

Impact for Electronic Warfare (EW) and SIGINT

Introduction and concept

In today's rapidly evolving military and security landscape, the electromagnetic spectrum has become a highly contested domain. Electronic Warfare (EW) and Signals Intelligence (SIGINT) operations increasingly depend on the ability to detect, classify, and respond to complex signal environments in real time. The proliferation of diverse wireless communication standards - ranging from legacy analog systems to modern digital and adaptive protocols such as 5G, satellite links, and software-defined radios - has made traditional analysis methods insufficient for the speed and complexity of contemporary threat scenarios.



Artificial Intelligence (AI) algorithms have emerged as a decisive enabler for **modern and broad-spectrum analysis**. Leveraging machine learning, deep learning, and advanced pattern recognition, AI can ingest massive volumes of raw RF data from across the spectrum, automatically detect signals of interest, and classify their modulation, source, and potential intent. These systems can handle both narrowband and wideband data, ensuring coverage across all known wireless standards, as well as the capacity to adapt to unknown or non-standard waveforms.

A critical advantage of AI-powered spectrum analysis lies in **real-time processing**. Traditional workflows often relied on post-event analysis, which limited operational responsiveness. AI-enabled EW/SIGINT platforms can now process high-throughput data streams instantly, providing operators with immediate alerts on anomalies, jamming attempts, or emerging hostile transmissions. This real-time situational awareness not only accelerates the **detection–classification–decision** cycle but also enhances mission effectiveness in contested environments.

These advancements have led to the emergence of **cognitelligent solutions**—systems that combine cognitive computing with intelligent automation. Such solutions support human operators by filtering out irrelevant data, highlighting critical threats, and offering decision recommendations based on learned patterns and contextual mission parameters. By reducing cognitive load and increasing confidence in the data, AI empowers faster and more informed human decision-making, a decisive factor in time-critical defense scenarios.

In the modern battlefield, **superiority in the electromagnetic spectrum** hinges on speed, adaptability, and precision. AI algorithms, integrated into EW and SIGINT platforms, deliver all three: transforming the vast complexity of wireless communications into actionable intelligence at machine speed. The result is a force multiplier that reshapes the tempo and outcome of military and security operations.

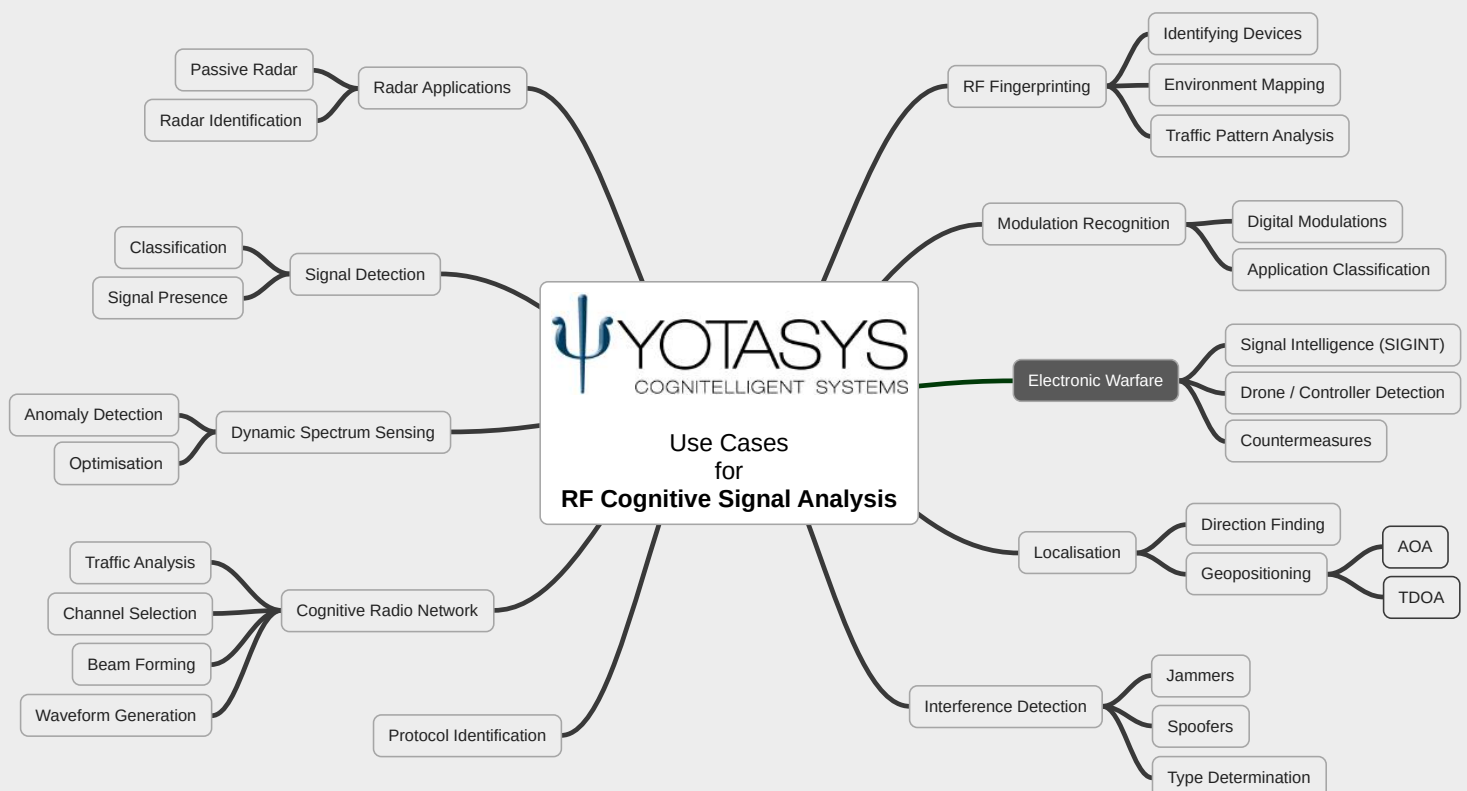
Highlights

- Full spectrum coverage from **9 kHz to 54 GHz**
- **Realtime** Signal procession enabling immediate detection and classification of signals
- **Adaptive** to unknown waveforms and modern signals
- Enhanced **decision support** and shorten the detect-decide-act cycle
- Cognitelligent solutions reduces operator workload and improves **decision accuracy**
- Scalable to **complex environments** like multi-signal and interference-loaded spectrum conditions
- **Actionable intelligence** delivery with filtered and prioritized alerts and recommendations
- Force multiplier effects by transforming signal measurement into precise and timely intelligence

Applications and use cases

- **Automatic Modulation Recognition (AMR)** – AI models identify the modulation scheme of an intercepted signal (e.g., QPSK, OFDM, FHSS) in milliseconds, even under noisy or jammed conditions.
- **Unknown Signal Discovery** – Machine learning detects and clusters never-before-seen waveforms, flagging potential new threats or covert communications.
- **Spectrum Occupancy Mapping** – Real-time heatmaps of spectrum usage help operators pinpoint hostile emitters, jammers, or unauthorized transmissions.
- **Adaptive Jamming Response** – AI-driven EW systems can recommend or execute countermeasures against enemy communications in real time.
- **Low-Probability-of-Intercept (LPI) Signal Detection** – Neural networks trained to recognize faint, hidden transmissions that evade traditional receivers.
- **Cognitive SIGINT Filtering** – Systems prioritize relevant intelligence based on mission context, ignoring benign civilian or irrelevant military signals.
- **Wideband Intercept & Search** – AI searches hundreds of MHz of spectrum at once, finding narrowband emitters buried in dense RF environments.
- **Multi-Standard Fusion Analysis** – Simultaneously decoding and correlating signals from different protocols (e.g., Wi-Fi, LTE, satellite) to track hybrid communication tactics.

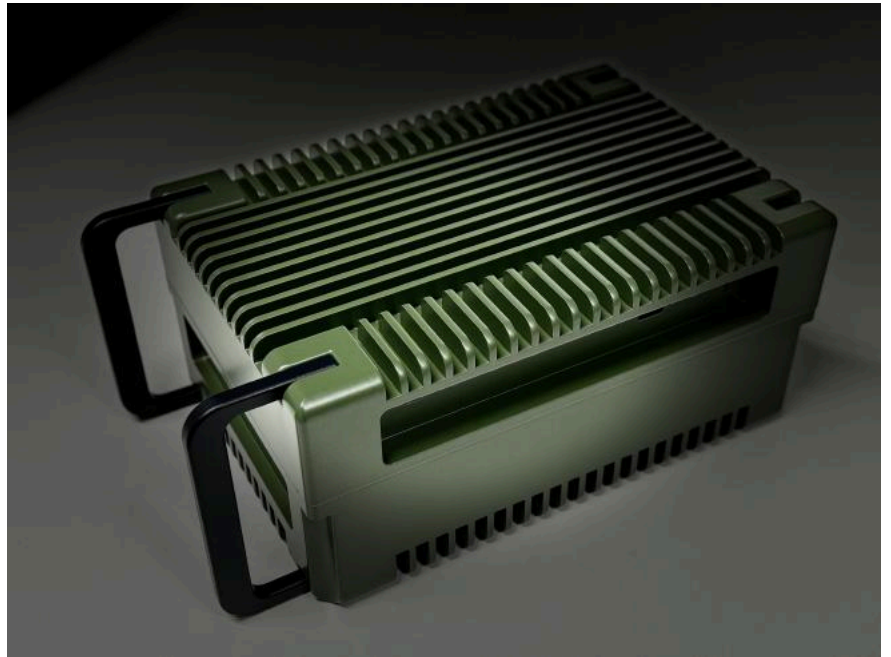
In contemporary Electronic Warfare (EW) and Signals Intelligence (SIGINT), Artificial Intelligence has shifted the operational model from reactive analysis to proactive, adaptive engagement. Modern AI systems leverage deep learning, pattern recognition, and anomaly detection to automatically process vast amounts of RF data in real time, identifying known and unknown signals across the entire electromagnetic spectrum.



Product Y9860A AI enabled Realtime-Spectrumanalyzer (RTSA)

The Y9860A is a high-performance state-of-the-art AI algorithm processing and deep learning inference hardware, perfectly developed for the combination with a modern Spectrum Analyzer board Anritsu MS27200A and using performant communication. The combination of an embedded graphics processing unit (CPU/GPU) enables real-time neural network signal (CNN) processing algorithms to be executed in software, with additional specialized signal analysis development.

The GPU is one of the most utilized processor type for machine learning, therefore the Y9860A significantly reduces the efforts for developers to create autonomous signal identification, modulation recognition, interference mitigation and many other machine learning applications for RF technologies.



Using a most performant CPU/GPU, the Y9860A is capable of analyzing an RF signal source and also generate IQ data files and reports. Thanks to the powerful AI capabilities of the integrated software, RF signals can be inspected in a very sophisticated modern way.

In one single box, the Y9860A includes numerous functions - such as interference recognition - and open source APIs. The system includes complete software packages and is based on a Linux UBUNTU operating system with drivers, FPGA firmware, and everything required for a professional operation. This system is the base for customer specific software developments.

The YOTASYS Y9860A is an innovative and modern solution for a performant portable setup for the capturing, analysis and reporting of RF signals. Based on the sophisticated IQ streaming streaming of MS27200A, this system expands the need of measuring and investigating RF signals up to 9 GHz (or higher) with unique features for the detection and analysis of unknown (or unwanted) signals in the RF space.

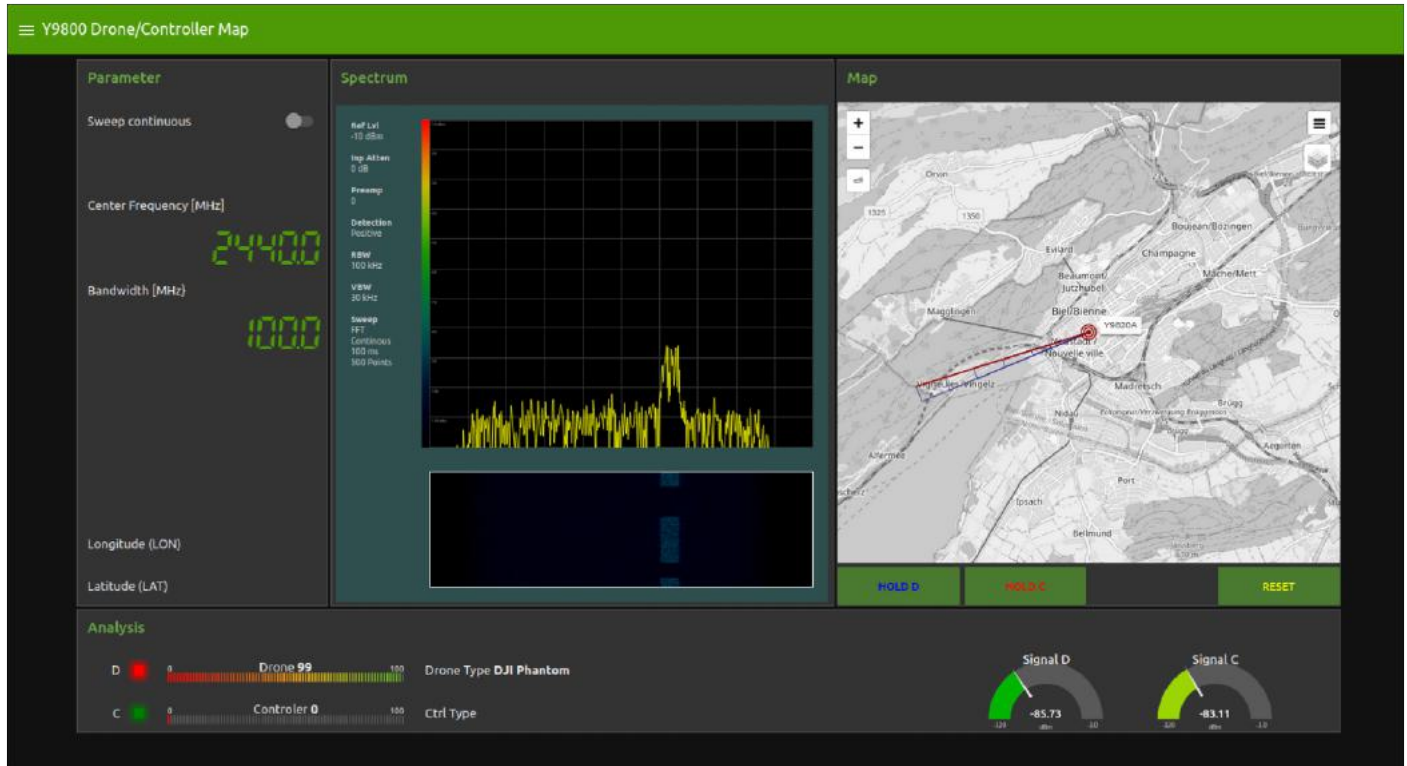
One single sensor Y9860A can cover a complete wide geographical area and the system will monitor a suspicious wireless signal activities.

This approach using the Y9860A enables applications such as automatic modulation recognition, detection of low-probability-of-intercept transmissions, spectrum occupancy mapping, and adaptive countermeasure planning.

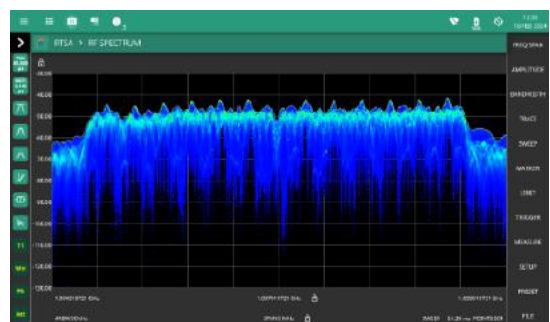
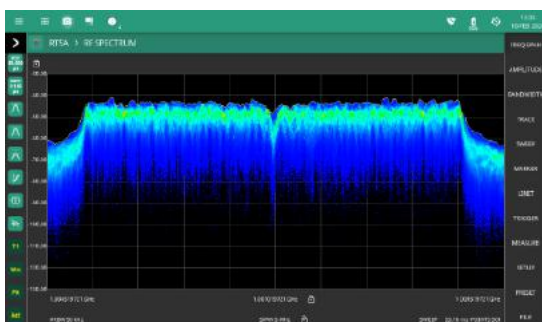
By integrating cognitive filtering and mission-context awareness, AI platforms can separate critical intelligence from background noise, dramatically reducing operator workload. The result is a faster detect-classify-respond cycle—delivering what is now known as cognitelligent solutions, where machine-speed analysis supports human decision-making in the most demanding spectrum environments.

Easy graphical user interface

The software of the Y9860A is flexible and modular, and can be tailored to customer specific needs. YOTASYS is offering the development of customer specific software and/or tools for fast prototyping and installation.



A web interface allows the enduser to operate and configure the Y9860A, using comprehensive and application-specific dashboard with charts, buttons, status LED and map information.



For **drone and controller detection**, the systems allows differentiation of even multiplexed and similar signals - these signals can be used to geographically isolate the emitters of the signal.

The system Y9860A can be easily integrated into existing radio monitoring solutions. The alarms can be tailored to specific interfaces such as HTTP, MQTT or SNMP.

Technical specifications

RF specifications (based on Y9860A)

Parameter	Value	Unit	Comment
Frequency range / bandwidth	9	kHz	RX lower frequency limit
	up to 54	GHz	RX upper frequency limit (see datasheet)
	2 .. 150	MHz	Realtime / IQ Bandwidth
Antennas	1		RX Antenna on front connector N(f) for <20GHz or K(f) for <43.5GHz and V(f) for <54GHz
Sampling rate	200	MSpS	ADC/DAC sample rate at 32bit resolution
Signal Bandwidth	0.036..150	MHz	
Bit resolution	8, 10, 16 or 32	bit	
Trigger source	Free run External 1/2 Video		
Capture Memory	2	GB	Internal at MS27200A
GNSS Antenna	1		RX Antenna on front connector SMA(f)

The RF specifications are depending on setup and configuration of Anritsu MS27200A.

Disclaimer

The specifications and instructions for our customers in this document reflect the product engineering level at the time of manufacturing. Please consider the valid data sheet release at a time. For questions please contact the YOTASYS customer service. YOTASYS AG accepts no liability for damages resulting from unprofessional installation or application or misuse for a purpose. This disclaimer also includes damages to third parties. It is the customer's responsibility to check the delivered products and immediately notify YOTASYS AG of detected faults. It is also the customer's responsibility to test the delivered product on its applicability for the intended purpose. YOTASYS AG will accept no liability or responsibility for their products if a product or a YOTASYS system is combined or used together with third-party products, i.e. products from other companies than YOTASYS AG. Jurisdiction in all legal disputes concerning product liability has the courts of the canton of Bern/Switzerland. Swiss law applies.

For more information and the newest data sheet releases go to: www.yotasys.com

YOTASYS AG

Aarbergstrasse 46
CH-2503 Biel/Bienne
Switzerland

www.yotasys.com
info@yotasys.com