beechat

Kaonic 1S Datasheet

Zero-Trust Tactical Mesh Radio Platform

Document Title: Kaonic 1S Datasheet			
Document ID: 17022026			
Date: 17/02/2026			
Confidentiality:	☑ Public	☐ Internal	☐ Confidential

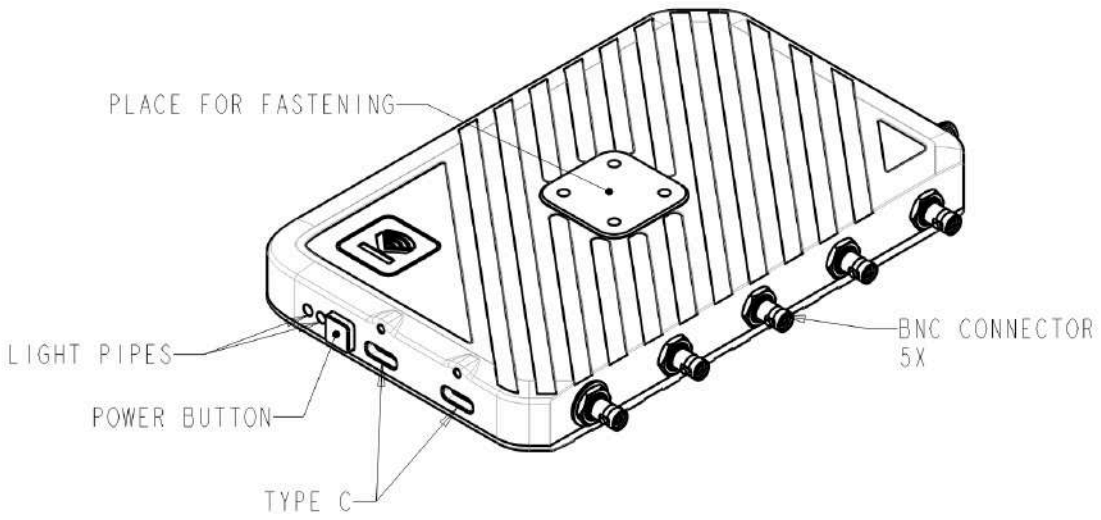


Table of Contents

Executive Summary

The Kaonic 1S is a European-built, NDAA-compliant tactical Software-Defined Radio platform engineered for resilient, infrastructure-free communications in contested environments. Built around dual AT86RF215 transceivers and the STM32MP1 SoC, it delivers secure, decentralised mesh networking with native support for TAK, MAVLink, and open protocols.

At its core, Kaonic 1S is designed around a zero-trust, cryptographic mesh architecture in which every node operates with identity-native encryption and authentication. The platform supports up to 128 encrypted mesh hops, enabling large-scale, infrastructure-free deployments across dynamic operational environments. Simultaneous dual-band operation across sub-GHz 862 to 928 MHz and 2.4 GHz bands provides flexibility, range, and resilience under varying spectrum conditions.

An open-source PHY implementation on a modular FPGA enables optional MIMO capability and customizable waveforms, giving integrators control over performance characteristics without dependence on proprietary SDR chipsets. HopSync frequency hopping enhances LPI and LPD characteristics, increasing resistance to detection and interference in contested spectrum environments.

Kaonic 1S is fully NDAA-compliant and ITAR-free, with European sourcing to simplify procurement and export within allied markets. Native ATAK integration supports tactical situational awareness, while rns-vpn-rs provides seamless IP application support, allowing standard UDP, TCP and IP applications to operate transparently over the mesh without modification.

1. Introduction

1.1 Operational context

Modern defence and security operations increasingly require communications systems capable of operating independently of satellite positioning services, fixed infrastructure, and centralised network coordination. Conventional architectures typically assume the availability of GPS/GNSS, base stations, managed backhaul, and persistent internet connectivity. In contested, denied, or infrastructure-degraded environments, these assumptions introduce critical vulnerabilities.

Jamming, satellite disruption, infrastructure destruction, cyber compromise, or power loss can render traditional communications systems ineffective. Systems dependent on central coordination or static topology are particularly susceptible to single points of failure.

Kaonic 1S is designed specifically to operate under these conditions. The system employs a fully decentralised mesh architecture in which no node is required for overall network continuity, eliminating single points of failure. Network routing is identity-based and secured through cryptographic mechanisms, enabling authenticated peer-to-peer communication without reliance on external servers.

To enhance resilience against electronic attack, Kaonic 1S implements frequency-hopping spread spectrum (HopSync™), providing anti-jam capability and spectral agility. Multi-band operation further improves operational flexibility and resilience across diverse regulatory and operational environments. The system is designed to function entirely offline, without dependence on GNSS, fixed infrastructure, or internet connectivity, ensuring continuity of communication in denied or disconnected scenarios.

1.2 Platform Overview

Kaonic 1S is a ruggedised, embedded Linux-based tactical radio platform designed

to deliver resilient, infrastructure-independent communications for defence, security, and unmanned system applications.

The system integrates dual-band software-defined radio capability across sub-GHz and 2.4 GHz frequency ranges, enabling flexible deployment across multiple operational environments and regulatory domains. Decentralised mesh networking is implemented using the Reticulum protocol stack, providing distributed routing without reliance on centralised infrastructure or fixed coordination nodes.

Kaonic 1S supports native integration with Tactical Assault Kit (TAK/ATAK) environments, enabling real-time situational awareness and data exchange within existing tactical ecosystems. For unmanned and autonomous platforms, the system includes MAVLink protocol support, allowing telemetry, command, and data transport across resilient mesh links. Open protocol support further enables third-party system integration, custom applications, and OEM adaptation.

The platform is designed for flexible deployment. It may be fielded as a body-worn tactical radio for dismounted operations, or supplied as an OEM module for integration into unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), remote sensors, maritime systems, and other embedded platforms requiring secure, decentralised communications capability.

2. Technical Specifications

2.1 RF Performance

Bands	**Sub-GHz (868/902-928 MHz)**	**2.4 GHz**
Frequency Range	862-928 MHz	2400-2483.5 MHz
Max TX Power	1 W EIRP per RF Chain	250 mW EIRP per RF

Bands	Sub-GHz (868/902-928 MHz)	2.4 GHz
		Chain
Max. Sensitivity	-123 dBm @ 6.25 kbps	-121 dBm @ 6.25 kbps
Data Rate Range	6.25 kbps to 2.4 Mbps per RF chain	6.25 kbps to 2.4 Mbps per RF chain
Modulation Schemes	OFDM, QPSK, (G)FSK	OFDM, QPSK, (G)FSK
OFDM MCS	0-6	0-6

2.2 Throughput Performance

Configuration	PHY Throughput	Sensitivity
Base Configuration	4.8 Mbps per TRX	-92 dBm
With FPGA Module	14.4 Mbps = 9.6 Mbps with 2x2 MIMO + 2.4 Mbps x 2 SISO	-92 dBm
Long Range (MCS 0) per RF chain	6.25 kbps x 4	-123 dBm
High Rate (MCS 6) per RF chain	2.4 Mbps	-92 dBm

2.3 Electrical Specifications

Parameter	Value
Supply Voltage	5-20 VDC
Power Consumption (RX)	~1.3 W
Power Consumption (TX)	~11.3 W @ 100% duty cycle
Average Current (Idle)	~0.8 A @ 5V

2.4 Environmental Specifications

Parameter	Value
Operating Temperature	-40°C to +85°C
Cooling	Passive (no fans)

2.5 Mechanical Specifications

Parameter	Value
Dimensions (Board Only)	120 × 60 × 7.55 mm (L×W×H)
Weight (Board Only)	84 g
Dimensions (Enclosed)	135 x 85 x 17.5 mm (L×W×H)

Parameter	Value
Weight (excl. antennas)	270g
Board RF Connectors	6× u.FL, integrated 2.4 GHz
Enclosure RF connectors	5x microBNC
Board USB Connectors	2x USB-C (data + power) 1x USB 2.0 HS on J1402 connector
Enclosure USB Connectors	2x USB-C Screw-Lock (data + power)
Mounting	M3-screw Mounting frames on both front and back faces

2.6 Processing and Memory

Component	Specification
SoC	STM32MP1 (dual-core Cortex-A7 + Cortex-M4)
Operating System	Custom Yocto Linux distribution
RAM	512 MB
Storage	microSD card (8-32 GB recommended)
Interfaces	USB-C, UART

3. Hardware Overview

3.1 Core Components

System-on-Chip (SoC):

STM32MP1 microprocessor Dual-core ARM Cortex-A7 @ 650 MHz (application processor) ARM Cortex-M4 @ 209 MHz (real-time processor) with Integrated hardware security features.

Radio Transceivers: 2× AT86RF215 dual-band transceivers:

- Front-End Module A: Primary radio chain (862-928 1W + 2.4 GHz 250 mW)

- Front-End Module B: Secondary radio chain (862-928 1W + 2.4 GHz 250 mW)

- Independent configuration and dual transmission per module totaling 4 simultaneous RF channels

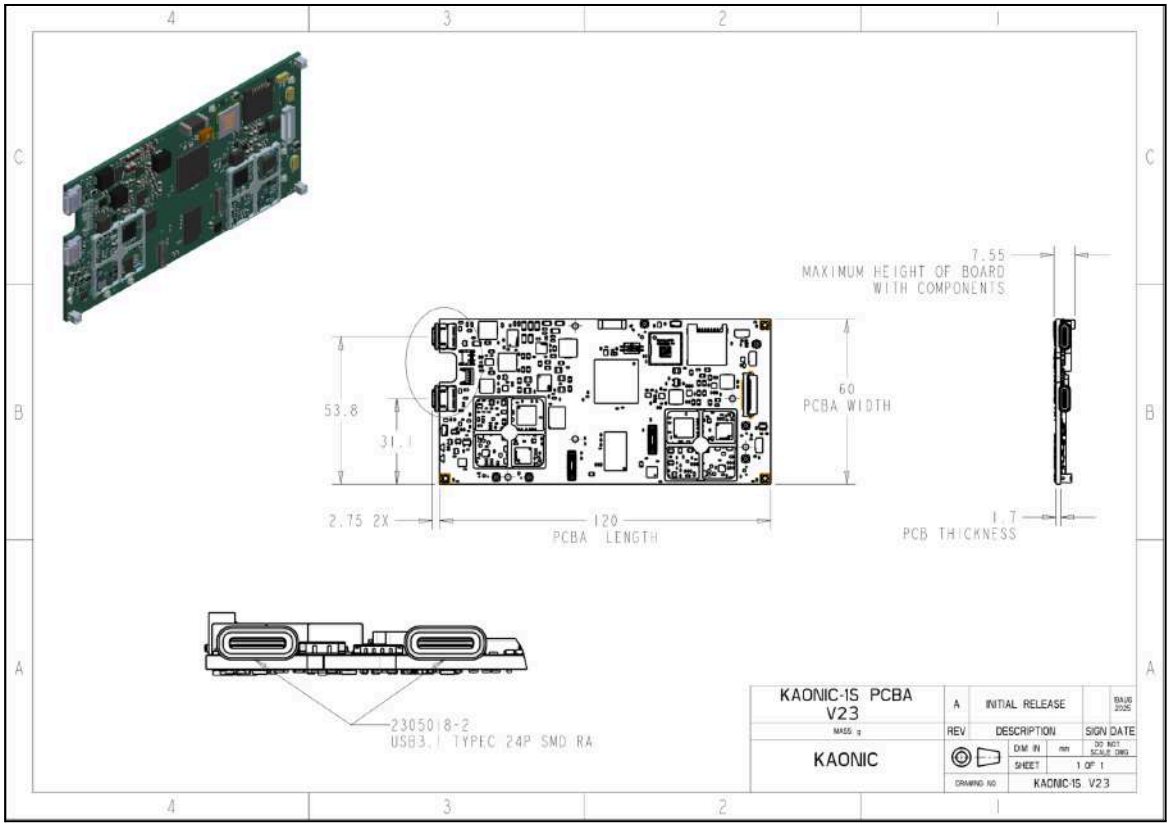
- Frequency-dependent filter switching, Power amplifiers, Low-noise amplifiers and Antenna switching

3.2 Hardware Configuration Options

Option A: OEM Board

The OEM Board configuration provides Kaonic 1S as a bare module for direct system integration. All primary I/O, serial, and RF interfaces are accessible, allowing integration at board level within a host platform.

This configuration is intended for embedded applications where enclosure, power management, and system-level design are handled by the integrator. It is suitable for integration into UAVs, UGVs, sensor platforms, maritime systems, and other autonomous platforms requiring resilient, decentralised communications capability.

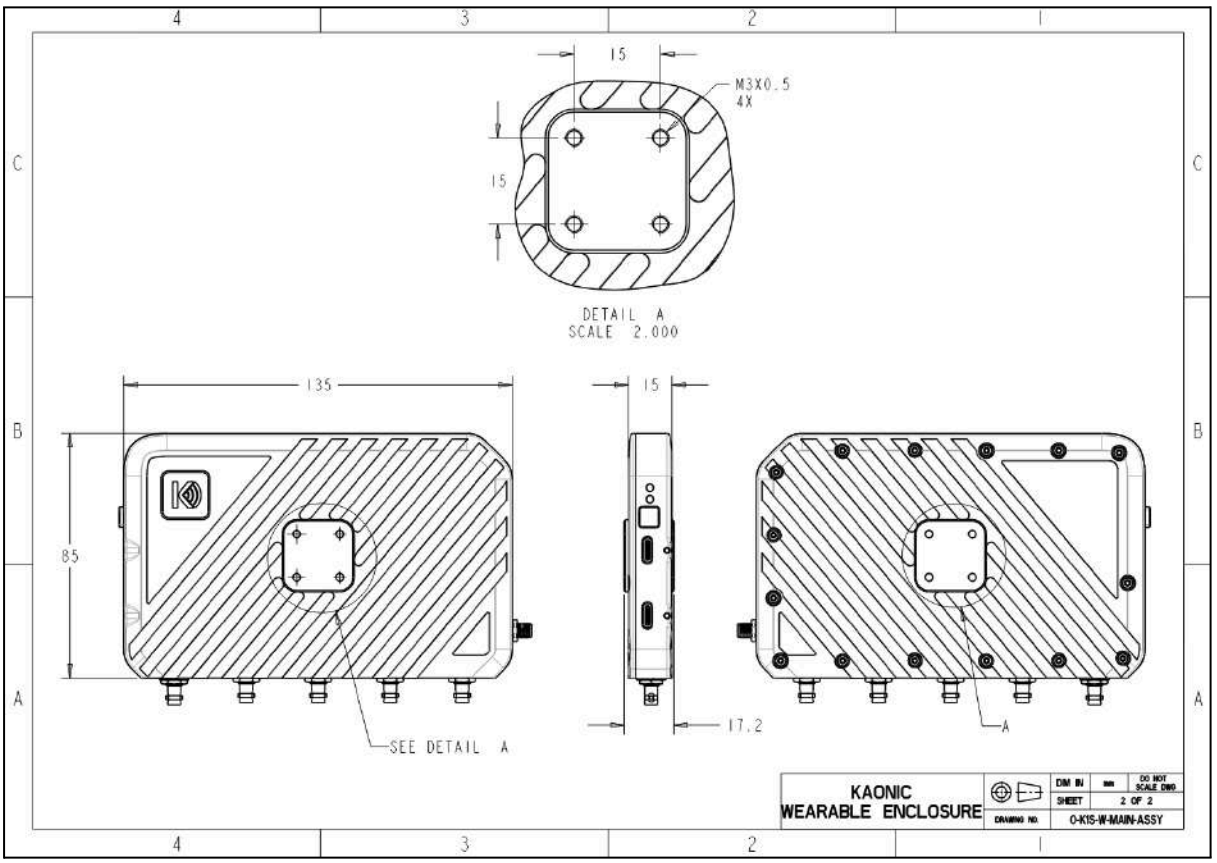


Option B: Enclosed Device (Recommended for Field Use)

The Enclosed Device configuration provides Kaonic 1S in a ruggedised, field-ready format intended for operational deployment. The unit is housed in an anodised aluminium enclosure rated to IP67 for environmental protection against dust and water ingress.

The device features two locking USB-C connectors supporting simultaneous data and power delivery. RF connectivity is optimised through diplexer support, reducing four RF connections to two external antenna interfaces and simplifying cable management in field use.

The enclosure supports shoulder-mounted wearable antenna configurations as well as gooseneck antenna options, providing flexibility across dismounted and vehicle-adjacent operations. A MOLLE-compatible mounting clip enables secure attachment to tactical load-bearing equipment.



Enclosure dimensions

3.3 Antenna Configuration

Antenna Recommendations:

Kaonic 1S supports multiple antenna configurations depending on deployment type and platform integration requirements. Proper antenna selection and placement are critical to achieving optimal range, diversity performance, and link reliability.

Sub-GHz operation (868/900 MHz): In dismounted, body-worn configurations, half-wave antennas of approximately 16–17 cm length are recommended, with 16–17 cm physical separation between elements to support effective spatial diversity. Shoulder-mounted positioning is recommended to maximise separation and radiation efficiency. For unmanned systems (UAVs, UGVs, USVs), sub-GHz antennas may be routed and mounted directly to the airframe or platform structure, subject to integration constraints.

2.4 GHz long-range operation: In user-worn configurations, shoulder-mounted placement is advised to improve diversity performance and reduce body shadowing effects. For unmanned platforms, antennas may be integrated into or mounted externally on the airframe in accordance with platform-specific RF layout considerations.

Wi-Fi and Bluetooth connectivity is supported via an integrated antenna. Where required by enclosure or integration constraints, an external 2.4 GHz side-mounted antenna may be used instead.

3.4 Rugged Enclosure Design Features

The Kaonic 1S enclosed configuration is engineered for durability and reliable operation in demanding environments. The housing is CNC-machined from anodised aluminium, providing mechanical robustness as well as inherent EMI shielding to protect internal RF and digital subsystems.

Thermal management is achieved through passive cooling, with no moving parts, reducing mechanical failure risk and improving long-term reliability in field conditions. The system is designed to operate across a wide temperature range from –40°C to +85°C, supporting deployment in extreme climates.

The enclosure is designed to meet an IP67 protection target and to withstand operational vibration and shock environments consistent with tactical and unmanned platform use.

4. Software Architecture

4.1 Operating System

Kaonic 1S operates on a custom Yocto-based embedded Linux distribution tailored for the STM32MP1 platform. The image is built from the meta-kaonic layer (kaonic-yocto), which packages kaonic-commd, the OTA service, kaonic-init, and kaonic-factory. WiFi Access Point (hostapd) and network bridging (br0, wlan0, usb0) are configured for client connectivity. Machine variants (protoa, protob, protoc) support different hardware revisions. Builds use a Docker-based workflow for reproducible images.

The distribution is built with a minimal footprint to improve system performance and enhance security by limiting unnecessary services and packages. Secure boot is implemented using signed firmware images, ensuring system integrity and preventing execution of unauthorised software.

The platform supports over-the-air (OTA) update capability, enabling controlled remote updates where operationally permitted. System services are managed using systemd, providing structured process supervision, service isolation, watchdog supervision, and predictable system startup behaviour.

The overall control architecture follows a service-separated daemon model. Radio control, mesh networking, and audio subsystems operate as independent system services to ensure fault isolation, deterministic RF behaviour, and modular maintainability.

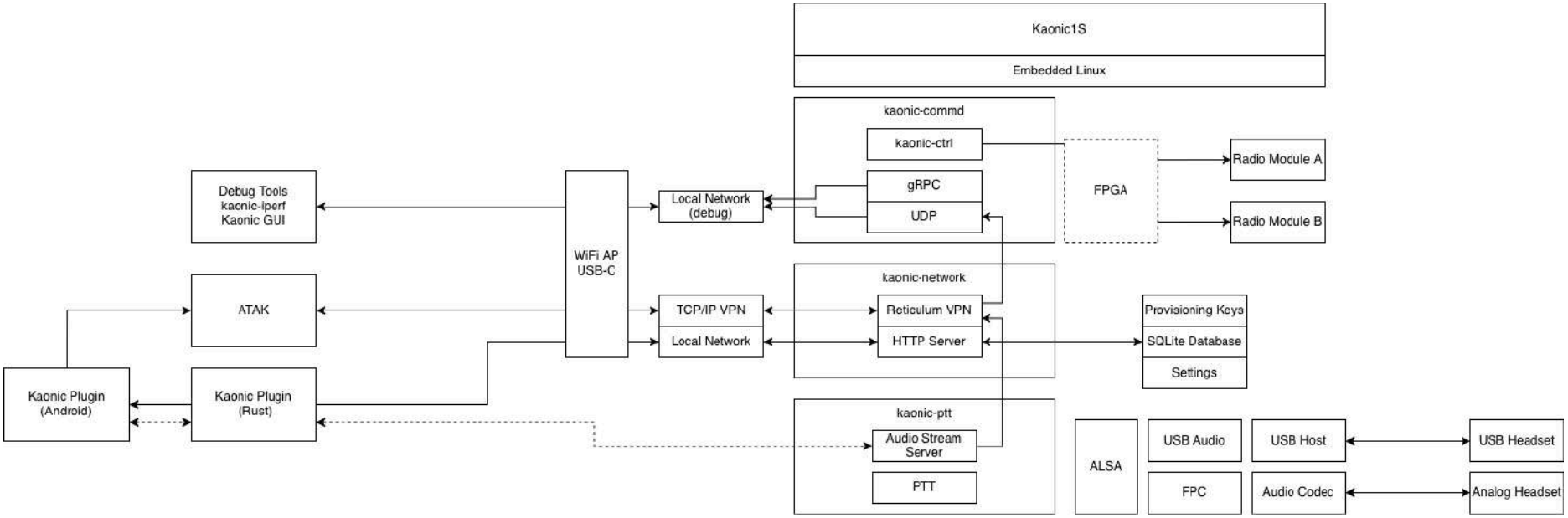
4.2 High-Level Architecture

Kaonic 1S is designed as a layered embedded system separating applications, mesh networking, radio control, and RF hardware.

The system is centred around three primary service domains: applications and client interfaces, the mesh networking and identity layer, and the deterministic radio control and FPGA baseband layer. This separation enables RF determinism, infrastructure-free mesh scalability, and clean IP abstraction for integrators.

Client access is typically provided via WiFi AP or USB-C for ATAK devices and plugins. In addition, the platform supports local debug access for engineering and commissioning workflows, including the Kaonic GUI and standard network testing tools such as iperf for configuration, monitoring, and performance validation.

4.2.1 System Architecture



4.3 Core Software Components

Kaonic 1S software functionality is structured around three primary system daemons:

- kaonic-commd (radio control layer)
- kaonic-gateway (mesh networking and management layer)
- kaonic-ptt (audio and push-to-talk subsystem)

This separation of concerns enables RF determinism, mesh scalability, and clean IP abstraction for integrators.

4.3.1 kaonic-commd (Communication Daemon)

The kaonic-commd service functions as the primary communications control layer within the system. It provides low-level radio control and deterministic frame handling between the mesh layer and the RF hardware.

Role: Radio control plane; interface between higher-layer networking services and the physical RF subsystem.

External Interface:

- UDP interface (default port 9090) via kaonic-ctrl binary protocol for configuration, frame transmission, and control.
- Used by kaonic-gui, kaonic-iperf, and other clients.

Internal Transport:

- UDP-based interface between mesh layer and kaonic-commd

Architecture:
The service uses a worker-thread architecture to ensure non-blocking operation. Dedicated event threads per radio module provide deterministic receive handling and prevent Linux scheduling variability from affecting RF timing.

Each radio is represented as a PlatformRadio instance, enabling dual-radio parallel operation.

Hardware Path:
kaonic-ctrl → (UDP) → kaonic-commd → kaonic-radio → FPGA/Radio

kaonic-ctrl Protocol

Message format: Fixed header (pattern 0xBACE, version, message ID, flags) + MessagePack-serialised payload

Radio frame size: 2048 bytes

Supported payload types include:

```
Ping,
Pong,
TransmitModuleRequest(TransmitModule),
TransmitModuleResponse,
ReceiveModule(ReceiveModule),
ScanRequest,
SetRadioConfigRequest(SetRadioConfigRequest),
SetRadioConfigResponse,
GetRadioConfigRequest(GetRadioConfigRequest),
GetRadioConfigResponse(GetRadioConfigResponse),
SetModulationRequest(SetModulationRequest),
SetModulationResponse,
GetModulationRequest(GetModulationRequest),
GetModulationResponse(GetModulationResponse),
GetInfoRequest,
GetInfoResponse(GetInfoResponse),
NotImplemented,
Error
```

Key details on:
"https://github.com/BeechatNetworkSystemsLtd/kaonic-radio/commit/c58db17b39163e479f2df60322b0b3a333217707"

Transmit requests are passed directly to the FPGA and RF modules with minimal software-layer latency. ReceiveModule events are broadcast to subscribed clients.

Design Rationale:
RF determinism is achieved by isolating radio timing from general-purpose Linux user space scheduling. The FPGA handles baseband operations while dedicated threads ensure predictable latency and consistent receive handling under load.

4.3.2 kaonic-gateway (Network Services Daemon)

The kaonic-gateway service provides mesh networking, identity management, system configuration, and IP abstraction.

Role: Mesh networking layer providing Reticulum VPN and management APIs.

Core Services: Reticulum VPN, HTTP management server, Persistent configuration management

Storage: Provisioning keys, SQLite configuration database, System settings

Interfaces: TCP/IP VPN interface for applications, Local network access (WiFi AP or Ethernet-over-USB-C), Internal UDP transport to kaonic-commd

Reticulum-rs Protocol

Kaonic 1S uses Reticulum-rs as its cryptographic mesh networking layer.

Reticulum-rs abandons traditional IP-centric routing in favour of identity-based addressing. Node identity is cryptographic and decoupled from physical location, enabling trustless routing across decentralised networks without reliance on central servers or fixed infrastructure.

Key characteristics:

- Identity-native encryption
- Infrastructure-free mesh operation

- Up to 128 encrypted mesh hops
- Persistent provisioning keys for secure peer discovery
- Deep, high-latency topology support

Application data flow:

Application → TCP/IP VPN → Reticulum VPN → kaonic-commd → FPGA/Radio

This architecture abstracts RF complexity from applications. Tactical software interacts with a standard TCP/IP interface while the mesh and radio layers operate transparently beneath.

4.3.3 kaonic-ptt (Push-to-Talk Daemon)

The kaonic-ptt service provides the audio subsystem for voice over mesh and push-to-talk control.

Role: Audio capture, encoding, streaming, and PTT signalling.

Audio Stack: ALSA-based audio subsystem

Supported Inputs:

- USB audio headsets (USB Host mode)
- Analog headsets (via onboard codec interface)

Voice data is encoded and routed through the mesh via kaonic-gateway and kaonic-commd, enabling low-latency voice over mesh.

External plugins (Android and Rust implementations) can interact with kaonic-ptt for push-to-talk signalling and audio control.

4.4 Data Flow Architecture

4.4.1 Application Data Path

Application (ATAK / plugins)
→ TCP/IP VPN
→ Reticulum VPN (kaonic-gateway)
→ UDP internal interface
→ kaonic-commd
→ FPGA / Radio Module A / B

4.4.2 Voice Path

Microphone (USB / Analog headset)
→ ALSA
→ kaonic-ptt
→ Reticulum VPN
→ kaonic-commd
→ FPGA / Radios

4.4.3 Receive Path

Radio Modules A / B + FPGA
→ kaonic-commd (ReceiveModule events)
→ Reticulum VPN
→ TCP/IP VPN
→ Application

4.5 Transport Interfaces

Kaonic 1S provides multiple transport interfaces for integration flexibility. These interfaces support operational client devices, OEM integration, and engineering diagnostics.

Native radio transport is exposed via UDP (kaonic-ctrl protocol, port 9090), and Ethernet-over-USB is supported for straightforward wired connectivity and power delivery. Where required, the system can bridge into IP networks through a TCP server interface, provide lightweight datagram transport through a UDP interface, and support point-to-point integration through a serial interface.

For client access and field configuration, a WiFi Access Point mode is provided for ATAK devices, plugins, and authorised client endpoints. A USB-C device interface is also available for wired connectivity and power in dismounted or vehicle-adjacent deployments.

For engineering validation and diagnostics, Kaonic 1S supports a dedicated local debug network workflow. This includes network throughput testing using iperf, as well as system configuration and monitoring via the Kaonic GUI during integration, testing, and commissioning.

4.6 HopSync™ Frequency Hopping

HopSync™ is Beechat's patent-pending implementation of a stateless Frequency-Hopping Spread Spectrum (FHSS) protocol.

Unlike legacy FHSS systems, HopSync does not rely on over-the-air synchronisation beacons, centralised time servers, or handshake signalling to maintain frequency alignment between nodes.

Operating frequencies are deterministically derived using a cryptographic retrieval function (e.g., HMAC) based on a shared secret and a local time reference. Each node independently computes the same hop sequence without exchanging coordination messages.

This distributed model eliminates synchronisation traffic, reduces protocol overhead, and minimises electromagnetic signature exposure.

Key properties:

- Stateless frequency alignment
- No synchronisation beacons
- Intrinsic Low Probability of Intercept (LPI)
- Intrinsic Low Probability of Detection (LPD)
- Robust anti-jam protection via rapid frequency agility
- Scalable to large distributed node counts

4.7 Quality of Service (QoS)

Kaonic 1S implements an adaptive Quality of Service (QoS) framework designed to maintain link stability, optimise throughput, and mitigate interference under dynamic RF conditions.

The system continuously monitors channel state and automatically adjusts transmission parameters.

Key mechanisms:

Adaptive modulation, adaptive transmit power control, congestion management via exponential backoff, Clear Channel Assessment (EDV-based), and continuous multi-parameter channel quality assessment are employed to preserve link reliability and network stability.

4.8 Design Principles

The Kaonic 1S software architecture is built upon a set of foundational engineering principles intended to ensure reliability, scalability, and operational resilience in contested environments.

At its core, the system adopts a strict service separation model. Radio control, mesh networking, and audio subsystems operate as independent daemons, providing fault isolation, simplified maintainability, and clear architectural boundaries between timing-critical RF functions and higher-layer services.

RF determinism is achieved through the combination of FPGA-based baseband processing and dedicated radio event threads. This approach ensures predictable latency and stable timing behaviour, independent of general-purpose Linux scheduling variability.

The platform is designed for infrastructure-free operation. Mesh networking does not rely on central servers, fixed gateways, or external synchronisation sources, enabling autonomous deployment in GNSS-degraded or disconnected environments.

Security is identity-native by design. Routing and addressing are cryptographically derived rather than location-based, ensuring that trust relationships are intrinsic to the protocol architecture rather than layered externally.

Applications interact with the system through a standard TCP/IP abstraction layer, while radio and mesh complexity remain encapsulated within the platform. This IP abstraction enables straightforward integration with tactical applications, plugins, and external systems without requiring RF-specific knowledge.

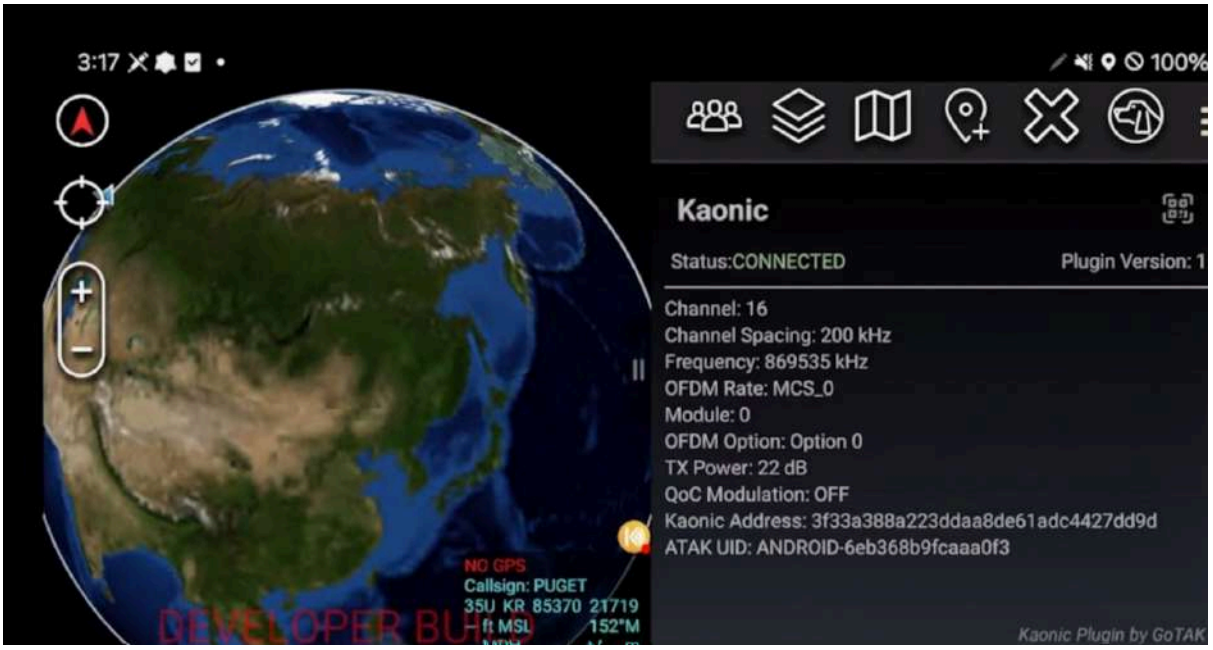
Finally, the modular architecture supports flexible OEM integration across a range of deployment models, including dismounted radios, UAV relay nodes, vehicle-mounted systems, static mast installations, and embedded radio modules within larger platforms.

5. ATAK Plugin Integration

5.1 Overview

The Kaonic ATAK plugin integrates Kaonic 1S mesh communications directly into the

Android Tactical Assault Kit (ATAK) environment, enabling secure, infrastructure-independent tactical communications. The plugin provides native interaction between ATAK applications and the Kaonic mesh layer, allowing users to operate within familiar workflows while leveraging decentralised radio networking.



Kaonic ATAK Plugin main screen

5.2 Key Capabilities

5.2.1 Secure Messaging

The plugin provides secure messaging, voice, file transfer, and situational awareness functionality over the Kaonic mesh network.

Encrypted text messaging is supported across the mesh, with acknowledgement-based (ACK) delivery confirmation to ensure message reliability. Contact-based addressing is implemented using cryptographic identity-derived identifiers, enabling authenticated peer-to-peer communication without central servers.

Bidirectional voice communication is supported using the OPUS codec, providing

real-time audio transmission over the mesh. A Push-to-Talk (PTT) mode is available upon request for tactical deployments. Voice communications are designed for low latency operation, with typical round-trip times of approximately 100 ms under suitable link conditions. Call control functions include answer, reject, and termination management.

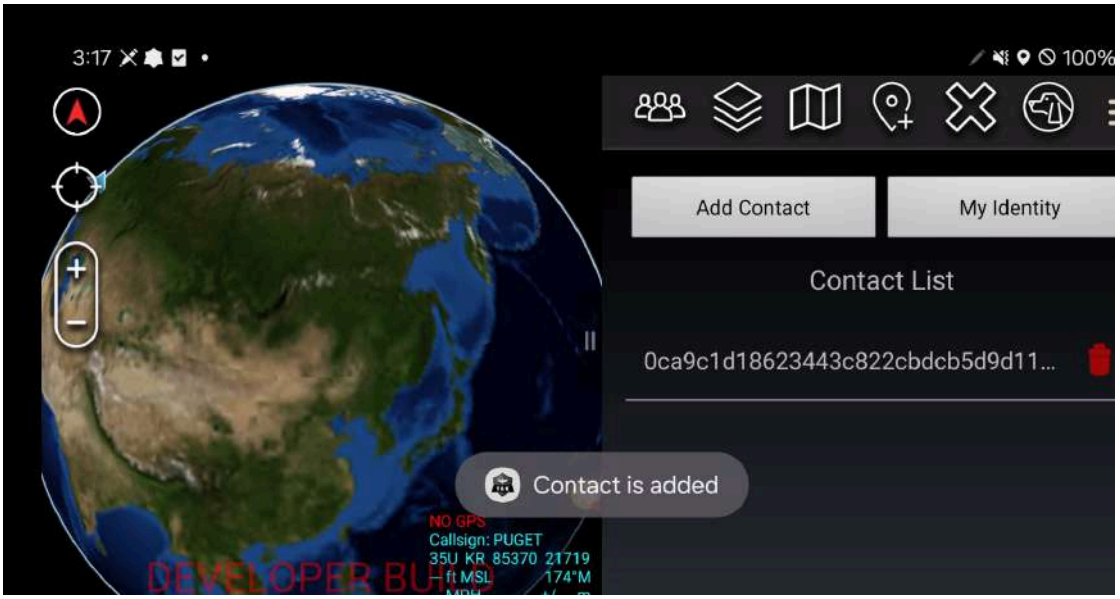
Secure file transfer enables controlled distribution of mission data between authorised participants. Location sharing supports transmission of GPS position, Precise Location Information (PLI), waypoints, and related tactical data. All communications are protected using end-to-end encryption.

5.2.2 Contact Management

Mesh participants are automatically discovered within a defined whitelist. Access control is configurable through a contact whitelist mechanism, restricting communications to authorised identities. The system provides real-time presence and connectivity status indicators for discovered contacts.

Identity management is cryptographically enforced, with addressing derived from secure identity constructs rather than network-layer identifiers, enhancing authenticity and reducing spoofing risk.

“My identity” screen



“My Contacts” screen

5.2.3 CoT (Cursor on Target) Integration

The plugin provides native support for Cursor on Target (CoT) message processing. Position updates, operational status, and field observations can be transmitted across the Kaonic mesh. Tactical graphics and overlays are supported, enabling exchange of map-based mission data. The system allows distribution of

mission-critical information without reliance on centralised CoT servers.

5.2.4 Voice Communications

The Kaonic ATAK plugin supports real-time voice communication over the Kaonic mesh network, enabling direct peer-to-peer audio exchange without infrastructure dependency. Voice transmission is optimised for tactical environments, maintaining low latency performance with typical round-trip times of approximately 100 ms under suitable link conditions.

Push-to-Talk (PTT) functionality is available upon request for deployments requiring controlled, half-duplex tactical voice operation. The system also supports standard call management features, including call initiation, answer, rejection, and termination controls, integrated directly within the ATAK interface.

All voice communications are transported over the secure mesh layer and benefit from the same cryptographic protections applied to data messaging and situational awareness traffic.

5.3 Connection Modes

5.3.1 TCP/IP Mode

In TCP/IP mode, the plugin connects to a Reticulum TCP server instance. This configuration enables the Kaonic radio mesh to be bridged into IP-based networks, facilitating integration with existing infrastructure or extended backhaul links.

This mode is particularly suitable for fixed installations, command posts, or gateway nodes where long-range IP connectivity is available and persistent network bridging is required.

5.3.2 UDP Mode

UDP mode provides lightweight datagram-based communication between the plugin and the Kaonic system. This configuration reduces protocol overhead and may be preferred in environments where lower latency or simplified transport behaviour is required.

UDP mode is suitable for controlled network environments where connection persistence and reliability are managed at higher layers.

5.3.3 Ethernet-over-USB Mode

In Ethernet-over-USB mode, the ATAK device connects directly to the Kaonic 1S hardware via USB, without requiring a WiFi connection. This configuration simplifies deployment and reduces system complexity.

Ethernet-over-USB operation provides lower latency compared to network-bridged configurations and is well suited for dismounted users or mobile deployments requiring rapid setup and minimal infrastructure.

5.4 Plugin Architecture

The Kaonic ATAK plugin is implemented as a modular Android component set designed for clear separation between lifecycle management, communications handling, user interface integration, and identity control.

The primary entry point is `Kaonic.java`, which serves as the main plugin class and manages integration with the ATAK plugin framework, including initialisation, registration, and lifecycle control.

The `KaonicCommunicationManager` provides the communications management layer. It is responsible for handling connectivity with the Kaonic radio subsystem, managing message exchange, and coordinating data flow between ATAK services and the underlying mesh transport.

User interface integration is provided through the `KaonicWidget`, which displays operational status and connectivity information within the ATAK interface. Configuration and user-adjustable parameters are managed through a dedicated `PreferencesFragment`, which exposes plugin settings and connection options within the ATAK settings environment.

Contact management functionality is integrated within the plugin architecture, enforcing whitelist-based access control and handling identity-based contact discovery and session management.

5.5 Configuration and Setup

Initial Setup:

1. Install plugin APK on ATAK device

2. Enable plugin in ATAK settings

3. Configure connection (TCP/IP or USB)

4. Set up contact whitelist

5. Boot Kaonic 1S radios and start communication

5.6 Use Cases

The Kaonic ATAK integration is designed to support operations in environments where communications infrastructure is unavailable, degraded, or untrusted.

In tactical operations, the system enables secure team communications across distributed units using decentralised mesh networking. Real-time situational awareness can be maintained through position sharing, tactical overlays, and mission data exchange within the ATAK environment. The platform supports coordinated mission execution without reliance on central servers, fixed base

stations, or internet connectivity, making it suitable for fully off-grid deployments.

In emergency response scenarios, the system provides resilient communications for disaster response and recovery operations. It enables search and rescue teams to coordinate in infrastructure-denied environments and supports field teams operating in areas affected by power loss, network collapse, or environmental disruption. The decentralised architecture allows rapid deployment and infrastructure-independent coordination across multiple agencies or units.

6. Security and Compliance

6.1 Security Architecture

Zero-Trust Design:

Kaonic 1S is designed according to a zero-trust security model in which each device operates as its own root of trust. The system does not rely on a central authority for authentication or routing control. Instead, trust is established through cryptographic identity mechanisms embedded within the device architecture. All communications are protected by end-to-end encryption by default, ensuring confidentiality and integrity across the mesh network.

Cryptographic Features:

Security is identity-based rather than location- or network-based. Devices are addressed using cryptographic identities, reducing exposure to spoofing and unauthorised network participation. The architecture supports forward secrecy to limit exposure in the event of key compromise, and no key escrow mechanisms are implemented, preserving end-user control over cryptographic material. A post-quantum cryptography update is planned for Q2 2026 to further strengthen long-term resilience against emerging cryptographic threats.

Secure Boot:

System integrity is enforced through secure boot mechanisms. Firmware images are cryptographically signed, and signature verification is performed at boot time to prevent execution of unauthorised or modified software.

OTA Updates:

Over-the-air (OTA) updates are delivered as signed packages and are subject to automatic cryptographic verification prior to installation. In the event of update failure or validation error, the system supports automatic rollback to a known-good firmware state, preserving operational continuity and device integrity.

6.2 Compliance and Certifications

Kaonic 1S is designed with regulatory and export considerations integrated at both hardware and supply-chain levels.

NDAA Compliance:

The platform is designed and manufactured within the European Union and does not incorporate prohibited components under NDAA Section 889. The architecture and bill of materials are structured to support NDAA compliance requirements for U.S. government and defence procurement contexts.

ITAR Status:

The system is designed to be ITAR-free. No ITAR-controlled components are incorporated into the hardware design, supporting export-friendly deployment across multiple jurisdictions, subject to applicable local regulations.

Regulatory Compliance:

From a regulatory perspective, the platform is developed to support European CE marking under the Radio Equipment Directive (RED) and corresponding EMC and safety requirements. FCC compliance is supported for applicable U.S. frequency bands and deployment configurations, with region-specific certification profiles managed according to target markets.

7. Performance Characteristics

7.1 Range Performance

Sub-GHz Band (868/900 MHz):

- **Line of Sight**: Up to 50+ km (depending on terrain and power)

- **Urban Environment**: 1-5 km typical

- **Dense Foliage**: 500 m - 2 km typical

2.4 GHz Band:

- **Line of Sight**: Up to 10+ km (depending on power)

- **Urban Environment**: 500 m - 2 km typical

- **Dense Foliage**: 200 m - 1 km typical

Note: Actual range performance is dependent on transmission power configuration, antenna selection and placement, terrain profile, environmental conditions, selected modulation and coding scheme (MCS), and prevailing interference levels. Real-world performance will vary based on deployment geometry and RF environment.

You may use https://plan.beechat.network to simulate networks with different

settings.

7.2 Mesh Network Performance

Multi-Hop Routing:

Kaonic 1S implements decentralised multi-hop routing designed for resilient, infrastructure-independent operation. The mesh architecture supports up to 128 hops within a single routing path. Path discovery is performed automatically, with multiple redundant routes maintained where available to improve fault tolerance. Route maintenance is dynamic, allowing the network to recover from link degradation or node loss without manual intervention.

Network Scalability:

The system is designed to scale to hundreds of nodes within a single mesh domain. Routing overhead is optimised to minimise control traffic while preserving convergence performance. The topology adapts automatically to node mobility, enabling stable operation in dynamic environments involving moving personnel or platforms.

Latency:

Latency is dependent on link quality and network depth. Typical single-hop latency is in the range of approximately 20–50 ms. In multi-hop configurations, latency typically increases by approximately 50–70 ms per additional hop, subject to modulation settings, channel conditions, and traffic load.

8. Deployment Scenarios

8.1 Tactical Field Operations

In small-unit tactical deployments, Kaonic 1S is typically configured as an enclosed, ruggedised device with shoulder-mounted antennas to optimise diversity and minimise body shadowing. The network operates as a direct peer-to-peer mesh between team members, without reliance on external infrastructure.

Integration with the ATAK plugin enables real-time situational awareness, secure messaging, and mission coordination. In typical operational environments, expected range performance is approximately 1–5 km, depending on terrain, antenna configuration, and RF conditions**.**

8.2 Unmanned Systems Integration

For UAV and UGV command-and-control applications, Kaonic 1S operates as a resilient mesh link between ground control elements and unmanned vehicles. The system supports MAVLink protocol bridging and integrates with common Ground Control Station (GCS) software environments, including ArduPilot Mission Planner and QGroundControl.

Hardware integration includes a DF52 Hirose USB 2.0 High-Speed interface for encoded video or high-rate data streaming, and a DF52 Hirose UART interface for command-and-control connectivity to the unmanned vehicle flight controller. The mesh architecture enables distributed vehicle operations without dependence on centralised radio infrastructure.

8.3 Fixed Installation Bridge

In fixed installations, Kaonic 1S can be deployed with externally mounted antennas

to maximise coverage and link margin. In this configuration, the system functions as a bridge between the radio mesh and IP-based networks.

Connectivity can be established via a TCP server bridge or through VPN-based tunnelling (rns-vpn-rs), enabling transparent IP transport over the mesh. Standard TCP/IP applications, including web services, SSH, databases, and other networked services, can operate across the mesh without modification.

8.4 Maritime Operations

For maritime environments, the enclosed ruggedised configuration is recommended. Antennas are typically mounted at elevated positions to improve line-of-sight performance and reduce multipath interference.

The system supports ship-to-ship and ship-to-shore mesh networking across distributed vessels. Integration may be achieved through ATAK or custom mission applications, depending on operational requirements.

8.5 Emergency Response

In disaster response and search-and-rescue scenarios, Kaonic 1S can be deployed as portable field devices with flexible antenna configurations. Units automatically form an ad-hoc mesh network without the need for pre-existing infrastructure.

Integration with ATAK enables coordination, position sharing, and mission data exchange among responders, supporting resilient communications in environments affected by infrastructure loss or network disruption.

9. Integration Capabilities

9.1 Protocol Support

Kaonic 1S supports a range of native and bridged protocols to enable integration across tactical, unmanned, and standard IP-based environments.

- **Reticulum**: At the mesh layer, the system natively implements the Reticulum protocol stack, providing cryptographically secured, decentralised networking with identity-based routing.

- **TAK/ATAK**: For tactical situational awareness, native integration with TAK/ATAK enables secure message exchange, position sharing, and mission data transport within established Android Tactical Assault Kit workflows.

- **MAVLink**: For unmanned systems, MAVLink protocol support enables telemetry, command, and control communication between ground control elements and UAV or UGV platforms over the resilient mesh transport layer.

In addition, standard IP protocols are supported through the rns-vpn-rs VPN/TUN implementation. This allows transparent IP tunnelling across the mesh network, enabling conventional TCP/IP applications to operate without modification over Kaonic infrastructure.

9.2 API Interfaces

Kaonic 1S exposes structured application interfaces to enable configuration, monitoring, and integration with external systems.

UDP Interface:

A UDP-based interface provides lightweight datagram transport for client applications and plugins. This interface reduces protocol overhead compared to TCP and may be preferred where lower latency or simplified transport behaviour is required. The ATAK plugin and other clients can connect via UDP mode for mesh access.

gRPC API:

A gRPC interface (port 8080) may be used for Reticulum and rns-vpn-rs integration,

enabling mesh transport for VPN-over-mesh and multi-hop routing. Availability depends on deployment configuration.

REST API (OTA only):

A REST-based interface is available exclusively through the OTA service layer for firmware updates. This interface supports firmware update management, version reporting, and update status monitoring. It is not used for general configuration or mesh control; those functions are provided by the UDP and gRPC interfaces.

9.3 Software Development Kits

Software Development Kits (SDKs) are provided to support application development and system integration across multiple environments.

Android SDK:

The Android SDK exposes a Java and Kotlin API built on an event-driven architecture. It supports both USB and TCP/IP connection modes and provides complete messaging, voice, and call control interfaces for integration into Android applications, including ATAK-based or custom deployments.

Rust SDK:

The Rust SDK provides a native Rust API for low-level interaction with the Kaonic system. It enables direct hardware access, granular radio configuration control, and development of high-performance or embedded applications requiring deterministic behaviour and minimal abstraction overhead.

9.4 Third-Party Integration

Kaonic 1S is designed for interoperability across tactical, embedded, and general-purpose computing platforms.

Supported Platforms:

Supported environments include Android devices (including ATAK and custom applications), Linux systems in both embedded and desktop configurations, and unmanned platforms interfacing via UART using MAVLink. Custom applications may interface directly through the gRPC API.

Integration Examples:

Integration examples include the provided ATAK plugin, the MAVLink bridge for unmanned system control, and VPN-over-mesh functionality using rns-vpn-rs. The VPN implementation enables standard TCP/IP applications to operate transparently across the Kaonic mesh without modification. Additional custom integrations can be developed using the provided SDKs and documented APIs.

9.5 IP Application Support via *rns-vpn-rs* VPN

The rns-vpn-rs component provides a TUN/TAP interface that enables any standard IP application to run transparently over the Kaonic mesh network without modification. This powerful capability bridges the gap between mesh networking and traditional IP-based applications. Key Features:

Key Features:

- **Deterministic IP derivation:** Each node's IP address is derived from its Reticulum identity (address hash). The same identity always maps to the same IP within a given network prefix, enabling predictable addressing without manual mapping.

- **Whitelist-based access:** Only peers listed in the configuration can communicate. Traffic is routed only to configured peer destination hashes; unknown identities are not reachable.

- **Transparent IP Tunneling:** Creates a virtual network interface (TUN) that routes IP traffic over the Reticulum mesh

- **Zero Application Modification**: Standard IP applications work without any code changes

- **P2P VPN Architecture**: Point-to-point VPN connections between mesh nodes

- **Automatic Routing**: IP packets are automatically encapsulated and routed through the mesh

- **Multi-Protocol Support**: Supports all TCP and UDP protocols

Supported Applications

Through the rns-vpn-rs VPN/TUN implementation, Kaonic 1S enables standard IP-based applications to operate transparently over the mesh network without modification.

Network Services:

Supported network services include web servers (HTTP/HTTPS), SSH remote access, database connections such as MySQL and PostgreSQL, file transfer services including FTP, SCP, and SFTP, and remote desktop protocols such as VNC and RDP.

Communication Applications:

Communication applications are also supported, including VoIP clients using SIP or WebRTC, video conferencing platforms, instant messaging systems such as XMPP

and IRC, and email clients using SMTP, IMAP, or POP3.

Custom Applications:

In addition, any custom or legacy application utilising standard TCP/IP or UDP sockets can operate across the Kaonic mesh. This includes enterprise software requiring network connectivity, legacy systems designed for conventional IP infrastructure, and IoT device management protocols requiring IP-based transport.

Configuration:

The VPN uses a network prefix (CIDR) and a whitelist of peer destination hashes. Each node's IP is deterministically derived from its Reticulum identity hash combined with the network prefix. Peers must add each other's destination hashes to their configuration to establish connectivity.

Example Configuration:

```
network = "10.20.0.0/16"

peers = [ "db332f13541eb2e4b47d02923fbbcb9a",
"758727c1d044e1fd8a838dc8d1832e95" ]
```

Use Cases

The VPN-over-mesh capability enables seamless integration of conventional IP-based systems into the Kaonic mesh environment.

Legacy System Integration:

In legacy system integration scenarios, existing IP-based infrastructure can be connected directly to the mesh network without software modification. Enterprise applications can be bridged into tactical or field-deployed networks, and legacy equipment designed for traditional IP connectivity can be integrated without

hardware or firmware changes.

Service Deployment:

For service deployment, web services can be hosted directly over the mesh, database servers can be made accessible across distributed nodes, and remote access services such as SSH or RDP can be provided through the decentralised network. This enables distributed service architectures without reliance on centralised internet connectivity.

Application Flexibility:

From an application flexibility perspective, developers may continue to use standard development tools, libraries, and IP-based programming models. Existing applications can be deployed without modification, leveraging familiar IP infrastructure while operating across a resilient mesh transport layer.

Benefits:

- **No Code Changes**: Existing applications work immediately

- **Standard Protocols**: Use familiar TCP/IP protocols

- **Development Flexibility**: Develop using standard tools

- **Integration Ease**: Connect existing systems seamlessly

- **Protocol Transparency**: All IP traffic automatically routed

10. Support and Services

10.1 Technical Support

Kaonic 1S is delivered with structured technical support to ensure reliable deployment and operational continuity.

Included Support (Year 1):

During the first year, support includes priority technical assistance with a typical response time of 24–48 hours, system integration guidance, and remote training sessions. Firmware updates and security patches are provided as part of ongoing lifecycle maintenance. Customers also receive network configuration guidance and Return Material Authorisation (RMA) support beyond the baseline warranty framework.

Extended Support (Year 2+):

Extended support packages are available from Year 2 onward. These include continued priority technical assistance, additional structured training sessions, and accelerated RMA turnaround where required. On-site support services and custom engineering engagements are available upon quotation, depending on project scope and operational requirements.

10.2 Training

Available Training:

Structured training programmes are available to support deployment across operational, technical, and integration teams. Training may be tailored to different user roles, including operators, technical support staff, system administrators, and integration developers.

Custom training programmes can be developed to address mission-specific

workflows, integration requirements, or advanced system configuration scenarios.

10.3 Documentation

Available Documentation

Comprehensive documentation is provided to support deployment, integration, and lifecycle management. Available materials include detailed technical specifications, user guides, API documentation, integration guides, troubleshooting resources, and developer-focused documentation.

Documentation Formats

Documentation is available through structured online resources built using Sphinx, as well as downloadable PDF technical sheets. API references and code examples are provided to support software development and third-party integration.

10.4 Warranty

Standard Warranty: 12 months from delivery for manufacturing defects only. Repair or replacement with RMA process support.

Warranty Exclusions: Misuse or unauthorised modification, Environmental stress beyond specifications, Water ingress, Operation outside specifications.

11. Conclusion

Kaonic 1S represents a next-generation approach to tactical communications, combining:

Resilience: Infrastructure-free operation with mesh networking

Security: Zero-trust architecture with cryptographic security
Flexibility: Multiple deployment options and integration capabilities
Compliance: NDAA-compliant, ITAR-free European sourcing
Performance: Dual-band operation with adaptive QoS
Integration: Native TAK support for tactical operations

The platform is designed for defence, security, and critical infrastructure applications where reliable, secure communications are essential, even in contested or denied environments.

12. Contact Information

Beechat Network Systems Ltd

Web: www.beechatnetwork.com

Sales Inquiries: sales@beechat.network

Technical Support: outreach@beechat.network

Address: 86-90 Paul Street EC2A 4NE, London, England

Document Control

Version	Date	Author	Changes
1.0	Dec 2025	Beechat Network Systems	Initial release
1.1	Feb 2026	Beechat Network Systems	Updated Enclosure