move beyond lab use. Vendor-provided software is tightly coupled to hardware, which limits portability and integration. Proprietary defense systems can deliver strong capabilities but are costly, slow to adapt, and generally unavailable outside specialized organizations.

As a result, users face several persistent challenges:

- Integration gaps across tools and platforms
- Limited adaptability when new signals or tactics emerge
- Barriers to entry for smaller teams and training environments

- Lack of continuity between research, education, and operational use

Despite these efforts, no framework today combines open accessibility, modular extensibility, and operational applicability. The landscape is rich in individual tools but lacks a unified system that lowers the barrier to entry while remaining capable of scaling into real deployments.

4. SOLUTION: FISSURE FRAMEWORK

FISSURE is an open-source, modular framework for RF analysis, electronic warfare, and cyber experimentation. It combines COTS hardware, software-defined radios, and a flexible plugin-based architecture to create a system that can scale from a single laptop to distributed networks of coordinated sensor nodes.

The framework provides a comprehensive set of capabilities. It supports RF reverse engineering, signal conditioning and feature extraction, protocol analysis, packet crafting, fuzzing, and vulnerability exploration. Users can capture and archive signals, build protocol libraries, and generate datasets for machine learning and AI-driven classification. FISSURE enables data logging, storage, and retrieval through integrated database support, creating a foundation for both real-time operations and long-term analysis.

FISSURE extends beyond research and analysis into deployment. Remote sensor nodes can operate with low-throughput networking such as Meshtastic or with higher-throughput links like Wi-Fi HaLow, making them adaptable to both disconnected and connected environments. Nodes can be packaged as lightweight payloads on drones, installed on vehicles, or deployed as portable kits or fixed stations. Integration with GPS and TAK systems allows FISSURE to feed alerts and sensor outputs directly into common operational tools.

This combination of software flexibility and distributed deployment makes FISSURE a practical bridge between research, training, and operations. It is equally suited for classroom instruction, laboratory experimentation, and real-world missions, providing an accessible yet mission-ready framework for spectrum reconnaissance, ISR, EW, and cyber operations.

5. DEPLOYMENT SCENARIOS

FISSURE's flexibility allows it to support a broad spectrum of research, training, and operational missions. Its modular design and distributed architecture make it suitable for both academic environments and real-world operations.

Training and Education: FISSURE is actively used in universities, senior projects, and hands-on workshops. Its open-source foundation makes it ideal for teaching RF fundamentals, electronic warfare concepts, and cyber operations without requiring costly proprietary systems. The FISSURE Challenge capture-the-flag (CTF) site provides an always-available environment for practicing analysis, exploitation, and problem solving.

Research and Development: Researchers use FISSURE to explore new signal processing algorithms, machine learning models, and multi-sensor fusion approaches. The plugin system makes it simple to test novel ideas in a live environment, while dataset-building tools and AI training pipelines enable rapid iteration on classification and detection techniques.

Operational Sensing: FISSURE supports remote sensor nodes that can be deployed in the field with low-throughput networking via Meshtastic or high-throughput networking via Wi-Fi HaLow or other radios. Nodes can operate autonomously, store data locally, and forward alerts to central hubs or operator dashboards when connectivity is available.

Drone Payloads and Mobile Platforms: FISSURE has been deployed on drone payloads of varying sizes, extending sensing and exploitation capabilities into airborne operations. Its lightweight architecture also supports installation on vehicles, portable kits, or fixed stations.

ISR, EW, and Cyber Effects: Beyond monitoring, FISSURE supports replay, spoofing, protocol disruption, and other exploitation techniques when rules of engagement permit. These capabilities extend its use from passive data collection to active effects that can support ISR missions, cyber assessments, and training exercises.

Integration with Existing Systems: FISSURE integrates with platforms such as GPS, WebTAK, and soon ATAK, enabling sensor data and alerts to feed directly into widely used operational tools. PostgreSQL support allows large datasets to be stored, queried, and analyzed, creating a foundation for fleet-wide sensing or multi-node coordination.

6. KEY BENEFITS

FISSURE provides a set of advantages that distinguish it from both fragmented open-source toolchains and closed proprietary systems:

Open Source and Extensible: Community-driven and fully modifiable, with support for new radios, sensors, detection methods, and countermeasures without vendor lock-in.

Low Cost and Scalable: Runs on COTS hardware and general-purpose computing, reducing entry costs while scaling from a single workstation to distributed multi-node networks.

Dual-Use Value: Equally effective for academic research, workforce training, and operational missions, allowing the same framework to move seamlessly from classroom use to field deployment.

Multi-Sensor, Multi-Domain Support: Integrates RF, acoustic, visual, GPS, and protocol-specific inputs to improve detection accuracy and enable cross-domain fusion.

Flexible Deployment: Operates as a workstation toolkit, portable sensor node, or payload on unmanned systems, supporting a wide range of mission profiles.

Machine Learning Integration: Provides a foundation for protocol discovery, anomaly detection, classification, and large-scale data analysis with custom datasets and feature extraction pipelines.

Artificial Intelligence for Operations: Enables AI-driven workflows, adaptive GUIs, and automated coordination of distributed tactical nodes for smarter and more autonomous spectrum operations.

Robust Data Management: PostgreSQL support for scalable storage and retrieval of datasets, sensor logs, and model outputs across research and operational workflows.

Rapid Adaptation: A plugin architecture that supports rapid integration of new algorithms, effects, or hardware to stay adaptable to emerging needs.

Interoperability with Existing Ecosystems: Integrates with GPS, WebTAK, and ATAK (in development) to fit seamlessly into operational workflows.

7. RELEVANT EXPERIENCE

Assured Information Security (AIS) has its roots in cybersecurity, with decades of experience supporting the Air Force, Department of Defense, and national security missions. The company has built a reputation for expertise in cyber operations, reverse engineering, trusted systems, vulnerability research, and advanced R&D. Its work spans both offensive and defensive domains, combining deep technical skills with applied mission understanding.

FISSURE grew out of this foundation, extending AIS's cyber and reverse engineering expertise into the electromagnetic spectrum. The framework incorporates the same principles of modularity, adaptability, and open experimentation that AIS has applied in cyber contexts, now brought to bear on RF analysis, spectrum monitoring, and electronic warfare. This convergence allows FISSURE to bridge cyber and spectrum operations, supporting missions that demand both technical depth and operational relevance.

The framework has steadily expanded in capability. It now includes signal conditioning, feature extraction, dataset building, AI-driven classification, and PostgreSQL-backed data management. Its plugin architecture enables rapid development of new functions, while distributed deployments have been demonstrated on remote sensor nodes, low- and high-throughput networking links, and drone payloads. These features combine to make FISSURE adaptable to a wide range of operational scenarios.

FISSURE has also been adopted beyond defense organizations. Universities use it in senior projects and coursework, training programs employ it for hands-on learning, and the FISSURE Challenge CTF site provides an always-available environment for practicing analysis and exploitation skills. Documentation and system diagrams support community adoption, while demonstrations and joint research efforts ensure continued growth.

AIS continues to refine FISSURE through internal R&D and external collaboration. This sustained effort reflects both the company's heritage in cybersecurity and its commitment to creating tools that bridge research, training, and operations across cyber and spectrum domains.

8. CONCLUSION

Modern spectrum operations demand tools that are accessible, adaptable, and capable of spanning research, training, and real-world missions. Proprietary systems often remain costly and closed, while fragmented toolchains lack the integration needed to support evolving operational needs.

FISSURE provides a clear alternative. Its open-source foundation, modular design, and distributed architecture give users the ability to experiment, learn, and deploy within a single framework. By supporting RF reverse engineering, spectrum analysis, cyber experimentation, and operational sensing, FISSURE delivers both technical depth and field-ready utility.

Its dual-use nature ensures broad applicability. The same system that supports hands-on education and academic research can also be deployed as a mission-ready capability in operational contexts. This accessibility lowers barriers for new learners while equipping experienced operators with a flexible toolset for ISR, EW, and cyber missions.

Assured Information Security remains committed to advancing FISSURE as a sustainable, scalable solution. Through continual refinement, community engagement, and operational integration, FISSURE stands as a proven foundation for addressing the complexity of modern spectrum operations. It is positioned to remain a cornerstone for spectrum research, training, and operations as future conflicts increasingly demand affordable, distributed, and adaptable capabilities.