

Testing Cognitive Radar Systems

SPONSORED CONTENT FROM [ROHDE & SCHWARZ](#)

ROHDE & SCHWARZ

Make ideas real



With today's emerging threats, traditional approaches to radar and electronic warfare (EW) systems that utilize static threat libraries are vulnerable to "mode-agile" or wartime reserve modes (WARM) threats operating in non-traditional modes. Use of a closed-loop integrated record, analysis & playback system (IRAPS)-based hardware-in-the-loop/software-in-the-loop (HIL/SIL) system is an excellent testbed to train, evaluate, and improve the artificial intelligence and machine learning (AI and ML) algorithms that are needed to implement the next generation of cognitive radar and EW systems and protect lives and assets against unknown threats.

A cognitive RF [radio frequency] system perceives the RF spectrum by converting that spectrum into a stream of RF data. Through reasoning and understanding of the context of the data stream, the system makes autonomous judgements and determines a course of action without human intervention. The end goal of the system is to deny the use of the RF spectrum by an adversary (electronic attack or EA), protect a platform, for instance by employing antijam techniques to protect a communications link (electronic protect, or EP) and/or delivering supporting information to another system (electronic support, or ES). A cognitive system uses a continuous feedback loop of situational perception, learning, reasoning, interaction, and action. (Figure 1.)

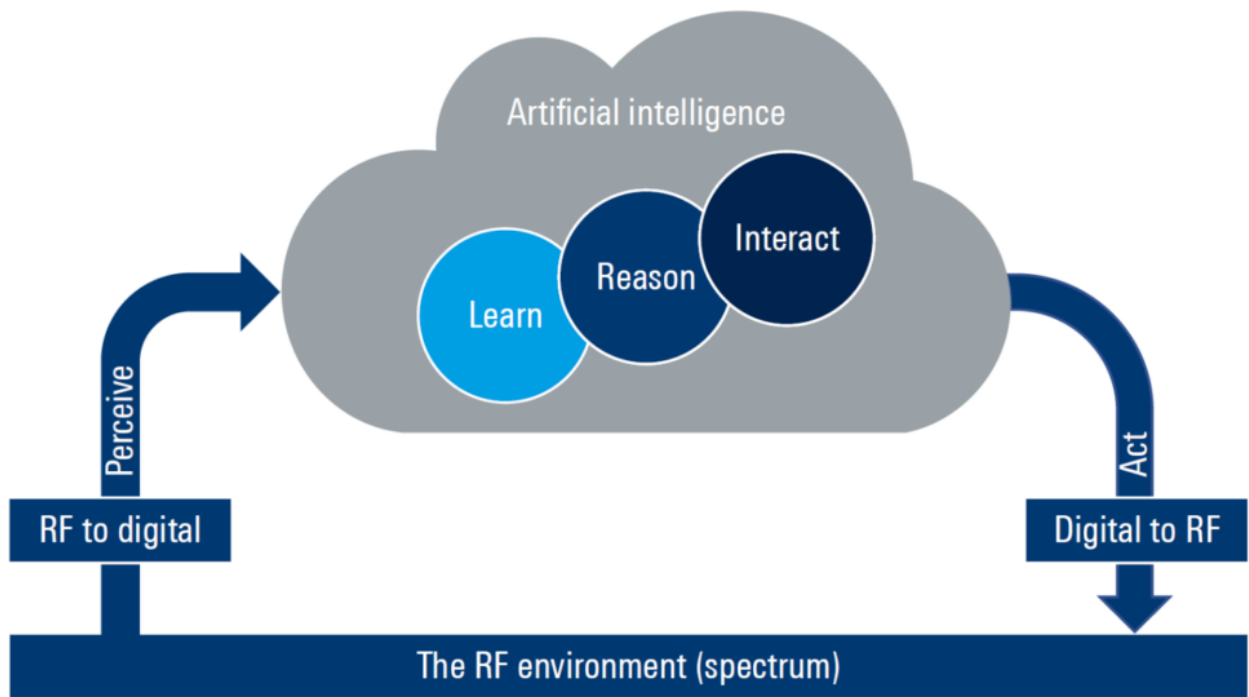


Fig. 1: Cognitive radar/electronic warfare (EW) system

With today's emerging threats, traditional approaches to radar and electronic warfare (EW) systems that use static threat libraries, as shown in Figure 2, are vulnerable to "mode-agile" or wartime reserve modes (WARM) threats operating in non-traditional modes. In a static-threat system, traditional threats such as an antimissile radar are characterized by their operating parameters, such as center frequency, occupied bandwidth, hopping characteristics, modulation, pulse repetition interval (PRI), and other parameters that are known, repetitive, and quantifiable. The static-threat library approach matches and classifies these parameters against a database. The classified threat may be converted into pulse descriptor words (PDWs) and fed to other systems on the platform, some of which may potentially deploy countermeasures.

WARM threats are signal characteristics and operating procedures that are held in reserve for wartime or emergency use and do not conform to the pre-defined parameters in a static threat library. These modes may include new operating frequencies, modulation techniques, pulse repetition intervals

and hopping schemas. A static threat technique cannot match WARM modes against the database, and the electronic protect, attack, and support (EP, EA, & ES) system consequently has no method to counter this threat. WARM modes are not seen outside of a serious conflict.

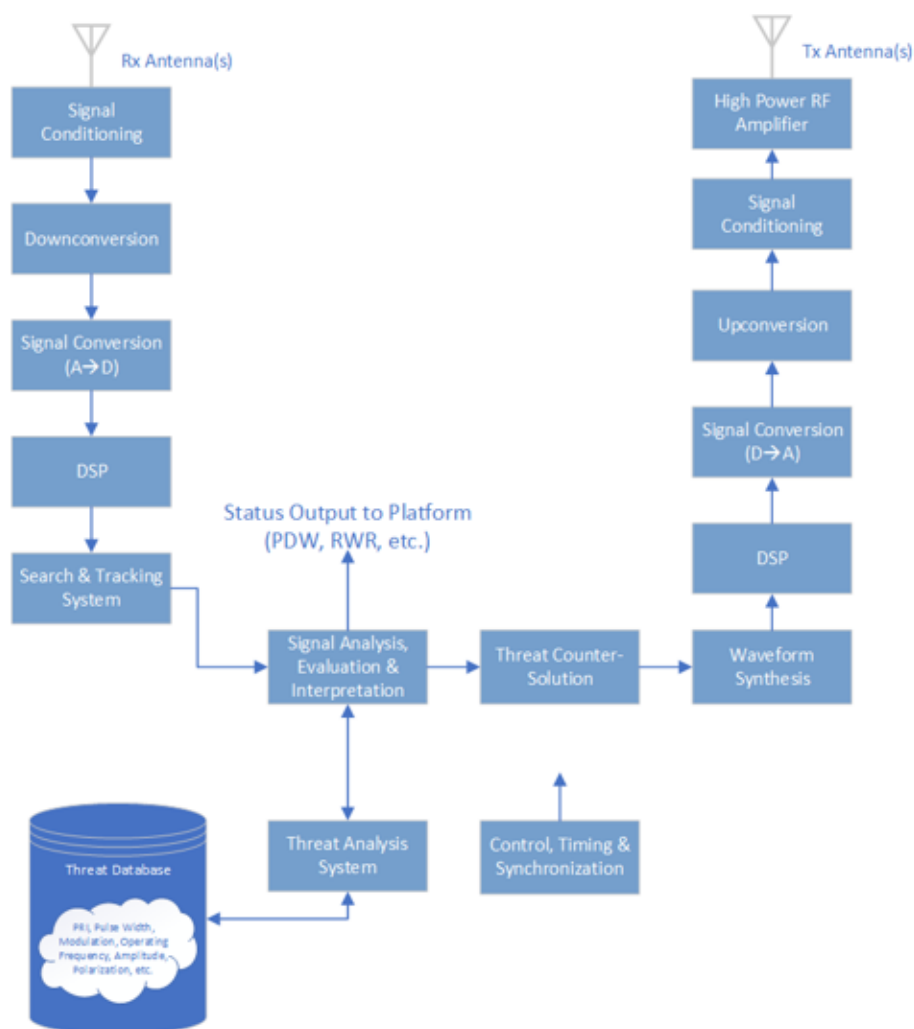


Fig 2: Traditional static-library radar/EW system

In a cognitive or adaptive radar/EW system, artificial intelligence (AI) and machine learning (ML) techniques are applied to the incoming spectrum to develop a counter to the perceived threat in the spectrum on the fly. It is entirely possible that a WARM threat may have the capability to detect that it has encountered a system that is using cognitive AI/ML techniques and may itself change its operating parameters, potentially on a continual basis. This requires flexibility to

quickly adapt to changing threats.

There are several challenges to the implementation of a cognitive radar/EW system:

1. Significant computational resources are required at the tactical edge where the threat is encountered. The computational resources may combine FPGA [field-programmable gate array] GPGPUs and multicore host processors to implement the AI/ML algorithms. On-platform compute elements must meet the often-harsh environments of in-theatre operating conditions.
2. An effective system needs to minimize the detect-to-counter time or RF-in to RF-out latency to improve platform survivability. This is a challenge to design and implement as GPGPU and COTS [commercial off-the-shelf] data converters are deeply pipelined, which adds to the system latency design budget.
3. By nature, WARM emitters may operate in unexpected frequency bands, hop across wider bandwidths, and use wideband modulation techniques. This mode of operation requires a wide bandwidth RF spectrum stare which has its own challenges in terms of system dynamic range and noise floor, which affect standoff, detection, and jamming range. Wider bandwidth requirements also complicate the task of data movement and processing.
4. A wideband cognitive AI/ML system uses more electrical power, which drives size, weight, power, and cost (SWaP-C) requirements – all of which must always be optimized on smaller autonomous platforms, such as an unmanned aerial system (UAS).
5. Mode-agile emitters may also be expected to enter “Low Probability of Intercept” modes, which require higher-resolution analog-to-digital converters (ADCs) and digital-to-analog converters (DACs).
6. Platforms need to be able to share information, which requires reliable communication links. They also need a

common time reference, such as GPS, to ensure spatial and temporal information used in direction-finding and geotagging of emitters. Traditional GPS is vulnerable to jamming, spoofing, and deception; assured position, navigation, and timing (PNT) needs to be part of a system-level solution.

Elements of a cognitive radar/EW system

A cognitive radar/EW system uses AI, which uses computer science to apply nonhuman intelligence to systems that emulate human reasoning and problem-solving skills. Common AI techniques used in ML are artificial neural networks, deep learning/deep neural networks, fuzzy logic, and genetic algorithms.

Figure 3 shows a block diagram of a cognitive radar/EW system. It is comprised of the following functional blocks:

- RF acquisition: The RF acquisition block converts the RF spectrum into a digital data stream. One or more antenna signals are routed to a signal-conditioning system that filters, amplifies and/or attenuates the signal to ensure maximum dynamic range. It is followed by downconversion and digitization with ADCs. The digital data may use DSP such as digital filtering, digital downconversion, resampling, demodulation, or digital beamforming.
- Search and tracking system: The search and tracking system continually monitors one or more frequency bands to determine angle of arrival (AoA) and emitter location.
- Core AI/ML system: The core AI/ML system consists of the AI analysis engine that determines key parametric information about the signals, such as PRI, pulse width, signal power, polarization time of arrival [ToA], and AoA. The core AI/ML system also includes data from other sensors such as electro-optic, navigation, missile

awareness, etc. This information is delivered to the threat library, giving an evolving view of the electronic battlefield and electronic order of battle; the library also contains previously identified signals of interest. The signal analysis and inferencing AI block determines whether identified signals are friendly emissions or potential threats by comparing the signals against the database. The AI support system is primarily used as a final decision arbiter for a proposed course of action and communicates the threat and the proposed action to the rest of the platform and operator. The AI-driven threat countersolution determines key parameters of the signal in multiple domains such as time, frequency, and amplitude, whether jamming, spoofing, or something else.

- Waveform synthesis: The waveform synthesis block interprets the output of the threat countersolution block and generates a digital stream representing the digital implementation of the counter.
- RF generation: The RF generation block is the opposite of the RF acquisition block. It consists of DSPs and DACs. The upconverter converts the baseband analog signal into an RF signal and is followed by signal conditioning such as filtering, attenuation, etc. The signal is amplified before transmission to ensure it has sufficient power to jam or deceive the threat.

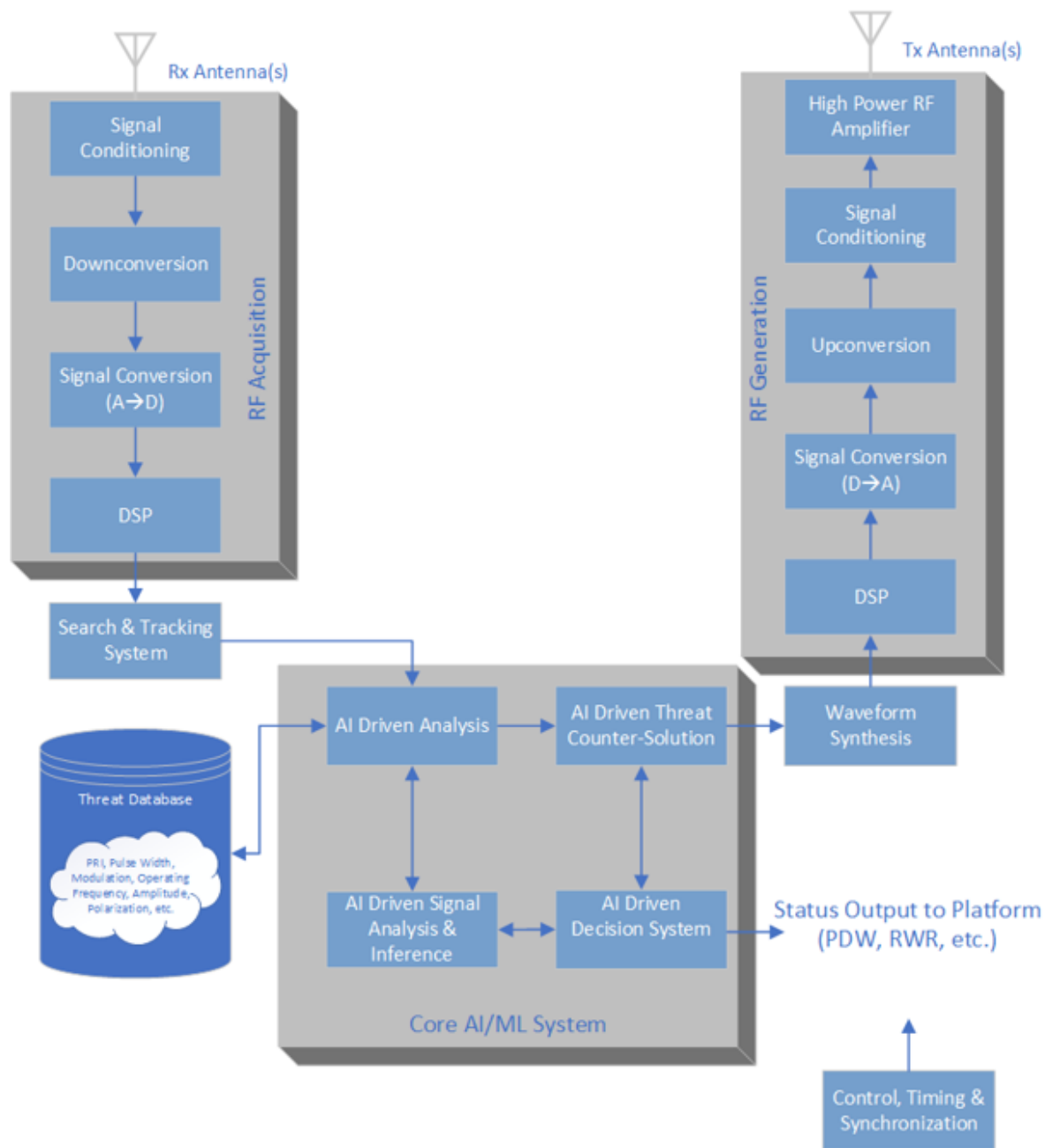


Fig 3: A block diagram lays out a cognitive radar/EW system.

Challenges in training cognitive radar/EW systems

AI techniques used in ML require rich training data. Training is the process of “feeding” the algorithms with representative sample sets of signals, analyzing the efficacy of the algorithm(s), modifying and improving the algorithm and repeating the training in a loop. This iterative process – known as RF hardware in the loop (RFHIL) – is long and therefore ideal for automation. RFHIL can be applied to initial algorithm development and evaluation; regression

testing; in reprogramming labs, where mission data sets are established in preparation for deployment in conflicted or contested environments; and at the operational level before mission execution to ensure the radar/EW systems are operational.

Acquisition of datasets

It is unlikely that a real-world collection would ever capture WARM signals. The collection process can still obtain valuable real-world signals that are useful in the hardware-in-the-loop/software-in-the-loop (HIL/SIL) lab as they contain representative signals complete with interference, poor signal-to-noise ratio, fading, multipath, and other aberrations. The AI/ML system can also be used to de-interleave and classify signals that are often difficult to discern in a complex real-world RF environment. The AI/ML system can be used to extract the signals of interest and save those as potential future training datasets.

Modeling and simulation (M&S) software such as Matlab, Simulink, R&S pulse sequencer and other commercially available software packages can be used to create training data sets. They enable almost infinite variations in the prototypes with the addition of interferers, noise, and other aberrations and foster the generation of complex scenarios such as multiple moving emitters in a low-risk, controlled laboratory environment.

Training the AI/ML system can be accomplished with an integrated record, analysis, and playback system (IRAPS). The heart of the IRAPS system is the ERISYS SigPro, which is a high-performance vector signal processor and server with between 8 and 64 cores, 8 x 256 GB of system memory, Gen-4 PCIe, bus, workstation graphics, and up to 60 TB of high-speed SSDs which can store thousands of training sets. The SigPro has 10 or 100 Gb Ethernet for fast movement of data. The SigPro includes a large FPGA development board for FPGA

algorithm prototyping and in-line DSP of the IQ data streams. The SigPro also coordinates system communication and configuration via Ethernet and stores the results of training runs for further analysis.

The vector signal generator used, the R&S SMW200A, generates the RF waveforms. It is connected to the SigPro via an optical QSFP+ connector, supporting up to 1 GHz of IQ data. The SMW can generate two independent RF signals, which could either be two RF signals played from the SigPro or one signal from the SigPro and one from the SMW's onboard memory, such as interference and commercial RF signals such as terrestrial TV, LTE, 5G, GNSS etc. These signals are amplified by a broadband amplifier.

After amplification, the RF signal is fed to the system under training (SUT). The SUT may receive RF either via a cabled interface or over the air (OTA) with antennas. If the system is using OTA testing, then an EMC [electromagnetic compatibility] chamber may be employed to ensure that RF emissions do not emanate outside of the chamber.

The generated RF response from the SUT, again either cabled or OTA, may need attenuation before acquisition by the vector signal and spectrum analyzer, which converts the 1 GHz of RF spectrum into an IQ data stream that is fed back to the SigPro. The tool can also be utilized for powerful radar-signal analysis with over 60 pulse and pulse train analysis capabilities including waveform independent timed-sidelobe measurements. The same tool can be used to validate the commercial RF signals in the electromagnetic environment. A multichannel oscilloscope may also be useful to capture the temporal and latency information from the system under test.

A closed-loop IRAPS-based HIL/SIL system is an excellent testbed to train, evaluate, and improve the AI/ML algorithms that are needed to implement the next generation of cognitive radar and EW systems and protect lives and assets against

unknown threats.

Authors:

Tim Fountain, RADAR & EW Market Segment Manager, Rohde & Schwarz

Leander Humbert, RADAR & EW Technology Manager, Rohde & Schwarz