LOCH TECHNOLOGIES

AirShield

WIRELESS AIRSPACE DEFENSE FOR ICS / OT

The air gap is gone. **See your plant's airspace.**

Use Case · Industrial Control Systems and Operational Technology

Software-Defined RF Sensor · 300 MHz – 6 GHz · Zero Trust for the Airspace



WI-FI | BLUETOOTH | CELLULAR | IoT / LPWAN | GPS / GNSS | DRONES

LOCH TECHNOLOGIES

www.loch.io

The plant floor went wireless, and wired OT security cannot see it.

The ICS/OT Wireless Problem

Sensors report over WirelessHART and LoRaWAN, remote sites backhaul over LTE, substations take their time from GPS, and technicians configure equipment over Bluetooth. None of that traffic crosses a firewall or a span port.

80%
of new IIoT deployments connect wirelessly

230×
rise in wireless vulnerabilities disclosed per year since 2010

20×
faster growth than software vulnerabilities overall

2.5 / day
new wireless CVEs published during 2025

CVE figures: NIST National Vulnerability Database analysis, 2010–2025 · IIoT figure: LOCH Technologies

Why wired OT defenses miss it

- **Wireless is in the control loop.** RTUs sit miles away, and radio is often the only practical link.
- **Every radio bypasses the Purdue model.** A vendor modem or hotspot links control assets straight to the outside.
- **One flaw, many vendors.** A bug in a shared wireless chipset exposes a whole device class.
- **No IP address, no visibility.** Deep packet inspection only sees devices on a monitored switch.
- **Unpatchable for years.** Uptime and safety come first, so controllers run with known flaws.
- **Proximity is the only credential.** The parking lot, the fence line or a drone overhead is close enough.



The cost of inaction

01 **Unplanned downtime** from jamming, interference or a compromised wireless link.

02 **Safety incidents** when process data or timing is manipulated.

03 **Audit findings and penalties** for an incomplete asset inventory.

04 **Theft of process data** over channels nobody is monitoring.

05 **No forensic record** to explain what happened, when, or from where.

Why ICS/OT operators need Wireless Airspace Defense.

Wireless paths reach the control layers without crossing the firewall

Levels 4-5	Enterprise network	
Level 3.5	**Industrial DMZ and firewalls**	Firewalls and wired OT monitoring only see traffic that crosses here
Level 3	Site operations and historian	Rogue AP or contractor hotspot
Level 2	Supervisory control: HMI, SCADA	Wi-Fi or Bluetooth on an HMI
Level 1	Basic control: PLC, RTU, DCS	Vendor cellular modem
Level 0	Process: sensors and actuators	Rogue 802.15.4 or LoRa node

Orange paths never pass a firewall rule or a span port. Only RF sensing sees them.

01 **You cannot defend what you do not know**
Every OT framework starts with asset inventory. One that stops at the wire misses the devices most likely to be unmanaged.

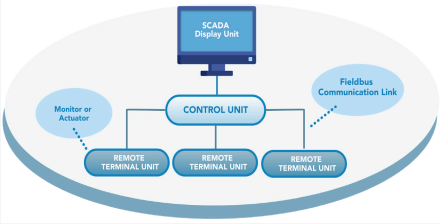
02 **Compliance already expects it**
NERC CIP, IEC 62443, NIST SP 800-82 and TSA pipeline directives require asset identification, access control and continuous monitoring.

03 **Threats arrive on every band**
GPS spoofing, rogue cell towers, planted Bluetooth devices and RF jamming sit outside what Wi-Fi intrusion detection can see.

04 **OT cannot tolerate active scanning**
Fragile controllers need monitoring that never transmits to them. Passive RF sensing is that method.

05 **Remote sites have the least protection**
Substations, pump stations and well pads depend on wireless and have nobody on site to notice an intruder or a drone.

06 **Detection has to come before the wire**
Seeing an attack at the radio layer gives early warning, before it reaches a controller or a historian.



Radio is already in the control loop

In a SCADA system, remote terminal units may sit in the next room or hundreds of miles from the control unit. Radio is often the only viable link, so the wireless path is part of the process itself.

Ten ways AirShield protects the plant you cannot see.

A software-defined RF sensor passively monitors 300 MHz to 6 GHz and reports to a single LOCH console, in the cloud or on-premises.

Complete wireless inventory

Discovers every RF-emitting device, on or off your network. Closes the gap between the CMDB and the plant.

Zero impact on operations

Passive monitoring: no agents, no network changes and no packets sent to fragile controllers or safety systems.

Risk you can rank

Each device is fingerprinted, typed, given a trust level and a risk score, so engineers fix the worst exposures first.

Real-time threat detection

Wireless intrusion detection and behavioral analytics flag violations before an attack reaches the process network.

GPS integrity

GPS Canary detects jamming, spoofing and meaconing, protecting the timing that grid and SCADA systems rely on.

Cellular assurance

AirCell scores every tower across LTE, CBRS and 5G, exposing rogue towers and protecting private cellular networks.

A compensating control

Continuous monitoring of long-lived devices that cannot be patched reduces risk without a maintenance outage.

Find it and fix it

The Threat Hunting app locates devices to within 1 inch. AirTerminate breaks unacceptable connections.

Audit-grade evidence

Historical playback, incident tracking, daily alerts and summary reports give auditors proof and investigators a timeline.

Fits the OT stack, deploys anywhere

SIEM, SOAR, ITSM, CMDB and NAC integrations. PoE or LTE backhaul, with on-prem hosting for restricted networks.

One sensor, the whole spectrum

Most wireless security stops at Wi-Fi. AirShield listens from 300 MHz to 6 GHz.

300 MHz	600 MHz	900 MHz	1.5 GHz	2.4 GHz	3.5 GHz	5 GHz	6 GHz
LPWAN	LTE	Z-Wave LoRa	GPS L1	Wi-Fi BT	CBRS	Wi-Fi	5G

You can't defend what you don't know, and you can't certify it either.

Use Case 1: Compliance ASSET INVENTORY · AUDIT READINESS

An energy operator's asset inventory comes from its wired OT monitoring platform. It says nothing about the radios inside the electronic security perimeter: vendor cellular modems, Wi-Fi-enabled HMIs, Bluetooth dongles and contractor hotspots. Auditors ask how the operator knows there are no unauthorized access paths. Without wireless visibility, there is no evidence-based answer.

WITHOUT AIRSHIELD

Inventory stops at the wire. Wireless assets are found by walk-downs, if at all.

Wireless policy exists on paper with no proof it is enforced.

Transient and vendor devices pass through unrecorded.

Audit evidence is assembled by hand before each review.

WITH AIRSHIELD

Every RF-emitting device is discovered, classified and risk-scored continuously.

Trust-level policies alert on violations in real time, with full history.

Each device is logged with first seen, last seen and location.

Daily summaries and historical playback produce evidence on demand.

How AirShield maps to what OT frameworks ask for

Requirement	Where it appears	AirShield capability
Asset inventory	NERC CIP-002, IEC 62443, NIST SP 800-82	Passive discovery of every wireless device
Perimeter access paths	NERC CIP-005, IEC 62443-3-3 SR 1.6, SR 2.2	Rogue AP and cellular backdoor detection
Transient devices	NERC CIP-010	Alerts on unknown devices in restricted zones
Continuous monitoring	NIST SP 800-82, TSA pipeline directives	Always-on RF monitoring, 300 MHz to 6 GHz
Incident response	NERC CIP-008, IEC 62443	Forensic playback, SIEM and SOAR integration

Legacy tools

Wired OT monitoring and Wi-Fi-only intrusion detection cannot inventory cellular, Bluetooth or 802.15.4 devices.

The outcome

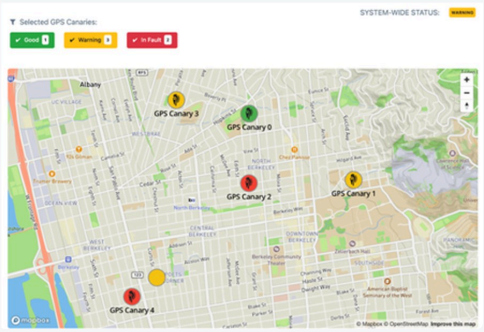
A complete, current wireless inventory and a record showing wireless policy is enforced every day.

Five wireless ecosystems run the plant. Most sites monitor one.

Use Case 2: Wireless Risk and Threat FULL-SPECTRUM VISIBILITY

A manufacturing and process facility's Wi-Fi controller reports on Wi-Fi. Nothing reports on the GPS signal that disciplines its clocks, the 802.15.4 mesh carrying instrument data, the cellular links to remote assets, or the Bluetooth radios in handhelds. An attacker only needs the weakest of the five.

PROTOCOL	THE THREAT IN OT	WHAT AIRSHIELD SEES
GPS / GNSS	Jamming, spoofing and meaconing shift the time behind grid protection and SCADA event logs.	GPS Canary flags signal loss, lost lock and shifts in position or clock.
IoT / LPWAN	Rogue nodes and hijacked relays on WirelessHART, ISA100.11a, Zigbee and LoRaWAN.	802.15.4, Zigbee, Z-Wave and LPWAN networks mapped node by node, with risk scores.
Cellular	IMSI catchers, fake base stations and vendor modems that bridge the perimeter.	AirCell rates every tower known, unknown or suspicious by carrier, band and tower ID.
Wi-Fi	Rogue APs, evil twins, deauth floods and devices left on default configuration.	Rogue and misconfigured devices, plus the trusted clients that connected to them.
Bluetooth	Planted trackers, keyloggers and covert data channels near handhelds and sensors.	Every Bluetooth and BLE emitter, with unauthorized devices flagged and located.



GPS Canary health by location

Legacy tools

Wi-Fi intrusion detection relies on MAC-based identification and has no view of GPS, cellular, Bluetooth or non-Wi-Fi IoT protocols.

The outcome

One risk-ranked picture of the plant's wireless exposure, and early warning of threats that would otherwise surface as unexplained downtime.

A drone is rarely the whole attack. It delivers a wireless one.

Use Case 3: One Platform

SIGNAL INTELLIGENCE · DRONE DETECTION

A utility runs substations, pump stations and pipeline facilities over a wide area, most of them unattended. Drones can survey these sites, carry a rogue access point over the fence, or threaten equipment directly. Cameras watch the ground and cyber tools watch the wire. Nobody connects a drone overhead with the new wireless device that appears a minute later.



WITHOUT AIRSHIELD

No awareness of drones approaching or loitering over critical assets.

Separate tools for drones, Wi-Fi, cellular and GPS, each with its own alerts.

Cyber and physical security teams work from different data.

Remote sites depend on periodic visits and sweeps.

WITH AIRSHIELD

SDR-based detection identifies and geolocates unauthorized drones.

One console places drone activity beside Wi-Fi, Bluetooth, IoT, cellular and GPS findings.

A shared RF baseline for each site, with alerts on any change.

Continuous monitoring over PoE or LTE backhaul, with no staff on site.

Why one platform

With one sensor and one timeline, analysts link the aircraft, the device it carried and the connection it attempted.

Legacy tools

Wireless IDS has no drone detection. Stand-alone drone systems have no view of wireless threats inside the fence.

The outcome

One platform covers the airspace above the facility and the spectrum inside it, for cyber and physical teams alike.

The threat of wireless compromise is invisible, but very real.

Summary: The Cost of Staying Blind

CAPABILITY	LOCH AIRSHIELD	WIRED OT MONITORING AND WI-FI WIDS
Protocol coverage	Wi-Fi, Bluetooth, LTE/5G, CBRS, 802.15.4, LPWAN, GPS	Wired protocols and Wi-Fi only
Wireless asset inventory	Every RF emitter, on or off the network	Only devices on a monitored network
Impact on the process	None. Fully passive	Varies. Active scans can disrupt controllers
GPS jamming and spoofing	Included	Not supported
Rogue cell tower detection	Included	Not supported
Drone detection	Included, in the same console	Separate system or none
Device location	To within 1 inch	Not available
Audit evidence	Continuous logs, playback and reports	Manual and partial
Single pane of glass	Yes	No. Multiple tools required

Industrial operators have invested heavily in securing the wired plant. The wireless plant grew up beside it, unmonitored. One passive sensor and one console deliver the inventory compliance demands, visibility across GPS, IoT, cellular, Wi-Fi and Bluetooth, and a single platform for signal intelligence and drone detection.



10.2 × 10.2 in · PoE powered

AirShield at a glance

Frequency	300 MHz – 6 GHz
Coverage	25,000+ sq ft per sensor
Backhaul	GbE PoE · LTE optional
Hosting	LOCH Cloud or on-prem

See your airspace

www.loch.io

info@loch.io

1-888-725-9434