beechat

KAONIC 1S

Build the edge. Own the mission.

ITAR-free
NDAA-compliant

Executive Summary

Beechat Network Systems is a leading developer of zero-trust, low-SWaP radios, secure NFC tags, and mesh firmware stacks for military, defence, and security applications. Our hardware-first solutions combine open-source transparency with production-grade reliability, engineered to operate off-grid in austere, contested environments and regions without infrastructure.

The Kaonic 1S is our flagship tactical MIMO SDR platform, scalable from individual units to national networks. Designed and manufactured in Europe with NDAA-compliant sourcing, it meets MIL-STD-461 EMI standards and integrates seamlessly with ATAK, MAVLink, and open protocols.

The Problem Space

Modern tactical, defence, and unmanned operations require secure, resilient communications that operate independently of fixed infrastructure. Legacy systems often rely on GPS, master nodes, or centralised servers — creating vulnerabilities when facing jamming, interception, or infrastructure loss. In contested or denied environments, these dependencies can lead to communication breakdowns at critical moments.

The Kaonic 1S Solution

The Kaonic 1S is a rugged, embedded Linux-based tactical radio built for secure, decentralised mesh networking. It combines dual-transceiver, frequency-agile MIMO radios with advanced cryptographic protocols, allowing operation across sub-GHz and 2.4 GHz bands. Running the Reticulum mesh protocol, it supports up to 128 hops with full end-to-end, post-quantum-ready encryption.

The modular design of the Kaonic establishes it as a field-ready device, while also allowing for flexible OEM integration with custom expansions:

- AI/ML edge processing with the VANTAGE plugin
- Advanced MIMO configurations with the Spartan7 FPGA plugin

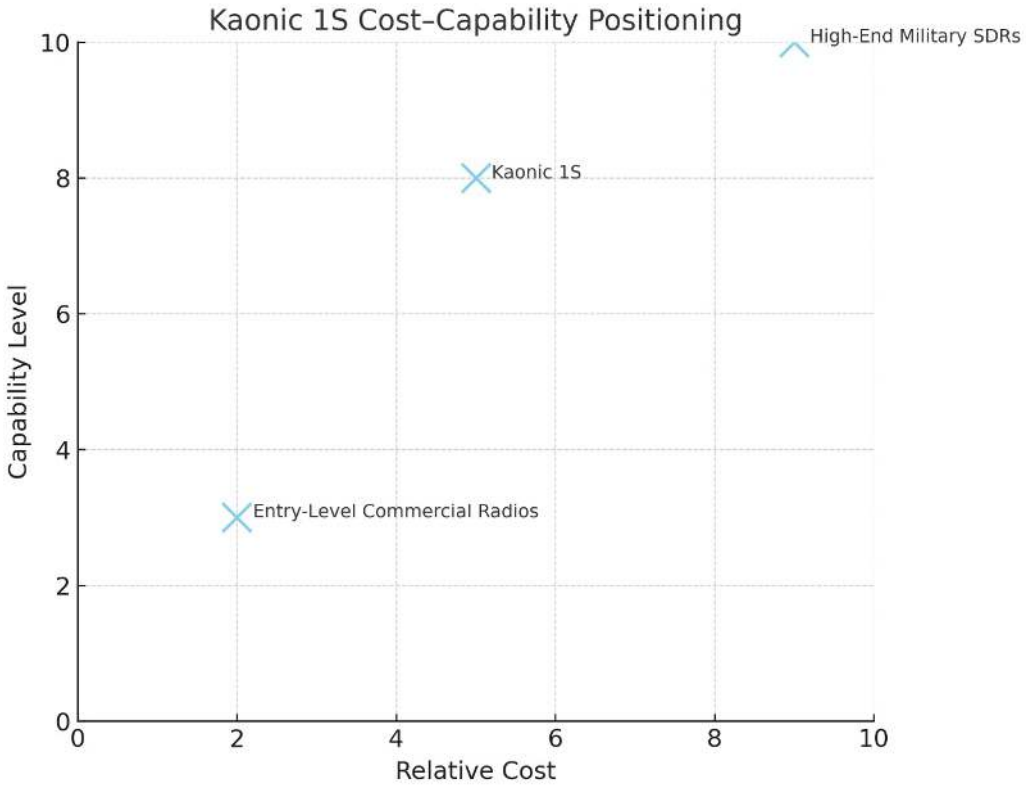
The result is a sovereign, flexible communications platform designed to endure and adapt in the harshest conditions.

Business Value & Use Cases

The Kaonic 1S delivers value as both a **field-ready tactical communications device** and as a **modular OEM component** for integration into larger platforms. Its combination of ruggedised hardware, advanced mesh networking, and modular expansion options enables deployment across defence, security, industrial, and humanitarian sectors. Whether deployed as a complete unit or embedded into third-party systems, Kaonic provides secure, resilient communications in environments where traditional infrastructure cannot be relied upon.

Key Business Benefits

- **Resilient & Infrastructure-Free** – Maintains communications in disconnected or denied environments using Reticulum mesh networking & HopSync frequency modulation
- **Stealth & Anti-Jamming Capability** – HopSync frequency-hopping for low probability of detection/interception and adaptive interference resistance
- **Secure by Design** – Post-quantum-ready encryption, secure boot, signed OTA updates, no central servers, tamper detection
- **Scalable & Flexible** – Multi-band operation, modular plugins to meet emerging challenges, sets the performance standard with 128 hops
- **Open & Sovereign** – ITAR-free, NDAA-compliant, European manufacturing
- **Low Power & Rugged** – Operates in harsh environments with minimal draw and IP67 ruggedisation
- **Dual-Market Capability** – Equally suited for intuitive field use and OEM integration
- **Cost-Effective Performance** – Delivers high-end capabilities without the cost burden of traditional military SDRs
- **High Throughput & Low Latency** – Spartan-7 FPGA MIMO PHY delivering up to 16 Mbps with advanced error correction and spatial multiplexing



Field-Ready Device Use Cases

- **Special Operations & Reconnaissance** – Stealth communications in GPS-denied or jammed areas using HopSync for low probability of detection/interception, with seamless ATAK integration for situational awareness in contested zones
- **Multi-UAV & Drone Swarm Operations** – Secure, resilient mesh control for coordinated ISR missions; MAVLink over mesh for beyond-line-of-sight operations without LTE or satellite dependency; linking air, ground, and maritime drones in one network
- **Border Security & Coastal Surveillance** – Linking patrols, fixed sensors, and UAVs to create continuous situational awareness without infrastructure; suited for coast guards and border agencies
- **Maritime & Offshore Operations** – Ship-to-ship and ship-to-shore communications independent of satellite; supports offshore energy platforms, fisheries protection, anti-piracy, and maritime SAR
- **Law Enforcement & Public Safety** – Secure comms for tactical police operations, counter-narcotics, crowd control, and covert surveillance; direct compatibility with TAK-based systems

- **Event, Expedition & Media Operations** – Rapidly deployable wide-area mesh for races, rallies, expeditions, or remote filming with minimal setup
- **Critical Infrastructure Protection** – Linking unmanned sensors, drones, and patrols for monitoring energy plants, railways, telecom sites, and pipelines
- **Emergency & Disaster Response** – Establishing instant mesh communications for coordination between agencies, NGOs, and volunteers when infrastructure is damaged or destroyed
- **Edge AI & Autonomous Systems** – Using the VANTAGE plugin for real-time AI-based perimeter monitoring, search-and-rescue, autonomous ISR, and threat detection

OEM Component Integration Use Cases

- **UAV Manufacturers** – Embedding Kaonic as a secure, long-range mesh module for air-to-air & air-to-ground
- **Drone Swarm Integrators** – Embedding Kaonic as the secure mesh backbone for coordinated swarm operations, enabling resilient beyond-line-of-sight control and real-time situational awareness
- **UGV & Robotics Platforms** – Integrating Kaonic into ground robots for remote operations in hazardous or GPS-denied areas
- **Maritime Systems** – Incorporating Kaonic into vessels, buoys, and offshore systems for persistent, infrastructure-free communications
- **Sensor Networks** – Deploying Kaonic as the mesh backbone for distributed, autonomous sensing systems in defence, industrial, or environmental monitoring roles
- **Industrial & Security OEMs** – Adding Kaonic modules to existing products to extend secure, decentralised communication capabilities without redesigning the entire system

Architecture

Hardware Layer

• Kaonic 1S Board – STM32MP1 MPU, Yocto Linux, dual RF front-ends for up to 4.8 Mbps (expandable to 14.4 Mbps with FPGA plugin), 868 MHz / 902–928 MHz sub-GHz + 2.4 GHz

• Kaonic VANTAGE Plugin – AI/ML co-processor (NXP i.MX8M Plus, 2.3 TOPS NPU) for edge inference, H.265/H.264 encoding, mesh-based visual telemetry, OTA model updates, MAVLink & ATAK integration

• Kaonic SPARTAN-7 FPGA Plugin – Implements advanced MIMO PHY with LDPC error correction, MMSE equalisation, and spatial multiplexing for increased link throughput, range, and resilience in high-interference environments

• Antennas – Four u.FL ports + integrated 2.4 GHz antennas

• IP67 Rugged Enclosure – Honeycomb shock protection, dust/moisture sealing, weatherproof, dual-antenna support

Software Layer

Core Networking & Communication:

• Reticulum-rs – Rust implementation of the Reticulum mesh networking protocol, enabling cryptographic, decentralised, resilient communications
• kaonic-comm – System-level program orchestrating connections, managing sessions, and coordinating routing
• kaonic-rfnet – Base layer of the Kaonic mesh network, handling peer-to-peer connectivity and link establishment
• kaonic-rf215 – Driver for AT86RF215 transceivers
• rns-tun-rs – IP tunnelling over the Reticulum mesh
• HopSync – Patent-pending, stateless frequency-hopping protocol with zero sync overhead, LPI/LPD stealth, high-speed hopping, adaptive anti-jamming, scalable to hundreds of nodes

Device OS & Firmware:

• kaonic-yocto – Custom Yocto Linux for Kaonic hardware

Applications & Interfaces:

• kaonic-android – Android integration for chat, file transfer, and audio calls
• kaonic-app-flutter – Cross-platform app for configuration and testing

Data & Connectivity Flow

Data from sensors, devices, or operator inputs enters the Kaonic 1S via antennas or expansion modules. It is processed on the STM32MP1 MPU running Yocto Linux and the Reticulum mesh stack, routed via RF modules using HopSync frequency hopping. Data can be transmitted across the mesh, tunnelled to the internet, or sent directly to connected field devices, mobile applications, or cloud systems.

Technical Specifications

Specification	Details
Processing & OS	Dual-core STM32MP1, Yocto Linux
Radios	Dual sub-GHz (868/902–928 MHz), dual u.FL ports; 2.4 GHz internal antennas
MIMO PHY	Spartan-7 FPGA, open-source PHY, LDPC, MMSE, 2×2
Mesh Protocol	Reticulum, 128 hops, encrypted, post-quantum ready
Throughput	Up to 9.2 Mbps at 2x2 MIMO via FPGA, –92 dBm + 2.4 Mbps SISO x 2 = 14.4 Mbps
Max Rx Sensitivity	–123 dBm

Power Consumption	~1.3 W RX, ~11.3 W TX
Transmit Power	Max 1 W EIRP (sub-GHz), 250 mW (2.4 GHz)
Security Features	Secure boot, HW crypto accel., signed OTA, HopSync
Interface & Protocols	MAVLink, ATAK, USB-C PD, CI/CD OTA updates
Environmental	–40 °C to +85 °C, MIL-STD-461 EMI, optional IP67 case
Weight (board only)	84 grams
Dimensions	120 × 60 × 6.7 mm
Manufacturing & Compliance	UK/EU, ITAR-free, NDAA-compliant

Build the edge. Own the mission.

Contact our team to request a technical brief, secure demo units, or discuss your operational requirements.

Email: sales@beechat.network | Website: beechat.network