FISSURE for Vehicle & Mobility Systems

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

1. EXECUTIVE SUMMARY

FISSURE enables vehicles to do far more than static monitoring. Teams can sense while driving, transmit while moving between sites, and conduct facility and clandestine monitoring from parked vehicles that blend into normal traffic. Fleets can protect routes and convoys, maintain team awareness over mesh links, and support protected Intelligence, Surveillance, and Reconnaissance (ISR) and cyber workflows within policy. Remote operators at a command center can control nodes on vehicles while drivers focus on driving. Units can perform tracking and pursuit, direction-finding and geolocation with single or multiple vehicles, and wardriving surveys that map infrastructure and detect anomalies.

Mobile operations are underserved by today's fragmented and fixed-site tools. Vehicle missions need one framework that works anywhere for almost anything, across mixed networks and changing contexts. Radio Frequency (RF) sensing, protocol analysis, and effects must survive intermittent links, varied platform roles, and short operator interactions. Single-purpose boxes are hard to extend, and monolithic suites are costly to field broadly. What is required is a flexible, policy-aware approach that adapts to link conditions, preserves provenance, and keeps workflows consistent from the vehicle to the operations center.

Assured Information Security, Inc. (AIS) offers the FISSURE Framework, an open-source and plugin-driven system built on commercial off-the-shelf (COTS) hardware and software-defined radios (SDRs). Vehicle-mounted nodes support on-the-move sensing and effects, shift behaviors with simple triggers, and publish compact messages on low-throughput paths while returning richer outcomes and artifacts on high-throughput Internet Protocol (IP) links. A central hub brokers tasking, records tasks and outcomes with timestamps, identifiers, and Global Positioning System (GPS) context, and publishes to TAK for a shared operational picture.

The result is a low-cost, scalable foundation for vehicle and mobility operations. FISSURE emphasizes interoperability, evidence handling, and policy control rather than hardware lock-in, so teams can start with a single kit and grow to coordinated fleets without rewriting workflows or adopting closed systems.

2. PROBLEM STATEMENT

Vehicle spectrum operations are still improvised. Most teams field people with laptops or pack rack mounts into trucks and Humvees. These builds are bulky, draw from the vehicle's primary electrical system, and sprawl across dashboards and trunks with ad hoc cabling. Each device brings its own interface, data format, and update path, which turns a moving vehicle into a collection of point solutions rather than a coherent capability.

This patchwork creates three persistent problems. First, operators lack a single, predictable way to work. Tasks that should be simple, such as starting a capture or running a quick classification, depend on the exact mix of gear in the vehicle and the person who set it up. There is no shared catalog that tells a mobile user what actions are actually available on that node, what parameters matter, or what task is safe to run while moving or parked.

Second, mobility stresses links and procedures. Connectivity varies by block and by mile, yet most tools assume stable bandwidth and continuous control. When the link drops, task status and evidence are often lost or never recorded in a consistent way. Policy constraints are hard to enforce from a moving platform. Effects that should be gated by location, speed, or operator role are either disabled entirely or left to informal practice, which raises operational and legal risk.

Third, evidence and fleet discipline suffer. Alerts from on-vehicle tools frequently arrive without the timing, location, configuration, and platform state needed for audit and training. Vehicles are hard to keep aligned on versions, playlists, and procedures, so results differ from crew to crew. Remote operators cannot reliably supervise or task what they cannot see, and drivers cannot be expected to manage a different workflow for every box in the car.

In short, the problem is not one missing sensor or radio. It is the lack of a unifying vehicle-ready framework that makes capabilities discoverable, adapts to changing links without losing tasks or evidence, enforces policy while moving, and accepts varied hardware mixes without rewrites so teams can scale from a single car to coordinated fleets.

3. CURRENT STATE OF PRACTICE

Vehicle work typically falls into a few buckets. Ad hoc kits pair a laptop with one or two radios and custom scripts, which depend on the original builder and rarely survive crew changes. Drive-test stacks from the telecom world map cellular coverage well, but they stay inside narrow protocol lanes and do not mix general RF sensing, protocol analysis, and effects. Spectrum monitoring and direction-finding packages localize emitters effectively, but they are proprietary, costly across fleets, and optimized for detection rather than evidence handling and policy controls. Rapid-response vehicle kits adapt fixed systems into rooftop boxes for events or convoys, with curated features and limited integration.

Across these approaches, the same gaps recur: multiple dashboards, duplicated training, weak provenance, uneven policy enforcement while moving, and an assumption of stable backhaul. Capabilities are not discoverable to the operator in a consistent way, task status is fragile when links drop, and artifacts are hard to review later.

FISSURE's point of departure is a single framework that travels with the vehicle and the mission, presents a plugin-driven catalog to the operator, tolerates intermittent links, and captures provenance by default.

4. SOLUTION: FISSURE FRAMEWORK

FISSURE is an open-source and plugin-driven framework built on commercial off-the-shelf hardware and software-defined radios. In vehicles, it can run entirely on a laptop with the Dashboard graphical user interface for customizing scripts and building playlists, or extend to remote operations with a central hub coordinating tactical nodes across multiple locations. Each node can also operate autonomously to execute preset actions or switch between modes of operation as configured.

Operator workflow is catalog-driven in the Dashboard. Plugins contribute techniques and variants for existing actions, and ad hoc scripts can be wrapped into playlists to keep use consistent. The catalog lists actions with their parameters, so operators can start a capture, run a quick classification, inspect a protocol, replay a focused sample, or perform other policy-approved effects. Playlists set defaults and add triggers that switch modes or start tasks when conditions are met.

Crews can operate over low-throughput links for simple commands and alerts, or use higher-throughput paths to move larger artifacts and stream data when available. Link behavior is configuration-driven. When an adequate network backhaul connection exists (cellular, mesh), results and markers may publish to TAK so operations centers, patrols, and partner units share a consistent picture.

Evidence handling is straightforward and transparent. Tasks write artifacts and logs locally with timestamps and identifiers for later export, review, or packaging for after-action use. Teams decide when and how to move those files to other stores or systems without changing the in-vehicle workflow. FISSURE provides a clear way to encode policy and permissions in named actions, standardizes messages across tasks and nodes, and interoperates with other solutions when connectivity and workflows require it.

5. DEPLOYMENT SCENARIOS

FISSURE gives vehicles flexible roles that can be retasked in minutes, mixing sensing, protocol analysis, and permitted effects whether moving or parked. The scenarios below show how one framework supports patrol, convoy protection, pursuit and geolocation, facility monitoring, pop-up perimeters, and wide-area surveys.

Patrol and Interdiction: A single cruiser runs a lightweight node for on-the-move detection of rogue access points, brief control-channel bursts, or GPS anomalies. Alerts appear in TAK with abbreviated status, and artifacts are written locally for export at the station or over a reliable link.

Convoy Protection: Multiple vehicles coordinate through a central hub to watch for telemetry links and non-standard emissions along a route. One node maintains wide watch while another performs targeted verification. Evidence is kept on each vehicle and transferred when connectivity is available.

Tracking, Pursuit, and Geolocation: One or more vehicles track a target signal, using coordinated tasking to tighten geolocation and pursue across city blocks or rural roads. Results are shared via TAK and stored locally for later reconstruction.

Facility and Clandestine Monitoring: Vehicles park near buildings to observe local infrastructure, log protocol behavior, and evaluate protections without drawing attention. Operators search for anomalies and suspicious behavior, then package artifacts for offline analysis.

Pop-Up Perimeter from a Parked Vehicle: A parked unit establishes a temporary perimeter at an incident scene or checkpoint, cross-cueing nearby cameras and routing alerts to TAK. When the scene ends, operators export bulk data and return the node to patrol mode.

Route Reconnaissance and Survey: Utility or military survey vehicles log band activity, cellular anomalies, and protocol beacons along planned waypoints. Results support wardriving-style maps that correlate detections with terrain, coverage, and infrastructure.

Surveying and Mapping: Teams conduct wide-area surveys to baseline spectrum use, map cellular behavior, and document protocol presence. Collected data supports change detection, route planning, and future incident response.

Disaster Response and Disconnected Operations: Command vans act as rolling coordination points for mesh-connected rovers. Nodes prioritize compact alerts on low-throughput links, then stream larger datasets when cellular or satellite communications links are available.

Brick-in-Vehicle Deployments: Self-contained "brick" nodes ride in vehicles as unattended sensors. They execute preset actions or switch modes on schedule, and crews retrieve logs and artifacts periodically or when a link is available.

Campus and Corporate Mobility: Security vehicles extend fixed coverage with on-demand verification. Operators receive geofenced alerts, trigger short captures, and coordinate with an operations center using the same tasking and evidence patterns.

Transit and Rail Police: Vehicle kits monitor platforms and yards during movements, correlating brief RF activity with time and location. Alerts route to TAK for joint action with fixed cameras or access control systems.

Border, Pipeline, and Utility Corridors: Trucks with weatherized kits patrol remote lines, forwarding concise alerts over mesh when backhaul is limited. Larger artifacts transfer at depots or when reliable connectivity returns.

6. KEY BENEFITS

FISSURE delivers practical advantages for vehicle operations without locking teams into a single hardware pattern.

Flexible Vehicle Deployment: Run on a laptop, compact brick, or single-board computer with peripherals, and optionally coordinate through a central hub.

Catalog-Driven Operator Workflow: Plugins and playlists present a clear action catalog with parameters for repeatable tasking.

Policy and Permissions: Encode allowable effects and defaults as named actions to keep tasks within policy.

Configurable Networking: Use low-throughput links for commands and alerts or higher-throughput paths for bulk data; publish to TAK when backhaul is available.

Evidence and Provenance: Tasks write artifacts and logs locally with timestamps and identifiers for export and review.

Open-Source and Plugin-Driven: Extend techniques without rewriting workflows, and incorporate ad hoc scripts into playlists.

Interoperability: Standardized messages support integration with TAK, a central hub, and partner systems.

Scales from Single Vehicle to Fleets: Start with one car and grow to coordinated deployments without adopting closed suites.

7. RELEVANT EXPERIENCE

AIS brings deep experience in RF, electronic warfare, and cyber operations across classrooms, laboratories, field demonstrations, and joint events. In the automotive sector, our teams have taught RF attack courses and hands-on labs for automotive security, cellular systems, and telematics, and we conduct vehicle testing and red teaming at the ORION technology accelerator in Rome, New York. ORION provides RF-safe lab space, controlled test areas, and vehicle bays that support protocol analysis, exploitation technique development, and realistic evaluation. These skills translate directly to mobile use in ground vehicles.

To date, FISSURE has been exercised primarily on drone payloads and in fixed or portable setups, where plugin-based techniques and playlists are used for sensing, protocol inspection, classification, and effects within policy. Radios and sensors have been integrated manually, outputs have been logged to local files for packaging and review, and, when adequate backhaul was available, results have been published to TAK. In demonstrations, a central hub has coordinated tasking across distributed nodes. Combined with our automotive training and assessment background, these patterns inform how we structure plugin catalogs, playlists, and operator workflows for vehicle scenarios even before dedicated in-vehicle kits are fielded.

8. CONCLUSION

Vehicle and mobility missions need a flexible way to sense, analyze, and act while staying within policy and keeping results reviewable. Fixed appliances and closed suites struggle to keep pace, and ad hoc builds are hard to maintain across crews and vehicles. Teams need one framework that fits their existing gear, keeps operator tasks consistent, and scales without vendor lock-in.

FISSURE meets that need. It is open-source, plugin-driven, and built on commercial off-the-shelf hardware and software-defined radios. In vehicles, it can run entirely on a laptop with the Dashboard graphical user interface or extend to remote operations through a central hub that coordinates tactical nodes across multiple locations. When backhaul is available, outputs may publish to TAK for a shared picture. Evidence is written to local files with timestamps and identifiers, and policy and permissions are encoded as named actions so mobile tasks align with mission rules.

Adoption can start with a single vehicle and grow to small fleets. The same plugins and playlists used at fixed sites and on aerial payloads carry over to mobile use, which reduces training time and avoids one-off workflows. As missions evolve, teams add techniques through plugins and refine playlists rather than replacing systems. The result is a practical foundation for vehicle and mobility operations that emphasizes interoperability, consistent operator experience, and clear provenance without forcing a single hardware pattern.