FISSURE for Maritime

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

1. EXECUTIVE SUMMARY

The maritime domain presents one of the most challenging environments for spectrum operations. Ships, ports, and coastal regions are saturated with RF activity from radar, Automatic Identification System (AIS), satellite links, and commercial communications, while the ocean itself creates unique propagation effects such as multipath reflections and ducting. Adversaries exploit this complexity by using covert signaling, GPS spoofing, and unconventional RF behaviors to mask their presence or disrupt operations.

Assured Information Security, Inc. (AIS) offers the FISSURE Framework, a modular, open-source system designed for distributed RF and sensor operations in demanding environments like the maritime domain. FISSURE enables customizable sensor nodes that detect, classify, and respond to unconventional signals using commercial off-the-shelf (COTS) hardware and a flexible plugin-based software architecture. It integrates across multiple sensing domains, supports operator-defined behaviors, and is compatible with platforms like the Team Awareness Kit (TAK) for real-time situational awareness.

FISSURE provides a scalable, adaptable foundation for maritime intelligence, surveillance, and reconnaissance (ISR), electronic warfare (EW), and security missions. Its flexible architecture, low deployment overhead, and ability to operate in disconnected environments make it a strong fit for shipboard defense, port security, and distributed fleet operations where adaptability, speed, and integration are critical.

2. PROBLEM STATEMENT

The maritime environment poses unique challenges for sensing, communications, and security. RF signals propagate differently over water, often creating multipath reflections, ducting, and unpredictable interference. Ships and ports are dense with overlapping emissions from radar, AIS, satellite communications, Wi-Fi, and cellular systems. This creates a congested, noisy spectrum where conventional tools struggle to reliably detect or classify unconventional signals.

Adversaries exploit these conditions with tactics such as Global Positioning System (GPS) spoofing, covert communications, or emissions designed to blend into background activity. Small teams can field low-cost systems that leverage non-standard modulation, frequency hopping, or encrypted protocols that evade traditional maritime monitoring solutions. In some cases, hostile actors rely on passive sensors or pre-programmed autonomy, leaving few RF signatures to detect at all.

At sea, operators often lack the benefit of fixed infrastructure or robust backhaul connections. Shipboard crews must rely on systems that can operate autonomously, provide actionable alerts, and adapt to rapidly changing conditions. Traditional maritime security tools such as radar, AIS monitoring, and optical surveillance are valuable but limited when facing unconventional or deceptive signaling methods. Proprietary and monolithic solutions are expensive, slow to update, and often unable to keep pace with emerging threats.

The result is a critical capability gap: a need for tools that are flexible, modular, and capable of operating across domains. These tools must be deployable on ships, ports, and unmanned platforms, able to integrate multiple sensor types, and adaptable enough to respond to unknown or evolving threats without requiring constant backend support or vendor-driven updates.

3. CURRENT STATE OF PRACTICE

Maritime security and spectrum awareness rely on a mix of traditional tools and modern technologies, but most remain fragmented, proprietary, or limited in scope. Shipboard and port defense often depend on radar for surface and air tracking, AIS for vessel identification, and optical or infrared cameras for visual monitoring. While effective for conventional maritime traffic, these systems are less reliable against unconventional signals, covert communications, or spoofing attempts.

Commercial and government solutions exist for maritime domain awareness, including coastal radar networks, satellite-based AIS tracking, and integrated port security suites. However, many of these systems assume predictable vessel behavior and standard signaling. They struggle when faced with non-standard emissions, low-power transmissions, or actors deliberately blending into background traffic. Systems designed for blue water operations may be too expensive or slow to deploy in smaller ports, while port security tools often lack the flexibility to extend coverage offshore.

Proprietary maritime security packages typically require specialized hardware, fixed installations, and vendor support for updates or integration. This limits adaptability and increases costs for both military and commercial users. Even modern “multi-sensor” solutions are often stovepiped, with radar, AIS, and camera inputs processed in isolation rather than fused into a flexible, operator-driven framework.

Several gaps remain consistent across the field:

- Reliance on fixed or proprietary architectures that are costly and hard to update
- Blind spots in detecting non-standard, low-power, or deceptive signals
- Limited interoperability with open tools like TAK or third-party sensor systems

- Dependence on centralized processing and high-bandwidth networks that may not be available at sea

These limitations highlight the need for maritime solutions that are modular, open, and field-adaptable. Operators require systems that work across sensing domains, scale from single ships to distributed fleets, and deliver timely, actionable intelligence without dependence on proprietary vendors or static infrastructure.

4. SOLUTION: FISSURE FRAMEWORK

FISSURE is an open-source, modular framework for distributed RF and sensor operations that addresses the unique challenges of the maritime domain. Instead of relying on fixed, vendor-driven systems, FISSURE enables users to deploy flexible sensor nodes built from COTS hardware and general-purpose computing platforms. These nodes can be configured for shipboard use, integrated into port security infrastructure, or deployed on unmanned platforms such as unmanned surface vehicles (USVs), unmanned aerial vehicles (UAVs), or buoys.

Each FISSURE node runs customizable playlists that define its sensing, analysis, and response actions. Playlists may include RF monitoring, feature extraction, protocol classification, or alerting routines, and can be tailored to mission needs before deployment or updated remotely while underway. This provides operators with the ability to adapt to evolving threats or conditions without requiring major system changes.

FISSURE is designed to support multiple sensing modalities, including:

- RF sensing with software-defined radios (SDRs)
- Protocol-specific detection for common maritime signals such as Wi-Fi, telemetry, AIS-adjacent, or satellite communications (SATCOM) links
- Acoustic and visual inputs for detecting anomalies in the environment
- Integration with radar or electro-optical/infrared (EO/IR) systems where available

Data from these nodes can be stored locally for offline analysis or transmitted back to a central hub (HIPRFISR) for coordination across a fleet or port. The system supports low-throughput communications like LoRa for alerts, as well as higher-bandwidth links such as cellular, SATCOM, or IP networks for bulk data transfer.

FISSURE's plugin architecture enables continuous improvement and rapid integration of new capabilities. Detection algorithms, countermeasures, or sensor types can be added as modular components without altering the core system. This open approach reduces vendor lock-in, lowers cost, and allows operators to share or adapt capabilities across teams.

By combining distributed sensor nodes, multi-domain detection, and a flexible software architecture, FISSURE provides a scalable solution for maritime ISR, EW, and security operations. It offers the adaptability needed for real-world missions, whether on a single vessel, across a port facility, or throughout a distributed fleet.

5. DEPLOYMENT SCENARIOS

FISSURE's flexibility allows it to support a wide range of maritime missions, from commercial port security to fleet operations in contested waters. Its sensor nodes can be adapted for multiple deployment models depending on the mission profile:

Shipboard Defense: Nodes mounted on naval vessels, coast guard cutters, or commercial ships can monitor the spectrum for GPS spoofing, covert communications, or drone activity near critical assets. Nodes operate autonomously when disconnected, providing crews with local alerts and storing data for later analysis.

Port and Coastal Security: FISSURE nodes can be distributed across docks, harbor entrances, or coastal facilities to detect unauthorized transmissions or identify unusual activity within busy RF environments. Integration with AIS and radar systems enhances awareness by combining traditional maritime monitoring with flexible, software-driven detection.

Blue Water ISR: In open-ocean operations, FISSURE nodes deployed on unmanned platforms such as USVs, UAVs, or free-floating buoys extend the sensor perimeter of a fleet. These nodes can collect RF and sensor data, forward alerts over SATCOM or mesh networks, and operate autonomously in denied or low-connectivity environments.

Convoy and Distributed Operations: When deployed across multiple vessels, FISSURE nodes coordinate through HIPRFISR, forming a distributed sensing network that provides a shared picture of the RF environment. This improves resilience against deceptive or low-probability-of-intercept signals by enabling multiple vantage points across a convoy or task group.

Training and Experimentation: Because FISSURE is open and modular, it is well suited for test ranges, training exercises, and rapid prototyping. Operators can use it to simulate adversary signals, evaluate new countermeasure techniques, or rehearse responses to unconventional threats without reliance on proprietary systems.

6. KEY BENEFITS

FISSURE brings several advantages to maritime ISR, EW, and security operations:

Open Source and Extensible: The framework is community-driven and fully modifiable. Operators can add new detection methods, sensors, or countermeasures without vendor lock-in, ensuring adaptability as maritime threats evolve.

Low Cost and Scalable: Nodes are built from COTS hardware and general-purpose computing platforms. This keeps costs low and enables deployment at scale, whether across a port facility or throughout a distributed fleet.

Multi-Sensor, Multi-Domain Support: FISSURE can integrate RF, acoustic, visual, AIS-adjacent, and radar/EO inputs. This layered approach improves detection confidence and reduces blind spots in complex maritime environments.

Flexible Deployment Options: Nodes can be mounted on ships, placed at docks, carried on unmanned surface vessels, or even deployed on buoys. This versatility supports operations in ports, coastal waters, or blue water.

Adaptable to Limited Connectivity: FISSURE nodes can operate autonomously and share alerts over low-throughput links such as LoRa or mesh radios. Larger datasets can be sent when high-bandwidth links like SATCOM or cellular are available.

Plugin-Based Development: New capabilities can be integrated as plugins without modifying the core system. This accelerates

field updates, enables experimentation, and reduces reliance on long vendor timelines.

Interoperability with Common Tools: Alerts and sensor data can be integrated into platforms such as TAK, providing operators with a familiar interface and map-based situational awareness.

Support for ISR, EW, and Cyber Operations: Beyond passive detection, FISSURE supports replay, protocol disruption, deception techniques, and cyber payloads. This allows operators to transition from sensing to active effects when mission rules permit.

7. RELEVANT EXPERIENCE

Assured Information Security has a proven track record in RF systems, electronic warfare, and distributed sensing, with direct experience developing, testing, and integrating technologies across command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance (C5ISR) domains. The FISSURE Framework builds on this foundation, incorporating lessons learned from counter-UAS research, spectrum monitoring, and cyber exploitation into a modular system applicable to maritime operations.

The company has supported projects involving protocol exploitation, GPS manipulation, RF characterization, and multi-sensor fusion in contested environments. The team has developed and demonstrated capabilities ranging from low-level signal analysis to full-spectrum countermeasure execution, many of which are directly applicable to maritime ISR and EW missions.

Assured Information Security has also applied its expertise in maritime contexts. The team has explored buoy-based sensing for AIS and RF logging, integrated open-source navigation tools such as OpenCPN, and participated in events like Cyber Boat to demonstrate cyber resilience in shipboard and port environments. Experience with marine radar, vessel data systems, and other maritime technologies further informs how the FISSURE Framework can extend into shipboard defense, port security, and distributed ocean sensing. These efforts highlight Assured Information Security's ability to adapt proven RF, cyber, and sensor capabilities to the unique challenges of the maritime domain.

The company also operates research and testing facilities that support rapid prototyping, integration, and evaluation. This includes controlled environments for RF experimentation, drone cages, and field sites where distributed sensing architectures have been exercised. These facilities provide a foundation for adapting FISSURE to maritime scenarios such as shipboard defense, port security, and distributed fleet operations.

8. CONCLUSION

The maritime domain demands sensing and security solutions that can adapt to complex environments, unpredictable threats, and limited infrastructure. Traditional systems are often too rigid, expensive, or narrowly focused to meet these challenges.

AIS' FISSURE Framework provides a flexible, modular alternative designed for real-world maritime operations. By supporting distributed sensing, multi-domain inputs, and operator-defined behaviors, FISSURE enables low-cost, field-ready solutions that can detect unconventional signals, adapt to emerging threats, and integrate seamlessly with existing workflows.

Its open-source foundation, plugin-based architecture, and proven adaptability make FISSURE well suited for missions ranging from shipboard defense to port security and distributed fleet ISR. AIS brings the experience and technical expertise to extend these capabilities into operational environments, ensuring that maritime operators have the tools they need to maintain awareness, control, and resilience in contested waters and busy ports alike.